

# CÓMO PROTEGER LAS ADMINISTRACIONES PÚBLICAS ANTE EL AUMENTO DE CIBERAMENAZAS



Hemos podido conocer de primera mano el trabajo de protección de las Administraciones Públicas ante el aumento constante de las ciberamenazas, en un observatorio en el que han participado representantes de la **Agència Ciberseguretat de Catalunya**, el **Ajuntament de Barcelona**, el **Ajuntament de Girona**, la **Diputació de Tarragona**, **Isdefe** (Ingeniería de Sistemas para la Defensa de España) y **SEGIPSA**, la Sociedad Mercantil Estatal de Gestión Inmobiliaria de Patrimonio, en una mesa redonda que ha contado con el patrocinio de **SonicWall** y **Stormshield**.



#FOROAAPP



# 2025

## Informe de Ciberamenazas de SonicWall



LA NECESIDAD DE RAPIDEZ Y DE ALIADOS FUERTES PARA  
SUPERAR EL CAMPO DE BATALLA DE LA CIBERSEGURIDAD

**El panorama de las amenazas sigue evolucionando a un ritmo sin precedentes, sin dejar inmune a ninguna organización.**

Muchos de los ataques destacados en este informe pueden prevenirse con una higiene de ciberseguridad sólida. Tomar medidas proactivas puede mejorar en gran medida su postura de seguridad. Descubra cuáles son en el Informe de Ciberamenazas 2025 de SonicWall.



**DESCARGUE EL  
INFORME COMPLETO**

# CÓMO PROTEGER LAS ADMINISTRACIONES PÚBLICAS ANTE EL AUMENTO DE CIBERAMENAZAS

CON UN VOLUMEN DE CIBERATAQUES NUNCA ANTES VISTO, POTENCIADO POR HERRAMIENTAS DE IA Y AUTOMATIZACIÓN, LAS ENTIDADES PÚBLICAS SIGUEN REFORZANDO SU POSTURA DE SEGURIDAD, MIENTRAS SE APOYAN EN LAS NORMATIVAS DE SEGURIDAD PARA AFRONTAR DESAFÍOS COMO LA COMPLEJIDAD TECNOLÓGICA Y ORGANIZATIVA, LA REALIDAD DEL LEGACY, LA FALTA DE PERSONAL CUALIFICADO O LA RESISTENCIA AL CAMBIO.

Según datos oficiales de INCIBE en 2024 se produjeron en España más 100.000 ciberataques, el 70% de ellos a organizaciones privadas y entidades públicas. Se trata de un incremento del 16% respecto a 2023, del 300% si tomamos como referencia el 2015. La compleja situación geopolítica contribuye a este crecimiento, particularmente en el sector público. A principios de marzo se supo de una oleada de ciberataques a instituciones españolas por parte de grupos prorrusos, una avalancha que supuso un incremento del 750% de ataques en una semana.

Las Administraciones Públicas llevan varios años digitalizándose a un ritmo muy rápido, lo que, igual que en el sector privado, ha supuesto un enorme aumento de la superficie de exposición. Pero la situación de las entidades públicas es





**“Actualmente existe una mayor concienciación con la ciberseguridad, pero hay que llegar a la sensibilización proactiva para que todos estemos realmente alineados y podamos combatir de forma más eficiente las ciberamenazas”**

Ignacio Pérez, director de estrategia de ámbitos, **Agència Cyberseguretat de Catalunya**

además muy compleja y muy diversa, compuesta tanto de municipios muy pequeños como de grandes urbes, de estructuras estatales, empresas públicas, agencias transversales, entidades regionales y una variedad de tecnologías, políticas y estrategias. Y con factores que de algún modo distorsionan su postura de seguridad, como los



**“El Esquema Nacional de Seguridad no es una finalidad en sí mismo, sino un medio para poder lograr una postura de seguridad adecuada”**

David Esteban, director de serveis de seguretat de la informació, **Ajuntament de Barcelona**

ciclos políticos o los tiempos de implantación sujetos a las licitaciones.

Hemos podido conocer de primera mano el trabajo de protección de las Administraciones Públicas ante el aumento constante de las ciberamenazas en un observatorio en el que han participado representantes de la **Agència Cyberseguretat de Catalunya**, el **Ajuntament de Barcelona**, el **Ajuntament de Girona**, la **Diputació de Tarragona**, **Isdefe** (Ingeniería de Sistemas para la Defensa de España) y **SEGIPSA**, la



**“Los ayuntamientos son cada vez más conscientes de las ciberamenazas y del impacto que supone no tener una buena postura de ciberseguridad”**

Marc García, director de seguridad informática, **Ajuntament de Girona**

Sociedad Mercantil Estatal de Gestión Inmobiliaria de Patrimonio, en una mesa redonda que ha contado con el apoyo de **SonicWall** y **Stormshield**.

### **UNA REALIDAD DIFERENTE EN LAS ADMINISTRACIONES PÚBLICAS**

A pesar de la compleja situación que se vive, el trabajo realizado en los últimos años está dando sus frutos. En la mesa hubo un consenso generalizado en que la postura de seguridad es en todo caso mu-





**“La ciberseguridad ha pasado de ser un problema de delincuencia a convertirse en una parte importante de los conflictos internacionales”**

Daniel Acuña, director de operaciones, **Isdefe**

cho mejor que en 2020, cuando la pandemia sirvió como disparador de la digitalización. La concienciación es uno de los terrenos en los que más se ha avanzado: aunque queda mucho por hacer, sin duda es mucho mayor que la de hace cinco años.

Así, Ignacio Pérez, director de estrategia de ámbitos en Agència Ciberseguretat de Catalunya, considera que, “desde luego, creo que estamos mucho mejor que hace unos años. Según la memoria de 2024 de la Agència Ciberseguretat de Catalunya, en las administraciones públicas catalanas se han



**“Pensamos más en legacy de software, pero también lo hay de hardware, y la mejor forma de afrontar ambos es a través de su impacto en la continuidad de negocio”**

Jesús Valverde, responsable de seguridad de la información, **SEGIPSA**

producido más de 7.000 millones de ataques, de los cuales hemos gestionado más de 3.300 ciberincidentes: cada dos horas y media estamos gestionando un ciberincidente. Esto supone un 26% más de lo que pudimos gestionar en el 2023. Hay más ciberincidentes, pero la mayor parte de ellos son leves. ¿Por qué? Porque somos capaces de detectar muchos más y hacerlo antes, con lo cual no son tan graves como los que estábamos sufriendo otros años. Ade-



**“La responsable de comunicación es uno de los puestos más importantes en el comité de ciber crisis, una figura clave en la gestión de crisis”**

Maite Velayos, jefa de servicio de la Unidad de Transformación digital y coordinación administrativa, **Diputació de Tarragona**

más, ahora colaboramos mucho más en el ámbito de la ciberseguridad”.

El observatorio también reflejó que, incluso dentro de una misma entidad, puede convivir realidades muy diferentes, con factores como la capacidad presupuestaria, la capacidad técnica, la resistencia al cambio o simplemente las decisiones estratégicas que se han adoptado. Todo ello supone diferentes niveles de madurez. Los





**PRESENTACIÓN >>** Sergio Martínez, country manager de SonicWall, explica el panorama de ciberamenazas al que se enfrenta el sector público y las principales claves para fortalecer su postura de ciberseguridad.

responsables de las entidades públicas tienen que adaptar sus estrategias para mejorar la ciberseguridad a esas diferentes realidades.

Maite Velayos, jefa de servicio de la Unidad de Transformación digital y coordinación administrativa en la Diputación de Tarragona, señala que “la realidad de las Administraciones Públicas es muy diversa. Tenemos muchos micropueblos que son puertas de

entrada de ciberataques, porque nos hemos dado cuenta de que la información de las administraciones es apetecible. Ante este panorama, la concienciación es máxima. Lo que a veces falta son recursos, en lo que entramos las Diputaciones. Nosotros formamos parte de la red de SOC, en relación directa con el CCN, ayudando a los ayuntamientos a auditarse y a implementar medidas de seguridad. En las adminis-



**“Según los datos de SonicWall, el 90% de cualquier brecha de ciberseguridad todavía tiene su origen en un error humano”**

Sergio Martínez, country manager, **SonicWall**

traciones más pequeñas, también es un reto interno la concienciación del personal: aún cuesta trasladar esta conciencia de la seguridad a todos los niveles”.

### **LA PALANCA QUE SUPONEN LAS NORMATIVAS DE SEGURIDAD**

La cuestión de las normativas de ciberseguridad fue una de las constantes en el desarrollo del observatorio. Si la profusión de noticias sobre ciberataques que llegan a los telediarios ha contribuido a mejorar la conciencia general sobre la ciberseguri-





**PRESENTACIÓN >>** Borja Pérez, country manager de Stormshield, explica cómo la ciberseguridad juega un papel muy importante en aspectos como la soberanía digital que se está potenciando desde la Unión Europea.

dad, las normativas suponen una importante palanca para mejorar la postura de seguridad, logrando el apoyo de la dirección, impulsando acciones específicas y logrando canalizar las inversiones de fondos como Next Generation EU.

El marco normativo en el que se mueven las Administraciones Públicas es el Esquema Nacional de Seguridad, en el que tienen que estar certificados todos los proveedores del sector. También es cada

vez mayor el número de entidades públicas certificadas aunque, nuevamente, la situación no es la misma para un pequeño ayuntamiento que para entidades con mayor capacidad presupuestaria y más personal especializado. También NIS2, bastante alineada con ENS, afecta al sector público.

Jesús Valverde, responsable de seguridad de la información en SEGIPSA, detalla que “en la organización hay una voluntad clara de mejorar la cultura



**“Antes cualquier evento en el mundo real tenía una consecuencia en el mundo ciber; ahora ya no hay separación entre uno y otro”**

Borja Pérez, country manager, **Stormshield**

de seguridad, cumplir con todo aquello que exige la norma y otras cosas que se demuestra que son importantes. Ya teníamos el Esquema Nacional de Seguridad a nivel básico, pero desde la presidencia de SEGIPSA se ha marcado para este año 2025 y 2026 la ciberseguridad como un objetivo estratégico. El ENS es un apoyo muy importante: solo con el catálogo de productos y soluciones de CCN, ya puedes establecer un primer filtro. Respecto a las terceras partes, hemos actualizado nuestra Política de Seguridad, la hemos colgado en la web y



la comunicaremos a todos los proveedores. En las renovaciones o los siguientes pliegos, se va a exigir la declaración responsable de cumplimiento de dicha política y unas medidas de seguridad acordes al servicio que van a dar”.

Por su parte, Marc García, director de seguridad informática del Ajuntament de Girona, explica que “el Esquema Nacional de Seguridad certifica que aplicamos una metodología de ciberseguridad. Para nosotros ha significado un cambio de madurez. El departamento de TI ha liderado la certificación al ENS, pero en ella han colaborado otros departamentos del ayuntamiento. El simple hecho de elaborar la política de seguridad y que se tenga que aprobar en

el Pleno ya supone llegar a sitios donde hasta ahora no llegábamos. Adoptar la metodología del ENS nos ha ayudado a llegar a muchos sitios y a lograr que la seguridad ya no se vea como algo solamente de informática, sino que compete a toda la organización”.

Aunque los procesos de certificación pueden llevar un tiempo, la visión de los proveedores también es positiva en este sentido. Borja Pérez, country manager de Stormshield, indica que, “muchas veces, el ciudadano no es consciente del nivel de colaboración que hay entre distintas administraciones. El trabajo del CCN seleccionando tecnologías y redactando guías para la adecuación al Esquema Nacional de Ciberseguridad es de gran ayuda. Las certifica-

ciones del CCN no solo sirven a las Administraciones para seleccionar proveedores o tecnologías, sino que para los fabricantes nos es de mucha utilidad. En el proceso de certificación se establece un diálogo entre el CCN y el fabricante. Los proveedores aceptan sugerencias del CCN para mejorar el producto y el CCN acepta sugerencias de los fabricantes para establecer buenas prácticas”.

### GRANDES RETOS DEL SECTOR

Unas buenas prácticas que ayudan a mejorar la capacidad de las entidades públicas para afrontar los retos que tienen por delante. David Esteban, director de serveis de seguretat de la informació del Ajuntament de Barcelona, hace un buen resumen de la situación actual: “Estamos en un contexto de automatización, inteligencia artificial, sistemas legacy, redes OT, proveedores conectados directamente a tu red, falta de talento, falta de personal. Para afrontarlo, debemos levantar la cabeza y mirarlo de forma global: hablamos de IT, de OT, de seguridad física. Hay que crear y potenciar una cultura de gestión de riesgos para hacer foco en lo que realmente es importante. Y hacer corresponsable a toda la organización de la seguridad, para lo que hay que crear la cultura de seguridad, ayudando a los equipos a hacer mapas de riesgos y modulando nuestro discurso en función de cuáles son los riesgos o el impacto que preocupa. Y hay que ser ciberresilientes: debemos estar preparados para tener un incidente. La diferencia la marcará cómo de rápidos y ágiles seamos gestionando la crisis”.



Daniel Acuña, director de operaciones de Isdefe (Ingeniería de Sistemas para la Defensa de España, empresa pública que conforma la ingeniería del Ministerio de Defensa y cuya presidenta es la actual Secretaria de Estado de Defensa), explica que “uno de los retos más importantes a los que nos hemos enfrentado es la gestión del cambio, las personas que se resisten a adoptar ciertos procedimientos que les causan inconvenientes. También es muy complicado transformar todo el legacy. Hay tecnología que no está en el Esquema Nacional de Seguridad y a veces cambiarla afecta al funcionamiento habitual de la organización o a los procedimientos internos. El tercer gran desafío es exigir a los proveedores también el Esquema Nacional de Seguridad y los procedimientos adecuados”.

El experto señaló durante el observatorio la relación cada vez mayor entre la ciberseguridad y la Seguridad Nacional, en lo que se ha dado en llamar ciberdefensa. Recordábamos al inicio del artículo la campaña de ciberataques contra instituciones públicas españolas en una sola semana, en un ejemplo de la influencia geopolítica de este sector, a menudo en el listado de los tres más atacados en todo el mundo, junto a otros que también son esenciales para la estabilidad de un país, como las industrias críticas o el sistema sanitario. Si bien es una situación que ya existía antes, se ha incrementado en los últimos años.

Los fabricantes de tecnología son sensibles a todos los cambios que se van produciendo en el sector. Sergio Martínez, country manager de Soni-

cWall, explica que, “en el último año, hemos cambiado un poco nuestro enfoque hacia dos ámbitos que están subiendo mucho. Por un lado, el cambio en el tipo de tecnología de acceso remoto, desde los portátiles y todos los endpoint: hay que modernizar el acceso remoto y hacerlo más acorde con los tiempos partiendo de estrategias de Zero Trust. Por otro lado, hemos construido una serie de SOC's y damos el servicio de SOC as a Service a entidades más pequeñas, ayuntamientos y administraciones públicas que no pueden permitirse disponer de un SOC propio”.

### EN UNA SITUACIÓN DIFÍCIL... MÁS PREPARADOS QUE NUNCA

Es cierto que la situación general es más compleja: incremento de la superficie de exposición a los ciberataques devenido de la digitalización acelerada; aumento constante de las ciberamenazas propiciado por tecnologías como la automatización y la inteligencia artificial; tensa situación geopolítica que pone a las instituciones públicas en el foco del cibercrimen, más allá del atractivo de los datos; escasez de personal cualificado; diferentes ciclos políticos que a veces impactan sobre las estrategias de seguridad...

...Y, sin embargo, las instituciones públicas están mucho más preparadas que antes para hacer frente a estos retos. Si bien aun queda mucho camino por recorrer, la cultura de la ciberseguridad está empezando a permear a todos los niveles, el trabajo de organismos como CCN-CERT está ayudando en la

evolución segura del sector y los marcos normativos como el Esquema Nacional de Seguridad y NIS2 están impulsando la apuesta por la ciberseguridad. Por último, el trabajo de los profesionales del sector, con profunda vocación de servicio público, está dando sus frutos para fortalecer la postura de seguridad de las Administraciones Públicas. ■

MÁS INFO +

- » [IX Foro de Administración Pública Digital: Eficiencia operativa del dato inteligente en la Administración Pública](#)
- » [Por qué necesitamos una nueva ciberseguridad](#)
- » [Soberanía digital europea. Ahora o nunca](#)
- » [Entrevista a Daniel Acuña, director de operaciones de Isdefe](#)
- » [Ponencia sobre “La compleja configuración del ENS en los procedimientos de compra pública”, por Enrique Arconada, consultor jurídico de Kalaman Consulting](#)



COMPARTIR EN REDES SOCIALES





**STORMSHIELD**

# **Stormshield, ciberseguridad industrial de confianza con la certificación IEC 62443**

Protección de sistemas operacionales

Stormshield ofrece a las empresas de todo el mundo una alternativa europea de confianza para la protección de infraestructuras críticas, datos sensibles y entornos operativos.

[www.stormshield.com](http://www.stormshield.com)





**PLAN ESTRATÉGICO DE LA AEPD 2025-2030 >>** Hablamos con Francisco Pérez Bes, nombrado recientemente adjunto a la presidencia de la Agencia Española de Protección de Datos, sobre la estrategia de la Agencia en los próximos años, marcada por un periodo de apertura y colaboración sectorial, por la exploración de nuevas tecnologías y el impacto que tiene sobre ella la Ley de Inteligencia Artificial.



**IMPACTO DEL DATO EN LA DIGITALIZACIÓN DE LAS ADMINISTRACIONES PÚBLICAS >>** Christian Cobas, director de la Oficina del Dato en la Junta de Comunidades de Castilla-La Mancha, explica en esta entrevista qué ha supuesto para su institución la reciente creación de la Oficina del Dato. Además, detalla las mejores prácticas de gobierno de los datos y su impacto sobre la digitalización de las AAPP.



**TECNOLOGÍAS CLAVE PARA LA DIGITALIZACIÓN DE LA SALUD >>** Rafael Pastor, jefe del Servicio de Informática del Servicio Andaluz de Salud, explica en esta entrevista cómo trabaja su entidad en la digitalización y cuáles están siendo las tecnologías más relevantes en su evolución. Especialmente sensible en su vocación de servicio al ciudadano, el sector sanitario se centra en la experiencia digital del ciudadano.



**PRINCIPALES RETOS PARA IMPULSAR LAS INICIATIVAS DE DIGITALIZACIÓN >>** En esta entrevista, Maite Velayos, jefa de servicio de la Unidad de Transformación digital y coordinación administrativa en la Diputació de Tarragona, detalla entre otras cosas cuáles son los principales desafíos que afrontan las Administraciones Públicas en su proceso transformación, así como la hoja de ruta de digitalización que han definido.



**IMPULSANDO LA POSTURA DE SEGURIDAD DE LAS ADMINISTRACIONES PÚBLICAS >>** Daniel Acuña, director de operaciones de Isdefe (Ingeniería de Sistemas para la Defensa de España), explica cómo la ciberseguridad ha pasado a jugar un papel muy importante en la geopolítica internacional y el modo en que este nuevo escenario ha impactado en Administraciones Públicas.



**LA COMPLEJA CONFIGURACIÓN DEL ENS EN LOS PROCEDIMIENTOS DE COMPRA PÚBLICA >>** Enrique Arconada, consultor jurídico de Kalamán Consulting, detalla las claves para la configuración del Esquema Nacional de Seguridad, que tiene un papel clave en todas las licitaciones de contratación pública.



# Cómo impulsar el desarrollo de la Administración Inteligente

¡Ver todos los contenidos!



@freepik

ORGANIZA



PATROCINADOR PLATINO



PATROCINADORES GOLD



STORMSHIELD

