Claves 48
Serie Claves del Gobierno Local

Las entidades locales frente al reto de la ciberseguridad

Directores: Luis FEIJOO GARCÍA
José Julio FERNÁNDEZ RODRÍGUEZ

Coordinador: Marcos ALMEIDA CERREDA

PRESENTACIÓN DE ALFREDO GALÁN GALÁN

Tamara ÁLVAREZ ROBLES
Noelia BETETOS AGRELO
Alexandre CASADEVALL PORTAS
Luis FEIJOO GARCÍA
José Julio FERNÁNDEZ RODRÍGUEZ
César FIEIRAS CEIDE
Miguel Á. LUBIÁN RUEDA
Icía MASID URBINA
Manfredi MATASSA
Fernando SUÁREZ LORENZO
Miguel TÚÑEZ LÓPEZ
Anxo VARELA HERNÁNDEZ

FUNDACIÓN DEMOCRACIA Y GOBIERNO LOCAL

Las entidades locales frente al reto de la ciberseguridad

Claves 48

Serie Claves del Gobierno Local

Las entidades locales frente al reto de la ciberseguridad

Directores: Luis FEIJOO GARCÍA
José Julio FERNÁNDEZ RODRÍGUEZ

Coordinador: Marcos ALMEIDA CERREDA

PRESENTACIÓN DE ALFREDO GALÁN GALÁN

Tamara ÁLVAREZ ROBLES
Noelia BETETOS AGRELO
Alexandre CASADEVALL PORTAS
Luis FEIJOO GARCÍA
José Julio FERNÁNDEZ RODRÍGUEZ
César FIEIRAS CEIDE
Miguel Á. LUBIÁN RUEDA
Icía MASID URBINA
Manfredi MATASSA
Fernando SUÁREZ LORENZO
Miguel TÚÑEZ LÓPEZ
Anxo VARELA HERNÁNDEZ

FUNDACIÓN
DEMOCRACIA
Y GOBIERNO LOCAL

Rambla de Catalunya, 126 - 08008 Barcelona
c/ Fernando el Santo 27, bajo A - 28010 Madrid
www.gobiernolocal.org

Corrección y revisión de textos: María Teresa Hernández Gil

Producción: Mailfactory, S.L.

Depósito legal: M-20452-2025
ISBN: 978-84-128852-8-6

Índice

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

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

PRESENTACIÓN

La ciberseguridad como oportunidad para el fortalecimiento de la democracia local

Alfredo Galán Galán
Director de la Fundación Democracia y Gobierno Local.
Catedrático de Derecho Administrativo de la Universidad de Barcelona

La digitalización ha revolucionado la forma en la que las personas interactuamos con el mundo que nos rodea, y los Gobiernos locales no han sido ajenos a esta transformación. La gestión electrónica de expedientes, la transparencia activa, la participación ciudadana inmediata y la prestación de servicios en línea a través de plataformas digitales, son solo algunos ejemplos de cómo la tecnología ha cambiado el modo de funcionar de las Administraciones locales.

Esta transformación, sin duda, ha mejorado la eficiencia, la accesibilidad y la calidad de los servicios públicos locales. No obstante, esta revolución digital también ha abierto las puertas a nuevas amenazas, en este caso, en el ámbito cibernético, que progresivamente, sin descanso ni tregua, se vuelven cada vez más complejas y sofisticadas. Los ciberataques pueden paralizar servicios esenciales, comprometer datos sensibles de ciudadanos y empresas, dañar la reputación de las instituciones, y, en última instancia, socavar la confianza en el sistema democrático.

Es por ello que la ciberseguridad ya no puede ser considerada como una cuestión de futuro ni un mero problema técnico, sino como un ele-

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

mento estratégico que debe ser integrado en la planificación, la gestión y la toma de decisiones de todas las áreas de los Gobiernos locales.

Por ello, la Fundación Democracia y Gobierno Local, consciente de esta realidad y fiel a su compromiso con el impulso de la modernización y mejora de la gestión de las Administraciones locales, ha promovido la elaboración de esta obra, con el objetivo de proporcionar a las entidades locales las herramientas y el conocimiento necesarios para hacer frente a este desafío. Obra que se inserta, por lo demás, en una creciente actividad de la Fundación de divulgación en la materia, a través de la organización de jornadas y otro tipo de publicaciones periódicas. En efecto, el año en que celebramos el centenario del Estatuto Provincial, uno después de conmemorar la misma efeméride en relación con el Estatuto Municipal, la Fundación, apegada siempre a la realidad, vuelve a centrar su atención en cuestiones de actualidad, como la ciberseguridad, que ni por asomo estaban entre las preocupaciones de los autores de aquellos venerables textos legales.

La ciberseguridad es un fenómeno complejo que requiere un enfoque multidisciplinar para ser comprendido y abordado de manera efectiva. Por ello, esta obra ha sido concebida por sus directores desde una perspectiva que integra diferentes áreas del conocimiento, tanto jurídico (derecho constitucional, administrativo y penal) como técnico (ingeniería informática) y sociológico (comunicación institucional). La Fundación, consciente de la importancia de la formación y el perfeccionamiento de los responsables públicos en este campo, ha reunido a un equipo de expertos de sólida trayectoria y de reconocido prestigio para elaborar este trabajo: profesores universitarios y técnicos de la Administración y del sector privado. Todos ellos han aunado sus conocimientos y sus experiencias para ofrecer una visión completa y rigurosa de la ciberseguridad en el ámbito local. De modo que, a lo largo de diez capítulos, se analizan los aspectos más relevantes de la ciberseguridad desde una óptica plural y especializada. Esta diversidad de voces, sin sombra de duda, enriquece el debate abierto en diferentes foros académicos y profesionales, y permite ofrecer una visión más completa y matizada de los desafíos y oportunidades que plantea la ciberseguridad para las entidades locales.

Hay que destacar que, más allá del análisis teórico y normativo, esta obra se distingue por su enfoque práctico y orientado a resultados. Se exponen, de modo claro y estructurado, las lecciones aprendidas, a partir de

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

incidentes reales, y se realizan propuestas operativas para mejorar la resiliencia digital de las entidades locales para hacer frente a los desafíos de la ciberseguridad. Su objetivo es proporcionar a las entidades locales criterios, modelos y experiencias para afrontar el riesgo cibernético en un contexto de recursos limitados, ofreciendo soluciones innovadoras y adaptadas a las necesidades específicas de cada entidad.

La obra que el lector tiene en sus manos, en definitiva, es una invitación a la reflexión y a la acción. Una invitación a que los responsables públicos locales tomen conciencia de la importancia de la ciberseguridad y se comprometan a adoptar las medidas necesarias para proteger sus sistemas, sus datos y a sus ciudadanos. Tal y como señalan sus directores, este libro invita a mirar la ciberseguridad no como un obstáculo, sino como una oportunidad para fortalecer nuestras democracias locales en una época de creciente complejidad digital. La Fundación Democracia y Gobierno Local, al poner a disposición de las Administraciones locales esta herramienta, reafirma su compromiso con la construcción de un futuro digital más seguro, inclusivo y democrático, en el que los derechos de los ciudadanos estén protegidos y las instituciones públicas gocen de la confianza de la ciudadanía.

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

PRÓLOGO

Luis Feijoo García
Funcionario de carrera del Cuerpo Superior de Técnicos de Administración Local.
Asesor jurídico de Administración Electrónica, Transparencia y Protección de Datos en la Diputación de Pontevedra

José Julio Fernández Rodríguez
Catedrático de Derecho Constitucional.
Universidad de Santiago de Compostela

Vivimos en una época en la que los sistemas digitales son ya el tejido invisible que sostiene gran parte del funcionamiento de nuestras instituciones públicas. La información, los datos y las herramientas tecnológicas ya constituyen elementos esenciales del funcionamiento institucional, lo que convierte a la ciberseguridad en un eje estratégico de la acción pública.

Las entidades locales, por ser la Administración más cercana a la ciudadanía, desempeñan un papel esencial en la prestación de servicios, en la gestión del territorio y en la salvaguarda de derechos fundamentales. Sin embargo, este papel se encuentra hoy más amenazado que nunca por un fenómeno transversal y complejo: la ciberseguridad. De esta forma, tales entidades enfrentan un escenario especialmente desafiante: por un lado, deben garantizar la continuidad, calidad y seguridad de los servicios que prestan a la ciudadanía; por otro, lo hacen con recursos limitados y en un entorno cada vez más expuesto a amenazas tecnológicas sofisticadas y persistentes.

La digitalización de los servicios públicos ha traído consigo avances innegables en eficiencia, accesibilidad y transparencia, pero también ha abierto nuevas puertas a riesgos inéditos. Los ciberataques a ayuntamientos y diputaciones no son ya escenarios hipotéticos o anecdóticos; son realidades frecuentes que pueden paralizar servicios básicos, comprometer datos personales o incluso socavar la confianza ciudadana en las instituciones democráticas.

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

Este libro nace precisamente de la urgencia de afrontar este nuevo paradigma. Intentamos responder con acierto a una necesidad creciente de las Administraciones locales españolas, que se concreta en la exigencia de disponer de herramientas, conocimientos, marcos normativos y buenas prácticas que les permitan enfrentar los desafíos del ciberespacio desde una perspectiva integral, operativa y alineada con los valores constitucionales. El volumen parte de una convicción central: la ciberseguridad no puede entenderse solo como una cuestión técnica o informática. Es, ante todo, una cuestión de gobernanza pública, de protección de derechos fundamentales, de garantía del interés general y de legitimidad democrática. La protección de los datos personales, la integridad de los sistemas municipales, la capacidad de respuesta ante incidentes y la preservación de la confianza ciudadana no son aspectos secundarios, forman parte de la esencia del servicio público del siglo XXI.

A lo largo de sus capítulos, el lector encontrará un análisis riguroso, multidisciplinar y estructurado de los principales desafíos, normativas, estrategias y herramientas que configuran el mapa actual de la ciberseguridad en el ámbito local. Ofrecemos diez capítulos con los que se trata de hacer este recorrido general por la problemática objeto de estudio, con una visión multidisciplinar y práctica, estructurada con claridad y escrita por autoras y autores de sólida trayectoria académica, técnica y jurídica.

La obra se abre con una reflexión necesaria sobre el papel de la ciberseguridad como garantía del servicio público y de los derechos fundamentales, a cargo de José Julio Fernández Rodríguez y Tamara Álvarez Robles, quienes abordan la dimensión preferentemente constitucional del problema, vinculando seguridad digital, derechos fundamentales y Estado de derecho. El avance tecnológico ha creado nuevas amenazas para las Administraciones públicas locales, que manejan datos sensibles y prestan servicios esenciales. La ciberseguridad se presenta, entonces, como clave para garantizar derechos como la privacidad, la participación política y el acceso a servicios. Sin embargo, los ciberataques se suceden, y su prevención se dificulta por obstáculos como la falta de recursos, personal poco cualificado y ausencia de formación. El capítulo propone una estrategia integral basada en prevención, formación, cooperación y cumplimiento normativo. Concluye que las entidades locales deben asumir un rol proactivo en ciberseguridad para proteger derechos y asegurar la prestación continua de sus servicios en un entorno digital cada vez más complejo.

A esta primera aportación le siguen dos análisis detallados de los marcos normativos europeo y español, de la mano de Manfredi Matassa y Anxo

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

Varela, lo que permite entender el contexto regulatorio en el que deben operar las entidades locales, lo que debe ser siempre el parámetro básico de referencia. Así, se incluyen instrumentos clave como la Directiva NIS II, el Reglamento ENISA, la Estrategia Nacional de Ciberseguridad o el Esquema Nacional de Seguridad. La Directiva NIS2 refuerza y amplía las obligaciones en materia de gestión de riesgos, notificación de incidentes, supervisión y sanciones, e incluye tanto a entidades esenciales (como infraestructuras críticas) como a importantes (como proveedores de servicios digitales). Se evidencia que la UE avanza hacia una ciberseguridad colectiva y cooperativa, aunque enfrenta retos estructurales y políticos, especialmente en relación con la soberanía estatal en materia de seguridad nacional. Con relación a España, se muestra la ciberseguridad como un pilar estratégico para el Estado de derecho en nuestro país, enfocándose en su impacto en las Administraciones locales. Destaca la necesidad de una ciberseguridad integral ante la digitalización creciente y el aumento de ciberataques. Ese capítulo III también subraya la inclusión de la ciberseguridad en la Ley de Seguridad Nacional, y la relevancia del Esquema Nacional de Seguridad para las Administraciones públicas. Finalmente, enfatiza la importancia de la cooperación público-privada, la descentralización y la responsabilidad compartida para un sistema nacional de ciberseguridad resiliente.

A continuación, en el capítulo IV, dedicado a analizar incidentes reales, Noelia Betetos extrae lecciones prácticas a partir de los informes de órganos de control, subrayando las debilidades detectadas y las áreas de mejora, valiosas para cualquier gestor público local. Así, aborda los ciberataques en las Administraciones locales españolas, destacando la falta de un registro exhaustivo de incidentes, al tiempo que describe los ataques más comunes: *ransomware*, denegación de servicio y suplantación de identidad. El estudio también evalúa el nivel de madurez y resiliencia en ciberseguridad de las entidades locales, basándose en auditorías que miden el cumplimiento del Esquema Nacional de Seguridad, para lo cual se examinan ocho parámetros clave. De esta forma, se señalan deficiencias en personal y políticas, y se proponen mejoras, destacando iniciativas de éxito como el modelo valenciano de ciberseguridad.

A esto se suma la aportación, en el capítulo V, de Icía Masid en el terreno más técnico, con una mirada hacia el presente y futuro de las herramientas de ciberdefensa y la aplicación de inteligencia artificial. En este sentido, la IA está transformando la ciberseguridad, siendo usada por atacantes para sofisticar sus métodos y por defensores para reforzar las defensas, especialmente en Administraciones locales. El documento detalla ciberataques comunes y cómo la IA, mediante la detección de patrones,

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

clasificación, automatización y procesamiento del lenguaje natural, puede mejorar la detección y respuesta a amenazas. La implementación de la IA ofrece beneficios como reducción de incidentes, mayor protección de datos y eficiencia operativa, siendo crucial para la seguridad y confianza ciudadana. Además, se ofrecen directrices para su implementación efectiva.

El cumplimiento normativo —y en particular del Esquema Nacional de Seguridad (ENS)— constituye otro eje clave del libro, abordado con claridad por Miguel Á. Lubián. El punto de vista prioritario es ese cumplimiento por parte de los Gobiernos locales, tanto grandes como pequeños, explorando marcos de certificación y estructuras de apoyo. De este modo, analiza cómo el Centro Criptológico Nacional ayuda a las Administraciones locales españolas a cumplir con el Esquema Nacional de Seguridad mediante los perfiles de cumplimiento específicos. Se detalla el proceso de adecuación a dicho esquema y la categorización de sistemas. A pesar de los citados "perfiles", el cumplimiento sigue siendo bajo, aunque se destaca el papel de los Gobiernos intermedios para mejorarlo y la futura influencia de la Directiva NIS2.

Este análisis se complementa en el capítulo VII con una perspectiva organizativa y de gobernanza, presentada por Luis Feijoo, que nos recuerda que la ciberseguridad no es solo una cuestión tecnológica, sino también política, administrativa y cultural. El capítulo aborda la ciberseguridad como un elemento clave de la gobernanza pública ante la dependencia digital. Se destaca la necesidad de políticas de protección de la información y cumplimiento normativo, y se definen la gobernanza y los modelos sectoriales, enfatizando la importancia de roles determinados (responsables de información, servicio, seguridad, sistema, comité de seguridad, delegado de protección de datos) y principios como la claridad de roles, la estrategia continua y la cultura de ciberresiliencia para una gobernanza de ciberseguridad eficaz en las Administraciones locales. Finalmente, el documento propone principios para una gobernanza de ciberseguridad sostenible, como la claridad de roles, estrategia continua, escalabilidad, integración de riesgos y una cultura de ciberresiliencia.

Fernando Suárez completa esta mirada organizativa en el capítulo VIII con una propuesta sistematizada de actuación ante ciberataques. En efecto, el trabajo analiza la vulnerabilidad de las Administraciones locales españolas ante ciberataques, y propone un marco de respuesta basado en el ciclo de vida de la ciberseguridad (identificar, proteger, detectar, responder, recuperar), enfatizando la preparación, las políticas de ciberseguridad municipal, la protección de infraestructuras críticas y la colaboración con organismos especializados. Además, detalla las fases de actuación (detección, contención,

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

investigación, recuperación, aprendizaje) y la necesidad de una comunicación transparente, con el objetivo de mejorar la resiliencia municipal.

Asimismo, el libro no descuida un aspecto crucial muchas veces olvidado como es la comunicación institucional en situaciones de crisis cibernética. Los profesores Fieiras Ceide y Túñez López ofrecen en el capítulo IX orientaciones sobre cómo preparar, gestionar y comunicar adecuadamente un incidente, teniendo en cuenta la sensibilidad pública, la imagen institucional y la necesidad de mantener informada a la ciudadanía sin generar alarma ni ocultar información. En este orden de cosas se evidencia que la comunicación preventiva es crucial para gestionar crisis y proteger la reputación de una organización. Ello requiere un plan detallado y ensayado previamente, ya que la improvisación es ineficaz. El proceso incluye fases de precrisis (planificación), crisis (ejecución) y postcrisis (evaluación), donde la honestidad y la transparencia son clave. Ante un ciberataque, se aplican los mismos principios, adaptando las respuestas a la velocidad de propagación de la información en el ciberespacio.

Cierra este interesante volumen el capítulo X, de Alexandre Casadevall, centrado en el papel del derecho penal como herramienta de tutela frente a los ciberdelitos, en donde se recogen las nuevas formas de criminalidad en el entorno digital, incluyendo el ciberterrorismo y los ataques a infraestructuras críticas. Examina la función del derecho penal en la protección del ciberespacio. Subraya la creciente expansión de la ciberdelincuencia, con un aumento del 26 % de delitos informáticos en España entre 2022 y 2023, y una preocupante disminución en el porcentaje de esclarecimiento. Se destaca la necesidad de cooperación internacional y se examinan ciberdelitos específicos del Código Penal español que atacan la confidencialidad, integridad y disponibilidad de sistemas informáticos, como el acceso ilegal, interceptación, daños informáticos y estafas.

Estos capítulos finales denotan que la obra se ha construido con la intención de proporcionar una visión integral en el objeto de estudio, que va desde la prevención hasta la reacción y la sanción. Se intenta reflejar en todo momento que las amenazas a la ciberseguridad en el ámbito local no son un riesgo abstracto ni futurista, sino una realidad tangible que exige planificación, conocimiento y compromiso. No se trata de crear barreras tecnológicas inabordables, sino de fomentar una cultura de la ciberseguridad pública, basada en la anticipación, la responsabilidad compartida y la cooperación institucional. Así las cosas, el presente libro constituye una aportación actual, rigurosa y necesaria para todos aquellos responsables públicos que desempeñan sus funciones en el ámbito local, ya sean car-

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

gos electos, técnicos municipales, responsables de servicios informáticos o personal jurídico-administrativo. También resulta de interés, sin duda, para operadores jurídicos, expertos en gobernanza y académicos interesados en los procesos de transformación digital del sector público.

Por todo ello, vemos cómo esta obra representa una contribución valiosa y necesaria en un momento como el actual. No es solo un libro técnico o normativo, es una llamada a reforzar nuestras instituciones en un tiempo de incertidumbre digital, y a tomar conciencia de que la protección del ciberespacio público es parte de la protección de lo común. Todos/as los/as autores/as hemos trabajado con esa visión horizontal anclada en la creciente relevancia del tema y de la problemática que genera la ciberseguridad, lo que determinará el éxito o el fracaso de las políticas públicas y la participación o desafección ciudadana.

La ciberseguridad no debe entenderse como una meta estática, sino como un proceso continuo de mejora, aprendizaje y adaptación. Y en ese camino, es fundamental implicar a todos los actores: responsables políticos, técnicos municipales, empresas proveedoras de servicios tecnológicos y, por supuesto, la ciudadanía. Porque la seguridad digital, al igual que ocurre con la seguridad ciudadana, es un bien común que solo puede garantizarse desde la corresponsabilidad y la cooperación. Proteger nuestros sistemas no es solo proteger datos, es también proteger derechos, garantizar servicios esenciales y asegurar la estabilidad de nuestra democracia desde sus raíces más próximas. La ciberseguridad en las entidades locales no es un reto del futuro; es una urgencia del presente.

En definitiva, este libro invita a mirar la ciberseguridad no como un obstáculo, sino como una oportunidad para fortalecer nuestras democracias locales en una época de creciente complejidad digital. Solo con Administraciones preparadas, informadas y coordinadas podremos garantizar a la ciudadanía el pleno ejercicio de sus derechos en el entorno digital, y preservar la legitimidad del poder público en el siglo XXI.

No olvidemos que nos hallamos ante un desafío colectivo que requiere planificación, formación, inversión y, sobre todo, conciencia institucional. Los responsables de nuestras entidades locales deben estar a la altura del desafío tecnológico que se alza ante sus instituciones. La ciudadanía, por otra parte, así se lo reclamará cada vez con más intensidad. Si algo demuestra esta obra es que las respuestas existen, pero deben activarse desde el conocimiento, la sensibilización y la cooperación. Este libro es ciertamente un paso firme en esa dirección. Pasen a descubrirlo.

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

CAPÍTULO I

La ciberseguridad como garantía de la continuidad de las funciones y servicios públicos locales en el mundo tecnológico

José Julio Fernández Rodríguez
Catedrático de Derecho Constitucional.
Universidad de Santiago de Compostela

Tamara Álvarez Robles
Prof.ª Permanente Laboral de Derecho Constitucional.
Universidad de León

1. Introducción

Es posible que muchos de los lectores no estén familiarizados con la historia de los primeros virus informáticos Creeper o Wabbit, en los años setenta del pasado siglo, ni con uno de los primeros *softwares* dañinos, conocido como gusano Morris, de finales de los años ochenta (Rodríguez, 2023). Empero, es probable que hayan leído o escuchado hablar de los *ransomware* Petya (2016) y WannaCry (2017) debido a la atención mediática que recibieron y al impacto que tuvieron en las Administraciones públicas y en las empresas, en una época en la cual los Estados ya habían iniciado su transición digital. Seguramente sean conocedores de la caída

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

que sufrió Microsoft a consecuencia de un fallo de seguridad de uno de sus proveedores, CrowdStrike, en julio de 2024, ampliamente difundida no solo por la repercusión en los medios de comunicación, sino preeminentemente por la paralización de los servicios públicos y privados a nivel mundial. A pesar de que la ciudadanía no está familiarizada con los nombres de estos virus —troyanos, *ransomware* y demás tipos de *malware*—, somos plenamente conscientes de los efectos perjudiciales que tienen en nuestro día a día. La ciberseguridad se configura, así, como una de las categorías esenciales para conseguir el progreso individual, social e institucional.

Sin duda, nos hallamos en un mundo convulso e incierto, en el cual el inusitado desarrollo tecnológico de las últimas décadas ha incidido en todos los órdenes de nuestra vida. Se ha conformado una nueva sociedad, la denominada "sociedad de la información", aunque también podríamos rotularla como "sociedad tecnológica", en la que ya nada será como antes. Incluso podemos hablar en la actualidad de un segundo momento de la sociedad de la información, determinado por el auge de las tecnologías disruptivas, como la inteligencia artificial, la computación en nube, el *blockchain*, la impresión 3D, la robótica, el 5G o, incluso, la computación cuántica. Un escenario abierto que justifica la incertidumbre a la que nos referíamos antes.

Debemos tener en cuenta que la tecnología es ambivalente y dicotómica, en el sentido de que presenta tanto elementos positivos como negativos. En el lado favorable encontramos, por ejemplo, las enormes posibilidades para la comunicación, el ocio y el comercio electrónico. En el lado negativo podemos situar las amenazas a la privacidad, la manipulación informativa, la ciberdelincuencia, el aislacionismo social o la banalización de la información. Esta realidad enfatiza la importancia de las cuestiones de ciberseguridad[1].

1. Usamos un entendimiento amplio de ciberseguridad, como las acciones, métodos e instrumentos para garantizar en soportes tecnológicos la confidencialidad, integridad, disponibilidad y autenticación de la información y de los servicios (seguridad en el mundo digital) (Fernández Rodríguez, 2018: 53). Sin embargo, hay conceptos más específicos, en los que la ciberseguridad se enfoca más en la protección de datos y sistemas interconectados, mientras que el concepto de seguridad de la información aborda un enfoque más holístico, incluyendo la gestión integral de la información y sus riesgos (Álvarez Robles, 2024a: 268). Aun así, optamos por dicha visión amplia: "La ciberseguridad será la seguridad del Estado tecnológico y del Estado tecnológico-digital. De este modo, atenderemos a una conceptualización de ciberseguridad integral (que va desde el Estado y sus Administraciones hasta los ciudadanos y empresas), transversal (que se proyecta en el sistema normativo, en las políticas públicas, en las normas técnicas, etc.) y descentralizada (en una visión internacional, supranacional [nacional] e infraestatal, con los principios de cooperación y colaboración como pilaras); a una ciberseguridad

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

Como se ve, el tema resulta esencial, por lo que los poderes públicos deben prestarle la suficiente atención, con el ánimo de apoyar elementos positivos de la tecnología y mitigar los aspectos negativos. Sorprende que a veces los responsables públicos no muestren interés por esta problemática, ni la conozcan en sus elementos nucleares, ni sean conscientes de que cada vez presentará mayor trascendencia. En el ámbito local resulta incuestionable cómo la ciberseguridad debe situarse en la parte prioritaria de su agenda.

Podemos considerar que los ciberataques que sufrió Estonia entre el 27 de abril y el 18 de mayo de 2007 simbolizan el antes y el después de la ciberseguridad. Estos ciberataques tuvieron un profundo impacto en el normal funcionamiento del Estado estonio, de sus Administraciones y empresas, y en la vida cotidiana de sus ciudadanos. Estaban dirigidos contra los sistemas informáticos públicos y privados, y provocaron la disrupción y el bloqueo de las páginas web del Ejecutivo, del Legislativo, de distintas Administraciones, así como de los sistemas bancarios y medios de comunicación. Este suceso representó un punto de inflexión en la ciberseguridad, tanto del propio Estado estonio como a nivel supranacional —de la Unión europea— e internacional, con la implicación de la OTAN. A partir de ese momento la seguridad de la información evolucionaría hacia la ciberseguridad, ampliando sus horizontes más allá del ámbito estatal. Dentro del Estado se fortalecerían las capacidades de las Administraciones y empresas estratégicas y críticas, con el objetivo de garantizar la protección integral, y de continuar con las funciones y los servicios públicos frente a las ciberamenazas (Liga de Ciberdefensa de Estonia). A nivel internacional cobrarían fuerza los principios de cooperación y coordinación en la Unión Europea (Agencia de la Unión Europea para la Ciberseguridad) y en la OTAN (revisión del art. 5 del Tratado y Centro Integrado de Ciberdefensa).

En España, el incidente estonio, unido al incremento del 55 % en los ataques que se comenzaban a producir en los últimos años (CCN-CERT, *Principales Amenazas y Tendencias de la Seguridad Cibernética*, 2007)[2],

público-privada centrada en los sistemas de información, en y del ciberespacio (*security and safety)* y en los ciudadanos, cultura de ciberseguridad" (Álvarez Robles, 2024a: 269). En todo caso, el fin que ha de perseguir cualquiera de las acepciones de ciberseguridad, para ser continuista y evolutiva del concepto de seguridad, es la salvaguarda de los derechos y libertades, esto es, una ciberseguridad humanista.

2. https://www.ccn-cert.cni.es/es/comunicacion-eventos/comunicados-ccn-cert/1910-las-amenazas-y-vulnerabilidades-sobre-los-sistemas-de-informacion-se-incrementaron-un-55.html (fecha de última consulta: 01/12/2024).

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

contribuyó a impulsar la creación de instituciones encargadas de velar por la ciberseguridad (Centro Nacional de Inteligencia, 2002; Centro Criptológico Nacional, 2004; CCN-CERT, 2006, y Consejo Nacional de Ciberseguridad, 2018), a legislar sobre protección de infraestructuras críticas (Ley 8/2011, de 28 de abril, de Protección de Infraestructuras Críticas) o sobre la conservación de datos (Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones), y a desarrollar estrategias de ciberseguridad (por ejemplo, Estrategia de Ciberseguridad Nacional 2013 y Estrategia Nacional de Ciberseguridad 2019).

Los ejemplos antedichos nos muestran una creciente preocupación por la seguridad, ciberseguridad, resiliencia y ciberresiliencia (DSN, *La Resiliencia en el Marco de la Seguridad Nacional*, 2024)[3], máxime cuando somos conocedores de que los fallos de seguridad y los ciberataques han evolucionado en cuanto a técnicas, métodos y actores implicados, y han aumentado en impacto a lo largo de los años (intensificándose en la pandemia de la COVID-19, según el Informe *Ciberamenazas y Tendencias*, edición 2020, del CCN-CERT)[4].

Estos ciberataques y fallos de seguridad nos hacen ser cada vez más conscientes de la interdependencia que tienen los sistemas y las sociedades (incluidas Administraciones), y han puesto de relieve el papel crucial del factor tiempo, tanto en la rápida propagación de estos eventos como en la urgencia de resolución de los mismos. Por ello, es primordial desarrollar una ciberseguridad que, además de proteger las infraestructuras críticas y estratégicas, se centre en los derechos de las personas y garantice una relación pacífica y armoniosa con las Administraciones públicas; una ciberseguridad que trascienda la visión tradicional que opone la Administración pública a la ciudadanía y que permita crear una verdadera cultura de ciberseguridad. A este relevante fin se dedica este capítulo.

En todo caso, vivimos tiempos de incertidumbre con relación al futuro, y también de cambios, que a nivel normativo, en el campo de la tecnología y ciberseguridad, provienen sobre todo de la Unión Europea (UE). La UE ha aprobado en los últimos años distintas normas que inciden en lo que estamos comentando de una forma u otra, aunque en términos de ciberseguridad debemos citar la Directiva UE 2022/2555, de 14 de di-

3. https://www.dsn.gob.es/sites/dsn/files/Resiliencia%20marco%20SN.pdf (fecha de última consulta: 25/10/2024).

4. https://www.ospi.es/export/sites/ospi/documents/documentos/Informe-Ciberamenazas-Tendencias_2020.pdf (consulta en diciembre 2024).

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

ciembre, relativa a las medidas destinadas a garantizar un elevado nivel de ciberseguridad en toda la Unión (es la que se denomina Directiva NIS 2). Esta directiva debe ser transpuesta, lo que ha llevado a España a tener, en enero de 2025, un anteproyecto de ley de coordinación y gobernanza de la ciberseguridad[5].

2. La Administración local ante el mundo tecnológico: su papel central

2.1. La realidad de las amenazas y la necesidad de respuesta

Estonia fue, como mencionamos antes, el ejemplo más claro de cómo un Estado podía paralizar su normal funcionamiento por ciberataques coordinados. En este orden de cosas, y con relación a España, conviene señalar que desde el año 2006 el CCN-CERT ha asumido la gestión de más de 30 000 incidentes catalogados con un nivel de peligrosidad crítico o muy alto. Además, ha detectado 28 177 vulnerabilidades críticas con impacto en la seguridad de las tecnologías empleadas en el sector público; en la última década el número de incidentes gestionados anualmente por este organismo se ha incrementado un 1384,7 % (CCN-CERT, 23 de abril de 2024)[6]. A este número habría que sumar los ciberataques a empresas y otros organismos gestionados por el INCIBE-CERT y, en el marco de defensa, por el DEF-CERT, para tener un panorama completo.

El *ransomware* es el protagonista de gran parte de los ciberataques a entidades locales en estos últimos años. Así, podemos referirnos al troyano Emotet (especializado en el robo de datos financieros) en conjunción con el *ransomware* Ryuk, que afectó al Ayuntamiento de Jerez de la Frontera en octubre 2019[7] y cifró los archivos alojados en más de 50 servidores informáticos, paralizando, de este modo, los servicios del propio ayun-

5. La citada Directiva 2022/2555 (conocida con NIS 2) se aplica a las Administraciones públicas centrales y regionales (art. 2.2.f), aunque también deja la puerta abierta a los Estados para que amplíen esta previsión a la Administración local (art. 2.5.a). En el anteproyecto español de transposición que se conoce en febrero de 2025 no se realiza tal posibilidad (en su anexo 1, punto 10, las entidades de la Administración pública son tan solo las centrales y regionales). Este anteproyecto se puede consultar en 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.

6. https://www.ccn-cert.cni.es/es/seguridad-al-dia/actualidad-ccn/12943-el-centro-criptologico-nacional-ha-gestionado-mas-de-30-000-ciberincidentes-de-peligrosidad-muy-alta-y-critica-en-sus-20-anos-de-trayectoria.html#:~:text=El%20pasado%20a%C3%B1o%2C%20el%20CCN,incrementado%20un%201.384%2C7%25 (última consulta: 01/12/2024).

7. Este *ransomware* sería el introducido en el Servicio Público de Empleo Estatal-SEPE en 2021. Recordemos que tres meses más tarde se produjo un ciberataque a distintas secciones

tamiento junto a otros servicios públicos dependientes de este. En esa época fuimos testigos de sucesos similares: en noviembre de 2019 se vería afectado el Instituto Municipal de Empleo y Fomento Empresarial del Ayuntamiento de Zaragoza, por el secuestro de información. Los Mossos informaron durante 2020 de diferentes ciberataques en ayuntamientos tales como Guixers, Lliçà de Vall, L'Escala y Sant Just Desvern. La operación Oceansx, de la Guardia Civil, reveló cómo, desde octubre de 2022, se perpetraron distintos ataques a organismos públicos: ayuntamientos de León y Salamanca, y diputaciones de Jaén y Málaga. Ese mismo año 2022, la Asociación Navarra de Informática Municipal comunica la caída de sus servidores (webs, correos y sedes electrónicas inutilizadas), con Hive y Cobalt Strike, afectando a 137 ayuntamientos y 35 entidades navarras. El año 2023 se estrenaría, a finales de enero, con el ciberataque a la Diputación Foral de Vizcaya, lo que desactivó los servicios de su sede electrónica. Este ciberataque afectó a la gestión interna de los ayuntamientos integrados en la red de BiscayTIK, 107 de los 112 ayuntamientos de Vizcaya. A mediados de año, en junio de 2023, Lockbit visitaría el Concello de Cangas (Galicia), que vería cómo la mitad de los ordenadores quedaban paralizados, afectando, entre otros, a la gestión y al pago de las nóminas de 229 empleados; mientras que en septiembre atacó los servicios informáticos del Ayuntamiento de Sevilla, dejando su sede electrónica inutilizada y reclamando 5 millones de euros. Granada, en octubre de 2023, sería objetivo del grupo criminal NoName057[8], afectando al normal funcionamiento de las webs del transporte urbano del Ayuntamiento. El Ayuntamiento de Torre Pacheco sería víctima de un *ransomware* en abril de 2024, en el que se vio comprometida información sensible de los ciudadanos y procedimientos administrativos. Tampoco se libraría el Ayuntamiento de Benalmádena, cuyo sistema de cita previa se vio afectado en junio de 2024[9].

De todo lo anterior podemos inferir que los ciberataques son habituales en el ámbito local y que existen diversos tipos de ciberataques que

de la Sede Electrónica de la web del Ministerio de Trabajo, afectando a organismos dependientes, como las consejerías de Trabajo.

8. Presuntamente, el mismo grupo criminal que perpetró ciberataques a distintas webs estatales en la época de las elecciones generales españolas. El referido ataque a Granada se produjo cuando en esa ciudad se celebraba una cumbre europea de jefes de Estado y de Gobierno, lo que denota el interés geopolítico de este grupo de ciberatacantes.

9. Mismo año en el que varias webs de hospitales pertenecientes al Servicio Andaluz de Salud vieron afectado su normal funcionamiento. En efecto, el 9 de julio se detectó en los hospitales universitarios Clínico San Cecilio y Virgen de las Nieves, y en el Área de Gestión Sanitaria Sur de Granada y Distrito Sanitario Granada-Metropolitano, un incidente de seguridad que afectó a las páginas web de dichos hospitales, pero no a la infraestructura, servicios o datos personales de empleados o usuarios.

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

pueden afectar gravemente a los servicios de un ayuntamiento, comprometiendo la seguridad de la información y la continuidad de sus servicios. Incluso se puede sostener que hemos asistido a un incremento de los ciberataques dirigidos específicamente contra las entidades locales. Muchas entidades locales están migrando servicios a la nube, lo que conlleva nuevos desafíos de ciberseguridad relacionados con el almacenamiento de datos, la seguridad de las plataformas y el control de acceso. También la aparente debilidad que se refleja en el ámbito local estimula las amenazas.

Los protagonistas de los ciberataques suelen ser estos tres: el *malware* en general[10], el *ransomware*[11] y el *phishing*[12]. Al ser los ayuntamientos responsables de servicios esenciales (agua, saneamiento, gestión de residuos, pagos, servicios sociales, etc.), los ataques de *ransomware* (cifrando datos y exigiendo un rescate) pueden tener consecuencias graves. A su vez, los ataques de *phishing* también son un riesgo importante, ya que los empleados municipales pueden ser víctimas de correos electrónicos fraudulentos que comprometen sus credenciales o permiten la instalación de *malware*. En todo caso, es habitual que el éxito del ataque acabe afectando directamente a la población.

En otras ocasiones la amenaza a la que se enfrentan los consistorios se dirige contra sus dirigentes. Este tipo de amenazas, que forman parte de campañas hibridas, lo pudimos observar con el *deepfake* al alcalde de Madrid en junio de 2022. De esta forma, se consiguió suplantar la identidad de su homólogo ucraniano de la ciudad de Kiev, Vitali Klitscko. Esta

10. El *malware* puede afectar a los servicios de un ayuntamiento partiendo de un troyano diseñado para infiltrarse en los sistemas informáticos municipales. Este tipo de *malware* se oculta en un archivo aparentemente inofensivo, como un documento o una aplicación que un empleado descarga sin sospechar nada. Una vez dentro del sistema, el troyano puede abrir una puerta trasera que permite a los atacantes acceder de manera remota a la red interna del ayuntamiento. Desde allí, los ciberdelincuentes pueden robar datos sensibles, como información personal de los ciudadanos, registros de impuestos o expedientes confidenciales.

11. Uno de los ataques más comunes en estos últimos años es el *ransomware*, un tipo de *malware* que cifra los archivos de los sistemas informáticos y exige un rescate para su liberación. Hemos podido comprobar que se han parado servicios como los de petición de citas, pagos a empleados, la recaudación de impuestos o el acceso a documentos públicos, afectando gravemente la prestación de servicios a sus ciudadanos.

12. Una técnica bastante utilizada es el *phishing*: los empleados municipales son engañados a través de correos electrónicos o mensajes fraudulentos, con enlaces o archivos maliciosos, permitiendo a los atacantes infiltrarse en las redes internas y acceder a información. Esto no solo compromete la seguridad de la información, sino que también pone en riesgo la integridad de servicios como la tramitación electrónica de expedientes o el sistema de atención al ciudadano, lo que podría conllevar la alteración o el robo de datos personales y la interrupción de procesos administrativos clave.

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

acción usó inteligencia artificial e hizo pensar que se estaba manteniendo una conversación en tiempo real que resultó ser falsa. En realidad no hubo daños, pero se sembró la desconfianza en este tipo de videoconferencias.

Estos son solo unos pocos ejemplos ilustrativos de cómo las Administraciones y los organismos públicos locales han padecido las consecuencias de los ataques realizados por un enemigo silencioso y elusivo que, a través de distintos mecanismos, busca alterar su normal funcionamiento. A ello se han de añadir los errores derivados de la ausencia de políticas de seguridad de la información, o de una inadecuada implementación de las mismas. Como se ha podido comprobar, las Administraciones han sido objeto de distintos ataques producidos por la ciberdelincuencia (*malware*, *ransomware*, *phishing*, ingeniería social, explotación de vulnerabilidades, denegación de servicios, accesos no autorizados a información, suplantaciones); también han tenido que enfrentarse al *hacktivismo* personas que han tenido información privilegiada, al espionaje y a distintos errores y daños físicos (fuego, agua, cortes de suministro)[13]. Estas anomalías han impedido el normal funcionamiento de los servicios municipales, incidiendo directamente en la vida diaria de los ciudadanos, que no han podido realizar sus trámites administrativos, han visto cortados los suministros, no han recibido la ayuda social a tiempo, o han visto cómo se hacían públicos datos de carácter personal.

En suma, del análisis de lo anterior se puede derivar la existencia de varios tipos de ataques en función del daño que sufren los consistorios: por un lado, el cifrado y robo de la información usando *ransomware* supone una doble extorsión y causa graves daños, por cuanto afecta a la disponibilidad de los datos y suele implicar perjuicios económicos; por otro, se producen robos de información que termina vendiéndose en la *dark web*, y cuya protección depende en gran medida de las copias de seguridad (que se tengan, que estén disponibles, que estén actualizadas); asimismo, hay ataques de denegación de servicio (*DDoS*), que suelen tener un menor impacto porque, en principio, se podría recuperar el servicio fácilmente una vez que se identificase la procedencia del ataque; o aquellos que tratan de afectar a la confianza de la sociedad por estar dirigidos contra una persona determinada, sin llegar a poner en riesgo el conjunto de la actividad del ayuntamiento, pero que demuestran la interrelación entre la seguridad de la información y la ciberseguridad de los dirigentes con la

13. Para mayor información, nos remitimos al *Prontuario de ciberseguridad para entidades locales*, fechado en abril de 2021, del Centro Criptológico Nacional y la Federación Española de Municipios y Provincias.

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

propia Administración (incluidos sus dispositivos personales, dada la información sensible que pueden manejar). De este modo, la imagen municipal se deteriora y, por ende, se incrementa la desconfianza ciudadana. Y, subsiguientemente, incluso asistiríamos a un coste electoral para el partido que gobierna la entidad, y se atraerían más ataques al dar muestras de debilidad tecnológica.

Hay que tener presente, como decimos más abajo, que las entidades locales tanto deben garantizar los derechos fundamentales en el entorno digital actual como prestar servicios a su ciudadanía, los cuales en gran parte ya dependen de una infraestructura tecnológica. De este modo, resultan esenciales la atención que debe prestar y el trabajo que debe realizar la Administración local en ambos sentidos. La ciberseguridad no es una elección para los entes locales, al contrario, ha de ser considerada una prioridad en una sociedad comprometida con la digitalización. Este esfuerzo tiene que comenzar con el máximo representante de la corporación (el alcalde) y extenderse a todos los niveles de la institución (incluyendo a todos y cada uno de los empleados y miembros de la corporación, y a las empresas que le prestan servicios). La ciberseguridad debe ser el eje que oriente la implementación de los sistemas y tecnologías que se instalen (tanto a nivel *hardware* como *software*), una verdadera cultura de funcionamiento que hay que integrar en la dinámica cotidiana de los entes locales.

En definitiva, la realidad de las crecientes ciberamenazas lleva a la imperiosa necesidad de que las Administraciones locales se protejan frente a ellas, con una respuesta bien planificada en sus vertientes estratégica, táctica y operativa. De esta forma, tal respuesta garantizará los pilares de confidencialidad, integridad y disponibilidad de la información, ejes nucleares de esta problemática.

2.2. Las oportunidades de las características de la Administración local

En este escenario incierto y convulso por el que transitamos en el siglo XXI, la Administración local desempeña un papel clave. Sus propias características así lo determinan, provocando la necesidad de que las entidades locales afronten de manera decidida y efectiva el desafío que marca el mundo tecnológico. Los rasgos de las entidades locales se convierten en una oportunidad para que jueguen ese rol trascendental que estamos comentando. Es decir, tales características son elementos oportunos, convenientes y favorables para que avance la ciberseguridad en el predio local,

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

lo que no significa que ello suceda automáticamente, ya que se deben realizar distintas acciones que veremos más adelante, en el apartado 6.

Con base en la premisa apuntada, abordamos a continuación estos elementos que determinan el citado papel central. Como se verá, se trata de cuestiones conectadas unas con otras que en algunos de sus aspectos se solapan.

En primer lugar, la **autonomía** de los entes que conforman la Administración local les debe permitir organizar de forma adecuada las respuestas que hay que articular frente al desafío tecnológico, lo que tiene que incluir un plan propio para la ciberseguridad. La autonomía local posibilita una respuesta ágil y adaptativa a los desafíos tecnológicos, dado que esta autonomía les otorga competencias propias, capacidad de gestión y de decisión en el ámbito propio, así como la posibilidad de implementar políticas y estrategias alineadas con las necesidades específicas de sus comunidades. En este sentido, la autonomía refuerza la cercanía a la ciudadanía, la gestión eficiente de recursos al permitir que las entidades locales prioricen la inversión en tecnologías específicas, el fomento de la participación ciudadana digital, la colaboración público-privada y la resiliencia frente a los riesgos tecnológicos. Resulta imprescindible que esta autonomía se emplee para desarrollar políticas específicas de ciberseguridad y protección de datos, necesarias en un contexto donde los riesgos tecnológicos, como ciberataques o el uso indebido de datos personales, son cada vez más relevantes. Así será también en el futuro.

Además, las entidades locales tienen **competencias específicas** que destacan por su **proximidad a la ciudadanía**, lo que las convierte en actores clave en la prestación de servicios y la gestión de recursos a nivel social. Estas competencias están definidas en la legislación y varían según el marco normativo de cada país, pero suelen incluir servicios básicos esenciales (que comentamos después); bienestar social y comunitario, con servicios sociales como la asistencia a personas mayores y personas con discapacidad o en riesgo de exclusión social; atención a situaciones de vulnerabilidad social; gestión de ciertos aspectos de los servicios educativos, como escuelas infantiles o actividades extraescolares; urbanismo y medio ambiente (gestión del suelo, parques, jardines, zonas verdes, promoción de la movilidad sostenible); cultura, deporte y ocio (organización de actividades de esta índole, gestión de bibliotecas, centros culturales y polideportivos, promoción del turismo local y la conservación del patrimonio histórico); seguridad y protección ciudadana (policía local, protección civil, emergencias); y fomento económico y empleo (apoyo a pequeñas y

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

medianas empresas locales, promoción del empleo mediante programas de formación y desarrollo local).

Estas competencias, y la propia proximidad geográfica y administrativa de las entidades locales a la población, les permiten actuar de manera más rápida y adaptada a las necesidades concretas de sus comunidades, fomentando la participación ciudadana y la implementación de políticas orientadas al desarrollo local sostenible. Las entidades locales, gracias a su proximidad, pueden comprender mejor las demandas y expectativas de los ciudadanos en cuanto al uso de nuevas tecnologías. Esto permite respuestas más personalizadas y rápidas, como la digitalización de trámites administrativos o la creación de aplicaciones para reportar problemas urbanos en tiempo real.

A mayor abundamiento, las competencias sobre los **servicios públicos básicos** enfatizan lo dicho. Nos referimos a suministro de agua potable, alcantarillado y gestión de residuos; alumbrado público, pavimentación y mantenimiento de calles; o gestión de cementerios y servicios funerarios. Los servicios públicos básicos pueden ver mejorada su eficiencia con el apoyo tecnológico, lo que redundará en beneficio de la ciudadanía. Los entes locales deben trabajar en ello de manera correcta para que esta oportunidad se concrete en verdadera ventaja.

Los elementos de **financiación propia** explican también esta posición central de las entidades locales para asumir el reto tecnológico y los desafíos emergentes ligados al mismo, como la ciberseguridad. El marcado carácter mercantilizado y economicista de nuestro mundo demuestra lo imprescindible que es poseer recursos para cumplir las funciones propias. Este financiamiento permite que los Gobiernos locales dispongan de recursos suficientes para implementar políticas, programas y medidas que aseguren servicios públicos eficientes, la protección de datos de los ciudadanos y la resiliencia ante amenazas digitales. Una financiación adecuada posibilita recursos que se pueden emplear directamente en áreas prioritarias como salud, educación, infraestructura y digitalización de servicios. Esta autonomía es esencial para financiar plataformas tecnológicas que faciliten el acceso a derechos, como trámites en línea, consultas ciudadanas y servicios públicos digitales. Al mismo tiempo, disponer de recursos propios permite a los Gobiernos locales modernizar su infraestructura tecnológica, lo que incluye las medidas de ciberseguridad. La financiación otorga resiliencia frente a riesgos cibernéticos, como invirtiendo en auditorías de seguridad y formación especializada para el personal. También fomenta la inclusión digital: se reduce la brecha digital, al

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

promover el acceso equitativo a tecnologías y servicios en línea; y da flexibilidad en la implementación de soluciones locales, diseñando respuestas específicas a los desafíos tecnológicos y de ciberseguridad que enfrentan sus comunidades, en lugar de depender exclusivamente de recursos centralizados o transferencias condicionadas.

La **capacidad de adaptación** es otro elemento para considerar y que, de nuevo, refleja el papel central de la Administración local frente al desafío tecnológico. La capacidad de adaptación de las entidades locales frente a este desafío radica en su flexibilidad administrativa, la cercanía ya comentada con la ciudadanía y su posibilidad de diseñar políticas específicas en función de las necesidades locales. Además, también son factores de estas posibilidades de adaptación la autonomía de gestión, la colaboración con otras entidades o empresas para establecer alianzas estratégicas en transformación digital, el cierto grado de flexibilidad normativa, las alternativas en formación y capacitación, o la posible promoción de la participación ciudadana. Esta capacidad permite implementar soluciones innovadoras y enfrentar los retos tecnológicos de manera eficiente, lo que siempre debería tener como objetivo la mejora de la calidad de los servicios públicos y la garantía de los derechos fundamentales en un entorno digital.

En fin, además de lo dicho, también vemos de forma más general, al margen del tema tecnológico, que la Administración local es un agente esencial en la **protección de los derechos fundamentales**, sobre todo por esa posición comentada de cercanía a las personas y de asunción de servicios públicos básicos. Incluso esa garantía de derechos viene de la mano del papel que tienen que jugar las entidades locales en términos de ciberseguridad. Por lo tanto, no solo las específicas cuestiones de ciberseguridad, sino también el papel de estas entidades desde una perspectiva más general en la defensa de los derechos, subraya su trascendencia en lo que ahora nos ocupa.

3. La ciberseguridad como garantía de los derechos fundamentales

La ciberseguridad se ha convertido en una garantía de los derechos fundamentales. Ello puede parecer una afirmación atípica desde la dogmática jurídica de estos derechos, en donde se suele distinguir entre garantías normativas, jurisdiccionales e institucionales. No obstante, aun partiendo de tal construcción, semeja conveniente completarla con otras visiones más amplias, pues las diversas amenazas que se ciernen sobre los derechos aconsejan tal aproximación. A esto nos referimos cuando afirmamos

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

que la ciberseguridad se ha convertido en una garantía esencial para la protección de los derechos, asediados por diversos aspectos negativos de la tecnología. Para ilustrar estos extremos nos referimos a continuación a varios derechos, aunque lo hacemos en una aproximación escueta para no dilatarnos en demasía.

Para entender esta cuestión más cabalmente recordemos, como ya publicamos en su momento (Fernández Rodríguez, 2020), que el encuentro entre derechos y tecnología se puede ver desde la óptica del pasado, del presente o del futuro. Es decir, desde la visión de los derechos que hemos recibido (los derechos del pasado), los que se están creando a raíz del progreso tecnológico (derechos del presente), y los que posiblemente se plantearán en el futuro mediato o lejano (derechos del futuro). Con respecto a los **derechos del pasado** comentamos lo siguiente desde la óptica de la ciberseguridad:

– En primer lugar, la ciberseguridad sirve para mantener nuestra privacidad. El mundo tecnológico ha originado múltiples problemas para los derechos ligados a la privacidad o intimidad, como el derecho al honor, la propia imagen, la protección de las comunicaciones, la protección de domicilio o la protección de datos. Se trata de derechos diferentes, como objetos propios, pero que ahora los podemos conectar para ilustrar las amenazas tecnológicas en este ámbito. Ahí tenemos herramientas diseñadas en gran parte para atacar la intimidad, como virus, troyanos, gusanos, *ransomware*... *Malware* en general que refleja ese lado negativo de la tecnología. De esta forma, nos topamos con interceptaciones de *mails*, entradas en el disco duro sin consentimiento, suplantación de personalidad, perfilado de personas, *spam*, denegación de servicios, bloqueo de equipos informáticos, etc. Los datos se destruyen, se modifican, se fabrican o se roban. Al mismo tiempo, la tecnología también presenta una cara amable y ofrece herramientas de respuesta, como antivirus, cortafuegos, programas antiespía o antispam, criptografía. Por lo tanto, la implementación de correctas medidas de ciberseguridad es imprescindible y lo será cada día más. Una protección robusta de nuestros datos personales solo es en la actualidad posible con niveles avanzados de ciberseguridad.

– De igual forma, los derechos ligados a las libertades comunicativas también se hallan muy afectados en el mundo digital. Nos referimos a las libertades de expresión e información, y a las opciones y los derechos de participación posibilitados por tales libertades.

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

La tecnología ha creado un ecosistema desinformador que se ha expandido por doquier. Ya antes existía manipulación informativa, obviamente, pero ahora las posibilidades de expansión tecnológica nos sumen en un momento diferente. Por un lado, la tecnología posibilita el envío masivo y automatizado de *fake news* por distintos soportes, sobre todo por las redes sociales; por otro, la inteligencia artificial generativa produce por sí misma estas noticias falsas con un realismo casi insuperable (texto, imágenes, sonidos). Así, se dificulta sobremanera el control que la opinión pública debería ejercer sobre el poder, y se plantean trabas para la limpieza del proceso electoral, en el que el votante puede no tomar libremente su decisión al estar seducido por los sesgos que lo engañan. De esta forma, nos hemos planteado si la manipulación informativa destruirá o no a la democracia (Fernández Rodríguez, 2024). Este problema se ha convertido en un verdadero reto ante el que debemos reaccionar con distintas medidas, entre las cuales se encuentran acciones de ciberseguridad que sirvan para detectar las *fake news* y realizar labores de contrapropaganda.

– Los derechos de participación política, como el derecho de sufragio, son ejercidos cada vez en más lugares por medio de instrumentos digitales, entre los que destacan las urnas electrónicas y las votaciones en línea. La ciberseguridad, en todo caso, debe ser robusta para evitar ataques que imposibiliten esta participación e, incluso, alteren el resultado electoral. Los sistemas de votación electrónica y las plataformas de consulta ciudadana requieren, por lo tanto, una ciberseguridad adecuada para afrontar los riesgos de las interferencias externas y los fraudes. Solo así habrá confianza ciudadana en las instituciones, y solo así el intercambio de ideas será más libre y seguro. Debemos tener garantías suficientes para asegurar los elementos distintivos del voto democrático: un voto universal, libre, igual y secreto.

– El derecho de tutela judicial emplea distintos soportes digitales en el marco de una administración electrónica judicial que ya incluye la presentación de demandas, las comunicaciones o la gestión de muchas pruebas y peritajes. Para que todo ello funcione con garantías es imprescindible un nivel de ciberseguridad adecuado, lo que de nuevo se revela como una garantía para el correcto ejercicio de la tutela judicial. En este sentido, en un trabajo de hace algunos años sosteníamos que los progresos técnicos son herramientas que se emplean para "conseguir los objetivos de impartición justa y rec-

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

ta de la justicia", y que la presencia del derecho fundamental de tutela judicial "exige especial intensidad en la implementación del e-gobierno en sede jurisdiccional" (Fernández e Iglesias, 2012: 75).

– También los distintos derechos sociales se ven protegidos por la ciberseguridad. Pensemos en la garantía del funcionamiento de la atención sanitaria, evitando ataques a sus sistemas; o en el suministro de productos de primera necesidad, como el agua o los alimentos, que puede verse truncado por la actuación de ciberdelincuentes. Sin embargo, el mayor reto es para los consumidores, objetivo habitual de los ataques informáticos con la intención de venderles productos fraudulentos, robarles datos o imponerles toda suerte de engaños. Incluso se han conformado técnicas sociales de ataque para ganar en persuasión (el ya comentado *phishing*). La ciberseguridad es, de igual modo, esencial en las actividades de consumo ante este amenazante panorama en el mercado digital.

Con relación a los **derechos del presente**, estamos asistiendo a la aparición de unos derechos nuevos ligados al desarrollo tecnológico, para los que se habla de derechos de cuarta generación. En este sentido, el más destacado en lo que ahora nos interesa es un derecho a la seguridad digital. Así, el art. 82 de la Ley Orgánica 3/2018, de protección de datos personales y garantía de los derechos digitales, prevé que "los usuarios tienen derecho a la seguridad de las comunicaciones que transmitan y reciban a través de Internet". De esta forma, la ciberseguridad se convierte en el contenido de uno de los nuevos derechos que aparecen en el desarrollo tecnológico de estas décadas. Además, existen otros derechos ya contemplados expresamente, como el derecho de neutralidad de internet (art. 80 de la citada LO 3/2018) o el derecho de acceso universal (art. 81 de esta LO 3/2018), que evidencian las muchas novedades que trae el progreso tecnológico en este campo (Álvarez Robles, 2024b).

Por último, parece claro que el **futuro** supondrá la aparición de nuevos derechos que todavía están sin perfilar, pero que seguramente se ligarán, entre otros, a los derechos de los robots o de las personas transhumanas (Fernández Rodríguez, 2023). Además, se hará necesario precisar neuroderechos para proteger nuestro cerebro y pensamiento (como derechos de identidad digital, de libre albedrío, de privacidad digital, de acceso equitativo o de protección frente a los sesgos). Por lo tanto, ante este incierto e intenso futuro en el campo de los derechos, la ciberseguridad tendrá un creciente papel para que los nuevos desarrollos en este terreno puedan ser satisfactorios y no suponer una involución.

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

Con los distintos ejemplos de derechos mostrados en los párrafos precedentes creemos que corroboramos la afirmación que hemos empleado al inicio de este apartado: la ciberseguridad es una imprescindible garantía para los derechos en el mundo presente y futuro. Como las entidades locales deben también proteger los derechos de las personas, se ven obligadas indefectiblemente a apostar por un nivel suficiente de ciberseguridad.

4. Ciberseguridad y continuidad de los servicios y funciones de las entidades locales

Además del rol de las entidades locales en términos de ciberseguridad para proteger derechos, de igual manera un correcto entramado de ciberseguridad es imprescindible para asegurar que los servicios y funciones de esas entidades locales se desarrollen con normalidad. Por eso hablamos de garantía de la continuidad de estos servicios municipales, lo que de nuevo evidencia la relevancia actual y futura de la correcta gestión de las cuestiones relacionadas con el progreso tecnológico. Por todo ello consideramos que la protección de los municipios resulta esencial, debido al tipo de servicios que deben prestar a sus habitantes.

La ciberseguridad se revela como un componente crítico para garantizar esta continuidad de los servicios y funciones esenciales de las entidades locales. Recordemos que en España, según el art. 26 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local, los municipios han de prestar una serie de servicios a sus ciudadanos, que en la actualidad pueden presentar relevantes vulnerabilidades ante ciberataques. Así, en la línea de lo apuntado antes en el apdo. 2.2, encontramos aquellos servicios que deben proveer con independencia de su tamaño: alumbrado público, cementerio, recogida de residuos, limpieza viaria, abastecimiento domiciliario de agua potable, alcantarillado, acceso a los núcleos de población y pavimentación de las vías públicas. Si la población es superior a 20 000 habitantes se incluyen protección civil, evaluación e información de situaciones de necesidad social y atención inmediata a personas en situación o riesgo de exclusión social, prevención y extinción de incendios e instalaciones deportivas de uso público. E incluso transporte colectivo urbano de viajeros y medio ambiente urbano, para aquellos municipios con una población superior a 50 000 habitantes.

Por lo tanto, estas instituciones manejan infraestructuras y datos sensibles que sustentan servicios básicos, como el suministro de agua, electricidad, transporte, educación y salud, así como funciones adminis-

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

trativas vitales. Es más, en la actualidad gran parte de estos servicios públicos municipales dependen de sistemas digitales, como el alumbrado público o la recolección de residuos. Por lo tanto, una brecha en la seguridad cibernética podría interrumpir significativamente estas operaciones, con consecuencias graves, tanto a nivel institucional como en el predio de la ciudadanía. Estos servicios dependen en gran medida de la administración electrónica, de la infraestructura tecnológica, que implica un manejo masivo de información, considerada el petróleo del siglo XXI. No obstante, esta acumulación de datos (en ocasiones sensibles) y su tratamiento por parte de empleados, quienes son el eslabón más débil de la cadena de seguridad, pueden aumentar la superficie de ataque y las vulnerabilidades a distintos tipos de ataques (en especial los relativos a la ingeniería social o *phishing*). Estas amenazas ponen en riesgo la integridad de los sistemas municipales y requieren la implementación de medidas y controles, de políticas de seguridad adecuadas para salvaguardar tanto la información como la propia infraestructura tecnológica por la que discurren los servicios municipales, activos tangibles e intangibles.

En este sentido, las entidades locales administran sistemas que forman parte de infraestructuras críticas, como plantas de tratamiento de agua y sistemas de transporte. La ciberseguridad asegura que estos sistemas sean resistentes a ataques que podrían causar interrupciones masivas. Es fácil imaginar de manera aquilatada la necesidad de esta ciberseguridad en, por ejemplo, el suministro de agua. Pensemos en las consecuencias de un sabotaje a los productos químicos que se vierten a la misma o en qué sucedería si no nos llegase agua, o si se rompiesen las bombas de agua. Otro ejemplo evidente es el caso de un apagón de los semáforos de la ciudad o si se ponen todos en verde. Dado que estas infraestructuras dependen en gran medida de tecnología interconectada y, además, son gestionadas por empleados que podrían ser objetivo de ataques, es crucial que se establezcan medidas de protección robustas para garantizar su funcionamiento continuo y la seguridad de la información manejada.

Igualmente, de nuevo debemos tener presente la temática de los datos personales. Las entidades locales almacenan información personal de los ciudadanos, incluidos datos sensibles que están presentes en impuestos, servicios sociales, registros de salud y empadronamiento o permisos. La ciberseguridad protege esta información contra accesos no autorizados y robos, que se convierten en uno de los principales desa-

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

fíos para garantizar los principios de seguridad de la información (acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de datos, información y servicios), en consonancia con sus respectivas competencias y para la adecuada prestación de los servicios.

De esta forma, la respuesta ante emergencias digitales en el ámbito local es clave para desactivar estos incidentes cibernéticos y restaurar rápidamente los servicios en caso de un ataque, lo que deberá incluir sistemas de respaldo y recuperación de datos. Pero tan importante como ello será la planificación previa desde una lógica proactiva, a lo que nos referimos más abajo en el punto 6.

Así las cosas, la ciberseguridad también se revela como un factor esencial para mantener la confianza en los servicios públicos. Las grietas en estas garantías materializan riesgos y amenazas que afectan a la vida diaria de la ciudadanía[14]. La interrupción de los sistemas municipales y la imposibilidad de prestar servicios con normalidad pueden tener consecuencias graves para la operatividad o el normal desarrollo de la actividad de los ayuntamientos, y para la vida diaria de la ciudadanía. Como hemos podido ejemplificar, estos incidentes (debidos a fallos y ataques) de ciberseguridad no solo generan retrasos en la prestación de servicios, sino que también pueden conllevar la percepción de inseguridad y la pérdida de confianza en las autoridades e instituciones locales. La desconfianza deriva en una percepción de inseguridad que a su vez desencadena quejas, malestar, e incluso ansiedad o miedo ante lo tecnológico-digital, ante la administración electrónica.

5. Obstáculos en las entidades locales para afrontar los retos de la ciberseguridad

14. No es difícil imaginar problemas realistas: el ayuntamiento ha sido víctima de un ataque y no se pueden conseguir copias del padrón municipal, lo que se exige en distintos trámites (como el del DNI); o la necesidad de acceder a un listado de ayudas sociales que se encuentra encriptado por un *ransomware*, y esa falta de acceso imposibilita el cobro de cierta ayuda; o la afectación del servicio municipal de transportes provoca retrasos para llegar al colegio, trabajo o citas médicas (lo que se puede producir en un momento en el que se depende del transporte público, ya que la ciudad tiene restringido el tráfico privado por estar celebrándose una cumbre de jefes de Estado); incluso, en alguna ocasión, hemos comprobado cómo el pago de las nóminas de los empleados municipales no se pudo realizar en tiempo y forma, con las consecuencias que ello puede tener para quien ha de realizar el pago del alquiler o hipoteca y los demás gastos corrientes y habituales. Pero más peligroso sería que se ponga en riesgo la integridad física, alterando los semáforos de la ciudad y causando colisiones entre los turismos, o saboteando los equipos que controlan el suministro de agua.

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

A pesar de la trascendencia de la ciberseguridad para las entidades locales, y de la severidad de las amenazas planteadas en el escenario tecnológico, también es de reseñar la gravedad de los obstáculos que detectamos en este ámbito para afrontar dichos retos. Tales desafíos limitan su capacidad para proteger sistemas críticos, asegurar datos sensibles y garantizar la continuidad de los servicios públicos, además de suponer una relevante mengua en la protección de los derechos. Esquematizamos a continuación lo que hemos calificado de obstáculos:

– Limitaciones presupuestarias: Muchas entidades locales operan con recursos financieros restringidos en estas cuestiones, lo que dificulta la inversión en tecnología avanzada de ciberseguridad, personal especializado y formación adecuada. Los fondos disponibles suelen priorizar otros servicios, dejando la ciberseguridad en un segundo plano, lo que demuestra la poca altura de miras de algunos decisores locales.

– Falta de personal especializado: Todavía existe una escasez generalizada de profesionales capacitados en ciberseguridad, y las entidades locales tienen dificultades para atraer y retener talento, debido a salarios menos competitivos en comparación con el sector privado. Incluso, en muchos casos, el personal técnico local no tiene formación específica para enfrentar amenazas cibernéticas avanzadas. Es peligrosísimo que exista una brecha digital entre los *hackers* y ese personal técnico local.

– Infraestructuras tecnológicas obsoletas: Los sistemas informáticos en muchas entidades locales no están actualizados, y son más vulnerables a ataques cibernéticos. La dependencia de tecnologías antiguas complica la integración de soluciones modernas de seguridad. El empleo de *software* sin soporte o sistemas no actualizados es una puerta de entrada común para los atacantes.

– Falta de concienciación y formación: Tanto los funcionarios como los ciudadanos a menudo desconocen los riesgos asociados a la ciberseguridad, lo que aumenta la probabilidad de incidentes —como ataques de *phishing*— o del uso indebido de sistemas digitales. Un empleado que no identifica un correo de *phishing* o que reutiliza contraseñas débiles puede poner en riesgo toda la red. La formación en buenas prácticas de ciberseguridad no siempre se considera una prioridad, lo que otra vez evidencia lo ya dicho de falta de verdadero conocimiento de la gravedad de estos asuntos por parte de los decisores locales.

– Fragmentación y falta de cooperación: Las entidades locales a menudo trabajan de manera aislada, sin coordinarse con otras Administraciones

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

o agencias nacionales en temas de ciberseguridad. Esto limita el acceso a recursos compartidos, herramientas avanzadas y estrategias unificadas para enfrentar amenazas comunes.

– Pero al mismo tiempo que lo que acabamos de indicar, las entidades locales también suelen estar interconectadas con sistemas regionales o nacionales, lo que amplía la superficie de ataque. Un fallo en los sistemas de ciberseguridad de la Administración local puede tener consecuencias en cascada, afectando a otros organismos y servicios interconectados.

– Aumento en la sofisticación de las amenazas: Los ciberdelincuentes utilizan técnicas cada vez más complejas, como *ransomware* y ataques dirigidos, que son difíciles de prevenir y gestionar con los recursos locales limitados. Es decir, la sofisticación de las amenazas hace más peligrosos los déficits locales en ciberseguridad.

– Normativas complejas y en constante cambio: Las regulaciones de ciberseguridad, como el Reglamento UE 2016/679, de protección de datos, o la Directiva 2022/2555 (la NIS 2) en Europa, imponen obligaciones adicionales que las entidades locales pueden tener dificultades para cumplir, debido a su falta de capacidad técnica y financiera. Las normas europeas se han convertido habitualmente en muy complejas y abigarradas, lo que complica su aplicación. Las entidades locales deben cumplir con tales normativas de protección de datos y seguridad. Sin embargo, la falta de recursos y personal cualificado puede hacer que el cumplimiento sea difícil de garantizar.

Por lo tanto, como se ve, existen obstáculos relevantes que generan verdaderas dificultades para lograr una respuesta adecuada al desafío tecnológico, y que reclaman una concienciación rotunda por parte de los dirigentes locales.

6. ¿Qué deben hacer las entidades locales?

Visto todo lo anterior, se hace necesario que nuestro hilo argumental se centre ahora en la concreta respuesta que consideramos debe articular una entidad local, partiendo de esa lógica que impone la garantía de los derechos de las personas y la necesidad de que los servicios que se prestan tengan continuidad. En este sentido, las acciones para implementar deben ser diversas, algunas de calado, pero en todo caso articuladas de manera coordinada y coherente con ese fin último de garantía de los de-

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

rechos y mantenimiento de los servicios municipales, que tienen que ser la referencia permanente en estas actuaciones.

El punto de partida debe ser un **enfoque estratégico** que combine tecnología, capacitación, normativa y cooperación. Es decir, un planteamiento inicial horizontal y ambicioso, que parta desde el rigor. Una verdadera política que sea permanente y que evidencie la relevancia del desafío tecnológico. El responsable primero de esta política tiene que ser alguien de alto nivel en el *staff* de la entidad local, capaz de imponer las decisiones que haya que tomar y que pueda actuar de forma ágil. La inmediatez de los ciberataques obliga a dotar de similares características al entramado que protege frente a ellos.

Crear una **cultura de seguridad** dentro de las Administraciones locales es fundamental para que todos los empleados sean conscientes de las amenazas cibernéticas y de las mejores prácticas para proteger los sistemas. De este modo, la ciberseguridad debe constituir una política local clave y una inversión continua (económica, personal y material), una política que trate de diseñar e implementar un sistema de gestión de riesgos de la información adaptado al municipio, lo que implica ese enfoque estratégico al que nos referimos. Así, la ciberseguridad, desde esta lógica estratégica, debe ser considerada como un proceso continuo de mejora que desarrolle las fases de planificación[15], ejecución e implementación[16], que continúe con el seguimiento y la auditoría de medidas y controles implementados, y prosiga con la incorporación de mejoras o de adaptaciones correctivas respecto a la fase anterior, o medidas preventivas respecto de los nuevos riesgos que puedan surgir[17]. La seguridad de los sistemas de información "deberá comprometer a todos los miembros de la organización" (art. 13 del Real Decreto 311/2022, que regula el Esquema Nacional de Seguridad).

15. Fase encargada de establecer la política, objetivos, procesos y procedimientos relativos a la gestión del riesgo y a la mejora de la seguridad de la información de la organización, para ofrecer resultados acordes con sus políticas y objetivos generales.

16. En esta fase, se trataría de implementar y gestionar el sistema de gestión de seguridad de la información de acuerdo con su política, controles, procesos y procedimientos.

17. Pensemos que, si disponemos de copias de seguridad actualizadas y sufrimos un ataque de *ransomware*, el tiempo durante el cual dejemos de prestar los servicios será menor, al poder restaurarlos desde las copias. Una correcta segmentación de redes en los ayuntamientos ayudará en la contención de estos ataques, afectando solo a parte de los servicios municipales. De igual forma, frente a ataques de denegación de servicio, se preverá la instalación de sistemas distribuidos con balanceo de cargas, y se tendrá en cuenta el monitoreo de redes, de manera que los sistemas de detección y respuesta automatizada identifiquen y bloqueen el tráfico ante intentos de acceso no autorizados o sospechosos.

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

A partir de esta política general de ciberseguridad, se deben aplicar un conjunto de acciones ya más específicas, entre las cuales destacamos las siguientes, que casi podemos considerar como imprescindibles ante el tamaño desafío que existe:

– La **evaluación de riesgos** y vulnerabilidades requiere efectuar auditorías regulares de ciberseguridad para identificar debilidades en sistemas y procesos. Se trata de adoptar un planteamiento de planificación proactivo, que se anticipe a los problemas que puedan surgir y se prepare ante las futuras contingencias. Esta política preventiva es la más aconsejable en el volátil y peligroso escenario tecnológico que nos envuelve, además de ser una exigencia del citado Esquema Nacional de Seguridad y de la normativa de protección de datos, ambos aplicables a las entidades locales.

  Así, el análisis de riesgos en protección de datos se deriva del principio de responsabilidad proactiva, considerándose obligatorio partir de dicha inferencia (art. 5 Reglamento UE 2016/679). A su vez, recordemos que el Esquema Nacional de Seguridad es en España un marco normativo establecido actualmente por el Decreto 311/2022, de 3 de mayo, que tiene como objetivo garantizar la protección adecuada de la información, los sistemas y los servicios electrónicos utilizados por las Administraciones públicas, lo que también incluye las entidades locales. De esta forma, se establecen medidas y principios para asegurar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de los datos que manejan los organismos públicos. La gestión de la seguridad basada en los riesgos es uno de los principios básicos de dicho Esquema Nacional de Seguridad, lo que significa que las medidas de seguridad se deben adaptar al nivel de riesgo que supone la información o el servicio.

– A partir de esta evaluación de riesgos, hay que desarrollar **políticas internas** claras sobre el uso de sistemas informáticos y la gestión de datos. En este sentido, deben elaborarse planes de contingencia y resiliencia que incluyan protocolos para responder a incidentes cibernéticos. Con dichos planes hay que asegurar la respuesta adecuada al hipotético ciberataque y la continuidad de los servicios. En este orden de cosas, también se puede aludir al diseño e implementación de soluciones tecnológicas específicas, como plataformas digitales para mejorar la participación ciudadana, sistemas de gestión de residuos inteligentes o redes de movilidad urbana conectadas. Sin una planificación adecuada, los ciberataques pueden paralizar servicios clave y afectar gravemente a los ciudadanos.

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

– Es recomendable **categorizar** los distintos sistemas y procesos para priorizar aquellos más relevantes por razones objetivas, como el suministro de agua y electricidad o las bases de datos sensibles. Por ello, hay que priorizar la modernización de infraestructuras y áreas críticas mediante soluciones escalables y sostenibles.

– Resultan imprescindibles **buenas prácticas** de seguridad, como mantener *software* y sistemas operativos actualizados con los últimos parches de seguridad, o encriptar datos sensibles tanto en tránsito como en reposo, para prevenir accesos no autorizados. Las buenas prácticas mitigan en grado sumo el riesgo de los ataques.

– Hoy en día resulta inexcusable una **infraestructura tecnológica** robusta, asentada en unos estándares avanzados de seguridad y en herramientas de monitoreo constante. Se deben implementar medidas de protección tecnológica, herramientas que eviten la actuación del *malware* de los ciberataques. Así, deben emplearse *firewalls*, antivirus avanzados, sistemas de detección de intrusos, o herramientas de monitoreo en tiempo real. De igual forma, deben contemplarse sistemas de respaldo (*backups*) regulares para restaurar datos en caso de ataques. Y también sistemas de alerta temprana: sensores conectados para detectar anomalías, por ejemplo, en sistemas de suministro de agua o energía, protegidos contra ciberataques. Una aplicación de este tipo puede reportar los problemas municipales en tiempo real. Igualmente, las Administraciones locales deben garantizar que los servicios en la nube que contratan cumplan con los estándares de seguridad adecuados y ofrezcan protección contra vulnerabilidades.

  Pero no solo hay que poseer y reclamar los instrumentos tecnológicos oportunos, sino que también debemos tenerlos actualizados para que no se conviertan en un problema adicional. La actualización tecnológica es a veces una asignatura pendiente en los órganos públicos. Las entidades locales deben estar preparadas para realizar auditorías de seguridad y responder ante incidentes de manera rápida y efectiva, lo cual es un reto sin una estructura sólida de ciberseguridad.

– Como complemento de lo anterior deben realizarse **simulaciones** y pruebas de continuidad. Las simulaciones de ciberataques sirven para evaluar la capacidad de respuesta y la eficacia real de los protocolos de recuperación.

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

– Sumamente útil resulta contar con un **plan de comunicación** para el tratamiento informativo de un ciberataque, en el que se debe buscar un equilibrio entre la adecuada transparencia de un poder público democrático y la necesidad de no mostrar una debilidad que atraiga más ataques. En nuestro mundo, la comunicación y la información se han vuelto imprescindibles en cualquier entramado organizacional y social. Un tratamiento correcto de estos extremos reporta estabilidad, credibilidad, confianza y, por ende, fortaleza. Los déficits en este campo son una verdadera debilidad, sobre todo en lo que concierne a la ciberseguridad.

– Hay que tener presente que el principal elemento de riesgo de ciberseguridad en una organización son sus empleados, que con su falta de **concienciación** en estos temas se convierten de forma involuntaria en una verdadera amenaza. Son los que no saben identificar un correo *phishing*, abren y pinchan en los enlaces sospechosos o intercambian datos de modo irreflexivo. Por ello, resulta fundamental **capacitar** al personal mediante una formación continua sobre buenas prácticas de ciberseguridad, en la que conozcan la realidad de los posibles ataques y de los medios de defensa, y logren estar concienciados y sensibilizados respecto de esta problemática. Así adoptarán siempre una actitud de cautela y precaución, y podrán identificar las amenazas comunes. Esta capacitación continua debe aplicarse a todo el personal, aunque más intensamente al personal técnico y administrativo y a los cuadros directivos.

– También puede ayudar de forma poderosa tener personas en el entramado administrativo con **especialización y responsabilidad específica** en estos ámbitos. El primero de ellos es el delegado de protección de datos (exigido para las entidades locales por el art. 37.1.a del citado Reglamento UE 2016/679). Este delegado debe ocupar un lugar clave en la política de ciberseguridad. Con sus funciones de asesoramiento y supervisión desempeña ese relevante rol.

  Pero, de igual forma, se puede designar a un encargado específico de ciberseguridad o a un equipo especializado en la gestión de riesgos digitales, que, en todo caso, deben estar coordinados con el delegado de protección de datos, evitando cualquier tipo de desajuste. Los desajustes internos favorecerán el éxito de los ciberataques y frustrarán o ralentizarán las respuestas.

  En este sentido, recordemos que el citado Real Decreto 311/2022, que regula el Esquema Nacional de Seguridad, en su art. 11.1 diferencia cuatro responsabilidades: “En los sistemas de información se diferenciará el res-

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

ponsable de la información, el responsable del servicio, el responsable de la seguridad y el responsable del sistema". La política de seguridad de la entidad municipal "detallará las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos" (art. 11.3)[18].

– Al margen de la dimensión interna de la Administración municipal, citamos igualmente en este apartado la actuación de cara al exterior, que también resultará útil en el propósito de incrementar la ciberseguridad. Así, las entidades locales deben **educar** a los ciudadanos sobre los riesgos cibernéticos, y promover su concienciación. En particular, hay que instruirlos en cómo proteger sus datos al interactuar con servicios digitales locales. A mayores, una opción interesante también es realizar campañas informativas sobre la importancia de contraseñas seguras y la verificación de identidad.

  Lo que debemos buscar es generar, a partir de varias iniciativas, una cultura de seguridad ciudadana. No cabe duda de que el fomento de la educación digital es la verdadera clave para conseguir una sociedad más protegida y vigilante ante los riesgos y amenazas del entorno tecnológico.

– El fomento de la **colaboración interinstitucional** es otro elemento útil que a veces no se contempla desde la óptica de la ciberseguridad. Conviene establecer redes de cooperación y apoyo mutuo con otras entidades locales, regionales y nacionales, para compartir información sobre amenazas y mejores prácticas. Incluso, en este sentido, podría resultar sugerente participar en programas o redes de ciberseguridad organizados por agencias estatales o internacionales. Recordemos que en España hay entidades que pueden colaborar, como el INCIBE o el Centro Criptológico Nacional. La necesaria interconexión exige una mayor coordinación y compartición de información sobre ciberamenazas con otros niveles de gobierno, lo que será complicado de gestionar sin las herramientas adecuadas. La cooperación interinstitucional es clave para mejorar las defensas y coordinar respuestas frente a incidentes.

18. El art. 13 de dicho decreto separa las cuatro funciones: "a) El responsable de la información determinará los requisitos de la información tratada b) El responsable del servicio determinará los requisitos de los servicios prestados. c) El responsable de la seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones. d) El responsable del sistema, por sí o a través de recursos propios o contratados, se encargará de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad". El responsable de seguridad será en principio distinto al responsable del sistema.

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

– De igual modo, gracias a su autonomía, los Gobiernos locales pueden establecer alianzas estratégicas con **empresas tecnológicas** para abordar problemas locales, como soluciones de eficiencia energética, proyectos de movilidad inteligente o desarrollo de aplicaciones de salud pública. En ello no deben comprometerse el servicio público ni la neutralidad propia de las entidades públicas.

– La **financiación** resulta clave para poder abordar esta problemática de manera robusta. Así, es fundamental aprovechar recursos externos y fondos públicos para modernizar infraestructuras y adoptar tecnologías avanzadas de ciberseguridad. En este sentido, pueden servir de referencia los estándares internacionales como la norma ISO/IEC 27001 para mejorar la gestión de la seguridad de la información. Asimismo, deben promoverse programas de financiamiento específicos para reforzar la ciberseguridad a nivel local, para lo cual se puede recurrir a fondos estatales y europeos.

– En línea de varias de las cosas comentadas, es imprescindible el **cumplimiento de la normativa**, tanto de protección de datos como más específica de ciberseguridad. Las entidades locales tienen que ser ejemplo del respeto al ordenamiento jurídico, en una época donde algunos relativizan estas cuestiones.

  En este sentido, en el derecho fundamental de **protección de datos**, la referencia es el tándem normativo que conforman el Reglamento UE 2016/679 y la Ley Orgánica 3/2018. Esta regulación ofrece un modelo proactivo para el tratamiento de los datos personales en el que el responsable del tratamiento asume la obligación de adoptar las medidas técnicas y organizativas adecuadas para respetar este derecho. En el ámbito local los responsables del tratamiento de datos suelen ser las personas jurídicas que suponen los ayuntamientos, diputaciones o cabildos. Se prevén una serie de principios que regirán este tratamiento, como el de transparencia, minimización, exactitud o confidencialidad; además, se contemplan derechos en manos de las personas interesadas que la entidad local debe cumplir (como los de acceso, rectificación, supresión, limitación, oposición o portabilidad) y obligaciones que pesan sobre estos órganos públicos (como las de información, realización de análisis de riesgos o evaluaciones de impacto, establecer un registro de actividades de tratamiento, nombrar al delegado de protección de datos, o formalizar el contrato con el encargado del tratamiento). El régimen sancionador en este sector normativo expone a la entidad local a sanciones si se producen violaciones de datos.

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

– Hay que trabajar en **resiliencia** digital para mitigar las consecuencias negativas de un ciberataque. Así, debe contarse con redes municipales con copias de seguridad en la nube y procesos automáticos de restauración de datos tras un ataque.

– Aprovechando el progreso tecnológico, las entidades locales tienen que tratar de mejorar su funcionamiento democrático, lo que también podría ser útil en términos de ciberseguridad. De este modo, con mejores conocimientos en ciberseguridad, se puede apostar sin reticencias por vías tecnológicas que incrementen y dinamicen la **participación ciudadana**, esencia del propio concepto de democracia. Se trata de cuestiones relacionadas recíprocamente, pues una ciudadanía alfabetizada digitalmente puede usar mejor y sin temor esas nuevas opciones de participación, y tales nuevas opciones entrenan en parte a la ciudadanía en las habilidades tecnológicas. Así, las entidades locales pueden promover plataformas digitales que refuercen la participación activa de los ciudadanos, como consultas populares *online*, presupuestos participativos o mecanismos de transparencia en la gestión pública.

– En el mismo orden de cosas, los órganos locales deben esforzarse en la reducción de la **brecha digital** y en la subsiguiente inclusión digital, una cuestión básica en el moderno entendimiento del Estado social. En una comunidad local puede haber desigualdades injustificadas respecto al acceso a la tecnología, sea por razón de edad, capacidad económica o ubicación en el territorio del municipio. El Gobierno local tiene la obligación de afrontar estas desigualdades, que muchas veces se convierten en discriminación, y tratar de revertir la situación. Esto también incidirá de manera positiva en el incremento de los niveles de ciberseguridad.

Por lo tanto, son muchas las tareas que deben llevar a cabo las entidades locales en lo que ahora nos ocupa, la mayor parte de ellas necesarias en este momento de enorme penetración de la tecnología en la ciudadanía y en las distintas entidades privadas y públicas.

7. Conclusiones

Las entidades locales del presente y del futuro enfrentan importantes retos de ciberseguridad debido a la creciente digitalización de sus servicios, la limitada capacidad de recursos, la diversidad de datos que gestionan y el aumento de los ciberataques. La ciberseguridad no solo protege los derechos fundamentales de las personas, sino que también garantiza la información y los sistemas digitales de las entidades locales y asegura la

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

continuidad de servicios esenciales para la comunidad. Invertir en protección digital y establecer protocolos sólidos en la planificación y recuperación resultan esenciales para mantener la confianza pública y garantizar el bienestar local en un entorno tecnológico en constante evolución. El futuro incierto de esta evolución es un poderoso argumento adicional para reclamar esta constante y atenta atención que debe mostrarse en el ámbito local con la ciberseguridad. Tal atención tiene que basarse en una serie de ejes clave, como la defensa de la privacidad de las personas, la garantía de sus datos, y la efectividad de la participación ciudadana, que en buena medida depende de tener satisfechas sus exigencias de privacidad.

Se trata de una problemática de creciente complejidad, que en el futuro inmediato se hará más delicada y trascendente. Enfrentar estos desafíos requiere un enfoque estratégico, con apoyo financiero, formación adecuada y una coordinación efectiva entre los niveles de gobierno y la sociedad. Solo así podremos asegurar que las entidades locales estén mejor preparadas para proteger sus sistemas y garantizar la seguridad digital de su ciudadanía. Existen dos argumentos poderosos para obligar a la Administración local a prestar especial atención a la ciberseguridad, incluso para convertirla en un actor clave en ese sentido. Por un lado, la necesaria garantía de los derechos fundamentales, ahora ligados al mundo digital; y, por otro, lo imprescindible que resulta asegurar la continuidad de las funciones y los servicios, en la actualidad con habitual soporte tecnológico.

En Europa encontramos ya buenos ejemplos de trabajo municipal adecuado en términos de ciberseguridad, además de la implementación de distintos servicios y políticas que apuestan por la digitalización de forma segura. Un caso relevante son las plataformas de *smart cities* en municipios europeos, donde la autonomía local ha permitido la instalación de sensores en tiempo real para monitorizar el tráfico, mejorar el transporte, controlar la calidad del aire y mejorar la eficiencia energética y la recogida de residuos. Estas soluciones tecnológicas son posibles gracias a la flexibilidad y a la capacidad de decisión que proporciona la autonomía local. La digitalización correcta de servicios municipales debe traducirse en portales en línea para pagar impuestos, solicitar licencias o registrar quejas ciudadanas, que en todo caso aseguran la confidencialidad y la integridad de la información.

Desde la lógica de un análisis DAFO, la existencia de autonomía local es una verdadera oportunidad para tener éxito en ese esfuerzo. La autonomía local es un pilar fundamental para que las entidades locales enfrenten correctamente los desafíos tecnológicos, promoviendo respues-

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

tas innovadoras, eficaces y orientadas al bienestar de la ciudadanía. Esto asegura un entorno digital más seguro para la Administración y la ciudadanía. Ciertas características de las entidades locales también se configuran como una fortaleza. Es lo que sucede con la flexibilidad que podemos conseguir en la Administración local. La capacidad de adaptación de las entidades locales al desafío tecnológico depende de su flexibilidad, cercanía con los ciudadanos e inversión en recursos tecnológicos y humanos. Estas características las posicionan como actores fundamentales en la transformación digital de las comunidades, mejorando tanto la calidad de vida como la participación democrática en el entorno digital.

Sin embargo, la financiación puede ser una amenaza o una fortaleza en función de si resulta suficiente y adecuada o no. No cabe duda de que la financiación propia es clave para que las entidades locales puedan garantizar derechos fundamentales y desarrollar medidas eficaces de ciberseguridad. Este recurso otorga independencia, flexibilidad y capacidad para adaptarse a las necesidades locales, promoviendo un entorno más seguro y equitativo para la ciudadanía. Por tanto, las entidades locales deben esforzarse para conseguir los niveles de financiación que se necesitan.

En fin, la ciberseguridad como garantía de los derechos en el ámbito local repercute de manera directa en la confianza pública y participación ciudadana. Un entorno digital seguro fomenta la confianza de los ciudadanos en el uso de servicios en línea, como pagos electrónicos, consultas digitales y participación en presupuestos participativos. Esta ciberseguridad ya es la base imprescindible para la aplicación de las vías y los instrumentos de participación ciudadana, verdadera clave de un sistema democrático que controla efectivamente al poder. Esperemos que nuestras entidades locales puedan asumir todos estos retos y sean capaces de tener éxito en su marcha por el creciente mundo tecnológico.

8. Bibliografía

Álvarez Robles, T. (2018). Derechos digitales: especial interés en los derechos de acceso a internet y a la ciberseguridad como derechos constitucionales sustantivos. En A. I. Dueñas Castrillo, D. Fernández Cañueto y G. Moreno González (coords.). *Juventud y Constitución. Un estudio de la Constitución Española por los jóvenes en su cuarenta aniversario* (pp. 135-158). Zaragoza: Fundación Manuel Giménez Abad de Estudios Parlamentarios y del Estado Autonómico.

Álvarez Robles, T. (2024a). 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). Valencia: Tirant lo Blanch.

Álvarez Robles, T. (2024b). *El derecho de acceso a Internet: especial referencia al constitucionalismo español*. Valencia: Tirant lo Blanch.

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). Cizur Menor: Aranzadi.

Fernández Rodríguez, J. J. (2020). Derechos y progreso tecnológico: pasado, presente y futuro. En W. Engelmann (coord.). *Sistema do direito, novas tecnologias, globalização e o constitucionalismo contemporâneo: desafios e perspectivas* (pp. 259-277). São Leopolodo: Casa Leiria.

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). Madrid: Dykinson.

Fernández Rodríguez, J. J. (2024). *¿La manipulación informativa destruirá a la democracia?* A Coruña: Colex.

Fernández Rodríguez, J. J. e Iglesias Barral, S. (2012). Gobierno electrónico: posibilidades en el ámbito judicial. *Revista Mexicana de Análisis Político y Administración Pública*, 1 (2), 73-93.

Greiff, G. (2005). Terrorismo y seguridad nacional. El derecho internacional que hereda el siglo XXI. En R. Méndez Silva (coord.). *Derecho y seguridad internacional. Memoria del Congreso Internacional de Culturas y Sistemas Jurídicos Comparados* (pp. 137-159). Ciudad de México: UNAM.

Hobbes, T. (1651). *El Leviatán*. Londres: Andrew Crooke.

Pérez Royo, J. (2010). La democracia frente al terrorismo global. En J. Pérez Royo y M. Carrasco Durán (dirs.). *Terrorismo, democracia y seguridad, en perspectiva constitucional* (pp. 7-12). Barcelona: Marcial Pons.

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). Pamplona: Aranzadi.

Ridaura Martínez, M.ª J. (2014). La seguridad ciudadana como función del Estado. Estudios de Deusto, 62 (2), 319-346.

Rodríguez, R. J. (2023). *A brief history of malware* (part 1). Blog Rme-Disco Research Group, 28 de febrero de 2023. Disponible en https://reversea.me/index.php/a-brief-history-of-malware-part-1/.

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

CAPÍTULO II

La normativa y organización europea sobre ciberseguridad

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

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

1. Introducción

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

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

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

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

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

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

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

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

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

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

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

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

2. El marco europeo de ciberseguridad

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

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

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

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

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

4. Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

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

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

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

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

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

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

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

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

10. Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión.

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

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

2.1. La Directiva NIS2

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

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

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

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

2.1.1. Las entidades incluidas

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.1.2. Las obligaciones

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

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

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

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

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

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

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

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

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

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

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

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

25. Art. 6, apdo. 7, Dir. (UE) 2022/2555: "'incidente de ciberseguridad a gran escala': un incidente que cause perturbaciones que superen la capacidad de un Estado miembro para responder a él o que afecte significativamente por lo menos a dos Estados miembros".

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.2. El Reglamento DORA y la Directiva CER

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

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

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

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

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

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

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

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

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

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

3. La organización europea de ciberseguridad

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4. El marco europeo de certificación de la ciberseguridad

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Fuente: elaboración propia.

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

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

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

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

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

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

5. Conclusiones

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

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

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

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

6. Bibliografía

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

CAPÍTULO IV

Glosa y *summa* de incidentes de ciberseguridad sufridos por entidades locales

Noelia Betetos Agrelo
Profesora lectora.
Universidad de Barcelona

SUMARIO. 1. Introducción. 2. Los ciberataques en el ámbito local: situación actual y perspectivas de futuro. 3. Taxonomía de ciberataques contra entidades locales. 3.1. El acceso ilegítimo y secuestro de datos. 3.2. Los ataques de denegación de servicios. 3.3. La utilización fraudulenta de la identidad de terceros. **4. El grado de madurez y resiliencia en materia de ciberseguridad de los entes locales.** 4.1. El inventario y control de los dispositivos físicos. 4.2. El inventario y control de *software* autorizado y no autorizado. 4.3. La existencia de un procedimiento continuo de identificación y remediación de vulnerabilidades. 4.4. El uso controlado de privilegios administrativos. 4.5. La existencia de configuraciones seguras de *hardware* y *software* en los sistemas informáticos y servidores de la entidad local. 4.6. El control de la actividad de los usuarios. 4.7. La realización de copias de seguridad sobre los datos y sistemas. 4.8. La revisión del cumplimiento de la legalidad. **5. El futuro de la ciberseguridad en el ámbito local: iniciativas de éxito y propuestas de mejora.** 5.1. Experiencias piloto y buenas prácticas. 5.1.1. *El modelo valenciano de ciberseguridad: un ejemplo de colaboración impulsado a nivel autonómico*. 5.1.2. *El rol de las diputaciones provinciales en el establecimiento de un estándar de ciberseguridad adecuado a nivel municipal*. 5.2. Algunas propuestas de mejora para fortalecer la ciberseguridad en los entes locales. **6. Bibliografía. 7. Anexo: resultados de los informes sobre controles básicos en materia de ciberseguridad elaborados por los órganos de control externo.**

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

1. Introducción

La progresiva consolidación del modelo de administración electrónica y la generalización en el uso de las nuevas tecnologías por parte de las entidades públicas conllevan un correlativo aumento de los riesgos a los que estas se hallan expuestas[1]. Las Administraciones públicas en general, y las entidades locales en particular, se han convertido, como se verá a continuación, en uno de los blancos predilectos de la ciberdelincuencia.

Partiendo del contexto descrito, en el presente estudio, se acomete un análisis del estado actual de la ciberseguridad en las entidades locales españolas. A este respecto, es necesario advertir que, en estas líneas, no se pretende efectuar una revisión exhaustiva de la totalidad de incidentes de ciberseguridad que han sufrido nuestras Administraciones locales en los últimos años; en parte porque no existe un registro completo y fiable en el que se recoja información exacta sobre esta cuestión; y, en parte, porque a los efectos de ilustrar sobre esta problemática, bastará con traer a colación algunos de los ejemplos más representativos, sin abrumar al lector con más datos de aquellos que resulten estrictamente imprescindibles para comprender la magnitud del desafío al que se enfrentan nuestros municipios y diputaciones provinciales.

Realizadas las anteriores consideraciones, el primer epígrafe del presente trabajo contiene algunos ejemplos de ciberataques que se han perpetrado contra las Administraciones locales españolas, a nivel provincial y municipal. En segundo lugar, se lleva a cabo una revisión e intento de clasificación de los principales incidentes de ciberseguridad que se han utilizado con mayor frecuencia para comprometer las redes y los dispositivos de esta tipología de entidades. En tercer lugar, se examinarán los informes publicados por los órganos autonómicos de control externo, que estén disponibles en el momento de publicación de esta contribución, con el objetivo de verificar el grado de madurez y de ciberresiliencia existente en estas organizaciones. Por último, se incluirá un conjunto propuestas de mejora que se considera que habrían de introducirse urgentemente en los sistemas de seguridad informática de las entidades locales, para asegurar que las mismas cumplen con el estándar mínimo fijado por el Esquema Nacional de Seguridad; señalándose, a su vez, algunas experiencias piloto,

1. El análisis de las profundas transformaciones digitales que se han ido sucediendo en las últimas décadas, y que constituyen un presupuesto previo al contenido de esta investigación, excedería de los límites del presente estudio. Para una revisión en profundidad sobre esta cuestión, se pueden consultar: Martín Delgado (2016), Piñar Mañas (2011) o Valero Torrijos (2007).

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

desarrolladas e implementadas por iniciativa autonómica o provincial, que podrían servir de inspiración para el resto de entidades públicas.

2. Los ciberataques en el ámbito local: situación actual y perspectivas de futuro

Las Administraciones públicas son uno de los principales objetivos a los que se dirigen los ciberataques, porque en ellas concurren un conjunto de circunstancias singulares que las convierten en un blanco ideal para los cibercriminales. Entre los factores que han contribuido a esta situación se han de destacar, como mínimo, los siguientes. En primer lugar, se trata de entidades que tienen acceso a un volumen de información y de datos personales de los ciudadanos que son de interés para los delincuentes cibernéticos, bien por su carácter estratégico, bien porque de ellos se espera obtener un beneficio económico mediante su comercialización en mercados ilegales. En segundo lugar, son organizaciones burocráticas complejas y escasamente preparadas para hacer frente a los desafíos relacionados con la ciberseguridad, puesto que no cuentan con los instrumentos técnicos ni con la formación necesaria para prevenir, detectar y responder ágilmente a este tipo de amenazas, lo que, en última instancia, facilita a los *hackers* la tarea de comprometer la integridad de sus sistemas informáticos. En tercer lugar, existe una notable falta de conocimiento y de concienciación entre los empleados públicos acerca del impacto que puede derivar de un ciberataque exitoso, lo que deja a la entidad local en una posición de gran vulnerabilidad. Por último, pero no por ello menos importante, se trata de organizaciones que disponen de un volumen de recursos financieros más elevado que la mayoría de las empresas privadas que integran el tejido productivo español, por lo que estas operaciones suelen resultar más rentables, puesto que, con una única artimaña —como aquellas dirigidas a la suplantación de la identidad de los acreedores de la Administración—, se pueden estafar cientos de miles de euros.

En este sentido, el Centro Criptológico Nacional (en lo sucesivo, CCN) ha informado de que el Gobierno y las Administraciones públicas soportan aproximadamente el 35 % de los ciberataques que se producen en Europa[2]. Esta cifra, para el conjunto de las Administraciones públicas, se traduce en 55 000 ciberataques en el año 2022, 107 000 en 2023, y, solo en los dos primeros meses de 2024, estas entidades han afrontado otras 25 000 nue-

2. *Vid*. CCN-CERT IA-04/24 (2024: 27).

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

vas amenazas[3]. Estos valores reflejan claramente la rápida consolidación de esta nueva tipología de delincuencia, por lo que la detección preventiva y la gestión eficaz de los incidentes en materia de ciberseguridad requieren un incremento inmediato de los esfuerzos que se están llevando a cabo para minimizar su impacto.

Pese a la imposibilidad material de acometer un examen pormenorizado de la totalidad de ciberataques que han sufrido las entidades locales en estos últimos años, se ha optado por incluir una selección de casos de estudio, que han afectado a diputaciones provinciales, cabildos, consejos y ayuntamientos, puesto que estos ejemplos pueden servir para contextualizar la gravedad y el alcance de la problemática objeto de estudio.

En diciembre de 2019, la Diputación de Ourense fue víctima de un ciberataque informático, en virtud del cual se desviaron fondos públicos, por importe de 200 000 euros, destinados a sufragar un conjunto de subvenciones concedidas por dicha entidad local a diferentes asociaciones que operaban en la provincia, las cuales, al no recibir el dinero en el plazo convenido, procedieron a dar la voz de alarma. El presunto *hacker* logró acceder a las partidas presupuestarias y modificar los números de cuenta de los beneficiarios originales, transfiriendo esos fondos a un agente de inversiones, residente en Canarias, con el objetivo de que este último hiciese varios movimientos bancarios para distribuir el dinero. Sin perjuicio de la depuración de la responsabilidad penal atribuida a los anteriores sujetos, la rápida actuación conjunta de la entidad local y de la Unidad de Delitos Informáticos del Cuerpo Nacional de Policía, permitió bloquear las sucesivas operaciones y recuperar de modo inmediato el 95 % del dinero desviado (aproximadamente 195 000 euros). No obstante, tras el ataque, la Diputación de Ourense optó por ejecutar un análisis forense para determinar el origen del incidente de seguridad, acordándose, como medida de precaución, el cierre temporal de su página web y la suspensión de las cuentas de correo electrónico de sus empleados públicos[4].

3. El informe del CCN-CERT en el que se publican los datos empleados en la elaboración de este estudio se halla protegido por razones de seguridad nacional, por lo que toda la información en él contenida tiene carácter confidencial. Sin perjuicio de ello, son numerosas las noticias de prensa que se han hecho eco de las cifras reflejadas en el presente trabajo. En concreto, sin ánimo de exhaustividad, se pueden mencionar: https://acortar.link/oxDJgT, https://acortar.link/SIxOUk y https://acortar.link/kBVsTZ (consultados por última vez en abril de 2025).

4. La información utilizada se ha extraído de la bitácora de ciberseguridad del Instituto Nacional de Ciberseguridad (en lo sucesivo INCIBE) y de las noticias de prensa publicadas a raíz de dicho acontecimiento. Disponibles en https://acortar.link/FDgyMe y https://acortar.link/h7IPui (consultado por última vez en abril de 2025).

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

En mayo de 2021, los sistemas informáticos de la Diputación de Segovia sufrieron un ciberataque dirigido al secuestro y encriptación de datos, afectando a 14 000 GB de información de dicha entidad local. Esta práctica se emplea frecuentemente por los *hackers* como mecanismo para extorsionar a los organismos públicos, ya que, una vez que se hacen con el control del ente, exigen un pago en criptomonedas a cambio de la liberación de la información y el desbloqueo de los sistemas. Para evitar una posible propagación de este virus informático, la Diputación acordó interrumpir, de forma temporal, toda su actividad, no solo la tramitación de los procedimientos, sino también la prestación de aquellos servicios erogados electrónicamente, incluidos los de mero acceso a la información publicada en su página web. En este concreto supuesto, la Diputación de Segovia contaba con unas adecuadas medidas de protección, puesto que tienen programada la realización de copias automáticas de seguridad, una que se realiza a lo largo del día en sus diferentes sistemas, otra que se ejecuta diariamente sobre todos sus datos y dispositivos, y otra global cada semana y cada mes. Además, dichas copias de seguridad se almacenan en dos servidores separados físicamente de la red de la Diputación, lo que permitió evitar que el virus se propagase. No obstante, pese a que los efectos de este incidente pudieron mitigarse, fueron necesarios más de veinte técnicos informáticos de la Diputación y del CCN y más de tres semanas para empezar a recuperar la normalidad en dicha Administración, viéndose afectadas las tareas más básicas de la entidad local, tales como la posibilidad de efectuar el pago de las nóminas a los trabajadores, el abono de las facturas a los proveedores o el acceso a los servicios por parte de los ciudadanos[5].

En febrero de 2023, la Diputación de Córdoba emitió un comunicado en su portal web oficial para informar sobre un ciberincidente que afectaba a sus sistemas de información. Este suceso, similar al acontecido en Segovia, se dirigió al secuestro y encriptación de los datos de la citada diputación y de la empresa provincial de gestión de tributos municipales, a las que se amenazó con divulgar la información recopilada si no abonaban las cantidades exigidas por los ciberdelincuentes. Al igual que en el supuesto anterior, la entidad local disponía de copias de respaldo, por lo que los datos encriptados han podido recuperarse en su totalidad, pero

5. Los datos empleados se han extraído de las diferentes noticias de prensa publicadas a raíz de dicho acontecimiento. Disponibles en https://acortar.link/6J7mBq y https://acortar.link/oMCk70 (consultado por última vez en abril de 2025).

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

fueron necesarias varias semanas para revertir los daños y restablecer el normal funcionamiento[6].

En julio de 2023, los servidores de la Diputación Provincial de Zaragoza se vieron comprometidos por un ciberincidente que inutilizó varios de sus servicios, impidiendo, entre otras cosas, que más de 400 empleados de dicha institución pudiesen desarrollar sus funciones con regularidad. En este caso, la detección temprana de la amenaza permitió que los técnicos del servicio de Nuevas Tecnologías de la Diputación interviniesen inmediatamente, minimizando el alcance de los perjuicios y evitando que los *hackers* tuvieran acceso a información sensible o que ejecutasen cualquier tipo de virus para infectar los sistemas informáticos. La rápida gestión del incidente posibilitó que la entidad pudiese restaurar los servicios en pocos días. Sin perjuicio de ello, ante el aumento del número de ciberataques dirigidos contra las entidades locales zaragozanas, la Diputación ha acordado declarar la urgencia en la contratación de nuevos sistemas de ciberseguridad para reforzar sus dispositivos y aplicaciones[7].

Un último ejemplo a nivel provincial lo ha protagonizado el Cabildo de Tenerife, que, por otra parte, es una víctima frecuente de esta tipología de amenazas. Según uno de sus portavoces, el Cabildo sufre una media de 100 000 ciberataques a la semana, algunos de ellos de alta gravedad. En concreto, entre 2020 y 2023, cuatro de sus entidades instrumentales dependientes (Titsa, Metropolitano de Tenerife, Balten y el IASS) fueron objeto de varios incidentes de seguridad, perpetrados mediante el método *phishing*, que han desembocado en la desviación de fondos por valor de 818 000 euros. Los ciberdelincuentes recurrieron a la suplantación de la identidad de los proveedores de la entidad y a la falsificación de documentos bancarios, logrando que se ordenase el abono de las facturas pendientes. Aunque estos cuatro sucesos son los más relevantes o llamativos en términos de pérdidas económicas directas, en otras ocasiones anteriores ya se habían intentado ejecutar virus informáticos dirigidos al robo y encriptación de datos[8].

6. Toda la información reflejada en el texto, para ilustrar sobre el incidente de seguridad que ha afectado a la Diputación de Córdoba, se ha obtenido de las noticias de prensa publicadas en los diarios locales. Disponibles en https://acortar.link/D6010M y https://acortar.link/mLf2kq (consultado por última vez en abril de 2025).

7. La información relativa al incidente de ciberseguridad que ha afectado a la Diputación de Zaragoza se ha obtenido a partir del Boletín Oficial de la citada Diputación y de una de las múltiples noticias de prensa publicadas en los diarios locales. Disponibles en https://acortar.link/9bfBCi y https://acortar.link/ajyBud (consultados por última vez en abril de 2025).

8. Para informar sobre el incidente de seguridad que ha afectado al Cabildo de Tenerife se han consultado algunas de las noticias de prensa publicadas en los diarios locales. Disponibles en https://acortar.link/BxkzcE y https://acortar.link/iI9wkI (consultados por última vez en abril de 2025).

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

Por su parte, en el ámbito municipal, son también incontables los municipios que han sufrido uno o múltiples ciberataques en el último lustro. A modo de ejemplo, en mayo de 2022, la empresa pública navarra Asociación Navarra de Informática Municipal (ANIMSA), que es la principal encargada de dar soporte informático a 137 ayuntamientos y a otras 35 entidades de dicha comunidad foral, fue víctima de un ciberataque. Este incidente afectó directamente a todas las mencionadas entidades, puesto que los ciberdelincuentes utilizaron un prototipo de *ransomware*, denominado *Hive*, que tiene la capacidad de buscar, encriptar y eliminar de los sistemas y de los servidores la información original y las copias de seguridad previamente efectuadas, lo que impide o dificulta la recuperación de los datos robados. La gravedad de dicho incidente obligó a estos entes locales a suspender sus respectivas webs municipales, a restringir el acceso a las sedes electrónicas, e, incluso, a inutilizar los correos electrónicos de los empleados públicos. Durante las semanas posteriores, las citadas Administraciones locales tuvieron que volver a la tramitación en papel de los expedientes y a la atención telefónica y presencial, y, en algunos casos, se han perdido datos que a priori parece que no podrán restablecerse[9].

En septiembre de 2023, los sistemas informáticos del Ayuntamiento de Sevilla fueron objeto de un ciberataque que afectó a más de cuatro mil equipos municipales. Nuevamente, se trató de un caso de secuestro de datos, dirigido a inutilizar los sistemas de la entidad local, por el cual se pidió un rescate de 1,5 millones de euros. Los dirigentes de la citada corporación, que trabajaron en la recuperación de los dispositivos informáticos, afirmaron que, tras el análisis forense realizado, no habían detectado ninguna fuga de datos personales. No obstante, la gravedad del incidente obligó a suspender el acceso a la sede electrónica del municipio, así como la tramitación electrónica de los procedimientos durante más de 40 días. En este sentido, conviene poner de manifiesto que dicha entidad local ya había sido objeto de varios ciberataques graves en años precedentes, uno de los cuales se dirigió contra la sociedad municipal de transportes, lo que obligó a desactivar la aplicación y otros servicios digitales complementarios; y, en otra ocasión, se suplantó la identidad de un contratista, efectuándose una transferencia de 962 797 euros, correspondientes al pago del alumbrado navideño[10].

9. Los datos empleados en el texto se han obtenido de un comunicado oficial publicado en el portal web de la Asociación Navarra de Informática Municipal (ANIMSA), así como de las noticias publicadas en diarios de dicha región. Disponibles en https://acortar.link/it8BT7 y https://acortar.link/8nHPJH (consultados por última vez en abril de 2025).

10. La información sobre el ciberataque al Ayuntamiento de Sevilla se ha obtenido a través de las noticias de prensa publicadas a nivel local y, muy especialmente, en el Diario de Sevilla. Disponible en https://acortar.link/iKmMIr (consultado por última vez en abril de 2025).

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

En enero de 2024, el Ayuntamiento de Teo (A Coruña), que cuenta con una población de poco más de 18 000 habitantes, fue víctima de un incidente de ciberseguridad, que obligó a paralizar la actividad administrativa del consistorio y a restringir, de forma temporal, el acceso a los sistemas informáticos para evitar una posible propagación de sus efectos. En este supuesto concreto, aunque inicialmente los delincuentes informáticos se pusieron en contacto para solicitar un rescate a la corporación local, nunca llegaron a concretar los términos y el importe del mismo. Tras dos semanas de realización de los correspondientes análisis forenses, de revisión de los servidores municipales y de recuperación de las copias de seguridad de los datos, alojadas en los servidores de la Diputación de A Coruña, el municipio pudo dar los primeros pasos para retomar su normal funcionamiento[11].

En ese mismo mes, el Ayuntamiento de Calvià (Mallorca) también sufrió un ciberataque de similares características, pero, en este caso, los *hackers* lograron acceder y secuestrar información sensible de dicho municipio, pidiendo un rescate de 10 millones de dólares. La imposibilidad de reestablecer íntegramente los sistemas informáticos y los datos obligó a dicha corporación a recuperar, durante algunas semanas, la atención presencial y telefónica y la tramitación de expedientes en formato papel, sin perjuicio de que los daños pudieron revertirse restaurando una de las copias de seguridad. No obstante, las consecuencias derivadas de este incidente de ciberseguridad fueron especialmente graves, pues los datos personales de la ciudadanía y de los empleados públicos municipales fueron difundidos a través de la *Dark Web*, ante la negativa de la entidad local a abonar las cantidades solicitadas[12].

Estos supuestos ilustran perfectamente el elevado riesgo al que se encuentran expuestos nuestros municipios y diputaciones provinciales. Además de los ejemplos enunciados en los párrafos precedentes, otras muchas entidades públicas locales, tales como las diputaciones provinciales de Jaén y Málaga, o los ayuntamientos de Madrid, Guadalajara, León, Salamanca, Torre Pacheco, Granada, Burriana, Jerez de la Frontera, Gijón, Benalmádena y Sant Antoni de Portmany, conforman la larga lista de su-

11. La información relativa al incidente de ciberseguridad que ha afectado al Ayuntamiento de Teo se ha extraído de las noticias de prensa publicadas en los diarios locales a raíz de dicho suceso. Disponibles en https://acortar.link/C38fWo y https://acortar.link/j3OFue (consultados por última vez en abril de 2025).

12. Los detalles acerca del ciberataque perpetrado contra el Ayuntamiento de Calvià se han extraído del portal web de la citada corporación local, así como de los diarios locales en los que se dio cuenta de dicho suceso. Disponibles en https://acortar.link/HGORSQ, https://acortar.link/8oMc1o y https://acortar.link/pLcpMY (consultados por última vez en abril de 2025).

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

jetos jurídico-públicos afectados por incidentes graves de ciberseguridad. Este elenco demuestra que ningún ente local se halla a salvo de esta nueva forma de criminalidad, puesto que este tipo de amenazas se han perpetrado indistintamente contra las diputaciones y ayuntamientos, con independencia de su tamaño o de sus recursos. Ahora bien, cabe presuponer que los pequeños municipios se hallan en una situación especialmente vulnerable, puesto que, a menudo, carecen de una financiación suficiente para acometer las inversiones necesarias para asegurar la resiliencia de sus sistemas informáticos[13].

3. Taxonomía de ciberataques contra entidades locales

Con carácter general, la mayoría de los ciberataques perpetrados contra las entidades locales persigue como objetivo principal la obtención de un beneficio económico, bien a través de medidas de suplantación de la identidad de proveedores o contratistas de la Administración, bien mediante la extorsión. Aunque los incidentes de ciberseguridad de esta naturaleza son los más comunes, también se han individuado otro tipo de amenazas, que se centran en difundir mensajes de reivindicación política o información falsa para generar o incrementar el malestar social.

Con el propósito de sistematizar los tipos de ciberataques que se emplean con mayor frecuencia contra las entidades locales, se ha optado por incluirlos en tres grandes categorías. En un primer grupo, se hallarían todas aquellas amenazas ejecutadas con la finalidad de acceder ilegítimamente a los datos de una entidad, normalmente con la intención de comercializar con ellos, a través de su venta en el mercado negro o pidiendo un rescate. En un segundo grupo, se encontrarían aquellos ciberataques que tratan de comprometer el normal funcionamiento de los sistemas e infraestructuras informáticas, forzando el colapso de los mismos e impidiendo que los usuarios puedan acceder a los servicios. Finalmente, en un tercer grupo, se englobarían todas aquellas prácticas consistentes en suplantar la identidad de otro sujeto con la intención de obtener información confidencial o para modificar los datos de pago de terceros con los que la Administración mantiene relaciones (contratos públicos, subvenciones, ayudas, etc.).

13. La problemática de la infrafinanciación de las entidades locales y los problemas que esto ocasiona ha sido extensamente tratada en los estudios de Velasco Caballero (2024) y Salinas *et al.* (2024).

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

3.1. El acceso ilegítimo y secuestro de datos

En este primer grupo, se incluyen, por un lado, los ataques de *ransomware*, al tratarse de una de las ciberamenazas que más afectan a las Administraciones públicas. El *ransomware* es una modalidad de ataque cibernético en virtud de la cual el *hacker* introduce un *malware* o virus informático en los servidores o sistemas de la Administración, lo que le permite bloquear el acceso o encriptar las bases de datos de dicha entidad, solicitando un rescate para que dicha información sea liberada[14]. Los ciberataques de esta naturaleza son especialmente peligrosos y complejos de gestionar[15], en cuanto que, ante la imposibilidad de satisfacer las cantidades solicitadas[16], si la entidad pública no cuenta con copias de seguridad actualizadas de sus bases de datos, que, a su vez, no se hayan visto comprometidas por el virus ejecutado, se perderá toda la información administrativa (los expedientes, los datos personales de los ciudadanos o de los empleados que prestan servicios en dicha entidad, la contabilidad, entre otros)[17].

Estos ciberataques no solo suponen un riesgo inaceptable en términos de pérdida o filtración de datos, sino que también tienen un gran impacto en la propia organización administrativa y en la gestión de los servicios públicos, puesto que el bloqueo y la suspensión de los mismos suelen durar, en el mejor de los casos, varias semanas, durante las cuales los técnicos informáticos habrán de trabajar de modo incansable para restablecer los sistemas.

Por otro lado, también es necesario reforzar y mejorar el estándar de protección de los dispositivos y servidores de las organizaciones públicas frente a aquellos ciberataques que tienen por objeto el acceso no autorizado y el robo de datos, con independencia de la finalidad perseguida por los

14. *Vid*. INCIBE (2020a: 47).

15. El INCIBE, en su guía *Ransomware. Una guía de aproximación para el empresario* (INCIBE, 2020b: 29), recomienda que no se paguen los rescates solicitados cuando se produzca la encriptación de datos, por cuanto no se garantiza que vaya a recuperarse la información perdida y, al mismo tiempo, se promueve que se siga desarrollando este tipo de ciberdelincuencia.

16. Recientemente, la Fiscalía Provincial de Pontevedra ha iniciado un proceso penal por la comisión de dos delitos de prevaricación y malversación de fondos de los que tuvo conocimiento a raíz de una denuncia, en la que se informaba sobre el pago de dos facturas irregulares por parte del Concello de Cangas que se habían destinado a pagar el rescate solicitado tras un ciberataque de *ransomware*. Información disponible en https://acortar.link/g5urFx (consultado por última vez en mayo de 2025).

17. A su vez, en el informe elaborado por SOPHOS (2020: 12), se pone de manifiesto que el pago de estos rescates suele duplicar el coste económico que las entidades han de asumir, puesto que, además del pago de las cantidades solicitadas por los *hackers*, se habrán de afrontar las inversiones necesarias para evitar que esto ocurra de nuevo.

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

ciberdelincuentes. Las Administraciones públicas locales disponen de un volumen de datos personales de los ciudadanos y sobre sectores estratégicos de la actividad administrativa[18], cuya divulgación y comercialización puede poner en riesgo a las personas, sus derechos y el normal desarrollo de las funciones públicas[19].

3.2. Los ataques de denegación de servicios

Los ciberataques de denegación de servicios, también conocidos por sus siglas en inglés DoS, son aquellos que se llevan a cabo con el propósito de bloquear el funcionamiento de un sistema, una aplicación o una máquina, con el objetivo último de superar su capacidad operativa y lograr que quede inhabilitado o temporalmente inutilizado. En los ataques DoS, los *hackers* suelen usar una misma IP para enviar solicitudes masivas a un concreto servicio que, estando programado para atender un número máximo de usuarios de forma simultánea, al recibir una mayor demanda de peticiones de las que puede gestionar de acuerdo con su configuración, ralentizará su funcionamiento o se paralizará del todo[20].

Para ejecutar un ciberataque de estas características, los delincuentes informáticos utilizan un virus (*malware*) mediante el cual infectan y se hacen con el control remoto de otros equipos, que, a su vez, se convierten en bots a su servicio, a través de los cuales se enviarán o presentarán esas solicitudes que sirven para bloquear el servidor de la entidad pública local. Este tipo de incidentes de ciberseguridad inciden, principalmente, en la accesibilidad a los portales web para consultar la información pública y en el disfrute de aquellos servicios que las Administraciones prestan en formato digital[21].

3.3. La utilización fraudulenta de la identidad de terceros

En este tercer grupo, se pueden incluir todas aquellas ciberamenazas que tienen como objetivo suplantar la identidad de una persona o de una en-

18. Para un análisis pormenorizado sobre las medidas de ciberseguridad que han de adoptarse para proteger las infraestructuras críticas, se puede consultar el documento de trabajo elaborado por la Cámara de Comercio Internacional (2024).

19. Existen varios estudios de gran interés en los que se abordan las implicaciones que puede tener un ciberataque para el derecho a la protección de datos de carácter personal. Entre estas contribuciones, se pueden mencionar, sin ánimo de exhaustividad, Ribagorda Garnacho (2021) o Domínguez Álvarez (2024).

20. *Vid*. INCIBE y Oficina de Seguridad del Internauta (2020: 24).

21. *Vid*. INCIBE (2019b).

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

tidad pública para obtener alguna ventaja, normalmente económica o de acceso a datos sensibles, valiéndose de la confianza que el receptor de la comunicación tiene en el destinatario[22].

Esta modalidad de incidentes de seguridad, consistentes en usurpar instrumentalmente la identidad de otros sujetos, puede materializarse de múltiples formas. Entre las prácticas más habituales en el ámbito del sector público se han de mencionar el *phishing* y la suplantación de identidades.

En primer lugar, el *phishing* se basa en el envío masivo de correos electrónicos o en la creación de duplicados de páginas web que simulan proceder de un organismo público o de una empresa con la que la entidad local o los particulares se habían relacionado previamente. Estos ciberataques se dirigen a los ciudadanos o a los empleados públicos, con el objetivo de que estos faciliten datos o información sensible sobre sí mismos o sobre el ente en el que prestan servicios[23]. Además, en estos correos electrónicos o webs suelen incluirse enlaces fraudulentos a través de los cuales la víctima, bien cede voluntariamente sus datos personales o bancarios rellenando un formulario que parece oficial, en cuanto cree estarse relacionando con la verdadera entidad, o bien, tras clicar en el *link* corrupto, permite que se infecten los dispositivos del ente local con un programa maligno que concede al *hacker* acceso a toda la información almacenada en los mismos[24].

A modo de ejemplo, el INCIBE ha alertado de una campaña de *phishing* dirigida a contactar con los proveedores o contratistas de diversas entidades públicas, suplantando la identidad de estas últimas, valiéndose, en algunas ocasiones, de los datos publicados en la Plataforma de Contratación del Sector Público para dotar de legitimidad al mensaje. En estas comunicaciones se requiere a los interesados para que aporten las facturas pendientes de pago y cualquier otra información sensible, para contactar a posteriori con la Administración y lograr que se desvíen las transferencias[25].

En segundo lugar, también es frecuente recurrir a estas técnicas para obtener información confidencial de las entidades locales, dirigiendo este tipo de ciberataques para sustraer las credenciales de sus empleados públicos y, muy especialmente, de aquellos que tienen atribuidos permisos o privilegios especiales para llevar a cabo determinadas operaciones finan-

22. *Vid*. INCIBE (2020a: 51).
23. *Vid*. CCN y FEMP (2021: 7).
24. *Vid*., en este sentido, Cuesta García (2020) u Ortego Ruiz (2024: 385 y ss.).
25. Se puede acceder a la información utilizada en el cuerpo del texto a través del siguiente enlace: https://www.incibe.es/node/526827 (consultado por última vez en abril de 2025).

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

cieras. Se trata de incidentes de seguridad especialmente graves, porque no solo permiten a los ciberdelincuentes efectuar determinadas actuaciones con un enorme potencial lesivo dentro de la organización, sino que también podrán utilizar la identidad de ese usuario para ponerse en contacto con terceros.

Por último, entre los ciberataques basados en la suplantación de la identidad, es necesario hacer una mención específica a todos aquellos supuestos de estafas en los que los *hackers* se hacen pasar por contratistas de entidades locales, enviándoles facturas falsificadas, e informando de que todavía no han recibido el pago de las mismas. Normalmente, en la documentación presentada solicitan que se actualice el número de cuenta al que ha de efectuarse el pago, logrando desviar los fondos sin que el verdadero contratista sea consciente de lo que está ocurriendo.

Muchas entidades locales han sido víctimas de esta tipología de ciberataques; entre ellas, el propio *Institut Municipal d'Informàtica* del Ayuntamiento de Barcelona, órgano especializado en la materia, que abonó 13 facturas por importe de más de 350 000 euros, ardid que no se descubrió hasta varios meses después, cuando los verdaderos proveedores requirieron a dicha entidad para que abonase el importe de esos contratos[26]. Esto mismo le ha ocurrido al Ayuntamiento de Palma, que efectuó un pago de más de 300 000 euros, que iba dirigido a la empresa Samyl, adjudicataria del servicio municipal de limpieza[27], o al Ayuntamiento de Vitoria, al que se le han estafado 90 000 euros a través de esta misma modalidad de ciberataque[28], entre otros muchos ejemplos que se podrían traer a colación.

4. El grado de madurez y resiliencia en materia de ciberseguridad de los entes locales

El deber de proteger las infraestructuras y los sistemas de información, así como de asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones

26. Los detalles acerca del ciberataque perpetrado contra el Institut Municipal d'Informàtica del Ayuntamiento de Barcelona se han extraído del diario La Vanguardia. Disponible en https://acortar.link/5hBqgB (consultado por última vez en abril de 2025).

27. Se puede profundizar acerca del ciberataque de *phishing* dirigido contra el Ayuntamiento de Palma en el siguiente enlace: https://acortar.link/DQrIIc (consultado por última vez en abril de 2025).

28. Los detalles de este ciberataque se comunicaron mediante un post publicado en la bitácora del INCIBE-CERT, disponible en https://acortar.link/qKy9MP (consultada por última vez en abril de 2025).

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

y servicios digitales utilizados por las entidades locales para el ejercicio de sus competencias y el desarrollo de sus funciones, impone a estas Administraciones la obligación de implementar los procedimientos y las herramientas que resulten adecuadas para garantizar la resiliencia de sus sistemas, ajustándose a los parámetros de seguridad definidos en el Esquema Nacional de Seguridad (en lo sucesivo, ENS)[29]. Para lograr el establecimiento de una adecuada política de seguridad de los sistemas de información pública, en el artículo 31 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, se ordena la realización periódica, como mínimo cada dos años, de una auditoría regular ordinaria, mediante la cual se verifique el cumplimiento de los requerimientos exigidos en dicha norma.

Además, algunos órganos de control externo como la Sindicatura de Comptes de la Comunidad Valenciana, la Sindicatura de Comptes de Cataluña, el Consello de Contas de Galicia o el Consejo de Cuentas de Castilla y León, realizan auditorías propias que permiten medir el nivel de madurez y de resiliencia de los sistemas de información de los entes locales situados en sus respectivos ámbitos territoriales de actuación. Los resultados derivados de las mismas son esenciales para detectar y corregir las posibles vulnerabilidades existentes en estas organizaciones, contribuyendo a configurar servicios e infraestructuras resistentes frente a los inevitables ciberataques que se perpetrarán contra aquellas.

Para simplificar la labor de estos organismos, se ha publicado la guía práctica *GPF-OCEX 5311 Ciberseguridad, seguridad de la información y auditoría externa*. En ella, se describen sucintamente tres posibles enfoques para abordar la realización de estas auditorías en materia de ciberseguridad. Una primera opción consistiría en la realización de una evaluación completa y exhaustiva. Para acometer este examen con un nivel óptimo de profundidad y rigor, se precisaría que tanto el órgano auditor como el ente auditado dispusiesen de un gran volumen de medios materiales y personales. Una segunda posibilidad permitiría restringir el alcance de la auditoría, analizando únicamente los sistemas que estén directamente relacionados con áreas estratégicas de la actividad administrativa, en especial aquellas que afecten a la gestión financiera de la entidad local. Por último, como tercera alternativa y, *de facto*, aquella que están empleando los órganos

29. A este respecto, es necesario recordar que, de conformidad con el artículo 2.1 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, las disposiciones previstas en dicha norma resultan de aplicación a todos los entes integrantes del sector público, incluidas, naturalmente, las entidades locales.

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

autonómicos de control externo, se fundamenta en la revisión de los denominados controles básicos en materia de ciberseguridad[30].

Este tipo de auditorías se efectúan sobre algunos aspectos esenciales de los sistemas informáticos de la organización, seleccionando aquellos ámbitos que permiten comprobar el nivel general de ciberseguridad de la entidad. Esto es, no se acomete un examen completo y exhaustivo, sino que se seleccionan elementos concretos a partir de los cuales es posible obtener una visión global acerca de la situación del ente fiscalizado. En definitiva, se trata de un conjunto de controles que, a pesar de su alcance limitado, pueden ser determinantes para lograr una reducción significativa del número de ciberataques exitosos.

En los informes de los órganos autonómicos de control externo que se han publicado hasta el momento, se ha optado por examinar los siguientes ocho parámetros: CBCS 1. inventario y control de dispositivos físicos; CBCS 2. inventario y control de *software* autorizado y no autorizado; CBCS 3. la existencia de un proceso continuo de identificación y remediación de vulnerabilidades; CBCS 4. el uso controlado de privilegios administrativos; CBCS 5. la implementación de configuraciones seguras de *software* y *hardware* de dispositivos móviles (portátiles, equipos de sobremesa y servidores); CBCS 6. el registro de la actividad de los usuarios; CBCS 7. la realización de copias de seguridad de datos y sistemas; y CBCS 8. análisis sobre el nivel de cumplimiento normativo (en concreto: ENS, legislación sobre protección de datos y la Ley 25/2023, de 27 de diciembre)[31].

Una vez evaluados todos estos elementos, a cada uno de ellos se le atribuye una puntuación, lo que da lugar al denominado índice de madurez de los sistemas, que equivale a la capacidad de resistencia que tiene el ente local frente a ciberataques, otorgándole un valor de entre 0 y 100 %. Esto, a su vez, sirve como punto de partida para medir el índice de cumplimiento, fijado en función del tipo de sistema auditado. Por su parte, el índice de cumplimiento se obtiene de comparar el grado de madurez con el nivel mínimo de seguridad que se exige en el ENS para esa específica categoría de sistemas. En este sentido, es necesario tener presente que el ENS exige que todos los dispositivos y aplicaciones empleados por las Administracio-

30. *Vid*. Comisión Técnica de los OCEX (2017: 7-10).

31. Para un análisis más detallado acerca de los distintos elementos que se examinan dentro de cada uno de los controles básicos en materia de ciberseguridad, se puede consultar Comisión Técnica de los OCEX (2018: 4 y ss.).

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

nes públicas tengan, como mínimo, una calificación L3, equivalente a un grado de madurez del 80 %[32].

Con carácter previo a exponer de forma sistemática los principales resultados obtenidos a partir de los informes de los órganos de control externo, conviene aclarar que el objetivo de este estudio no es efectuar una revisión exhaustiva acerca del estado de la ciberseguridad en todos los entes locales españoles. En parte, porque no todas las comunidades autónomas cuentan con un órgano de control externo e, incluso, entre aquellas que sí lo tienen, no todos ellos han emitido informes sobre los controles básicos en materia de ciberseguridad. Por tanto, partiendo de esta premisa, únicamente es posible comparar el nivel de madurez de los sistemas de ciberseguridad de algunos de los ayuntamientos y diputaciones provinciales de Castilla y León, Cataluña, Galicia y la Comunidad Valenciana, sin perjuicio de que las vulnerabilidades detectadas y las propuestas de mejora que se formularán al final del presente estudio puedan extrapolarse a cualquier entidad local.

4.1. El inventario y control de los dispositivos físicos

El CBCS 1 tiene como objetivo verificar la existencia de un adecuado proceso de gestión de los sistemas informáticos existentes en la entidad pública, no solo de los ordenadores en sentido estricto, sino también de otros dispositivos que se hallen conectados a la red de la organización, tales como impresoras, móviles, tabletas o cualquier otro equipo, incluidos los de uso personal de los empleados públicos cuando estos tengan acceso a dicha red[33]. La realización de este inventario permite determinar exactamente los activos informáticos que se están utilizando en la corporación local, para poder definir una política de seguridad que se adapte a sus necesidades e implementar aquellas medidas que resulten adecuadas para asegurar que dichos dispositivos estén protegidos frente a accesos no autorizados[34].

32. *Vid*. CCN (2020: 9-10).

33. En este sentido, en CCN (2017: 36) se señala la información mínima que debería hacerse constar en el inventario de activos. En concreto, será necesario describir los siguientes extremos: el fabricante, modelo y número de serie de los equipos; su configuración general; el *software* que se ha instalado para llevar cabo las funciones; el equipamiento de red; la ubicación y la propiedad del activo, esto es, la persona responsable del mismo.

34. *Vid*. Comisión Técnica de los OCEX (2018: 9-10).

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

Con carácter general, casi todos los ayuntamientos auditados disponen de un inventario de sus sistemas informáticos[35]. No obstante, la mayoría de ellos no contienen una relación completa de todos los equipos y dispositivos utilizados por la entidad para el desarrollo de sus funciones, ni tampoco cuentan con un procedimiento formalizado y automático para darlos de alta y de baja, lo que impide asegurar un nivel óptimo de protección.

Así pues, tras la revisión de los informes emitidos por los órganos de control externo, es posible constatar una notable disparidad entre las cuatro comunidades autónomas examinadas. Así, en la mayoría de los ayuntamientos valencianos y en los tres ayuntamientos catalanes auditados, se logra alcanzar el estándar mínimo de cumplimiento. En cambio, en prácticamente todos los municipios de Castilla y León (exceptuando Salamanca) y en tres de las cuatro diputaciones provinciales gallegas (Lugo, Ourense y Pontevedra) no se ha logrado implementar un nivel de salvaguardias mínimo para alcanzar un índice de cumplimiento cercano al 80 %.

En dichos informes se identifican un conjunto de debilidades comunes, en mayor o menor medida, a todas las entidades locales[36]. En concreto, se ha constatado que muchas de estas organizaciones no disponen de personal suficiente que esté formado específicamente en el sector de las nuevas tecnologías. Esto implica que muchos de los puestos de trabajo ligados a las áreas TIC, pese a estar recogidos en las RPT, no se hallan todavía cubiertos o únicamente logran ocuparse transitoriamente con personal interino, lo que impide desarrollar e implementar medidas de ciberseguridad efectivas. Esto se justifica, en parte, por la falta de aprobación de una política de seguridad clara, en la que, por un lado, se defina la estrategia general de protección de la organización, y, por otro lado, se diseñe la estructura organizativa interna y se proceda al nombramiento de los distintos responsables que en cada caso serán competentes para gestionar la seguridad informática del ente local.

Además, también se ha verificado que en varias de estas organizaciones se acumulan, en una única persona, muchas de las tareas y funciones relacionadas con la gestión de la seguridad informática y la protección de datos. La inexistencia de una distribución efectiva de las responsabilidades en materia de seguridad entre varios sujetos supone un claro riesgo en

35. Entre las entidades locales que cumplen con mayor solvencia este primer control básico en materia de ciberseguridad se pueden destacar, a modo de ejemplo, la Diputación Provincial de A Coruña o los ayuntamientos de Salamanca, Mataró, Elda y Benidorm.

36. *Vid*. en este sentido, sin ánimo de exhaustividad, Consejo de Cuentas de Castilla y León (2024a: 24).

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

caso de ciberataque, puesto que se reducen las barreras de seguridad que el *hacker* tendrá que superar para hacerse con el control de la entidad local.

4.2. El inventario y control de *software* autorizado y no autorizado

El CBCS 2 se orienta a examinar el modo en que se gestionan los sistemas de *software*; en concreto, se emplea para comprobar si existen cortapisas suficientes para restringir la capacidad individual de los empleados de instalar y ejecutar, en los dispositivos informáticos de la entidad pública, cualquier programa que no haya sido previamente auditado y autorizado por la persona u órgano responsable en materia de nuevas tecnologías[37]. Este tipo de control pretende reducir el riesgo de que se introduzca, deliberada o inconscientemente, mediante la descarga de aplicaciones o sistemas no seguros, algún *malware* que pueda comprometer la integridad y la disponibilidad de datos de la organización, o que sirva de vía de acceso al ciberdelincuente para hacerse con el control del ente local.

Para implementar eficazmente estas salvaguardias es imprescindible que la entidad local identifique y planifique adecuadamente aquellos programas o aplicaciones que precise para el desarrollo de su actividad, y, una vez individuadas las necesidades operativas de la organización, habrá de bloquear automáticamente la descarga de nuevos programas de *software* distintos de aquellos recogidos en el inventario.

Aunque no se trata de una solución infalible, sí que puede ser una medida eficaz para prevenir que los servicios digitales de los municipios y diputaciones provinciales se vean comprometidos[38]. Además, como ventaja adicional, su puesta en marcha no reviste una especial complejidad, ni requiere un gran desembolso de recursos, por lo que estará al alcance de la generalidad de entidades públicas.

En todo caso, para maximizar los beneficios derivados de esta tipología de control, es menester que el listado de sistemas autorizados se mantenga actualizado, incorporando o dando de baja los programas o aplicaciones en función de las exigencias organizativas de la entidad local. A su vez, también será preciso establecer un procedimiento formalizado para supervisar y ejecutar con agilidad las actualizaciones del *software* autorizado, cuando estas sean facilitadas por sus respectivos desarrolladores, lo que

37. *Vid*. Comisión Técnica de los OCEX (2017: 14).
38. *Vid*. Comisión Técnica de los OCEX (2018: 10).

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

permitirá aprovechar al máximo las sucesivas mejoras de rendimiento o de seguridad que se vayan incorporando.

Tras analizar las auditorías elaboradas por los distintos órganos de control externo, se constata que, en las entidades locales de Castilla y León y Galicia, la existencia de medidas de esta naturaleza es meramente anecdótica. Esto supone que, en la mayoría de los ayuntamientos de Castilla y León y en tres de las cuatro diputaciones gallegas, no se alcanza el nivel mínimo exigido para superar el segundo control básico en materia de ciberseguridad. En cambio, en los ayuntamientos catalanes y valencianos, se ha hecho un mayor esfuerzo para limitar la instalación de programas informáticos en los dispositivos municipales, superándose, en casi todos los casos, el índice de cumplimiento requerido legalmente[39].

4.3. La existencia de un procedimiento continuo de identificación y remediación de vulnerabilidades

El tercero de los controles tiene como objetivo verificar si las entidades locales disponen de un proceso continuo para obtener información acerca de las vulnerabilidades a las que se halla expuesta la organización. La identificación de estas debilidades ha de tomarse como punto de partida al establecer una política de ciberseguridad personalizada, por cuanto permitirá reducir el impacto generado por los ciberincidentes. Se trata, en definitiva, de que los municipios y diputaciones provinciales tomen conciencia de las flaquezas de que adolecen sus sistemas informáticos, con el fin de incorporar las mejoras técnicas disponibles para corregir las deficiencias detectadas[40].

Para garantizar un adecuado cumplimiento de esta previsión normativa, la entidad pública debe ir más allá de la realización de un análisis o una supervisión humanos, aunque estos se acometan por personal especializado. Para ello, aprovechando el potencial de las nuevas tecnologías, se podrían utilizar programas informáticos específicos que se hallen siempre en funcionamiento, escaneando los sistemas y tratando de localizar las posibles vulnerabilidades de la organización, sin necesidad de una interven-

39. A modo de ejemplo, se ha de destacar la magnífica labor que se lleva a cabo en las diputaciones de A Coruña y Alicante, o en los ayuntamientos de Benidorm, Elva o Mataró. En todas estas entidades locales se ha hecho un gran esfuerzo para fortalecer las medidas dirigidas a inventariar y controlar el *software* autorizado y no autorizado, superándose ampliamente el índice de cumplimiento normativo, correspondiente al 80 %.

40. *Vid*. Olano Salvador (2024: 102).

ción humana activa y directa en este sentido[41]. La correcta implantación de estas salvaguardias en materia de ciberseguridad requiere que se examinen las aplicaciones o los dispositivos que pretenda emplear la entidad local, con carácter previo a su activación, para comprobar que los mismos se ajusten al estándar de protección definido, y, que, con su incorporación, no se reduce el grado de efectividad de la política de seguridad informática.

Finalmente, tras la puesta en marcha del plan de ciberseguridad, se habrán de efectuar revisiones periódicas para verificar que los sistemas son seguros, ejecutando, en la medida de lo posible, *hackeos* éticos dirigidos a cerciorarse de que los sistemas continúen siendo ciberresilientes durante todo su ciclo de vida. Además, resultará imprescindible establecer y gestionar activamente una estrategia de mantenimiento y actualización de los dispositivos, de tal forma que, en aquellos casos en los que el fabricante notifique o alerte de posibles vulnerabilidades que afecten a los sistemas o aplicaciones, se adopten inmediatamente todas las precauciones necesarias para evitar que esa deficiencia o fallo se emplee como vía de entrada por los ciberdelincuentes.

Al igual que ocurría al examinar el CBCS1, los resultados de las auditorías realizadas por los órganos de control externo no son homogéneos, constatándose que tan solo la mitad de los entes locales sometidos a examen logran alcanzar el estándar mínimo de cumplimiento. Entre aquellos que superan el mínimo requerido se puede destacar, a título meramente ejemplificativo, el caso del Ayuntamiento de Salamanca. En dicha entidad local, se ha optado por licitar un contrato con una empresa especializada en materia de ciberseguridad, cuya principal función consiste en identificar, de forma proactiva, las debilidades que presentan los sistemas informáticos de dicho municipio y emitir, en su caso, las correspondientes alertas cuando se detecte algún problema relacionado con sus sistemas informáticos. Una vez recibida la antedicha comunicación será el propio Departamento municipal de Tecnologías de la Información y de las Comunicaciones el órgano responsable de definir e implementar las medidas y acciones que permitan contrarrestar estas deficiencias, antes de que se produzca un incidente[42].

En todo caso, los órganos autonómicos de control externo coinciden, como elemento común a mejorar en todas las entidades locales auditadas, en la necesidad de diseñar procedimientos formalizados para poder con-

41. *Vid*. Comisión Técnica de los OCEX (2018: 11).
42. *Vid*. Consejo de Cuentas de Castilla y León (2023a: 23).

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

trarrestar eficazmente las carencias en materia de seguridad informática dentro de la organización. Además, la solución óptima a este problema requiere que se avance en el desarrollo o la adquisición de programas que permitan ofrecer una respuesta automatizada, de tal forma que el éxito de este tipo de controles no se haga depender, al menos no de forma exclusiva, de la capacidad de respuesta humana de los empleados públicos.

4.4. El uso controlado de privilegios administrativos

El cuarto de los parámetros que se evalúan sirve para verificar la existencia e implementación de procesos y herramientas dirigidas a identificar, controlar, prevenir y corregir el uso, la asignación y la configuración de privilegios administrativos en los ordenadores, las redes y las aplicaciones de las entidades locales auditadas[43]. La introducción de este tipo de restricciones se ha demostrado útil a los efectos de dificultar el éxito de los ciberataques, puesto que permite reducir el número de sujetos, dentro una misma organización pública, que tienen reconocidos privilegios de administración de los sistemas informáticos. Dicho en otras palabras, se ha constatado que la atribución generalizada de poderes de administrador en todos o en la mayoría de los dispositivos o aplicaciones informáticas, la utilización de las mismas contraseñas o el hecho de compartir un único usuario entre varias personas supone que, en caso de que se produzca un incidente de ciberseguridad, el *hacker* podrá comprometer rápidamente la integridad de todos los equipos de la organización, al haber menos cortafuegos que superar.

Estas limitaciones deben fijarse buscando un equilibrio entre la comodidad y la operatividad de la actuación de los empleados públicos, puesto en relación con el nivel de riesgo que podría llevar aparejado el acceso ilegítimo a un concreto privilegio administrativo o a la información pública protegida. Así pues, ponderando conjuntamente estos elementos se podrá establecer una configuración que, sin restar efectividad al funcionamiento de la entidad, sea lo suficientemente garantista para alcanzar el índice de cumplimiento exigido en la normativa[44].

El respeto a este control básico en materia de ciberseguridad exige que se observen las siguientes cautelas: en primer lugar, el acceso a estos privilegios administrativos debe estar prohibido por defecto (desde la fase de diseño), otorgándose, de forma excepcional e individualmente, a aquellos puestos de trabajo que lo precisen para el desarrollo de sus funciones;

43. *Vid*. Comisión Técnica de los OCEX (2017: 15).
44. *Vid*., en este sentido, las consideraciones efectuadas por CCN (2017: 23).

en segundo lugar, han de quedar perfectamente identificados los sujetos que los utilizarán y la finalidad que justifica su uso; en tercer lugar, se han de implementar medidas de protección para impedir que se acceda de modo ilegítimo a los equipos o a la información de la entidad local aprovechándose de estos privilegios; en cuarto lugar, se ha de precisar, para cada entidad local, quién tendrá acceso a cada programa y dispositivo, los límites a los que se hallará sometido y la autorización que se habrá de recabar para emplearlo; en quinto lugar, en la medida en que la estructura organizativa lo permita, conviene separar en diferentes empleados públicos las tareas de autorización, utilización y control de los dispositivos informáticos; y, por último, deberían registrarse y supervisarse, de forma constante, los accesos a los equipos de la entidad local, tanto a nivel interno como remotamente.

En definitiva, con este nuevo modelo de gestión de privilegios se pretende limitar el alcance de los derechos de acceso de los usuarios, de tal forma que cada empleado público solo podrá utilizar los programas y consultar la información que sea estrictamente indispensable para el desarrollo de sus funciones. Al mismo tiempo, también se debe restringir el número de sujetos que van a tener reconocida capacidad para alterar la configuración de los equipos informáticos y aplicaciones, en especial en relación con el régimen de concesión de permisos.

Por lo que respecta a los resultados plasmados en los informes de los órganos de control externo, se constata que prácticamente todas las entidades locales auditadas han incorporado, en mayor o menor medida, algunas salvaguardias dirigidas a limitar los privilegios administrativos dentro de su organización. Ahora bien, exceptuando los casos ejemplares de la Diputación de A Coruña o de los ayuntamientos de Benidorm, Castellón de la Plana o Elda, el índice de cumplimiento de este control básico en materia de ciberseguridad se encuentra muy por debajo del estándar mínimo de cumplimiento requerido en la normativa[45].

Entre las principales prácticas de riesgo detectadas por los órganos de control externo se han de destacar: la ausencia de mecanismos de autenticación robustos para acceder a las cuentas y, muy especialmente, a aquellas con privilegios administrativos; la utilización de una única cuenta por parte de todos los sujetos que ostentan la consideración de administradores, con independencia de que estén ejercitando funciones que re-

45. A modo de ejemplo, entre aquellos entes locales que se encuentran en una situación más preocupante, ya que el índice de madurez del CBCS 4 no alcanza siquiera un 30 %, están los ayuntamientos de Astorga (0 %), Béjar (0 %), Benavente (0 %), Ciudad Rodrigo (0 %), La Bañeza (14 %), Santa Marta de Tormes (20 %), Torrevella (27,3 %), Ávila (28 %) o Mataró (30 %).

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

quieran el uso de esos privilegios especiales o no, y la falta de definición de un procedimiento para designar a los responsables que van a ocuparse de gestionar las restricciones de acceso que afectan al resto de los empleados públicos.

4.5. La existencia de configuraciones seguras de *hardware* y *software* en los sistemas informáticos y servidores de la entidad local

El quinto de los CBCS se emplea, por un lado, para verificar si la entidad local cuenta con una configuración base segura en todos sus dispositivos móviles, portátiles, equipos de sobremesa y servidores. Y, por otro lado, también servirá para evaluar si se están gestionado activamente los citados dispositivos, utilizando un procedimiento manual o automático de incorporación de cambios y configuraciones, que resulte eficaz para prevenir los ataques cibernéticos[46].

Con carácter general, cuando los fabricantes o proveedores ponen a disposición de las entidades locales los dispositivos y aplicaciones informáticas que estas han adquirido para el desempeño de sus funciones, lo hacen ofreciendo una configuración de los sistemas informáticos que pretende hacer más sencilla su instalación y utilización, sin que se tengan en cuenta o se prioricen los aspectos relacionados con la seguridad. Por tanto, tras la compra de los sistemas o programas informáticos, es esencial que los empleados públicos especialistas en TIC ejecuten las alteraciones pertinentes para asegurar que los dispositivos cuentan con unas adecuadas propiedades en materia de ciberseguridad. Es más, resulta conveniente que la incorporación de estas salvaguardias y cautelas se confíe a personal especializado, ya que, en algunos casos, pueden revestir un cierto grado de complejidad que exceda las capacidades y competencias digitales básicas que poseen la generalidad de los empleados públicos.

Con estas medidas parece que trata de extrapolarse al ámbito de la ciberseguridad un principio propio del derecho a la protección de datos[47], creándose el principio de seguridad por defecto, asegurando que las entidades locales utilicen únicamente aquellos productos y servicios que ofrezcan suficientes garantías de seguridad desde la fase de diseño y desarrollo. Para ello, es esencial que los dispositivos informáticos estén configurados de tal forma que sean sencillos de manejar, y que solo se habiliten aquellas

46. *Vid*. Comisión Técnica de los OCEX (2018: 16).
47. Sobre los principios de privacidad desde el diseño y por defecto en el ámbito de la protección de datos, se puede consultar Duaso Calés (2023) o Martínez Martínez (2019).

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

funcionalidades que sean estrictamente indispensables para llevar a cabo las tareas propias de cada órgano o puesto de trabajo, bloqueando la ejecución de nuevos programas, limitando el acceso a la información y reduciendo el número de personas autorizadas.

Esto implica, en la práctica, que las organizaciones han de apartarse del modelo tradicional, en virtud del cual se instalan en bloque paquetes de programas informáticos proporcionados por el proveedor, normalmente como complemento a la prestación principal, sin tener en cuenta las necesidades específicas de cada entidad local, puesto que esto introduce un riesgo innecesario en la gestión de los sistemas informáticos, pudiendo generar nuevas vulnerabilidades o brechas de seguridad que comprometan la integridad de los servicios y de la información pública.

Por lo que respecta al grado de cumplimiento de este control básico en materia de ciberseguridad, se constata que es otro de los principales puntos débiles en las entidades locales. En concreto, en los informes de los órganos de control externo analizados se pone de manifiesto que, en la mayoría de las organizaciones locales auditadas[48], no se ha implementado satisfactoriamente esta tipología de configuraciones seguras por defecto, y, con carácter general, tampoco se han establecido mecanismos específicos para detectar e impedir que se lleven a cabo modificaciones en la configuración de la seguridad de sus respectivos dispositivos y aplicaciones.

4.6. El control de la actividad de los usuarios

El sexto control básico en materia de ciberseguridad tiene por objeto determinar si la entidad local dispone de un procedimiento que permita registrar la actividad de los usuarios conectados a la red municipal, de tal forma que se recojan, gestionen y analicen los datos relativos a los inicios de sesión y a las acciones ejecutadas durante los mismos, todo ello con el objetivo de prevenir y detectar precozmente cualquier acceso no autorizado. Se trata, por tanto, de garantizar que los entes locales cuenten con un programa que sea capaz de dejar constancia de las personas que acceden a las aplicaciones, desde qué lugar o dispositivo lo hacen, los datos que consultan, las actuaciones que se realizan y el momento en que se efectúan dichas operaciones[49].

48. Entre aquellas entidades que se hallan más lejos de alcanzar el índice de madurez requerido, se pueden mencionar las diputaciones de Lugo y Ourense, y los ayuntamientos de Astorga, Ávila, Badalona, Béjar, Benavente, Ciudad Rodrigo, Santa Coloma de Gramenet, La Bañeza, Mataró o Santa Marta de Tormes.

49. *Vid*. Comisión Técnica de los OCEX (2018: 18).

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

En este sentido, el artículo 24 del ENS impone la obligación de registrar los movimientos y actuaciones que llevan a cabo los usuarios dentro del sistema, reteniendo aquella información que resulte necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, e identificando a la persona responsable de las mismas. Esta medida de seguridad permite asegurar la trazabilidad de la actuación de los empleados públicos o, en su caso, de los terceros que accedan ilegítimamente a los sistemas de la entidad local. Por tanto, si se produjese un ciberataque en un municipio o una diputación provincial, sería posible conocer exactamente a qué información se ha accedido y qué cambios se han introducido en los sistemas, adoptando las contramedidas necesarias para restablecer el estado de los mismos a la situación existente con carácter previo al incidente. A su vez, la recopilación y el tratamiento de esta información, a través de programas que examinen de forma automatizada esos datos, se podrían emplear como herramientas para individuar patrones anormales de comportamiento, o para establecer correlaciones anómalas a partir de las cuales emitir las correspondientes alertas[50].

Esta monitorización constante y las posteriores tareas de fiscalización y auditoría que han de efectuarse sobre la base de la información recopilada —porque aquí radica el potencial impacto que puede derivar de la implementación de este tipo de medidas— podrían ser cruciales para hacer frente a aquellos ciberataques en los que no se pretende colapsar el servicio o codificar la información de la entidad para pedir un rescate, sino que el *hacker* trata de que sus actos pasen desapercibidos para poder instalar virus informáticos, ejecutar programas o realizar operaciones sin que ningún empleado público se percate. En este contexto, el mero hecho de registrar los inicios de sesión y las acciones realizadas por los usuarios permitirá verificar que no se hayan producido intromisiones ilegítimas, dirigidas a comprometer la información o los sistemas informáticos de las entidades locales.

En los informes de los órganos de control externo se constata, una vez más, la existencia de una notable disparidad entre las diferentes entidades locales. Con carácter general, la mayoría de los ayuntamientos y diputaciones provinciales auditados no alcanzan el estándar mínimo de ciberseguridad exigido, ya que carecen de un registro que reúna las características mencionadas en los párrafos anteriores[51]. Sin perjuicio de ello, también es

50. *Vid*. CCN (2018: 5 y ss.).

51. A modo de ejemplo, entre aquellos ayuntamientos que se encuentran más lejos de satisfacer el índice de madurez requerido se pueden mencionar los de Badalona, Béjar,

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

necesario destacar que, en aquellas entidades locales en las que existe una política de ciberseguridad más desarrollada, este control básico suele ser uno de los índices en los que se obtiene una puntuación más elevada[52].

Además, entre las principales deficiencias detectadas se ha de mencionar la ausencia de procedimientos definidos para gestionar el funcionamiento de este registro, tales como la información que se va a recopilar, el período de conservación de esos datos o las medidas que se van a adoptar si se constata algún acceso no autorizado. Incluso en aquellos supuestos en los que se ha implementado un sistema de registro, no siempre se lleva a cabo un análisis posterior (humano o automatizado) para controlar la información obtenida, por lo que no se aprovechan al máximo las ventajas inherentes a la implantación de esta medida de ciberseguridad.

Finalmente, también es necesario poner de manifiesto que la incorrecta utilización de estos sistemas de registro puede generar conflictos relacionados con la tutela de los derechos fundamentales y laborales de las personas afectadas, ya que con ello podría incurrirse en un incumplimiento de la normativa en materia de protección de datos de carácter personal, así como vulnerarse algunos de los derechos que el ordenamiento jurídico confiere a los empleados públicos.

4.7. La realización de copias de seguridad sobre los datos y sistemas

Con el séptimo de los controles básicos en materia de ciberseguridad se pretende comprobar si las entidades locales llevan a cabo, periódicamente, copias de seguridad sobre sus dispositivos. En particular, se verificará que los municipios y diputaciones provinciales emplean procedimientos y herramientas adecuados para realizar copias de seguridad sobre su información crítica, de tal forma que, llegado el caso, sea posible acceder y recuperar la información comprometida en el menor tiempo posible. Por lo que respecta al alcance de esta medida, la copia de seguridad deberá incluir, como mínimo: aquella información que resulte necesaria para que el ente local pueda continuar desarrollando su actividad, procedente de sus aplicaciones y sistemas operativos; los datos de configuración, servicios, aplicaciones, equipos, u otros de análoga naturaleza; así como las contraseñas utilizadas para proteger la información confidencial o sensible[53].

Benavente, Ciudad Rodrigo o La Bañeza.

52. *Vid*. Comisión Técnica de los OCEX (2018: 20).
53. *Vid*. INCIBE (2018: 7-10).

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

La adopción de este tipo de precauciones se ha demostrado especialmente eficaz para restaurar el normal funcionamiento de una entidad que ha sufrido un ciberataque consistente en el secuestro y la encriptación de datos, puesto que permite minimizar las consecuencias que derivan del mismo, sin necesidad de preocuparse por el pago del rescate exigido. Asimismo, estas copias de seguridad también son fundamentales para resolver aquellos incidentes de seguridad que tienen por objeto modificar la configuración de los sistemas o la información pública contenida en las bases de datos, puesto que se podrá recuperar siempre una versión previa al ciberincidente.

En este sentido, es preciso advertir que, en algunos de los últimos ciberataques de *ransomware* dirigidos contra Administraciones públicas, se ha constatado que los virus de encriptación que emplean los ciberdelincuentes son cada vez más sofisticados. En concreto, los citados programas permiten cifrar y comprometer no solo la información de los equipos y dispositivos de la entidad local, sino también las copias de seguridad que hayan sido depositadas en otros servidores o repositorios, cuando estos estén conectados a la misma red. Para evitar que esto ocurra es esencial que al menos una de las copias de seguridad realizadas se encuentre aislada, es decir, que resulte inaccesible a través de la red utilizada por la entidad[54].

En los informes elaborados por los órganos de control externo, se pone de relieve que prácticamente todas las entidades locales sometidas a auditoría están concienciadas de la necesariedad de efectuar copias de seguridad periódicas para proteger la integridad de sus sistemas y de la información que poseen. De hecho, de los ocho parámetros que se someten a control, este es, en casi todos los casos, aquel en el que se verifica un índice más elevado de cumplimiento. Esto no significa que todos los municipios o diputaciones provinciales cumplan con el estándar legal exigido, pero sí demuestra que se trata de uno de los ámbitos a los que las entidades locales están dedicando una mayor atención[55].

Sin perjuicio de lo anterior, como regla general, los principales motivos por los que no se alcanza el nivel mínimo de ciberseguridad requerido son: la ausencia de un procedimiento formalizado que contemple los elemen-

54. *Vid*. INCIBE (2025).

55. Con carácter general, en la mayoría de las entidades locales se realizan copias de seguridad periódicas para garantizar que las Administraciones podrán recuperar la información en caso de ciberataque. Como excepción, en los ayuntamientos de Benavente, Ciudad Rodrigo, La Bañeza o Santa Marta de Tormes, el índice de madurez del CBCS 7 se mantiene todavía peligrosamente bajo.

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

tos clave para ejecutar los backups (la periodicidad, el modo de almacenamiento, etc.); no disponer de un sistema que efectúe de forma automática las copias de seguridad, confiando esta función a la disponibilidad de los empleados públicos; o la no realización de pruebas que sirvan para comprobar que la información protegida se puede restaurar si fuese necesario.

4.8. La revisión del cumplimiento de la legalidad

Por último, se ha añadido un octavo control básico en materia de ciberseguridad, en virtud del cual se examina el nivel de cumplimiento normativo respecto de diversas disposiciones relacionadas, directa o indirectamente, con la seguridad de la información. En particular, se verifica el grado de observancia del Esquema Nacional de Seguridad, de la normativa en materia de protección de datos de carácter personal y de la Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas[56].

Por lo que respecta al ENS, los órganos de control externo se centran en identificar los preceptos de esta norma que no se están respetando, y ponen en conocimiento de la entidad local las medidas que esta puede implementar para corregir dicha situación, y los eventuales riesgos que corre su organización en caso de no hacerlo. Por lo que atañe al cumplimiento de la legislación en materia de protección de datos de carácter personal, se comprueban aspectos clave, tales como que la entidad haya designado un delegado de protección de datos, que disponga del registro de actividades de tratamiento, y que se realicen las oportunas evaluaciones de impacto de las operaciones de tratamiento para precisar el nivel de riesgo inherente a la mismas. Por último, en vista de los numerosos ciberataques que se han dirigido a las entidades locales para obtener el pago de facturas, a través de la usurpación de la identidad de los contratistas y proveedores de la Administración, también se ha incluido la realización de una auditoría para garantizar que las entidades locales estén incorporando las salvaguardias previstas en la Ley 25/2013, de 27 de diciembre.

A este respecto, los informes emitidos por los órganos de control externo confirman que muy pocas de las entidades locales auditadas alcanzan el estándar mínimo exigido legalmente[57]. Por tanto, pese a tratarse de dis-

56. *Vid*. Comisión Técnica de los OCEX (2018: 4).

57. Entre aquellas entidades locales que alcanzan un elevado grado de cumplimiento normativo se pueden mencionar las diputaciones de Alicante, Castellón y A Coruña, y los ayuntamientos de Salamanca, Burgos, Badalona, Sagunt, Valencia, Paterna, Benidorm o Vigo.

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

posiciones de obligado cumplimiento, muchos municipios y diputaciones provinciales todavía no han implantado un paquete de acciones que resulte suficiente para ajustar su actuación a este marco normativo.

Finalmente, aunque todavía queda un largo camino por recorrer para mejorar y optimizar las políticas y herramientas de que disponen las organizaciones públicas para aumentar su ciberresiliencia, no se puede obviar que existe una preocupación creciente por adaptarse a este nuevo desafío. No obstante, al tratarse de ámbitos relativamente novedosos, no todas las entidades locales pueden destinar el mismo volumen de medios personales y financieros a protegerse frente a ciberataques, sin comprometer o sacrificar la prestación de otros servicios públicos. En especial, los pequeños municipios o micromunicipios[58], que carecen de la capacidad operativa y económica para afrontar este nuevo reto, precisarán de la asistencia de las diputaciones provinciales para garantizar que puedan convertirse en entornos verdaderamente seguros.

5. El futuro de la ciberseguridad en el ámbito local: iniciativas de éxito y propuestas de mejora

5.1. Experiencias piloto y buenas prácticas

5.1.1. El modelo valenciano de ciberseguridad: un ejemplo de colaboración impulsado a nivel autonómico

En 2021, la Generalitat Valenciana aprobó el Plan de Choque de Ciberseguridad para las Entidades Locales, que ha permitido desarrollar e implementar medidas de protección y de mejora de la seguridad informática y de soporte técnico en 584 entidades locales, dando lugar al denominado modelo valenciano de ciberseguridad. Este programa de colaboración entre el Gobierno autonómico y los entes locales, que ha sido seleccionado por el Centro Criptológico Nacional como modelo de excelencia, surge para paliar las dificultades que tenían algunos municipios de este territorio para establecer una política de ciberseguridad. En dicho plan se pone de manifiesto que los ayuntamientos, en especial aquellos de menores dimensiones, pese a tratarse de las Administraciones más cercanas a los ciudadanos y, por tanto, aquellas que gestionan un importante volumen de sus datos personales, a menudo no poseen los medios financieros, la capacidad téc-

58. *Vid*. Almeida Cerreda (2023: 61 y ss.).

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

nica o el personal especializado que resultan necesarios para implantar unas medidas de ciberseguridad apropiadas, lo que las convierte en un blanco fácil frente a ciberataques.

Así pues, ante el aumento del número de incidentes de seguridad, la Generalitat puso en marcha este plan de emergencia dirigido a fortalecer la resiliencia de los sistemas informáticos de sus entes locales. Para ello, se formularon tres objetivos prioritarios que requerían: la adopción de herramientas de ciberseguridad capaces de proteger a las entidades locales de los ataques más frecuentes, especialmente los de *ransomware*; desplegar sondas, esto es, programas o dispositivos dirigidos a recopilar información sobre una red o un sistema con el fin de evaluar su grado de seguridad y detectar situaciones de riesgo; y dotar a estas entidades de los conocimientos necesarios para saber cómo reaccionar frente a un ciberataque, y qué cautelas implementar inmediatamente después para minimizar su impacto en los servicios. Además, como complemento, también se prestó asistencia para que los municipios pudieran adaptar sus organizaciones a nivel interno y acreditar el cumplimiento de las obligaciones derivadas del Esquema Nacional de Seguridad[59].

5.1.2. El rol de las diputaciones provinciales en el establecimiento de un estándar de ciberseguridad adecuado a nivel municipal

Las diputaciones provinciales están llamadas a desempeñar un papel central en este ámbito, prestando soporte y asistencia a los municipios, en especial a aquellos que carecen de los medios materiales y personales necesarios para implementar de forma autónoma sus propias políticas y medidas en materia de ciberseguridad. Para ilustrar este punto, sin pretensión alguna de exhaustividad, se ha optado por seleccionar algunas experiencias y buenas prácticas puestas en marcha por los Gobiernos locales intermedios con el fin de proteger a sus respectivos ayuntamientos frente a esta nueva modalidad de delincuencia.

La Diputación de Teruel ha desarrollado un proyecto, financiado con fondos *Next Generation*, a través del cual se ha creado un Centro de Operaciones de Ciberseguridad (SOC), que asume la gestión de la seguridad informática de algunos de los municipios de dicha provincia. En esta primera

59. Para profundizar en el modelo valenciano de ciberseguridad se puede consultar la información que la Generalitat Valenciana ha puesto a disposición en su portal web. Disponible en https://acortar.link/U8gSqS y https://acortar.link/kfXfr3 (consultado por última vez en mayo de 2025).

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

fase de la iniciativa, se han visto beneficiados un total de 125 ayuntamientos, aunque se espera que vayan integrándose de modo progresivo nuevas corporaciones locales en los próximos años[60].

El citado Centro de Operaciones de Ciberseguridad da cobertura a las necesidades de vigilancia, prevención, protección y detección frente a ciberataques, al mismo tiempo que se han desarrollado otras medidas dirigidas a incrementar la capacidad de reacción y respuesta de las Administraciones locales ante este tipo de acontecimientos. En concreto, se han implantado un sistema de alerta temprana y otras herramientas previstas en el catálogo del Centro Criptológico Nacional, que permiten monitorizar constantemente la actividad de los dispositivos informáticos de las entidades locales.

La Diputación se erige, por tanto, como el ente responsable de coordinar y proveer servicios a través del Centro de Operaciones de Ciberseguridad; de proporcionar el asesoramiento técnico y el equipamiento necesario a los ayuntamientos, y de asistirles en el procedimiento de acreditación para obtener la certificación requerida en el Esquema Nacional de Seguridad.

El modelo de la Diputación de Teruel no constituye un caso aislado, ya que cada vez se encuentran más ejemplos de buenas prácticas desarrolladas por los Gobiernos locales intermedios, que promueven el desarrollo de proyectos en materia de ciberseguridad, en especial aquellos dirigidos a fortalecer la ciberresiliencia en los municipios de menores dimensiones[61]. En este sentido, se puede citar también el caso de la Diputación de Huesca, que ha proporcionado sistemas antivirus y cortafuegos a todos los municipios sitos en su territorio, al mismo tiempo que les asiste en el proceso de realización de copias de seguridad. Además, ha puesto en marcha su propio Centro de Operaciones de Seguridad, que será el órgano encargado de prevenir, monitorizar, controlar y resolver automáticamente todas aquellas incidencias de seguridad que se produzcan en las redes y los sistemas municipales y provinciales[62].

60. La información empleada se ha extraído del portal web de la propia Diputación de Teruel, disponible a través del siguiente enlace: https://acortar.link/oUJEJS (consultada por última vez en mayo de 2025).

61. En este sentido, y sin ánimo de exhaustividad, se pueden mencionar las iniciativas desarrolladas por la Diputación de Cáceres (https://acortar.link/9aqDKe), por la Diputación de Jaén (https://acortar.link/Y43U1E), por la Diputación de Palencia, que ha sido pionera en lograr que varios de sus municipios se acrediten bajo la vigencia del nuevo Esquema Nacional de Seguridad (https://acortar.link/SZtECj), o por la Diputación de Málaga (https://acortar.link/ebBLQJ) (consultados por última vez en mayo de 2025).

62. Los datos utilizados se han recabado del portal web de la Diputación de Huesca, disponibles a través del siguiente enlace: https://goo.su/kK35yu (consultado por última vez en mayo de 2025).

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

5.2. Algunas propuestas de mejora para fortalecer la ciberseguridad en los entes locales

El análisis efectuado en los epígrafes precedentes ofrece un diagnóstico claro del estado de la ciberseguridad de las entidades locales españolas, ya que, por un lado, ha permitido identificar la naturaleza y dimensionar la magnitud y el alcance de los principales incidentes en materia de ciberseguridad; y, por otro lado, también ha servido para individuar, a partir de los informes de los órganos de control externo, las debilidades comunes de que adolecen los sistemas informáticos de los municipios y diputaciones. Como complemento, en este último epígrafe, se ha optado por diseñar y desarrollar una hoja de ruta en la que se expondrán sucintamente algunas propuestas de mejora que deberían implementarse para fortalecer la resistencia de las organizaciones públicas frente a ciberataques.

En primer lugar, es esencial que estas Administraciones aborden la compleja tarea de definir una política propia en materia de ciberseguridad. Para ello, se puede recurrir a instrumentos como las estrategias, los planes y los programas[63], que resultan de gran utilidad para garantizar que la organización cuente en todo momento con las herramientas necesarias para minimizar las posibilidades de que se produzca un ciberataque o para responder ante uno de ellos del modo más eficaz posible. La aprobación de una adecuada política de seguridad informática permitirá establecer reglas y procedimientos claros para determinar la información y los sistemas que deban protegerse, en función de los riesgos a los que se hallen expuestos y de su criticidad; configurar sistemas que sirvan para identificar tempranamente los eventuales incidentes, y articular mecanismos formalizados para responder ágilmente frente a las amenazas cibernéticas. En definitiva, la política de ciberseguridad debe ofrecer una protección integral, regulando medidas de prevención, detección y recuperación de datos para que la organización pueda defenderse frente a los ataques informáticos[64].

En segundo lugar, otra de las debilidades presentes en la mayoría de las entidades locales es la falta de empleados públicos especializados en materia de tecnologías de la información y de las comunicaciones y, muy especialmente, en el sector de la ciberseguridad. Aunque muchas de estas entidades locales han actualizado su relación de puestos de trabajo para dotarse de este tipo de perfiles, lo cierto es que les está resultando especialmente difícil dar cobertura a estas necesidades específicas de perso-

63. *Vid*. Rodríguez de Santiago (2023: 19-25) y Almeida Cerreda (2021: 413-416).
64. *Vid*. INCIBE (2019a).

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

nal, quedando vacantes al menos la mitad de los puestos convocados en la oferta pública de empleo, lo que las obliga a recurrir, en el mejor de los escenarios, a la contratación temporal.

A su vez, con el objetivo de dar cumplimiento a las obligaciones establecidas en el ENS y maximizar las posibilidades de éxito de las políticas en materia de ciberseguridad, es necesario designar a los sujetos que desempeñarán los diferentes cargos directivos estratégicos en este sector. En particular, se ha de nombrar: un responsable de la información (que será el encargado de identificar y gestionar los riesgos a los que se halla expuesta la información, y determinará los requisitos de seguridad que se han de implementar para su protección); un responsable del servicio (a quien corresponderá fijar las medidas de protección frente a las ciberamenazas que puedan comprometer los servicios públicos); un responsable de la seguridad (que ostentará la facultad para establecer la política general de seguridad, configurando los requisitos que han de observarse para proteger la información y los servicios); y un responsable del sistema (que se encargará de gestionar la forma de implantación de la política de seguridad de los dispositivos, así como de la supervisión de las operaciones diarias).

En tercer lugar, es preciso aumentar la alfabetización y la capacitación de los empleados públicos en materia de ciberseguridad, ya que los *hackers*, a menudo, dirigen ciberataques de *phishing* masivamente al personal de la Administración, con el objetivo de sustraerles información personal o para utilizarlos como vía de acceso para la posterior descarga y ejecución de algún virus informático. Para evitar este tipo de amenazas es imprescindible que se realicen cursos de difusión y concienciación en los que se expliquen, de forma clara y accesible, los incidentes de seguridad más comunes que se dirigen contra las entidades locales, y las cautelas que han de adoptarse para prevenirlos.

En cuarto lugar, para poder implementar eficazmente las políticas y medidas en materia de seguridad informática es esencial que, con carácter previo, se lleve a cabo una auditoría interna que permita determinar las necesidades específicas de cada entidad local. Para ello, primeramente, se ha de realizar una adecuada categorización de los sistemas existentes en la organización, lo que permitirá identificar los dispositivos y la información que los municipios y las diputaciones provinciales han de gestionar. A continuación, se efectuará una clasificación, atendiendo al nivel de riesgo y al posible impacto negativo que podría derivar de un ciberataque. Finalmente, en función del grado de riesgo, se establecerán unas medidas de ciberseguridad más o menos intensas.

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

En quinto lugar, se ha de aumentar la inversión en sistemas de ciberseguridad. La mayoría de las Administraciones locales que han sido sometidas a una auditoría no disponen de procedimientos automatizados para la realización de algunas de las tareas más relevantes relacionadas con la seguridad informática, por lo que el funcionamiento de todo el sistema se sustenta sobre la base de la confianza en que las personas físicas, responsables de las distintas secciones, supervisarán y ejecutarán manualmente todas las actuaciones necesarias. No obstante, este modelo ya se ha demostrado manifiestamente insuficiente para asegurar un adecuado nivel de protección, debiendo apostarse por la automatización de todos estos procedimientos[65].

En sexto lugar, pese a que, en mayor o menor medida, todas las entidades locales ya realizan copias de respaldo para garantizar la integridad de su información y de sus sistemas, conviene que los procedimientos de gestión de los backups se perfeccionen. Así, por un lado, esta tarea debe automatizarse, de modo que se programe su realización automática con una frecuencia adecuada en función de la información de que se trate. Esta medida garantiza que, en caso de producirse un ciberataque o una mera pérdida o destrucción involuntaria de información, será posible restaurar una copia reciente. Por otro lado, tal y como se anticipó anteriormente, los órganos de control externo han alertado de una nueva tipología de ciberataque de *ransomware* más sofisticado, capaz de extender el virus de encriptación a las copias de seguridad cuando las mismas se alojan en servidores que están conectados a la misma red que el resto de los dispositivos de la organización, por lo que deberán establecerse medidas adicionales dirigidas a mantener aisladas estas versiones de respaldo del resto de datos del ente local.

De acuerdo con el INCIBE, el método más seguro requiere implementar la "estrategia 3-2-1", porque maximiza las posibilidades de recuperar cualquier información perdida o encriptada, incluso frente a los incidentes de seguridad más avanzados. Para poner en marcha esta estrategia es necesario crear y mantener actualizadas tres copias de seguridad de cada uno de los ficheros que contengan información relevante de la entidad local. A continuación, los *backups* previamente realizados habrán de almacenarse, como mínimo, en dos soportes distintos (servidores externos, nube, discos duros, etc.), lo que permitirá aumentar la probabilidad de que al-

65. Esto permitirá que las entidades locales se doten de sistemas con los que escanear y detectar vulnerabilidades; efectuar copias de seguridad; llevar a cabo exámenes o pruebas para comprobar el grado de resistencia de los sistemas, todo ello de forma autónoma y en tiempo real.

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

guno de esos duplicados no llegue a verse comprometido. Finalmente, se recomienda que, como mínimo, una de esas copias de seguridad se almacene fuera de los sistemas de la organización, para impedir que el virus se extienda también a las versiones de respaldo[66].

En séptimo lugar, ha de promoverse un cambio de mentalidad en las entidades locales, abandonando, de una vez por todas, la actitud pasiva que han mantenido hasta la actualidad frente a los ciberataques, pasando a adoptar una posición proactiva tendente a reforzar los niveles de ciberseguridad existentes en sus respectivas organizaciones. Para ello, se han de realizar periódicamente procedimientos de auditoría y de autoevaluación para comprobar la existencia de debilidades de seguridad que puedan utilizarse como vía de acceso a los dispositivos de la corporación, adoptando todas aquellas medidas que resulten necesarias para contrarrestar dichas vulnerabilidades. Finalmente, en función de la capacidad técnica de cada entidad local, resultaría de gran utilidad efectuar pruebas de penetración, esto es, simulaciones de ciberataques realizados bajo la dirección de la propia entidad. Con este tipo de experimentos, se pretende detectar cualquier potencial brecha de seguridad, configuraciones inadecuadas de *hardware* o *software*, o deficiencias operativas, con carácter previo a que se produzca el verdadero ciberataque[67].

Por último, la configuración de un nivel óptimo de ciberseguridad en cualquier organización y, de modo especial, en las entidades locales, requiere llevar a cabo una adecuada programación de las necesidades[68]. La planificación se convierte en una herramienta esencial para que los municipios y las diputaciones provinciales puedan prever con la suficiente antelación la renovación de sus dispositivos tecnológicos, evitando que, con el paso del tiempo, estos queden obsoletos y, por ello, resulten más vulnerables ante las amenazas de ciberseguridad.

6. Bibliografía

Almeida Cerreda, M. (2021). Colaboración y planificación interadministrativa para la consecución de una distribución equilibrada de la población sobre el territorio. En F. J. Sanz Larruga y L. Míguez Macho (dirs.).

66. *Vid*. INCIBE (2018).
67. *Vid*. INCIBE (2017: 28).
68. *Vid*., sobre la importancia de llevar a cabo una adecuada planificación en las Administraciones públicas, y el modo en que esta debe efectuarse para aprovechar todas sus potencialidades, Almeida Cerreda (2021: 413-416).

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

Derecho y dinamización e innovación rural (pp. 399-439). Valencia: Tirant lo Blanch.

Almeida Cerreda, M. (2023). Un posible régimen especial para los pequeños municipios: justificación, naturaleza, contenido y articulación. *Revista de Estudios de la Administración Local y Autonómica*, 19, 59-81.

Cámara de Comercio Internacional. (2024). *Protección de la ciberseguridad de las infraestructuras críticas y sus cadenas de suministro*. Disponible en https://acortar.link/BhLH7i (consultado por última vez en abril de 2025).

CCN. (2017). *Guía de Seguridad de las TIC CCN-STIC 804*. Disponible en https://acortar.link/B2Ivju (consultada por última vez en mayo de 2025).

CCN. (2018). *Guía de Seguridad de las TIC CCN-STIC 831*. Registro de la actividad de los usuarios. Disponible en https://acortar.link/LEG0J8 (consultado por última vez en mayo de 2025).

CCN. (2020). *Guía de Seguridad de las TIC CCN-STIC 824*. Informe nacional del estado de seguridad de los sistemas TIC. Disponible en https://acortar.link/xSRKpD (consultado por última vez en abril de 2025).

CCN y FEMP. (2021). *Prontuario de ciberseguridad para entidades locales*. Disponible en https://acortar.link/whD6Zp (consultado por última vez en abril de 2025).

CCN-CERT IA-04/24. (2024). *Ciberamenazas y Tendencias. Edición 2024. Análisis de las ciberamenazas nacionales e internacionales, de su evolución y tendencias futuras*. Disponible en https://acortar.link/ZarAcj (consultado por última vez en abril de 2025).

Comisión Técnica de los OCEX. (2017). *Guía práctica de fiscalización de los OCEX. GPF-OCEX 5311. Ciberseguridad, seguridad de la información y auditoría externa*. Disponible en https://acortar.link/lGGIF8 (consultada por última vez en febrero de 2025).

Comisión Técnica de los OCEX. (2018). *Guía práctica de fiscalización de los OCEX. GPF-OCEX 5313. Revisión de los controles básicos de ciberseguridad*. Disponible en https://acortar.link/dzx5sa (consultada por última vez en abril de 2025).

Consejo de Cuentas de Castilla y León. (2021a). *Análisis de la seguridad informática del Ayuntamiento de Astorga (León)*. Disponible en https://acortar.link/4W7nsk (consultado por última vez en mayo de 2025).

Consejo de Cuentas de Castilla y León. (2021b). *Análisis de la seguridad informática del Ayuntamiento de Béjar (Salamanca*). Disponible en https://acortar.link/YuLqNl (consultado por última vez en mayo de 2025).

Consejo de Cuentas de Castilla y León. (2021c). *Análisis de la seguridad informática del Ayuntamiento de Benavente (Zamora)*. Disponible

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

en https://acortar.link/ByuypO (consultado por última vez en mayo de 2025).

Consejo de Cuentas de Castilla y León. (2021d). *Análisis de la seguridad informática del Ayuntamiento de Ciudad Rodrigo (Salamanca)*. Disponible en https://acortar.link/7oMByQ (consultado por última vez en mayo de 2025).

Consejo de Cuentas de Castilla y León. (2021e). *Análisis de la seguridad informática del Ayuntamiento de La Bañeza (León)*. Disponible en https://acortar.link/rs6TfR (consultado por última vez en mayo de 2025).

Consejo de Cuentas de Castilla y León. (2021f). *Análisis de la seguridad informática del Ayuntamiento de Santa Marta de Tormes (Salamanca)*. Disponible en https://acortar.link/bV2bh7 (consultado por última vez en mayo de 2025).

Consejo de Cuentas de Castilla y León. (2021g). *Análisis de la seguridad informática del Ayuntamiento de Villaquilambre (León)*. Disponible en https://acortar.link/rBSqjh (consultado por última vez en mayo de 2025).

Consejo de Cuentas de Castilla y León. (2022a). *Análisis de la seguridad informática del Ayuntamiento de Ávila*. Disponible en https://acortar.link/mbylEG (consultado por última vez en mayo de 2025).

Consejo de Cuentas de Castilla y León. (2022b). *Análisis de la seguridad informática del Ayuntamiento de Burgos*. Disponible en https://acortar.link/y9ooNg (consultado por última vez en mayo de 2025).

Consejo de Cuentas de Castilla y León. (2022c). *Análisis de la seguridad informática del Ayuntamiento de Palencia*. Disponible en https://acortar.link/dIKVTr (consultado por última vez en mayo de 2025).

Consejo de Cuentas de Castilla y León. (2023a). *Análisis de la seguridad informática del Ayuntamiento de Salamanca, ejercicio 2022*. Disponible en https://acortar.link/grzwws (consultado por última vez en mayo de 2025).

Consejo de Cuentas de Castilla y León. (2023b). *Análisis de la seguridad informática del Ayuntamiento de Valladolid, ejercicio 2022*. Disponible en https://acortar.link/JMQAYU (consultado por última vez en mayo de 2025).

Consejo de Cuentas de Castilla y León. (2024a). *Seguimiento de recomendaciones y actualización de la situación de seguridad informática del Ayuntamiento de Béjar (Salamanca)*. Disponible en https://acortar.link/kzcOxl (consultado por última vez en mayo de 2025).

Consejo de Cuentas de Castilla y León. (2024b). *Análisis de la seguridad informática del Ayuntamiento de León, ejercicio 2022*. Disponible

en https://acortar.link/r3USrG (consultado por última vez en mayo de 2025).

Consejo de Cuentas de Castilla y León. (2025). *Análisis de la seguridad informática del Ayuntamiento de Segovia*. Disponible en https://acortar.link/DCj7QD (consultado por última vez en mayo de 2025).

Consello de Contas de Galicia. (2023a). *Informe de fiscalización de los controles básicos de ciberseguridad. Diputación de Lugo. Ejercicio 2022*. Disponible en https://acortar.link/TnuShn.

Consello de Contas de Galicia. (2023b). *Informe de fiscalización de los controles básicos de ciberseguridad. Diputación de Ourense. Ejercicio 2022*. Disponible en https://acortar.link/pYZdUf.

Consello de Contas de Galicia. (2024a). *Informe de fiscalización de los controles básicos de ciberseguridad. Diputación de A Coruña. Ejercicio 2022*. Disponible en https://acortar.link/MaRf7y.

Consello de Contas de Galicia. (2024b). *Informe de fiscalización de los controles básicos de ciberseguridad. Diputación de Pontevedra. Ejercicio 2022*. Disponible en https://acortar.link/0hJ6ge.

Consello de Contas de Galicia. (2025a). *Informe de fiscalización de los controles básicos de ciberseguridad. Ayuntamiento de A Coruña. Ejercicio 2023*. Disponible en https://acortar.link/1QlSqd.

Consello de Contas de Galicia. (2025b). *Informe de fiscalización de los controles básicos de ciberseguridad. Ayuntamiento de Ourense. Ejercicio 2023*. Disponible en https://acortar.link/raaFPz.

Consello de Contas de Galicia. (2025c). *Informe de fiscalización de los controles básicos de ciberseguridad. Ayuntamiento de Vigo. Ejercicio 2023*. Disponible en https://acortar.link/Yff1J4.

Cuesta García, V. (2020). *Phising* en la Administración Pública. *Actualidad Administrativa*, 9.

Domínguez Álvarez, J. L. (2024). El carácter poliédrico del actual sistema europeo de protección de datos de carácter personal ante la transformación digital. *Anales de la Real Academia de Doctores de España*, 9 (3), 515-546.

Duaso Calés, R. (2023). Privacidad por diseño y por defecto e innovación tecnológica: hacia un estándar global. En J. L. Piñar Mañas (dir.). *Privacidad en un mundo global* (pp. 259-287). Valencia: Tirant lo Blanch.

INCIBE. (2017). *Glosario de términos de ciberseguridad. Una guía de aproximación para el empresario*. Disponible en https://acortar.link/zJnGm3 (consultado por última vez en marzo de 2025).

INCIBE. (2018). *Copias de seguridad. Una guía de aproximación para el empresario*. Disponible en https://acortar.link/ZUl5cC (consultado por última vez en mayo de 2025).

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

INCIBE. (2019a). *La importancia de la estrategia de ciberseguridad para la industria*. Disponible en https://acortar.link/6h2lJa (consultado por última vez en mayo de 2025).

INCIBE. (2019b). *Medidas de prevención contra ataques de denegación de servicio*. Disponible en https://acortar.link/NpX9XO (consultado por última vez en abril de 2025).

INCIBE (2020a). *Guía nacional de notificación y gestión de ciberincidentes*. Disponible en https://acortar.link/9D3AF2 (consultada por última vez en abril de 2025).

INCIBE (2020b). *Ransomware. Una guía de aproximación para el empresario*. Disponible en https://acortar.link/Lbi6JL (consultada por última vez en abril de 2025).

INCIBE. (2025). *Ransomware más frecuentes y cómo afectan a las pymes*. Disponible en https://acortar.link/ejyWTr (consultado por última vez en mayo de 2025).

INCIBE y Oficina de Seguridad del Internauta. (2020). *Guía de ciberataques*. Disponible en https://acortar.link/ZO6ZT7 (consultada por última vez en abril de 2025).

Martín Delgado, I. (2016). Administración electrónica. En M.ª C. Alonso García (coord.). *Derecho público de Castilla-La Mancha: libro homenaje al profesor Luis Ortega* (pp. 327-356). Madrid: Iustel.

Martínez Martínez, R. (2019). Un cambio de paradigma. De la protección de datos desde el diseño al Derecho desde el diseño. Como moverse rápido sin romper cosas. *LA LEY Privacidad*, 1. Disponible en https://acortar.link/vfZqZ0 (consultado por última vez en marzo de 2025).

Olano Salvador, M. (2024). La importancia de los controles de ciberseguridad en las fiscalizaciones de los ICEX. *Revista Auditoría Pública*, 83, 95-104.

Ortego Ruiz, M. (2024). *Manual de privacidad, protección de datos y ciberseguridad*. Valencia: Tirant lo Blanch.

Piñar Mañas, J. L. (dir.). (2011). *Administración electrónica y ciudadanos*. Navarra: Aranzadi.

Ribagorda Garnacho, A. (2021). La seguridad del tratamiento en el ámbito de las Administraciones Públicas: la ciberseguridad (Comentario al artículo 32 RGPD y a la Disposición adicional primera LOPDGDD). En A. Troncoso Reigada (dir.). *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales* (tomo 1, pp. 2009-2032). Navarra: Aranzadi.

Rodríguez de Santiago, J. M.ª (2023). *Planes administrativos. Una teoría general del plan como forma de actuación de la Administración*. Madrid: Marcial Pons.

Salinas Peña, P., Taberner, P. A. y Vilalta Ferrer, M. (2024). Propuestas de reforma del sistema de financiación local. *Anuario de Hacienda Local,* 1, 113-143.

Sindicatura de Comptes de Catalunya. (2024). *Informe 16/2024. Ajuntament de Santa Coloma de Gramenet. Controls bàsics de ciberseguretat, exercici 2023*. Disponible en https://acortar.link/JBgT6z.

Sindicatura de Comptes de Catalunya. (2025a). Informe 25/2024. *Ajuntament de Badalona. Controls bàsics de ciberseguretat, exercici 2023*. Disponible en https://acortar.link/g4FdUZ.

Sindicatura de Comptes de Catalunya. (2025b). Informe 9/2024. *Ayuntamiento de Mataró. Controles básicos de ciberseguridad, ejercicio 2023*. Disponible en https://acortar.link/f9j1Re.

Sindicatura de Comptes de la Comunitat Valenciana. (2021). *Informe d'auditoria dels controls bàsics de ciberseguretat de la Diputació d'Alacant. Exercici 2021*. Disponible en https://acortar.link/NnVaFm.

Sindicatura de Comptes de la Comunitat Valenciana. (2022a). *Informe d'auditoria dels controls bàsics de ciberseguretat de la Diputació de Castelló. Exercici 2021*. Disponible en https://acortar.link/zchkhU.

Sindicatura de Comptes de la Comunitat Valenciana. (2022b). *Informe d'auditoria dels controls bàsics de ciberseguretat de la Diputació de València. Exercici 2021*. Disponible en https://acortar.link/HEPdmE.

Sindicatura de Comptes de la Comunitat Valenciana. (2024a). *Informe sobre les actuacions realitzades per l'Ajuntament de Castelló de la Plana per mitjà de les subvencions destinades a la transformació digital i modernització, en el marc del PRTR, i de seguiment de les recomanacions sobre els controls bàsics de ciberseguretat. Situació a 31 de desembre de 2023*. Disponible en https://acortar.link/RzF7uY.

Sindicatura de Comptes de la Comunitat Valenciana. (2024b). *Informe sobre les actuacions realitzades per l'Ajuntament de Gandia per mitjà de les subvencions destinades a la transformació digital i modernització, en el marc del PRTR, i de seguiment de les recomanacions dels informes sobre els controls bàsics de ciberseguretat. Situació a 31 de desembre de 2023*. Disponible en https://acortar.link/ERn9fh.

Sindicatura de Comptes de la Comunitat Valenciana. (2024c). *Informe sobre les actuacions realitzades per l'Ajuntament de Sant Vicent del Raspeig per mitjà de les subvencions destinades a la transformació digital i modernització, en el marc del PRTR, i de seguiment de les recomanacions dels informes sobre els controls bàsics de ciberseguretat. Situació a 31 de desembre de 2023*. Disponible en https://acortar.link/sy4fBU.

Sindicatura de Comptes de la Comunitat Valenciana. (2024d). *Informe sobre les actuacions realitzades pels ajuntaments beneficiaris de les*

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

subvencions destinades a la transformació digital i modernització, en el marc del PRTR, i de seguiment de les recomanacions sobre els controls bàsics de ciberseguretat: Ajuntament de València. Situació a 31 de desembre de 2023. Disponible en https://acortar.link/eWlVbq.

Sindicatura de Comptes de la Comunitat Valenciana. (2025a). *Informe sobre les actuacions realitzades per l'Ajuntament d'Alacant per mitjà de les subvencions destinades a la transformació digital i modernització, en el marc del PRTR, i de seguiment de les recomanacions sobre els controls bàsics de ciberseguretat. Situació a 31 de desembre de 2023*. Disponible en https://acortar.link/lJ6oHs.

Sindicatura de Comptes de la Comunitat Valenciana. (2025b). *Informe sobre les actuacions realitzades per l'Ajuntament d'Alcoi per mitjà de les subvencions destinades a la transformació digital i modernització, en el marc del PRTR, i de seguiment de les recomanacions sobre els controls bàsics de ciberseguretat. Situació a 31 de desembre de 2023*. Disponible en https://acortar.link/aROK9N.

Sindicatura de Comptes de la Comunitat Valenciana. (2025c). *Informe sobre les actuacions realitzades per l'Ajuntament de Benidorm per mitjà de les subvencions destinades a la transformació digital i modernització, en el marc del PRTR, i de seguiment de les recomanacions sobre els controls bàsics de ciberseguretat. Situació a 31 de desembre de 2023*. Disponible en https://acortar.link/xGUBKR.

Sindicatura de Comptes de la Comunitat Valenciana. (2025d). *Informe sobre les actuacions realitzades per l'Ajuntament d'Elda per mitjà de les subvencions destinades a la transformació digital i modernització, en el marc del Pla de Recuperació, Transformació i Resiliència, i de seguiment de les recomanacions sobre els controls bàsics de ciberseguretat. Situació a 31 de desembre de 2023*. Disponible en https://acortar.link/o0c9KK.

Sindicatura de Comptes de la Comunitat Valenciana. (2025e). *Informe sobre les actuacions realitzades per l'Ajuntament d'Elx per mitjà de les subvencions destinades a la transformació digital i modernització, en el marc del Pla de Recuperació, Transformació i Resiliència, i de seguiment de les recomanacions sobre els controls bàsics de ciberseguretat. Situació a 31 de desembre de 2023*. Disponible en https://acortar.link/Swl6vo.

Sindicatura de Comptes de la Comunitat Valenciana. (2025f). *Informe sobre les actuacions realitzades per l'Ajuntament d'Oriola per mitjà de les subvencions destinades a la transformació digital i modernització, en el marc del Pla de Recuperació, Transformació i Resiliència, i de seguiment de les recomanacions sobre els controls bàsics de ciber-*

seguretat. Situació a 31 de desembre de 2023. Disponible en https://acortar.link/00GXdm.

Sindicatura de Comptes de la Comunitat Valenciana. (2025g). *Informe sobre les actuacions realitzades per l'Ajuntament de Paterna per mitjà de les subvencions destinades a la transformació digital i modernització, en el marc del PRTR, i de seguiment de les recomanacions sobre els controls bàsics de ciberseguretat. Situació a 31 de desembre de 2023.* Disponible en https://acortar.link/wjJpvL.

Sindicatura de Comptes de la Comunitat Valenciana. (2025h). *Informe sobre les actuacions realitzades per l'Ajuntament de Sagunt per mitjà de les subvencions destinades a la transformació digital i modernització, en el marc del PRTR, i de seguiment de les recomanacions sobre els controls bàsics de ciberseguretat. Situació a 31 de desembre de 2023*. Disponible en https://acortar.link/FvtHp8.

Sindicatura de Comptes de la Comunitat Valenciana. (2025i). *Informe sobre les actuacions realitzades per l'Ajuntament de Torrent per mitjà de les subvencions destinades a la transformació digital i modernització, en el marc del Pla de Recuperació, Transformació i Resiliència, i de seguiment de les recomanacions sobre els controls bàsics de ciberseguretat. Situació a 31 de desembre de 2023.* Disponible en https://acortar.link/KLLsKI.

Sindicatura de Comptes de la Comunitat Valenciana. (2025j). I*nforme sobre les actuacions realitzades per l'Ajuntament de Torrevella per mitjà de les subvencions destinades a la transformació digital i modernització, en el marc del PRTR, i de seguiment de les recomanacions sobre els controls bàsics de ciberseguretat. Situació a 31 de desembre de 2023*. Disponible en https://acortar.link/qR1g49.

Sindicatura de Comptes de la Comunitat Valenciana. (2025k). *Informe sobre les actuacions realitzades per l'Ajuntament de Vila-real per mitjà de les subvencions destinades a la transformació digital i modernització, en el marc del PRTR, i de seguiment de les recomanacions sobre els controls bàsics de ciberseguretat. Situació a 31 de desembre de 2023*. Disponible en https://acortar.link/3l0Kon.

SOPHOS. (2020). *The state of Ransomware 2020. Results of an independent study of 5,000 IT managers across 26 countries*. Disponible en https://acortar.link/AFe0Ml (consultado por última vez en mayo de 2025).

Valero Torrijos, J. (2007). *El régimen jurídico de la e-Administración. El uso de medios informáticos y telemáticos en el procedimiento administrativo común* (2.ª ed.). Granada: Comares.

Velasco Caballero, F. (2024). Insuficiencia financiera y desequilibrios presupuestarios municipales. *Istituzioni del Federalismo*, 3, 533-565.

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

7. Anexo: resultados de los informes sobre controles básicos en materia de ciberseguridad elaborados por los órganos de control externo

	CBCS 1	CBCS 2	CBCS 3	CBCS 4	CBCS 5	CBCS 6	CBCS 7	CBCS 8	Índice cumpl.[69]
CONSEJO DE CUENTAS DE CASTILLA Y LEÓN									
Ayuntamiento de Astorga	0 %	39 %	0 %	0 %	0 %	29 %	63 %	11 %	**22 %**
Ayuntamiento de Ávila	33 %	38 %	40 %	28 %	30 %	36 %	61 %	10 %	**43 %**
Ayuntamiento de Béjar	29 %	17 %	0 %	0 %	20 %	13 %	48 %	36 %	**20 %**
Ayuntamiento de Benavente	23 %	13 %	0 %	0 %	16 %	10 %	39 %	29 %	**20 %**
Ayuntamiento de Burgos	53 %	47 %	37 %	62 %	36 %	48 %	73 %	78 %	**67 %**
Ayuntamiento de Ciudad Rodrigo	16 %	8 %	0 %	0 %	0 %	0 %	0 %	0 %	**4 %**
Ayuntamiento de La Bañeza	18 %	34 %	0 %	14 %	18 %	0 %	39 %	36 %	**25 %**
Ayuntamiento de León	33 %	32 %	35 %	32 %	30 %	36 %	70 %	32 %	**47 %**
Ayuntamiento de Palencia	53 %	47 %	50 %	59 %	46 %	56 %	73 %	30 %	**65 %**
Ayuntamiento de Salamanca	72 %	43 %	73 %	57 %	33 %	84 %	75 %	68 %	**79 %**
Ayuntamiento de Santa Marta de Tormes	0 %	0 %	0 %	20 %	0 %	0 %	17 %	46 %	**13 %**
Ayuntamiento de Segovia	36 %	34 %	40 %	45 %	30 %	56 %	70 %	44 %	**56 %**
Ayuntamiento de Valladolid	52 %	47 %	55 %	46 %	46 %	56 %	75 %	50 %	**67 %**
Ayuntamiento de Villaquilambre	33 %	41 %	20 %	40 %	33 %	56 %	73 %	19 %	**49 %**

69. El índice de cumplimiento del ayuntamiento analiza igualmente el nivel de madurez alcanzado, pero en relación con la exigencia aplicable en cada caso, teniendo en cuenta la categoría del sistema. Es decir, compara el índice de madurez con el nivel mínimo exigido para dicha categoría en el ENS, que en la presente auditoría es N3 (80 %) para todos los casos.

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

SINDICATURA DE COMPTES DE CATALUNYA									
Ayuntamiento de Badalona	65 %	60 %	45 %	38 %	30 %	30 %	70 %	68 %	**64,22 %**
Ayuntamiento de Mataró	79,90 %	75 %	50 %	30 %	20 %	45 %	75 %	50 %	**66,39 %**
Ayuntamiento de Santa Coloma de Gramenet	60 %	75 %	45 %	40 %	30 %	70 %	78 %	60 %	**71,56 %**

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA									
Ayuntamiento de Alcoi	63,8 %	72 %	81,5 %	61,8 %	43,2 %	81,7 %	80 %	60 %	**68 %**
Ayuntamiento de Alicante	75 %	71,5 %	66,8 %	67,9 %	47 %	77,3 %	76,7 %	65 %	**68,4 %**
Ayuntamiento de Benidorm	76,5 %	87,7 %	89 %	81 %	83,5 %	85 %	89 %	80 %	**83,6 %**
Ayuntamiento de Castellón de la Plana	67,5 %	78 %	70,2 %	72 %	41,8 %	60 %	78 %	60 %	**65,9 %**
Ayuntamiento de Elche	77,5 %	75 %	67,5 %	72,5 %	48,8 %	70 %	77,5 %	55 %	**68 %**
Ayuntamiento de Elda	78,8 %	79 %	73,1 %	70,5 %	44,1 %	67,5 %	76,5 %	65 %	**69,3 %**
Ayuntamiento de Gandía	57,4 %	51,3 %	67,5 %	61,5 %	42,4 %	70 %	60,8 %	64 %	**59,4 %**
Ayuntamiento de Oriola	56 %	64 %	61,1 %	64 %	38,6 %	64 %	65,2 %	69 %	**60,2 %**
Ayuntamiento de Paterna	46,1 %	63,7 %	59,1 %	61,7 %	40 %	67,5 %	76,2 %	75 %	**61,2 %**
Ayuntamiento de Sagunt	53,8 %	65 %	69,4 %	57,6 %	43,8 %	75 %	76,7 %	75 %	**64,5 %**
Ayuntamiento de Sant Vicent del Raspeig	49,5 %	60 %	47,9 %	61,5 %	36,6 %	49 %	57,7 %	48,5 %	**51,3 %**
Ayuntamiento de Torrent	54,8 %	56,5 %	47,1 %	60 %	52,8 %	45,3 %	73,7 %	28 %	**52,3 %**
Ayuntamiento de Torrevella	57,7 %	63,8 %	43,8 %	27,3 %	40 %	75 %	58,3 %	50 %	**52 %**
Ayuntamiento de Valencia	60,4 %	66,8 %	70,1 %	50,1 %	41,6 %	64,6 %	75,3 %	79 %	**63,5 %**

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

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA									
Ayuntamiento de Vila-Real	21,6 %	51,5 %	29 %	51,3 %	36,6 %	49 %	65 %	50 %	**44,2 %**
Diputación de Alicante	85 %	80 %	63,8 %	82 %	53,2 %	55,3 %	62 %	80 %	**86,6 %**
Diputación de Castellón	63,8 %	65 %	54,8 %	67,5 %	50,3 %	66,7 %	66,7 %	75 %	**79,6 %**
Diputación de Valencia	50,3 %	45 %	47,9 %	55,5 %	44,1 %	75 %	60 %	30 %	**63,7 %**

CONSELLO DE CONTAS DE GALICIA									
Ayuntamiento de A Coruña	55 %	58 %	38 %	58 %	45 %	48 %	73 %	74 %	**69,9 %**
Ayuntamiento de Ourense	45 %	38 %	40 %	58 %	55 %	48 %	73 %	44 %	**62,4 %**
Ayuntamiento de Vigo	55 %	55 %	40 %	58 %	55 %	53 %	68 %	77 %	**71,8 %**
Diputación de A Coruña	85 %	90 %	85 %	94 %	100 %	98 %	91 %	97 %	**115,6 %**
Diputación de Lugo	25 %	38 %	25 %	58 %	25 %	40 %	55 %	72 %	**53 %**
Diputación de Ourense	55 %	43 %	18 %	53 %	25 %	50 %	73 %	67 %	**60 %**
Diputación de Pontevedra	55 %	43 %	25 %	68 %	45 %	60 %	73 %	55 %	**66,1 %**

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

CAPÍTULO V

Herramientas de ciberdefensa: los sistemas de inteligencia artificial aplicados a la ciberseguridad

Icía Masid Urbina
Ingeniera del Área de Ciberdefensa (ISDEFE).
Desarrolla su labor en el Mando Conjunto del Ciberespacio (MCCE)

SUMARIO. 1. Introducción. 2. Descripción de los instrumentos y técnicas de ciberataque más empleados. 2.1. Principales ciberataques. *2.1.1. Malware. 2.1.2. Ransomware. 2.1.3. Phishing. 2.1.4. Ingeniería social. 2.1.5. Explotación de vulnerabilidades. 2.1.6. Denegación de servicio. 2.1.7. Acceso no autorizado a la información. 2.1.8. Suplantación. 2.1.9. Hacktivismo. 2.1.10. Amenaza interna.* 2.2. Impacto de los ciberataques en las entidades locales. **3. Revisión de los mecanismos técnicos adecuados para hacer frente de forma proactiva a ciberataques.** 3.1. Detección de patrones. 3.2. Clasificación. 3.3. Automatización. 3.4. Procesamiento del lenguaje natural. 3.5. Caso de estudio. 3.6. Beneficios de la implementación de sistemas de IA guardianes en ciberseguridad para las entidades locales. **4. Directrices para la implementación de medidas de seguridad en el uso de medios electrónicos que empleen IA. 5. Conclusiones. 6. Bibliografía.**

1. Introducción

La inteligencia artificial (IA) está transformando rápidamente el panorama de la ciberseguridad, marcando una revolución que afecta tanto a los atacantes como a los defensores. En este entorno dinámico, las entida-

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

des locales se encuentran en una posición única. Estas Administraciones manejan una vasta cantidad de datos históricos y sensibles diariamente en casi todos los ámbitos. Todos estos datos son imposibles de gestionar por los humanos. Los algoritmos permiten estudiarlos, extraer patrones y exprimir todo su potencial. Su adecuada explotación ofrece innumerables ventajas para ellas y para los ciudadanos a través de su aplicación en la gestión de los servicios públicos, en la toma de decisiones y en la ciberseguridad.

Desde una perspectiva de ciberseguridad, la IA está jugando un papel crucial en dos direcciones. Por un lado, está siendo utilizada por los cibercriminales para lanzar ataques más sofisticados, y por otro, los profesionales de la seguridad la utilizan para desarrollar defensas más robustas y proactivas. Es decir, la IA juega un papel importante en ambos bandos, tanto del lado del atacante como del lado del defensor.

En el primer caso, los atacantes están empleando técnicas de IA para automatizar y mejorar sus métodos de infiltración. Los algoritmos de aprendizaje automático les permiten identificar vulnerabilidades en los sistemas de manera más eficiente, lanzar ataques de *phishing* altamente personalizados, y evadir las detecciones tradicionales. Este uso malicioso de la IA aumenta la frecuencia y la sofisticación de los ciberataques dirigidos a las entidades locales, poniendo en riesgo la integridad de los datos y la continuidad de los servicios públicos.

Por su parte, los defensores están aprovechando la IA para fortalecer sus estrategias de ciberseguridad. Los sistemas de IA guardianes, por ejemplo, permiten a los ayuntamientos monitorizar continuamente sus redes, detectar comportamientos anómalos en tiempo real, y responder de manera automatizada a las amenazas. Estas soluciones avanzadas pueden identificar patrones de ataque previamente desconocidos, predecir posibles vulnerabilidades, y proporcionar informes detallados que facilitan la toma de decisiones informadas.

En este escenario de constante evolución, es imperativo que las entidades locales comprendan y adopten las tecnologías de IA tanto para protegerse como para anticiparse a los ciberataques. Al hacerlo, no solo salvaguardan la información y los servicios esenciales de sus ciudadanos, sino que también refuerzan la confianza pública en su capacidad para gestionar la seguridad en un mundo digital cada vez más complejo.

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

2. Descripción de los instrumentos y técnicas de ciberataque más empleados

Nuestras Administraciones reciben ataques informáticos de diverso tipo y gravedad cada día. Un factor determinante que contribuye al auge de los ciberataques contra las Administraciones públicas es el desarrollo cada vez mayor de las herramientas de ataque gracias a la IA. Y es que la IA ha revolucionado la forma en que se ejecutan los ataques cibernéticos, ya que ofrece a los ciberdelincuentes herramientas más sofisticadas y difíciles de detectar por el *software* y expertos en ciberseguridad, permitiendo lanzar ataques más complejos, precisos, personalizados y a gran escala, y, por tanto, mucho más efectivos.

El Prontuario de ciberseguridad para entidades locales, elaborado por el Centro Criptológico Nacional (CCN) y la Federación Española de Municipios y Provincias (abril, 2021), muestra la realidad de los riesgos y amenazas que emanan del ciberespacio, y que pueden amenazar el normal desenvolvimiento de los procedimientos administrativos, las funciones involucradas en el desarrollo institucional provincial o municipal, y la gestión y administración de las entidades locales. Además, establece que, aunque el nivel de amenaza varía según los ayuntamientos, todos ellos poseen información o infraestructura de interés para los ciberatacantes.

A continuación, se describen las principales amenazas presentadas en dicho prontuario, y se presenta un análisis de cómo pueden ser potenciadas por la IA cuando es utilizada de forma malintencionada por los ciberatacantes, así como el riesgo que suponen para las entidades locales.

2.1. Principales ciberataques

2.1.1. *Malware*

El prontuario lo define como un *software* malicioso, como puede ser un virus, troyano, gusano, o cualquier código o contenido que pueda tener un impacto adverso en organizaciones o individuos.

Una de las aplicaciones más importantes de la IA en el mundo del cibercrimen es la generación automatizada de *malware*. Los algoritmos de aprendizaje automático pueden analizar grandes conjuntos de datos de *malware* existente y aprender a crear variantes nuevas y únicas. Esto significa que los ciberdelincuentes pueden crear *malware* adaptado a

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

objetivos específicos, aumentando la eficacia y reduciendo la probabilidad de detección.

Por ejemplo, los ciberatacantes podrían utilizar IA para crear un *malware* de espionaje (*spyware*) altamente sofisticado, que se instalara en los sistemas de una entidad local sin ser detectado. Este *spyware* podría tener capacidades avanzadas para analizar grandes volúmenes de datos y extraer información valiosa de forma automática, como correos electrónicos, documentos internos, grabaciones de audio, y cualquier otra información sensible almacenada en los sistemas de la entidad. Gracias a la IA, el *malware* puede aprender y adaptarse para evitar ser detectado por los sistemas de seguridad, modificando su comportamiento dinámicamente en respuesta a las defensas cibernéticas, y haciendo que sea extremadamente difícil de identificar y eliminar. Esto supondría una amenaza significativa para las entidades locales, ya que puede llevar a la filtración de información sensible, comprometer la privacidad de los ciudadanos, y causar un daño duradero a la reputación y funcionalidad de la entidad.

2.1.2. *Ransomware*

Se trata de un tipo de *malware* que bloquea los sistemas o los datos de los ordenadores de sus víctimas, permitiéndoles el acceso una vez que se satisface un pago (extorsión).

La IA puede ser utilizada por ciberatacantes para crear un *ransomware* altamente sofisticado y específico para una entidad local mediante la automatización de diversas etapas del ataque.

Utilizando algoritmos de aprendizaje automático, los atacantes pueden analizar el tráfico de red y los patrones de comportamiento de los usuarios para identificar las vulnerabilidades más críticas en la infraestructura de la entidad. Una vez infiltrado, el *ransomware* potenciado por la IA puede evadir la detección mediante la modificación dinámica de su código y comportamiento. Además, puede emplear técnicas avanzadas de cifrado para asegurar que los datos sean irrecuperables sin el pago del rescate, y moverse lateralmente dentro de la red para maximizar su impacto, comprometiendo sistemas críticos y servicios esenciales.

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

2.1.3. *Phishing*

El *phishing* consiste en enviar correos electrónicos que simulan proceder de un organismo público o de una persona, persiguiendo extraer información sensible de los ciudadanos, de la propia entidad, o de sus responsables o empleados. Con la ayuda de la IA, los ciberdelincuentes suplantan la identidad de empresas en correos electrónicos muy persuasivos, animando al usuario a facilitar información personal, a clicar en enlaces o a descargar archivos adjuntos que pueden contener *software* malicioso. Es, sin duda, uno de los usos malintencionados más frecuentes de la IA por parte de los atacantes.

Los riesgos derivados de una campaña de *phishing* dirigida contra una entidad local son numerosos y graves. Entre los principales se encuentra el robo de credenciales, que puede dar a los atacantes acceso no autorizado a sistemas internos y datos sensibles, incluyendo información personal de ciudadanos y documentos críticos. Esta brecha de seguridad puede llevar a violaciones de privacidad, pérdidas económicas significativas debido a transacciones fraudulentas, y la interrupción de servicios esenciales como agua, electricidad y transporte público. Además, un ataque exitoso puede dañar gravemente la reputación de la entidad, erosionando la confianza de los ciudadanos y otras partes interesadas.

2.1.4. Ingeniería social

Consiste en la recopilación de información personal sin el uso de la tecnología, como, por ejemplo, a través de mentiras, trucos, sobornos, etc.

La IA mejora significativamente la efectividad de los ataques de ingeniería social al permitir una recopilación de información más exhaustiva, ya que puede analizar grandes volúmenes de datos de redes sociales, foros, correos electrónicos y otras fuentes públicas, para obtener información detallada sobre los objetivos. También puede crear mensajes altamente personalizados y convincentes que se dirigen a las vulnerabilidades específicas del objetivo, utilizando técnicas como el procesamiento del lenguaje natural (NLP). Estos mensajes pueden parecer provenir de colegas, amigos o familiares, aumentando su credibilidad. Además, puede generar *deepfakes*, que son simulaciones de vídeo y audio realistas, para imitar a personas de confianza. Esto puede ser utilizado para hacer llamadas telefónicas fraudulentas o enviar mensajes de vídeo falsos que persuadan al objetivo de realizar acciones específicas, como transferir dinero o revelar información confidencial.

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

Por ejemplo, un ciberatacante podría utilizar algoritmos de aprendizaje automático para analizar las redes sociales y los correos electrónicos de los empleados de una entidad local. La IA podría identificar a un empleado clave del departamento de finanzas, y recopilar información sobre sus interacciones y horarios. Usando esta información, el atacante podría crear un *deepfake* convincente de la voz del alcalde solicitando urgentemente una transferencia de fondos para un proyecto municipal crítico. El *deepfake* se enviaría como un mensaje de voz a través del sistema de comunicación interno del ayuntamiento. Debido a la personalización y el alto nivel de realismo, el empleado de finanzas, confiando en la autenticidad del mensaje, podría realizar la transferencia de fondos a una cuenta controlada por el atacante, resultando en una pérdida financiera significativa para la entidad local.

2.1.5. Explotación de vulnerabilidades

Consiste en un intento de comprometer un sistema o interrumpir un servicio mediante la explotación de las vulnerabilidades organizativas o técnicas del sistema atacado.

Los ciberdelincuentes utilizan la IA para identificar vulnerabilidades en sistemas y aplicaciones. Los algoritmos pueden analizar miles de líneas de código para encontrar debilidades que puedan explotarse. Esto acelera el proceso de encontrar vulnerabilidades y, en última instancia, facilita la creación de *exploits* que aprovechen estas debilidades.

Un ataque de explotación de vulnerabilidades con IA a una entidad local podría involucrar a un ciberatacante que utiliza una herramienta de IA avanzada para escanear y analizar continuamente la infraestructura de TI de una entidad local en busca de debilidades. La IA identifica una vulnerabilidad no parcheada en el servidor web que gestiona los servicios ciudadanos en línea. Aprovechando esta vulnerabilidad, el atacante despliega un *exploit* que le permite obtener acceso no autorizado al servidor. Una vez dentro, la IA ayuda al atacante a moverse lateralmente dentro de la red, identificando y explotando otras debilidades en sistemas interconectados. Esto permite al atacante extraer datos sensibles, como información personal de los ciudadanos y registros financieros, y potencialmente instalar *ransomware* para cifrar los sistemas críticos, dejando a la entidad local incapacitada para operar hasta que se pague un rescate.

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

2.1.6. Denegación de servicio

Se trata de la interrupción o ralentización de un servicio por múltiples peticiones, normalmente aplicaciones web.

La IA, al analizar patrones de tráfico en tiempo real, podría organizar ataques para sobrecargar los servidores de una empresa específica, adaptándose continuamente para superar sin esfuerzo las medidas de ciberseguridad, y causando interrupciones prolongadas en los servicios *online*.

Por ejemplo, un ciberatacante podría emplear una red de bots controlada por IA para coordinar un ataque masivo. La IA analiza el tráfico de red normal de los servidores de la entidad local para identificar patrones y horarios de menor resistencia. Aprovechando esta información, el atacante lanza un ataque de denegación de servicio sofisticado durante un momento crítico, como el periodo de inscripción para servicios municipales, o el pago de impuestos. La IA ajusta dinámicamente la intensidad y los vectores de ataque en tiempo real para evadir las defensas y maximizar el impacto, inundando los servidores con un volumen abrumador de solicitudes falsas. Esto provoca que los sistemas se sobrecarguen y dejen de funcionar, interrumpiendo los servicios esenciales para los ciudadanos y causando caos y frustración, además de posibles daños a la reputación de la entidad local.

2.1.7. Acceso no autorizado a la información

El prontuario define este ataque como la sustracción de credenciales de acceso mediante interceptación de tráfico o mediante el acceso a documentos físicos.

Los algoritmos de IA pueden aprender de los patrones de detección de sistemas de seguridad como *firewalls*, sistemas de detección de intrusos (IDS) y sistemas de prevención de intrusos (IPS). Utilizando esta información, la IA puede adaptar el comportamiento del ataque para evadir estas defensas, por ejemplo, modificando el tráfico de red para que parezca legítimo, o fragmentando el ataque en paquetes más pequeños y menos detectables.

También puede optimizar ataques de fuerza bruta para adivinar contraseñas de manera más eficiente. Utilizando algoritmos de aprendizaje automático, la IA puede analizar patrones comunes en la creación de contraseñas y priorizar intentos que tienen más probabilidades de éxito. Esto puede reducir significativamente el tiempo necesario para romper

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

una contraseña. Además, puede mejorar el funcionamiento de *keyloggers*, que son programas maliciosos diseñados para registrar las pulsaciones de teclas en un dispositivo infectado. La IA puede filtrar y analizar los datos recogidos para identificar automáticamente credenciales de acceso, como nombres de usuario y contraseñas, y otros datos sensibles, como números de tarjetas de crédito. O puede ser utilizada para analizar grandes volúmenes de datos robados con el fin de identificar rápidamente información valiosa, como credenciales de acceso, números de tarjetas de crédito y otros datos sensibles, facilitando así el robo de información crítica de manera eficiente y efectiva.

El riesgo de un ataque de este tipo a una entidad local es diverso y puede tener consecuencias graves y duraderas. Primero, la exposición de credenciales y documentos confidenciales puede llevar a un acceso no autorizado continuo, permitiendo a los atacantes explotar la información robada para cometer fraudes financieros, como el desvío de fondos municipales o el robo de identidades de empleados y ciudadanos. Segundo, la pérdida de datos sensibles puede resultar en la interrupción de servicios esenciales, afectando la capacidad de la entidad local para operar eficazmente y brindar servicios críticos a la comunidad. Además, la filtración de información podría dañar gravemente la reputación de la entidad local, minando la confianza de los ciudadanos y otras partes interesadas. La entidad también podría enfrentar consecuencias legales y regulatorias, incluyendo multas y sanciones por no proteger adecuadamente la información. Por último, la reparación de los sistemas comprometidos y la recuperación de la información robada pueden ser costosas y llevar mucho tiempo, impidiendo el funcionamiento normal de la entidad, y poniendo en riesgo la seguridad y el bienestar de la comunidad que sirve.

2.1.8. Suplantación

Consiste en un tipo de ataque en el que una entidad suplanta a otra para obtener beneficios ilegítimos.

La IA puede analizar grandes volúmenes de datos públicos y privados para recopilar información detallada sobre los funcionarios clave de la entidad que se pretende suplantar, como sus nombres, cargos y patrones de comunicación. Esta información se utiliza para crear perfiles detallados que facilitan la personalización del ataque.

Luego, puede generar *deepfakes* muy realistas, imitando a los funcionarios de la entidad suplantada. Estos *deepfakes* pueden ser utilizados en

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

llamadas telefónicas, videoconferencias o mensajes de voz para convencer a la entidad objetivo de que está interactuando con representantes legítimos.

También puede generar documentos falsificados pero realistas, como cartas oficiales, formularios de solicitud de fondos y contratos, que pueden ser presentados a la entidad objetivo como parte de una solicitud de fondos o recursos. Estos documentos falsos se respaldan con la información y los perfiles previamente recopilados, haciendo que el engaño sea más difícil de detectar. En conjunto, estas técnicas permiten a los atacantes obtener beneficios ilegítimos, como la transferencia de fondos o el acceso a recursos, al hacer creer a la entidad objetivo que está interactuando con otra entidad local legítima.

2.1.9. *Hacktivismo*

Se trata de ataques a sitios web o cuentas de redes sociales para publicitar una causa concreta.

Por ejemplo, un grupo activista podría querer publicitar una causa concreta, como la oposición a un proyecto de construcción en una entidad local. Para lograr una mayor visibilidad y apoyo, podría utilizar técnicas avanzadas de IA para comprometer sitios web y cuentas de redes sociales. Por ejemplo, podrían generar bots impulsados por IA que pueden crear y gestionar cuentas en redes sociales para difundir desinformación a gran escala. Estos bots pueden interactuar con usuarios reales, compartir contenido falso y amplificar narrativas engañosas. También podrían generar comentarios automáticos en la página web de la entidad local, en sus foros y redes sociales, para influir en discusiones y sembrar discordia. Estos comentarios pueden parecer genuinos y provenientes de usuarios reales.

2.1.10. Amenaza interna

Las amenazas mencionadas hasta ahora surgían por el uso malintencionado de la IA por parte de los ciberatacantes. Pero hay que tener en cuenta que no todas las amenazas provienen de fuentes externas.

Los errores humanos en el uso de la IA dentro de una entidad local representan una amenaza interna que puede tener repercusiones graves en términos de seguridad de datos, eficiencia operativa y equidad social.

Uno de los principales riesgos radica en la posibilidad de que datos sensibles o confidenciales sean manejados inadecuadamente, lo que po-

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

dría llevar a filtraciones de información o a la exposición de datos personales de los ciudadanos. Esto no solo compromete la privacidad de los individuos, sino que también puede erosionar la confianza pública en la entidad local y sus capacidades para gestionar de manera segura y efectiva la información.

Además, los errores cometidos por los empleados en el uso de la IA pueden tener consecuencias operativas significativas. Por ejemplo, si un empleado introduce datos incorrectos en un sistema de IA encargado de optimizar la asignación de recursos municipales, esto podría resultar en una distribución ineficiente de esos recursos, afectando negativamente la prestación de servicios públicos. En un contexto más crítico, la interpretación inadecuada de los análisis proporcionados por la IA podría llevar a decisiones mal fundamentadas que afecten negativamente a la planificación urbana, la seguridad pública o la gestión de emergencias.

La falta de formación y entendimiento sobre cómo funcionan los sistemas de IA también contribuye a la amenaza interna. Los empleados que no están adecuadamente capacitados pueden no ser conscientes de los sesgos inherentes en los algoritmos de IA, o de cómo sus propias acciones pueden influir en los resultados generados por estos sistemas. Esto puede perpetuar desigualdades y dar lugar a decisiones basadas en datos sesgados, exacerbando problemas sociales y económicos dentro de la comunidad.

2.2. Impacto de los ciberataques en las entidades locales

Los ciberataques a entidades locales pueden tener impactos profundos y diversos, afectando tanto a sus operaciones como a la confianza de los ciudadanos.

En primer lugar, los ataques pueden causar una interrupción significativa de los servicios esenciales. Por ejemplo, los sistemas informáticos que gestionan el suministro de agua, la recolección de basura, el transporte público y los servicios de emergencia pueden quedar paralizados, lo que resulta en la interrupción de la vida cotidiana de los ciudadanos y en retrasos y cancelaciones de servicios.

Además, los ciberataques pueden comprometer datos sensibles. La exposición de información personal, como números de seguridad social, direcciones, información de salud y datos financieros, puede tener graves consecuencias para la privacidad de los ciudadanos. La pérdida o alteración

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

de datos críticos también puede afectar la capacidad de la entidad local para operar de manera efectiva y tomar decisiones informadas.

El impacto económico de un ciberataque puede ser significativo. Los costos asociados con la recuperación de sistemas afectados, la restauración de datos y la mejora de las medidas de seguridad pueden ser elevados. En algunos casos, las entidades locales pueden verse obligadas a pagar rescates para recuperar el acceso a sus sistemas y datos.

La reputación de la entidad local también puede sufrir. La confianza del público en la capacidad de la entidad para gestionar y proteger sus intereses puede erosionarse, afectando su imagen y su relación con los ciudadanos y otras partes interesadas.

Desde una perspectiva legal y regulatoria, los ciberataques pueden tener consecuencias severas. Las entidades locales están sujetas a regulaciones de protección de datos y pueden enfrentar sanciones legales y multas si se violan estas normas. Además, los ciudadanos afectados por la exposición de sus datos personales pueden emprender acciones legales, resultando en litigios costosos.

La seguridad pública puede estar en riesgo debido a los ciberataques. Los ataques a infraestructuras críticas, como la red eléctrica o los sistemas de agua, pueden tener consecuencias graves para la seguridad de los ciudadanos. Asimismo, los ataques a los sistemas de comunicación y operación de servicios de emergencia pueden dificultar la respuesta a incidentes y emergencias.

El impacto en los empleados de la entidad local también es notable. El estrés y la ansiedad pueden aumentar debido a la presión adicional para gestionar las consecuencias del ataque, lo que puede afectar su moral y desviar su atención de otras tareas importantes.

Finalmente, los ciberataques pueden afectar la planificación y los presupuestos futuros de la entidad local. Los recursos financieros destinados a proyectos y mejoras pueden tener que ser redirigidos para abordar las consecuencias del ataque y fortalecer las defensas cibernéticas. Esto puede resultar en ajustes en las prioridades y en la planificación estratégica a largo plazo.

En definitiva, los ciberataques a entidades locales pueden tener impactos diversos que afectan todos los aspectos de su funcionamiento y relación con el público. La recuperación de un ataque requiere tiempo, re-

cursos y un esfuerzo concertado para restaurar la confianza y la seguridad. Por eso, es necesario establecer los mecanismos técnicos adecuados para hacer frente de forma proactiva a estos ataques.

3. Revisión de los mecanismos técnicos adecuados para hacer frente de forma proactiva a ciberataques

Para contrarrestar estas amenazas, se han desarrollado mecanismos técnicos avanzados, como los sistemas de IA guardianes, que permiten una defensa proactiva contra los ciberataques. En este sentido, la IA puede potenciar la ciberseguridad, y ser muy beneficiosa integrándose en estos mecanismos, mejorándolos frente a enfoques más tradicionales.

Los sistemas de IA guardianes son soluciones avanzadas diseñadas para proteger redes, sistemas y datos frente a amenazas cibernéticas. Estos sistemas utilizan tecnologías de IA, como el aprendizaje automático (*Machine Learning*) y el procesamiento del lenguaje natural (NLP), para identificar, analizar y responder a actividades sospechosas en tiempo real. A diferencia de los sistemas de seguridad tradicionales que dependen de reglas predefinidas y firmas conocidas de *malware*, los sistemas de IA guardianes tienen la capacidad de aprender y adaptarse continuamente, mejorando su efectividad a medida que recopilan y procesan más datos.

Las principales características de los sistemas de IA guardianes incluyen la detección de patrones, la clasificación, la automatización, y el procesamiento de lenguaje natural. A continuación, se detalla cómo pueden dichas características ayudar a las entidades locales a hacer frente de forma proactiva a los ciberataques.

3.1. Detección de patrones

Los sistemas de IA utilizan técnicas de aprendizaje automático para detectar patrones de comportamiento en tiempo real, y esto permite identificar comportamientos anómalos en los sistemas, y predecir posibles ataques antes de que ocurran.

Esto va a ser muy útil en la detección de vulnerabilidades en un sistema. Los sistemas de detección de intrusión (IDS) tradicionales se basan en detectar firmas o patrones conocidos. Esto significa que un tipo de ataque completamente nuevo puede no ser detectado en absoluto, porque la firma no existe en la base de datos. Por el contrario, la IA revisa el tráfico de

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

red, la actividad de los usuarios, los registros de eventos y de auditoría del sistema, en busca de actividad inusual o comportamientos sospechosos, que puedan indicar una actividad maliciosa que implique una vulnerabilidad.

Lo mismo ocurre con la detección de *malware*. Los antivirus tradicionales se basan en la detección de firmas. La IA analiza los ficheros para decir si son buenos o malos con un cierto grado de probabilidad. El veredicto no está basado en una característica, sino en múltiples características que van a dar una clasificación benigna o maligna del fichero. Esto permite extraer "el ADN" del *malware*, las características fundamentales por las que podemos decir que esto es un *malware* que se comporta como otro *malware* conocido. Por lo tanto, debe ser de la misma familia. Es decir, la IA no utiliza firmas, sino ciertas características de comportamiento o estructura de los ficheros, y determina si ese fichero está infectado por un *malware* conocido, o por un *malware* relacionado con esa familia. De esa manera, la defensa contra campañas es más efectiva, porque durante una campaña la misma familia de *malware* va mutando, y esto nos puede ayudar a ser más efectivos a la hora de detectar esa mutación de las campañas. Esto es especialmente interesante en las amenazas de tipo *zero day*, que no se pueden detectar por medios convencionales, porque aún no se han creado las firmas.

En definitiva, gracias a la capacidad de detección de patrones de la IA, una entidad local puede identificar y responder rápidamente a actividades sospechosas antes de que se conviertan en incidentes de seguridad graves. Esto no solo protege la infraestructura de red y los datos sensibles de los ciudadanos, sino que también asegura la continuidad de los servicios municipales y mantiene la confianza pública en la capacidad del ayuntamiento para salvaguardar la información y los recursos críticos.

3.2. Clasificación

Esta característica de la IA se refiere a su capacidad para categorizar datos en diferentes grupos o clases basándose en sus características y patrones. Este proceso implica que un algoritmo de IA aprende a identificar y diferenciar entre distintos tipos de datos a partir de ejemplos previamente etiquetados durante una fase de entrenamiento. Una vez entrenado, el modelo puede asignar nuevas entradas a las categorías adecuadas con un alto grado de precisión.

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

En el ámbito de la ciberseguridad, la capacidad de clasificación de la IA puede ser extremadamente útil en la caza de amenazas. Esta se basa en el descubrimiento de concatenaciones de sucesos que puedan responder a un patrón de ataque. La IA puede clasificar la información que le llega y predecir qué tipo de ataque estamos sufriendo, incluso aunque sea un ataque desconocido. O verificar si un conjunto de esos ataques que estamos viendo en los millones de ficheros que estamos analizando al día se puede atribuir a una campaña. En definitiva, enriquecer toda la inteligencia de la caza de amenazas y así mejorar las medidas preventivas.

Asimismo, la IA puede ser útil en el análisis de comportamiento. Puede clasificar comportamientos de usuarios y dispositivos para detectar actividades anómalas que podrían indicar una brecha de seguridad. Por ejemplo, si un usuario que normalmente accede a ciertos sistemas durante el horario laboral comienza a descargar grandes cantidades de datos fuera de horario, un sistema de IA podría clasificar este comportamiento como sospechoso y alertar a los administradores de seguridad.

O también en la respuesta a incidentes. Durante un incidente de seguridad, la clasificación de la IA puede ayudar a priorizar las alertas y gestionar los recursos de respuesta. Por ejemplo, la IA puede clasificar las alertas de seguridad en función de su gravedad y el potencial impacto, permitiendo a los equipos de respuesta centrarse primero en las amenazas más críticas.

Finalmente, puede ayudar en el filtrado de correo electrónico. Los sistemas de IA pueden clasificar correos electrónicos entrantes en categorías como “spam”, “phishing” o “legítimos”. Esta capacidad ayuda a prevenir que los correos electrónicos maliciosos lleguen a los usuarios finales, reduciendo el riesgo de ataques de ingeniería social y robo de información.

En resumen, la clasificación por IA puede mejorar significativamente la detección de amenazas, la protección de datos y la eficiencia operativa en la ciberseguridad de una entidad local. La IA puede analizar y clasificar correos electrónicos entrantes para detectar y bloquear mensajes maliciosos, monitorizar el comportamiento de los empleados para identificar actividades anómalas que podrían indicar una brecha de seguridad, y gestionar vulnerabilidades en los sistemas municipales, priorizando las más críticas. Además, puede proteger la infraestructura de red, al clasificar el tráfico en tiempo real y asegurar los datos personales en las solicitudes de servicios ciudadanos.

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

3.3. Automatización

La automatización es una de las características más poderosas y transformadoras de la IA. Se refiere a la capacidad de los sistemas de IA para realizar tareas y procesos de manera autónoma, sin intervención humana constante, basándose en algoritmos y modelos entrenados. En el ámbito de la ciberseguridad, la automatización puede desempeñar un papel crucial, especialmente en entidades locales como ayuntamientos y Administraciones municipales, al mejorar la eficiencia, la precisión y la rapidez de las respuestas ante amenazas.

La automatización a través de la IA mejora significativamente la ciberseguridad de una entidad local, al reducir la dependencia de la intervención humana, lo que permite una respuesta más rápida y efectiva ante amenazas. La automatización de las tareas mencionadas anteriormente, como la detección de vulnerabilidades, de *malware*, la caza de amenazas, o la respuesta a incidentes, libera a los equipos de TI de tareas repetitivas y laboriosas, y les permite centrarse en actividades estratégicas y de mayor valor añadido, como proteger los datos y servicios críticos de los ciudadanos.

Además, la IA puede automatizar la generación de informes de seguridad y cumplimiento normativo, recopilando y organizando datos relevantes de manera precisa y eficiente. Esto es especialmente útil para entidades locales que deben cumplir con regulaciones específicas sobre protección de datos y seguridad de la información. Esto reduce la carga de trabajo manual y garantiza que los informes estén siempre actualizados y listos para auditorías.

3.4. Procesamiento del lenguaje natural

El procesamiento del lenguaje natural (PLN) es una rama de la IA que se enfoca en la interacción entre los ordenadores y los seres humanos a través del lenguaje natural. El objetivo del PLN es permitir que las máquinas comprendan, interpreten y generen el lenguaje humano de una manera que sea valiosa. Estamos hablando de la IA Generativa, que está suponiendo una revolución en estos momentos, y también promete revolucionar la ciberseguridad, y ser una herramienta poderosa en este ámbito, especialmente en las entidades locales.

En primer lugar, puede ayudar a la detección de amenazas. Utilizando el PLN para analizar grandes volúmenes de datos, como correos electrónicos, mensajes y registros de actividad, se pueden identificar patrones sos-

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

pechosos y posibles amenazas. Por ejemplo, detectar correos electrónicos de *phishing* mediante el análisis del contenido del mensaje.

También puede ayudar en el análisis de vulnerabilidades, analizando informes de vulnerabilidades y alertas de seguridad, resumiendo información crucial, y sugiriendo acciones prioritarias para mitigarlas. Además, puede monitorizar estas plataformas en busca de menciones de posibles amenazas o actividades maliciosas que puedan afectar a la entidad.

Los chatbots y asistentes virtuales que utilizan PLN pueden dar soporte para responder automáticamente a consultas relacionadas con la ciberseguridad, proporcionando información y recomendaciones a los usuarios en tiempo real.

Por último, pueden ayudar a generar y analizar contenido de ciberseguridad, como políticas de seguridad, definiéndolas, revisándolas, y asegurando que estén actualizadas y cumplan con las normativas vigentes.

3.5. Caso de estudio

A continuación, se plantea un caso de uso detallado de cómo una IA puede mejorar la ciberseguridad de un ayuntamiento.

Imaginemos que un ayuntamiento ha experimentado un aumento en intentos de ciberataques dirigidos a sus sistemas administrativos, incluyendo el sistema de gestión de ciudadanos, el portal de servicios *online* y las bases de datos de empleados. Estos ataques han generado preocupación entre los funcionarios debido a la posibilidad de robo de datos sensibles y la interrupción de servicios municipales esenciales.

Para abordar estas preocupaciones, el ayuntamiento decide implementar una solución de ciberseguridad basada en IA, diseñada para detectar, responder y mitigar amenazas cibernéticas en tiempo real.

El primer paso es realizar una evaluación exhaustiva de riesgos. Esto implica identificar las áreas más vulnerables de la infraestructura tecnológica del ayuntamiento, tales como bases de datos que contienen información personal de los ciudadanos, sistemas de pago de impuestos, y redes internas que soportan la operación diaria del ayuntamiento. Basado en la evaluación inicial, el ayuntamiento selecciona una solución de IA guardián que mejor se adapta a sus necesidades específicas. Las características clave a considerar incluyen la capacidad de integración con los sistemas exis-

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

tentes, la robustez de los algoritmos de detección de anomalías, y la facilidad de uso y gestión.

Una vez seleccionada la solución, el siguiente paso es la integración con la infraestructura existente del ayuntamiento. El equipo de TI del ayuntamiento integra la IA con sus sistemas existentes. La IA se conecta a la red del ayuntamiento y a todos los dispositivos críticos, comenzando a recopilar datos sobre el tráfico y las actividades de la red.

El sistema de IA guardián necesita un período de aprendizaje para establecer una línea base de comportamiento normal dentro del entorno del ayuntamiento. Durante los primeros meses, la IA se entrena utilizando datos históricos y tráfico en tiempo real, y aprende los patrones normales de comportamiento en la red del ayuntamiento, así como las actividades típicas de los empleados y ciudadanos.

Una vez entrenada, la IA comienza a monitorizar activamente la red en busca de patrones anómalos que puedan indicar un ciberataque. Por ejemplo, detecta intentos inusuales de acceso a la base de datos de ciudadanos desde ubicaciones no autorizadas. Utilizando algoritmos de clasificación, la IA puede determinar si estos intentos son legítimos o sospechosos.

La IA detecta una actividad sospechosa que sugiere un posible ataque de *phishing* dirigido a los empleados del ayuntamiento. Utilizando su capacidad de PLN, analiza los correos electrónicos sospechosos para identificar patrones de *phishing*. Inmediatamente, la IA alerta al equipo de ciberseguridad y comienza a tomar medidas automatizadas para contener la amenaza, como bloquear los correos electrónicos sospechosos y aislar las cuentas comprometidas.

Con base en el análisis del ataque de *phishing*, la IA actualiza sus modelos de detección y mejora su capacidad para identificar correos electrónicos similares en el futuro. Además, el equipo de ciberseguridad implementa nuevas políticas de formación para empleados sobre cómo reconocer y reportar correos electrónicos sospechosos.

Es fundamental que el personal del ayuntamiento esté bien capacitado en el uso del sistema de IA guardián. Esto incluye la interpretación de alertas y reportes generados por el sistema, la comprensión de las acciones automáticas que el sistema puede tomar, y el manejo de incidentes de seguridad. La capacitación también debe abarcar la concienciación sobre las mejores prácticas de seguridad para minimizar errores humanos.

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

Después de mitigar la amenaza, la IA realiza un análisis forense para entender cómo se originó el ataque y qué vulnerabilidades fueron explotadas. Utilizando sus capacidades de detección de patrones y clasificación, la IA identifica áreas de mejora en las políticas de seguridad. Los hallazgos se utilizan para actualizar las políticas de seguridad y mejorar la respuesta a futuros incidentes.

La IA continúa aprendiendo y adaptándose a nuevas amenazas. A través de actualizaciones regulares y del aprendizaje automático, se vuelve más eficiente en la detección y mitigación de ciberataques. Su capacidad de procesamiento del lenguaje natural también se mejora continuamente, permitiendo una mejor identificación y respuesta a amenazas basadas en texto.

3.6. Beneficios de la implementación de sistemas de IA guardianes en ciberseguridad para las entidades locales

Como se ha visto en el caso de estudio anterior, al aprovechar las capacidades avanzadas de detección, análisis y respuesta de la IA, las entidades locales pueden proteger mejor sus infraestructuras críticas y datos sensibles, responder de manera eficaz a las amenazas, y optimizar el uso de sus recursos. En última instancia, esto no solo fortalece la seguridad de la información, sino que también contribuye a la confianza y satisfacción de los ciudadanos, cumpliendo con el mandato de proporcionar servicios seguros y eficientes.

A continuación, se resumen los principales beneficios para una entidad local, después de la implementación exitosa de un sistema de IA guardián.

1. Reducción de incidentes de seguridad: Con la monitorización continua y la respuesta automatizada, el número de incidentes de seguridad puede reducirse significativamente.

2. Protección mejorada de datos: Los datos sensibles de los ciudadanos y las operaciones críticas del ayuntamiento están mejor protegidos contra accesos no autorizados y filtraciones.

3. Eficiencia operativa: La automatización de tareas de monitorización y respuesta libera al personal de TI para enfocarse en proyectos estratégicos y mejorar la infraestructura tecnológica del ayuntamiento.

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

4. Confianza de los ciudadanos: Una postura de seguridad sólida y proactiva genera confianza entre los ciudadanos, quienes se sienten más seguros al saber que sus datos personales y la información crítica de la ciudad están protegidos. Esto puede mejorar la percepción pública del ayuntamiento y su gestión.

5. Cumplimiento normativo: Los sistemas de IA guardianes ayudan al ayuntamiento a cumplir con regulaciones y normativas de protección de datos y ciberseguridad. Esto es especialmente importante para evitar sanciones legales y para demostrar una gestión responsable de la información.

6. Detección temprana de amenazas: La capacidad de detectar anomalías y patrones de comportamiento sospechosos en tiempo real permite al ayuntamiento identificar y neutralizar amenazas antes de que puedan causar daños significativos.

7. Respuesta rápida a incidentes: La automatización de la respuesta a incidentes asegura que las amenazas se gestionen de manera inmediata y eficiente, minimizando el tiempo de exposición y el impacto potencial de los ciberataques.

8. Análisis y reportes detallados: Los sistemas de IA pueden generar reportes detallados sobre las actividades de seguridad, proporcionando a los administradores una visión clara y completa del estado de la ciberseguridad. Esto facilita la toma de decisiones informadas y la planificación estratégica.

9. Mejora continua: La IA permite una mejora continua de las defensas cibernéticas. A medida que el sistema recopila y analiza más datos, se vuelve más efectivo para predecir y responder a nuevas amenazas, adaptándose a un entorno de amenazas en constante cambio.

10. Optimización de recursos: La automatización y la inteligencia avanzada permiten al ayuntamiento optimizar el uso de sus recursos de ciberseguridad. Esto es particularmente beneficioso para entidades locales que a menudo enfrentan limitaciones de presupuesto y personal.

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

4. Directrices para la implementación de medidas de seguridad en el uso de medios electrónicos que empleen IA

Mejorar la resiliencia de las entidades locales frente a ciberataques implica adoptar un enfoque sistemático y bien planificado, que incluya la evaluación de riesgos, la selección de herramientas adecuadas, la capacitación del personal y la colaboración con entidades externas, entre otros aspectos.

A continuación, se describen una serie de directrices para implementar las medidas de seguridad en el uso de medios electrónicos que hagan uso de la IA, lo que puede transformar significativamente la capacidad de una entidad local para protegerse contra ciberamenazas.

1. Primero, se recomienda realizar una evaluación exhaustiva de las necesidades de ciberseguridad del ayuntamiento, identificando las áreas críticas que pueden beneficiarse de la implementación de la IA. Esto incluye definir objetivos claros, como la detección temprana de amenazas, la automatización de respuestas y la mejora de la capacidad de análisis forense.

2. Una vez identificadas las necesidades, se debe seleccionar una plataforma de IA adecuada que pueda integrarse sin problemas con los sistemas de TI y las infraestructuras de seguridad existentes. Es crucial entrenar los modelos de IA utilizando datos históricos y en tiempo real sobre el tráfico de red, los comportamientos del sistema y los incidentes de seguridad para detectar patrones anómalos y clasificar amenazas.

3. La implementación debería incluir agentes de detección de anomalías que monitoricen continuamente el tráfico de red y el comportamiento del sistema. Estos agentes deben estar actualizados con las últimas amenazas y técnicas de ataque conocidas. Además, se recomienda configurar agentes de respuesta a incidentes para automatizar la contención de amenazas, como el aislamiento de sistemas comprometidos y el bloqueo de direcciones IP sospechosas.

4. Para asegurar una respuesta efectiva, es importante realizar simulaciones de ciberataques y ejercicios de respuesta a incidentes para evaluar la efectividad de los agentes de IA y preparar al equipo de ciberseguridad. Los resultados de estas simulaciones deben utilizarse para ajustar y mejorar los modelos de IA.

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

5. Para garantizar la seguridad de la infraestructura, es necesario mantener todos los sistemas y *software* de IA actualizados con los últimos parches de seguridad para proteger contra vulnerabilidades conocidas. Además, se debe asegurar que existan sistemas de respaldo y redundancia para mantener la operatividad en caso de fallos o ataques.

6. La protección de datos sensibles es fundamental. Se recomienda implementar medidas de anonimización y cifrado de datos, asegurando el cumplimiento con las regulaciones y normativas relevantes, como el Reglamento General de Protección de Datos (RGPD). También es esencial establecer canales de comunicación seguros para la coordinación entre los agentes de IA y el equipo de ciberseguridad, utilizando cifrado de extremo a extremo.

7. La capacitación continua del personal del ayuntamiento sobre las mejores prácticas de ciberseguridad y el uso de herramientas de IA es crucial. Esto incluye campañas de concienciación sobre *phishing* y otros ataques basados en ingeniería social, utilizando ejemplos reales y simulaciones para mejorar la preparación del personal. Es esencial invertir en la capacitación continua de los empleados y desarrollar protocolos robustos de manejo y supervisión de los sistemas de IA. Solo así se podrá garantizar que la integración de la IA en las operaciones de la entidad local se realice de manera segura y beneficiosa para todos los ciudadanos.

8. La colaboración con otras entidades locales y organismos de ciberseguridad es importante para compartir información sobre amenazas y mejores prácticas. Participar en redes y foros de ciberseguridad ayudará a mantenerse al día con las últimas tendencias y desarrollos en el campo.

9. Se recomienda realizar auditorías periódicas para evaluar la efectividad de la implementación de IA en ciberseguridad y ajustar los protocolos de respuesta según sea necesario. Mantener los sistemas de IA actualizados con las últimas técnicas de ciberseguridad y amenazas emergentes es esencial para una mejora continua.

10. Es importante implementar técnicas para la detección de anomalías de contenido, con el fin de asegurar que los modelos de IA no produzcan resultados que sean maliciosos, inexactos o ilegales. Los sistemas de IA generativa, como los modelos de lenguaje na-

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

tural, pueden generar respuestas o contenido que, sin una adecuada supervisión, podrían incluir información falsa, desviaciones no intencionadas (conocidas como "alucinaciones"), o incluso contenido que infrinja derechos de autor. Para mitigar estos riesgos, se deben emplear técnicas avanzadas de monitorización y validación, que permiten identificar y corregir anomalías en tiempo real, asegurando que el contenido generado sea preciso y conforme a las normativas legales.

11. Además, es conveniente asegurar que la infraestructura de IA sea escalable para manejar un aumento en el volumen de datos y la complejidad de las amenazas a medida que la entidad local crece. Los sistemas de IA deben ser flexibles para adaptarse a cambios en las políticas de seguridad y las necesidades operativas del ayuntamiento.

12. Finalmente, mantener una documentación completa y actualizada de todos los procesos, políticas y herramientas de ciberseguridad implementadas es crucial. Generar informes periódicos sobre el estado de la ciberseguridad ayudará a evaluar el rendimiento de los agentes de IA y tomar decisiones informadas sobre futuras mejoras.

Por su parte, los propios usuarios de la IA en una entidad local también son responsables de hacer un buen uso de esta tecnología. En este sentido, deben contemplar las siguientes directrices para garantizar una operación segura, responsable y efectiva:

1. Es crucial que los usuarios reciban una capacitación continua sobre el uso seguro y efectivo de los sistemas de IA, así como sobre las mejores prácticas en ciberseguridad. Deben mantenerse actualizados sobre las últimas amenazas y técnicas de ciberataque que podrían explotar vulnerabilidades en los sistemas de IA.

2. El manejo seguro de los datos es fundamental. Los usuarios deben asegurarse de que todos los datos utilizados y procesados por los sistemas de IA estén protegidos mediante técnicas de cifrado y anonimización siempre que sea posible. Además, deben cumplir con todas las leyes y regulaciones de protección de datos relevantes, como el Reglamento General de Protección de Datos (RGPD), para evitar violaciones de privacidad. Un reto importante es la concienciación de los usuarios, para recordarles que siempre validen

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

la salida de la IAG para comprobar su precisión antes de incorporarlos a sus trabajos, que no introduzcan información confidencial, etc.

3. Los usuarios deben monitorizar continuamente el comportamiento de los sistemas de IA, y reportar cualquier actividad sospechosa o anomalía al equipo de ciberseguridad de inmediato. Para ello, es esencial establecer canales claros y seguros para que los usuarios puedan informar sobre posibles incidentes de seguridad o vulnerabilidades.

4. Es fundamental que los usuarios comprendan cómo funcionan los sistemas de IA y las decisiones que toman. Los modelos de IA deben ser transparentes y sus decisiones explicables. Además, se deben realizar evaluaciones de impacto en la privacidad y la seguridad, para identificar y mitigar los riesgos asociados al uso de la IA.

5. El uso responsable y ético de los sistemas de IA es otra directriz importante. Los usuarios deben evitar utilizar estos sistemas para actividades que puedan ser consideradas abusivas o poco éticas, como la vigilancia excesiva o la toma de decisiones discriminatorias. Deben ser conscientes de su responsabilidad en el uso de la IA, y actuar en consecuencia para minimizar los riesgos.

6. Es esencial que los usuarios conozcan y sigan los protocolos establecidos para la gestión de incidentes de ciberseguridad, incluyendo la contención, mitigación y recuperación de incidentes. Participar en simulacros y ejercicios de respuesta a incidentes ayudará a mejorar la preparación y la capacidad de respuesta ante ciberataques.

7. Finalmente, fomentar la colaboración y la comunicación entre los usuarios, así como con el equipo de ciberseguridad, es crucial para una respuesta efectiva y coordinada ante cualquier amenaza. Los usuarios deben trabajar en equipo y compartir información relevante para mejorar la seguridad general de los sistemas de IA.

5. Conclusiones

La IA está transformando rápidamente el panorama de la ciberseguridad, marcando una revolución que afecta tanto a los atacantes como a los defensores. En este entorno dinámico, las entidades locales se encuentran en

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

una posición única. Estas Administraciones manejan una vasta cantidad de datos históricos y sensibles diariamente en casi todos los ámbitos. Todos estos datos son imposibles de gestionar por los humanos. Los algoritmos permiten estudiarlos, extraer patrones y exprimir todo su potencial. Su adecuada explotación ofrece innumerables ventajas para ellas y para los ciudadanos, a través de su aplicación en la gestión de los servicios públicos, en la toma de decisiones y en la ciberseguridad.

Desde una perspectiva de ciberseguridad, la IA está jugando un papel crucial en dos direcciones. Por un lado, está siendo utilizada por los atacantes para desarrollar ciberataques más sofisticados y difíciles de detectar. Por otro lado, los defensores están empleando la IA para fortalecer sus mecanismos de defensa y proteger sus sistemas de información.

Entre los ciberataques más comunes se encuentran el *malware*, el *ransomware*, el *phishing*, la ingeniería social, la explotación de vulnerabilidades, la denegación de servicio, el acceso no autorizado a la información, la suplantación, el *hacktivismo* y las amenazas internas. Estos ataques representan una amenaza constante para las entidades locales, y pueden tener un impacto devastador en la continuidad de los servicios públicos, la confianza de los ciudadanos y la integridad de los datos.

Para hacer frente a estos desafíos, se han desarrollado diversos mecanismos técnicos que utilizan IA, tales como la detección de patrones, la clasificación, la automatización y el procesamiento del lenguaje natural. Estos mecanismos permiten una respuesta más rápida y precisa ante las amenazas, mejorando la capacidad de detección y respuesta de las entidades locales.

La implementación de sistemas de IA en ciberseguridad ofrece numerosos beneficios, incluyendo una mayor capacidad de detección de amenazas, una respuesta más rápida y eficiente, y una mejor gestión de los recursos. Además, la IA puede ayudar a identificar vulnerabilidades y prevenir ataques antes de que ocurran, proporcionando una capa adicional de protección para los datos y servicios públicos.

Finalmente, es esencial seguir directrices claras para la implementación de medidas de seguridad en el uso de medios electrónicos que emplean IA. Estas directrices son fundamentales para garantizar la protección de los datos y la continuidad de los servicios públicos, asegurando así la seguridad y confianza de los ciudadanos.

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

En conclusión, la IA se presenta como una herramienta poderosa y esencial en la lucha contra los ciberataques. Las entidades locales deben adoptar y adaptar estas tecnologías para proteger sus datos y servicios, garantizando así la seguridad y confianza de los ciudadanos.

6. Bibliografía

Centro Criptológico Nacional y Federación Española de Municipios y Provincias. (2021). *Prontuario de ciberseguridad para entidades locales. Abril 2021*. Disponible en https://transparencia.gob.es/transparencia/es/transparencia_Home/index/MasInformacion/Informes-de-interes/Seguridad/ProntuarioCiberseguridad-Abr2021.html.

ENISA (European Union Agency for Cybersecurity). (2020). *AI Cybersecurity Challenges*. Disponible en https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges.

European Commission. (2020). *White Paper on Artificial Intelligence - A European approach to excellence and trust*. Disponible en https://commission.europa.eu/document/download/d2ec4039-c5be-423a-81ef-b9e44e79825b_en?filename=commission-white-paper-artificial-intelligence-feb2020_en.pdf.

Ministerio para la Transformación Digital y de la Función Pública. (2024). *Estrategia de Inteligencia Artificial 2024*. Disponible en https://portal.mineco.gob.es/es-es/digitalizacionIA/Documents/Estrategia_IA_2024.pdf.

Presidencia del Gobierno. (2019). *Estrategia Nacional de Ciberseguridad*. Disponible en https://www.dsn.gob.es/sites/default/files/documents/Estrategia%20Nacional%20de%20Ciberseguridad%202019.pdf.

CAPÍTULO VI

El cumplimiento del Esquema Nacional de Seguridad (ENS) en las entidades locales

Miguel Á. Lubián Rueda
Ingeniero en Informática.
Director General de CIES (Grupo Seresco)

SUMARIO. 1. Introducción. 2. El marco de certificación del ENS para entidades locales: grandes y pequeños municipios. 2.1. Cómo abordar una implantación. 2.2. Categorización del sistema y declaración de aplicabilidad. **3. El perfil de cumplimiento específico del ENS para entidades locales: grandes municipios y pequeños municipios.** 3.1. ¿Qué es un PCE? Regulación, ejemplos de principales perfiles publicados. 3.2. ¿Por qué un PCE para las entidades locales? 3.3. PCE 890. 3.4. PCE 883. **4. Los Gobiernos intermedios como organismos de certificación del ENS. 5. Implicaciones de la Directiva relativa a las medidas para un elevado nivel común de ciberseguridad en toda la Unión (Directiva NIS2) en las entidades locales. 6. Bibliografía.**

1. Introducción

En el presente capítulo se analizan diferentes modelos desarrollados por el Centro Criptológico Nacional (en adelante, CCN) para ayudar a las entidades locales a la mejora de la seguridad de los sistemas de información, incluyendo las especialidades de los Perfiles de Cumplimiento Específicos de gobernanza en seguridad (en adelante, PCE).

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

Se analizará, también, la relevancia que adquieren las diputaciones provinciales, los cabildos y consejos insulares y las comunidades autónomas uniprovinciales en la mejora de la seguridad de la información de los ayuntamientos de menor tamaño, un papel desarrollado en el marco de sus competencias.

Por último, sin perjuicio de las adaptaciones de la transposición de la Directiva NIS2, que a fecha de elaboración de este capítulo aún no se ha aprobado, se analizará su impacto en las entidades locales, abordando la clasificación de determinados servicios que prestan como esenciales o importantes y la necesidad de definir nuevas estrategias para la gestión de los riesgos en ciberseguridad.

2. El marco de certificación del ENS para entidades locales: grandes y pequeños municipios

Para poder abordar las peculiaridades de los PCE, es necesario primero analizar aspectos clave de la conformidad con el ENS en el modelo estándar o tradicional.

Si bien a lo largo de este libro ya se han ido exponiendo las implicaciones del nuevo ENS y su afección a las entidades locales, pasaremos ahora a comentar, desde un punto de vista más práctico, los detalles de cómo abordar la conformidad con el ENS, bien porque la entidad desee iniciar el camino de la adecuación a la norma con este modelo, o bien porque ya disponga de una declaración de aplicabilidad en categoría básica o se haya adaptado con un PCE, que explicaremos en el siguiente apartado de este capítulo, para entidades locales, y quiera continuar evolucionando hacia un sistema de gestión más completo.

Es importante destacar que la seguridad de la información es trasversal a toda la organización y afecta no solo a los sistemas de información, sino también a los tradicionales expedientes en formato papel, por lo que la complejidad de abordar un proyecto de implantación en el modelo estándar debe iniciarse en aquellos sistemas de información más críticos para la organización. La identificación de los sistemas más críticos se realizará previo análisis inicial de riesgos, teniendo siempre también presente que uno de los principios básicos tanto de la seguridad de la información como de otros sistemas, como el relacionado con el cumplimiento de la normativa de protección de datos, es el de mejora continua, es decir, nunca se debe mantener una actitud estática, sino proactiva, por lo que una entidad local debe continuar extendiendo las medidas del ENS a los distintos sistemas

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

de información, bien porque sirvan de forma directa para prestar servicios a las personas interesadas (servicios finalistas como, a modo de ejemplo, prestaciones sociales, subvenciones, urbanismo...) o bien porque sirvan de soporte a estos (a modo de ejemplo, gestión del personal, contratación, compras, contabilidad...).

La conformidad con el ENS supone evidenciar el cumplimiento de las medidas de la norma, si bien, a priori, podría verse como algo ajeno a las Administraciones públicas. El ENS, recordemos, es una obligación del art. 156 de la Ley 40/2015 que ha ido adquiriendo especial relevancia con la implantación de los procesos administrativos electrónicos y los nuevos riesgos a los que se exponen las entidades locales. Pensemos, por ejemplo, que palabras como ciberseguridad, *hacking*, *phishing* o *ransomware* no eran conocidas hasta hace pocos años; tampoco los incidentes se materializaban con la gravedad con la que ocurren en la actualidad (cifrado y secuestro de bases de datos, suplantaciones y estafas cibernéticas...). Es, por tanto, una necesidad prioritaria que las entidades locales pongan todos los medios para evitar que un incidente de seguridad se materialice, o, si esto ocurre, para que su gravedad sea mínima[1].

Cuando se produce un incidente de seguridad o una brecha de datos personales[2] y se debe comunicar a los organismos de control, una mane-

1. La Sentencia núm. 188/2022 de la Sección Tercera de la Sala de lo Contencioso-Administrativo del Tribunal Supremo, de 15 de febrero de 2022, en su Fundamento de Derecho Tercero, establece lo siguiente:

"La obligación de adoptar las medidas necesarias para garantizar la seguridad de los datos personales no puede considerarse una obligación de resultado, que implique que producida una filtración de datos personales a un tercero exista responsabilidad con independencia de las medidas adoptadas y de la actividad desplegada por el responsable del fichero o del tratamiento.

En las obligaciones de resultado existe un compromiso consistente en el cumplimiento de un determinado objetivo, asegurando el logro o resultado propuesto, en este caso garantizar la seguridad de los datos personales y la inexistencia de filtraciones o quiebras de seguridad.

En las obligaciones de medios el compromiso que se adquiere es el de adoptar los medios técnicos y organizativos, así como desplegar una actividad diligente en su implantación y utilización que tienda a conseguir el resultado esperado con medios que razonablemente puedan calificarse de idóneos y suficientes para su consecución, por ello se las denomina obligaciones 'de diligencia' o 'de comportamiento'".

2. Se incorpora también la referencia a las violaciones de seguridad o brechas de datos personales de la normativa de protección de datos, ya que la disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales vincula las medidas del ENS con la protección de datos: "1. El Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679".

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

ra de evidenciar el cumplimiento de la normativa es la conformidad con el ENS, pero siempre que se haya mantenido en el tiempo el despliegue de las medidas de forma proactiva, supervisando y mejorando aquellos aspectos que sean precisos para evitar o mitigar el impacto de un incidente, teniendo en cuenta que el riesgo 0 no existe.

A fecha de redacción de este capítulo, el número de entidades locales que contaban con la conformidad con el ENS en sus sistemas de información era de 31 ayuntamientos, 3 diputaciones y un consorcio, además de aquellas que certifican el sistema de información que soporta la tramitación de sus servicios conforme al PCE de requisitos esenciales, que, según anuncia el CCN, pasará a denominarse PCE de Requisitos Fundamentales de Seguridad. Es evidente que son pocas las entidades locales que han afrontado un proceso de conformidad con el ENS; esto puede deberse a múltiples factores (lejanía del mundo administrativo con la seguridad, escasez de medios o de personal con suficiente capacitación en la materia, costes del proceso, falta de sensibilización sobre la relevancia de la seguridad de la información...). Si bien el número de entidades locales que disponen de conformidad con el ENS es reducido, el número de empresas privadas que ha optado por certificar sus sistemas de información (aquellas que son proveedoras para las Administraciones públicas) se ha ido elevando paulatinamente hasta alcanzar a fecha actual las 1754, distribuyéndose en categoría alta 618, en media 1104 y en básica 32.

La ampliación del número de empresas se debe a una mayor concienciación, por parte de las Administraciones públicas, de exigir el cumplimiento del ENS en la contratación, tal y como ya se indicaba en la Resolución de 13 octubre 2016 que aprobaba la Instrucción *Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad*, y que ahora se recoge en el art. 2.3 del ENS:

> "Este real decreto también se aplica a los sistemas de información de las entidades del sector privado, incluida la obligación de contar con la política de seguridad a que se refiere el art.12, cuando, de acuerdo con la normativa aplicable y en virtud de una relación contractual, presten servicios o provean soluciones a las entidades del sector público para el ejercicio por estas de sus competencias y potestades administrativas.
>
> La política de seguridad a que se refiere el art. 12 será aprobada en el caso de estas entidades por el órgano que ostente las máximas competencias ejecutivas.

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

> Los pliegos de prescripciones administrativas o técnicas de los contratos que celebren las entidades del sector público incluidas en el ámbito de aplicación de este Real Decreto contemplarán todos aquellos requisitos necesarios para asegurar la conformidad con el ENS de los sistemas de información en los que se sustenten los servicios prestados por los contratistas, tales como la presentación de las correspondientes declaraciones o certificaciones de conformidad con el ENS.
>
> Esta cautela se extenderá también a la cadena de suministro de dichos contratistas, en la medida que sea necesario y de acuerdo con los resultados del correspondiente análisis de riesgos".

El control de la cadena de proveedores, como se verá en el último apartado, es también uno de los aspectos más destacados de la Directiva NIS2. Las entidades locales en muchas ocasiones no disponen de sistemas de información propios, sino que son adquiridos a proveedores externos en diferentes modalidades de prestación de servicios y/o suministros que pueden instalarse en local o en la nube (PaaS[3], IaaS[4], SaaS[5]), por lo que deben reforzar su control para evitar que los medios no sean los adecuados a los riesgos de la información y/o los servicios que prestan.

Como puede observarse, reiteradamente se hace referencia a la necesidad de analizar los riesgos en relación con los servicios y la información (incluyendo los datos personales) que gestionan las entidades. El análisis de riesgos no solo va a permitir identificar áreas críticas, sino también implementar los medios de seguridad adecuados a las mismas, descritos en el Anexo II del ENS, preservando la debida confidencialidad, integridad, autenticidad o trazabilidad de la información, así como la disponibilidad de los servicios.

Si bien la confidencialidad y, ligadas a ella, la integridad y la autenticidad son dimensiones que se deben asegurar de forma reforzada, en ocasiones, como cuando se tratan datos personales de categorías especiales o cuando existe una norma con rango legal que obliga a ello (a modo de ejemplo, los datos tributarios), la disponibilidad debe ser interpretada de acuerdo, también, con la posibilidad de alargar los plazos administrativos en caso de ciberincidentes graves, según se dispone en la adición del apdo. 5 al art. 32 de la Ley 39/2015, por la disposición final 21.ª del Real Decreto-ley 6/2022, de 29 de marzo.

3. Plataforma como servicio, por sus siglas en inglés (*Platform as a Service*).
4. Infraestructura como servicio, por sus siglas en inglés (*Infrastructure as a Service*).
5. *Software* como servicio, por sus siglas en inglés (*Software as a Service*).

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

2.1. Cómo abordar una implantación

A continuación, veremos de una forma más práctica lo que supone el proceso de adecuación al ENS, que, con carácter general, se estructura en las siguientes fases, independientemente de si se trata de una adecuación estándar o de si nos acogemos a un PCE.

Fuente: elaboración propia

A continuación, se describen brevemente estas fases:

- **Definición de la gobernanza de la seguridad**. Es muy conveniente iniciar el proceso de adecuación con esta tarea, pues, como norma general, el proceso de identificación de los roles de seguridad puede llevar su tiempo, e incluso se pueden identificar necesidades formativas que será necesario llevar a cabo. Además, durante el proceso de implantación de la seguridad habrá actuaciones (procedimientos, normas, declaración de aplicabilidad...) que deberán ser evaluadas y aprobadas por los roles de seguridad y/o el comité de seguridad de la información, si bien no es necesario haber finalizado esta tarea para que podamos seguir con la siguiente fase en la implantación del ENS.

- **Elaboración del plan de adecuación**, que requerirá las siguientes acciones:

    - Identificación del **alcance de la conformidad con el ENS**. Es importante, ya desde el principio del proceso de adecuación, concretar los servicios que se incluirán en el alcance.

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

- **Categorización del sistema**. Este proceso se realizará tal y como se ha definido en el Anexo I del ENS y en las guías del CCN. Se prestará especial atención al requisito necesario de que las soluciones proporcionadas por terceros que formen parte de la prestación del servicio (total o parcialmente) dispongan de la conformidad con el ENS para el servicio proporcionado y en la categoría requerida.

- Elaboración de la **declaración de aplicabilidad** provisional, análisis de riesgos y declaración de aplicabilidad definitiva; por su importancia se ampliarán estos conceptos más adelante.

- Realización del **diagnóstico** de cumplimiento de las medidas de seguridad recogidas en la declaración de aplicabilidad, y elaboración del **plan de implantación** con definición de tareas, responsables y plazos de ejecución. Es muy recomendable que este plan sea aprobado formalmente; esto hará que el proceso de implantación del ENS se interiorice en la entidad.

- **Implantación de la seguridad**, compuesta por las siguientes acciones:

  - **Seguimiento del plan de implantación** mediante revisiones regulares de su cumplimiento, y, llegado el caso, reprogramación de las tareas necesarias.

  - Despliegue de **medidas técnicas, organizativas y legales**, desarrollando a la par el marco normativo, políticas, normas, procedimientos, instrucciones técnicas que forman parte del Sistema de Gestión de Seguridad de la Información (SGSI).

  - **Aprobación por parte de la dirección** de la entidad (alcaldía/presidencia de la diputación) del **SGSI**.

- **Obtención de la conformidad**. Recordemos que, para sistemas de categoría básica, será suficiente que, cada dos años, se realice una declaración de conformidad mediante una autoevaluación de cumplimiento. No obstante, resulta altamente recomendable realizar una auditoría de certificación, ya que esto permitirá que la entidad local figure en la lista de entidades certificadas del portal web

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

del CCN[6]. Para sistemas de categoría media o alta, será necesario realizar una auditoría de conformidad bienal y auditorías internas todos los años, tal y como se refleja en la Guía CCN-STIC IC-01/19 ENS sobre Criterios Generales de Auditoría y Certificación[7], cuyo objeto es servir de referencia y establecer los criterios generales para la Auditoría y Certificación de los sistemas de información del ámbito del ENS. Una vez superado el proceso de auditoría de certificación o autoevaluación, la entidad local estará en condiciones de obtener la certificación de conformidad con el ENS en el primer caso, y la declaración de conformidad en el segundo.

- **Definición de métricas** (Encuesta INES): será necesario definir las métricas para conocer el grado de implantación de las medidas de seguridad y para dar respuesta al informe anual requerido por el art. 32 del ENS, relativo al Informe Nacional sobre el Estado de la Seguridad (denominado INES). Para cumplir con este mandato, el CCN ha desarrollado el proyecto INES, para recopilar los datos a través de la plataforma habilitada a tal fin. Además, para sistemas de categoría media y alta, se definirán las métricas necesarias para conocer la efectividad del sistema de gestión de incidentes de seguridad y la eficiencia del sistema de gestión de la seguridad.

- **Vigilancia y mejora continua**. La gestión de la seguridad conllevará como mínimo las siguientes acciones:

    - **Al menos anualmente** se revisarán (con actualización y aprobación en caso de que sea necesario):

        - Los roles de seguridad[8], los miembros del Comité y el texto de la Política de Seguridad. Si existen vacantes, o nuevas incorporaciones.

        - El alcance de la certificación y su categorización, si es necesario incorporar nuevos servicios o bien revisar alguno que haya cambiado.

6. Lista de entidades certificadas: https://gobernanza.ccn-cert.cni.es/certificados.
7. La disposición adicional segunda del ENS señala que el CCN, en el ejercicio de sus competencias, elaborará y difundirá las correspondientes guías de seguridad de las tecnologías de la información y la comunicación, que se incorporarán al conjunto documental utilizado para la realización de las auditorías de seguridad.
8. Para información más detallada, puede acudirse a la Guía CCN-STIC 801, *Responsabilidades y Funciones en el ENS*.

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

- El análisis de riesgos y el seguimiento del plan de tratamiento de riesgos. Será necesario identificar si hay nuevas amenazas que afecten al sistema, si se han realizado cambios sustanciales en el sistema de información o si se han incorporado nuevos servicios, además de realizar el seguimiento periódico de las actuaciones reflejadas en el plan.

- El análisis de impacto, como resultado de los puntos anteriores, por incorporación de nuevos servicios o variación de los existentes, o de los criterios para valorar el impacto de la interrupción de dichos servicios.

- La declaración de aplicabilidad. También como resultado de las revisiones anteriores y de otras tareas de seguimiento del sistema, puede ser necesario incorporar nuevas medidas, o desarrollar medidas compensatorias o complementarias de vigilancia.

o **Al menos anualmente** se realizarán:

- La cumplimentación de la encuesta INES.

- Auditorías internas opcionales para sistemas de categoría básica y obligatorias para media y alta.

- La actualización de la documentación que forma parte del SGSI, ya sea derivada de las tareas anteriores, o bien por corrección de errores o inconcreciones.

o **Cada dos años** se realizará la auditoría de certificación de conformidad con el ENS, obligatoria para sistemas de categoría media y alta, o bien para sistemas de categoría básica, si bien para estos es suficiente con la declaración de conformidad con el ENS mediante una autoevaluación realizada por la propia entidad.

2.2. Categorización del sistema y declaración de aplicabilidad

Antes de proseguir con las explicaciones relativas a los PCE para las entidades locales, creemos conveniente definir los conceptos de categorización del sistema y declaración de aplicabilidad.

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

La determinación de la categoría de seguridad de un sistema de información, tal y como se define en el Anexo I del ENS, se basa en la valoración del impacto que tendría sobre las entidades un incidente de seguridad que afectase a la seguridad de la información o de los servicios prestados para alcanzar sus objetivos, proteger los activos a su cargo y garantizar la conformidad con el ordenamiento jurídico. Para la determinación del impacto se tendrán en cuenta las cinco dimensiones de seguridad ya citadas: Confidencialidad [C][9], Integridad [I][10], Trazabilidad [T][11], Autenticidad [A][12] y Disponibilidad [D][13]. Cada una de estas dimensiones se adscribirá a uno de los siguientes niveles de seguridad: bajo, medio o alto; y, en caso de no verse afectada, no se adscribirá a ningún nivel, según los criterios indicados en el mencionado anexo. De acuerdo con la valoración, tal y como se indica en el Anexo I del ENS:

"1. Se definen tres categorías de seguridad: básica, media y alta.

a) Un sistema de información será de categoría alta si alguna de sus dimensiones de seguridad alcanza el nivel de seguridad alto.

b) Un sistema de información será de categoría media si alguna de sus dimensiones de seguridad alcanza el nivel de seguridad medio, y ninguna alcanza un nivel de seguridad superior.

c) Un sistema de información será de categoría básica si alguna de sus dimensiones de seguridad alcanza el nivel bajo, y ninguna alcanza un nivel superior".

La valoración de los servicios y la información la realizarán los responsables de la información y los servicios, pudiendo contar con la opinión del responsable de seguridad y/o del responsable del sistema. Y deberá ser aprobada formalmente por los responsables de la información y los ser-

9. [C]: Se establecerá en función de las consecuencias que tendría su revelación a personas no autorizadas o que no necesitan conocer la información.

10. [I]: Se establecerá en función de las consecuencias que tendría su modificación por alguien que no está autorizado a modificar la información.

11. [T]: Se establecerá en función de las consecuencias que tendría el no poder rastrear a posteriori quién ha accedido a —o modificado— una cierta información.

12. [A]: Se establecerá en función de las consecuencias que tendría el hecho de que la información no fuera auténtica.

13. [D]: Se establecerá en función de las consecuencias que tendría el que una persona autorizada no pudiera usar el servicio cuando lo necesitase.

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

vicios, respectivamente. La Guía CCN-STIC 803 sobre la valoración de los sistemas ayuda a realizar el proceso de categorización.

Por otro lado, la declaración de aplicabilidad en el ámbito del ENS es un documento en el que se formalizarán las medidas de seguridad que resultan de aplicación al sistema de información. Este documento pasará por dos estados: uno inicial, denominado declaración de aplicabilidad inicial, que contendrá las medidas de seguridad del Anexo II del Real Decreto ENS, conforme a la categoría del sistema tal y como se ha definido anteriormente; y otro definitivo, aprobado por el responsable de seguridad, tras un análisis de riesgos. A la hora de seleccionar las medidas de seguridad hay que tener en cuenta los siguientes aspectos:

- Las medidas se seleccionarán en función de la valoración de cada una de las cinco dimensiones de seguridad. Por ejemplo, si las valoraciones por dimensiones son las siguientes ([C]: medio, [I]: medio, [T]: medio, [A]: medio, [D]: bajo), la categoría del sistema será media y las medidas de seguridad del Anexo II del ENS que se aplicarán al sistema serán solo 65, en lugar de las 68 que corresponden a un sistema de categoría media cuando las cinco dimensiones de seguridad tienen un valor medio. Pero ¿por qué son 65 medidas en vez de 68? Esto se debe a que la dimensión de Disponibilidad [D] se valora en nivel bajo, y por tanto no son aplicables las medidas de análisis de impacto [op.cont.1], protección frente a inundaciones [mp.if.6] y protección frente a la denegación de servicio [mp.s.4], que se corresponden con la Disponibilidad [D] en nivel medio.

- Conforme a lo establecido en el ENS, las medidas de seguridad referenciadas en el Anexo II podrán ser reemplazadas por otras denominadas compensatorias, siempre y cuando se justifique documentalmente que los activos se protegen igual o mejor frente al riesgo, y que también se satisfacen los principios básicos y los requisitos mínimos previstos en los Capítulos II y III del ENS. Para documentar las medidas compensatorias se podrá tomar como referencia la Guía CCN-STIC 819 *Medidas Compensatorias*, y se incluirán en la declaración de aplicabilidad.

En base a lo mencionado anteriormente tendremos la declaración de aplicabilidad inicial, y posteriormente se procederá a la realización del análisis de riesgos. Tras realizar el análisis, si el resultado (el riesgo residual) no es aceptado por la entidad será necesario aplicar nuevas medidas para mitigar el riesgo, medidas que serán de aplicación al sistema y por tanto for-

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

marán parte de la declaración de aplicabilidad, considerándose entonces como la definitiva.

En este punto también es cuando la entidad podrá acogerse a un PCE que sea de aplicación, tras la aceptación del riesgo residual.

La declaración de aplicabilidad es uno de los documentos más importantes, ya que nos servirá para identificar las medidas de seguridad que debamos implementar sobre el sistema y, a su vez, en un proceso de auditoría tanto interna como externa, será el documento de apoyo para su revisión. Por tanto, es importante que la declaración de aplicabilidad contemple lo siguiente:

- Para cada una de las 73 medidas de seguridad del Anexo II del ENS, se indicará no solo si aplica o no al sistema de información, sino también, de forma muy resumida, cómo aplica y/o la documentación donde se detalla y, en su caso, por qué no aplica.

- En el caso de medidas de seguridad que planteen la opción de aplicabilidad con refuerzos elegibles, se deberá indicar cuál se ha aplicado.

- Si la medida se sustituye por una compensatoria, deberá indicarse y referenciarse la ubicación de la descripción de la medida compensatoria.

- Si en la medida indicada se ha aplicado una medida complementaria de vigilancia[14].

- Para cada medida de aplicación, se indicará el nivel de madurez y el grado de implementación, conforme a lo establecido en la Guía CCN-STIC-808 *Verificación del cumplimiento de las medidas en el ENS*.

14. Esta medida complementa y equilibra los requisitos exigibles que se han implementado para una determinada medida de seguridad, ya sean base o de refuerzo, cuando estos no son suficientes, a juicio de la entidad, para poder alcanzar el cumplimiento del ENS para dicha medida. También puede complementar a una medida compensatoria que no consigue igualar o mejorar el riesgo de la medida original. En ocasiones, dichas medidas serán transitorias (limitadas en el tiempo) hasta que se consiga la efectividad plena en la implantación de una medida. Conforme a lo establecido en la Guía CCN-STIC-808 "Verificación del cumplimiento de las medidas en el ENS".

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

La declaración de aplicabilidad será aprobada formalmente por el responsable de supervisión/vigilancia (responsable de la seguridad). Para su elaboración, podemos tomar como referencia la Guía y su Anexo CCN-CERT_BP_14_Declaración de Aplicabilidad ENS.

Como ya se ha señalado, se pueden integrar otras medidas, y aquí es relevante destacar, por la propia conexión que hace el texto del ENS, el plan de tratamiento del riesgo derivado de un análisis de riesgos y/o evaluación de impacto en protección de datos.

En relación con la normativa de protección de datos, el propio ENS indica que deberán tenerse en cuenta las medidas recogidas en el análisis de riesgos en privacidad y, en su caso, una evaluación de impacto, debiendo consultarse al delegado de protección de datos, tal y como se recoge, entre otros, en el art. 3.2 del ENS.

Asimismo, se indica en el apdo. 3.3 del ENS que resultarán de aplicación las medidas derivadas del análisis de riesgos en privacidad o de las evaluaciones de impacto cuando estas sean más exigentes que las derivadas del análisis de riesgos del ENS.

Atendiendo a la definición que el propio ENS da de análisis de riesgos [15], la valoración de la información (donde se incluyen los datos personales), como ya se ha venido comentando, se hace sobre cuatro dimensiones: confidencialidad [C], integridad [I], autenticidad [A] y trazabilidad [T], siendo la dimensión que afecta a los servicios la de disponibilidad [D].

Como puede observarse, las dimensiones del ENS para la información son similares a las analizadas por la normativa de protección de datos, a excepción de la autenticidad y la trazabilidad. Por ello, en los análisis de riesgos se deberán tener en cuenta aquellas especificaciones propias relacionadas con los datos personales, como pueden ser las normativas sectoriales que los afectan[16] o la calificación de los datos como "categorías especiales"[17].

15. En el Anexo IV se define como "estudio de las consecuencias previsibles de un posible incidente de seguridad, considerando su impacto en la organización (en la protección de sus activos, en su misión, en su imagen o reputación, o en sus funciones) y la probabilidad de que ocurra".

16. Véase, a modo de ejemplo, la especial confidencialidad sobre los datos de índole tributaria que se regula en el art. 95 de la Ley 58/2003, de 17 de diciembre, General Tributaria.

17. El Reglamento General de Protección de Datos define las categorías especiales de datos, sujetas a una especial protección, en su art. 9.

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

Teniendo en cuenta los conceptos básicos y cómo abordar una adecuación estándar, procederemos ahora a exponer los PCE que el CCN ha aprobado específicamente para las entidades locales, como sector con características singulares.

3. El perfil de cumplimiento específico del ENS para entidades locales: grandes municipios y pequeños municipios

3.1. ¿Qué es un PCE? Regulación, ejemplos de principales perfiles publicados

Para dar comienzo a este apartado, en sintonía con lo que se ha ido comentando en los capítulos precedentes, es necesario señalar que, entre los diferentes cambios introducidos por el Real Decreto 311/2022 (ENS), se encuentra la posibilidad de crear perfiles de cumplimiento específicos (en adelante PCE), tal y como se indica en su art. 30.

Un PCE, como una postura de seguridad adaptada a unas circunstancias concretas, tal como se indica en el preámbulo del Real Decreto, es un reajuste de las medidas del ENS adaptadas a un sector o sistema[18] concreto que cuenta con unas peculiaridades propias; en concreto, se señala que entre los tres grandes objetivos del ENS se encuentra el siguiente:

> "[...] introducir la capacidad de ajustar los requisitos del ENS, para garantizar su adaptación a la realidad de ciertos colectivos o tipos de sistemas, atendiendo a la semejanza que presentan una multiplicidad de entidades o servicios en cuanto a los riesgos a los que están expuestos sus sistemas de información y sus servicios. Ello aconseja la inclusión en el ENS del concepto de 'perfil de cumplimiento específico' que, aprobado por el Centro Criptológico Nacional, permita alcanzar una adaptación del ENS más eficaz y eficiente, racionalizando los recursos requeridos sin menoscabo de la protección perseguida y exigible".

18. El nuevo ENS modifica en el glosario el concepto de sistema de información, que ahora incluye cualquiera de los elementos siguientes:
1.º- Las redes de comunicaciones electrónicas que utilice la entidad del ámbito de aplicación de este real decreto sobre las que posea capacidad de gestión.
2.º- Todo dispositivo o grupo de dispositivos interconectados o relacionados entre sí, en el que uno o varios de ellos realicen, mediante un programa, el tratamiento automático de datos digitales.
3.º- Los datos digitales almacenados, tratados, recuperados o transmitidos mediante los elementos contemplados en los números 1.º y 2.º anteriores, incluidos los necesarios para el funcionamiento, utilización, protección y mantenimiento de dichos elementos.

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

Es interesante reseñar que el legislador ha entendido la necesidad de realizar adaptaciones de las medidas estándar definidas en el Anexo II del ENS, teniendo en cuenta los recursos —en muchas ocasiones escasos— con los que cuentan las diferentes entidades incluidas en el ámbito de aplicación del ENS, en aras de una mayor eficacia y eficiencia, principios que —recordemos— rigen la actuación de las Administraciones públicas, tal y como se señala en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

El glosario del ENS define al PCE como "conjunto de medidas de seguridad, comprendidas o no en el anexo II de este real decreto, que, como consecuencia del preceptivo análisis de riesgos, resulten de aplicación a una entidad o sector de actividad concreta y para una determinada categoría de seguridad, y que haya sido habilitado por el CCN".

Por su parte, el art. 30 del ENS regula los PCE en los siguientes términos:

> "1. En virtud del principio de proporcionalidad y buscando una eficaz y eficiente aplicación del ENS a determinadas entidades o sectores de actividad concretos, se podrán implementar perfiles de cumplimiento específicos que comprenderán aquel conjunto de medidas de seguridad que, trayendo causa del preceptivo análisis de riesgos, resulten idóneas para una concreta categoría de seguridad. [...]
>
> 3. El CCN, en el ejercicio de sus competencias, validará y publicará los correspondientes perfiles de cumplimiento específicos que se definan y los antedichos esquemas de acreditación y validación, de acuerdo con las instrucciones técnicas de seguridad y guías de seguridad aprobadas conforme a lo previsto en la disposición adicional segunda. [...]".

De lo hasta aquí comentado sobre la regulación del ENS, se pueden extraer las principales características de los PCE:

- Se crean para entidades, sectores de actividad específicos o sistemas de información con características comunes.
- Pueden aplicarse tanto a entidades públicas como privadas, ya que debe tenerse en cuenta que el art. 2 del ENS abarca tanto a las Administraciones y su sector público como a las entidades privadas que prestan servicios a estas.

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

- Suponen una adaptación de las medidas del ENS para racionalizar su cumplimiento, en atención a las características peculiares del sector, atendiendo a los riesgos.

- Pueden incluir las medidas del Anexo II o bien otras no previstas que se recogen en la declaración de aplicabilidad.

- Dichas medidas siempre parten de un análisis de riesgos necesario para la redacción del PCE.

- Las entidades incluidas en el alcance del PCE podrán acogerse a este tras realizar el preceptivo análisis de riesgos, e implementar las medidas recogidas en la declaración de aplicabilidad, adaptadas a sus características peculiares, solicitando la acreditación de conformidad con el ENS respecto al PCE.

- Los PCE son aprobados y publicados por el CCN, lo que permite una actualización común y ágil de los riesgos y medidas a adoptar por las entidades ante nuevas amenazas en materia de seguridad.

Hasta la fecha, el CCN ha aprobado los siguientes PCE, incluidos en las guías CCN-STIC 800:

- 852 PCE Organismos pagadores
- 881 PCE Universidades
- 883 PCE Entidades Locales
- 884 PCE para Azure de Servicios Cloud Corporativo
- 885 PCE para Office 365 Servicio de Cloud Corporativo
- 886 PCE para LORETO NG Base
- 887 PCE para AWS Servicio de Cloud Corporativo
- 888 PCE para Google Servicio de Cloud Corporativo
- 889 PCE para Oracle Cloud Servicio de Cloud Corporativo
- 890 PCE Requisitos Fundamentales de Seguridad

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

- 891 PCE Prestaciones Sanitarias a Pacientes (atención primaria y especializada)

- 892 PCE para organizaciones en el ámbito de aplicación de la Directiva NIS2 (PCE NIS2). A fecha de redacción de este artículo, este PCE se había despublicado, pendiente de la aprobación de una versión modificada tras los cambios introducidos por el anteproyecto de transposición.

Volviendo a los PCE, es interesante resaltar que, para cada uno, se realiza un análisis de riesgos, lo que facilita en gran medida la labor de implantación por parte de las entidades incluidas en su ámbito. Esto se debe a que se parte de una selección de medidas adaptadas a las amenazas específicas del ecosistema en cuestión (infraestructura, recursos, tecnología, etc.), lo que puede derivar en la inclusión de medidas propias del ENS o de otras no previstas, desarrolladas en la detallada declaración de aplicabilidad que acompaña a cada PCE. Esta última opción permite, entre otras cosas, adaptar el sistema a nuevas obligaciones derivadas de modificaciones legislativas, tanto a nivel estatal como europeo. A modo de ejemplo, cabe mencionar la legislación relativa a la protección de datos o a la ciberseguridad (como la Directiva NIS2).

Si bien el PCE proporciona una declaración de aplicabilidad, la entidad incluida en su ámbito —o que desee acogerse a uno concreto, motivando así el inicio del camino hacia la adecuación al ENS mediante dicho PCE— deberá, en todo caso, valorar sus propios riesgos y asumir el riesgo residual.

Otro ejemplo que ilustra la capacidad de los PCE para adaptarse a nuevas obligaciones se encuentra en el perfil elaborado para los Organismos Pagadores. Este fue diseñado con el objetivo de que dichas entidades pudieran cumplir no solo con los requisitos establecidos por el ENS, sino también con los exigidos por el legislador europeo[19] en materia de seguridad de los sistemas de información.

19. Reglamento Delegado (UE) 2022/127 de la Comisión de 7 de diciembre de 2021 que completa el Reglamento (UE) 2021/2116 del Parlamento Europeo y del Consejo con normas relativas a los organismos pagadores y otros órganos, la gestión financiera, la liquidación de cuentas, las garantías y el uso del euro (en adelante, Reglamento Delegado (UE) n.º 2022/127), Anexo I, 3 INFORMACIÓN Y COMUNICACIÓN, letra B): "La seguridad de los sistemas de información deberá estar certificada de conformidad con la norma ISO 27001: Information Security management systems – Requirements (ISO) (Sistemas de gestión de la seguridad de la información-Requisitos) (ISO)".

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

3.2. ¿Por qué un PCE para las entidades locales?

Las entidades locales tienen unas características especiales en relación con el resto de las Administraciones territoriales del Estado, tanto desde el punto de vista organizativo como económico o competencial, sin olvidarnos de su gran volumen.

A fecha actual, según los datos publicados por el INE, el número de ayuntamientos alcanza los 8132, a los que deberíamos añadir otras entidades locales como diputaciones, mancomunidades, consorcios y entidades dependientes (fundaciones, empresas municipales). Sin embargo, el número de entidades locales que cuentan con una certificación acreditativa de conformidad con el ENS (con 185 ayuntamientos y un consorcio conforme al PCE, y en certificación tradicional del ENS en torno a 31 ayuntamientos, 3 diputaciones y 1 consorcio, como ya se ha señalado) es significativamente inferior. Es decir, han sido relativamente pocas las que han logrado un nivel de seguridad adecuado a los riesgos que presentan la información y los servicios que proporcionan.

No podemos obviar que las entidades locales, tradicionalmente, vienen reclamando una mayor capacidad de financiación para hacer frente a un ingente volumen de gastos derivados de las competencias propias que les atribuye la legislación básica del Estado, como aquellas otras que, calificadas como impropias, son asumidas sin tener una competencia específica, o las que son delegadas por otras Administraciones.

Además, la población (envejecida) en aquellas provincias con una amplia dispersión territorial se distribuye en ayuntamientos de pequeño tamaño. Según datos del INE, el número de municipios por debajo de los 5000 habitantes supera los 6000.

Esta situación compleja, junto con la competencial, es a la que pretenden dar solución los PCE para entidades locales en el ámbito de la seguridad de la información.

A modo de ejemplo, el análisis realizado por el Tribunal de Cuentas en 2022 en su informe *de fiscalización de la asistencia a municipios por las diputaciones provinciales o entidades equivalentes en materia de administración electrónica y el estado de implantación en los ayuntamientos de municipios de población entre 10 000 y 20 000 habitantes*, en relación con esta competencia de las diputaciones, en el apartado referido al cumplimiento del ENS, señala:

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

> "El 43 % de las entidades que prestaron asistencia, veinte de ellas, lo hicieron en relación con el cumplimiento del ENS. El número total de ayuntamientos que recibieron asistencia ascendió a 2489, el 32 % del total de los de población inferior a 20 000 habitantes del territorio nacional. No desarrollaron asistencia veintiséis entidades, ascendiendo a 3768 el número de ayuntamientos de población inferior a 20 000 habitantes en dichos territorios. [...] El contenido de la asistencia fue heterogéneo y consistió, entre otras cuestiones, en la realización de talleres formativos, servicios de atención a usuarios, apoyo en materia normativa y resolución de dudas. Las especiales características de los ayuntamientos de menor población y sus recursos limitados hacen que la adecuación al ENS y su ulterior certificación constituyan obligaciones de difícil cumplimiento de manera individualizada. Por ello, se hace necesario medidas para su implementación en grupos homogéneos de entidades, así como un Marco de Certificación Específico que contemple un procedimiento de auditoría y certificación que optimice los recursos. No obstante, únicamente el 33 % de las entidades que desarrollaron asistencia en ENS, siete de ellas, habían llevado a cabo actuaciones relacionadas con dicho Marco de Certificación para entidades locales del Centro Criptológico Nacional, al objeto de cubrir transversalmente las necesidades de seguridad de todas las entidades adheridas, mediante la implantación conjunta del ENS en ayuntamientos de características similares de la misma provincia, con el objetivo de alcanzar la Certificación de Conformidad para sus sistemas de información".

3.3. PCE 890

Pasaremos ahora a describir las principales características de los PCE que afectan a las entidades locales.

En primer lugar, abordaremos el PCE de la Guía CCN-STIC 890, que pasará a denominarse de Requisitos Fundamentales de Seguridad, en adelante PCE-RFS.

Este PCE se desarrolla para aquellas entidades que, por la falta de recursos (económicos, organizativos o de personal), tienen serias dificultades para abordar un proceso de certificación ordinario, por lo que, además de analizar los riesgos y describir las medidas aplicadas, es, obviamente, un primer acercamiento a la implementación de una Política de Seguridad vinculada al ENS en categoría básica en los sistemas de información que soportan la tramitación de los servicios prestados en estas entidades.

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

El PCE proporciona un catálogo de servicios conforme a lo establecido en el art. 25 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local (LBRL), y cuenta con medidas de seguridad básicas y fáciles de asumir, teniendo a su disposición herramientas adaptadas a los requisitos del PCE (herramientas ABS - Análisis Básico de Seguridad), que son proporcionadas por el CCN para apoyar la implementación y obtener así la certificación de conformidad en el ENS, en base a una metodología específica del CCN denominada μCeENS, automatizada en las herramientas de Gobernanza de la Ciberseguridad del CCN.

Es importante destacar la relevancia que adquiere la diputación provincial en la implementación del PCE. Tal como se indica en el art. 36.1.g) de la LBRL, tiene entre sus competencias: "La prestación de los servicios de administración electrónica y la contratación centralizada en los municipios con población inferior a 20 000 habitantes", regulándose en el art. 30 del Texto Refundido de 1986 los distintos tipos de cooperación con los ayuntamientos. En desarrollo de las competencias, especialmente para los ayuntamientos de una población inferior a los 1000 habitantes, con una escasa capacidad de financiación de sus servicios, las diputaciones, con carácter general, han provisto a los municipios de menos de 20 000 habitantes que así lo necesitasen de los medios electrónicos necesarios para abordar los retos de la gestión electrónica de los procedimientos ya con la Ley 11/2007 y, especialmente, con las leyes 39 y 40 de 2015, apoyando con medios técnicos y humanos el despliegue de la administración electrónica.

Pasaremos ahora a abordar de forma sucinta las diferentes fases del proceso, desde un punto de vista práctico, y las medidas de seguridad que se deben implementar, si bien, en primer lugar, se debe señalar que el PCE, a fecha actual, cuenta con dos variantes: una para entidades locales de escasos recursos, y otra para el resto de entidades de la Administración General o las comunidades autónomas de reducido tamaño, recursos limitados y que presten un número limitado de servicios, obviamente no esenciales, o bien como un primer acercamiento al sistema de gestión del ENS.

Modelo de gobernanza simplificado

El tipo de entidades al que se dirige este PCE tiene, como ya se ha comentado, una estructura organizativa de pequeño tamaño y un número reducido de personal. Esto supone que desde el CCN se haya propuesto una adaptación del modelo de gobernanza estándar.

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

El modelo de gobernanza propuesto, por bloques de responsabilidad, unifica y simplifica funciones, pero respetando las obligaciones impuestas por la normativa:

1.- Bloque de Gobierno o Responsable de Gobierno, que en un ayuntamiento se corresponderá con la alcaldía o concejalía delegada. Incluye las funciones clásicas de:

- Comité de Seguridad de la Información.
- Responsable de la Información.
- Responsable del Servicio.

¿Qué supone en la práctica? Que la alcaldía o concejalía delegada será la encargada de aprobar los documentos que forman parte del sistema de gestión, comprometerse con la implantación del modelo, y determinar el riesgo de la información que gestiona o de los servicios.

2.- Bloque de Supervisión, que en un ayuntamiento de pequeño tamaño corresponde a la secretaría-intervención:

- Responsable de Supervisión/Vigilancia, cuyo rol ENS será el de responsable de la seguridad.
- Delegado de Protección de Datos, en apoyo al anterior en las materias que le son propias.

¿Qué supone en la práctica? Que realizan las funciones de supervisión (fiscalización) y asesoramiento propias de ambos puestos. Además, el Responsable de Supervisión deberá aprobar la declaración de aplicabilidad, tomando en cuenta las valoraciones realizadas por el Responsable de Gobierno.

3.- Bloque de Operación, que corresponde a un empleado del ayuntamiento, pudiendo ser, en caso de que exista, una persona con conocimientos en informática:

- Responsable de Operación, cuyo rol ENS será el de responsable del sistema.

¿Qué supone en la práctica? Qué realizará las funciones de solventar las pequeñas ineficiencias del sistema y comunicará los fallos que detecte

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

en los equipos bien a la diputación o bien a una entidad privada que gestione los servicios de soporte.

Si bien a *priori* puede causar cierta incertidumbre en relación con la complejidad de las funciones a desarrollar, máxime si observamos las competencias estándar en los diferentes roles del ENS, siempre se debe tener en cuenta que estos ayuntamientos cuentan con la cooperación de la diputación, que suministra los servicios de administración electrónica y asistencia jurídico-técnica, bien prestada de forma directa o indirecta mediante entidades públicas (a modo de ejemplo, CAST en Asturias o ANIMSA en Navarra) o privadas.

Análisis de riesgos y declaración de aplicabilidad

Como se indicó anteriormente, la declaración de aplicabilidad asociada a un PCE de cumplimiento se fundamenta en la realización del preceptivo análisis de riesgos. En el caso particular del PCE-RFS, que, como comentábamos, está dirigido a entidades que disponen de recursos limitados, para la realización de este análisis se han tenido en cuenta las principales situaciones que pueden propiciar que se materialicen diversas amenazas, comprometiendo así la seguridad de los sistemas de información. Entre otras, podemos citar la navegación por sitios inseguros, el uso indebido del correo electrónico, deficiencias en la configuración, inadecuado acceso a los recursos, etc.

En definitiva, el objetivo que persiguen estas medidas es proporcionar un *framework* de seguridad que se constituye como básico para proteger los sistemas de información, propiciando:

- El uso eficiente de los recursos mediante el desarrollo de normas que regulen el uso de los medios electrónicos (correo electrónico, internet, equipos de usuario, dispositivos portátiles, puestos de trabajo despejados, limpieza de metadatos, etc.) que se ponen a disposición de los usuarios y que incluyan la responsabilidad frente a los usos indebidos.

- El control y seguridad en la definición del sistema, estableciendo los requisitos para la adquisición de nuevos componentes y el posterior proceso de autorización para su entrada en el sistema. Disponiendo también la necesidad de su inventariado, la aplicación de una configuración de seguridad, el mantenimiento y el parcheado

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

de seguridad, evitando así los posibles errores y que los sistemas sean vulnerables.

- La trazabilidad de las actuaciones mediante la activación de los registros de actividad, al menos en los servidores.

- La prevención frente accesos no autorizados al sistema y a la información, estableciendo identificadores únicos para entidades, usuarios o procesos; políticas de control de acceso basadas en los principios de "mínimo privilegio", "necesidad de conocer", "responsabilidad de compartir y capacidad de compartir", y la implementación del doble factor de autenticación recomendado para el acceso local y necesario para el acceso remoto.

- La protección frente a la pérdida de datos y el aseguramiento de la continuidad de la actividad mediante el establecimiento de una completa política de copias de seguridad y el desarrollo de los procedimientos de operación del sistema necesarios.

- La concienciación en seguridad y profesionalidad, exigiendo la necesidad de disponer de planes de concienciación y formación que contemplen también la evaluación de la eficacia de las acciones realizadas.

- La reducción del impacto de los incidentes de seguridad, definiendo un proceso integral de gestión de los incidentes, que tenga en cuenta también la normativa de protección de datos y que detalle los organismos y autoridades de control a los que será necesario comunicar.

- La protección de la red interna frente a la red exterior (internet) mediante el despliegue de soluciones de seguridad perimetral, que, en el caso de sitios pequeños donde no exista red, se limitará a la activación del firewall del sistema operativo y a la utilización de VPN[20] cuando la comunicación discurra fuera del propio dominio de seguridad.

- El cumplimiento normativo, estableciendo que, cuando un sistema trate datos personales, se deberá atender a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de

20. Redes privadas virtuales, por sus siglas en inglés: *Virtual Private Networks*.

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

27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos), y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

- La protección de la información cuando se aloja en soportes extraíbles, definiendo las medidas de seguridad a observar para su custodia y transporte, debiendo aplicarse mecanismos de cifrado en caso de que estos soportes alojen copias de seguridad. Para la reutilización de estos dispositivos deberá realizarse un borrado seguro. Medida que será de aplicación también a los discos duros de los equipos.

- La protección del sistema frente al código dañino y otras amenazas, mediante el despliegue de soluciones antivirus, de protección del correo electrónico y de la navegación web por parte de los usuarios.

- La protección de las claves criptográficas durante todo su ciclo de vida (generación, transporte, custodia, retirada y destrucción final) y de la firma electrónica mediante el empleo de cualquiera de los sistemas previstos en el vigente ordenamiento jurídico, entre ellos los sistemas de código seguro de verificación vinculados a la Administración pública, órgano, organismo público o entidad de derecho público, en los términos y condiciones establecidos en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y en la Ley 40/2015, de 1 de octubre.

- La mejora continua del sistema mediante la definición de un sistema de métricas para recopilar los datos necesarios para conocer el grado de implantación de las medidas de seguridad y para dar respuesta a la encuesta INES (Informe Nacional del Estado de la Seguridad).

Proceso de Adecuación al PCE de Requisitos Fundamentales (PCE-RFS) en base a la metodología µCeENS

La metodología µCeENS desarrollada por el CCN, proporciona a las entidades un instrumento para abordar el proceso de adecuación al PCE-RFS, acompañándolas hasta la obtención de la certificación de conformidad

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

con el ENS conforme a dicho PCE. Este proceso se encuentra automatizado en la plataforma de Gobernanza del CCN, constituyendo un asistente para la adecuación que proporciona:

- Un modelo práctico de gobierno de la seguridad organizado por bloques de responsabilidad, tal y como se mencionó anteriormente. Ofrece los modelos de documentos necesarios para la designación de roles y la elaboración de la Política de Seguridad.

- Una categorización del sistema, básica, que incluye un catálogo de servicios contemplando las competencias de las entidades a las que va dirigido, conforme a lo establecido en el Anexo I del ENS, descargable y preparado para su aprobación.

- Una declaración de aplicabilidad definitiva, que incluye, a modo de ejemplo, una propuesta para la elaboración, en caso necesario, de medidas compensatorias relacionadas con la posible dependencia jerárquica que pueda existir entre el rol de Responsable de Supervisión (responsable de la seguridad) y el Responsable de Operación (responsable del sistema), la utilización de cuentas privilegiadas, sistemas operativos sin soporte de seguridad, política de contraseñas insuficientemente rigurosa o plan de formación-concienciación (si no es de aplicación el propuesto). Documentación descargable y lista para su aprobación.

- Un informe de riesgos y aceptación del riesgo residual disponible para su descarga, generado por el Módulo de Verificación de Perfiles de Cumplimiento en función de los riesgos (MVPCR) disponible en el asistente.

- Un plan de formación-concienciación listo para su descarga, de dos años de duración, con el objetivo de proporcionar los conocimientos necesarios para conseguir la concienciación adecuada, e impulsar el conocimiento de amenazas y vulnerabilidades. Está compuesto por seis módulos (introductorio µCeENS, concienciación en ciberseguridad y ENS, básico de ciberseguridad, seguridad en correo electrónico, navegación segura y seguridad en dispositivos móviles). Cada módulo va dirigido a un perfil concreto. Los módulos se ofrecen a través de la plataforma Ángeles.

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

- Un repositorio para descargar el marco normativo con modelos de documentación (políticas, normas, procedimientos y otros documentos del sistema) necesarios durante la implantación, tales como:

    - Normativas: de uso de medios electrónicos (incluyendo procedimiento de limpieza de metadatos y acuse de recibo para difundir a los usuarios), de gestión documental, de registros de actividad, de acceso remoto, y el modelo de adhesión a la política de firma electrónica de la Administración General del Estado (AGE).

    - Procedimientos: de gestión del mantenimiento y parcheado, de gestión de usuarios, de copias de seguridad, de requisitos legales, de soportes y registro de entrada y salida, de adquisición de nuevos componentes, de autorizaciones, de gestión de incidentes, y de soportes y dispositivos conectados a la red.

    - Otros documentos: lista de mantenimiento, acciones puntuales y registro de entrada y salida de soportes.

- Un apartado de implantación donde se irán subiendo las evidencias de cumplimiento de las 38 medidas de seguridad que forman parte del PCE-RFS.

Una vez subidas todas las evidencias, se podrá solicitar la auditoría de conformidad con el ENS, conforme al PCE-RFS. La entidad de certificación u Órgano de Auditoría Técnica (OAT), una vez tramitada la solicitud, procederá a iniciar el proceso de auditoría evaluando las evidencias aportadas. En caso de que se requiera aclaración o documentación adicional, estas entidades se pondrán en comunicación a través del foro de la plataforma. Una vez finalizado el proceso de auditoría, estas entidades emitirán de forma automática el correspondiente certificado de conformidad con el ENS o bien, en caso de que el dictamen no sea favorable (no conformidad), solicitarán que se les remita el Plan de Acciones Correctivas (PAC) en un plazo de un mes. Una vez analizado y considerado como correcto, emitirán el certificado de conformidad.

A fecha de redacción de este capítulo, el CCN había anunciado la modificación del PCE para su actualización y mejora, reforzando además las medidas de seguridad conforme a la criticidad de los servicios afectados por la Directiva NIS2.

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

3.4. PCE 883

Una vez analizado el PCE-RFS como un primer paso en la implantación del ENS en entidades locales de pequeño tamaño, procederemos a analizar el PCE 883. Al igual que en el PCE anterior, debe tenerse en cuenta que el CCN ha anunciado recientemente su modificación, así como la actualización de sus rangos poblacionales en un proceso de mejora continua.

Este PCE se subdivide según las especialidades de las entidades locales y los riesgos derivados de los servicios e información que gestionan; es decir, cuantas más competencias y habitantes, mayor riesgo, pero también mayor capacidad económica y de personal para implementar las medidas. Por ello, las declaraciones de aplicabilidad correspondientes a los subtipos del PCE 883 son diferentes. Así:

- Tiene en cuenta la escasez de medios de los ayuntamientos con menos de 5000 habitantes, así como sus menores competencias y su organización más sencilla.

- También contempla las peculiaridades de los ayuntamientos con menos de 20 000 habitantes y el apoyo que reciben de las diputaciones provinciales.

- Considera que los ayuntamientos con más de 20 000 habitantes, pese a disponer de más competencias, recursos económicos y estructura organizativa, no siempre tienen la suficiente madurez en el sistema de gestión de seguridad, y requieren las adaptaciones que facilita el PCE.

- Recoge las peculiaridades de diputaciones, comunidades autónomas uniprovinciales, cabildos y consejos insulares respecto a sus sistemas de información.

Si bien, al tratarse de un capítulo, no es posible detallar las peculiaridades de cada subtipo del PCE, se abordan algunos aspectos destacados y la forma de implementación global del PCE.

Modelo de gobernanza

En el PCE no existe un modelo de gobernanza adaptado, como ocurre con los bloques de gobierno del PCE 890, debiéndose acudir al modelo estándar descrito en la Guía CCN-STIC 801.

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

Es importante destacar que, aunque no forma parte de la organización interna de las entidades, uno de los aspectos que regula el PCE 883 es la aplicación de medidas en función de si existe externalización en la nube. En esos casos, se debe exigir a los prestadores de servicios TIC (incluidos los de la nube, incluso si el contrato es un suministro, tal y como ha declarado la Junta Consultiva de Contratación) que dispongan de un punto de contacto (POC). Esta figura es una de las novedades introducidas por el Real Decreto 311/2022 y tiene importancia crucial en la gestión de la seguridad, ya que es el contacto de la entidad con el prestador del servicio y debe ser quien comunique y gestione los incidentes de seguridad.

El POC, que será el responsable de la seguridad o alguien en quien este delegue, debe ser identificado por el adjudicatario comunicando un medio de contacto. Como recomendación, se debería exigir su designación o comunicación bien en los pliegos del contrato, en la resolución de adjudicación o —cuando sea un prestador con condición de encargado del tratamiento— incluso en el contrato de encargado del tratamiento, al igual que se exige un POC en materia de protección de datos, cargo que será ejercido en ese caso por el delegado de protección de datos de la entidad adjudicataria en el apartado correspondiente a las comunicaciones en dicha materia.

Análisis de riesgos y declaración de aplicabilidad

El PCE sigue el modelo de gobernanza estándar, pero modifica y adecúa la declaración de aplicabilidad según los rangos poblacionales y los servicios prestados por las entidades locales, dependiendo también de si cuentan o no con el apoyo de las diputaciones para la prestación de esos servicios.

En esta declaración de aplicabilidad se recogen las medidas conforme a los riesgos y a las características propias de las entidades locales —según sus peculiaridades como servicios prestados o información tratada—, aunque la adecuación es igual a la estándar. Gracias a esta declaración, no es necesario justificar las medidas de seguridad que no se aplican; siempre será necesario disponer de un análisis de riesgos y asumir el riesgo residual resultante, planificando actuaciones que permitan cumplir con el principio de mejora continua del art. 27 del ENS.

Es interesante, de cara a facilitar la implementación del sistema de gestión del ENS, que el CCN ha facilitado un asistente, al igual que ya se ha comentado en el apartado del PCE de Requisitos Fundamentales de Seguridad.

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

El asistente, que sirve como repositorio documental en la generación de evidencias, comunicándose con el auditor, permite la concreción del alcance del sistema, disponiendo de un catálogo de servicios e información ya predefinido al que se podrán incorporar otros nuevos, así como un modelo de política, normativas y diferentes procedimientos. Además, tras la definición de la información y los servicios, se genera la declaración de aplicabilidad provisional que permite a la entidad valorar la adecuación de las medidas, procediendo después al paso a definitiva una vez realizado el correspondiente análisis de riesgos. Es decir, el CCN diseña un asistente que, paso tras paso, permite a la entidad llegar a la conformidad con el ENS, bien en el modelo estándar o bien mediante un PCE específico.

4. Los Gobiernos intermedios como organismos de certificación del ENS

A lo largo del presente capítulo se ha ido reiterando la importancia de que las diputaciones provinciales, cabildos, consejos insulares o comunidades uniprovinciales apoyen proactivamente a los ayuntamientos de menor tamaño para que puedan cumplir con el ENS. Dentro de esas labores de apoyo se encuentra, también, el Marco de Certificación ENS para Entidades Locales, en el cual el CCN propone un modelo de implantación conjunta en ayuntamientos con características tecnológicas y administrativas similares, contando con el soporte de la diputación provincial, cabildo, consejo insular o entidad competente en materia de administración electrónica o informatización de las entidades locales dependientes, adheridas o conveniadas, con el objetivo de alcanzar la certificación de conformidad con el ENS para los sistemas de información municipales, sobre todo los relacionados con Sede Electrónica.

Además, estas entidades pueden desempeñar una interesante función como órgano de auditoría técnica (en adelante OAT). La posibilidad de que las diputaciones actúen como OAT está dentro de las competencias que tienen atribuidas en materia de cooperación para el despliegue seguro de la administración electrónica y el soporte técnico-jurídico a los municipios dentro de su ámbito territorial.

Las entidades locales que, como las diputaciones, tienen competencias en la cooperación y colaboración con otras, pueden constituirse como un órgano de auditoría técnica que les permita realizar auditorías de conformidad con el ENS a las entidades incluidas en su territorio, siempre que cumplan determinados requisitos y puedan acreditarlos. A fecha actual, no existe ninguna entidad local acreditada como OAT; sí lo están algunos or-

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

ganismos públicos, como el CESTIC (Centro de Sistemas y Tecnologías de la Información y las Comunicaciones) o la *Agència de Ciberseguretat de Catalunya*.

Para constituirse como OAT, la entidad debe disponer de un área diferenciada con personal cualificado que incluya un responsable del área, un responsable técnico y un equipo de auditores especializados en ENS (senior, junior), encabezado por un auditor jefe y el comité o persona que aprueba la certificación de conformidad.

El proceso de acreditación como OAT requiere cumplir varios requisitos:

- Que la entidad disponga de roles diferenciados y autónomos que garanticen la debida imparcialidad y ausencia de conflicto de intereses entre el área de auditoría y otras, como las que prestan apoyo a la implantación en los ayuntamientos o los servicios técnicos. Esta independencia debe mantenerse también respecto de los propios auditados.

- Que el área tenga independencia funcional y no reciba instrucciones externas relacionadas con sus funciones.

- La Guía CCN STIC 122, que describe el procedimiento para ser un OAT, establece, entre otros requisitos, la confidencialidad del personal y el cumplimiento de las siguientes condiciones:

    - Competencia profesional: experiencia de al menos 3 años en auditorías o inspecciones de sistemas de información y su seguridad.

    - Competencia técnica del personal del área especializada en auditorías y ENS.

    - Disponer de procedimientos y metodologías que permitan llevar a cabo las auditorías.

La consideración de la entidad como OAT será realizada por el CCN, que además de verificar los requisitos citados, exigirá una parte práctica: los integrantes del OAT deberán asistir a dos auditorías realizadas por el CCN, y el CCN participará en dos auditorías realizadas por el OAT.

El reconocimiento como OAT tendrá una validez de dos años, y deberá ir renovándose por el mismo periodo.

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

5. Implicaciones de la Directiva relativa a las medidas para un elevado nivel común de ciberseguridad en toda la Unión (Directiva NIS2) en las entidades locales

Para finalizar el capítulo, abordaremos las implicaciones de la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva NIS2), en relación con las entidades locales, si bien los términos de este apartado pueden sufrir modificaciones tras la transposición de dicha directiva, que, a fecha de redacción, estaba aún sin completarse.

La Directiva NIS2 afronta los nuevos retos en la ciberseguridad a nivel de la Unión Europea, ampliando el alcance de la anterior directiva y mejorando la coordinación entre los distintos actores implicados. Así, la Directiva NIS2 indica lo siguiente:

> "Los sistemas de redes y de información se han convertido en un aspecto crucial del día a día gracias a la velocidad de la transformación digital y la interconexión de la sociedad, también en los intercambios transfronterizos. Esta evolución ha causado una expansión del panorama de las ciberamenazas, con la consiguiente aparición de nuevos desafíos que requieren respuestas adaptadas, coordinadas e innovadoras en todos los Estados miembros. El número, la magnitud, la sofisticación, la frecuencia y los efectos de los incidentes van en aumento y representan una grave amenaza para el funcionamiento de los sistemas de redes y de información. Como consecuencia de ello, los incidentes pueden interrumpir las actividades económicas en el mercado interior, generar pérdidas financieras, mermar la confianza de los usuarios y ocasionar grandes daños a la economía y la sociedad de la Unión. Por consiguiente, la preparación y la eficacia en materia de ciberseguridad son más esenciales que nunca para que el mercado interior funcione correctamente. Además, la ciberseguridad es un factor facilitador esencial para que muchos sectores críticos se sumen con éxito a la transformación digital y aprovechen plenamente las ventajas económicas, sociales y sostenibles de la digitalización".

La ampliación del alcance de la Directiva NIS2 incluye a las Administraciones públicas territoriales, tanto la Administración General del Estado, las autonómicas y las locales como su sector público, imponiendo nuevas

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

obligaciones. Si bien la Directiva incluye en su alcance a las Administraciones públicas, queda a la transposición de cada país la concreción del tipo de entidades locales a las que se aplica, según se indica en su art. 2.5.

El alcance de la Directiva se determina en función del tamaño de las entidades (gran, mediana o pequeña empresa), y las actividades incluidas en los anexos I y II se consideran esenciales o importantes. En dichos anexos se describen sectores estratégicos como el energético, transporte, investigación o sanitario.

Aunque la aplicación de la Directiva a las entidades locales puede variar según la transposición, en los anexos I y II se incluyen actividades que son competencias municipales según la LBRL, y que pueden considerarse servicios esenciales o importantes. A continuación, se enumeran los sectores incluidos en esos anexos cuyos servicios pueden ser prestados por las entidades locales (ya sea de forma directa o indirecta) mediante diputaciones, ayuntamientos, mancomunidades, consorcios, empresas públicas u otras figuras jurídicas:

ANEXO I

- Agua potable: suministradores y distribuidores de aguas destinadas al consumo humano, según la Directiva (UE) 2020/2184:

  "a) todas aquellas aguas, ya sea en su estado original, ya sea después del tratamiento, utilizadas para beber, cocinar, preparar alimentos y otros usos domésticos, en locales tanto públicos como privados, sea cual fuere su origen e independientemente de que se suministren a través de una red de distribución, de una cisterna o envasadas en botellas u otros recipientes, incluidas las aguas de manantial;

  b) todas las aguas utilizadas en empresas alimentarias para fines de fabricación, tratamiento, conservación o comercialización de productos o sustancias destinados al consumo humano".

- Aguas residuales: empresas dedicadas a la recogida, la eliminación o el tratamiento de aguas residuales urbanas, domésticas o industriales, conforme a la Directiva 91/271/CEE:

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

- o "Aguas residuales urbanas: las aguas residuales domésticas o la mezcla de las mismas con aguas residuales industriales y/o aguas de correntía pluvial".

- o "Aguas residuales domésticas: las aguas residuales procedentes de zonas de vivienda y de servicios y generadas principalmente por el metabolismo humano y las actividades domésticas".

- o "Aguas residuales industriales: todas las aguas residuales vertidas desde locales utilizados para efectuar cualquier actividad comercial o industrial, que no sean aguas residuales domésticas ni aguas de correntía pluvial".

Estos servicios están contemplados en el art. 25.2 c) de la LBRL: "c) Abastecimiento de agua potable a domicilio y evacuación y tratamiento de aguas residuales", sin perjuicio de las competencias de la diputación.

ANEXO II

- Gestión de residuos: según la Directiva 2008/98/CE, se define como "la recogida, el transporte, la valorización y la eliminación de los residuos, incluida la vigilancia de estas operaciones, así como el mantenimiento posterior al cierre de los vertederos, incluidas las actuaciones realizadas en calidad de negociante o agente".

Además, en los anexos se incluyen otras actividades que en ocasiones prestan las entidades locales, como servicios sanitarios o de investigación.

La prestación de estos servicios descritos en los anexos puede realizarse, según el art. 85 de la LBRL, de forma directa o indirecta, por lo que deberá prestarse especial atención tanto al sector público municipal (gestión directa) como a las empresas contratadas para la prestación de dichos servicios (gestión indirecta). Será, por lo tanto, tarea de la entidad local verificar si algunas de las empresas públicas o entidades de su sector público se encuentran en el ámbito de NIS2 para fortalecer sus medidas de seguridad y, si los servicios son prestados por empresas privadas, establecer mecanismos de control de la cadena de proveedores, como veremos más adelante.

Además, las entidades locales pueden estar bajo el alcance de NIS2 cuando hayan sido declaradas como operadores críticos, que son aquellas entidades u organismos responsables de las inversiones o del funcionamiento diario de una instalación, red, sistema o equipo físico o de tecno-

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

logía de la información designada como infraestructura crítica. Pueden incluirse las entidades cuando, según el art. 14 del Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas, al menos una de las infraestructuras por ellas gestionadas reúna la consideración de infraestructura crítica, existiendo en la ley los parámetros para la consideración como tal.

A fecha de redacción del presente capítulo, aún no se había aprobado la transposición de la Directiva, pero se había publicado un anteproyecto denominado "Ley de Coordinación y Gobernanza de la Ciberseguridad". Entre otras novedades relacionadas con las entidades locales, se puede destacar la inclusión de los ayuntamientos como entidades esenciales o importantes, así como de su sector público institucional.

- Son entidades esenciales la Administración General del Estado, las comunidades autónomas, las provincias, cabildos, islas y los ayuntamientos de gran población, más el sector público institucional de todas ellas.

- Se consideran entidades importantes los ayuntamientos de más de 20 000 habitantes y su sector público institucional.

- El ENS se configura como el *framework* de referencia que sirve, cuando exista certificación, como evidencia de cumplimiento de las obligaciones de esta normativa, pudiendo aprobarse por parte del CCN un PCE específico.

- Se destaca la importancia del Responsable de la Seguridad, que deberá ser interno, pero que contará con un equipo multidisciplinar de apoyo que puede ser interno o externo.

- Se regulan también las acciones de supervisión y las medidas a adoptar por las autoridades de control de los diferentes sectores.

- Se detalla el régimen de infracciones, así como la responsabilidad de los órganos de gobierno en caso de incumplimientos, quedando exoneradas las Administraciones públicas de la imposición de sanciones consistentes en una multa económica.

Como se ha explicado, la aplicación de NIS2 supone que las entidades bajo su alcance deban establecer medidas de seguridad reforzadas. La dirección adquiere nuevas responsabilidades en el cumplimiento de la seguridad, y el Responsable de la Seguridad en NIS2 adquiere un peso más

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

relevante dentro de la organización. También es preciso un control exhaustivo de la cadena de prestadores y los suministros, así como una adecuada gestión de los incidentes de seguridad.

En relación con las medidas de seguridad en NIS2, el CCN había aprobado un PCE —la Guía CCN-STIC 892— para organizaciones en el ámbito de aplicación de la Directiva NIS2 (PCE NIS2), que podrá ser objeto de adaptación una vez que se haya transpuesto dicha norma, si bien, a fecha actual, este perfil se ha despublicado para su actualización.

Todo apunta a que la nueva regulación que aprobará el CCN desarrollará, para España, el reglamento de ejecución de NIS2 relacionado con los sectores TIC[21], en el que se abordarán las medidas de seguridad aplicables a determinadas entidades y las especialidades en la comunicación de ciberincidentes.

Con carácter general, en una entidad local que no se encuentra en el ámbito de los PCE 890 u 883 antes señalados, las medidas de seguridad, tras el análisis de riesgos correspondiente, tienden a las correspondientes a la categoría media del ENS, por lo que aquellas entidades locales ya certificadas en el ENS que entren dentro del ámbito de aplicación de NIS2 (tanto del sector público como privadas) tendrán gran parte del camino ya recorrido de cara a la adaptación desde el punto de vista de la seguridad, sin perjuicio de cumplir con otras obligaciones, como el registro de la entidad como esencial o la comunicación de incidentes en ciberseguridad, que se analizarán, someramente, al final del capítulo.

Cuestión relevante en la Directiva NIS2 es, sin duda, el control de la cadena de prestadores/proveedores de las entidades en el ámbito de aplicación de la Directiva, algo que también ya recogía el ENS en la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, estando ahora recogido en el art. 2.3 del ENS, y existiendo también una alineación entre los requisitos exigidos por ambas normas en relación

21. El Reglamento de Ejecución (UE) 2024/2690 de la Comisión, de 17 de octubre de 2024, por el que se establecen las disposiciones de aplicación de la Directiva (UE) 2022/2555, regula las condiciones específicas en relación —entre otras— con las medidas de seguridad para los sectores tecnológicos de la Directiva, en concreto: los proveedores de servicios de DNS, los registros de nombres de dominio de primer nivel, los proveedores de servicios de computación en la nube, los proveedores de servicios de centro de datos, los proveedores de redes de distribución de contenidos, los proveedores de servicios gestionados, los proveedores de servicios de seguridad gestionados, los proveedores de mercados en línea, los motores de búsqueda en línea, las plataformas de servicios de redes sociales, y los proveedores de servicios de confianza.

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

con la necesidad de controlar a las empresas proveedoras de servicios o suministros tecnológicos y a la cadena de subcontratistas.

La Directiva NIS2 aborda el control de los proveedores en su considerando 85:

> "Hacer frente a los riesgos de ciberseguridad provenientes de la cadena de suministro de una entidad y su relación con sus proveedores, como los proveedores de servicios de almacenamiento y tratamiento de datos o los proveedores de servicios de seguridad gestionados y editores de *software*, resulta especialmente importante habida cuenta de la prevalencia de incidentes en los que las entidades han sido víctimas de ciberataques y en que agentes malintencionados han podido comprometer la seguridad de los sistemas de redes y de información de una entidad aprovechándose de las vulnerabilidades que afectan a productos y servicios de terceros. Por ello, las entidades esenciales e importantes deben evaluar y tener en cuenta la calidad general y la resiliencia de los productos y los servicios, las medidas para la gestión de riesgos de ciberseguridad integradas en ellos y las prácticas en materia de ciberseguridad de sus proveedores y prestadores de servicios, incluidos sus procedimientos de desarrollo seguro. En particular, debe fomentarse que las entidades esenciales e importantes incorporen medidas para la gestión de riesgos de ciberseguridad en los acuerdos contractuales con sus proveedores y prestadores de servicios directos. Dichas entidades podrían tomar en consideración los riesgos provenientes de otros niveles de proveedores y prestadores de servicios".

Y en el art. 21.2, apdos. c) y d), cuando se detallan las medidas se seguridad: "d) la seguridad de la cadena de suministro, incluidos los aspectos de seguridad relativos a las relaciones entre cada entidad y sus proveedores o prestadores de servicios directos; e) la seguridad en la adquisición, el desarrollo y el mantenimiento de sistemas de redes y de información, incluida la gestión y divulgación de las vulnerabilidades". Incorporando el anteproyecto la obligación de los prestadores de servicios de comunicar el POC antes referido.

Estas obligaciones de control de la cadena de suministro que, desde un punto de vista jurídico, deben concretarse en los pliegos de condiciones técnicas y administrativas o, en contratos de menor cuantía (negociados, menores), en el contrato de encargado del tratamiento[22] o en la resolución

22. El contrato de encargado del tratamiento es un acto jurídico que vincula a las partes, como se indica en el art. 28 del RGPD, y en su contenido se pueden indicar las medidas técnicas y organizativas en el tratamiento de los datos personales.

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

de adjudicación, podrán corresponderse con las siguientes medidas del Anexo II:

- [op.ext.3] Protección de la cadena de suministro (en categoría alta, como hemos señalado).
- [op.ext.1] Contratación y acuerdos de nivel de servicio.
- [op.ext.2] Gestión diaria.
- [op.ext.4] Interconexión de sistemas.
- Art. 19. Adquisición de productos de seguridad y contratación de servicios de seguridad. [op.pl.3] Adquisición de nuevos componentes.
- [op.pl.5] Componentes certificados.
- [mp.sw.1] Desarrollo de aplicaciones.
- [mp.sw.2] Aceptación y puesta en servicio.
- [op.exp.4] Mantenimiento y actualizaciones de seguridad.
- [op.mon.3] Vigilancia.

Otro de los puntos importantes que las entidades en el alcance de NIS2 deben abordar es la revisión de los procedimientos para la gestión de los incidentes en ciberseguridad. Si bien hasta la fecha las entidades locales ya deben disponer de un procedimiento para gestionar los incidentes de seguridad, que tendrá en cuenta los criterios de la Guía CCN-STIC 817, y de un procedimiento —integrado o no con el anterior— para la gestión de las violaciones de seguridad o brechas de datos personales, conforme a los arts. 33 y 34 del RGPD, sin perjuicio de otros a los que estén obligadas, como los relacionados con la posible consideración como infraestructura crítica, ahora deberán también canalizar los incidentes de ciberseguridad, detallándose en el anteproyecto que, para las entidades públicas, se deberán comunicar al CCN como organismo de control, como hasta la fecha, si bien se propone la creación de un organismo nuevo para coordinar las diferentes acciones y entidades que controlan los diferentes sectores.

El procedimiento de gestión de incidentes de ciberseguridad en NIS2, que para los sectores tecnológicos se detalla en el Reglamento de Ejecu-

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

ción[23], presenta similitudes en cuanto a plazos con el procedimiento de brechas de datos personales de los arts. 33 y 34 del RGPD, desarrollado en la *Guía para la notificación de violaciones de seguridad* de la Agencia Española de Protección de Datos. En NIS2, las notificaciones a la autoridad de control (pendiente de concretar en España en la transposición definitiva de la Directiva) deberán realizarse de forma paulatina, tal como recoge el considerando 101 de la Directiva:

> "La presente Directiva establece un enfoque en varias etapas respecto a la notificación de incidentes significativos a fin de alcanzar el equilibrio adecuado entre, por un lado, una notificación ágil que ayude a reducir la posible propagación de incidentes significativos y permita a las entidades esenciales e importantes buscar asistencia, y, por el otro, una notificación minuciosa que extraiga lecciones valiosas de cada incidente y mejore con el tiempo la ciberresiliencia de las entidades individualmente y de sectores completos. En este sentido, la presente Directiva debe incluir la notificación de incidentes que, según una evaluación inicial realizada por la entidad afectada podrían provocar perturbaciones operativas o perjuicios económicos graves para dicha entidad o podrían afectar a otras personas físicas o jurídicas causándoles perjuicios materiales o inmateriales considerables. Tal evaluación inicial debe tener en cuenta, entre otros aspectos, los sistemas de redes y de información afectados, y en particular su importancia para la prestación de los servicios de la entidad, la gravedad y las características técnicas de la ciberamenaza, así como las vulnerabilidades subyacentes que se estén aprovechando y la experiencia de la entidad con incidentes similares. Indicadores como la medida en que se ve afectado el funcionamiento del servicio, la duración de un incidente o el número de destinatarios de los servicios afectados podrían ser importantes a la hora de determinar si la perturbación operativa del servicio es grave".

23. Reglamento de Ejecución (UE) 2024/2690 de la Comisión, de 17 de octubre de 2024, por el que se establecen las disposiciones de aplicación de la Directiva (UE) 2022/2555 en lo que respecta a los requisitos técnicos y metodológicos de las medidas para la gestión de riesgos de ciberseguridad y en el que se detallan los casos en que un incidente se considera significativo con respecto a los proveedores de servicios de DNS, los registros de nombres de dominio de primer nivel, los proveedores de servicios de computación en nube, los proveedores de servicios de centro de datos, los proveedores de redes de distribución de contenidos, los proveedores de servicios gestionados, los proveedores de servicios de seguridad gestionados, los proveedores de mercados en línea, motores de búsqueda en línea y plataformas de servicios de redes sociales, y los proveedores de servicios de confianza ("DOUE" núm. 2690, de 18 de octubre de 2024).

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

Las etapas para la comunicación del incidente significativo son las siguientes:

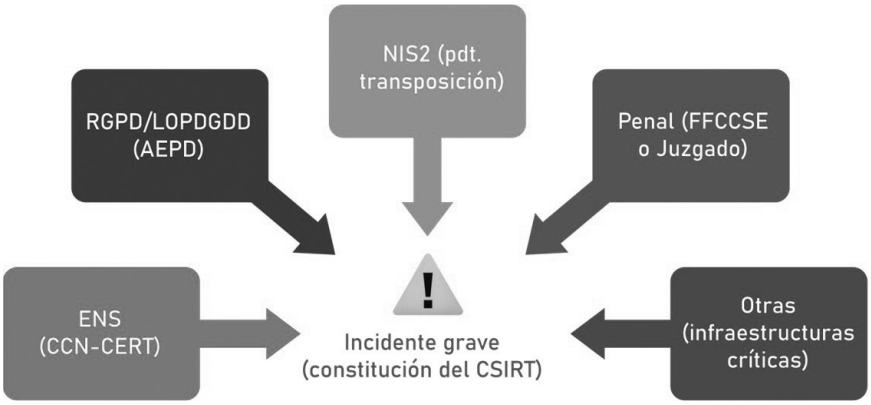
- Alerta temprana, en el plazo de 24 horas: se trata de una primera comunicación con los datos básicos del incidente —tipología, alcance dentro de la organización, si se produce por una actuación ilícita y si tiene implicaciones transfronterizas—.

- Dentro de las 72 horas desde que se conoce el incidente: se incluirá la información disponible y, cuando sea preciso, la actualización de los datos de la alerta temprana. Además, se realizará una evaluación inicial de la gravedad e impacto en la organización y, en caso de que ya sean conocidos, los indicadores de compromiso.

- El CSIRT al que se comunique el incidente podrá solicitar información adicional, debiendo la entidad emitir un informe sobre los puntos requeridos.

- Comunicación completa, en el plazo de 30 días desde la alerta: tras realizar el correspondiente informe forense, se detallará el vector de ataque, la causa raíz, el impacto y las medidas adoptadas para la mitigación y contención.

El modelo de gestión de incidentes debe tener en cuenta las distintas normas que puedan afectarle, debiendo coordinarse entre todos los actores implicados para su correcta gestión. A modo de ejemplo, en el siguiente gráfico se muestran las diferentes normativas aplicadas junto con la autoridad que las gestiona.



Fuente: elaboración propia

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

6. Bibliografía

Guías y buenas prácticas CCN

CCN. Mar. 2024. Guía CCN-STIC IC-01/19 ENS sobre Criterios Generales de Auditoría y Certificación. (Categoría: Serie 100 Procedimientos).

CCN. Mar. 2019. Guía CCN-STIC 801 Responsabilidades y Funciones en el ENS. (Categoría: Serie 800 ENS).

CCN. May. 2020. Guía CCN-STIC 803 sobre la Valoración de los Sistemas. (Categoría: Serie 800 ENS).

CCN. Abr. 2024. Guía CCN-STIC-892 Perfil de Cumplimiento Específico para Organizaciones en el Ámbito de Aplicación de la Directiva NIS2 (PCE-NIS2). (Categoría: Serie 800 ENS).

CCN. Oct. 2018. Guía CCN-STIC 819 Medidas Compensatorias. (Categoría: Serie 800 ENS).

CCN. Oct. 2023. Guía CCN-STIC-808 Verificación del Cumplimiento de las Medidas en el ENS. (Categoría: Serie 800 ENS).

CCN. Feb. 2023. Informe de Buenas Prácticas CCN-CERT_BP_14 Declaración de Aplicabilidad ENS. (Categoría: Serie 800 ENS).

CCN. May. 2023. Guía CCN-STIC-852 Perfil de Cumplimiento Específico Organismos Pagadores. (Categoría: Serie 800 ENS).

CCN. May. 2022. Guía CCN-STIC-881A Perfil de Cumplimiento Específico Universidades. (Categoría: Serie 800 ENS).

CCN. May. 2020. Guía CCN-STIC-883 Guía de Implantación del ENS para Entidades Locales y Anexos. (Categoría: Serie 800 ENS).

CCN. Abr. 2020. Guía CCN-STIC-817 Gestión de Ciberincidentes. (Categoría: Serie 800 ENS).

CCN. Mar. 2023. Guía CCN-STIC-890A Perfil de Cumplimiento Específico de Requisitos Esenciales de Seguridad - Entidades Locales. (Categoría: Serie 800 ENS).

CCN. Mar. 2023. Guía CCN-STIC-890C Perfil de Cumplimiento Específico de Requisitos Esenciales de Seguridad. (Categoría: Serie 800 ENS).

CCN. Sep. 2023. Guía CCN-STIC-122 Procedimiento de Reconocimiento de Entidades de Certificación del ENS del Sector Público y Requisitos del Órgano de Auditoría Técnica. (Categoría: Serie 100 Procedimientos).

CCN. Abstract. Marco de Certificación ENS para Entidades Locales. (Categoría: Serie 800 ENS).

Otros documentos y normativa relacionada

AEPD. Jun. 2021. Guía para la Notificación de Brechas de Datos Personales.

Anteproyecto Ley de Coordinación y Gobernanza de la Ciberseguridad.

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

CAPÍTULO VII

La gobernanza de la ciberseguridad en las entidades locales y a nivel local

Luis Feijoo García
Funcionario de carrera del Cuerpo Superior de Técnicos de Administración Local.
Asesor jurídico en Administración Electrónica, Transparencia y Protección de Datos de la Diputación de Pontevedra

SUMARIO. 1. Introducción. 2. Gobernanzas. 2.1. Concepto. 2.2. Modelos sectoriales de gobernanza. *2.2.1. Gobernanza en administración electrónica. 2.2.2. Gobernanza en protección de datos. 2.2.3. Gobernanza en reutilización de la información del sector público. 2.2.4. Gobernanza en accesibilidad web. 2.2.5. Gobernanza de la inteligencia artificial en las Administraciones públicas*. 2.3. Gobernanza en materia de ciberseguridad. Estructura funcional y roles definidos. 2.4. Principios sostenibles de gobernanza de la ciberseguridad. **3. Modelos de roles y responsabilidades en materia de ciberseguridad.** 3.1. Marco general del Esquema Nacional de Seguridad (ENS) y gobernanza. *3.1.1. Principales roles definidos por el ENS. 3.1.2. Asignación formal y trazabilidad.* 3.2. Modelo de gobernanza adaptado a las entidades locales (EE. LL.). 3.3. La función de los cargos electos y habilitados nacionales. *3.3.1. Alcaldes/presidentes y la Junta de Gobierno Local. 3.3.2. Secretarios e interventores.* **4. Cooperación y coordinación entre distintas áreas y Administraciones.** 4.1. Cooperación interna: una estrategia de gestión integrada. 4.2. Coordinación interadministrativa: el papel de la colaboración institucional. **5. Conclusiones. 6. Bibliografía.**

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

1. Introducción

Es indudable que en el mundo actual, caracterizado por una creciente interconexión global y una cada vez mayor dependencia digital, las tecnologías de la información y la comunicación (TIC) han adquirido una centralidad en el funcionamiento de nuestra sociedad. Esta realidad plantea desafíos significativos que trascienden territorios y los distintos niveles de gobierno, exigiendo respuestas coordinadas y eficaces[1]. Entre esos desafíos, uno de los más relevantes es, sin duda, la protección del ciberespacio institucional, que afecta a todos los niveles administrativos.

Así, la digitalización de servicios, tanto públicos como privados, ha traído consigo una creciente exposición a riesgos derivados de amenazas de índole tecnológica[2]. A este respecto, resulta evidente que la garantía de continuidad de los servicios públicos digitales, la integridad de los sistemas y la confidencialidad de la información tratada son condiciones esenciales a tener en cuenta en toda actividad administrativa.

Por ello, la ciberseguridad ha dejado de ser una cuestión meramente técnica para convertirse en un componente esencial de la gobernanza pública. Las Administraciones, tanto estatales como autonómicas y locales, deben implementar políticas de protección de la información y resiliencia digital que cumplan con el marco normativo vigente, liderado por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD); 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, por la que se modifican el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (NIS2); el Real Decreto 311/2022, de 3 de mayo, por el que se regula

1. A modo ilustrativo, en el reciente conflicto entre Israel e Irán, los ciberataques dirigidos a Israel aumentaron un 700 % en los dos días posteriores al anuncio público de los bombardeos israelíes sobre instalaciones iraníes: https://www.jpost.com/business-and-innovation/tech-and-start-ups/article-857790.

2. Según la nota de prensa publicada el 6 de mayo de 2024 por el Ministerio para la Transformación Digital y de la Función Pública, con motivo de la aprobación de un conjunto de actuaciones en ciberseguridad y ciberdefensa que complementan las medidas incluidas en el Plan Nacional de Ciberseguridad (aprobado el 29 de marzo de 2022), en 2024 se detectaron más de 100 000 ciberataques en España, y cada tres días se registró uno considerado como muy grave. Desde 2015, los ciberataques han aumentado un 300 %.

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

el Esquema Nacional de Seguridad; y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP).

Además, la aprobación del Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad[3] supondrá un avance significativo en la definición del marco normativo de ciberseguridad en España, y debe ser valorado también desde la perspectiva de las entidades locales. A pesar de que muchas de las disposiciones están orientadas a operadores de sectores esenciales o importantes en el sentido de la NIS2, el impacto normativo y organizativo en las entidades locales será innegable, especialmente en lo relativo a la gobernanza interna, la gestión de riesgos y la notificación de incidentes.

En este escenario, la Administración local, por su cercanía y competencia directa en múltiples áreas sensibles —padrón de habitantes, servicios sociales, gestión tributaria, licencias, entre otros—, custodia información de especial relevancia para la seguridad y privacidad de los ciudadanos. Por tanto, su operatividad segura no es solo una cuestión técnica, sino también una exigencia de responsabilidad institucional.

Los actores locales desarrollan ya gran parte de su labor a través de medios digitales. Esta dependencia de lo digital, aunque positiva en términos de eficiencia y eficacia, nos convierte también en potenciales blancos de ciberataques, con independencia del tamaño de nuestra Administración o nuestro presupuesto. Por ello, puedo afirmar con rotundidad que todas las entidades locales, grandes o pequeñas, disponen de información y sistemas que pueden resultar valiosos para actores maliciosos[4].

En este proceso de generalización de los medios electrónicos las entidades locales (ayuntamientos, diputaciones provinciales, cabildos y consejos insulares) deben hacer frente a sus obligaciones en lo que se refiere a la defensa de la infraestructura tecnológica, así como los datos que manipulan en su día a día, y todo ello con unas evidentes limitaciones en recursos humanos y materiales.

En este marco el Centro Criptológico Nacional (CCN) y la Federación Española de Municipios y Provincias (FEMP), como entidades de referen-

3. 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.

4. En lo que va de 2025 se han notificado incidentes de ciberseguridad en ayuntamientos como los de Badajoz, Mérida, Benavente, San Sebastián, Irún, Hondarribia, Calvé y Vigo, así como en las diputaciones de Valencia, Cáceres, Badajoz y Guipúzcoa.

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

cia para la mejora de la ciberseguridad y para la representación municipal respectivamente, han llevado a cabo un trabajo creciente para presentar a las corporaciones locales instrucciones claras, herramientas operativas y apoyo institucional.

Una vez más las actuaciones en ese contexto no son otras que las de robustecer de forma coordinada y conjunta la resiliencia de los diferentes entornos digitales locales, así como la contribución para el fomento de una cultura de la seguridad conjunta. Por ello, a mi modo de ver, este es el único modo de avanzar hacia una Administración (solo puede ser digital) más robusta, más eficiente y más alineada con el interés general mediante un modelo colaborativo que comprometa a los cargos electos y a personal funcionario: alcaldes, secretarios, interventores, etc.

Es más, la creciente complejidad de las amenazas digitales como el *ransomware* avanzado, ataques de *phishing* y *smishing* mejorados por el uso de IA por parte de los ciberdelincuentes, no solamente requiere respuestas estructuradas, sino también sostenibles en el tiempo, lo que exige dotar a las entidades locales de unos marcos organizativos internos sólidos, flexibles y adaptados a su propia realidad administrativa.

Por ello, un elemento central de este enfoque debe ser, sin duda, la implementación de modelos de gobernanza humana en nuestros entornos administrativos, aplicando, además, mecanismos de coordinación entre los diversos actores participantes. Este modelo tiene que expresar los valores y principios de cada organización, tareas como la determinación de los roles y de las funciones más específicas, la delimitación de los responsables en los diferentes niveles jerárquicos, la correspondencia entre procesos de toma de decisiones en materia de seguridad, el establecimiento de canales de comunicación entre las áreas técnicas, jurídicas y políticas... Esta gobernanza no debe limitarse a aspectos normativos, sino que debe fomentar también una cultura de concienciación, capacitación y compromiso institucional coordinado.

Esto no va de disponer de herramientas de tecnología avanzada si no hay un modelo de liderazgo que garantice la utilización de estas tecnológicas para dar respuesta a cada vez más incidentes cibernéticos. Únicamente a partir de una gobernanza bien diseñada y ejecutada será posible garantizar que las medidas adoptadas no solo sean técnicamente adecuadas, sino que puedan llevarse a cabo, sean transparentes y tengan en cuenta el interés público.

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

Es preciso, por lo tanto, que los órganos de gobierno de los ayuntamientos, diputaciones y otras entidades locales tomen un papel activo en la planificación, en la supervisión y en la evaluación de sus políticas de ciberseguridad. Insisto: a pesar de que, por regla general, la mayor parte de nuestras entidades locales ya tienen políticas de seguridad aprobadas, me temo que la mayoría de estas contienen modelos de gobernanza inaplicables o que no se adaptan a la realidad de su organización.

En definitiva, con el presente artículo pretendo exponeros distintos modelos de gobernanza diferenciados y personalizables según vuestra capacidad operativa (pequeños municipios, municipios medianos, diputaciones, cabildos, etc.), permitiendo adoptar un enfoque escalonado, realista, conforme con los recursos disponibles, y sostenible a medio y largo plazo.

2. Gobernanzas

2.1. Concepto

Si pensamos en qué podemos entender por "gobernanza" aplicada al contexto que hoy nos ocupa, se me ocurre que podría entenderse como el conjunto de estructuras, prácticas, mecanismos y procesos mediante los cuales las instituciones públicas, en interacción con actores sociales y económicos, ejercen la toma de decisiones, ejecutan políticas públicas y rinden cuentas, promoviendo transparencia, eficiencia y participación.

En el contexto actual de transformación digital y riesgos crecientes en el ciberespacio, el concepto de gobernanza adquiere una dimensión estratégica para el sector público, particularmente en el ámbito de las entidades locales.

Diversas instituciones han contribuido a ampliar y precisar este concepto desde diferentes ópticas. Así, la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos ha subrayado que la buena gobernanza exige respeto por los derechos fundamentales, procesos institucionales transparentes, participación efectiva y mecanismos de rendición de cuentas. En la misma línea, la Comisión Europea ha destacado que la calidad de la gobernanza incide directamente en el bienestar ciudadano y en el rendimiento económico de los Estados.

Este concepto resulta especialmente valioso por su capacidad de abarcar y articular el conjunto de instituciones, mecanismos y vínculos que

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

configuran los procesos de dirección y gestión pública, permitiendo una comprensión más amplia e inclusiva del gobierno contemporáneo.

En el caso español, la Secretaría de Estado de Función Pública ha subrayado que la gobernanza moderna implica una reconfiguración de las relaciones administrativas, apostando por la colaboración intersectorial y por marcos normativos estables que promuevan confianza institucional, competitividad empresarial y simplicidad en la interacción entre ciudadanía y Administración. Esta visión resulta especialmente relevante para las entidades locales, que representan el nivel más próximo a la ciudadanía, siendo clave para garantizar servicios públicos digitales seguros y accesibles.

Pero es preciso también diferenciar entre gobernanza y gobernabilidad[5], dos conceptos frecuentemente confundidos. Mientras que la gobernabilidad se refiere a la capacidad efectiva del aparato de gobierno para ejercer sus funciones y responder a las demandas sociales con estabilidad y legitimidad, la gobernanza incorpora una dimensión más amplia e inclusiva, que abarca tanto los mecanismos del ejercicio del poder como las relaciones entre múltiples actores implicados en los procesos de decisión y control.

2.2. Modelos sectoriales de gobernanza

La transformación digital de las Administraciones públicas ha dejado de ser una opción para convertirse en una necesidad estructural. En este contexto, los modelos de gobernanza sectorial en el ámbito digital emergen como herramientas fundamentales para garantizar la eficacia, la coordinación y la rendición de cuentas en el ejercicio de las competencias públicas. En el caso de la Administración local, caracterizada por su proximidad al ciudadano y por una diversidad notable en cuanto a tamaño, capacidades técnicas y recursos disponibles, resulta imprescindible articular estructuras de gobernanza digital que se ajusten a sus particularidades organizativas.

La gobernanza sectorial en el entorno local no se refiere únicamente a la existencia de normas o políticas generales sobre tecnología o ciberseguridad. Más bien, implica la creación de marcos operativos diferenciados que permitan gestionar de forma coherente los distintos ámbitos digitales que afectan al gobierno local. Cada uno de estos sectores requiere un modelo específico de liderazgo, responsabilidades, procesos de control y

5. Almonacid Lamelas (2025).

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

mecanismos de participación, articulado dentro de una gobernanza global coherente.

Este enfoque sectorial permite a los entes locales adaptar sus estrategias digitales a la naturaleza concreta de cada organización, lo que favorece una toma de decisiones más eficiente, adecuada a la realidad local.

2.2.1. Gobernanza en administración electrónica

Desde la entrada en vigor de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPAC), y la LRJSP, las entidades locales han asumido la obligación de garantizar la tramitación electrónica de sus procedimientos. Esta transformación ha implicado crear órganos internos de dirección tecnológica, tales como comités de administración electrónica o juntas de digitalización local.

En este sentido, el Ayuntamiento de Gijón ha realizado una elección del modelo de gobernanza que pretende acelerar las sinergias que persiguen la instrucción institucional compartida y la propia participación ciudadana. Este modelo, que forma parte de la estrategia Gijón 2026[6], se basa en la idea de una gobernanza urbana multinivel que responde a la demanda de mayor participación en la gestión de la ciudanía.

El modelo de gobernanza se implementa a través de diferentes mecanismos, como la creación de comisiones de trabajo, la organización de consultas públicas, la puesta en marcha de plataformas de participación *online* y la colaboración con otras instituciones. El objetivo es crear un sistema más transparente, eficiente y participativo, que responda a las necesidades de los ciudadanos y contribuya al desarrollo sostenible de Gijón.

2.2.2. Gobernanza en protección de datos

El Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), imponen a todas las entidades públicas la obligación de designar un Delegado de Protección de Datos (DPD) con independencia funcional.

6. Plan estratégico de Gijón 2026: https://drupal.gijon.es/sites/default/files/2019-09/11%20GIJON_PEG2026_DocFinal.pdf.

En este contexto, son numerosas las entidades locales que han optado por modelos de gobernanza compartida, apoyándose en estructuras supramunicipales como diputaciones provinciales, mancomunidades, consorcios o entidades públicas regionales que asumen funciones de asesoramiento, auditoría y representación ante la Agencia Española de Protección de Datos (AEPD).

La Diputación de Lugo y la Diputación de Barcelona tienen activo un servicio centralizado de Delegado de Protección de Datos que da cobertura a las entidades locales de la provincia. Este modelo permite no solo cumplir con la normativa vigente, sino también establecer una red pública de colaboración en torno a la protección de datos, en la que se comparten recursos, conocimientos, herramientas tecnológicas y procedimientos armonizados. La Diputación, además, presta formación continua a los responsables municipales y facilita modelos de documentos, políticas y registros adaptados al entorno local.

Por su parte, órganos intermedios como la Diputación de Pontevedra ofrecen servicios integrales de asesoramiento en materia de protección de datos a todas las entidades locales de hasta 50 000 habitantes, sin asumir de forma directa el rol de delegado de protección de datos, que deberá ser nombrado internamente. El objetivo es aportar conocimiento interno a través del servicio, de modo que, en un futuro, estos delegados puedan "caminar solos" una vez finalizado el periodo de asesoramiento. Para ello, este servicio se vincula a un plan de formación específico para delegados que imparte directamente la Diputación de Pontevedra.

2.2.3. Gobernanza en reutilización de la información del sector público

La Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, obliga a las Administraciones, para garantizar la gobernabilidad del dato, a designar una unidad responsable de información para cada entidad que coordine la apertura y reutilización de los datos, y que se encargue de responder a las solicitudes y demandas ciudadanas.

Algunas entidades municipales han desarrollado portales de datos abiertos bajo esquemas de gobernanza con participación conjunta de la ciudadanía y del sector privado. El Ayuntamiento de Zaragoza ha sido pionero en establecer una Comisión de Datos Abiertos, con presencia de técnicos municipales y expertos externos, que orienta la estrategia de datos abiertos local.

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

Por su parte, la Federación Española de Municipios y Provincias (FEMP) aprobó en el último trimestre de 2023 dos ordenanzas tipo orientadas al fortalecimiento de políticas públicas en materia de transparencia institucional y gobernanza del dato. Estas herramientas normativas constituyen un paso significativo hacia la consolidación de modelos organizativos interoperables, que promueven no solo la eficiencia en los procesos administrativos, sino también el acceso abierto, la gestión ética y la reutilización efectiva de los datos generados por las entidades locales.

La ordenanza tipo de gobierno del dato[7] parte de la premisa de que los datos públicos deben ser concebidos como un activo colectivo al servicio del interés general, y no como recursos aislados o fragmentados. En ese sentido, el texto normativo articula un conjunto de principios, funciones y procedimientos jurídicos y técnicos destinados a garantizar la apertura, accesibilidad, calidad, trazabilidad y reutilización de los datos en el ámbito de la Administración local. Este enfoque busca mejorar la capacidad analítica de las entidades locales, facilitar la toma de decisiones fundamentadas, optimizar la prestación de servicios públicos y fomentar la innovación social.

Así, el marco propuesto por esta ordenanza dota a las Administraciones locales, con independencia de su tamaño o nivel de madurez digital, de una herramienta jurídica flexible y escalable, capaz de ser integrada en distintos modelos organizativos. Asimismo, representa un ejemplo de cómo la gobernanza sectorial, desde una perspectiva jurídica, puede facilitar la transformación digital en el ámbito municipal, asegurando la protección de derechos fundamentales, la transparencia, y el uso estratégico de la información pública al servicio del ciudadano.

2.2.4. Gobernanza en accesibilidad web

El Real Decreto 1112/2018, de 7 de septiembre, sobre accesibilidad de los sitios web y aplicaciones para dispositivos móviles del sector público, obliga a los sitios web y aplicaciones móviles del sector público a cumplir con los requisitos de accesibilidad universal. Para ello, el legislador obliga a las entidades locales a determinar una unidad responsable de garantizar el cumplimiento de los requisitos de accesibilidad de los sitios web y aplicaciones para dispositivos móviles dentro de su ámbito competencial.

7. http://femp.femp.es/files/3580-2414-fichero/ORDENANZA%20DEL%20DATO.pdf.

A modo de ejemplo, la Diputación de Pontevedra creó la Unidad Responsable de Accesibilidad[8], que es el órgano colegiado adscrito a la Secretaría General al que corresponde garantizar el cumplimiento de los requisitos de accesibilidad de los sitios web y aplicaciones para dispositivos móviles en la Diputación de Pontevedra.

En todos estos ámbitos, se observa una tendencia común: la necesidad de estructuras de gobernanza funcionales, multidisciplinares, sostenidas en el tiempo y capaces de integrar la dimensión normativa con la dimensión operativa. La coordinación interdepartamental y la colaboración interadministrativa se han consolidado como ejes vertebradores de una gobernanza pública digital eficaz.

2.2.5. Gobernanza de la inteligencia artificial en las Administraciones públicas

El avance de la inteligencia artificial (IA) en la gestión pública ha impulsado la necesidad de establecer modelos sólidos de gobernanza que garanticen el uso ético, seguro y eficaz de estas tecnologías. Así, la incorporación de sistemas de IA exige marcos institucionales claros, que delimiten responsabilidades, procesos de toma de decisiones, mecanismos de control y participación ciudadana, de forma que se asegure la alineación de estos desarrollos con los principios democráticos y el respeto de los derechos fundamentales.

Para ello, es fundamental la definición de estructuras organizativas internas, como oficinas técnicas o comités éticos. La Estrategia Nacional de Inteligencia Artificial (ENIA) contempla explícitamente la necesidad de introducir principios de gobernanza en el uso público de la IA.

Una de las piedras angulares de la gobernanza en IA es la transparencia algorítmica, es decir, la capacidad de conocer, explicar y supervisar cómo funcionan los algoritmos en procesos administrativos. A nivel local, el Ayuntamiento de Barcelona ha desarrollado una guía de algoritmos automatizados en servicios públicos[9], estableciendo criterios de transparencia, trazabilidad y participación ciudadana para su utilización.

8. https://boppo.depo.gal/web/boppo/detalle/-/boppo/2020/10/30/2020048771.
9. https://ajuntament.barcelona.cat/digital/sites/default/files/2023-11/Mesura-de-Govern-Intel-ligencia-artificial_cat-v2.47-ca-ES_.pdf.

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

2.3. Gobernanza en materia de ciberseguridad. Estructura funcional y roles definidos

La gobernanza de la ciberseguridad en el sector público implica definir políticas, asignar responsabilidades, garantizar recursos y controlar el cumplimiento. Las entidades deben aprobar una política de seguridad de la información, alineada con el Esquema Nacional de Seguridad; establecer órganos colegiados, como comités de seguridad; y designar responsables técnicos (de seguridad, de servicio, de sistemas y de protección de datos, entre otros). La LRJSP refuerza el principio de actuación coordinada, mientras que la NIS2 exige mecanismos de supervisión y rendición de cuentas efectivos.

Desde esta perspectiva ampliada, la gobernanza en materia de ciberseguridad en el ámbito local debe diseñarse como un modelo participativo, adaptable y orientado al bien común, que permita estructurar responsabilidades, garantizar la protección de los sistemas de información y fomentar la cooperación entre niveles institucionales. Solo mediante una gobernanza integral y efectiva será posible consolidar una cultura organizativa basada en la prevención de riesgos, la resiliencia tecnológica y la protección de derechos fundamentales en el entorno digital.

La implementación de un modelo organizativo efectivo es un requisito esencial para garantizar una gestión integral de la ciberseguridad en las entidades locales. Tal modelo debe estructurarse en torno a funciones claramente definidas, responsabilidades compartimentadas y niveles jerárquicos específicos, de manera que se facilite la ejecución, el seguimiento y la mejora continua de las políticas de seguridad.

Un modelo organizativo robusto requiere identificar y asignar tareas clave dentro de la estructura de la entidad local. Al menos, deben existir funciones diferenciadas para:

- Gestión de riesgos de ciberseguridad, encargada de realizar análisis periódicos de amenazas y vulnerabilidades, así como de proponer y validar controles técnicos y organizativos apropiados.

- Gestión de incidentes, responsable de la detección, notificación, investigación, respuesta y documentación de los eventos de seguridad que puedan afectar a la funcionalidad municipal.

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

- Arquitectura y diseño de seguridad, cuyo cometido es garantizar que las infraestructuras, aplicaciones y procesos incorporen mecanismos de protección adecuados desde el diseño.

- Educación y concienciación, encargada de fomentar una cultura de seguridad dentro de las entidades locales, con formación adaptada a cada perfil profesional y simulacros orientados a detectar y preparar a los equipos frente a amenazas reales.

La definición precisa de roles y niveles de autoridad, alineada con las exigencias del Esquema Nacional de Seguridad, garantiza la trazabilidad de las decisiones y la rendición de cuentas. Es recomendable que estos perfiles —como el Responsable de Seguridad, el Responsable de Información y los equipos técnicos— estén institucionalizados a través de puestos consolidables y no meramente circunstanciales.

Pero no podemos olvidar que muchas entidades locales, especialmente las de menor tamaño, carecen de equipos propios de ciberseguridad o de personal experto. Ante ello, modelos colaborativos e interadministrativos se presentan como la alternativa más viable y eficiente. Un ejemplo consolidado es el rol de las diputaciones provinciales o los cabildos insulares, que ya están actuando como nodos de gobernanza compartida, o la constitución de redes de respuesta a incidentes coordinadas con el CCN-CERT.

En lugar de que cada entidad local desarrolle de forma independiente su propia estrategia, se pueden crear marcos comunes o modelos de gobernanza escalables, que permitan aplicar criterios mínimos homogéneos pero adaptables a la realidad de cada institución. Así, el desarrollo de ordenanzas tipo, guías de referencia o servicios comunes de ciberseguridad ofrecidos por organismos supramunicipales puede facilitar que incluso los ayuntamientos con menor capacidad técnica puedan contar con una estructura funcional y roles definidos adaptados a su realidad y recursos.

2.4. Principios sostenibles de gobernanza de la ciberseguridad

Los principios rectores de la gobernanza de la ciberseguridad son indispensables para orientar la actuación de los órganos de gobierno municipal. Entre los más destacados se encuentran:

- Claridad en roles y responsabilidades. Cada miembro de la organización debe conocer sus competencias y límites. La alta dirección

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

tiene la obligación de integrar la seguridad como un asunto habitual en los órganos de decisión —un elemento fundamental para crear resiliencia digital institucional—.

- Estrategia de seguridad continua. Debe existir un marco estratégico claro, revisado de forma periódica, con inventario de activos, clasificación según criticidad, evaluación de riesgos y definición de controles. Este marco debe adaptarse a las exigencias legales y a las amenazas emergentes, como los sistemas de inteligencia artificial.

- Escalabilidad y adecuación al contexto. Los modelos propuestos deberán ser escalables, permitiendo aplicar criterios mínimos homogéneos, pero adaptables a la realidad de cada institución.

- Integración de la ciberseguridad en la gestión de riesgos global. El riesgo cibernético debe ser tratado como un riesgo operativo prioritario, y gestionarse con los mismos estándares que el resto de riesgos institucionales. La gestión no puede limitarse a cumplir exigencias legales, sino que debe incluir evaluaciones periódicas, auditorías internas y autonomía para verificar el cumplimiento de proveedores y servicios externos.

- Cultura de ciberresiliencia. Es imprescindible desarrollar programas periódicos de formación y concienciación —incluyendo *phishing* simulado, ejercicios de *pentesting*[10] y simulacros de respuesta a incidentes— que lleguen a todos los niveles jerárquicos. Para ello, se debe garantizar un entorno donde la comunicación fluida y la denuncia de incidentes no acarreen perjuicios al informante

- Estrategias claras de comunicación interna y externa, especialmente ante incidentes de seguridad. En el plano interno, las entidades deben contar con un plan de comunicación que defina canales jerárquicos de información, responsables de activación, niveles de alerta y mecanismos de coordinación entre unidades técnicas, jurídicas, de comunicación institucional y responsables políticos.

Estos principios tienen como objetivo crear un modelo de gobernanza como elemento de resiliencia local que no solo dé respuesta ante incidentes, sino que también ofrezca una estructura real como herramienta

10. El *pentesting*, también conocido como prueba de penetración, consiste en la simulación de un ataque a un sistema *software* o *hardware* con el objetivo de encontrar vulnerabilidades para prevenir ataques externos.

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

jurídica y técnica que fortalezca la articulación institucional y la confianza democrática a escala local.

3. Modelos de roles y responsabilidades en materia de ciberseguridad

La entrada en vigor del Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad, ha reforzado la arquitectura organizativa que las entidades del sector público deben adoptar en materia de seguridad de la información y ciberseguridad. Esta normativa establece no solo principios y medidas técnicas, sino también un modelo estructurado de roles y responsabilidades, que debe integrarse en la gobernanza interna de cada organismo.

La adecuada delimitación de los roles y responsabilidades en materia de ciberseguridad constituye uno de los pilares fundamentales de la gobernanza digital en el sector público. En un entorno institucional cada vez más digitalizado y expuesto a riesgos tecnológicos, resulta imprescindible que las organizaciones públicas dispongan de una arquitectura organizativa clara, documentada y funcional, que permita articular de forma efectiva la protección de la información, la prevención de incidentes y la respuesta ante amenazas.

El Esquema Nacional de Seguridad, hoja de ruta en ciberseguridad, sienta las bases para la asignación formal de funciones específicas en relación con la seguridad de los sistemas de información. Esta normativa introduce una clasificación de perfiles organizativos (responsables de la información, del servicio, del sistema, de la seguridad, entre otros), con el fin de garantizar que cada actor institucional conozca sus competencias, responsabilidades y ámbitos de actuación dentro del ciclo de vida de la seguridad de la información.

La implementación de estos roles no solo responde a una exigencia legal, sino que también permite mejorar la trazabilidad de las decisiones, reforzar los mecanismos de control interno, facilitar auditorías y promover una cultura de ciberseguridad transversal. El alcance de estas funciones debe variar en función del tamaño y complejidad de cada entidad, por lo que el Esquema Nacional de Seguridad admite enfoques escalables y adaptados, especialmente relevantes en el caso de las entidades locales con recursos limitados.

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

3.1. Marco general del Esquema Nacional de Seguridad (ENS) y gobernanza

El ENS define la necesidad de que todas las entidades públicas —incluyendo ayuntamientos, diputaciones, organismos autónomos y empresas públicas— dispongan de una estructura organizativa clara para asegurar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información tratada. Esto exige identificar roles clave que asuman funciones específicas en el diseño, implantación, supervisión y mejora continua de las políticas de ciberseguridad.

La gobernanza de la ciberseguridad en este marco se basa en la asignación de responsabilidades de forma formal y documentada, y en la existencia de una comisión o un grupo de seguridad que garantice la coordinación entre todos los actores implicados.

3.1.1. Principales roles definidos por el ENS

El Real Decreto 311/2022 y las guías CCN-STIC[11] recogen los principales roles y perfiles funcionales que deben existir en cualquier entidad sujeta al ENS:

- *Responsable de la Información (RI)*

  Es la persona designada por la entidad titular de la información, encargada de definir los requisitos de seguridad sobre dicha información. Tiene autoridad sobre los datos y su clasificación, y debe coordinarse con los responsables de los servicios y la seguridad.

- *Responsable del Servicio (RS)*

  Este rol tiene la responsabilidad sobre el servicio prestado (p. ej., una sede electrónica, la plataforma de contratos, o una aplicación de gestión tributaria). Su función es garantizar que el servicio funcione correctamente, cumpliendo los requisitos de seguridad establecidos por el Responsable de la Información y en coordinación con el Responsable de Seguridad.

11. Guía CCN-STIC 801: "Esquema Nacional de Seguridad - Responsabilidades y Funciones", publicada por el Centro Criptológico Nacional (junio 2025): https://www.ccn-cert.cni.es/es/800-guia-esquema-nacional-de-seguridad/501-ccn-stic-801-responsibilidades-y-funciones-en-el-ens/file.html. La guía tiene por objeto establecer un marco de referencia organizativo para definir los roles y responsabilidades en la gestión de la seguridad de los sistemas de información, conforme al Esquema Nacional de Seguridad (ENS). Cada entidad debe adaptar este marco a su estructura, dimensión y recursos, documentándolo en su Política de Seguridad de la Información.

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

- *Responsable de la Seguridad (RSeg)*

  Encargado de promover y supervisar las medidas de seguridad aplicables a los sistemas de información. Es el rol clave para la ciberseguridad operativa, y debe coordinar el análisis de riesgos, el cumplimiento del ENS y la respuesta ante incidentes. Este perfil puede coincidir con el Responsable de Seguridad de la Información (CISO).

- *Responsable del Sistema (RSI)*

  Gestor técnico de los sistemas de información. Es responsable de aplicar y mantener las medidas técnicas de seguridad, coordinar la configuración de infraestructuras, sistemas y redes, y facilitar auditorías o revisiones técnicas. Colabora estrechamente con el Responsable de Seguridad.

- *Administrador del Sistema y de la Seguridad*

  Aunque no es un rol formal con responsabilidad estratégica, es una figura operativa relevante, encargada de las tareas técnicas del día a día: configuración, mantenimiento, monitoreo, y gestión de vulnerabilidades.

- *Comité de Seguridad o Comisión de Seguridad de la Información*

  Órgano colegiado recomendado para la coordinación estratégica y supervisión de las funciones de ciberseguridad. Su composición debe incluir a los responsables anteriores y representantes de los órganos directivos.

- *Delegado de Protección de Datos*

  El Delegado de Protección de Datos (DPD), figura contemplada en el RGPD y en la LOPDGDD, desempeña una función clave en la gobernanza de la ciberseguridad en las Administraciones públicas. Aunque su misión principal es velar por el cumplimiento de la normativa de protección de datos personales, su papel se encuentra intrínsecamente relacionado con la seguridad de la información, especialmente en contextos institucionales donde el tratamiento de datos personales se apoya en sistemas informáticos sujetos a riesgos de seguridad.

  El DPD debe formar parte del ecosistema organizativo de seguridad, participando en los comités de seguridad de la información y colaborando con los responsables de seguridad (RSeg), de la

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

información (RI) y del sistema (RSI). Su independencia funcional debe ser garantizada, y no debe recaer sobre personas que participen directamente en la operación o supervisión de los sistemas, para evitar conflictos de intereses.

3.1.2. Asignación formal y trazabilidad

El ENS exige que todos estos roles estén formalmente designados y documentados, generalmente a través de resoluciones internas o instrucciones del órgano de gobierno. Además, debe asegurarse la trazabilidad de las decisiones, especialmente en relación con la evaluación de riesgos, auditorías, planes de continuidad y la respuesta ante incidentes.

Dicha estructura debe plasmarse formalmente en la Política de Seguridad de la entidad, debiendo mantenerse debidamente documentada y actualizada.

El modelo propuesto por el ENS es jerárquico, pero promueve la colaboración transversal. Cada responsable debe asumir competencias claras y establecer mecanismos de comunicación con los demás actores implicados. Además, deben preverse medidas de continuidad operativa y protocolos de notificación de incidentes.

3.2. Modelo de gobernanza adaptado a las entidades locales (EE. LL.)

La designación de los distintos roles y responsabilidades implica la configuración de una arquitectura organizativa específica para la gestión de la ciberseguridad en todas las entidades del sector público. No obstante, en el ámbito de las entidades con menor capacidad económica o de gestión, dicha implementación exige una adaptación que, muchas veces, resulta irreal por la falta de recursos técnicos o económicos.

Por ello, el ENS permite cierta adaptabilidad en los modelos de gobernanza con el objetivo de permitir una adaptación que tenga en cuenta la heterogeneidad de capacidades institucionales, técnicas y económicas existentes en cada organización.

En el caso de las EE. LL., especialmente las de menor tamaño, la implementación plena de todos estos roles puede no ser viable por limitaciones de personal. En estos casos, el ENS admite la posibilidad de compartir roles entre varias entidades o de recurrir al apoyo de estructuras supramunicipales, como las diputaciones provinciales, los cabildos o los consorcios TIC.

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

En este contexto, la Guía CCN-STIC 890, sobre la adecuación al ENS conforme a los requisitos esenciales de seguridad según μCeENS[12], establece un enfoque de cumplimiento modular, que permite aplicar el principio de proporcionalidad y escalabilidad en función de las características de cada entidad. El objetivo debe ser el cumplimiento normativo sin generar cargas desproporcionadas en aquellas EE. LL. que no dispongan de medios suficientes para estructurar una organización compleja.

La aplicación del ENS en las EE. LL. representa un reto jurídico y organizativo que exige un enfoque progresivo y adaptado a las características propias de estas Administraciones. A diferencia de los organismos de la Administración General del Estado o las comunidades autónomas, las EE. LL. presentan una notable diversidad en cuanto a estructura, medios y competencias, lo que hace imprescindible segmentar su adaptación al ENS por niveles o bloques. Este enfoque permite garantizar el cumplimiento normativo sin generar cargas desproporcionadas en aquellas entidades con menor capacidad técnica o presupuestaria.

El nuevo marco jurídico de ciberseguridad reconoce la posibilidad de una implementación proporcional y basada en la categoría de los sistemas de información, lo que ofrece una base legal para modular las obligaciones de seguridad conforme al principio de responsabilidad activa. Así, las EE. LL. pueden y deben configurar su modelo de cumplimiento conforme a su exposición al riesgo, la criticidad de los servicios electrónicos que prestan y su capacidad institucional para desplegar roles clave como el Responsable de Seguridad, el Responsable del Sistema o el Responsable de la Información.

La adaptación por bloques implica, por tanto, una diferenciación funcional que puede tomar como referencia criterios como la población, el presupuesto, la existencia de servicios públicos digitales críticos o el grado de madurez digital de la entidad. Esta metodología permite facilitar la adopción escalonada de medidas técnicas, organizativas y documentales en materia de ciberseguridad.

12. μCeENS es una metodología innovadora que aprovecha las novedades introducidas por el Real Decreto 311/2022, de 3 de mayo, para facilitar la obtención de la certificación de conformidad con el ENS, basada en un Perfil de Cumplimiento Específico (PCE). Esta metodología proporciona el acompañamiento y la asistencia necesarios para alcanzar dicha certificación, desde la fase previa a la adecuación hasta el seguimiento posterior a su obtención, todo ello automatizado a través de las herramientas de Gobernanza de la Ciberseguridad (INES-AMPARO). Vid. https://ens.ccn.cni.es/es/conformidad/microceens.

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

A continuación, se presenta una propuesta de clasificación en tres grupos de EE. LL., diferenciados según su tamaño, como base para una adaptación progresiva al ENS en el ámbito local. Esta categorización puede servir como referencia orientativa para que cada entidad local aborde su adecuación al ENS de forma proporcional y realista.

Distribución de grupos de adecuación

- **Grupo 1: Grandes municipios y diputaciones**

En este grupo se incluyen las EE. LL. con una capacidad institucional consolidada, normalmente con poblaciones superiores a 50 000 habitantes o con competencias supramunicipales, como es el caso de diputaciones, cabildos y consejos insulares. Desde el punto de vista jurídico-administrativo, estas entidades tienen capacidad plena para cumplir con la totalidad de las obligaciones impuestas por el ENS.

En estos casos, el principio de responsabilidad proactiva adquiere toda su intensidad, siendo exigible la implantación integral de los roles y procedimientos previstos en el ENS y en las guías del CCN-CERT, en particular la Guía CCN-STIC 801.

Modelo propuesto:

- La designación formal del Responsable de la Seguridad (RSeg), con competencias propias, nivel técnico-jurídico avanzado y autonomía funcional, asimilable a la figura del CISO recogida en el estándar ISO 27001.

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

- La designación diferenciada de un Responsable del Servicio (RS), con competencias propias, nivel técnico-jurídico avanzado y autonomía funcional.

- La existencia de un Responsable del Sistema de Información (RSI) con personal TIC a su cargo y con autoridad técnica suficiente para coordinar la implementación de medidas.

- La constitución de un Comité de Seguridad de la Información con carácter permanente, multidisciplinar, y con capacidad decisoria para proponer al órgano competente la aprobación de las medidas de seguridad acordadas.

- La integración del Delegado de Protección de Datos (DPD) en la estructura organizativa, con independencia funcional conforme al artículo 37 del RGPD y al artículo 34 de la LOPDGDD.

Desde el punto de vista organizativo, estas entidades pueden desarrollar políticas de seguridad completas, llevar a cabo auditorías internas y externas anuales y ejecutar planes de formación, concienciación y respuesta a incidentes de forma autónoma.

- **Grupo 2: Municipios medianos (10 000 - 50 000 habitantes)**

En este grupo se encuentran municipios con recursos limitados, pero con un cierto grado de madurez organizativa. Aunque no siempre cuentan con una estructura TIC completa, sí pueden asumir roles clave, combinando funciones o externalizando servicios.

Desde el punto de vista jurídico, es esencial que los acuerdos de cooperación, convenios o contratos administrativos de asistencia técnica especifiquen claramente las funciones asumidas por terceros, en cumplimiento de los principios de licitud, necesidad y proporcionalidad. Además, estos municipios pueden formar parte de consorcios intermunicipales o adherirse a servicios provinciales que les permitan cumplir con las exigencias normativas del ENS.

Para este grupo se propone un modelo de gobernanza por bloques de responsabilidad. El objetivo es que cada organismo, entidad u organización la adapte en función de su naturaleza y capacidad, designando los roles y constituyendo el Comité de Seguridad.

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

Modelo de gobernanza por bloques de responsabilidad:

- Bloque de Gobierno: Responsable de Gobierno, cuyas funciones podrán ser ejercidas por la Alcaldía, la Presidencia, la Gerencia (u órgano similar) de la organización, y que integra los siguientes roles y funciones del ENS:

  • Responsable de la Información (RI)

  • Responsable del Servicio (RS)

- Bloque de Supervisión: Responsable de Supervisión, cuyas funciones podrán ser ejercidas por la Secretaría General de la Organización (u órgano similar), y que integra el siguiente rol del ENS:

  • Responsable de la Seguridad (RSeg)

  En este bloque de supervisión se considerará también la figura del Delegado de Protección de Datos, apoyando al Responsable de Supervisión, con funciones de asesoramiento y supervisión en materia de protección de datos.

- Bloque de Operación: Responsable de Operación, cuyas competencias podrán ser ejercidas por un empleado de la organización con perfil TIC, y que integra el siguiente rol del ENS:

  • Responsable del Sistema (RSI)

- Comité de Seguridad: Órgano diferenciado en el que se integrarán las personas que desempeñen los roles de seguridad previstos en el modelo.

■ **Grupo 3: Municipios pequeños (< 10 000 habitantes)**

Este grupo comprende la mayoría de los municipios españoles, caracterizados por su baja densidad poblacional, estructura administrativa reducida y limitada capacidad tecnológica. El objetivo de este bloque es habilitar a este tipo de organizaciones una implantación gradual, mínima y razonable, guiada por el principio de proporcionalidad y eficiencia en el uso de recursos públicos.

La gobernanza en este grupo se basa en modelos simplificados, funcionales y escalables.

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

Modelo de gobernanza simplificado por bloques de responsabilidad:

- Bloque de Gobierno: Responsable de Gobierno, cuyas funciones podrán ser ejercidas por la Alcaldía, la Presidencia, la Gerencia (u órgano similar) de la organización, y que integra los siguientes roles y funciones del ENS:

  - Responsable de la Información (RI)
  - Responsable del Servicio (RS)
  - Comité de Seguridad

- Bloque de Supervisión: Responsable de Supervisión, cuyas funciones podrán ser ejercidas por la Secretaría General de la Organización (u órgano similar), y que integra el siguiente rol del ENS:

  - Responsable de la Seguridad (RSeg)

  En este bloque de supervisión se considerará también la figura del Delegado de Protección de Datos, apoyando al Responsable de Supervisión, con funciones de asesoramiento y supervisión en materia de protección de datos.

- Bloque de Operación: Responsable de Operación, cuyas competencias podrán ser ejercidas por un empleado de la organización o mediante externalización o delegación del RSI en entes supramunicipales —como diputaciones, mancomunidades o empresas TIC—, previa formalización de convenios o contratos de asistencia técnica, y que integra el siguiente rol ENS:

  - Responsable del Sistema (RSI)

Seguidamente, se presenta una tabla comparativa que resume las principales diferencias y ofrece una visión clara del grado de autonomía, especialización y complejidad de cada rol o mecanismo de gobernanza en función del grupo al que pertenece la entidad local.

Esta aproximación segmentada no solo mejora la viabilidad del cumplimiento normativo, sino que también facilita la implantación de medidas de seguridad ajustadas a la realidad de cada tipo de entidad, garantizando así una protección adecuada y sostenible de la información pública.

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

Rol ENS	Grandes municipios y diputaciones	Municipios medianos (10 000-50 000 hab.)	Municipios pequeños (<10 000 hab.)
Responsable de la Información (RI)	Asignado internamente, especializado	Asignado internamente, con formación específica	Cargo compartido (p. ej. secretario municipal)
Responsable del Servicio (RS)	Diferenciado por unidad o área	Compatible con otros roles	Unificado con RI o RSeg
Responsable del Sistema (RSI)	Técnico interno especializado	Mixto: interno o externo según servicio TIC	Externo o delegado en diputación/consorcio
Responsable de la Seguridad (RSeg)	Independiente, con funciones tipo CISO	Asumido junto a RSI, si no hay conflicto	Consolidado con RS o externo (mínimo)
Administrador de Seguridad (AS)	Perfil técnico propio	Técnico compartido o de servicio externo	Integrado en soporte TIC supramunicipal
Delegado de Protección de Datos (DPD)	Interno, con autonomía funcional	Compartido con diputación o consorcio	Compartido por convenio
Comité de Seguridad de la Información	Permanente y multidisciplinar	Comité mixto o reuniones técnicas periódicas	Integrado en el Bloque de Gobierno, coordinación simplificada
Política formal de seguridad	Completa, aprobada por órgano competente	Parcial, con anexos y medidas comunes	Modelo básico adaptado (vía uCeENS)
Auditorías y análisis de riesgos	Internos y externos anuales	Con apoyo supramunicipal o contratados puntuales	Coordinados por diputación u organismo TIC

Tabla comparativa de roles por grupos de entidades

3.3. La función de los cargos electos y habilitados nacionales

Como hemos visto en el modelo de gobernanza propuesto, con independencia del grupo de entidad local objeto de adecuación al ENS, se exige un compromiso activo tanto por parte de los órganos políticos (alcaldes/presidentes, concejales/diputados) como de los órganos de apoyo técnico-administrativo (secretarios e interventores). El *Prontuario de ciberseguridad para entidades locales*, elaborado por el CCN-CERT y la FEMP[13], refuerza este planteamiento, señalando la responsabilidad directa de los alcaldes y concejales en la gobernanza de la seguridad, la adecuada asignación de recursos y la supervisión del cumplimiento del ENS.

En efecto, el documento dedica un apartado específico a las funciones y responsabilidades del alcalde y del resto de responsables de la corporación municipal, subrayando que los órganos de dirección política deben garantizar un sistema de control interno eficaz que responda a las cinco

13. Centro Criptográfico Nacional y Federación Española de Municipios y Provincias (2022).

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

dimensiones del ENS: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.

Este enfoque integral sitúa a los alcaldes en un papel de liderazgo estratégico, debiendo impulsar políticas, aprobar marcos normativos internos y velar por el cumplimiento efectivo del ENS en su entidad.

3.3.1. Alcaldes/presidentes y la Junta de Gobierno Local

En el marco de la Administración local, los alcaldes/presidentes y la Junta de Gobierno representan el máximo órgano responsable de velar por la existencia de controles adecuados en la protección de la información y de los sistemas de comunicación. Esta responsabilidad última no es meramente formal, sino que constituye un pilar esencial para garantizar la seguridad de los datos y el correcto funcionamiento de los servicios públicos en la era digital.

El rol de los poderes ejecutivos locales en esta materia se concreta en diversas funciones clave. En primer lugar, corresponde al alcalde/presidente y a la Junta de Gobierno la definición y aprobación de la política de seguridad, que debe estar plenamente alineada con los principios recogidos en el ENS y con el conjunto del marco normativo vigente. Esta política no solo debe responder a las exigencias legales, sino también reflejar el compromiso de la Administración local con la protección de los derechos de la ciudadanía y con la integridad de los servicios públicos.

Asimismo, la asignación de los recursos humanos, materiales y financieros necesarios para desplegar las medidas de seguridad es un cometido irrenunciable de los órganos de gobierno. Sin un respaldo presupuestario adecuado y sin un equipo humano con las competencias requeridas, cualquier intento de implantación de los controles del ENS quedaría reducido a un mero formalismo sin eficacia real.

La supervisión de la gobernanza de la ciberseguridad constituye otro eje esencial de esta responsabilidad política. Los alcaldes/presidentes y la Junta de Gobierno deben impulsar la creación y consolidación de órganos específicos, como el Comité de Seguridad de la Información en su caso, que actúen como mecanismos de coordinación y seguimiento de las políticas y medidas adoptadas. Estos órganos permiten articular de manera efectiva la participación de los distintos perfiles técnicos y jurídicos necesarios para un cumplimiento integral del ENS.

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

Por último, no puede olvidarse la obligación de rendición de cuentas y de transparencia política que recae sobre los poderes ejecutivos locales. Garantizar que en la Administración local se implementen, revisen y mantengan los controles previstos en el ENS no es solo un imperativo legal, sino también un requisito para la generación de confianza en la ciudadanía y para la legitimidad de la actuación pública en el entorno digital.

Si bien es cierto que los alcaldes y los órganos ejecutivos locales no desempeñan directamente las tareas operativas vinculadas a la ciberseguridad, su implicación activa y su respaldo político son factores determinantes para que las medidas técnicas que se adopten sean sostenibles y eficaces, y perduren en el tiempo. La solidez de las políticas de seguridad de la información de una entidad local depende, en última instancia, del compromiso de sus máximos responsables políticos, de su capacidad para dotar de estructura y recursos al sistema, y de su voluntad de liderar la transformación hacia una Administración más segura y resiliente.

3.3.2. Secretarios e interventores

En el marco de la Administración local, los secretarios e interventores, en su condición de habilitados nacionales, desempeñan un papel insustituible en la correcta implantación y aplicación del ENS. Su función, de naturaleza doblemente institucional, combina el asesoramiento jurídico y técnico con la necesaria coordinación interna, constituyéndose como garantes de que las políticas de seguridad no solo se diseñen y aprueben, sino que se ejecuten conforme al marco normativo vigente.

Por un lado, los secretarios ejercen una función esencial de asesoramiento jurídico y técnico. A través de sus informes y valoraciones, verifican que las políticas, los procedimientos y los contratos vinculados a la seguridad de la información se ajusten a lo establecido en el ENS y en el marco legal aplicable. Los secretarios, por tanto, aportan la seguridad jurídica indispensable para que cualquier medida en materia de ciberseguridad cumpla con los principios de legalidad, eficacia y eficiencia.

Por otro lado, los habilitados nacionales ejercen un papel crucial en la coordinación interna de la Administración. En este ámbito, actúan como el nexo natural y necesario entre los órganos políticos —la Alcaldía/Presidencia, la Junta de Gobierno local— y los responsables operativos del ENS —responsables de los sistemas, de la seguridad y de la protección de datos, entre otros—. Gracias a su posición, los secretarios aseguran que las decisiones políticas en materia de seguridad se traduzcan en acciones tan-

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

gibles, en aprobaciones regladas y en documentación administrativa que garantice la formalización y trazabilidad de las medidas adoptadas. Esta función de enlace sistemático es fundamental para evitar la dispersión de responsabilidades y para lograr que la estrategia de seguridad se articule de manera coherente en la entidad local.

La condición de habilitados nacionales otorga a los secretarios e interventores un perfil singular, que los convierte en piezas clave del sistema de control interno necesario para satisfacer las exigencias del ENS. No basta con que las políticas de seguridad se enuncien o se proyecten; es imprescindible que se formalicen mediante los actos administrativos correspondientes, que se inserten en el circuito jurídico-administrativo y que se documenten de manera adecuada para permitir la trazabilidad, la auditoría y la rendición de cuentas. Los secretarios garantizan que estas políticas se configuren como instrumentos jurídicos válidos y eficaces, dotados de la seguridad formal que exige cualquier actuación en el ámbito de la Administración pública.

En el caso de las EE. LL. de menor tamaño o con recursos limitados, el secretario, en su condición de habilitado nacional, no solo asume estas funciones de asesoramiento y coordinación, sino que, en muchos casos, debe integrar en su ámbito de actuación los roles de seguridad definidos en el ENS. Así, el secretario puede actuar directamente como responsable de seguridad o incluso asumir tareas vinculadas a la gestión de los sistemas de información, dada la imposibilidad de contar con personal específico para cada perfil técnico. Esta concentración de funciones refuerza la importancia de su figura en estos entornos, donde resulta indispensable para que la aplicación del ENS sea posible y eficaz.

Por ello, el ENS no podría desplegar todos sus efectos en el ámbito local sin la participación activa y comprometida de los secretarios e interventores. Su intervención asegura que el sistema de seguridad de la información de la entidad local no solo responda a los estándares técnicos requeridos, sino que también quede plenamente integrado en el marco normativo y en el sistema de control interno, con el rigor jurídico-administrativo que caracteriza a una gestión pública responsable y transparente.

4. Cooperación y coordinación entre distintas áreas y Administraciones

Como ha quedado ya ampliamente establecido en este artículo, las Administraciones municipales, en especial las de menor tamaño, se enfrentan a dificultades específicas vinculadas a la escasez de recursos técnicos y

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

humanos para hacer frente a dichos riesgos. En este contexto, la cooperación y coordinación entre distintas áreas internas y entre Administraciones públicas constituye un principio fundamental para articular una respuesta eficaz y garantizar el cumplimiento del ENS.

4.1. Cooperación interna: una estrategia de gestión integrada

En el ámbito interno, la ciberseguridad de una entidad local no puede ser entendida como una tarea exclusiva de los departamentos de informática o de los responsables de los sistemas de información. Por el contrario, es necesario un enfoque transversal, en el que participen activamente todas las áreas de la organización. Desde los responsables políticos —Alcaldía/Presidencia y Junta de Gobierno— hasta los servicios jurídicos, económicos y de recursos humanos, cada unidad tiene un papel en la identificación de riesgos, en la implantación de controles y en la gestión de incidentes.

Esta cooperación se materializa en la creación de órganos internos como el Comité de Seguridad de la Información, en el que se integran representantes de las distintas áreas, y que actúa como foro de coordinación para aprobar políticas, supervisar medidas y establecer los procedimientos necesarios para cumplir con el ENS. La implicación de todas las áreas refuerza la cultura de la seguridad y evita la fragmentación de responsabilidades, uno de los principales riesgos para la eficacia de cualquier política de ciberseguridad.

4.2. Coordinación interadministrativa: el papel de la colaboración institucional

Más allá de los esfuerzos que cada entidad local pueda realizar en el ámbito de la seguridad de la información, resulta evidente que la coordinación entre Administraciones públicas se ha convertido en un requisito imprescindible para garantizar una gestión eficaz y sostenible de la ciberseguridad en el sector público. La complejidad creciente de las amenazas digitales, unida a la escasez de recursos técnicos y económicos que caracteriza a gran parte de los ayuntamientos —especialmente los de menor tamaño—, obliga a estructurar modelos colaborativos que permitan optimizar los recursos disponibles y dar una respuesta coherente y coordinada frente a los desafíos comunes.

La normativa vigente, y en particular el ENS, reconoce de forma expresa la necesidad de que las EE. LL. articulen mecanismos de cooperación

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

interadministrativa y de apoyo mutuo para cumplir con sus obligaciones. El artículo 156 de la LRJSP refuerza este principio, al establecer que las Administraciones deben actuar de forma coordinada, prestarse asistencia mutua y facilitarse la información necesaria para el ejercicio de sus competencias.

En este marco, las diputaciones provinciales, los cabildos y los consejos insulares desempeñan un papel esencial como estructuras de soporte para los ayuntamientos, especialmente aquellos que carecen de capacidad técnica propia. Por ejemplo, la Diputación de Barcelona ofrece desde hace años un servicio de soporte en materia de ciberseguridad, que incluye la elaboración de políticas de seguridad, asesoramiento jurídico-técnico y la realización de auditorías de cumplimiento del ENS.

El soporte no se limita al nivel provincial. Las EE. LL. encuentran un aliado fundamental en organismos estatales como el Centro Criptológico Nacional (CCN-CERT), cuya misión, conforme al Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional, es garantizar la seguridad de los sistemas, redes y tecnologías de la información en el ámbito de la Administración. El CCN-CERT proporciona a las Administraciones locales servicios de asesoramiento en la implantación del ENS, formación especializada (a través de iniciativas como el Plan de Capacitación Nacional en Ciberseguridad) y soporte técnico frente a incidentes de seguridad. Un ejemplo concreto es el servicio de alerta temprana y análisis de amenazas que el CCN-CERT pone a disposición de los ayuntamientos adheridos, facilitando así una capacidad de detección y respuesta que sería inasumible de forma individual para muchos municipios.

Esta coordinación interadministrativa no solo permite compartir recursos y abaratar costes, sino que también facilita la homogeneización de procedimientos, la aplicación de estándares comunes y el intercambio de buenas prácticas, aspectos que son expresamente recomendados por el ENS y que resultan imprescindibles para alcanzar un nivel de protección uniforme y eficaz en todo el territorio. El desarrollo de ordenanzas tipo por parte de la FEMP o la elaboración de guías prácticas, como la Guía de adecuación al ENS para entidades locales de menos de 2000 habitantes (Federación Española de Municipios y Provincias, 2018b), son ejemplos de cómo la acción conjunta permite a las corporaciones locales avanzar de manera ordenada y coherente en la implantación de sus sistemas de seguridad.

En definitiva, la acción colaborativa es el único camino viable para garantizar que la ciberseguridad en el ámbito local no se convierta en un objetivo inalcanzable para las entidades con menos recursos. La construcción

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

de redes de apoyo mutuo, la formalización de convenios de colaboración y la integración en servicios mancomunados deben entenderse no como una opción, sino como un elemento estructural del sistema de gobernanza de la seguridad pública en el entorno digital. Solo mediante este modelo de cooperación y coordinación será posible garantizar el cumplimiento efectivo del ENS y consolidar una cultura de seguridad que refuerce la confianza de la ciudadanía en las Administraciones públicas.

5. Conclusiones

La obligación de implantar un modelo de gobernanza de la ciberseguridad en las EE. LL., conforme a los estándares del ENS, es hoy un mandato jurídico que deriva no solo del marco normativo español y europeo, sino también de la necesidad esencial de proteger los derechos fundamentales de la ciudadanía en el entorno digital.

Así, es responsabilidad de los órganos superiores de las EE. LL. y de los titulares de los puestos de secretaría, intervención y tesorería que existan controles acomodados en los sistemas de información y comunicaciones. Su implicación y compromiso son fundamentales para implantar con éxito un sistema de gestión de la seguridad de la información que garantice la ciberresiliencia en cada entidad.

Sin embargo, esta exigencia choca con una realidad organizativa compleja: la mayoría de las corporaciones locales, especialmente los municipios pequeños y medianos, se enfrentan a serias limitaciones de recursos que dificultan la materialización de dichos modelos en los términos previstos por la normativa.

Los nuevos requerimientos en materia de seguridad de la información han generado una sobrecarga añadida en estructuras ya tensionadas por sus competencias ordinarias y por la escasez de personal cualificado en ciberseguridad. En muchos casos, la falta de medios impide la designación efectiva de responsables diferenciados para cada función del ENS, forzando la acumulación de responsabilidades en un reducido número de personas o incluso en un solo funcionario. Esta situación no solo afecta al cumplimiento formal de las obligaciones, sino que pone en riesgo la eficacia real de las medidas de protección adoptadas, dado que los roles quedan a menudo diluidos o sin el respaldo organizativo necesario para su ejercicio independiente y profesionalizado.

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

Ante este escenario, resulta imprescindible que las EE. LL. definan un modelo de gobernanza de la ciberseguridad que sea operativo, proporcionado y sostenible, que adapte las exigencias del ENS a la capacidad real de cada organización. Este modelo debe incorporar medidas que, sin sacrificar los principios del marco legal, permitan cumplir con las obligaciones de seguridad mediante estructuras más eficientes. Esto podría incluir la consolidación de funciones bajo una sola autoridad cuando sea pertinente, el establecimiento de convenios de colaboración con entidades supramunicipales, y la utilización de plataformas y marcos de cumplimiento simplificado que faciliten el cumplimiento normativo, especialmente en los sistemas de información de categoría básica.

Es por ello que, a mi modo de ver, la gobernanza debe trascender el plano teórico para consolidarse como un instrumento operativo de control interno, de gestión de riesgos y de rendición de cuentas. Ello exige, sin duda, voluntad política, respaldo normativo interno (con políticas de seguridad formalmente aprobadas y actualizadas) y el compromiso de articular mecanismos efectivos de cooperación entre Administraciones. La solución no pasa únicamente por sofisticar estructuras, sino también por diseñar un modelo de gobernanza que, siendo jurídicamente válido, responda a las características propias de la Administración local y garantice el cumplimiento de los principios de legalidad, eficacia, eficiencia y transparencia.

En definitiva, la única vía para que la ciberseguridad en las EE. LL. se convierta en una realidad es mediante la adopción de un modelo de gobernanza bien definido, realista y ejecutable, acompañado de una hoja de ruta que oriente la progresiva implantación de los controles y medidas previstos por el ENS, de forma ajustada a las capacidades y al contexto de cada Administración.

6. Bibliografía

Almonacid Lamelas, V. (2025). *Gobernanzas*. Disponible en https://nosoloaytos.wordpress.com/2025/02/09/gobernanzas/.

Canals Ametller, D. (2022). La seguridad digital en medianas y pequeñas entidades locales: hacia una gestión municipal colaborativa. En J. Fondevila Antolín (dir.). *Transformación digital en las medianas y pequeñas entidades locales. Retos en clave de eficiencia y sostenibilidad*. Madrid: Wolters Kluwer.

Centro Criptográfico Nacional y Federación Española de Municipios y Provincias. (2022). *Prontuario de ciberseguridad para entidades locales*

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

(diciembre 2022). Disponible en https://ens.ccn.cni.es/es/docman/documentos-publicos/25-ccn-cert-prontuario-ciberseguridad/file.

Federación Española de Municipios y Provincias. (2018a). *Guía Estratégica en Seguridad para Entidades Locales. Esquema Nacional de Seguridad (ENS). Cuaderno de Recomendaciones. Tomo 1*. Disponible en https://www.ccn-cert.cni.es/es/pdf/documentos-publicos/ens/2449-femp-ens-tomo-1-guia-estrategica-en-seguridad-para-entidades-locales/file?format=html.

Federación Española de Municipios y Provincias. (2018b). *Guía para Entidades Locales de menos de 2.000 habitantes. Esquema Nacional de Seguridad (ENS). Cuaderno de Recomendaciones. Tomo 2*. Disponible en https://www.ccn-cert.cni.es/es/pdf/documentos-publicos/ens/2452-femp-ens-tomo-2-guia-para-entidades-locales-de-menos-de-2000-habitantes/file?format=html.

- **Guías y buenas prácticas CCN**

CCN. May. 2020. Guía CCN-STIC 803 sobre la Valoración de los sistemas.

CCN. Abr. 2024. Guía CCN-STIC-892 Perfil de Cumplimiento Específico para organizaciones en el ámbito de aplicación de la Directiva NIS2 (PCE-NIS2).

CCN. May. 2020. Guía CCN-STIC-883 Guía de implantación del ENS para Entidades Locales.

CCN. Mar. 2023. Guía CCN-STIC-890A Perfil de Cumplimiento Específico de Requisitos Esenciales de Seguridad - Entidades Locales.

CCN. Mar. 2023. Guía CCN-STIC-890 Adecuación al ENS conforme Requisitos Esenciales Seguridad según µCeENS.

CCN. Mar. 2023. Guía CCN-STIC-890A Perfil de Cumplimiento Específico de Requisitos Esenciales de Seguridad - Entidades Locales.

CCN. Mar. 2023. Guía CCN-STIC-890C Perfil de Cumplimiento Específico de Requisitos Esenciales de Seguridad.

CCN. Jun. 2025. Guía CCN-STIC 801 Responsabilidades y Funciones en el ENS.

CAPÍTULO VIII

Actuaciones a seguir frente a un ciberataque a una entidad local

Fernando Suárez Lorenzo
Ingeniero en Informática.
Presidente del Colexio Profesional de Enxeñaría en Informática de Galicia (CPEIG) y del Consejo General de Ingeniería Informática (CCII)

SUMARIO. 1. Introducción. 2. Marco general de respuesta ante ciberataques. 2.1. La importancia de la preparación previa. 2.2. Políticas de ciberseguridad municipal. 2.3. Infraestructuras críticas en el ámbito local. 2.4. Colaboración con actores externos. **3. Fases de actuación frente a un ciberataque.** 3.1. Detección y respuesta inicial. 3.2. Contención del ataque. 3.3. Investigación y análisis forense. 3.4. Recuperación y restablecimiento. 3.5. Lecciones aprendidas y plan de mejora continua. **4. La política de ciberseguridad municipal.** 4.1. Gestión de riesgos. 4.2. Roles y responsabilidades. 4.3. Formación y sensibilización. 4.4. Implementación y monitorización. **5. Análisis DAFO. 6. Conclusiones. 7. Bibliografía.**

1. Introducción

El auge de la digitalización ha transformado significativamente la manera en que las entidades locales gestionan sus servicios. La incorporación de tecnologías como los sistemas de gestión electrónica, las plataformas de participación ciudadana y las infraestructuras críticas digitalizadas ha traído consigo ventajas indiscutibles, como la mejora en la eficiencia y la

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

accesibilidad. Sin embargo, esta dependencia tecnológica también expone a los municipios a nuevos y complejos riesgos de ciberseguridad.

Estudios recientes destacan que más del 70 % de las entidades locales europeas han reportado al menos un incidente de ciberseguridad en los últimos tres años. Estos ataques van desde *ransomware* y *phishing* hasta accesos no autorizados a datos personales de los ciudadanos. En muchos casos, las entidades locales carecen de los recursos humanos, financieros y técnicos para enfrentar estas amenazas de manera efectiva, situándolas en una posición de vulnerabilidad crítica.

Los ciberataques a nivel local pueden tener un impacto desproporcionado, dado que afectan directamente a servicios esenciales como:

- la gestión del agua potable y el saneamiento;
- la emisión de certificados y permisos;
- la recaudación de impuestos municipales;
- los sistemas de seguridad ciudadana, como cámaras de vigilancia o sistemas de alarmas.

Además del impacto operativo, estos incidentes erosionan la confianza pública y generan altos costos económicos. Un informe de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) estima que el coste promedio de un ciberataque a una entidad local puede superar los 300 000 euros, sin contar las posibles sanciones derivadas del incumplimiento normativo.

El marco normativo europeo, liderado por la Directiva NIS II y el Esquema Nacional de Seguridad en España, establece obligaciones claras para proteger las infraestructuras críticas. Sin embargo, la implementación de estas medidas a nivel local sigue siendo desigual. Este capítulo pretende conectar la teoría normativa con la práctica, brindando una guía paso a paso adaptada a las características y limitaciones de las Administraciones locales.

Este capítulo tiene tres objetivos principales:

- proporcionar un marco estructurado para responder a ciberataques en el ámbito local;

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

- establecer las responsabilidades y los roles necesarios para una respuesta efectiva;

- ofrecer herramientas prácticas que permitan a los municipios mejorar su resiliencia frente a amenazas cibernéticas.

En las secciones siguientes se abordará cómo las entidades locales pueden organizar su respuesta a un incidente desde una perspectiva técnica y de gestión, destacando la importancia de la cooperación interinstitucional, la capacitación continua y el aprendizaje posincidente.

2. Marco general de respuesta ante ciberataques

2.1. La importancia de la preparación previa

La preparación previa es el cimiento de una respuesta efectiva ante ciberataques. En el ámbito de las entidades locales, donde los recursos pueden ser limitados y la dependencia de sistemas tecnológicos es alta, contar con medidas proactivas puede marcar la diferencia entre una interrupción temporal y un colapso prolongado de servicios esenciales.

La ciberseguridad debe abordarse como un proceso continuo y cíclico. El marco del ciclo de vida de la ciberseguridad, que comprende las fases de identificar, proteger, detectar, responder y recuperar, proporciona una guía estructurada para las entidades locales:

1. Identificar: Esta etapa implica mapear los activos críticos de la organización, evaluar sus vulnerabilidades y entender las amenazas específicas del entorno. Por ejemplo, un pequeño ayuntamiento podría priorizar la protección de sus sistemas de recaudación de impuestos y expedición de certificados.

2. Proteger: Una vez identificados los activos, es esencial implementar controles técnicos, administrativos y físicos que reduzcan el riesgo de ataques. Esto incluye medidas como el uso de *firewalls*, políticas de contraseñas robustas y segmentación de redes.

3. Detectar: La capacidad de detectar amenazas de forma temprana es crucial para minimizar el impacto de un ataque. Las entidades locales pueden recurrir a soluciones como sistemas de detección

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

de intrusos (IDS) o colaborar con centros de respuesta a incidentes de seguridad (CSIRT).

4. Responder: Un plan claro y bien practicado para reaccionar ante un incidente es esencial. Esto incluye identificar responsables, comunicar el incidente a las partes relevantes y ejecutar medidas de contención.

5. Recuperar: Finalmente, la recuperación se centra en restaurar los servicios afectados y analizar el incidente para evitar futuras recurrencias. Esto también incluye la comunicación a los ciudadanos sobre las medidas adoptadas para garantizar la continuidad de los servicios.

Planes de contingencia y continuidad operativa

Un plan de contingencia bien diseñado asegura que las entidades locales puedan mantener sus servicios esenciales incluso durante un ciberataque. Este plan debe incluir:

- Inventarios de activos y servicios críticos: ¿qué sistemas deben restaurarse primero?; ¿cuáles son las dependencias clave?

- Planes de recuperación ante desastres (DRP): procedimientos técnicos para recuperar sistemas y datos en caso de ataque.

- Pruebas regulares y simulaciones: validar los planes mediante ejercicios prácticos como simulacros de *ransomware*.

Por ejemplo, un ayuntamiento podría realizar una simulación en la que se bloquea el acceso a su sistema de emisión de certificados, verificando la capacidad de restaurar el servicio dentro del tiempo objetivo definido.

Evaluación de riesgos periódica

Una evaluación regular de riesgos permite a las entidades locales adaptarse a nuevas amenazas. Este proceso incluye:

- Identificación de amenazas emergentes: por ejemplo, un incremento en ataques de *phishing* dirigidos a empleados municipales.

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

- Clasificación de activos según criticidad: un análisis que priorice la protección de datos ciudadanos frente a sistemas de menor relevancia.

- Priorización de inversiones: asegurar que los recursos limitados se asignen de forma estratégica.

Además, esta evaluación debe estar alineada con las normativas nacionales y europeas, como el Esquema Nacional de Seguridad, para garantizar el cumplimiento regulatorio.

Cultura organizativa: la clave para la preparación

La ciberseguridad no es solo responsabilidad del equipo técnico; debe involucrar a toda la organización. Esto incluye:

- Capacitación del personal: Desde los altos cargos hasta los operativos, todos deben ser conscientes de los riesgos y las mejores prácticas.

- Sensibilización a nivel político: Los responsables municipales deben entender la importancia de priorizar la ciberseguridad en sus agendas.

- Definición de roles y responsabilidades: Asegurar que cada empleado sepa cómo actuar en caso de un incidente.

2.2. Políticas de ciberseguridad municipal

Las políticas de ciberseguridad son documentos estratégicos que establecen las directrices, procedimientos y responsabilidades necesarias para proteger los activos digitales de una organización. En el contexto de las entidades locales, estas políticas no solo deben adaptarse a la normativa vigente, sino también considerar las particularidades de los recursos y las infraestructuras de los municipios.

Una política de ciberseguridad municipal es un marco de trabajo diseñado para proteger los sistemas de información, los datos de los ciudadanos y los servicios públicos locales. Este documento tiene como objetivo:

- establecer directrices claras para la gestión de riesgos de ciberseguridad;

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

- definir roles y responsabilidades específicas dentro de la organización;
- describir los procedimientos para prevenir, detectar y responder a incidentes de ciberseguridad;
- fomentar una cultura organizativa de ciberseguridad que trascienda las áreas técnicas.

El diseño y la implementación de esta política deben ser liderados por los responsables técnicos, pero con un fuerte compromiso de los equipos políticos y administrativos.

Elementos clave de una política de ciberseguridad

Una política efectiva debe contener, al menos, los siguientes apartados:

1. Declaración de objetivos: una declaración que exprese el compromiso de la entidad local con la protección de los datos y servicios digitales.
2. Gestión de riesgos: incluir un enfoque sistemático para identificar, evaluar y mitigar riesgos. Esto puede involucrar matrices de riesgos y planes de acción específicos.
3. Roles y responsabilidades: especificar quién es responsable de cada aspecto de la ciberseguridad, desde el responsable político hasta los técnicos y personal operativo.
4. Formación y sensibilización: establecer programas regulares para educar al personal sobre prácticas seguras, como evitar el *phishing* y gestionar contraseñas de manera adecuada.
5. Procedimientos de respuesta a incidentes: un conjunto de pasos que detallen cómo actuar ante un ciberataque, desde la detección inicial hasta la recuperación completa.
6. Revisión y mejora continua: incluir mecanismos para evaluar y actualizar la política de forma periódica, adaptándose a nuevos riesgos y tecnologías.

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

La colaboración interinstitucional

Muchas entidades locales, especialmente los pequeños municipios, enfrentan limitaciones en recursos técnicos y humanos. En este contexto, la colaboración con otras Administraciones y organismos especializados es crucial. Ejemplos de esta colaboración incluyen:

- Diputaciones provinciales: Estas instituciones pueden actuar como nodos de ciberseguridad, ofreciendo soporte técnico y asesoramiento a los municipios de menor tamaño.
- CSIRT regionales y nacionales: Proporcionan orientación y apoyo técnico en la gestión de incidentes.
- Instituto Nacional de Ciberseguridad (INCIBE) y Centro Criptológico Nacional (CCN): Organismos que ofrecen formación, herramientas y recursos específicos para entidades locales.

Beneficios de una política de ciberseguridad municipal

Implementar una política de ciberseguridad aporta ventajas tangibles, como:

- reducción de riesgos asociados a ciberataques;
- cumplimiento normativo con marcos como el ENS o la Directiva NIS II;
- mejora de la confianza de los ciudadanos en los servicios municipales;
- ahorro de costos a largo plazo, al prevenir incidentes y sus consecuencias económicas.

2.3. Infraestructuras críticas en el ámbito local

Las infraestructuras críticas constituyen el corazón operativo de las entidades locales, ya que soportan servicios esenciales que afectan directamente a la calidad de vida de los ciudadanos. En el ámbito municipal, estas infraestructuras incluyen sistemas de abastecimiento de agua, gestión de residuos, transporte público, alumbrado y comunicaciones, entre otros. La creciente digitalización de estos sistemas los hace más eficientes, pero

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

también más vulnerables a ciberataques que pueden generar graves consecuencias económicas, sociales y políticas.

Un ejemplo paradigmático de la vulnerabilidad de estas infraestructuras ocurrió en Baltimore (EE. UU.) en 2019, cuando un ataque de *ransomware* paralizó los sistemas municipales durante semanas. La ciudad sufrió pérdidas millonarias no solo por el rescate exigido, que no se pagó, sino también por los costes asociados a la interrupción de servicios, como la recaudación de impuestos y la emisión de licencias. Este caso evidencia cómo un ciberataque puede sobrepasar las barreras tecnológicas y afectar directamente al tejido social y económico.

Identificación y protección de infraestructuras críticas

En el caso de las entidades locales, la identificación de infraestructuras críticas debe ser una prioridad. Aunque estas varían dependiendo del tamaño y de las competencias de cada municipio, ciertos sistemas suelen ser considerados críticos en la mayoría de los casos, como los sistemas de gestión de emergencias o las redes de suministro eléctrico. Identificar estas infraestructuras requiere un análisis exhaustivo de los servicios prestados y de las posibles consecuencias de su interrupción.

Una vez identificadas, el siguiente paso es asegurar su protección. En el marco del Esquema Nacional de Seguridad, las entidades locales tienen la obligación de garantizar la seguridad de los sistemas que soportan sus servicios esenciales. Esto implica implementar medidas técnicas y organizativas específicas, como la segmentación de redes, el cifrado de datos sensibles y la adopción de estándares de ciberseguridad reconocidos.

En España, los ayuntamientos tienen acceso a herramientas y recursos proporcionados por organismos nacionales como el CCN y el INCIBE. Estos organismos ofrecen guías, formación y soporte técnico para fortalecer la seguridad de las infraestructuras locales. Sin embargo, la implementación efectiva de estas medidas depende en gran medida de la voluntad política y de la asignación de recursos adecuados a nivel municipal.

Retos específicos de las infraestructuras críticas locales

Uno de los mayores desafíos que enfrentan las entidades locales es la falta de recursos humanos y financieros especializados en ciberseguridad. Mientras que grandes ciudades como Madrid o Barcelona cuentan con

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

departamentos dedicados a la seguridad digital, muchos pequeños municipios dependen de un único técnico de sistemas para gestionar toda su infraestructura tecnológica. Esta brecha de capacidades puede ser abordada mediante la colaboración interinstitucional, como la ofrecida por las diputaciones provinciales o los Gobiernos autonómicos.

Además, las infraestructuras locales suelen estar integradas por sistemas heterogéneos y, en ocasiones, obsoletos, lo que dificulta su protección. Por ejemplo, sistemas *Supervisory Control and Data Acquisition* (SCADA) utilizados para el control del suministro de agua en algunos municipios han sido diseñados sin considerar las amenazas cibernéticas modernas, lo que los convierte en blancos fáciles para los atacantes. La modernización de estos sistemas requiere no solo inversiones económicas, sino también la adopción de una estrategia integral de ciberseguridad que priorice la prevención sobre la reacción.

El papel del Esquema Nacional de Seguridad

El ENS establece un marco común para garantizar la protección de los sistemas de información en las Administraciones públicas, incluyendo las locales. Aunque su implementación ha avanzado significativamente en los últimos años, aún existen retos en su aplicación práctica, especialmente en municipios pequeños y medianos. Una de las soluciones más efectivas ha sido la creación de perfiles de cumplimiento específicos para entidades locales, que adaptan las exigencias del ENS a las realidades de estas Administraciones.

Por ejemplo, los perfiles de cumplimiento distinguen entre grandes municipios, que deben cumplir con todas las medidas del ENS, y pequeños municipios, a los que se permite priorizar ciertas acciones esenciales. Esta flexibilidad ha facilitado que más entidades locales inicien el proceso de certificación, lo que a su vez mejora la seguridad de sus infraestructuras críticas.

En definitiva, las infraestructuras críticas en el ámbito local representan un punto neurálgico de la ciberseguridad municipal. Su protección no solo asegura la continuidad de los servicios esenciales, sino que también refuerza la confianza de los ciudadanos en sus instituciones. Sin embargo, lograr una protección efectiva requiere un enfoque multidimensional que combine recursos técnicos, formación especializada, colaboración interinstitucional y compromiso político. Solo a través de este enfoque integral será

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

posible garantizar la resiliencia de las infraestructuras críticas locales frente a las amenazas cibernéticas actuales y futuras.

2.4. Colaboración con actores externos

La colaboración con actores externos es un elemento esencial en la estrategia de ciberseguridad de cualquier entidad local. Dada la limitada capacidad técnica y financiera de muchos municipios, establecer alianzas con organismos especializados, proveedores tecnológicos y otras Administraciones es crucial para garantizar una respuesta efectiva frente a ciberataques. Este enfoque colaborativo permite compartir conocimientos, acceder a recursos avanzados y optimizar la gestión de riesgos.

Uno de los actores clave en la colaboración externa son los centros de respuesta a incidentes de seguridad informática (CSIRT) y los centros de operaciones de ciberseguridad (SOC). En España, el CCN-CERT y el INCIBE-CERT lideran la gestión de incidentes a nivel nacional y ofrecen soporte directo a las Administraciones públicas, incluidas las locales.

Estos centros proporcionan una variedad de servicios, como:

- la detección y análisis de amenazas emergentes;
- el apoyo técnico en la mitigación y recuperación de ciberataques;
- la capacitación de personal técnico a través de talleres y simulacros;
- la distribución de guías y herramientas específicas para proteger infraestructuras críticas.

Por ejemplo, durante la pandemia de COVID-19, el CCN-CERT intensificó su colaboración con las Administraciones locales para proteger las plataformas de teletrabajo y los sistemas de atención al ciudadano, que se convirtieron en objetivos frecuentes de ataques.

Ciber.gal: un modelo de colaboración regional en ciberseguridad

En Galicia, la Axencia para a Modernización Tecnolóxica de Galicia (AMTEGA) lidera un modelo ejemplar de colaboración interinstitucional en ciberseguridad, especialmente a través de su iniciativa Ciber.gal. Esta alianza estratégica reúne a Administraciones públicas, empresas tecnológicas, centros de

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

conocimiento y otros actores relevantes para fortalecer las capacidades de ciberseguridad en todos los niveles.

La AMTEGA no solo proporciona herramientas y servicios específicos a los ayuntamientos, sino que también promueve la sensibilización, formación y cooperación a través de iniciativas como el Encuentro Cibergal. Este evento anual se ha consolidado como un referente en el ámbito de la ciberseguridad, sirviendo como punto de encuentro para compartir experiencias, identificar buenas prácticas y fomentar la innovación en la protección de infraestructuras críticas locales.

Entre las acciones impulsadas por la AMTEGA se incluyen:

- Servicios tecnológicos compartidos: soluciones avanzadas de protección para los sistemas municipales, como *firewalls* y herramientas de monitorización en tiempo real.

- Capacitación del personal técnico: programas formativos diseñados para dotar a los responsables municipales de las competencias necesarias para gestionar riesgos cibernéticos.

- Simulacros de ciberseguridad: ejercicios prácticos que permiten a los ayuntamientos evaluar y mejorar su capacidad de respuesta ante incidentes.

- Fomento de la colaboración público-privada: integración de empresas tecnológicas en proyectos que refuercen las capacidades locales, como la implementación de soluciones basadas en inteligencia artificial para la detección de amenazas.

El Encuentro Cibergal, además, facilita el acceso de los municipios a redes de expertos y recursos avanzados, consolidando a Galicia como un modelo de referencia en la construcción de un ecosistema de ciberseguridad regional.

Colaboración con proveedores tecnológicos

Los proveedores tecnológicos desempeñan un papel doblemente relevante, tanto como aliados estratégicos en la protección de sistemas como posibles puntos vulnerables en la cadena de suministro. Es fundamental que las entidades locales establezcan relaciones claras y bien definidas con sus

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

proveedores, asegurando que estos cumplan con los estándares de ciberseguridad requeridos.

Un aspecto clave es la revisión de los acuerdos de nivel de servicio (SLA) para incluir cláusulas específicas sobre tiempos de respuesta ante incidentes, auditorías de seguridad y responsabilidad en caso de brechas de datos. Además, los proveedores pueden ser aliados en la capacitación del personal técnico, ofreciendo formaciones específicas sobre el uso seguro de sus plataformas y herramientas.

Casos de éxito en la cooperación público-privada

La colaboración público-privada es otro componente fundamental en la estrategia de ciberseguridad. Iniciativas como los foros de ciberseguridad organizados por INCIBE han facilitado la creación de alianzas entre Administraciones públicas y empresas del sector tecnológico. Estas alianzas no solo fortalecen las capacidades técnicas de las entidades locales, sino que también promueven la innovación en herramientas de protección.

Un caso exitoso es el proyecto CIBERLOCAL, desarrollado en colaboración con empresas tecnológicas y ayuntamientos piloto, que busca implementar soluciones de ciberseguridad adaptadas a las necesidades de municipios pequeños y medianos. Este proyecto incluye la creación de manuales prácticos, talleres de formación y la implementación de tecnologías avanzadas como sistemas de inteligencia artificial para la detección de amenazas.

La colaboración con actores externos amplía significativamente las capacidades de las entidades locales para enfrentar ciberataques, especialmente en un contexto de recursos limitados. La experiencia de iniciativas como Ciber.gal demuestra que, con una estrategia adecuada, es posible crear un ecosistema colaborativo que fortalezca la resiliencia de los municipios frente a las amenazas cibernéticas actuales y futuras.

3. Fases de actuación frente a un ciberataque

Responder de manera efectiva a un ciberataque requiere un enfoque estructurado que permita minimizar el impacto, proteger los activos críticos y restaurar los servicios afectados. Para las entidades locales, que gestionan sistemas esenciales y datos sensibles, este desafío es aún más complejo debido a las limitaciones de recursos y capacidades técnicas.

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

El proceso de gestión de un ciberataque no puede ser improvisado. Desde el momento en que se detecta un incidente hasta la recuperación completa, cada acción debe estar guiada por protocolos predefinidos y ejecutada con precisión. Estas fases no solo garantizan una respuesta ordenada, sino que también maximizan las posibilidades de contener el daño, identificar las vulnerabilidades explotadas y aprender de la experiencia para evitar incidentes futuros.

En este apartado, se describen las cinco fases fundamentales para actuar frente a un ciberataque:

1. Detección y respuesta inicial: La capacidad de identificar y evaluar rápidamente un incidente es clave para activar una respuesta eficaz.

2. Contención del ataque: Evitar que el ataque se propague o cause mayores daños es una prioridad en las primeras horas del incidente.

3. Investigación y análisis forense: Comprender cómo ocurrió el ataque y cuál fue su alcance permite tomar decisiones informadas para mitigar su impacto.

4. Recuperación y restablecimiento: Restaurar los sistemas afectados de manera segura y garantizar la continuidad de los servicios es el objetivo principal tras la contención.

5. Lecciones aprendidas y plan de mejora continua: Analizar el incidente permite identificar áreas de mejora y ajustar las políticas y los procedimientos para fortalecer la resiliencia.

Cada una de estas fases será abordada en detalle, proporcionando pautas prácticas para que las entidades locales enfrenten los ciberataques de manera efectiva y profesional.

3.1. Detección y respuesta inicial

La detección temprana y la respuesta inicial son etapas críticas en la gestión de un ciberataque. Estas fases determinan, en gran medida, el impacto del incidente en los servicios y sistemas de la entidad local. Una detección oportuna permite activar protocolos que limitan la extensión del ataque, minimizan daños y protegen los datos sensibles de los ciudadanos.

Herramientas y mecanismos de detección

En el contexto de las entidades locales, donde los recursos técnicos pueden ser limitados, la detección de un ciberataque puede depender tanto de herramientas automatizadas como de la intervención humana. Entre los mecanismos más comunes para identificar incidentes se encuentran:

- Sistemas de detección de intrusos (IDS): Tecnologías que monitorizan el tráfico de red en busca de comportamientos anómalos o patrones conocidos de ataque.

- Alertas de *software* de seguridad: Herramientas como antivirus o *firewalls* que detectan y bloquean actividades sospechosas.

- Informes de usuarios: En muchos casos, los primeros indicios de un ataque son reportados por empleados municipales que experimentan fallos inusuales en sus sistemas.

Un ejemplo ilustrativo es un incidente de ransomware en un pequeño municipio donde el ataque fue detectado cuando varios empleados no pudieron acceder a sus documentos, y sus pantallas mostraron un mensaje exigiendo el pago de un rescate. Este tipo de detección, aunque reactiva, es común en entidades sin soluciones avanzadas de monitorización.

Acciones inmediatas tras la detección

Una vez que se identifica un posible incidente, la respuesta inicial debe centrarse en confirmar su naturaleza y activar los protocolos adecuados. Este proceso incluye:

1. Confirmación del incidente: Es crucial determinar si se trata de un ataque real o un falso positivo. Esto puede implicar la revisión de los logs del sistema y la consulta con expertos técnicos internos o externos.

2. Notificación interna: Inmediatamente después de confirmar el incidente, debe informarse al equipo de respuesta a incidentes, que puede incluir tanto personal técnico municipal como organismos externos, como un CSIRT regional.

3. Establecimiento de prioridades: Evaluar rápidamente qué sistemas y datos están en riesgo para priorizar las acciones. Por ejemplo, si el

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

sistema afectado gestiona la emisión de certificados, podría considerarse crítico para la continuidad operativa del municipio.

Comunicación temprana y control de la información

La gestión adecuada de la comunicación interna y externa en esta etapa es esencial para evitar la desinformación y mantener el control del incidente. A nivel interno, se debe garantizar que todos los empleados municipales estén al tanto de las instrucciones clave, como no intentar acceder a sistemas comprometidos o no desconectar dispositivos sin autorización.

En cuanto a la comunicación externa, especialmente si el incidente afecta servicios públicos visibles para la ciudadanía, debe manejarse con cuidado para evitar alarmas innecesarias. Esto podría incluir:

- emitir un comunicado breve que informe del problema de manera general, asegurando que se están tomando medidas para solucionarlo;

- designar un portavoz que centralice todas las comunicaciones para evitar mensajes contradictorios.

Comunicación en caso de filtración de datos personales

La comunicación con los ciudadanos tras un ciberataque, especialmente en casos de filtración de datos personales, requiere una estrategia bien estructurada que combine transparencia, sensibilidad y cumplimiento normativo. Además de informar sobre el restablecimiento de servicios, las entidades locales tienen la responsabilidad legal y moral de comunicar adecuadamente las posibles afectaciones a la privacidad de los ciudadanos.

Los elementos clave de la comunicación en caso de filtración de datos personales son los siguientes:

1. Notificación inmediata y transparente:

    - Según el Reglamento General de Protección de Datos (RGPD), si una brecha de datos supone un riesgo para los derechos y libertades de las personas afectadas, la entidad local debe notificarlo de manera inmediata tanto a los afectados como a la Agencia Española de Protección de Datos (AEPD).

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

- La notificación debe incluir información clara sobre:
  - qué datos se han visto comprometidos (por ejemplo: nombres, direcciones, datos financieros);
  - cómo ocurrió la filtración;
  - las medidas adoptadas para mitigar los daños.

2. Establecimiento de un canal de atención directa:
   - crear un punto de contacto específico, como una línea telefónica o un correo electrónico, para responder a las dudas y preocupaciones de los ciudadanos;
   - designar a un responsable (posiblemente el delegado de protección de datos) que coordine las respuestas y garantice la coherencia en la información proporcionada.
3. Proporcionar orientación a los afectados:
   - Recomendar acciones concretas para minimizar posibles impactos, como:
     - cambiar contraseñas comprometidas;
     - monitorizar actividades inusuales en cuentas bancarias o de correo;
     - estar atentos a intentos de fraude relacionados con la filtración.
4. Reconocer la gravedad del incidente con profesionalismo:
   - reconocer públicamente el incidente y explicar las acciones tomadas para proteger los datos de los ciudadanos en el futuro;
   - evitar actitudes defensivas o culpar a terceros, ya que esto puede erosionar aún más la confianza pública.
5. Cumplimiento normativo:
   - además de notificar a la AEPD, documentar todas las acciones realizadas para gestionar la brecha de datos;

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

- mantener registros detallados del incidente para posibles auditorías o investigaciones posteriores.

Una buena estrategia de comunicación tiene una serie de beneficios claros y directos:

- Confianza ciudadana: La transparencia demuestra que la entidad local está actuando de manera responsable, incluso en situaciones críticas.

- Cumplimiento legal: Garantiza que la Administración cumple con las obligaciones establecidas por el RGPD y otras normativas aplicables.

- Reducción del impacto reputacional: Una respuesta clara y profesional puede minimizar las críticas y reforzar la percepción de compromiso con la seguridad.

La importancia de los planes preestablecidos

El éxito de esta fase depende en gran medida de la existencia y del conocimiento de un plan de respuesta a incidentes previamente definido. Este plan debe incluir:

- Roles y responsabilidades claras: saber quién debe ser contactado y qué decisiones deben tomarse en los primeros minutos tras la detección.

- Protocolos de escalado: definir en qué momento se requiere la intervención de actores externos, como un CSIRT o el proveedor del sistema afectado.

Un caso de referencia es el ataque sufrido por el Ayuntamiento de Castellón en 2022, donde la rápida activación del plan de contingencia permitió contener el incidente y evitar la pérdida de datos críticos. Este ejemplo destaca la importancia de estar preparado incluso con recursos limitados.

3.2. Contención del ataque

Una vez detectado y confirmado un ciberataque, la contención se convierte en la prioridad principal. Esta fase busca limitar el alcance del ataque,

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

evitar que se extienda a otros sistemas y proteger los activos críticos de la entidad local. La contención, aunque temporal, es clave para estabilizar la situación antes de avanzar hacia la investigación y la recuperación.

Estrategias de contención

La contención debe ser cuidadosamente planificada y ejecutada para no comprometer la evidencia necesaria para una posterior investigación. Algunas estrategias comunes incluyen:

- Aislamiento de sistemas comprometidos: Si un ataque afecta a un servidor o dispositivo específico, desconectarlo de la red puede evitar que el ataque se propague. Por ejemplo, en un caso de *ransomware*, desconectar inmediatamente las estaciones de trabajo infectadas puede proteger el resto de la red.

- Restricción de accesos: Imponer restricciones temporales a usuarios y dispositivos mientras se investiga el incidente. Esto puede incluir bloquear cuentas comprometidas o limitar los privilegios de administrador.

- Monitorización activa: Implementar una vigilancia más rigurosa de los sistemas no afectados para detectar señales de que el ataque intenta moverse lateralmente dentro de la red.

Un ejemplo práctico de esta estrategia ocurrió durante el ataque de *ransomware* WannaCry en 2017. Organizaciones que aislaron rápidamente los sistemas infectados lograron minimizar el impacto, mientras que otras que no tomaron medidas inmediatas enfrentaron una propagación masiva del *malware*.

Uso de herramientas y apoyo externo

Para muchas entidades locales, la contención efectiva puede requerir la ayuda de herramientas avanzadas o de actores externos. Por ejemplo:

- Herramientas de respuesta automatizada: sistemas de *Endpoint Detection and Response* (EDR) que permiten aislar dispositivos afectados con un solo clic.

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

- Apoyo de CSIRT o SOC regionales: expertos en ciberseguridad que pueden proporcionar análisis en tiempo real y asesorar sobre las mejores prácticas de contención.

- Colaboración con proveedores tecnológicos: especialmente si el ataque afecta a un sistema proporcionado por un tercero, como una plataforma de gestión de servicios municipales.

En Galicia, la colaboración a través de la red Ciber.gal ha demostrado ser un modelo efectivo de apoyo interinstitucional, donde los ayuntamientos afectados por incidentes de ciberseguridad pueden contar con asistencia técnica inmediata de la AMTEGA y sus aliados.

Consideraciones específicas en infraestructuras críticas

Cuando el ataque afecta a infraestructuras críticas locales, como sistemas SCADA para el suministro de agua o electricidad, la contención requiere un enfoque aún más delicado. En estos casos, es esencial:

- Priorizar la continuidad del servicio: Si desconectar un sistema puede causar un impacto significativo en la ciudadanía, deben evaluarse medidas alternativas de contención que minimicen la interrupción.

- Evitar daños colaterales: Las acciones deben ejecutarse de manera que no afecten a servicios interdependientes. Por ejemplo, al contener un ataque en un sistema de transporte público, es importante asegurarse de que las plataformas de pago no queden inutilizables.

Un caso notable es el ataque al sistema de agua de Oldsmar, Florida, en 2021, donde un atacante intentó modificar químicamente los niveles de tratamiento del agua. La contención inmediata del sistema comprometido evitó un desastre potencial, demostrando la importancia de protocolos claros y la capacidad de reacción rápida.

La importancia de los procedimientos establecidos

Para que la contención sea efectiva, debe apoyarse en procedimientos predefinidos y bien practicados. Estos procedimientos deben incluir:

- Pasos específicos para diferentes tipos de ataques: desde *phishing* hasta *ransomware* o accesos no autorizados.

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

- Coordinación clara: asegurarse de que todos los involucrados, desde técnicos hasta responsables políticos, comprendan su rol en la contención.

- Pruebas regulares: simulacros y ejercicios prácticos que preparen al personal para actuar con rapidez y confianza.

Equilibrio entre contención y preservación de evidencias

Una de las mayores dificultades en esta fase es equilibrar la necesidad de detener el ataque con la preservación de evidencias que puedan ser cruciales para la investigación forense. Tomar decisiones precipitadas, como apagar sistemas sin realizar una copia forense, puede dificultar la identificación del vector de ataque o los métodos utilizados por los ciberdelincuentes.

Por ello, se recomienda trabajar con herramientas y procedimientos que permitan:

- crear instantáneas de los sistemas afectados antes de aislarlos;

- registrar todas las acciones realizadas durante la contención para garantizar la trazabilidad.

La contención no es una solución definitiva, pero establece una barrera esencial que permite ganar tiempo para preparar la recuperación y el análisis posterior. En el caso de las entidades locales, donde los recursos son limitados, disponer de una estrategia clara de contención puede marcar la diferencia entre un incidente manejable y un desastre que paralice los servicios esenciales.

3.3. Investigación y análisis forense

Tras contener un ciberataque, la etapa de investigación y análisis forense se centra en comprender la naturaleza, el alcance y las implicaciones del incidente. Este proceso es esencial para identificar vulnerabilidades, aprender de la experiencia y tomar medidas que refuercen la seguridad futura de la entidad local.

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

Objetivos de la investigación forense

La investigación forense tiene varios objetivos fundamentales:

- Identificar el punto de entrada del ataque: determinar cómo los atacantes accedieron al sistema, ya sea a través de un fallo en la configuración, una vulnerabilidad en el *software* o un error humano, como un clic en un correo malicioso;

- Evaluar el alcance del daño: detectar qué sistemas y datos han sido comprometidos, incluidos los que pueden haber sido exfiltrados o manipulados;

- Recolectar evidencias: recopilar datos que puedan ser utilizados para análisis internos, prevención de futuros incidentes o, en casos específicos, procedimientos legales.

Este proceso debe realizarse de manera meticulosa y documentada, siguiendo estándares de buenas prácticas en ciberseguridad y en cumplimiento de las normativas aplicables, como el Reglamento General de Protección de Datos (RGPD), si el incidente afecta a datos personales.

Metodología del análisis forense

El análisis forense en ciberseguridad sigue un enfoque sistemático que incluye varias etapas:

1. Adquisición de evidencias digitales:

    - Se realiza una copia forense de los sistemas afectados, asegurando la integridad de los datos mediante técnicas de *hash*. Esto evita que las evidencias sean manipuladas o cuestionadas. Ejemplo: Si un servidor es infectado por *ransomware*, se copia todo su contenido para su análisis, dejando el sistema original intacto.

2. Preservación del entorno afectado:

    - Mantener el estado de los sistemas tal como fueron encontrados en el momento del ataque. Esto incluye evitar reinicios o desconexiones innecesarias que puedan alterar las evidencias.

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

3. Análisis detallado:

    - Identificar los patrones de comportamiento del atacante, los archivos o procesos sospechosos y los vectores de ataque utilizados. Por ejemplo, analizar *logs* de acceso, conexiones remotas y cambios realizados en el sistema.

4. Correlación de datos:

    - Cruzar información con bases de datos de amenazas conocidas (como indicadores de compromiso) para identificar herramientas o técnicas empleadas por los atacantes.

Herramientas y recursos para el análisis

En el ámbito local, muchas entidades no cuentan con equipos especializados en análisis forense, lo que hace necesario recurrir a herramientas específicas o a la colaboración con expertos externos. Algunas herramientas comúnmente utilizadas incluyen:

- Autopsy y EnCase: para análisis de discos duros y recuperación de datos.
- Wireshark: para examinar tráfico de red sospechoso.
- Volatility: para análisis de memoria y detección de *malware* en sistemas en ejecución.

Adicionalmente, organismos como el CCN-CERT, INCIBE o Ciber.gal ofrecen servicios de soporte y asesoramiento en análisis forense, permitiendo que incluso los pequeños municipios accedan a recursos avanzados.

Preservación de evidencias para acciones legales

Si existe la posibilidad de emprender acciones legales contra los responsables del ataque, es crucial que las evidencias recopiladas cumplan con los requisitos legales de admisibilidad. Esto incluye:

- Registrar la cadena de custodia: documentar quién tuvo acceso a las evidencias en cada momento.

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

- Garantizar la integridad de los datos: utilizar técnicas de *hash* para certificar que los archivos analizados no han sido alterados.

Un caso relevante es el ataque a la ciudad de Atlanta en 2018, donde las autoridades locales trabajaron en estrecha colaboración con expertos forenses y fuerzas del orden para rastrear a los responsables, lo que resultó en arrestos y procesamientos.

Evaluación del impacto del ataque

La investigación también debe centrarse en medir el impacto real del ataque, considerando:

- Impacto operacional: servicios que fueron interrumpidos y tiempo necesario para su recuperación.
- Impacto económico: costes directos de la respuesta y la recuperación, así como posibles sanciones por incumplimiento normativo.
- Impacto reputacional: nivel de confianza ciudadana afectado por el incidente y cómo mitigarlo a través de la comunicación adecuada.

Por ejemplo, un ataque de *ransomware* en un ayuntamiento que gestione datos de ciudadanos puede tener implicaciones legales y financieras significativas si los datos afectados incluyen información personal sensible.

Incorporación de los resultados en las estrategias de seguridad

Los hallazgos del análisis forense no solo deben documentarse, sino también integrarse en las estrategias de ciberseguridad del municipio. Esto puede incluir:

- revisar y fortalecer las políticas de acceso a sistemas;
- actualizar herramientas de seguridad para prevenir vectores de ataque similares;
- implementar procesos de formación basados en los errores detectados durante el incidente.

La investigación y el análisis forense son más que una reacción al ataque; representan una oportunidad para fortalecer la ciberseguridad muni-

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

cipal y convertir una crisis en aprendizaje. Al comprender cómo y por qué ocurrió el incidente, las entidades locales pueden prepararse mejor para evitar recurrencias y responder con mayor eficacia en el futuro.

3.4. Recuperación y restablecimiento

La recuperación es una de las fases más críticas tras un ciberataque, ya que su objetivo es restablecer la funcionalidad de los sistemas afectados y garantizar que puedan operar de manera segura. Para las entidades locales, que suelen gestionar servicios esenciales, una recuperación exitosa es fundamental para minimizar el impacto en la ciudadanía y restaurar la confianza pública.

El primer paso en la recuperación es restaurar los sistemas afectados, priorizando aquellos que soportan servicios críticos. Este proceso implica:

- Validar las copias de seguridad: Antes de proceder a la restauración, es necesario garantizar que las copias de seguridad no estén comprometidas. En ataques de *ransomware*, por ejemplo, las copias conectadas a los sistemas infectados podrían haber sido cifradas.

- Restaurar los servicios prioritarios: La recuperación debe seguir un orden establecido en el plan de continuidad operativa, asegurando que los servicios más críticos sean los primeros en ser restablecidos. Por ejemplo, un ayuntamiento podría priorizar el sistema de emisión de certificados frente a otros menos esenciales.

- Realizar pruebas de integridad: Una vez restaurados, los sistemas deben ser sometidos a pruebas exhaustivas para confirmar que funcionan correctamente y no contienen elementos maliciosos residuales.

Un ejemplo práctico es el ataque sufrido por el Ayuntamiento de Jerez de la Frontera en 2020. La Administración utilizó copias de seguridad para restablecer sus sistemas, priorizando aquellos necesarios para atender a la ciudadanía. Sin embargo, la falta de pruebas iniciales causó problemas en algunos servicios secundarios, lo que subraya la importancia de la validación previa.

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

Implementación de medidas preventivas

Una vez restaurados los sistemas, es crucial implementar medidas que prevengan recurrencias del ataque. Estas acciones incluyen:

- Actualizar y parchear sistemas: Muchas brechas de seguridad ocurren debido a vulnerabilidades conocidas en *software* desactualizado. Es fundamental aplicar parches de seguridad a todos los sistemas restaurados.

- Reforzar controles de acceso: Esto puede incluir la implementación de autenticación multifactor para usuarios y sistemas sensibles.

- Actualizar configuraciones de seguridad: Revisar y mejorar configuraciones de *firewalls*, antivirus y otros mecanismos de protección.

Comunicación con los ciudadanos

En los casos en que un ciberataque afecte servicios visibles para la ciudadanía, la recuperación debe ir acompañada de una estrategia de comunicación clara y transparente. Esto incluye:

- Informar sobre el restablecimiento de servicios: comunicar cuándo y cómo los servicios afectados estarán disponibles nuevamente.

- Explicar las medidas tomadas: detallar las acciones realizadas para garantizar la seguridad de los sistemas y la protección de los datos de los ciudadanos.

- Reforzar la confianza pública: reconocer el incidente de manera profesional y destacar los esfuerzos realizados para evitar futuros problemas.

Colaboración durante la recuperación

En esta fase, la colaboración con actores externos puede ser determinante. Las entidades locales pueden apoyarse en:

- CSIRT y SOC: Estos equipos proporcionan herramientas y conocimientos para garantizar una recuperación segura.

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

- Proveedores tecnológicos: Ayudan en la restauración de servicios específicos, como plataformas de gestión municipal.

- Otras Administraciones: En casos de ataques que afectan a múltiples municipios, la cooperación interinstitucional permite compartir recursos y acelerar el proceso de recuperación.

3.5. Lecciones aprendidas y plan de mejora continua

La fase final tras un ciberataque, aunque a menudo subestimada, es una de las más valiosas para fortalecer la ciberseguridad de una entidad local. Este momento ofrece la oportunidad de reflexionar sobre lo sucedido, identificar áreas de mejora y establecer un plan de acción que minimice el riesgo de futuros incidentes. Una gestión adecuada de las lecciones aprendidas puede convertir un evento crítico en un punto de inflexión hacia una mayor resiliencia organizativa.

Evaluación posincidente

La evaluación posincidente es un análisis exhaustivo que busca responder a preguntas clave sobre el ataque y la respuesta adoptada. Este proceso debe ser sistemático e incluir:

1. Revisión de los eventos: Reconstruir cronológicamente lo sucedido, desde el momento en que se detectó el ataque hasta la restauración completa de los sistemas.

2. Identificación de debilidades: Evaluar qué aspectos fallaron, ya sean técnicos, organizativos o de comunicación. Por ejemplo, un análisis podría revelar que el ataque fue posible debido a una configuración incorrecta del *firewall* o a la falta de formación del personal.

3. Documentación de fortalezas: Identificar qué elementos de la respuesta funcionaron bien y cómo podrían replicarse en el futuro.

Este análisis debe involucrar a todos los actores que participaron en la gestión del incidente, desde técnicos hasta responsables políticos, para obtener una visión integral.

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

Ajuste de políticas y procedimientos

Los hallazgos de la evaluación deben traducirse en ajustes concretos en las políticas y los procedimientos de ciberseguridad. Esto incluye:

- Actualización de los planes de respuesta a incidentes: incorporar lecciones aprendidas para mejorar la rapidez y eficacia de las acciones futuras.
- Revisión de la política de ciberseguridad municipal: ajustar directrices, roles y responsabilidades según los problemas identificados durante el incidente.
- Optimización del plan de continuidad operativa: modificar las prioridades de restauración de servicios basándose en la experiencia adquirida.

Por ejemplo, tras un ataque en un ayuntamiento español, se detectó que el plan de contingencia no cubría el acceso remoto de los empleados municipales, lo que retrasó la recuperación. Como resultado, el plan fue ampliado para incluir protocolos específicos para teletrabajo.

Formación y sensibilización del personal

Uno de los factores más comunes detrás de los ciberataques exitosos es el error humano. Por ello, tras un incidente, es fundamental reforzar la formación y sensibilización del personal. Esto incluye:

- Capacitación específica: enseñar a los empleados cómo identificar y responder a tácticas comunes, como *phishing* o *malware*.
- Simulacros regulares: realizar ejercicios prácticos que permitan al personal practicar la respuesta a diferentes tipos de ataques.
- Sensibilización a nivel político: involucrar a los responsables municipales en la formación, para garantizar su apoyo y comprensión de la importancia de la ciberseguridad.

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

Implementación de mejoras tecnológicas

El análisis posincidente suele revelar deficiencias en las herramientas tecnológicas utilizadas. Las mejoras en este ámbito pueden incluir:

- Adopción de nuevas tecnologías: como sistemas de detección de amenazas basados en inteligencia artificial o soluciones avanzadas de monitorización de red.
- Actualización de *hardware* y *software*: reemplazar sistemas obsoletos que representan un riesgo para la seguridad.
- Fortalecimiento de la infraestructura tecnológica: mejorar la segmentación de redes, el cifrado de datos y los controles de acceso.

Un ejemplo es el ataque de *ransomware* a Baltimore en 2019, donde la falta de copias de seguridad adecuadas agravó el impacto. Tras el incidente, la ciudad invirtió en soluciones avanzadas de *backup* y recuperación.

Establecimiento de métricas de rendimiento

Para garantizar la mejora continua, es esencial establecer métricas que permitan medir el desempeño de la ciberseguridad en la entidad local. Estas métricas pueden incluir:

- tiempo promedio de detección de incidentes;
- tiempo de respuesta y recuperación;
- número de incidentes detectados y resueltos;
- grado de cumplimiento de normativas como el Esquema Nacional de Seguridad.

La monitorización regular de estas métricas permite evaluar la efectividad de las medidas implementadas y ajustar las estrategias según sea necesario.

Promoción de una cultura de resiliencia

Finalmente, una lección clave que debe surgir de cualquier ciberataque es la importancia de construir una cultura organizativa orientada a la resiliencia. Esto implica:

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

- Compromiso a todos los niveles: desde los responsables políticos hasta el personal técnico y operativo.

- Fomento de la colaboración: establecer alianzas con otros municipios, organizaciones y expertos en ciberseguridad.

- Comunicación abierta y transparente: informar a los ciudadanos sobre las acciones tomadas y su impacto positivo en la seguridad de los servicios públicos.

La fase de lecciones aprendidas y mejora continua cierra el ciclo de gestión del incidente y abre la puerta a un futuro más seguro. Para las entidades locales, que suelen operar bajo restricciones presupuestarias y de personal, este proceso representa una oportunidad única para maximizar el valor de cada experiencia, convirtiendo un desafío en una fortaleza organizativa.

4. La política de ciberseguridad municipal

La política de ciberseguridad municipal es un documento estratégico que establece las directrices, los principios y los procedimientos necesarios para garantizar la protección de los sistemas, datos y servicios digitales de una entidad local. Más que una declaración de intenciones, es una herramienta operativa que guía tanto las acciones preventivas como las reactivas ante incidentes de ciberseguridad.

Los objetivos principales de una política de ciberseguridad municipal son:

- Proteger los activos digitales: asegurar la integridad, disponibilidad y confidencialidad de la información y los sistemas.

- Garantizar la continuidad operativa: minimizar el impacto de los incidentes de ciberseguridad en los servicios esenciales.

- Cumplir con las normativas aplicables: adaptarse a marcos como el Esquema Nacional de Seguridad (ENS) y el Reglamento General de Protección de Datos (RGPD).

- Fomentar una cultura de seguridad: promover prácticas responsables entre empleados y colaboradores municipales.

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

Una política de ciberseguridad municipal eficaz debe incluir componentes esenciales que aseguren la protección integral de los sistemas, datos y servicios. Estos componentes abarcan desde la identificación y gestión de riesgos hasta la capacitación del personal y el monitoreo continuo de la infraestructura tecnológica.

4.1. Gestión de riesgos

La gestión de riesgos es el pilar fundamental de cualquier política de ciberseguridad municipal. Este proceso permite a las entidades locales identificar y mitigar de manera proactiva las amenazas que puedan comprometer sus sistemas, datos y servicios. Dado que los recursos de los municipios son a menudo limitados, una gestión de riesgos efectiva ayuda a priorizar las inversiones y los esfuerzos en ciberseguridad.

La gestión de riesgos permite a las entidades locales adoptar un enfoque proactivo frente a las amenazas cibernéticas. Al identificar y abordar los puntos débiles antes de que sean explotados, los municipios no solo minimizan el impacto de los incidentes, sino que también optimizan el uso de sus recursos, enfocándolos en las áreas más críticas.

Inventario de activos críticos

Un paso inicial y esencial en la gestión de riesgos es realizar un inventario exhaustivo de los activos digitales del municipio. Esto incluye:

- Sistemas de información: plataformas de recaudación de impuestos, registros civiles, portales web municipales y otros sistemas críticos.
- Infraestructuras tecnológicas: servidores, redes, dispositivos de almacenamiento y sistemas SCADA utilizados en infraestructuras críticas como el suministro de agua o energía.
- Datos sensibles: información personal de los ciudadanos, datos financieros y otros registros confidenciales que deben protegerse.

El inventario debe clasificar estos activos según su importancia para la continuidad operativa y el impacto que tendría un incidente en cada uno. Por ejemplo, la base de datos de contribuyentes puede considerarse más crítica que un sistema de reservas para instalaciones deportivas.

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

Evaluaciones periódicas de riesgos

Una vez identificados los activos críticos, es necesario evaluar regularmente los riesgos asociados. Esta evaluación debe considerar:

- Amenazas externas: ataques de *ransomware*, intentos de *phishing*, accesos no autorizados desde el exterior o interrupciones por ataque de denegación de servicio distribuido (*Distributed Denial-of-Service*, DDoS).
- Vulnerabilidades internas: configuraciones incorrectas, *software* obsoleto o credenciales débiles.
- Impacto potencial: consecuencias económicas, operativas y reputacionales que podría tener un incidente.

Las herramientas de evaluación de riesgos, como matrices de probabilidad e impacto, ayudan a priorizar los problemas más urgentes. Por ejemplo, un análisis podría identificar que un servidor clave, aún operativo con un sistema operativo sin soporte, representa un riesgo crítico que debe abordarse de inmediato.

Planes de mitigación

Basándose en los resultados de la evaluación, los municipios deben desarrollar planes específicos para reducir los riesgos detectados. Estos planes incluyen:

- Actualización de sistemas: garantizar que el *software* y el *hardware* utilizados estén actualizados con los últimos parches de seguridad.
- Segmentación de redes: separar las redes críticas de los sistemas menos sensibles para limitar la propagación de ataques.
- Controles de acceso: implementar políticas de acceso restringido, asegurando que solo el personal autorizado pueda interactuar con sistemas críticos.
- Uso de herramientas de monitorización: implementar sistemas de detección de intrusos (IDS) o herramientas avanzadas de análisis de tráfico para identificar comportamientos anómalos.

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

Por ejemplo, tras evaluar el riesgo de un ataque de *ransomware*, un municipio podría priorizar la implementación de una política de copias de seguridad automatizadas, asegurándose de que los datos críticos puedan restaurarse rápidamente en caso de un ataque.

Gestión de riesgos como proceso continuo

La gestión de riesgos no es un ejercicio puntual, sino un proceso dinámico y continuo. Esto implica:

- Reevaluaciones periódicas: repetir el análisis a intervalos regulares o tras cambios significativos en la infraestructura, como la adopción de nuevas tecnologías.
- Adaptación a nuevas amenazas: mantenerse actualizado sobre las tendencias en ciberataques y ajustar los planes de mitigación según sea necesario.
- Integración con planes de contingencia: asegurar que las estrategias de gestión de riesgos estén alineadas con los procedimientos de respuesta a incidentes.

Un ejemplo práctico es la revisión anual de riesgos que realiza un municipio para actualizar su inventario de activos y ajustar sus prioridades de ciberseguridad en función de nuevos proyectos, como la digitalización de servicios ciudadanos.

4.2. Roles y responsabilidades

Una política de ciberseguridad municipal efectiva debe establecer claramente quién es responsable de cada aspecto de la seguridad, desde la planificación hasta la respuesta a incidentes. La claridad en los roles y responsabilidades no solo mejora la coordinación, sino que también asegura que todos los actores involucrados comprendan sus funciones y contribuyan a la protección de los activos digitales.

Responsables políticos

Los líderes políticos, como el alcalde y los concejales responsables de áreas tecnológicas, desempeñan un papel fundamental en la ciberseguridad municipal. Sus principales responsabilidades incluyen:

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

- Compromiso institucional: asegurar que la ciberseguridad sea una prioridad estratégica, destinando recursos adecuados y estableciendo políticas claras.

- Supervisión y aprobación: revisar y aprobar la política de ciberseguridad, así como los planes de contingencia y respuesta.

- Comunicación: informar de manera transparente a los ciudadanos sobre incidentes significativos, y las medidas adoptadas para resolverlos y prevenirlos.

Por ejemplo, el alcalde de un municipio podría liderar una iniciativa para certificar el cumplimiento del Esquema Nacional de Seguridad (ENS) y presentar los resultados en un pleno municipal.

Responsable de ciberseguridad (CISO)

El *Chief Information Security Officer* (CISO) o responsable de ciberseguridad es el encargado de implementar y supervisar la política de ciberseguridad. En los municipios más pequeños, esta función puede recaer en un técnico municipal con conocimientos específicos en seguridad digital. Sus funciones incluyen:

- Diseño e implementación: desarrollar y aplicar medidas técnicas y organizativas para proteger los sistemas y datos.

- Supervisión continua: monitorizar los sistemas para detectar y prevenir posibles amenazas.

- Gestión de incidentes: coordinar la respuesta ante ciberataques, incluyendo la comunicación con actores externos como CSIRT o proveedores tecnológicos.

- Capacitación del personal: liderar programas de formación y simulacros para preparar a los empleados ante posibles incidentes.

Un CISO en un municipio mediano, por ejemplo, podría liderar la instalación de herramientas de monitorización automatizada y garantizar que todos los empleados estén capacitados en las prácticas básicas de ciberseguridad.

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

Técnicos municipales

Los técnicos municipales desempeñan un papel operativo en la implementación de medidas de ciberseguridad y en la gestión de sistemas tecnológicos. Sus responsabilidades incluyen:

- Gestión de infraestructura: mantener los sistemas actualizados, aplicar parches de seguridad y gestionar las configuraciones de red.
- Monitorización activa: utilizar herramientas de detección para identificar actividades sospechosas.
- Soporte en incidentes: actuar como el primer nivel de respuesta técnica en caso de ciberataque.

Por ejemplo, un técnico municipal podría ser el encargado de restaurar un sistema comprometido utilizando copias de seguridad validadas.

Empleados municipales

Todos los empleados municipales tienen un rol en la ciberseguridad, incluso si no trabajan directamente con tecnologías, ya que sus acciones individuales pueden influir significativamente en la protección de los sistemas. Sus responsabilidades incluyen:

- Cumplimiento de políticas: seguir las directrices establecidas, como el uso de contraseñas seguras y la autenticación multifactor.
- Notificación de anomalías: informar de correos sospechosos, actividades inusuales o posibles brechas de seguridad.
- Formación continua: participar en talleres y simulacros organizados para mejorar su conocimiento y sus habilidades en ciberseguridad.

Un empleado que detecte un correo sospechoso de *phishing* y lo reporte de inmediato podría evitar que el incidente se convierta en un ataque mayor.

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

Colaboradores y proveedores externos

Los contratos con proveedores tecnológicos deben incluir cláusulas específicas de ciberseguridad para garantizar que estos cumplan con los estándares necesarios. Sus responsabilidades incluyen:

- Cumplimiento normativo: garantizar que los sistemas y servicios que proporcionan cumplen con el ENS y otras regulaciones aplicables.

- Soporte técnico: proporcionar asistencia en la configuración, el mantenimiento y la recuperación de sistemas críticos.

- Garantía de seguridad en la cadena de suministro: proteger sus propios sistemas para evitar que sean utilizados como vectores de ataque.

La seguridad en la cadena de suministro es fundamental para prevenir que las vulnerabilidades de los proveedores tecnológicos se conviertan en puntos de entrada para ciberataques, protegiendo así la integridad de los sistemas municipales y los datos sensibles que gestionan.

Un ejemplo reciente que ilustra la importancia de la seguridad en la cadena de suministro es el supuesto ciberataque a la Agencia Tributaria de España en diciembre de 2024. El grupo de piratas informáticos (no confundir con *hackers*) conocido como Trinity afirmó haber sustraído 560 GB de datos confidenciales de la Agencia, incluyendo información de contribuyentes, y exigió un rescate de 38 millones de dólares para no divulgar la información.

Sin embargo, la Agencia Tributaria negó haber detectado brechas de seguridad en sus sistemas y aseguró que todos sus servicios operaban con normalidad. Posteriormente, se indicó que una empresa privada externa, especializada en asesoría fiscal y laboral, podría haber sido la afectada, lo que sugiere que el ataque pudo haberse originado a través de un proveedor en la cadena de suministro.

Este incidente destaca la necesidad de que las entidades públicas y privadas garanticen que sus proveedores tecnológicos cumplan con estrictos estándares de ciberseguridad. La falta de medidas adecuadas en una empresa asociada puede convertirse en un punto de entrada para ciberataques que comprometan datos sensibles y afecten la integridad de los sistemas de la entidad principal.

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

Por lo tanto, es esencial que los contratos con proveedores incluyan cláusulas específicas de ciberseguridad y que se realicen auditorías periódicas para asegurar el cumplimiento de las normativas y la protección de la información en toda la cadena de suministro.

La colaboración entre estos actores es fundamental para una ciberseguridad efectiva. Por ejemplo, en caso de un incidente, el técnico municipal podría identificar el problema inicial, el CISO coordinaría la respuesta técnica y el alcalde informaría a los ciudadanos sobre las medidas adoptadas. Esta coordinación debe estar respaldada por protocolos claros que definan cómo interactúan los diferentes roles en situaciones normales y de emergencia.

La asignación clara de roles y responsabilidades no solo fortalece la capacidad de respuesta ante incidentes, sino que también fomenta una cultura organizativa orientada a la ciberseguridad. Cada actor, desde el responsable político hasta el proveedor externo, juega un papel indispensable en la protección de los sistemas y datos municipales, convirtiendo la ciberseguridad en un esfuerzo compartido.

4.3. Formación y sensibilización

El factor humano es considerado uno de los eslabones más vulnerables en la ciberseguridad. Por ello, la formación y la sensibilización de los empleados municipales y responsables políticos son componentes esenciales de cualquier política de ciberseguridad. Estas acciones ayudan a reducir los riesgos asociados con errores humanos y a fortalecer la cultura organizativa orientada a la protección de los sistemas y datos.

Invertir en la formación y sensibilización del personal no solo reduce los riesgos de ciberataques exitosos, sino que también promueve una cultura organizativa donde la seguridad es una responsabilidad compartida. Al combinar talleres, simulacros y campañas de concienciación, los municipios pueden convertir a sus empleados en una primera línea de defensa eficaz frente a las amenazas digitales.

Objetivos de la formación y sensibilización

La capacitación en ciberseguridad debe estar diseñada para lograr los siguientes objetivos:

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

- Incrementar la conciencia sobre las amenazas: ayudar a los empleados a identificar y comprender los riesgos asociados con prácticas inseguras.

- Promover comportamientos seguros: fomentar el uso de contraseñas robustas, la autenticación multifactor y el manejo adecuado de la información sensible.

- Facilitar una respuesta eficaz ante incidentes: asegurar que todos los empleados sepan cómo actuar en caso de un ciberataque, reduciendo el impacto y facilitando la recuperación.

- Fortalecer el compromiso de los responsables políticos: garantizar que los líderes municipales entiendan la importancia estratégica de la ciberseguridad y respalden las iniciativas necesarias.

Programas de formación continuos

La formación debe ser accesible, regular y adaptada a las funciones de los distintos empleados municipales. Algunos enfoques clave incluyen:

- Talleres básicos de ciberseguridad: Dirigidos a todos los empleados, estos talleres pueden cubrir temas como:

  - cómo detectar correos de *phishing*;

  - manejo seguro de contraseñas;

  - prácticas seguras en el uso del correo electrónico y de dispositivos conectados.

- Capacitación avanzada para técnicos municipales: Incluir temas como:

  - análisis de incidentes de seguridad;

  - configuración segura de redes y sistemas;

  - uso de herramientas de detección de intrusos y respuesta a incidentes.

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

- Sesiones específicas para responsables políticos: Asegurar que comprendan:
  - el impacto económico y reputacional de los ciberataques;
  - la importancia de destinar recursos adecuados a la ciberseguridad;
  - su rol en la comunicación con los ciudadanos en caso de incidentes.

Simulacros y ejercicios prácticos

Los simulacros son una herramienta poderosa para evaluar y mejorar la preparación del personal ante incidentes reales. Estos ejercicios deben incluir:

- Simulaciones de *phishing*: enviar correos falsos para medir cuántos empleados caen en el engaño y utilizar los resultados para reforzar la capacitación.
- Simulacros de ataques de *ransomware*: evaluar la capacidad del equipo técnico y de los empleados para contener el ataque y restaurar los sistemas.
- Ejercicios de respuesta en equipos interdisciplinarios: integrar a los responsables políticos, técnicos y administrativos en un escenario simulado para mejorar la coordinación y la toma de decisiones.

Un ejemplo exitoso es el de un municipio que, tras realizar un simulacro de *phishing*, detectó que más del 30 % de los empleados había hecho clic en un enlace sospechoso. Esto llevó a un refuerzo inmediato de la formación, reduciendo el porcentaje a menos del 10 % en un segundo ejercicio.

Campañas de concienciación

Además de la formación formal, las campañas de concienciación pueden mantener a los empleados alerta frente a las amenazas diarias. Estas campañas pueden incluir:

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

- Boletines informativos: enviar recordatorios periódicos con consejos de ciberseguridad, como “no compartas contraseñas” o “verifica los remitentes de correos electrónicos”.

- Material visual: colocar carteles en áreas comunes con mensajes clave, como “piensa antes de hacer clic”.

- Reconocimientos: premiar a los empleados que demuestren buenas prácticas de ciberseguridad, fomentando comportamientos positivos.

Personalización según roles

No todos los empleados municipales enfrentan los mismos riesgos o manejan información del mismo nivel de sensibilidad. Por ello, la formación debe adaptarse a las responsabilidades específicas de cada rol:

- Administrativos: centrarse en el manejo seguro de datos personales y cómo proteger documentos confidenciales.

- Técnicos: enfocarse en la configuración segura de sistemas y la gestión de incidentes.

- Directivos: enseñar la toma de decisiones estratégicas y la gestión de la comunicación ante incidentes.

Evaluación de impacto y mejora continua

Para garantizar la efectividad de la formación y sensibilización, es necesario medir su impacto y ajustarla según sea necesario. Esto puede incluir:

- Encuestas de conocimiento: evaluar periódicamente el nivel de conciencia sobre ciberseguridad entre los empleados.

- Análisis de incidentes: revisar cuántos incidentes han sido causados por errores humanos y ajustar la capacitación en consecuencia.

- Revisión de simulacros: identificar debilidades observadas durante los ejercicios y reforzar esas áreas específicas.

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

4.4. Implementación y monitorización

La implementación y la monitorización son los pilares que aseguran que la política de ciberseguridad municipal no solo quede como un documento formal, sino que también se traduzca en acciones concretas y efectivas. Este componente esencial abarca desde la planificación inicial hasta la supervisión continua, permitiendo ajustar estrategias según cambien las circunstancias o evolucionen las amenazas.

La implementación y la monitorización continua aseguran que la política de ciberseguridad sea más que un documento formal, convirtiéndola en una herramienta activa de protección. Al priorizar acciones, supervisar su cumplimiento y adaptarse a un entorno cambiante, los municipios pueden garantizar una protección sostenible y efectiva para sus sistemas y servicios.

Implementación estructurada

La implementación de la política de ciberseguridad debe ser un proceso planificado y estructurado que garantice su adopción efectiva en toda la organización. Los pasos clave incluyen:

1. Aprobación institucional:

    - La política debe ser aprobada por el órgano correspondiente (pleno municipal, junta de gobierno, etc.), asegurando su legitimidad y respaldo institucional.

    - Este proceso debe incluir una presentación clara de los objetivos y beneficios de la política para todos los actores implicados, desde responsables políticos hasta empleados.

2. Asignación de recursos:

    - Presupuesto: garantizar que se disponga de recursos financieros suficientes para implementar las medidas necesarias, como la adquisición de herramientas de ciberseguridad o la contratación de formación externa.

    - Personal: designar a un equipo o responsable técnico que lidere el proceso de implementación, asegurando que los roles y responsabilidades estén claramente definidos.

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

3. Priorización de acciones:

    - Comenzar por las medidas más críticas, como la actualización de sistemas, la implementación de controles de acceso y la formación inicial del personal.

    - Establecer un calendario realista que permita implementar la política en fases, reduciendo la presión sobre recursos limitados.

Monitorización continua

La monitorización es una actividad permanente que garantiza que las medidas implementadas se mantengan efectivas frente a nuevas amenazas o cambios en la infraestructura tecnológica. Los elementos clave de la monitorización incluyen:

1. Supervisión técnica:

    - Sistemas de detección de intrusos (IDS): herramientas que analizan el tráfico de red en tiempo real para identificar comportamientos anómalos o posibles intentos de ataque.

    - Monitorización de eventos: revisar los logs generados por sistemas críticos para detectar patrones sospechosos, como intentos de acceso fallidos o cambios no autorizados en configuraciones.

2. Auditorías periódicas:

    - Realizar auditorías internas o externas que evalúen el cumplimiento de la política y la efectividad de las medidas implementadas.

    - Estas auditorías pueden incluir simulacros de ciberataques, pruebas de penetración (*pentesting*) y revisiones de la infraestructura tecnológica.

3. Indicadores clave de desempeño (KPI):

    - Definir métricas para evaluar el éxito de la política, como:

        o tiempo promedio de detección de incidentes;

        o número de vulnerabilidades corregidas en cada revisión;

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

  - o porcentaje de empleados capacitados en prácticas de ciberseguridad.

- Utilizar estos indicadores para identificar áreas de mejora y justificar nuevas inversiones.

Actualización y adaptabilidad

El entorno de ciberseguridad es dinámico, con amenazas que evolucionan constantemente. Por ello, la política debe ser revisada y actualizada regularmente para reflejar:

- Cambios normativos: adaptarse a actualizaciones en el Esquema Nacional de Seguridad o nuevas regulaciones, como directivas europeas.

- Innovaciones tecnológicas: incorporar tecnologías emergentes que refuercen la seguridad, como herramientas de inteligencia artificial para la detección de amenazas.

- Lecciones aprendidas: ajustar estrategias tras la gestión de incidentes o los resultados de auditorías.

Un ejemplo práctico es la revisión anual que algunos municipios realizan de su política de ciberseguridad, incorporando hallazgos de simulacros o cambios en su infraestructura tecnológica, como la adopción de sistemas de teletrabajo.

Comunicación y transparencia

La implementación y la monitorización deben ir acompañadas de una comunicación efectiva que:

- informe regularmente a los responsables políticos sobre el estado de la ciberseguridad municipal, incluyendo logros, retos y necesidades;

- mantenga a los empleados al tanto de nuevas medidas o cambios en la política;

- en casos de incidentes, proporcione a los ciudadanos información clara sobre las acciones tomadas para resolver el problema y prevenir futuros ataques.

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

Buenas prácticas en implementación y monitorización

Algunos municipios han demostrado enfoques exitosos en este componente:

- Centralización de recursos: utilizar SOC regionales para monitorizar actividades y gestionar incidentes, optimizando recursos limitados.
- Integración con servicios externos: contratar servicios gestionados de seguridad que ofrezcan monitorización continua y respuestas rápidas a incidentes.
- Auditorías compartidas: participar en programas de revisión conjunta con otras entidades locales o Administraciones superiores para reducir costes y mejorar la eficacia.

5. Análisis DAFO

El análisis DAFO (debilidades, amenazas, fortalezas y oportunidades) es una herramienta estratégica ampliamente utilizada en la gestión organizativa, y en el ámbito de la ciberseguridad municipal resulta especialmente útil. Esta metodología permite a las entidades locales identificar y priorizar los factores internos y externos que afectan a su capacidad para prevenir, gestionar y responder a ciberataques. Además, el DAFO ofrece una visión clara y estructurada para tomar decisiones informadas y desarrollar políticas eficaces de ciberseguridad.

Debilidades

Las debilidades representan los factores internos que limitan la capacidad de una entidad local para protegerse contra ciberataques. Entre las más comunes destacan:

- Recursos humanos insuficientes: Muchas entidades locales, especialmente las más pequeñas, carecen de personal técnico especializado en ciberseguridad.
- Sistemas obsoletos: La falta de presupuesto para renovar infraestructuras tecnológicas deja a los municipios expuestos a vulnerabilidades conocidas.

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

- Falta de planes de contingencia: La ausencia de procedimientos claros para gestionar ciberataques dificulta la respuesta organizada ante incidentes.

- Baja formación del personal: Empleados municipales no capacitados pueden ser un punto de entrada para atacantes, especialmente a través de técnicas como el *phishing*.

- Dependencia de proveedores externos: La gestión delegada de sistemas críticos sin supervisión adecuada puede aumentar el riesgo.

Amenazas

Las amenazas representan los factores externos que pueden afectar negativamente la ciberseguridad de las entidades locales. Algunas de las más relevantes incluyen:

- Incremento en la sofisticación de los ataques: Los ciberdelincuentes utilizan herramientas avanzadas, como *ransomware* personalizado o ataques dirigidos (*spear phishing*), que son difíciles de detectar con sistemas tradicionales.

- Falta de coordinación interinstitucional: En algunos casos, la falta de colaboración entre Administraciones dificulta una respuesta rápida y efectiva a incidentes de gran magnitud.

- Regulación estricta y sanciones: El incumplimiento del Reglamento General de Protección de Datos o del Esquema Nacional de Seguridad puede derivar en sanciones económicas significativas tras un incidente.

- Escasez de soluciones tecnológicas accesibles: Las entidades pequeñas a menudo no tienen acceso a herramientas avanzadas de ciberseguridad, debido a sus costes.

Fortalezas

Las fortalezas son los elementos internos que aportan ventaja competitiva y pueden ser aprovechados para mejorar la ciberseguridad. En el caso de las entidades locales, algunas de las principales fortalezas incluyen:

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

- Proximidad a la ciudadanía: Permite una comunicación rápida y directa para gestionar incidentes y generar confianza en la respuesta adoptada.

- Colaboración interadministrativa: El proyecto RED ARGOS, en el que participan las comunidades de Andalucía, Castilla y León y País Vasco, tiene como principal objetivo contribuir a impulsar y fortalecer el ecosistema nacional de ciberseguridad y aumentar la adopción global de la misma, principalmente por empresas, basándose en la generación de capacidades especializadas, el trabajo en red de diferentes nodos de ciberseguridad regionales y la puesta en marcha de diferentes instrumentos de apoyo directo a las empresas.

- Acceso a subvenciones públicas: Programas de financiación específicos pueden facilitar la adquisición de herramientas y formación en ciberseguridad.

- Personal comprometido: Aunque falte especialización, muchos empleados muestran una gran disposición para adaptarse y mejorar sus competencias si reciben la formación adecuada.

Oportunidades

Las oportunidades son factores externos positivos que las entidades locales pueden aprovechar para mejorar su postura de ciberseguridad. Entre las más destacadas se encuentran:

- Avances tecnológicos: Soluciones basadas en inteligencia artificial y aprendizaje automático están haciendo más accesible la detección y respuesta a amenazas.

- Apoyo de organismos especializados: Entidades como INCIBE, CCN-CERT o iniciativas regionales proporcionan recursos técnicos y capacitación.

- Aumento de la sensibilización pública: Los ciudadanos son cada vez más conscientes de la importancia de la ciberseguridad, lo que facilita la implementación de medidas a nivel local.

- Programas europeos de ciberseguridad: La Unión Europea impulsa iniciativas y fondos para mejorar la ciberseguridad en Administraciones públicas.

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

Integración del DAFO en la planificación estratégica

El análisis DAFO no es un fin en sí mismo, sino una herramienta para orientar decisiones estratégicas. Una vez identificado el panorama interno y externo, las entidades locales deben:

1. Priorizar las áreas críticas: centrarse en abordar debilidades clave y contrarrestar las amenazas más inmediatas, como la actualización de sistemas o la formación del personal.

2. Explotar fortalezas y oportunidades: ampliar la colaboración con organismos especializados o participar en programas de financiación para implementar soluciones avanzadas.

3. Desarrollar planes de acción basados en el DAFO: integrar los resultados del análisis en políticas de ciberseguridad municipales y planes de contingencia.

Por ejemplo, un pequeño municipio que identifique como debilidad su falta de recursos técnicos podría priorizar acuerdos con su diputación provincial para acceder a servicios compartidos. Al mismo tiempo, podría aprovechar oportunidades como subvenciones autonómicas para financiar la capacitación de su personal.

El análisis DAFO permite a las entidades locales comprender su situación actual en materia de ciberseguridad y diseñar estrategias realistas y efectivas para mejorar su resiliencia. Al integrar esta herramienta en la planificación estratégica, los municipios no solo estarán mejor preparados para enfrentar ciberataques, sino que también podrán optimizar sus recursos y generar mayor confianza entre los ciudadanos y actores externos.

6. Conclusiones

Las entidades locales se enfrentan a un entorno cada vez más desafiante en términos de ciberseguridad. Su dependencia de infraestructuras tecnológicas, combinada con la responsabilidad de proteger datos sensibles y garantizar la continuidad de servicios esenciales, las coloca en una posición de riesgo elevado frente a ciberataques. Este capítulo ha proporcionado un marco integral para abordar estas amenazas, destacando tanto las acciones inmediatas como los elementos estratégicos necesarios para fortalecer la resiliencia.

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

Un resumen de los puntos clave para afrontar estos desafíos sería:

1. La importancia de la preparación y la planificación: La ciberseguridad debe ser vista como un proceso continuo que involucra no solo tecnología, sino también políticas claras, formación del personal y análisis estratégico. Contar con un plan de contingencia y continuidad operativa es fundamental para minimizar el impacto de cualquier incidente.

2. Pasos a seguir frente a un ciberataque: Desde la detección temprana hasta la recuperación, cada fase requiere protocolos bien definidos y una coordinación eficiente entre los actores implicados. La capacidad de aprender de cada incidente y ajustar las estrategias es clave para una mejora continua.

3. La política de ciberseguridad municipal como pilar estratégico: Este documento no solo guía las acciones preventivas y de respuesta, sino que también define responsabilidades, establece prioridades y asegura el cumplimiento normativo. Adaptar estas políticas a las características y los recursos de cada municipio es esencial.

4. El valor del análisis DAFO: Esta herramienta ofrece una visión clara de las debilidades y amenazas, pero también permite identificar fortalezas y oportunidades que pueden ser aprovechadas para mejorar la ciberseguridad municipal de manera realista y sostenible.

A la luz de los desafíos y soluciones presentados, se destacan las siguientes recomendaciones para las entidades locales:

- priorizar la formación y sensibilización del personal como elemento esencial para prevenir incidentes;

- fomentar la colaboración con organismos especializados y aprovechar los recursos disponibles a nivel regional y nacional;

- realizar evaluaciones periódicas de ciberseguridad mediante análisis DAFO para ajustar estrategias y priorizar inversiones;

- adoptar tecnologías avanzadas, como sistemas de detección automatizada, en función de las capacidades y necesidades específicas de cada municipio.

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

7. Bibliografía

Centro Criptológico Nacional y Federación Española de Municipios y Provincias. (2022). *Prontuario de ciberseguridad para entidades locales*. Disponible en https://ens.ccn.cni.es/es/docman/documentos-publicos/25-ccn-cert-prontuario-ciberseguridad/file.

Cotino, L. y Sánchez, M. (2021). *Guía de ciberseguridad para ciudades inteligentes*. Washington: BID.

Vila Avendaño, P. (2018). *Técnicas de análisis forense informático para peritos judiciales profesionales*. Madrid: OxWord.

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

CAPÍTULO IX

Comunicación preventiva. Cómo gestionar información en situaciones de crisis

César Fieiras Ceide
Profesor de Periodismo y Comunicación Audiovisual.
Universidad de Santiago de Compostela

Miguel Túñez López
Catedrático de Periodismo.
Universidad de Santiago de Compostela

1. Introducción: proactividad y estrés

Gestionar comunicación es gestionar credibilidad y confianza. En situaciones de crisis cambia el contexto de gestión y probablemente el contexto de recepción, pero este objetivo central debe reforzarse. Gestionar credibilidad no es contarlo todo, sino saber gestionar el mensaje. Rubenstein[1] recurre a una aparente paradoja para resumir la actitud que debe presidir la gestión preventiva: "La verdad nunca te va a perjudicar [...]. A no ser que te perjudique y no la sepas utilizar". Su propuesta es que cuando estamos ante una situación que nos perjudica, y que no podremos mantener oculta

1. En Rushkoff (2001).

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

ante la opinión pública, solo hay una salida: reconocer el problema, disculparse si es preciso, y, en actitud proactiva, planificar y ejecutar todas las acciones necesarias para que ese reconocimiento y esa situación acaben por incidir en un refuerzo de la imagen de la organización. En síntesis: gestionar proactivamente credibilidad a través de la veracidad y la honestidad de las actuaciones para fortalecer la confianza en la organización, en sus mensajes, en sus ideas, en sus productos, en sus dirigentes y en todo lo que esta representa.

Y ahí está uno de los elementos centrales: en momentos de crisis, la gestión de comunicación no puede realizarse de modo improvisado ni repitiendo las rutinas operativas de los momentos de normalidad, sino aplicando un plan de crisis diseñado anteriormente. Por eso, lo más importante en este caso es la capacidad de planificación previa: estar prevenidos para el momento, de modo que la gestión de crisis se pueda acompañar de una gestión ágil de la comunicación de crisis. En caso contrario, podría producirse un desajuste en los tiempos de actuación: la crisis avanza mientras la organización paraliza su comunicación buscando el mejor modo de ejecutarla, y cuando lo hace puede que los acontecimientos y el contexto hayan cambiado, y llegar tarde en la crisis es no llegar.

Al planificar debemos considerar que hay un componente emocional que también incide en el modo de implementar la comunicación. Cualquier amenaza genera una alteración psicológica que se traduce en un estado de incertidumbre y, en ocasiones, hasta de temor. Gestionar comunicación en situaciones de crisis significa asumir la gestión comunicativa de un riesgo en un contexto en el que es previsible que se den situaciones de estrés y un consiguiente aumento de la presión emocional, que puede alterar la capacidad de tomar o de ejecutar adecuadamente decisiones meditadas. También genera cambios en los contextos de recepción, que se ven alterados con tendencia a generar una hiperactividad social en redes.

La información aumenta la percepción de control en las personas que están en situaciones de incertidumbre y modifica sus emociones y conductas. Ante un acontecimiento relevante para nuestra vida, nos volvemos proactivos en la búsqueda de información. En esas circunstancias de incertidumbre, proporcionar información de utilidad contribuye a crear y sostener el liderazgo, porque la información suministrada contribuye a que los públicos den sentido a lo que ocurre, a la vez que difumina las percepciones erróneas que pueden originarse en situaciones ambiguas (García Álvarez, 2007: 225-226).

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

La tensión emocional puede ser un estímulo para afrontar los problemas mediante actuaciones moderadas orientadas a resolver la causa que genera esa tensión. Murphy (1959) dibujaba la incidencia de la tensión emocional en la resolución de conflictos como la silueta de una montaña; es decir, una primera etapa ascendente en la que el estrés emocional actúa como estímulo positivo, y una segunda descendente en la que la intensidad y el tiempo convierten el estrés en un factor negativo en la capacidad de gestión del conflicto. Así ocurre porque en ese estado de tensión se actúa de modo impulsivo para solucionar la situación de la manera más rápida posible, sin valorar la consecuencia a largo plazo (Holsti, 1987; Slatter, 1984). La curva o silueta que señalaba Murphy es una referencia mnemotécnica a tener en cuenta al elaborar el plan anticipado, porque debe preverse ese contacto entre actuación y percepción, y diseñar pautas de acción que eviten el riesgo de la etapa descendente.

2. Crisis en comunicación: amenaza de impacto de la imagen

En comunicación, una crisis es cualquier situación "natural o provocada, previsible o súbita, propia o ajena, declarada o latente", que supone una amenaza para la imagen o para la reputación de la organización, o para "las relaciones, internas o externas, entre esta y sus públicos o entre esta y sus miembros" (Túñez López, 2007: 53). Esa amenaza hace necesario que las organizaciones cuenten con estrategias planificadas de comunicación que ayuden a "evitar el impacto sobre la imagen, las relaciones y las actuaciones de la organización o, de producirse, minimizar el daño e intentar revertirlo como un activo positivo" (Túñez López, 2007: 54).

La gestión de la crisis desde las organizaciones se bifurca en una doble vía de acción: por un lado, las decisiones y acciones que permitan resolver la crisis, y, por otro, la comunicación de esas acciones y decisiones a todos los públicos vinculados con la organización y a la sociedad en general. El objetivo de la gestión de crisis es restablecer en la organización una situación de normalidad. El objetivo de la estrategia de comunicación en esa situación de crisis es, cuando menos, proteger la imagen interna y externa de la organización como un referente de credibilidad que genere confianza, y lograr que la reputación no quede dañada.

En general, las crisis pueden deberse a actuaciones de actores antagonistas, a decisiones propias de la empresa, a cálculos errados de gestión o al acontecer natural de las cosas. Las situaciones desfavorables, de riesgo o de conflicto, tanto pueden presentarse de forma inesperada como pueden permanecer latentes largo tiempo, estar causadas por decisiones de la

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

organización o por comportamientos de sus dirigentes o empleados, o deberse a fenómenos naturales. A modo de síntesis, diferenciamos tres tipos de amenazas que pueden desencadenar una crisis:

- **Amenazas previsibles**. Se pueden detectar a través de los sistemas de monitorización de alarmas, por la evolución del sector en el que desarrolla su actividad la organización y por las experiencias de organizaciones similares: a veces, los buzones de quejas, los libros de reclamaciones o los comentarios en redes sociales sirven de aviso. También lo hacen los análisis de evolución de mercado o de cambios sociales, y, entre otros, las encuestas sociológicas.

- **Amenazas provocadas**. Se desencadenan por una acción, premeditada o no, de la organización o de alguno de sus miembros. Son actuaciones programadas o la consecuencia previsible de actuaciones de riesgo de la entidad o de sus dirigentes.

- **Amenazas inesperadas**. Aparecen súbitamente y pueden ser naturales o provocadas por actuaciones de otras organizaciones, o incluso por miembros de la propia organización. También pueden deberse a errores en la gestión o en el manejo de las exposiciones públicas.

3. Anticipación y credibilidad, las claves

Las crisis son inevitables. Nadie quiere que se le asocie a una crisis, porque se identifica con vulnerabilidad, con cambios bruscos no deseados, con deficiencias de gestión, con estados de debilidad, con inestabilidad social, económica o personal, con conflictividad laboral, con una quiebra importante de la salud, con un desmoronamiento del sistema político, con la ruptura del consenso social, con las catástrofes naturales, con actuaciones ilícitas, y hasta con el caos.

En comunicación, hablar de gestión de crisis tiene matices diferenciadores, porque no se gestiona la crisis en sí, sino la comunicación que se realiza, y porque, bien ejecutada, debe ser la implementación de estrategias diseñadas y testadas con anterioridad para amortiguar impactos negativos sobre la imagen de la organización, de sus productos o servicios, o de sus dirigentes. Hablamos, por tanto, de anticipación en planes de comunicación preventiva: proyectas escenarios desfavorables para decidir cómo comportarnos del modo menos lesivo y cómo comunicar sin poner en riesgo la credibilidad de la imagen de la organización.

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

La velocidad de actualización, consumo y generación de respuesta en redes sociales es vertiginosa. También, en los medios, el tiempo de sus ciclos productivos es determinante. La persona que gestiona comunicación en situaciones de crisis ha de saber adaptarse a ellos a la perfección. En la crisis, ni hay tiempo para decidir cómo se va a proceder ni se puede improvisar. Por eso es fundamental contar con una planificación de comunicación bien fundamentada, de modo que las energías y el tiempo se inviertan de lleno en comunicar siguiendo el ritmo de evolución de la propia crisis, y no en decidir cómo se debería actuar en ese momento para mitigar su impacto.

Las crisis no comienzan cuando se hacen visibles para los públicos porque los medios empiezan a informar sobre ellas, ni se solucionan solo a través de herramientas de *publicity* o con el manejo de relaciones informativas. La repercusión de la crisis en medios y en soportes ajenos (no vinculados a la propia organización) es la dimensión pública del problema, y se identifica con la fase que más daño puede causar en la imagen o en la reputación de la entidad afectada por la crisis.

La comunicación de crisis es una planificación previa que se encara a largo plazo y que, por precaución, se inicia antes de que se desencadene el conflicto; se implementa durante la crisis trabajando con anticipación, agilidad, calidad y veracidad (Villafañé *et al.*, 1987); y se prolonga en el tiempo cuando esa situación desfavorable ya ha pasado, actualizando el plan y verificando su utilidad. Es, por tanto, una actuación que comienza siempre anticipadamente con una intencionalidad preventiva. Las personas expertas en gestionar comunicación de crisis coinciden en señalar que una buena manera de amortizar la inversión en comunicación de crisis es tener un plan detallado y realista, y que nunca llegue el momento de usarlo.

La gestión de la comunicación en situaciones de crisis parte de una actitud preventiva que se transforma, llegada la crisis, en una actitud proactiva, y, tras la crisis, evaluativa. El esquema es, sobre el papel, sencillo:

- **Precrisis: anticipación**. Planificar con detalle antes de que el conflicto se presente y diseñar todas las actuaciones que habrá que llevar a cabo para superarlo con éxito. Es el momento de sentar las directrices generales, decidir el papel que desarrollará el máximo mandatario según la intensidad que pueda adquirir la crisis, y planificar y simular con todo detalle la aplicación del plan de comunicación.

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

- **Crisis: actuación**. Es el momento de implementar las actuaciones previstas en el plan de comunicación, de actuar conforme a lo planificado, teniendo en cuenta de modo estratégico la evolución de la situación y el comportamiento de los demás actores implicados en la crisis.

- **Postcrisis: evaluación**. Investigación y evaluación de lo que ha ocurrido, de las reacciones ante cada hecho, de la efectividad de las medidas. Se trata de aprender de la experiencia para volver a prevenir, reformulando el plan y simulando de nuevo su aplicación.

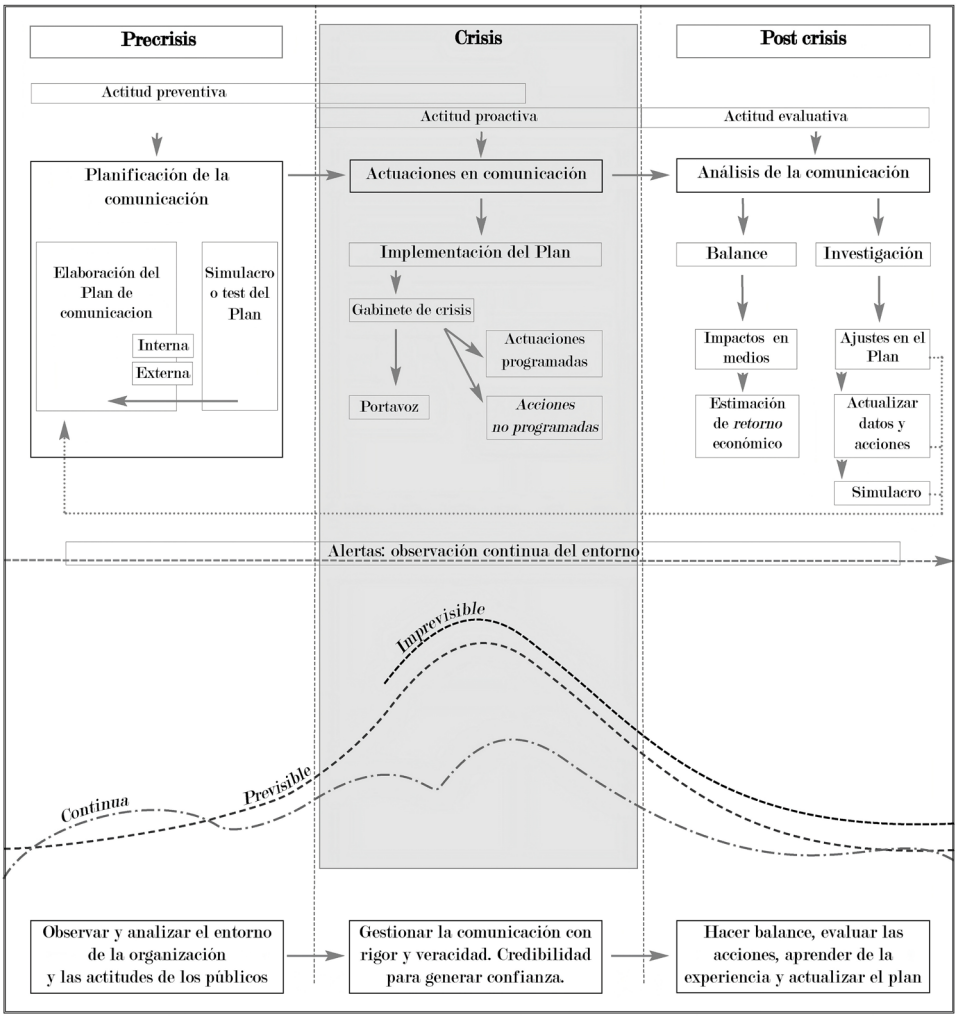


Figura 01. Fuente: Túñez López (2012: 192).

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

La intervención en comunicación de crisis comienza antes de que la crisis aparezca. Anticiparse es atender a los indicadores que pueden advertir de la posibilidad de una situación desfavorable para la organización y proyectar cómo comunicar en esa situación. En esta fase previa es cuando se elabora el plan de comunicación y se ensaya su efectividad, para asegurarnos de que las actuaciones están bien diseñadas y si cada uno de los actores involucrados conoce cómo, cuándo y dónde debe intervenir.

Los simulacros son una puesta en escena de las actuaciones en situaciones de crisis sin el riesgo de que los errores de planificación o de ejecución dañen el funcionamiento o la imagen de la organización. Cuando la crisis se presenta es el momento de actuar con dinámicas aprendidas, porque no es posible congelar la crisis mientras se lee el plan y se determina qué se debe hacer.

La anticipación es una tarea ardua que se ve limitada por la capacidad de proyección real de la situación. El contexto en el que va a desarrollarse y las reacciones de los implicados fundamentan el plan de actuación. Es deseable que sea una proyección rigurosa que permita prever planteamientos globales, de modo que todo el comportamiento futuro en la crisis sea coherente, pero no lo agota ni lo limita.

La implementación de un plan precisa siempre del monitoreo de reacciones de los públicos destinatarios y de los agentes implicados, y más en situaciones de crisis, en las que es necesario estar alerta para gestionar las variaciones que se puedan producir al margen de los supuestos preventivos. Es habitual porque se trabaja con intangibles en un entramado sistémico en el que el resultado de las acciones no solo depende de lo que una organización hace, sino también de la interacción con otras organizaciones, y, en ocasiones, de las acciones de otras entidades ajenas que acaban impactando sobre nosotros.

4. Actitud y estrategia ante la crisis

El auge de la comunicación preventiva se sitúa en las últimas décadas del siglo XX, aunque podemos remontar sus orígenes hasta los primeros pasos de las relaciones públicas, cuando, a principios del siglo XX, Ive L. Lee decide romper con la dinámica del "todo vale" que marcaba la actuación de los denominados "agentes de prensa" de finales del siglo XIX, y acuña la máxima de que cuando no puedes contar a los medios lo que la organización está haciendo lo efectivo no es engañar a los medios y a los públicos con un re-

lato favorable de lo que acontece, sino cambiar los modos de actuar de la organización[2].

Más de un siglo después, la recomendación sigue inalterable. La comunicación no garantiza la solución satisfactoria de todas las crisis, pero una buena gestión de comunicación en situaciones adversas puede hacer que el impacto no se agrave y que se revierta la situación hasta conseguir un reforzamiento de la imagen, siempre que las organizaciones acepten que han de asumir abiertamente las responsabilidades que correspondan y difundir únicamente mensajes veraces y claros para que todas las actuaciones de la organización sean creíbles.

La pandemia de COVID-19 puso en evidencia a nivel planetario la necesidad de contar con planes de comunicación preventiva. Los devastadores efectos de la DANA en Valencia en 2025, o el apagón general de ese mismo año, son dos muestras de cómo la realidad deja ejemplos continuos de situaciones de crisis en las que la gestión de la comunicación acaba siendo eje del debate. ¿Qué hacer cuando la crisis está desencadenada por un ciberataque? La respuesta es una sola: activar el protocolo de comunicación preventiva con las acciones que más se ajusten a los escenarios recreados en el momento de elaborarlos y al escenario real.

No hay dos crisis iguales ni una recomendación única para todos los supuestos de un mismo sector. Hay, eso sí, que contar con protocolos que deben mantenerse como referencia inequívoca de las actuaciones orientadas a todo tipo de públicos: anticipación y veracidad para generar confianza, confirmada a través de una irrenunciable actitud de compromiso con la exactitud de las informaciones que se ofrecen; elegir los canales y seleccionar los medios informativos que mejor permitan comunicarse con todos los públicos afectados; intentar lograr el control del mensaje que se transmita y convertirse en la referencia central de ese mensaje, aportando información de interés para el medio y suministrando información con frecuencias marcadas y, siempre que sea posible, ajustadas a las rutinas productivas de los medios, para que la procesen y la incluyan en sus temarios.

La actitud inicial de la organización ante la causa de la crisis definirá el rumbo de las intervenciones posteriores. La prevención obliga a identificar supuestos de comportamiento y a decidir roles para fijar la estrategia que resulta más conveniente en cada supuesto. De un modo general, podría-

2. Lee gestionaba la comunicación de la huelga de mineros de 1906, en Estados Unidos. Publicó una declaración de principios en la que se comprometía a ser veraz, transparente e inmediato en sus informaciones a la prensa y a la sociedad.

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

mos considerar que se mantiene vigente la diferenciación de Fita al señalar cuatro posicionamientos de partida: callar, negar, asumir o transferir. La crisis deja, en realidad, pocas opciones de elegir para no ir en contra de la recomendación principal de asumir los hechos y gestionar con honestidad, sin poner en riesgo la confianza en la organización y en sus portavoces. Aun así, esas cuatro opciones serían (Fita 1999, 2004).

- **El *silencio***. No se comenta ni se informa. Solo sería recomendable en crisis de muy baja intensidad que no afecten directamente a la organización. La inactividad no es recomendable porque siempre habrá otros actores, a veces antagonistas, que aprovechen la situación para hacer prevalecer su versión y modelar un relato favorable de la situación. La opción de aplicar estrategia de silencio es factible cuando se pueda prever que al romperla se agigantan dinámicas informativas que amplifiquen la exposición pública de la crisis.

- **La *negación***. La comunicación se centra en mensajes que nieguen la implicación o cualquier vinculación o participación en los hechos que provocan la crisis. Las negaciones como mensaje principal pueden tener fisuras si en alguno de los aspectos de la crisis se evidencian puntos débiles o argumentalmente inconsistentes, porque ello afectaría directamente la credibilidad y erosionaría la confianza en el resto de los argumentos y de las acciones. Las ambigüedades y las dificultades para garantizar que la recepción del mensaje se hace con todos los matices intencionales que se manejen al codificarlo hacen que sea una estrategia cuestionable y solo aplicable en casos que permitan una negativa con fundamentaciones sólidas, nunca como evasión.

- **La *transferencia de responsabilidades***. La organización no solo niega su implicación en la crisis, sino que deriva esa responsabilidad a un tercero. Solo cabe recomendar esta estrategia cuando esa transferencia de responsabilidades sea rotundamente cierta y se pueda demostrar públicamente. Activarla implica aumentar la controversia y el interés sobre la propia crisis, porque se promueve la respuesta de las organizaciones señaladas y la de otros actores de su órbita.

- **La *confesión***. Aparentemente podría parecer la menos recomendable, pero en supuestos de crisis acaba siendo la más eficaz, sobre todo cuando es inevitable que algo desfavorable se sepa. La organización asume su parte de responsabilidad en la crisis, explica cómo

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

le afecta, gestiona con veracidad la información que hace pública, y actúa de modo que pueda amortiguar el impacto de la crisis[3]. También se diseñan acciones que contrarresten ese impacto negativo y ayuden a preservar la imagen de la amenaza o del daño.

5. El plan de comunicación de crisis: gestionar reputación

Cada crisis es diferente a las anteriores, y no hay un modelo único que permita pautar los comportamientos recomendables en cada caso. Antes de que la crisis aparezca es el momento de diseñar el plan, evaluar la evolución del sector, atender a los avisos de los públicos, vigilar qué ocurre en otras organizaciones; pero ¿qué hacer cuando la crisis se desencadena? Partiendo de las consideraciones generales, podemos señalar un sencillo protocolo que nos puede ayudar a afrontarla: seguir alerta, identificar la crisis, reunir el comité, ejecutar el plan diseñado y testado con anterioridad para informar a los *stakeholders* con rapidez, veracidad y transparencia, y evaluar la idoneidad de las actuaciones ejecutadas una vez que la crisis se haya solucionado. Resumiendo: activar gabinete, ejecutar el plan y evaluar.

5.1. Constituir el gabinete

El primer paso ante la crisis es activar el gabinete de crisis y mantener la vigilancia. Las crisis se gestionan de modo más eficaz con mitradas poliédricas, por lo que es recomendable planificar la gestión como la responsabilidad de un reducido equipo multidisciplinar. Los equipos de comunicación de crisis han de tener un único responsable claramente identificado; estar en conexión directa con el principal responsable de la organización y con el responsable jurídico de la organización.

Previamente, al elaborar el plan de actuación y contingencia, ya se ha decidido quiénes integran el gabinete de crisis, y se han explicitado las funciones de cada uno. También debe estar decidido dónde se reúne, es decir, dónde se ubicará en centro de control de operaciones, y cuáles son los recursos tractivos disponibles. Este espacio no solo permite desarrollar la actividad, sino que se convierte en una ubicación referencial para estar localizable para los demás miembros de la organización involucrados o afectados por la crisis.

3. "Lo siento mucho. Me he equivocado. No volverá a suceder", es un mensaje que ha quedado fijado como síntesis de manual.

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

5.2. Implementar el plan

El plan de comunicación de crisis es la referencia de actuación en función de la naturaleza y la intensidad de la crisis. Como en el plan estratégico de comunicación, puede haber un plan global y previsiones de actuación en supuestos concretos que irán dirigidos a todos los públicos de la organización, internos y externos.

En algunos casos, las crisis se gestionan a través de los medios de comunicación propios y ajenos, incluidas las redes sociales, lo que significa un manejo del contacto con la audiencia en un intento de proteger globalmente la imagen de la organización. La táctica es buena, pero no ha de ser la única. Hay públicos que requieren especial atención. "No podemos transmitir transparencia, responsabilidad y control si tenemos 'descontrolada' nuestra primera audiencia que además puede convertirse en portavoz de la compañía sin pretenderlo" (Hortas, 2007: 151). Los empleados, los socios o los miembros de una organización no deben enterarse a través de los medios de comunicación de la existencia de una crisis y del papel que está desempeñando la entidad en esa situación.

Algunas organizaciones están obligadas a seguir protocolos de comunicación en situaciones de riesgo o en caso de accidente. Son actuaciones encaminadas a proteger la salud pública, y suelen ceñirse a empresas cuya actividad genera un riesgo potencial de impacto sobre la población. Los protocolos definen en cada caso cómo, quién y cuándo debe informarse a autoridades, entidades sanitarias, fuerzas de seguridad, trabajadores, etc.

En estos casos, la gestión de la comunicación de crisis ha de tener en cuenta los flujos y ritmos internos, no siempre acompasados al devenir de los hechos, o a las velocidades de actualizaciones de contenidos en medios o en redes sociales. Si hay un posible impacto de ese episodio sobre la sociedad y si es generador de alarma, debe combinarse la prioridad informativa de la organización con la necesidad de información que se despierta en la audiencia, y atenderse siempre a realizar una descripción del acontecimiento, explicar por qué es potencialmente peligroso, manejar con cuidado la emoción del miedo como motivación, anticipar la evolución prevista, anunciar y comprometer un nuevo contacto informativo en un plazo concreto que se ha de respetar estrictamente (García Álvarez, 2007: 227).

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

5.3. Evaluar resultados

El éxito de la estrategia de crisis puede decirse que está en su planificación, pero se mide por los resultados. Hacer balance no es preparar una relación de méritos, sino testar la efectividad de las previsiones de actuación una vez ejecutadas, para determinar propuestas que deben incorporarse a las rutinas de gestión e identificar aspectos que se revelaron débiles o inoperantes, y descubrir por qué no fueron válidos. Analizar resultados es el modo de comenzar a planificar próximas intervenciones ante otras crisis.

6. Herramientas. La meta es la salida

Los entornos *online* son cada vez más un escenario de participación colectiva, sobre todo por el papel *prosumer* de los públicos y la universalización de aplicaciones que permiten codificar y gestionar el envío de mensajes, así como por la popularización de herramientas de inteligencia artificial que multiplican estas opciones. Los bots se han convertido en un aliado en la gestión para el manejo de relaciones en entornos *online*, pero también en una amenaza disruptiva cuando se orientan desde entidades agitadoras a la irrupción en la crisis con intenciones que distorsionen las referencias de veracidad y agiten la crisis.

En cualquier caso, para el diseño de un plan de crisis la referencia general es revisar todos los aspectos que integran un plan de comunicación reforzando el control y el rigor de las actuaciones, aunque se haga de un modo preventivo con antelación. Es necesario, por tanto, tener en cuenta:

- **Contexto**. La organización no actúa aislada. No solo es necesario conocer su funcionamiento, sino también el entorno social y económico del sector en el que se desarrollan sus actividades. También debe reseñarse cómo conocer y monitorizar el contexto de recepción, es decir, los indicadores de comportamiento y actividad de los públicos y de todos los actores que puedan incluirse como dinamizadores en la difusión de información u opiniones sobre la crisis.

- **Autodiagnóstico**. Toda organización conoce sus puntos débiles. Sin embargo, la identificación de fortalezas y debilidades de la organización puede verse alterada en contextos de crisis. El análisis debe hacerse desde la comunicación, no desde la entidad.

- **Circuitos informativos**. La identificación de canales y los flujos informativos internos y externos. Diseño de nuevos que permitan

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

contacto con públicos para satisfacer necesidades informativas y dar mayor agilidad en la respuesta. Diseñar los flujos también sirve para determinar supuestos de respuesta y el perfil bajo, medio o alto de quien responde, y para fijar el uso de recursos de modo que esos flujos sean lo más efectivos posible (móvil, redes, mail...).

- **Metas**. Son el punto de partida del plan. Primero, qué queremos conseguir, y después, todo lo demás. Las acciones comunicativas se diseñan para lograr un objetivo concreto. Es fundamental determinar qué se pretende alcanzar con la estrategia de crisis: proteger la marca, el producto o las personas, etc., y jerarquizar resultados deseados identificando objetivos prioritarios y secundarios en entornos internos y externos, de modo que llegado el momento esté claro qué metas son más importantes para la organización.

- **Elenco**. Anticiparse es también identificar quién podría intervenir en la crisis y cómo se posicionaría: aliados, adversarios, neutrales (indiferentes) e imprevisibles. La identificación de posibles partícipes en la crisis debe ir acompañada de la lista de contacto con todas/os, incluidos los agentes internos con responsabilidad en la gestión de crisis y todas las personas que de alguna manera están presentes en los flujos de comunicación interna y externa que se activen.

- **Públicos y audiencias**. Es necesario anticipar cuáles van a ser los públicos afectados o involucrados en la crisis y medir sus posibles reacciones, e incluso las posibilidades de que evolucionen hacia público hostil, tanto en la fase de planificación como durante el desarrollo del conflicto. Quiénes son y dónde y cómo se comportan: Es esencial establecer los focos de atención en internet, prestando atención especial a las reacciones de los públicos en redes, foros, blogs y comentarios a las noticias de los medios de comunicación. Es evidente que interesa definir, de todos los públicos, cuál será el segmento hacia el que se dirijan las principales actuaciones de protección de la imagen, para determinar ámbitos de cobertura mediática y los canales/soportes a priorizar.

- **Apoyos externos**. Los apoyos externos pueden venir de las actuaciones de los actores aliados, pero también del impulso de voces coincidentes, o, si se prevé una crisis prolongada o de alto impacto social, puede fomentarse la irrupción en el panorama mediático de una autoridad de referencia con credibilidad en el tema, que no se vincule directamente con la organización, pero que sostenga un

discurso en línea con los intereses de esta. Se verá como una, lo que reforzará la aceptación del mensaje de la organización.

- **Proactividad y reactividad**. Comunicar es el manejo de iniciativas para ser referencia en la propuesta de argumentos narrativos o para responder a las propuestas que hacen otros. El plan define los supuestos de actitud de silencio, y cuándo se debe ser reactivo, manteniéndose a la espera y actuando en función de cómo evolucione la crisis, o proactivo, tomando la iniciativa en las actuaciones informativas directas o indirectas.

- **Alcance**. La dimensión externa de la crisis acaba siendo visible por su repercusión en los medios de comunicación ajenos. Es conveniente, pues, hacer una previsión de las posibilidades reales de la crisis y sus diferentes formas de evolución e impacto.

- **Medios ajenos**. En función del alcance estimado, se identifican cuáles son los medios externos que deberíamos tener en cuenta, sus estructuras, sus contenidos, y las personas a las que se deben dirigir las propuestas que lancemos. Los gabinetes acostumbran a trabajar con un doble mapa mediático: atendiendo a la zona de cobertura geográfica y en función de la vertebración de contenidos del medio, para calibrar el alcance real de las informaciones sobre la organización y para hacer estimaciones de cuál puede ser la evolución informativa de la crisis.

- **Argumentarios**. El plan esboza los argumentos que se van a utilizar, que se plasman por escrito para que sean asumidos por los actores involucrados, como referencias a seguir para mantener un discurso convergente. También se puede definir la posición oficial de la organización de la que se derivan los argumentarios.

- ***Publicity***. En la crisis, la credibilidad aumenta cuando el mensaje aparece derivado; es decir, cuando se refleja en medios que no son los propios de la organización. El manejo de relaciones con los públicos a través de medios ajenos cobra importancia; por eso es oportuno tener en cuenta que para ejecutar acciones mediante *publicity* es necesario que primero se identifiquen las necesidades informativas de los medios en los que se pretende impactar y que las propuestas se ajusten a esas necesidades.

- **Oratoria y kinésica**. También es recomendable preparar (incluso ensayar) las comparecencias ante los medios o directamente ante

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

los públicos; responder siempre, pero sin improvisaciones; entrenar al portavoz para el dominio de la oratoria, la kinésica y la escenografía, y para que use un lenguaje claro, sin ambigüedades, sin supuestos y sin especulaciones. Los medios no son enemigos ni están al servicio de la organización; su rol es cuestionar el discurso en situaciones de conflicto, y más en un momento en el que la competencia entre medios y entre fuentes/actores se refuerza con la universalización de la capacidad de ser emisor y con la potencial posibilidad de transcomunicación a través de la glocalización de internet.

- **Publicidad**. Si las propuestas informativas no tienen el impacto deseado en medios (da igual si se debe a errores de planificación estratégica o al éxito de acciones de comunicación de antagonistas en la crisis), es deseable tener diseñada una campaña publicitaria para poder actuar con rapidez o por si simplemente se ve necesario un refuerzo de la estrategia informativa. Comunicación no gestiona la crisis, pero debe proponer acciones que permitan generar mensajes o sentimientos favorables. Acciones de refuerzo o propuesta de gestión que se realizan desde el impacto sobre la imagen y están diseñadas atendiendo no tanto a las necesidades de la organización, sino a las prioridades informativas.

- **Presupuesto**. Toda acción necesita personal que la ejecute y genera un gasto. La comunicación preventiva comienza por ser capaces de calcular los recursos económicos y humanos de los que sería necesario disponer para mantener el normal funcionamiento de la organización y gestionar a la vez una crisis. El análisis ha de ser realista y debe comparar esas necesidades con la disponibilidad de ambos recursos para prever formas y mecanismos de actuación realizables.

Con el plan de comunicación se planifica el modo de abordar comunicativamente la crisis, y se definen las acciones, así como el modo y la oportunidad de llevarlas a cabo. También se diseña la estrategia de implementación, porque es el modo de anticipar supuestos para —con el sentido de oportunidad— calibrar la mejor manera de ejecutar el plan en función de las circunstancias.

7. Crisis por ciberataque… y nada cambia

Un nuevo entorno y un catálogo diferente de situaciones adversas que pudieran producirse en diferentes grados, pero no se alteran las bases de la

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

prevención comunicativa, solo corresponde ajustarla a la proyección de escenarios posibles para tener calibradas de antemano cuales serían las opciones de respuesta más ajustadas en cada situación.

Seguramente esta capacidad de anticipación en el diseño de situaciones de crisis cobre más importancia porque hablamos de ritmos de ejecución y de propagación vertiginosos, en los que el tiempo de reacción se reduce tanto que es difícil pensar en tener capacidad de respuesta sincrónica si no hay una eficaz anticipación preventiva que permita no solo esa reacción, sino también el manejo de la estrategia de implementación con criterios de oportunidad que ajustan las acciones al conocimiento e interpretación de los agentes implicados: provocan o sufren.

Podría parecer que todo es diferente: escenarios, actores, procesos, entornos, herramientas..., pero en síntesis la dinámica de crisis en ciberseguridad se remite al proceso de anticipar para actuar.

Seguramente por la temática, su incidencia y el nivel de penetración social de los entornos *online* se haga necesario perfilar acciones de comunicación centradas en ciberseguridad, y orientadas a acciones de formación y de divulgación con una intencionalidad de alfabetización que no solo aproxima al concepto, sino que también permite poner en práctica nuevos modos de comportarse y de llevar esa dinámica de anticipación preventiva a supuestos de acción que en realidad sean acciones preventivas orientadas a comportamientos seguros.

Esa es otra de las aristas de la comunicación: la "edu-comunicación". La comunicación como herramienta para la capacitación, la formación y la concienciación de todos los actores implicados —empresas, instituciones, usuarios...— es una prevención de doble filo: actúa como garantía de acciones correctas y como escudo ante simulaciones que se apropien de códigos de veracidad para promover situaciones de engaño.

Desde una perspectiva de gestión de comunicación de crisis, la atención se debe centrar en el ajuste a normativas y protocolos legales para el cumplimiento de las disposiciones vigentes y en el manejo de relaciones institucionales y organizacionales, pero el protocolo de actuación no se desmarca de las recomendaciones generales porque, independientemente de la causa y del sector, se procede a gestionar comunicación y, con la comunicación, a gestionar las relaciones de públicos/audiencias y entidades/organizaciones.

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

El listado que sintetiza los pasos ya explicados podría condensarse en los siguientes puntos:

- Prevención y anticipación en el diseño de un plan en el que se marquen claramente los objetivos que se persiguen con las actuaciones que se diseñen.

- Definición e identificación del equipo gestor de la crisis y del que se encargará de la comunicación durante la crisis, sus integrantes, la cadena de mando en la asunción de responsabilidades, sus roles, su ubicación y los modos y canales de comunicación internos y externos.

- Una previsión de escenarios de desarrollo de la crisis con el consiguiente análisis de gestión de riesgos en cada uno de ellos.

- Identificación de los públicos afectados y de los públicos prioritarios en las acciones de la organización.

- Diseño de las acciones para el complimiento de objetivos y, en cada caso, los mensajes y canales.

- Identificación de los sistemas de monitorización y alerta que será preciso mantener activos para estar al tanto de la evolución del impacto de la crisis.

- Borrador del mapa de escenarios para testar previamente cómo reaccionar ante las distintas evoluciones de los acontecimientos y para generar respuestas flexibles a entornos de gestión de crisis que van a ser cambiantes por la influencia del entorno, las acciones de otros implicados y la coparticipación social en plataformas *online*.

- El plan se diseña y se testa a través de simulacros. En entornos tan cambiantes como el ciberespacio, las revisiones y actualizaciones deberían ser constantes y no limitarse a ajustes en el plan, sino a la experimentación de la idoneidad de esos ajustes a través de la implementación de simulacros constantes.

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

8. Bibliografía

Alameda García, D. (2006). *Una nueva realidad publicitaria. La generación de valores corporativos en publicidad*. Madrid: Laberinto.

Andrade, H. (2005). *Comunicación organizacional interna: proceso, disciplina y técnica*. Coruña: Netbiblo, serie Comunicación Empresarial.

Arroyo, L. y Magali, Y. (2007). *Los cien errores de la comunicación en las organizaciones*. Madrid: Esic.

Barquero Cabrero, J. D. (2005). *Comunicación estratégica. Relaciones Públicas, Publicidad y Marketing*. Madrid: McGraw Hill.

Best, R. J. (2007). *Marketing estratégico*. Madrid: Pearson Educación.

Castelló Martínez, A. (2010). *Estrategias Empresariales en la web 2.0. Las redes sociales online*. Alicante: Editorial Club Universitario.

Celaya, J. (2008). *La empresa en la web 2.0*. Madrid: Gestión.

Chaves, N. (2005). *La imagen corporativa. Teoría y práctica de la identificación institucional* (3.ª ed.). Barcelona: Gustavo Gili.

Costa, J. (2009). *El DirCom hoy. Dirección y Gestión de la Comunicación en la nueva economía*. Barcelona: Costa Punto Com.

Fernández, F. y Barquero, J. D. (2004). *El libro azul del protocolo y las relaciones públicas*. Madrid: McGraw Hill.

Fita, J. (2004). Comunicación de crisis. En J. C. Losada Díaz (coord.). *Gestión de la comunicación en las organizaciones* (pp. 193-216). Barcelona: Ariel Comunicación.

Galindo Rubio, F. (2004). *Comunicación audiovisual corporativa. Cómo audiovisualizar la identidad de las organizaciones*. Salamanca: Universidad Pontificia.

García Álvarez, M. A. (2007). Apuntes sobre comunicación en emergencias y catástrofes. En M. Túñez López (coord.). *Comunicación preventiva. Planificación y ejecución de estrategias de información interna y externa ante situaciones de crisis*. A Coruña: Netbiblo.

González Herrero, A. (1998). *Marketing preventivo: la comunicación de crisis en la empresa*. Barcelona: Bosch Comunicación.

González Solas, J. (2002). *Identidad visual corporativa. La imagen de nuestro tiempo*. Madrid: Editorial Síntesis.

Gutiérrez-García, E. (2010). Gobierno corporativo y comunicación empresarial. ¿Qué papel cumplen los directores de comunicación en España? *Palabra Clave*, 13 (1). Disponible en http://www.scielo.unal.edu.co/scielo.php?script=sci_arttext&pid=S0122-82852010000100010&lng=en&nrm=iso.

Holsti, K. J. (1987). America meets the "English School": State Interests in International Society. *Mershon International Studies Review*, 41, 275-280.

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

Hortas, P. (2007). La comunicación de empresa ante una crisis. En M. Túñez López (coord.). *Comunicación preventiva: planificación y ejecución de estrategias de información interna y externa ante situaciones de crisis*. La Coruña: Netbiblo.

Lattimore, D., Baskin, O., Heiman, S. y Toth, E. (2008). *Relaciones públicas. Profesión y práctica*. México DF: McGraw Hill.

Lucas Marín, A. (1997). *La comunicación en la empresa y en las organizaciones*. Barcelona: Bosch Comunicación.

Meerman Scott, D. (2008). *As novas regras de Marketing e Relaçoes Públicas* [traducción al portugués: Vasco Mota Pereira]. Porto: Ideas de Ler.

Murphy, R. E. (1959). Effects of threat of shock, distraction, and task design on performance. *Journal of Experimental Psychology*, 58 (2), 134-141.

Regester, M. y Larkin, J. (1997). *Risk Issues and Crisis Management. A Casebook of Best Practice*. Kogan Page.

Robbins, S. P. y Judge, T. A. (2009). *Comportamiento organizacional* (13.ª ed.). México: Pearson.

Rushkoff, D. (2001). *Coerción. Por qué hacemos caso a lo que nos dicen*. Barcelona: La Liebre de Marzo.

Saló, N. (2005). *Aprender a comunicarse en las organizaciones*. Barcelona: Paidós.

Slatter, S. (1984). *Corporate recovery: Successful turnaround strategies and their implementation*. London: Penguin.

Sotelo, C. (2004). *Gestión de la comunicación en las organizaciones*. Barcelona: Ariel Comunicación.

Sousa, J. P. (2004). *Planificando a comunicação em relações públicas*. Florianópolis (Brasil): Letras Contemporâneas.

Túñez López, M. (coord.). (2007). *Comunicación preventiva. Planificación y ejecución de estrategias de información interna y externa ante situaciones de crisis*. A Coruña: Netbiblo.

Tuñez López, M. (2012). *La gestión de la comunicación en las organizaciones*. Zamora: Comunicación Social.

Varona, F. (2005). *El círculo de la comunicación*. Coruña: Netbiblo, serie Comunicación Empresarial.

Villafañé, J. (2006). *Quiero trabajar aquí. Las seis claves de la reputación interna*. Madrid: Pearson.

Villafañé, J., Bustamante, E. y Prado, E. (1987). *Fabricar noticias. Las rutinas productivas en radio y televisión*. Barcelona: Mitre.

Westphalen, M. H. (2004). *Communicator*. París: Dunod.

Xifra, J. (2007). *Técnicas de las Relaciones Públicas*. Barcelona: Editorial UOC.

CAPÍTULO X

La tutela de la ciberseguridad a través del derecho penal

Alexandre Casadevall Portas
Fiscal de la Fiscalía Provincial de Madrid

SUMARIO. 1. Introducción. 2. El derecho penal y la ciberseguridad. 2.1. La necesidad de un derecho penal eficaz contra la ciberdelincuencia. 2.2. Ciberdelincuencia transnacional, respuesta penal internacional. *2.2.1. Convenio de Budapest. 2.2.2. Normativa de la Unión Europea. 2.2.3. Otras iniciativas*. **3. Ciberdelitos.** 3.1. Concepto y tipologías de ciberdelitos. 3.2. Análisis de los delitos contra la ciberseguridad en el Código Penal. *3.2.1. Consideraciones previas. 3.2.2. Delitos de descubrimiento y revelación de secretos. 3.2.3. Delitos de daños informáticos. 3.2.4. Estafas informáticas. 3.2.5. Ciberterrorismo*. **4. Conclusión. 5. Bibliografía.**

1. Introducción

Vivimos en un mundo digital. La realidad diaria nos demuestra que gran parte de nuestra vida se desarrolla ya en un ámbito virtual, el ciberespacio. En este espacio las personas nos relacionamos y comunicamos las unas con las otras, trabajamos, compramos, realizamos operaciones financieras, contratamos servicios, nos informamos, nos expresamos... Obviamente existen diferencias en el grado de uso de las nuevas tecnologías, pero hoy en día es difícil encontrar a alguien que no las utilice de forma diaria de un modo u otro. Esto no solo es predicable de las personas físicas. Sería impensable el funcionamiento de empresas y Administraciones públicas sin estas

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

nuevas tecnologías. Y la tendencia es que este uso siga en aumento, dadas sus ventajas y el continuo desarrollo tecnológico.

Sin embargo, imaginemos que las pérdidas sufridas por las entidades financieras por los fraudes informáticos superaran a los beneficios que les supusiera la banca digital. O que hubiera tantas intrusiones informáticas que fuera altamente probable que cualquier información almacenada en nuestros dispositivos electrónicos terminara en manos de terceras personas. O que fueran diarios los ciberataques que inutilizaran infraestructuras críticas, desde aeropuertos a centrales hidroeléctricas. No estamos hablando de un escenario remoto: el Informe Anual de Seguridad Nacional 2023 recoge como principal preocupación entre los riesgos y amenazas las campañas de desinformación y el empleo del ciberespacio para fines irregulares. Para seguir disfrutando de las ventajas que ofrecen las nuevas tecnologías es necesario tener redes y sistemas suficientemente seguros si no queremos que su uso entrañe riesgos inasumibles. Aquí entra en acción la ciberseguridad.

Podemos definir la ciberseguridad como todas las actividades necesarias para la protección de las redes y los sistemas de información, de los usuarios de tales sistemas y de otras personas afectadas por las ciberamenazas[1]. La importancia de este objetivo de redes y sistemas seguros ha motivado las distintas iniciativas que se vienen desarrollando desde hace años tanto en el ámbito europeo como en el nacional, y que han sido analizadas en capítulos anteriores. Estas iniciativas conllevan medidas en todos los ámbitos y con actores muy diversos, pero en cualquier caso destacan la necesidad de un planteamiento global en materia de seguridad de las redes y de la información. De este planteamiento global forma parte relevante el derecho penal.

2. El derecho penal y la ciberseguridad

La finalidad del derecho penal es proteger la sociedad. Para hacerlo define qué conductas se consideran delito, y determina las penas o medidas de seguridad que deben imponerse a sus responsables. Estas conductas que se definen y castigan son aquellas que lesionan de manera efectiva o potencial bienes jurídicos que el legislador valora esenciales para el funcionamiento de nuestra sociedad. Para protegerlos utiliza el poder punitivo del Estado, por considerar que los restantes medios de tutela y sanción son ineficaces o insuficientes.

1. Artículo 2.1) del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.º 526/2013 ("Reglamento sobre la Ciberseguridad").

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

Por lo tanto, el derecho penal se configura como un instrumento de lucha contra la criminalidad informática que castiga aquellas conductas que el legislador considera que lesionan o ponen en peligro bienes jurídicos relacionados con la seguridad en el ciberespacio.

Este castigo penal tiene, por una parte, una finalidad retributiva, sancionando a quien ha cometido una conducta prohibida, para compensar el mal que ha causado con su conducta. Sin embargo, cumple además una importante función preventiva: la amenaza del castigo penal evita en muchos casos que se cometan delitos por parte de quienes, teniendo ocasión de delinquir, deciden finalmente no hacerlo por temor a las penas que se les puedan imponer si son descubiertos y condenados. El derecho penal contribuye así de forma esencial a la ciberseguridad.

2.1. La necesidad de un derecho penal eficaz contra la ciberdelincuencia

Los datos estadísticos y la propia experiencia práctica diaria ponen de manifiesto que la ciberdelincuencia se encuentra en clara expansión. El Informe sobre la cibercriminalidad en España 2023 del Ministerio del Interior constata el aumento de los delitos informáticos en el periodo comprendido entre 2019 y 2023. Destaca, por una parte, que en 2023 ha habido un 26 % más de hechos delictivos conocidos con respecto al año 2022 (pasando de 374 737 a 472 125), y, por otra, que el porcentaje de delitos informáticos respecto de la delincuencia en general ha pasado del 9,9 % en 2019 al 19,2 % en 2023.

Este crecimiento se explica en gran parte porque las nuevas tecnologías han abierto un gran abanico de posibilidades para cometer delitos de la más diversa índole. En algunos casos se trata de nuevas conductas que han aparecido a raíz del desarrollo digital. En otros se trata de delitos que ya existían, pero que han pasado a cometerse usando herramientas informáticas, aprovechando las ventajas que estas ofrecen.

Resulta especialmente preocupante que el porcentaje de esclarecimiento de estos delitos esté disminuyendo, según observa el mismo informe (15,9 % en 2021, 14,6 % en 2022 y 13,5 % en 2023). La estadística muestra que, a pesar de los esfuerzos de las autoridades policiales y judiciales, la mayor parte de los ciberdelitos quedan impunes. Esto compromete la eficacia del derecho penal como instrumento de prevención, que depende en gran medida de la posibilidad de identificar, enjuiciar y condenar a los autores de los delitos.

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

2.2. Ciberdelincuencia transnacional, respuesta penal internacional

La ciberdelincuencia tiene particularidades que dificultan una respuesta penal efectiva[2]. Junto a la constante aparición de nuevas modalidades delictivas a medida que se producen avances técnicos y a la capacidad de los autores de ocultar su identidad por diversos mecanismos, destaca el carácter transfronterizo de muchos de los delitos cometidos a través del ciberespacio. Ello hace que la persecución penal sea muy compleja.

De entrada, se exige la especialización de las autoridades policiales y judiciales que deberán investigar y enjuiciar estos delitos. Esta especialización se viene desarrollando desde hace años, y en ella cabe destacar la del Ministerio Fiscal, con la decisiva labor llevada a cabo por la Unidad de Criminalidad Informática de la Fiscalía General del Estado y por las secciones de Criminalidad Informática de las distintas Fiscalías. Pero, además, las autoridades nacionales se enfrentan al obstáculo de que frecuentemente autores, víctimas o pruebas se encuentran en otros países, con un ordenamiento jurídico distinto.

Es por ello que la respuesta penal contra la ciberdelincuencia exige trabajar siguiendo dos grandes líneas de actuación íntimamente vinculadas: la primera, la evolución ágil y efectiva de la legislación sobre la materia, procurando aproximar los ordenamientos jurídicos de los distintos Estados; la segunda, reforzar y agilizar los mecanismos de cooperación internacional. A continuación, analizaremos algunas de las iniciativas más relevantes en esta respuesta internacional, donde destaca la reciente aprobación de varios instrumentos llamados a mejorar de forma significativa la lucha contra la ciberdelincuencia.

2.2.1. Convenio de Budapest

El Convenio sobre la ciberdelincuencia del Consejo de Europa de 2001, conocido como Convenio de Budapest, desempeña un papel central en la lucha contra la criminalidad informática. Fue el primer tratado internacional en centrarse específicamente en la cibercriminalidad y en la prueba

2. Un ejemplo de estas particularidades es la tendencia conocida como *Crime as a Service* o *CaaS*, que consiste en subcontratar servicios ilegales: los ciberdelincuentes alquilan o venden *malware* u otros servicios a terceros para que estos puedan cometer delitos informáticos. Esto permite que personas sin conocimientos técnicos puedan lanzar ataques informáticos que excedan de sus capacidades, y al mismo tiempo contribuye a que dentro de la ciberdelincuencia se produzca una especialización en función de los servicios específicos que se comercialicen.

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

electrónica. A pesar de tratarse de un convenio del Consejo de Europa está abierto a terceros países, y en noviembre de 2024 los Estados parte ascendían a un total de 76 (entre los que destacan veintiséis de la Unión Europea y los Estados Unidos). Además, su influencia es patente en las legislaciones nacionales sobre la materia de otros muchos Estados. Todo ello contribuye a que siga siendo, aún hoy, el instrumento internacional de referencia en la lucha contra la ciberdelincuencia. Precisamente en el Convenio de Budapest se observan las dos líneas de actuación principales a las que nos referíamos anteriormente.

Primero, contiene un listado de delitos cometidos contra sistemas informáticos o utilizando tales sistemas y una serie de medidas de investigación tecnológica que los Estados deberán introducir en sus legislaciones nacionales. Los delitos son contra datos y sistemas informáticos (acceso e interceptación ilícitos, interferencia en datos y sistemas, abuso de los dispositivos), falsificación y fraudes informáticos, relacionados con la pornografía infantil y contra la propiedad intelectual. A ellos se añadieron en 2003 otros delitos de índole racista y xenófoba cometidos por medio de sistemas informáticos[3]. Esta regulación ha tenido gran influencia en la posterior configuración de tales delitos en la legislación europea y nacional.

En segundo lugar, el Convenio de Budapest regula distintos mecanismos de cooperación internacional como la extradición, la asistencia mutua, el intercambio espontáneo de información, la conservación de datos o una red 24/7 de puntos de contacto.

Aunque el Convenio de Budapest ha sido realmente exitoso al definir los delitos informáticos, la realidad ha demostrado que sus mecanismos de cooperación internacional no son suficientes. La ciberdelincuencia no ha dejado de aumentar, y en muchos procedimientos penales hoy es necesario recabar pruebas electrónicas. Sin embargo, los instrumentos de asistencia judicial tradicionales son lentos y complejos e impiden una investigación rápida de los ciberdelitos, cuyo esclarecimiento dependerá muchas veces de información volátil, que se puede ver alterada o eliminada en un corto lapso de tiempo (ya sea por el autor del delito o por las empresas proveedoras de servicios en virtud de la normativa sobre conservación de datos). Además, la realidad del mundo digital revela el papel central de unas pocas grandes compañías proveedoras de servicios, la mayor parte de ellas ubicadas en

3. Protocolo adicional al Convenio sobre la Ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos, hecho en Estrasburgo el 28 de enero de 2003.

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

Estados Unidos, que son las que frecuentemente tendrán la información requerida en las investigaciones por delitos informáticos. Esta situación motivó que en 2022 los Estados parte firmaran un Segundo Protocolo adicional relativo a la cooperación reforzada y la revelación de pruebas electrónicas[4]. Entre otras novedades el protocolo incluye mecanismos para una asistencia mutua más eficiente entre las autoridades, regula la cooperación directa entre las autoridades y los proveedores de servicio y una cooperación especialmente rápida en supuestos de emergencia, y prevé la transmisión electrónica de las solicitudes.

2.2.2. Normativa de la Unión Europea

En el ámbito de la Unión Europea también se han hecho importantes esfuerzos para ofrecer una respuesta penal efectiva contra la ciberdelincuencia. La necesidad de armonización normativa en esta materia ya se puso de manifiesto en el Consejo Europeo de Tampere de 1999, y ha motivado la aprobación de numerosos instrumentos para que los Estados miembros aproximen sus legislaciones penales en la lucha contra distintas manifestaciones de la ciberdelincuencia, como los ataques contra los sistemas de información[5], los abusos sexuales a menores, la pornografía infantil[6] y los fraudes informáticos[7]. Estos instrumentos han determinado la regulación actual de esta materia en nuestro ordenamiento jurídico, y siguen parámetros similares a los del Convenio de Budapest.

Junto a ello, el espacio de libertad, seguridad y justicia que supone la Unión Europea determina que la cooperación judicial penal, basada en el principio de reconocimiento mutuo de las resoluciones judiciales, sea espe-

4. Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia, relativo a la cooperación reforzada y la revelación de pruebas electrónicas, hecho en Estrasburgo el 12 de mayo de 2022.

5. Decisión marco 2005/222/JAI del Consejo, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información, y Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo.

6. Decisión marco 2004/68/JAI del Consejo, de 22 de diciembre de 2003, relativa a la lucha contra la explotación sexual de los niños y la pornografía infantil, y Directiva 2011/93/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil y por la que se sustituye la Decisión marco 2004/68/JAI del Consejo.

7. Decisión marco 2001/413/JAI del Consejo, de 28 de mayo de 2001, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo, y Directiva (UE) 2019/713 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo y por la que se sustituye la Decisión marco 2001/413/JAI del Consejo.

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

cialmente intensa, con múltiples instrumentos con los que las autoridades judiciales se auxilian entre sí, como las órdenes europeas de detención y entrega y las órdenes europeas de investigación. En la cooperación europea contra la ciberdelincuencia no puede olvidarse el importante papel de Europol, Eurojust, el proyecto SIRIUS (de acceso transfronterizo a la prueba electrónica), la Red Judicial Europea (EJN) y la Red Judicial Europea sobre Ciberdelincuencia (EJCN).

El fenómeno de la ciberdelincuencia ha evidenciado, sin embargo, que estos mecanismos de cooperación resultan insuficientes, y que es imprescindible agilizar las investigaciones penales en las que intervenga prueba electrónica. En un planteamiento similar al del Segundo Protocolo adicional al Convenio de Budapest, se ha concluido que hay que reforzar los mecanismos de cooperación entre autoridades y permitir la cooperación directa con los proveedores de servicio. Para lograrlo, se ha elaborado un paquete legislativo sobre pruebas electrónicas (el conocido como *E-Evidence Package*), que parte de estas premisas y de la idea central de que los proveedores de servicios que ofrezcan servicios en la Unión Europea deben atender las órdenes directas de las autoridades de los Estados miembros para preservar y entregar pruebas electrónicas. Este paquete legislativo consta de dos instrumentos. El primero es un reglamento[8] que regula la orden europea de entrega y la orden europea de conservación, a través de las cuales la autoridad de un Estado miembro podrá ordenar la entrega/preservación de pruebas electrónicas vinculadas a una investigación criminal a los proveedores que ofrezcan sus servicios en territorio de la Unión, con independencia del lugar donde se encuentren ubicados los datos. El segundo es una directiva[9] que, complementando el anterior, obliga a los proveedores de servicios a designar al menos un establecimiento o representante legal en un Estado miembro (que será el responsable de recibir y ejecutar las órdenes europeas de entrega y de conservación) y contiene las normas para tal designación.

8. Reglamento (UE) 2023/1543 del Parlamento Europeo y del Consejo, de 12 de julio de 2023, sobre las órdenes europeas de producción y conservación a efectos de prueba electrónica en procesos penales y de ejecución de penas privativas de libertad a raíz de procesos penales.

9. Directiva (UE) 2023/1544 del Parlamento Europeo y del Consejo, de 12 de julio de 2023, por la que se establecen normas armonizadas para la designación de establecimientos designados y de representantes legales a efectos de recabar pruebas electrónicas en procesos penales.

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

2.2.3. Otras iniciativas

La indicada necesidad de armonizar los ordenamientos jurídicos y reforzar los mecanismos de cooperación internacional para luchar de forma eficaz contra la ciberdelincuencia es una tendencia compartida a nivel global.

Estados Unidos aprobó en 2018 la conocida como *CLOUD Act* (*Clarifying Lawful Overseas Use of Data Act*), que facilita el acceso a la prueba electrónica en poder de las grandes compañías proveedoras de servicios estadounidenses por parte de las autoridades judiciales extranjeras en investigaciones criminales. En base a esta norma, los Estados Unidos ya han alcanzado acuerdos con el Reino Unido y Australia para dicho acceso, y están negociando con Canadá y la Unión Europea.

Además, en diciembre de 2024, la Asamblea General de las Naciones Unidas adoptó la Convención de las Naciones Unidas contra la Ciberdelincuencia, que se abrirá a la firma en 2025. El texto reproduce en gran parte las previsiones del Convenio de Budapest, y debería contribuir a mejorar la lucha contra la ciberdelincuencia a nivel mundial, extendiendo un marco normativo común a nuevos países.

3. Ciberdelitos

3.1. Concepto y tipologías de ciberdelitos

La primera cuestión que debemos plantearnos es qué es un ciberdelito. Según el *Diccionario panhispánico del español jurídico*, un ciberdelito o delito informático es una infracción penal cometida utilizando un medio o un instrumento informático. Por lo tanto, lo que caracteriza a estos delitos es su forma comisiva a través de las tecnologías de la información y la comunicación.

Dentro de los delitos informáticos debemos distinguir dos tipologías generales. Por un lado, tenemos conductas que afectan directamente a la seguridad de los datos, redes y sistemas de información. Por otro, hay comportamientos que no atacan directamente a redes y sistemas, pero que se ejecutan a través de las nuevas tecnologías, aprovechando las ventajas que estas ofrecen y que afectan a los más diversos bienes jurídicos. Esta

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

dualidad se puso ya de manifiesto desde los inicios de la lucha contra la ciberdelincuencia[10], y persiste en la actualidad[11].

En este capítulo nos centraremos en la primera tipología: los delitos que atacan la seguridad de una red o un sistema informáticos, afectando así a su disponibilidad, integridad o confidencialidad, y que son propiamente los relativos a la ciberseguridad. Ampliar nuestro análisis al segundo tipo de delitos exigiría un espacio mayor al disponible en este capítulo, puesto que el abanico de conductas es enorme: incluye delitos incluidos en el Convenio de Budapest y que han sido tradicionalmente tratados como delitos informáticos (por ejemplo, los delitos relacionados con la pornografía infantil), pero también se extiende a cualquier conducta delictiva que se cometa usando las nuevas tecnologías, como enviar un mensaje amenazante a la víctima a través de *WhatsApp* o publicar una calumnia en redes sociales. Además, esta segunda tipología no afecta a la ciberseguridad propiamente dicha. Son delitos que hacen del ciberespacio un lugar menos seguro porque tienen lugar en él o a través de él, pero que no comprometen la protección de redes y sistemas informáticos.

3.2. Análisis de los delitos contra la ciberseguridad en el Código Penal

3.2.1. Consideraciones previas

Hemos delimitado nuestro ámbito de análisis a las conductas que afectan directamente a la ciberseguridad, es decir, a la confidencialidad, la integridad o la disponibilidad de los datos y sistemas de información. Al regular estas conductas el legislador no lo ha hecho de forma conjunta, agrupando en un mismo apartado todos los comportamientos que versan sobre la

10. La Instrucción 2/2011, de la Fiscalía General del Estado, sobre el Fiscal de Sala de Criminalidad Informática y las Secciones de Criminalidad Informática de las Fiscalías, ya indicaba: "Efectivamente junto a tipos penales a través de los cuales el legislador ha protegido específicamente la seguridad de los datos, programas y/o sistemas informáticos, existen otras conductas ilícitas que, afectando a los más diversos bienes jurídicos, se planifican y ejecutan aprovechando las ventajas que ofrecen las nuevas tecnologías de la sociedad de la información y que presentan por tanto, a los efectos de su investigación y/o enjuiciamiento singularidades y dificultades similares a las de los primeramente indicados".

11. El Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021, incluye entre los riesgos y amenazas a la seguridad nacional la vulnerabilidad del ciberespacio, y expone: "Se distinguen dos tipologías generales de amenazas en el ciberespacio. Por un lado, los ciberataques, entendidos como acciones disruptivas que actúan contra sistemas y elementos tecnológicos. Ejemplos de ello son los ataques de *ransomware* (secuestro de datos) o la denegación de servicios, entre otros. Y, por otro lado, el uso del ciberespacio para realizar actividades ilícitas, como el cibercrimen, el ciberespionaje, la financiación del terrorismo o el fomento de la radicalización".

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

ciberseguridad. En cambio, ha optado por incluirlos en títulos o capítulos del Código Penal que ya existían, tomando en consideración el bien jurídico que considera afectado en última instancia (singularmente la intimidad y el patrimonio).

En nuestro análisis nos centraremos primero en los ataques más relevantes a la confidencialidad de datos y sistemas informáticos (delitos de descubrimiento y revelación de secretos) y a su integridad o disponibilidad (delitos de daños informáticos)[12]. A continuación, veremos las estafas informáticas, un fenómeno de gran relevancia por su volumen e impacto en el sistema económico, y que comprende diversas modalidades, entre las que destacan el empleo de manipulaciones informáticas y el uso fraudulento de datos, vinculados también con la ciberseguridad. Finalmente examinaremos el ciberterrorismo, que ataca a la confidencialidad, integridad o disponibilidad de datos y sistemas de información, pero que se caracteriza por perseguir unas finalidades específicas.

Antes de entrar en el examen de los delitos conviene aclarar dos términos que estos utilizan y cuya definición, contenida en la legislación comunitaria[13] y que no reproduce el Código Penal, es necesaria para comprender el tipo penal: sistema de información y datos informáticos.

Cuando hablamos de sistema de información, nos referimos a todo aparato o grupo de aparatos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático de datos informáticos, así como a los datos informáticos almacenados, tratados, recuperados o transmitidos por dicho aparato o grupo de aparatos para su funcionamiento, utilización, protección y mantenimiento.

Por su parte, los datos informáticos son toda representación de hechos, informaciones o conceptos de una forma que permite su tratamiento por un sistema de información, incluidos los programas que sirven para hacer que dicho sistema de información realice una función.

12. Estos delitos son examinados en profundidad por la Circular 3/2017, de 21 de septiembre, de la Fiscalía General del Estado, sobre la reforma del Código Penal operada por la LO 1/2015, de 30 de marzo, en relación con los delitos de descubrimiento y revelación de secretos y los delitos de daños informáticos, que ha servido de referente para nuestro estudio de estas figuras delictivas.

13. Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo.

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

3.2.2. Delitos de descubrimiento y revelación de secretos

En términos generales, estos delitos tipifican conductas que suponen la vulneración de la intimidad personal y de la privacidad. En el ámbito de la ciberseguridad estos comportamientos se caracterizan por atacar la confidencialidad de datos informáticos y sistemas de información. En función de la forma de vulnerar esta confidencialidad, de si el objetivo era acceder a información y de la naturaleza de esta información, podremos distinguir entre diversas figuras delictivas. Estos delitos se castigan más gravemente si se cometen en el seno de una organización o un grupo criminal (artículo 197 quater), y también se sanciona en su caso a las personas jurídicas (197 quinquies).

- **Descubrimiento y revelación de secretos (197 CP)**

El papel central en materia de descubrimiento y revelación de secretos lo ocupa el artículo 197 del Código Penal. Este precepto, objeto de constantes críticas doctrinales y jurisprudenciales por su redacción[14], castiga en sus apartados primero y segundo conductas de naturaleza muy distinta y que puedan afectar a bienes jurídicos diversos[15].

Centrándonos en las principales conductas relacionadas con la seguridad de los datos y sistemas informáticos, en el apartado primero podemos identificar el apoderamiento de datos, documentos, mensajes de correo y efectos personales (que incluye la captación intelectual, es decir, tomar conocimiento), y la interceptación de comunicaciones personales. En cuanto al apartado segundo, este sanciona al que, en perjuicio de otro[16] y sin estar autorizado, se apodera, utiliza, modifica, altera o accede a datos reservados de carácter personal registrados en cualquier tipo de ficheros o soportes. Estos comportamientos no siempre serán estancos, y en muchas ocasiones habrá conductas que podrán incardinarse en ambos apartados.

14. Entre otras, la STS 538/2021, de 17 de junio, FD 2, habla de "inabarcable amplitud y casuismo", y la STS 412/2020, de 20 de julio, FD 2, indica: "El artículo 197 del Código Penal, es calificado por la doctrina como auténtico galimatías jurídico con diabólica, atormentada e inacabable redacción".

15. La STS 538/2021, de 17 de junio, FD 2, dice: "El art. 197 sanciona conductas que pueden afectar a la inviolabilidad de las comunicaciones, al derecho a la protección de datos -entendido éste como el derecho a controlar los datos automatizados que los demás conocen de nosotros, habeas data- y los derechos a la intimidad y a la propia imagen, preservando su integridad frente a la injustificada difusión de esos datos".

16. Es necesario acreditar este perjuicio, pero si se trata de datos sensibles el mero conocimiento derivado del simple acceso ya se considera que conlleva un perjuicio.

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

Los supuestos en que estos delitos se producen son muy diversos, circunscribiéndose muchos de ellos a casos individuales, como acceder al contenido del teléfono móvil de la pareja para descubrir una infidelidad, o que un funcionario de la Agencia Tributaria consulte en la base de datos de esta la información fiscal sobre un vecino con el que tiene mala relación. Sin embargo, hoy en día están aumentando y son una grave amenaza para la ciberseguridad los ataques informáticos de diversa índole en que el objetivo es la exfiltración o extracción masiva de datos, sea para su uso por el propio atacante o para comercializar con ellos (y que los compradores después utilizarán para cometer delitos). Ejemplos habituales de robo de datos son ataques a los sistemas informáticos de empresas o instituciones de los que se extraen los datos, o bien el uso de mecanismos de *phishing* para engañar a las víctimas y hacer que compartan sus datos personales.

A continuación, el artículo 197 prevé agravaciones de las penas para los siguientes supuestos: si se difunden, revelan o ceden a terceros los datos, hechos o imágenes a que se refieren los números anteriores (197.3 CP); si los hechos se han cometido por los encargados o responsables de los ficheros o soportes, o si para hacerlo se han utilizado sin autorización datos personales de la víctima, como contraseñas (197.4 CP); si se afecta a datos sensibles —sobre ideología, religión, creencias, salud, origen racial o vida sexual—, o si la víctima es menor o una persona con discapacidad necesitada de especial protección (197.5 CP); y si los hechos se han realizado con fines lucrativos (197.6 CP).

- **Acceso ilegal a sistemas informáticos (197 bis.1 CP)**

Denominado por el Tribunal Supremo como "*hacking* de desafío"[17], este delito está previsto para sancionar a quien, por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o a una parte de un sistema de información, o se mantenga en él en contra de la voluntad de quien tenga derecho a excluirlo.

La conducta típica recae sobre el conjunto o una parte de un sistema de información, y se consuma con la simple entrada en el mismo. Por lo tanto, en este delito no es necesario tomar contacto con datos o programas que contengan informaciones concretas, ni que se vean afectados datos de carácter personal o la intimidad de otro de manera directa. Para la comi-

17. STS 494/2020, de 8 de octubre de 2020, FD 6.

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

sión del delito necesariamente debe tratarse de un acceso no autorizado, y debe lograrse vulnerando medidas de seguridad, entendiendo por tales aquellas establecidas para impedir el acceso al sistema, con independencia de su solidez o complejidad, siempre que se mantengan operativas. Además de acceder, se castiga facilitar el acceso a otro y mantenerse en el sistema contra la voluntad de quien tenga derecho a excluir. Como ejemplos de este delito, la Circular 3/2017, de 21 de septiembre, de la Fiscalía General del Estado, sobre la reforma del Código Penal operada por la LO 1/2015, de 30 de marzo, en relación con los delitos de descubrimiento y revelación de secretos y los delitos de daños informáticos, indica que podría constituirlo el acceso a un *router* —pues forma parte de un sistema de información— vulnerando su contraseña de seguridad.

La misma circular expone que en la práctica será frecuente que concurra este delito con alguna de las conductas de los apartados primero y segundo del artículo 197, con un delito del artículo 278 (si el objetivo fuera el descubrimiento de secretos de empresa) o con un delito del artículo 598 y siguientes (si el objetivo fuera el descubrimiento de secretos oficiales).

- **Interceptación ilícita (197 bis.2 CP)**

Comete este delito quien, mediante la utilización de artificios o instrumentos técnicos y sin estar autorizado, intercepta transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos.

La conducta delictiva requiere el uso de artificios o instrumentos técnicos (como dispositivos, *software*, contraseñas o códigos), y consiste en interceptar transmisiones automáticas de datos informáticos. Estas transmisiones pueden ser entre dos o más sistemas informáticos, entre distintos ordenadores dentro de un mismo sistema o incluso entre una persona y un ordenador, como las que se establecen a través del teclado. Se trata de transmisiones no públicas, en el sentido de que por la naturaleza del proceso de comunicación quedan excluidas del conocimiento de terceros, ya sea por producirse a través de redes privadas o por realizarse a través de redes públicas cuando se haya establecido algún mecanismo para garantizar la privacidad y excluir a terceros. Ejemplos de estas transmisiones son las que se producen dentro de una red de área local o una red privada virtual.

La conducta delictiva se extiende también a la captación de emisiones electromagnéticas de un sistema de información, que se generan por

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

la corriente al circular por el mismo. Usando los equipos apropiados pueden captarse estas emisiones y a partir de ellas reconstruirse datos informáticos.

- **Abuso de los dispositivos (197 ter CP)**

Denominado de esta forma en el Convenio de Budapest, consiste en producir, adquirir o facilitar herramientas e instrumentos preparados y diseñados para cometer alguno de los delitos de descubrimiento de secretos, acceso ilegal e interceptación ilegal. El objetivo de la tipificación es adelantar la barrera de protección del derecho penal. Es decir, con el fin primordial de evitar ciberataques a gran escala contra sistemas informáticos, se sancionan las fases previas de estos ataques, consistentes en la producción, adquisición y distribución de las herramientas o los instrumentos utilizados para cometerlos. En función de si el fin pretendido es el espionaje o el sabotaje informático, el Código Penal castiga estos comportamientos entre los delitos de descubrimiento y revelación de secretos (artículo 197 ter) o entre los delitos de daños informáticos (artículo 264 ter). Por ejemplo, en abril de 2023 tuvo lugar una operación de las fuerzas policiales de 17 países para desmantelar *Genesis Market*, un mercado de venta de credenciales robadas en el que se ofrecían bots que habían infectado dispositivos y recopilaban sus datos a tiempo real, datos que los compradores podían utilizar posteriormente para suplantar la identidad de la víctima y cometer estafas informáticas u otros delitos[18].

Las primeras herramientas que contempla el artículo son programas informáticos concebidos o adaptados principalmente para cometer los delitos indicados. Por lo tanto, consisten en un *software* malicioso o *malware*, diseñado para infiltrarse, obtener información y/o dañar un dispositivo o un sistema de información sin el consentimiento de su propietario. Entre ellos podemos incluir los programas espía o *spyware*, para recolectar información almacenada en un sistema informático y enviarla, como el *malware ZeuS* (utilizado en los ataques de *phishing* bancario para obtener credenciales de usuarios de banca electrónica) y los programas *keylogger* (que registran las pulsaciones en un teclado y así permiten conocer las contraseñas personales). Otros ejemplos son los conocidos *ransomware*, utilizados para cifrar archivos concretos o la totalidad del contenido de un sistema, como *Cryptolocker*, *WannaCry* o *NotPetya*.

18. Nota de prensa de Europol de 5 de abril de 2023. Disponible en https://www.europol.europa.eu/media-press/newsroom/news/takedown-of-notorious-hacker-marketplace-selling-your-identity-to-criminals.

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

En segundo lugar, estas herramientas o instrumentos pueden consistir en una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información. En otras palabras, se trata de medidas de seguridad para evitar la intromisión en archivos o sistemas, legítimamente creadas y utilizadas para el acceso regular a los mismos, que el autor adquiere o facilita con la finalidad de utilizarlas para cometer los delitos indicados.

3.2.3. Delitos de daños informáticos

Son diversas conductas relacionadas con ataques a la integridad y la disponibilidad de los datos y sistemas informáticos. También se sanciona a las personas jurídicas si fueran responsables (artículo 264 quater).

- **Daños informáticos (264 CP)**

En su apartado primero se castiga a quien, por cualquier medio, sin autorización y de manera grave, borre, dañe, deteriore, altere, suprima o haga inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido sea grave.

Se sancionan, por lo tanto, todas las conductas susceptibles de afectar a la integridad de los elementos informáticos, destruyéndolos o modificándolos, pero también hacer inaccesibles estos elementos, comprometiendo su disponibilidad. Ejemplo de esto último es un ataque con un programa *ransomware*, que cifra los archivos del sistema infectado, pidiendo frecuentemente los autores un rescate a la víctima para descifrarlos.

Las penas previstas para estas conductas se agravan en el apartado segundo del artículo, cuando los hechos se cometan en el marco de una organización criminal; se ocasionen daños de especial gravedad o se afecte a un número elevado de sistemas informáticos; se perjudique gravemente el funcionamiento de servicios públicos esenciales o la provisión de bienes de primera necesidad; se afecte al sistema informático de una infraestructura crítica (esencial para el mantenimiento de funciones vitales de la sociedad, la salud, la seguridad, la protección y el bien económico y social) o se cree una situación de peligro grave para la seguridad de la Unión Europea o de uno de sus Estados miembros; se utilice un programa informático concebido o adaptado para ello o una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a un sistema de información; o los hechos hubieran resultado de extrema gravedad. Por último, en el

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

apartado tercero se incrementan las penas si los hechos se cometen mediante la utilización ilícita de datos personales de otra persona para facilitar el acceso al sistema informático o para ganarse la confianza de alguien.

- **Obstaculización o interrupción del funcionamiento de sistemas informáticos (264 bis CP)**

Este delito consiste en obstaculizar o interrumpir la normal actividad de un sistema informático, de manera grave, a través de alguna de las conductas del artículo 264 (borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos, programas o documentos), introduciendo o transmitiendo datos, o destruyendo, dañando, inutilizando, eliminando o sustituyendo un sistema informático, telemático o de almacenamiento de información electrónica.

El delito es similar al de daños informáticos, pero la diferencia esencial es que en el artículo 264 se castigan las acciones ilícitas contra datos, programas informáticos y documentos electrónicos ajenos, y en el artículo 264 bis, aquellas cuyo objeto son los sistemas en sí mismos considerados, como conjunto interconectado de elementos informáticos.

Las penas para esta conducta se agravan si se hubiera perjudicado de forma relevante la actividad normal de una empresa, un negocio o una Administración pública (264 bis.1, inciso final); cuando concurra alguna de las ya mencionadas circunstancias del apartado segundo del artículo 264 (264 bis.2); y cuando los hechos se hubieran cometido mediante la utilización ilícita de datos personales de otra persona para facilitar el acceso al sistema informático o ganarse la confianza de un tercero (264 bis.3).

Un ejemplo de este delito sería un ataque de denegación de servicio, o *DDoS*, en el que se ataca un sistema informático desde muchos equipos a la vez mediante la entrada masiva de tráfico, hasta colapsar el sistema. Otro ejemplo fue el de una bomba lógica que inutilizó más de tres mil equipos informáticos de un banco[19].

- **Abuso de los dispositivos (264 ter CP)**

Es equivalente al delito del artículo 197 ter que hemos visto anteriormente. La diferencia es que en este se sanciona la producción, adquisición y distri-

19. STS 183/2024, de 29 de febrero de 2024.

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

bución de herramientas e instrumentos para cometer un delito de daños informáticos, o un delito de obstaculización o interrupción del funcionamiento de sistemas informáticos. Es decir, para determinar si estamos ante el delito del artículo 197 ter o el del artículo 264 ter, habrá que ver qué delito se tiene la intención de facilitar, cuestión que no siempre será fácil de dilucidar, sin que pueda descartarse que muchas veces concurran ambas finalidades.

3.2.4. Estafas informáticas

El delito de estafa es uno de los que, a raíz del uso de las nuevas tecnologías de la información y comunicación, han experimentado mayores evolución y crecimiento. Así, el Informe sobre la cibercriminalidad en España 2023 destaca que el 90,5 % de los delitos informáticos conocidos ese año fueron estafas. Sin embargo, bajo la denominación genérica de estafas informáticas tenemos que distinguir entre las dos tipologías generales de la cibercriminalidad a las que aludíamos anteriormente.

Desde una perspectiva amplia hablamos de estafas informáticas para referirnos a las estafas tradicionales —que consisten en engañar a otro induciéndole a realizar un acto de disposición en perjuicio propio o ajeno— cuando se cometen a través de las nuevas tecnologías, supuesto cada vez más frecuente. En estos casos no se afecta necesariamente a redes y sistemas informáticos, pero los autores aprovechan las ventajas que ofrecen las tecnologías de la información y comunicación para lograr su propósito criminal. La casuística es enorme: desde modalidades simples, como la publicación *online* de falsas ofertas de venta de bienes o de alquiler vacacional, hasta estafas más complejas, como los fraudes BEC[20]. Estas estafas se castigan en el artículo 248 del Código Penal, y en función de si el importe supera o no los 400 euros estaremos ante un delito menos grave o un delito leve.

En cambio, las estafas informáticas propiamente dichas se sancionan en el apartado primero del artículo 249. En él se castiga conseguir una transferencia no consentida valiéndose de cualquier tipo de manipulación informática, o utilizar fraudulentamente cualquier instrumento de pago distinto del efectivo o sus datos para hacer operaciones de todo tipo. Se tra-

20. Los fraudes BEC (*Business Email Compromise*) afectan a correos electrónicos empresariales: el ciberdelincuente se hace pasar, por ejemplo, por un superior jerárquico de la misma empresa, y ordena que se haga una transferencia de dinero, o bien por otra empresa con la que se mantienen relaciones comerciales, y envía una factura por unos servicios en la que ha cambiado el número de cuenta de destino. Este tipo de fraudes habitualmente se cometen por los autores usando una dirección de correo electrónico falsa, pero muy similar a la auténtica.

ta de comportamientos en los que lo determinante es que la transferencia u operación no la hace un tercero engañado (como ocurre con las estafas tradicionales, aunque se realicen por medios informáticos), sino que la realiza el autor utilizando distintos mecanismos y en perjuicio de otro. En estos supuestos es indiferente que el importe exceda o no de 400 euros.

A continuación, y de manera similar a los anteriormente vistos artículos 197 ter y 264 ter, en los apartados segundo y tercero del artículo 249 se adelantan las barreras de protección penal para castigar actos preparatorios de las estafas informáticas. El fundamento radica en la gravedad de esta tipología delictiva, que pone en grave peligro el mercado digital, genera gran desconfianza en el uso de los nuevos medios de pago y supone un importante riesgo para el funcionamiento del sistema financiero. De este modo, en el apartado segundo se castiga fabricar, adquirir, poseer y facilitar dispositivos, instrumentos informáticos o cualquier otro medio diseñado o adaptado específicamente para la comisión de las estafas previstas en este artículo, así como adquirir de forma ilícita cualquier instrumento de pago distinto del efectivo para su utilización fraudulenta. Y en el apartado tercero se sanciona, si bien con una pena más reducida, poseer, adquirir o poner a disposición de terceros cualquier instrumento de pago distinto del efectivo, para su utilización fraudulenta y sabiendo que se obtuvo ilícitamente.

Tanto para las estafas del artículo 248 como para las del artículo 249 se prevén penas agravadas en los supuestos específicamente previstos en el artículo 250, entre los que hay que destacar, tratándose de estafas informáticas, aquellos en que el valor de la defraudación supere los 50 000 euros o afecte a un elevado número de personas, y un supuesto hiperagravado cuando el valor de la defraudación supere los 250 000 euros.

3.2.5. Ciberterrorismo

En los últimos años están aumentando los ataques informáticos que, más allá de perseguir un beneficio económico o perjudicar individuos o empresas concretas, tienen el objetivo de perturbar nuestra sociedad, generando intranquilidad o miedo y contribuyendo a generar una situación de desestabilización.

El ciberterrorismo está específicamente castigado en el artículo 573.2 del Código Penal, y consiste en la comisión de los delitos informáticos de acceso e interceptación ilegal, daños informáticos y abuso de dispositivos que hemos visto anteriormente (artículos 197 bis, 197 ter y 264 a 264 quater), cuando la finalidad perseguida por los autores sea cualquiera de las

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

previstas en el artículo 573.1: subvertir el orden constitucional, suprimir o desestabilizar gravemente el funcionamiento de las instituciones políticas o de las estructuras económicas o sociales del Estado, obligar a los poderes públicos a realizar un acto o a abstenerse de hacerlo, alterar gravemente la paz pública, desestabilizar gravemente el funcionamiento de una organización internacional o provocar un estado de terror en la población o en una parte de ella.

Por lo tanto, el ciberterrorismo se caracteriza por dos elementos: uno externo, que es la comisión de un delito informático de los anteriormente mencionados, y otro tendencial o teleológico, consistente en perseguir una de las finalidades indicadas[21]. Esta intencionalidad será determinante para distinguir los delitos informáticos ordinarios de acceso e interceptación ilegal, daños informáticos y abuso de dispositivos analizados en el apartado anterior de los supuestos de ciberterrorismo, en que la pena impuesta por estas conductas será mayor (artículo 573 bis.3).

Un ejemplo que podría encuadrarse en el concepto de ciberterrorismo sería la actividad del grupo NoName057(16). A raíz de la guerra de Ucrania este grupo ha venido realizando ataques informáticos, sobre todo ataques de denegación de servicio o DDoS, contra páginas web de instituciones públicas y empresas de sectores estratégicos de aquellos países que se han posicionado a favor de Ucrania[22].

Sin embargo, la delimitación entre ciberterrorismo y cibercriminalidad genérica no siempre será fácil. Imaginemos un ataque informático con *ransomware* a una infraestructura crítica. Puede que los autores exijan o no un rescate por los archivos cifrados. Pedir un rescate no significa que no sea ciberterrorismo, puesto que pueden coexistir una finalidad terrorista y un ánimo de lucro personal, o incluso puede que el rescate sea una vía de

21. El ATS de 29-02-24, FD 4, señala: "En efecto, tal como acordó la Junta de Sección de Fiscales de la Fiscalía del Tribunal Supremo, Acta de 6-2-2024: "el concepto de terrorismo del articulo 573 CP se construye en la actualidad sobre dos elementos o requisitos: el elemento objetivo o material, es decir, la ejecución de unas determinadas acciones previstas como tales por el Código (las enumeradas en los ap. 1, 2 y 3 del precepto), y un elemento teleológico o tendencial (la acción debe ejecutarse con una específica finalidad o propósito que se describe en el ap. 1 del art.). No es necesario que el autor pertenezca o forme parte de una organización o grupo terrorista, o actúe de manera asociada u organizada, de modo que cualquier persona que ejecute, aunque sea individualmente, o bien colectivamente, alguna de las acciones previstas con las finalidades expresadas en el precepto, será autor o partícipe de un delito de terrorismo".

22. Nota de prensa de la Guardia Civil de 20 de julio de 2024. Disponible en https://web.guardiacivil.es/es/destacados/noticias/Tres-detenidos-por-delitos-de-danos-informaticos-con-fines-terroristas/.

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

financiación del grupo. Asimismo, la falta de exigencia de rescate no implica necesariamente que se trate de ciberterrorismo; para ello es necesario que persiga una de las finalidades indicadas. En esta línea cabe destacar la dificultad de distinguir entre el ciberterrorismo y los actos de *hacktivismo*, que consisten en ciberataques realizados por razones ideológicas y con impacto mediático o social, pero sin perseguir los fines recogidos en el artículo 573.1.

También hay que distinguir el ciberterrorismo en sentido estricto o ciberterrorismo genuino del uso de internet con fines terroristas. Las organizaciones o los grupos terroristas, como cualquier colectivo, han pasado a utilizar las nuevas tecnologías para desarrollar sus actividades, dadas las ventajas que estas ofrecen. Entre estos usos debemos destacar, puesto que nuestro Código Penal los castiga expresamente, el autoadoctrinamiento terrorista por medios telemáticos (artículo 575.2) y el enaltecimiento terrorista y la humillación a las víctimas por medios telemáticos (artículo 578.2). Se trata de conductas en las que se usa el ciberespacio para la comisión de actividades delictivas terroristas. Sin embargo, ni cabe incluirlas en el concepto de ciberterrorismo tal y como lo configura el artículo 573.2 ni afectan a la confidencialidad, integridad y disponibilidad de sistemas informáticos, por lo que no atacan a la ciberseguridad.

4. Conclusión

La vulnerabilidad del ciberespacio es uno de los principales riesgos a los que nos enfrentamos. A diferencia del plano físico, relativamente estable y al que miles de años de evolución nos han permitido adaptarnos como individuos y como sociedades, el ciberespacio constituye una realidad que cuenta con pocas décadas, está en constante cambio, y en la que una minoría de personas con avanzados conocimientos técnicos son capaces de moverse con una ventaja abrumadora sobre la generalidad de usuarios, sean particulares, empresas o instituciones. No podemos sustraernos a esta realidad. El ciberespacio ha venido para quedarse y todos estamos en él.

Tampoco podemos resignarnos a que el ciberespacio sea un lugar en el que los delincuentes campen a sus anchas, y a ser potenciales víctimas de ataques informáticos de la más diversa índole. Con nuestras luces y sombras, la historia de la humanidad nos demuestra que hemos sido capaces de ir extendiendo progresivamente el estado de derecho y la protección de los derechos humanos. El ciberespacio no puede ser la excepción.

En esta lucha el derecho penal no es suficiente, pero es necesario. Para poner freno a la vulnerabilidad del ciberespacio es responsabilidad de to-

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

dos adoptar medidas para proteger nuestros datos y sistemas de información. Sin embargo, el riesgo cero no existe, y debemos dotarnos de un sistema penal que dé una respuesta efectiva a los ataques a la ciberseguridad.

La irrupción de la cibercriminalidad ha sido impresionante, y en ocasiones puede dar la impresión de que nos desborda. Legislaciones nacionales divergentes y tratados internacionales que no se suscriben por la gran mayoría de países habilitan la existencia de nichos desde donde los ciberdelincuentes pueden actuar impunemente. Los sistemas penales requieren tiempo para adaptarse y dar respuesta a las nuevas realidades. Ante un fenómeno como la ciberdelincuencia, que opera con carácter transnacional desde cualquier lugar del mundo, esta respuesta debe ser global. A nivel sustantivo se están haciendo grandes esfuerzos para identificar y sancionar de manera armonizada entre los distintos Estados las conductas que lesionan o amenazan la ciberseguridad. Al mismo tiempo hemos visto que se están incorporando nuevos mecanismos para mejorar la cooperación internacional entre autoridades policiales y judiciales y poder llevar a cabo operaciones coordinadas contra la ciberdelincuencia, como de hecho se está haciendo de forma exitosa en los últimos años. Hay razones para ser optimistas.

5. Bibliografía

Conal, I. (2022). *Ciberseguridad y derecho penal*. Navarra: Thomson Reuters Aranzadi.

Delgado, J. (2023). *Apuntes sobre el derecho penal en los nuevos escenarios tecnológicos: inteligencia artificial, ciberseguridad y ciberterrorismo*. Madrid: Consejo General del Poder Judicial - Cuadernos digitales de formación.

López-Muñoz, J. (2020). Ciberterrorismo. En J. López-Muñoz. *Cibercriminalidad e investigación tecnológica* (pp. 165-184). Madrid: Dykinson.

Martín, A. (2023). Prueba digital. Marco normativo para la obtención de evidencias en la investigación de delitos cometidos a través de sistemas informáticos en la Unión Europea. Articulación y utilización de herramientas de investigación tecnológica. En E. Velasco Núñez (dir.). *Marco normativo de la UE para la transformación digital*. Las Rozas, Madrid: La Ley.

Tejada, E. (2023). Marco normativo frente a la ciberdelincuencia en la Unión Europea: impulso de la armonización en el ámbito penal - sustantivo como presupuesto para el fortalecimiento de la cooperación transnacional. En E. Velasco Núñez (dir.). *Marco normativo de la UE para la transformación digital*. Las Rozas, Madrid: La Ley.

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

Claves 48

Las entidades locales frente al reto de la ciberseguridad

La digitalización ha revolucionado la forma en la que las personas interactuamos con el mundo que nos rodea, y los Gobiernos locales no han sido ajenos a esta transformación. La gestión electrónica de expedientes, la transparencia activa, la participación ciudadana inmediata y la prestación de servicios en línea son ejemplos de cómo la tecnología ha cambiado el modo de funcionar de las Administraciones locales.

Esta transformación ha mejorado la eficiencia, la accesibilidad y la calidad de los servicios públicos, pero también ha abierto las puertas a nuevas amenazas en el ámbito cibernético, que se vuelven cada vez más complejas y sofisticadas. Los ciberataques pueden paralizar servicios esenciales, comprometer datos sensibles, dañar la reputación institucional y socavar la confianza en el sistema democrático. Por ello, la ciberseguridad ya no puede ser considerada como una cuestión de futuro ni un mero problema técnico, sino como un elemento estratégico que debe integrarse en la planificación, la gestión y la toma de decisiones de todas las áreas de los Gobiernos locales.

La Fundación Democracia y Gobierno Local, consciente de esta realidad y fiel a su compromiso con la modernización de las Administraciones locales, ha promovido esta obra para proporcionar herramientas y conocimiento que permitan hacer frente a este desafío. Concebida desde una perspectiva multidisciplinar, integra aportaciones jurídicas (constitucional, administrativa y penal), técnicas (ingeniería informática) y sociológicas (comunicación institucional). Profesores universitarios y técnicos de la Administración y del sector privado han aunado sus conocimientos y experiencias para ofrecer una visión completa y rigurosa de la ciberseguridad en el ámbito local.

A lo largo de diez capítulos se analizan los aspectos más relevantes de la ciberseguridad desde una óptica plural y especializada. Más allá del análisis teórico y normativo, se ofrece un enfoque práctico, basado en lecciones aprendidas de incidentes reales y en propuestas operativas para mejorar la resiliencia digital de las entidades locales en un contexto de recursos limitados.

La obra que el lector tiene en sus manos es, en definitiva, una invitación a la reflexión y a la acción: a que los responsables públicos tomen conciencia de la importancia de la ciberseguridad y adopten medidas para proteger sistemas, datos y ciudadanos. Este libro invita a mirar la ciberseguridad no como un obstáculo, sino como una oportunidad para fortalecer nuestras democracias locales en una época de creciente complejidad digital.

Alfredo Galán Galán
Director de la Fundación Democracia y Gobierno Local.
Catedrático de Derecho Administrativo de la Universidad de Barcelona

FUNDACIÓN DEMOCRACIA Y GOBIERNO LOCAL

www.gobiernolocal.org

9 788412 885286