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