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.