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