STORMSHIELD

CIBERSEGURIDAD PARA AUTORIDADES LOCALES

Un reto por el que las **ciudades inteligentes** no pueden esperar



www.stormshield.com

Ciberseguridad para autoridades locales

La revolución digital no ha perdonado a los servicios públicos. En los últimos veinte años, la transformación digital de las infraestructuras comunitarias y de la vida pública, impulsada por la urbanización generalizada y la explosión de las tecnologías de la información, ha ampliado la superficie de ataque de las autoridades locales y las ha expuesto a importantes retos de ciberseguridad.

Este periodo ha visto nacer el concepto de "ciudad inteligente" o "región inteligente", más eficiente gracias a las nuevas tecnologías, que incluyen un auténtico ecosistema de objetos conectados. Todo ello favorece una mejor calidad de vida y una mejor gestión de los recursos (elemento crucial en la lucha contra el calentamiento global).

Aunque el término "ciudad inteligente" se utilizó inicialmente para describir un concepto más bien tecno-céntrico, la expresión ha evolucionado con el tiempo para abarcar aspectos jurídicos, ecológicos y de otro tipo. Ya se conozca como "tecnociudad", "ecociudad" o cualquier otra palabra de moda, e independientemente de la realidad que se esconda tras este término comodín, las cuestiones de ciberseguridad tienen una importancia clave en todo experimento.

Las ciudades, las áreas intermunicipales, las áreas metropolitanas, las divisiones regionales y las regiones – inteligentes o no – están especialmente expuestos a riesgos de ciberseguridad debido a sus amplias responsabilidades. Este libro blanco expone los retos a los que se enfrentan las autoridades locales para garantizar que su transformación digital sea segura, así como las soluciones y perspectivas para garantizar que puedan seguir cumpliendo su misión de servicio público en el futuro... todo ello sin perder de vista su deber de proteger a sus electores y sus datos.

un reto por el que las ciudades inteligentes no pueden esperar

01 AUTORIDADES LOCALES Y LA CIUDAD INTELIGENTE: **LA CUESTIÓN DE LA SUPERFICIE DE ATAQUE** 07

02 AUTORIDADES LOCALES Y LA CIUDAD INTELIGENTE: **¿CÓMO PODEMOS APOYAR EL AVANCE HACIA LA TRANSFORMACIÓN DIGITAL?** 31

03 AUTORIDADES LOCALES Y LA CIUDAD INTELIGENTE: **UN MUNDO PROPIO, CON UNA MEZCLA DE CONSIDERACIONES ADMINISTRATIVAS Y POLÍTICAS** 45

04 AUTORIDADES LOCALES Y LA CIUDAD INTELIGENTE: **¿QUÉ NOS DEPARARÁ EL FUTURO?** 57

COLABORADORES



Yann Ariza

Director de seguridad de la información, Federación de municipios de Vallée du Garon

"Lo que más nos falta son recursos humanos. Necesitamos más personal a nivel intermunicipal para cubrir todas nuestras necesidades. La respuesta suele ser la externalización, pero esto plantea problemas de gestión y gobernanza".

P.38-39
Autoridades locales y la ciudad inteligente: ¿Cómo podemos apoyar el avance hacia la transformación digital?



Rodolphe de Beaufort

Director general adjunto de Gimelec

"Apoyamos la introducción de vehículos eléctricos en el mercado. Esto significa, por ejemplo, equipar casi 250.000 edificios residenciales plurifamiliares con aparcamientos con infraestructura de recarga de vehículos (EVSE) para 2035 o 2040".

P.56
¿Qué nos deparará el futuro para el concepto de ciudad inteligente?



Noël Chazotte

Jefe de producto, Stormshield

"Existen soluciones de seguridad, pero nuestro reto es adaptarlas a estos entornos y a la diversa gama de tipos de conexión de red".

P.16
Secretos de los ciberriesgos para las autoridades locales



Sébastien Dagot

Ingeniero de ventas, Stormshield

"El objetivo de los ataques dirigidos puede ser cortar el acceso a un servicio o impedir que la autoridad local se comunique con sus ciudadanos".

P.21
¿Por qué les interesan las autoridades locales a los ciberdelincuentes?



Jérôme Notin

Gerente general, Cybermalveillance.gouv.fr

"Observamos que casi el 20% de los encuestados no tiene ni idea de cómo se gestiona la seguridad informática en su autoridad local. Y lo que es aún más preocupante: el 8% de los encuestados afirma no hacer nada en absoluto para gestionar la seguridad informática".

P.24
Entrevista exclusiva sobre los principales hallazgos de la encuesta sobre autoridades locales

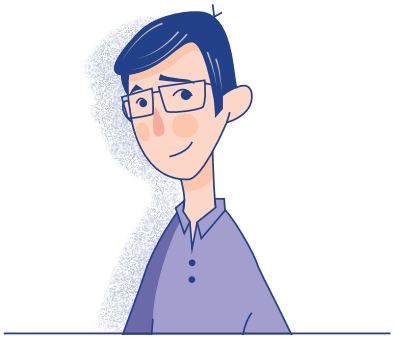


Vincent Nicaise

Responsable de partners y ecosistemas industriales, Stormshield

"A medida que las grandes ciudades recuperan el control de sus infraestructuras críticas, surge la necesidad de contratar cibertrabajadores especializados en redes industriales y sus PLCs".

P.49
Un marco regulatorio cada vez más estricto



Joël Rivallan

Presidente, ASTEE Bretagne Pays de la Loire

"El sector del agua, que tiene experiencia en realizar grandes inversiones para mejorar sus redes, necesita disponer de medios para invertir en equipos más avanzados para ponerse al día en materia de ciberseguridad".

P.51
Ciberseguridad para autoridades locales: no es (solo) cuestión de dinero



Testimonio ANÓNIMO

Director de Información de una ciudad francesa con más de 150.000 habitantes

"Hemos elaborado un ciberformulario, que ahora se cumplimenta al inicio de cada proyecto, para determinar las cuestiones y el nivel de seguridad exigido a los proveedores de servicios, en función de la criticidad del proyecto".

P.40
¿Cómo sigue las recomendaciones de las autoridades competentes?

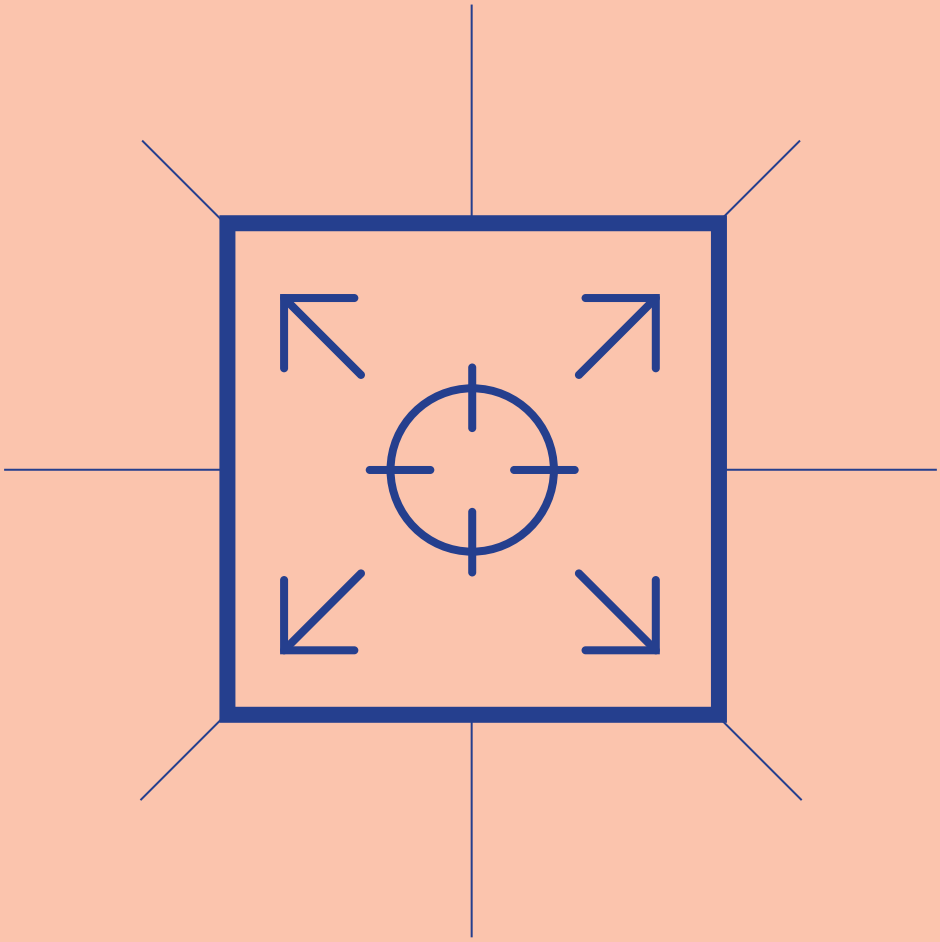
ÍNDICE

08
La transformación digital de las autoridades locales: apertura y ciberdesafíos

16
Secretos de los ciberriesgos para las autoridades locales

22
Inteligente o no, grande o pequeña: ¿Por qué les interesan las autoridades locales a los ciberdelincuentes?

26
Entrevista exclusiva con Jérôme Notin, Cybermalveillance.gouv.fr



Autoridades locales y la ciudad inteligente:

la cuestión de la superficie de ataque

Las autoridades locales, en su afán por mejorar sus relaciones con los ciudadanos, facilitar el trabajo de su personal y agilizar sus procesos y usos de todo tipo, se están digitalizando. Esto las hace más vulnerables a los incidentes informáticos y abre nuevas oportunidades a los ciberdelincuentes.

01

La transformación digital de las autoridades locales: apertura y ciberdesafíos

El concepto de “ciudad inteligente” se refiere a la decisión de un ayuntamiento, ciudad, área metropolitana, división regional o región de interconectar todos o parte de sus sistemas para crear nuevos servicios. ¿Qué riesgos plantean estas interconexiones emergentes y complejas para las autoridades locales?



La mayoría de los departamentos técnicos de los ayuntamientos reciben información cuando sus equipos fallan. Por ejemplo, si una farola funciona mal, los vecinos pueden informar directamente. En una autoridad local que haya digitalizado la gestión de su alumbrado público, por ejemplo, o en una ciudad inteligente, la propia farola inteligente informa de una avería a través de un dispositivo IIoT. Un algoritmo de mantenimiento predictivo también podría haber solicitado asistencia antes incluso de que se produjera la avería. El mismo principio de infraestructura comunicada puede aplicarse a los contenedores de recogida de vidrio, la gestión de aparcamientos, los espacios de las piscinas, etc.

Este tipo de infraestructura digital ofrece mejores servicios presenciales y a distancia, desarrolla nuevas funciones y racionaliza el consumo. Pero estas interconexiones entre sistemas informáticos tradicionales y sistemas operativos (OT) también contribuyen a crear un entorno más complejo y más difícil de proteger. Esto expone a las autoridades locales y a las ciudades inteligentes a nuevas vulnerabilidades y las obliga a afrontar el reto de la interoperabilidad.

IIoT – EL INTERNET INDUSTRIAL DE LAS COSAS

En última instancia, todas las autoridades locales se encuentran dependiendo de las nuevas tecnologías para abordar los grandes retos a los que se enfrenta la ciudad del futuro. Y aunque el alcance de la transformación digital de sus actividades varía enormemente en función de sus ambiciones y recursos individuales, todas comparten el mismo reto de garantizar que este proceso de transición sea seguro.

LAS "REGIONES" CONECTADAS SIGNIFICAN IIOT

El Internet Industrial de las Cosas hace referencia a sensores inteligentes que conectan a Internet activos físicos, como farolas o válvulas de agua. Esto permite intercambiar datos con ellos, que luego se introducen en soluciones de software.

Los servicios remotos ofrecidos a los ciudadanos son gestionados por el área metropolitana a la que pertenecemos. Sin embargo, proporcionamos a los distintos departamentos del ayuntamiento y a sus empleados servicios para agilizar la gestión operativa. Para ello, empezamos por trabajar en la ***interconexión segura entre sus redes (tanto informáticas como industriales) y los sistemas de información****".*

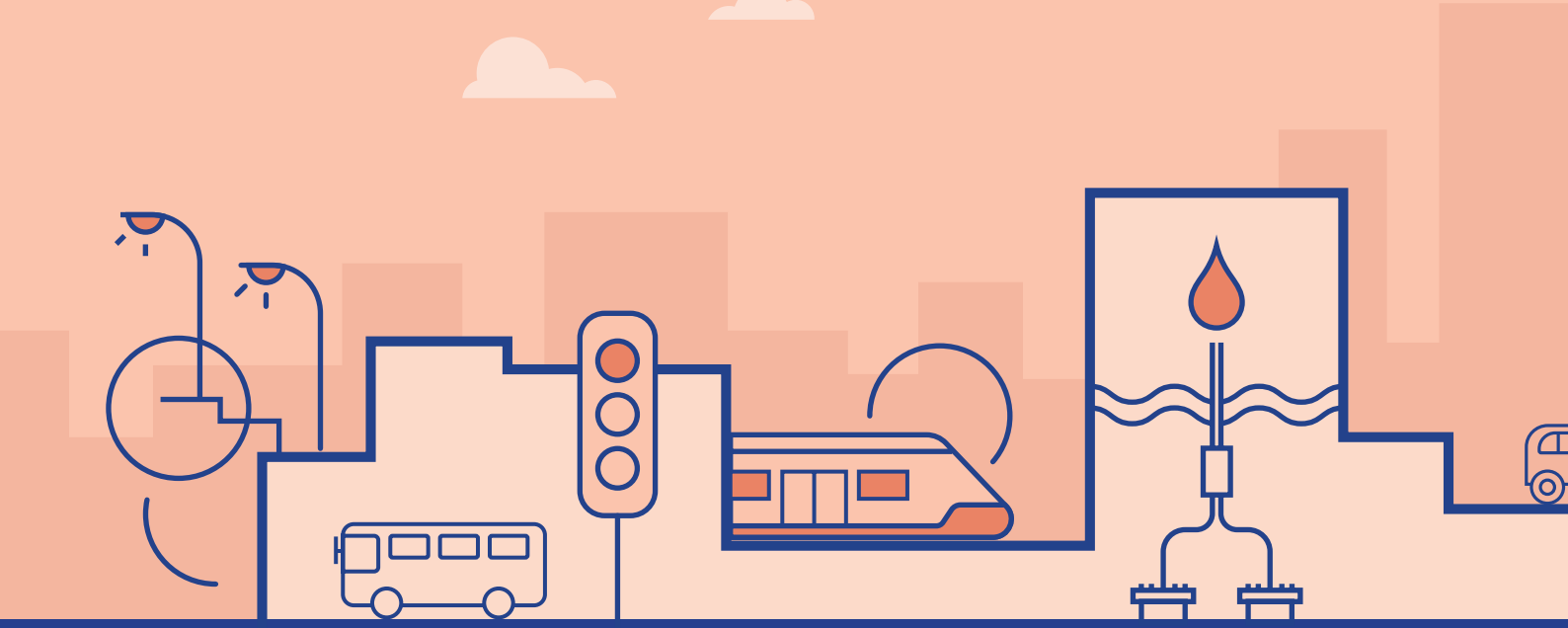
Director de Información de una ciudad francesa de más de 150.000 habitantes







Predicciones sobre las ciudades inteligentes **y los ciberriesgos asociados**



Alumbrado

Sumerge un barrio en la oscuridad pirateando el sistema de alumbrado

Señalización

Interrumpir el tráfico desincronizando los semáforos

Movilidad urbana

Interrumpir el transporte público infiltrándose en el sistema de gestión del tráfico

Agua

Crear contaminación desconectando una bomba de condensados, provocando que toda el agua se vierta a un río

Al interconectar sus sistemas esenciales, la ciudad inteligente abre nuevas oportunidades y, al mismo tiempo, amplía su superficie de ataque. He aquí una serie de ejemplos de los ciberriesgos a los que está expuesta.



Videovigilancia

Vigilar ilegalmente a personas secuestrando cámaras



Gestión técnica

Desactivar el sistema de seguridad contra incendios pirateando el sistema de gestión de edificios



Energía

Apagar la corriente electríca de un edificio público



Aparcamientos

Interrumpir la gestión dinámica de precios de aparcamiento



Rodolphe de Beaufort, Director general adjunto de Gimelec, explica las cuestiones que se plantean



¿Hacia la ciudad inteligente?

Hace casi 15 años, el mundo de los sistemas urbanos empezó a converger con el de la informática y las nuevas tecnologías. Este solapamiento dio lugar al concepto de ciudad inteligente – el cual ha madurado considerablemente desde entonces.

Aunque al principio muchos soñaban con un cuadro de mando único, varios experimentos han puesto de manifiesto la dificultad de fusionar todos los sistemas de gestión en una única plataforma.

Tras esta fase de maduración en los últimos años, volvemos ahora a un enfoque más pragmático de la ciudad conectada... un enfoque algo menos ambicioso en términos de interconexión. Las partes interesadas en las ciudades inteligentes se centran ahora en casos de uso específicos para explotar los datos que recopilan.

De este modo, la ciudad inteligente se ha dividido en partes aisladas más pequeñas. El objetivo es integrar las tecnologías de la información en las áreas OT de forma adaptada a cada área de negocio. El concepto es, por tanto, menos monolítico que antes, al menos en Europa, donde estamos obligados a trabajar con la infraestructura existente".



Secretos de los ciberriesgos para las autoridades locales

La ampliación de la superficie de ataque entre las autoridades locales en proceso de transformación digital las expone a las atenciones maliciosas de los ciberdelincuentes. Sus vulnerabilidades pueden explotarse ahora para atacar infraestructuras operativas, con consecuencias potencialmente dramáticas.

La puesta a disposición de datos accesibles, como en este caso con datos de la Metrópolis de Lyon, hace que su uso sea más destacado en las iniciativas públicas: además de informar sobre las decisiones, se convierte en una herramienta de comunicación.

Si se examinan más detenidamente, los factores que hacen que las autoridades locales sean digitalmente vulnerables pueden atribuirse a cuatro factores:

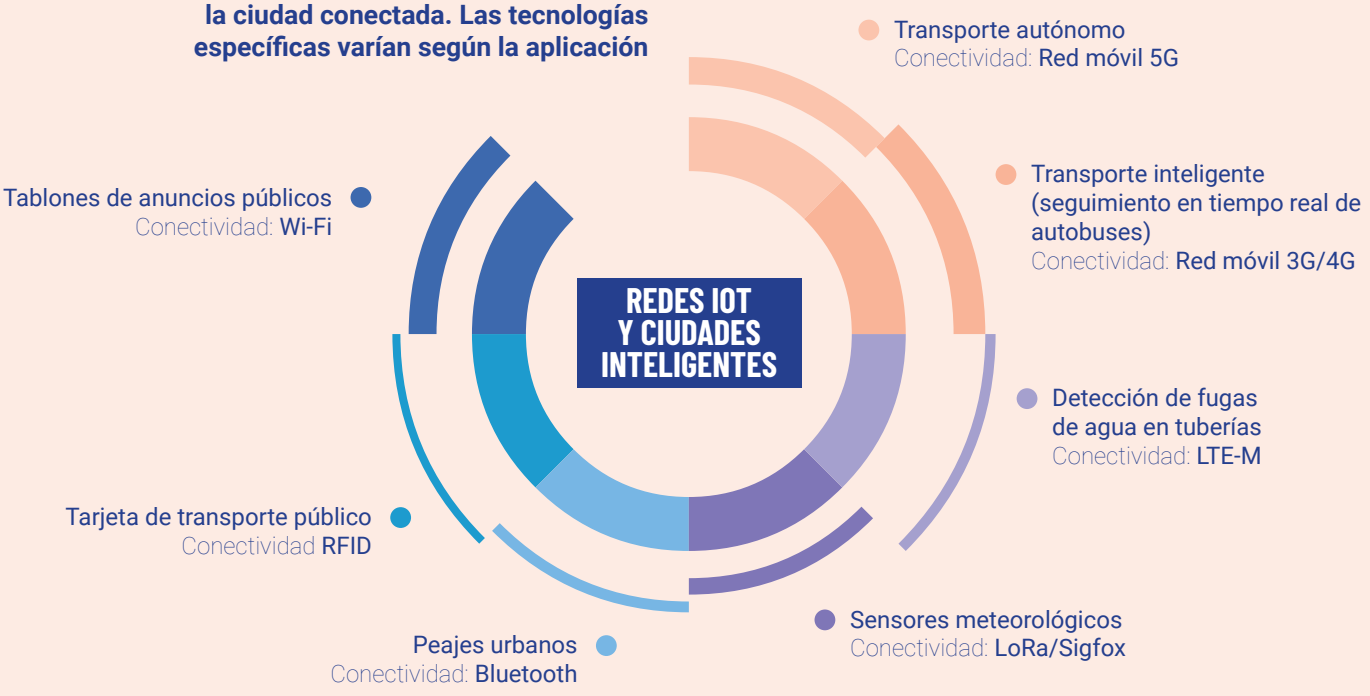
+ **Sistemas interconectados**
+ **Mantenimiento remoto**
+ **Presencia en espacios públicos**
+ **Una amplia gama de actores**

SISTEMAS INTERCONECTADOS

Los sensores instalados en el pavimento cuentan el número de vehículos que pasan. Esta información, procedente de las redes industriales, alimenta el sistema de gestión de los semáforos. Ahora también puede enviarse desde los sensores a redes informáticas, o incluso a Internet, con fines de gestión del tráfico. La integridad de estos datos debe preservarse durante su recogida, almacenamiento y tratamiento.



La conectividad está en el corazón de la ciudad conectada. Las tecnologías específicas varían según la aplicación



***Las soluciones de seguridad ya existen**: nuestro reto es tener en cuenta los cambios en estos entornos y la gran variedad de tipos de conexión a la red".*

Noël Chazotte,
Jefe de producto, Stormshield



MANTENIMIENTO REMOTO

El reto – especialmente durante y desde el periodo de COVID – ha sido proporcionar seguridad a las nuevas aplicaciones de mantenimiento remoto. La introducción generalizada del acceso remoto via VPN reduce la necesidad de viajar; por ejemplo, a ubicaciones de la red de distribución de agua que que a menudo están físicamente distantes. Pero también crea nuevas pasarelas para acceder a la infraestructura.

PRESENCIA EN LOS ESPACIOS PÚBLICOS

Los equipos de los sistemas urbanos también son más propensos al vandalismo porque son más accesibles que los armarios informáticos seguros de interior.

UNA AMPLIA GAMA DE ACTORES

Las operaciones a distancia están añadiendo nuevos actores al ya de por sí gran número de partes implicadas en las redes industriales urbanas: propietarios, contratistas y subcontratistas, todos deben cumplir las mejores prácticas en materia de ciberseguridad.

Esta situación puede provocar ataques, fallos e incluso averías, con graves repercusiones (apagones, pérdida de control, perturbaciones diversas, pérdida de datos, efectos de pánico). También puede ser aprovechada por los ciberdelincuentes (manipulación y paralización de infraestructuras urbanas, ataques de denegación de servicio, difusión de información falsa, fraudes, etc.).

A esto hay que añadir las limitadas capacidades de ciberseguridad que ofrecen los sistemas industriales. Esto se debe a la dificultad de mantener la seguridad de una base instalada heterogénea y/o no actualizable. La fiabilidad de los distintos tipos de conectividad inalámbrica también plantea cuestiones como la autenticación mutua, el cifrado y la continuidad de negocio.



CIFRA CLAVE

1 DE CADA 3 AUTORIDADES LOCALES

informan que tienen un bajo nivel de ciberprotección, según el estudio de 2023 de Cybermalveillance.gouv.fr

Incidentes y ciberataques contra autoridades locales en todo el mundo



Europa

Essen (Alemania, 2023)
Namur (Bélgica, 2023)
Sevilla (España, 2023)
Agen (Francia, 2023)
Lila (Francia, 2023)
Nápoles (Italia, 2023)
La Haya (Paises Bajos, 2023)
Olsztyn (Polonia, 2023)
Oporto (Portugal, 2023)
Gondomar (Portugal, 2023)
Bratislava (Eslovaquia, 2023)
Berna (Suiza, 2023)
Hannover (Alemania 2022)
Maguncia (Alemania , 2022)
Gijón (España, 2022)
Caen (Francia, 2022)
Palermo (Italia, 2022)
Praga (República Checa, 2022)
Leópolis (Ucrania, 2022)
Gloucester (Reino Unido, 2021)
Linz (Austria, 2021)
Lieja (Bélgica, 2021)
Turín (Italia, 2021)
Potsdam (Alemania, 2020)
Londres (Reino Unido, 2020)
Angers (Francia, 2020)
La Rochelle (Francia, 2020)
Marsella (Francia, 2020)
Frankfurt (Alemania, 2019)

Norteamérica

Montreal (Canadá, 2023)
Ottawa (Canadá, 2023)
Toronto (Canadá, 2023)
Dallas (Estados Unidos, 2023)
Pittsburgh (Estados Unidos, 2023)
Tampa (Estados Unidos, 2023)
Baltimore (Estados Unidos, 2019)
Atlanta (Estados Unidos 2018)

Olsztyn

Polonia, 2023

Oriente Medio

Teherán (Irán, 2022)

América Central y del Sur

Córdoba (Argentina, 2023)
Salvador (Brasil, 2023)
Kingston (Jamaica, 2023)
Tulancingo (México, 2023)
Quito (Ecuador, 2022)

Africa

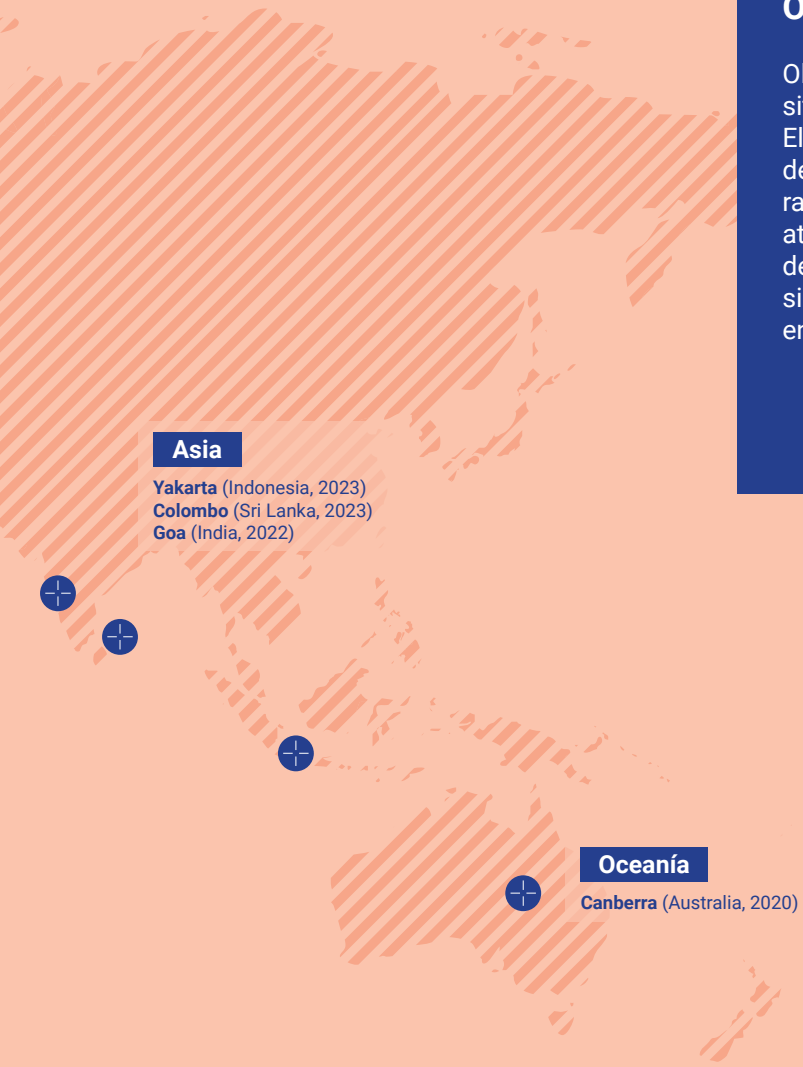
Nairobi (Kenia, 2023)
Ciudad del Cabo (Sudáfrica, 2022)
Johannesburgo (Sudáfrica, 2019)

Ninguna autoridad local del mundo es inmune a la ciberamenaza. Este fenómeno global está convirtiendo la seguridad de los datos de los ciudadanos en una preocupación clave para las autoridades locales.

Echamos un vistazo no exhaustivo a los ciberataques en todo el mundo.

Primer ciberataque reconocido contra una ciudad inteligente en Olsztyn (Polonia)

Olsztyn es una ciudad inteligente polaca situada a 200 km al norte de Varsovia. El 24 de junio de 2023, su autoridad de transportes sufrió un ataque de ransomware que provocó numerosos atascos e interrumpió la compra de billetes de transporte público. Afortunadamente, el sistema de señalización siguió funcionando en modo degradado.



Asia

Yakarta (Indonesia, 2023)
Colombo (Sri Lanka, 2023)
Goa (India, 2022)

Oceanía

Canberra (Australia, 2020)

Inteligentes o no, grandes y pequeñas: ¿por qué interesan las autoridades locales a los ciberdelincuentes?

Sea cual sea su fase de transformación digital, las autoridades locales son objeto de ataques reiterados. ¿Cómo evolucionan con el tiempo estas operaciones de amenaza? ¿Quién está detrás de ellas? ¿Qué motiva a esta red delictiva?

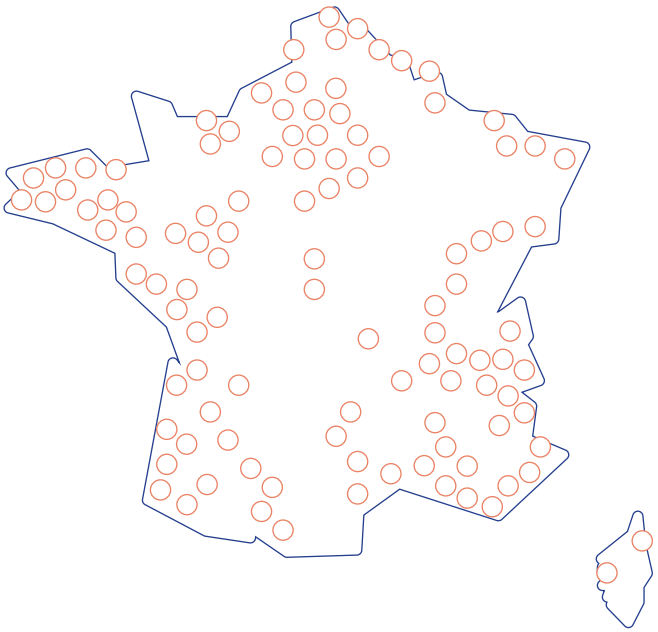
Muchas autoridades locales se ven afectadas por ataques oportunistas, o son simplemente víctimas colaterales de ataques a gran escala. Esto es lo que se observa generalmente en el caso del ransomware: **aunque las autoridades locales no son objetivo específico, se encuentran entre los miles de objetivos atacados.**

Sin embargo, las instituciones públicas se enfrentan a importantes retos relacionados con la seguridad, la continuidad de los servicios y la imagen. Por ello, a veces pueden ser el blanco de ataques debido a las molestias causadas por la interrupción de sus actividades. Por último, los datos personales sensibles tratados por el sector público pueden representar una importante ganancia financiera para los ciberatacantes que consigan obtenerlos: una foto utilizada para un documento oficial, como un documento de identidad expedido por el ayuntamiento, puede valer entre 2 y 5 euros. El precio de un expediente médico obtenido pirateando los sistemas de información de un centro sanitario de una autoridad local oscila entre 50 y 250 euros.

*En el caso de los ataques dirigidos, **el objetivo puede ser cortar el acceso a un servicio o impedir que la autoridad local se comunique con sus ciudadanos**. El modus operandi es similar al empleado contra empresas privadas, pero atacar un servicio público es a veces un acto político en la medida en que perjudica los intereses de los ciudadanos".*

Sébastien Dagot,
Ingeniero de ventas en Stormshield

Autoridades locales y hospitales públicos afectados por ciberataques



La asociación Déclic, que actúa como foro para la agrupación de estructuras de TI, es decir, operadores públicos de servicios digitales, ha elaborado este mapa para mostrar todas las autoridades locales, organismos intermunicipales, sindicatos, hospitales públicos, servicios públicos y servicios de bomberos y rescate que han sido víctimas de ciberactuaciones maliciosas desde 2019. (artículo en francés)

Una serie de ataques (poco frecuentes) contra las administraciones públicas son llevados a cabo por actores estatales como parte de un impulso para debilitar la geopolítica, o incluso como actos de guerra (como el ataque a la red energética ucraniana en 2015).

Orleans (2020), Aix-Marsella-Provenza (2020), Châlon-sur-Saône (2021), Frontignan (2022) y Caen (2022); Lille (2023), Morlaix (2023), Chantilly (2023) y también Mandeure (2023), y Beton (2023); ninguna autoridad local parece inmune. Independientemente de su tamaño o grado de digitalización, todos se ven afectados por los problemas cibernéticos.

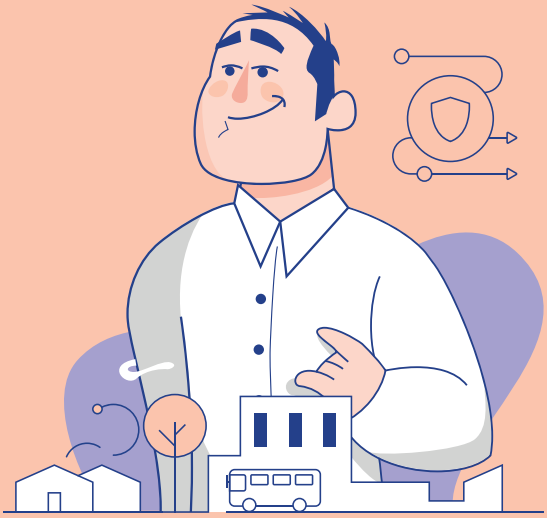
Esto es lo que impulsó al consorcio de interés público francés ACYMA a crear la plataforma Cybermalveillance.gouv.fr en 2017.

Su objetivo es sensibilizar a las autoridades locales, las pymes y los particulares sobre los problemas de ciberseguridad en Francia. El programa lleva a cabo campañas de sensibilización, la última de las cuales, a finales de 2023, será un barómetro específico de la ciberseguridad en las entidades locales de menos de 25.000 habitantes.

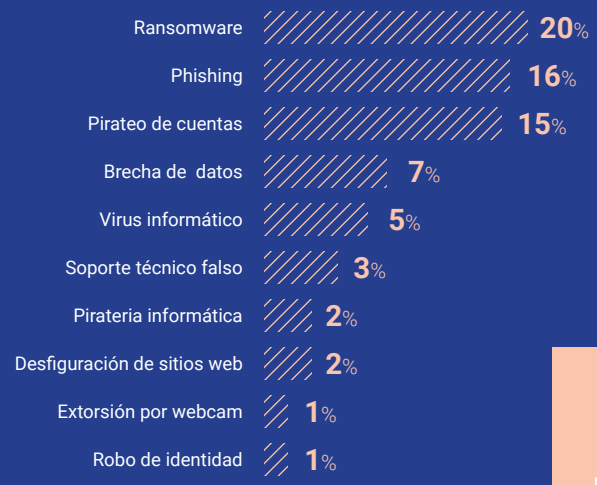
La transformación digital de la sociedad y los servicios públicos está acelerando el proceso de modernización de las infraestructuras e instalaciones de las autoridades locales. Esta carrera por la innovación en las ciudades conectadas puede tener a veces un impacto negativo en la seguridad, y un beneficio para el elemento delictivo. Entonces, ¿cómo apoyar este movimiento hacia una mayor interconectividad, garantizando al mismo tiempo una ciberseguridad completa?

*En dos ocasiones hemos detectado **intentos de pirateo por ransomware**. Afortunadamente, en ambos casos pudimos remediar la situación directamente. Dicho esto, la amenaza es alarmante. Independientemente de las consecuencias técnicas, me impresionó especialmente **el impacto humano** descrito en los testimonios de los CISO que habían sufrido las consecuencias".*

Yann Ariza, Director de seguridad de la información, federación de municipios de Vallée du Garon



PRINCIPALES BÚSQUEDAS PARA AYUDA EN LA PLATAFORMA CYBERMALVEILLANCE.GOUV.FR



CIFRA CLAVE

1 DE CADA 10 AUTORIDADES LOCALES

declaran haber sido víctimas de uno o varios ataques en los últimos 12 meses, según la encuesta de 2023 de Cybermalveillance.gouv.fr



ENTREVISTA EXCLUSIVA

Jérôme Notin, Cybermalveillance.gouv.fr

Encuesta sobre ciberseguridad en las autoridades locales: principales lecciones aprendidas

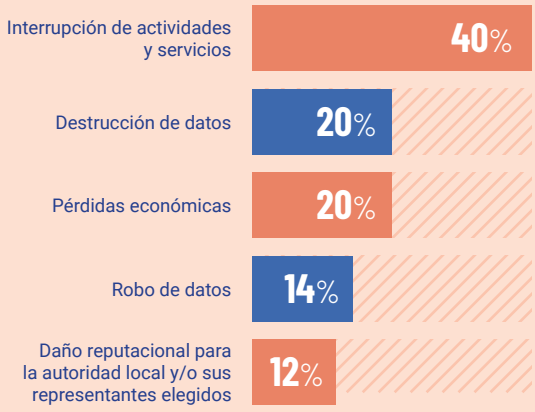


"Sólo los ciberataques a grandes autoridades locales son noticia, pero afectan a todas las entidades". Esta es la primera observación que hace el director general del plan nacional de asistencia a las víctimas de cibermalware.

La cuestión de la madurez a la hora de afrontar riesgos

Una segunda conclusión se refiere a la percepción del riesgo, ya que el 20% de las autoridades locales encuestadas son incapaces de evaluar su nivel de exposición a los ciberataques. Esta cifra puede reflejar una falta de madurez en este ámbito. *"No obstante, la concienciación sobre el riesgo está aumentando: El 33% de las autoridades locales recibía formación en 2021, frente al 78% en 2023. De hecho, una de cada tres recibía formación periódica"*. Porque las consecuencias son igual de dramáticas para las autoridades locales y sus electores.

Principales impactos de los ciberataques en la autoridades locales

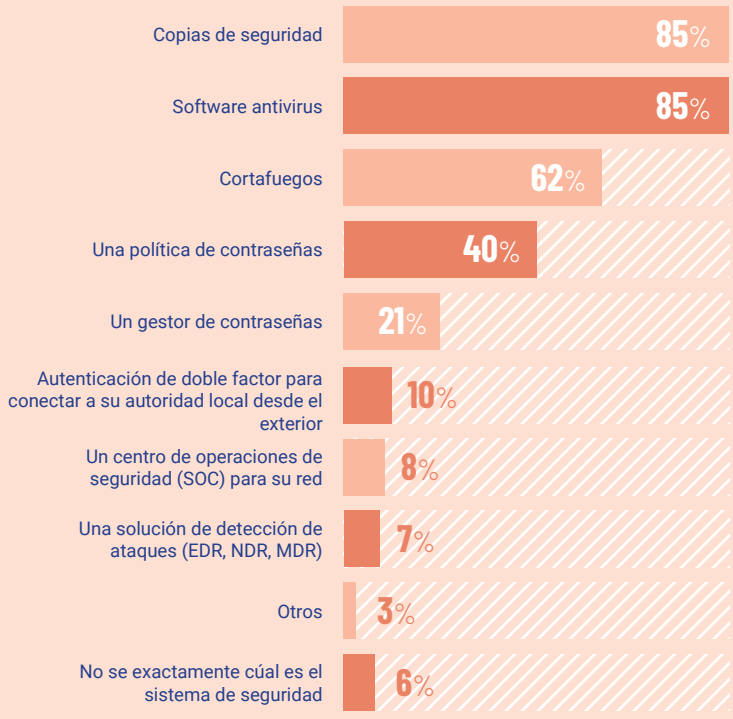


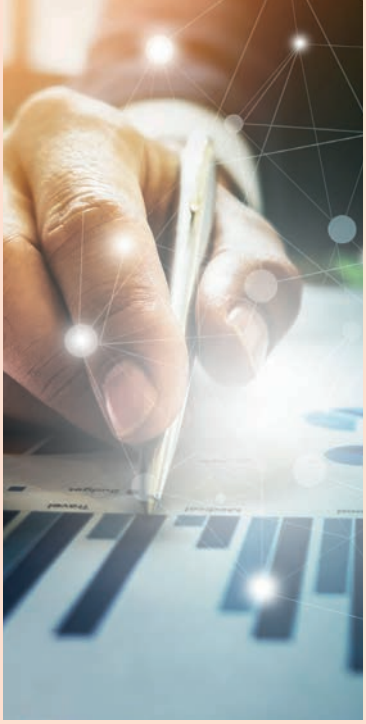
Observamos que casi el 20% de los encuestados no sabe cómo se gestiona la seguridad informática de su autoridad local. Y lo que es aún más preocupante: ***El 8% de los encuestados afirma no hacer nada en absoluto para gestionar la seguridad informática".***

La cuestión del ciberequipamiento

J.N. *La mayoría de las autoridades locales disponen de tres sistemas de seguridad por término medio, siendo los más habituales la copia de seguridad, el antivirus y el cortafuegos. Esta situación explica sin duda que una de cada dos entidades se sienta bien protegida – aunque a menudo erróneamente...*

Equipamiento de seguridad en autoridades locales





La cuestión de los presupuestos

J.N. *A pesar de las percepciones generalmente favorables, observamos que los recursos asignados a la ciberseguridad son limitados. El 65% de las autoridades locales encuestadas tiene un presupuesto anual de TI inferior a 5.000 euros, y el 75% tiene un presupuesto de ciberseguridad inferior a 2.000 euros. De ellos, sólo el 12% prevé una tendencia al alza durante el próximo año.*

Esta falta de recursos conduce a prácticas arriesgadas: una de cada dos autoridades locales no proporciona ni tableta ni teléfono, por ejemplo, con el resultado de que el 88% de los encuestados utiliza su teléfono móvil personal para trabajar. Esto representa un mayor riesgo para las autoridades locales, especialmente cuando los empleados también se ven obligados a utilizar sus propias memorias USB y ordenadores personales.

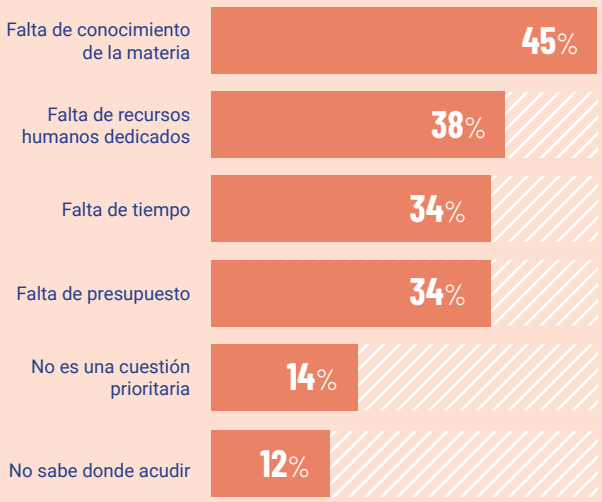
La cuestión de los obstáculos

J.N. *Sin embargo, a la pregunta de cuáles son los obstáculos a los que se enfrentan las autoridades locales en materia de ciberseguridad, el "presupuesto" se sitúa en un mero tercer puesto, al nivel de la "falta de tiempo".*

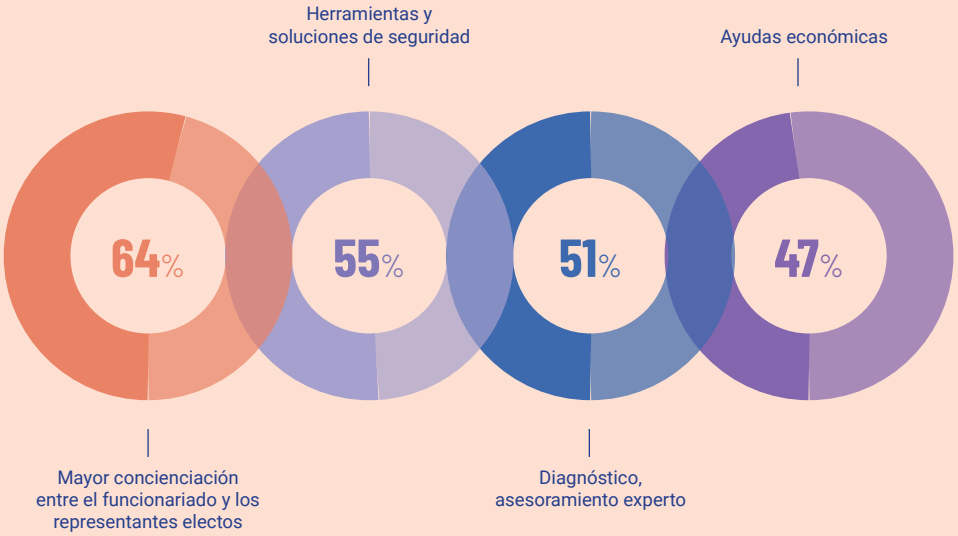
El hecho de que la falta de conocimientos sea el factor más citado (45%) refuerza nuestra convicción de que nuestras iniciativas de sensibilización son un verdadero motor. Por supuesto, una minoría de los encuestados considera que el tema no es prioritario (14%), pero el 64% de los encuestados cita la concienciación como la necesidad número uno.

Estamos asistiendo a un fuerte aumento de la concienciación, pero es necesario extenderla a todos los sectores de la población dentro de las autoridades locales, y apoyarla con medidas prácticas para garantizar que la ciberconcienciación arraigue a largo plazo. La utilización de productos de seguridad homologados por la ANSSI y algunas buenas prácticas bastan por sí solas para dar un salto cualitativo en materia de seguridad informática.

Los principales ciberobstáculos para las autoridades locales



Necesidades prioritarias en ciberseguridad de las autoridades locales



La cuestión de los requisitos

J.N. *Nuestro estudio señala las herramientas y soluciones, el asesoramiento y la mayor concienciación como los ámbitos en los que las autoridades locales tienen mayores expectativas. Estas exigencias se centran en los aspectos técnicos y humanos– un resultado que refleja una cierta toma de conciencia de los problemas.*

Esta concienciación, para que se desarrolle de forma positiva, debe llegar a todo el personal de las autoridades locales de forma regular, para que puedan establecerse pautas de comportamiento correctas a largo plazo y las autoridades locales puedan estar equipadas para hacer frente a los ciberataques.

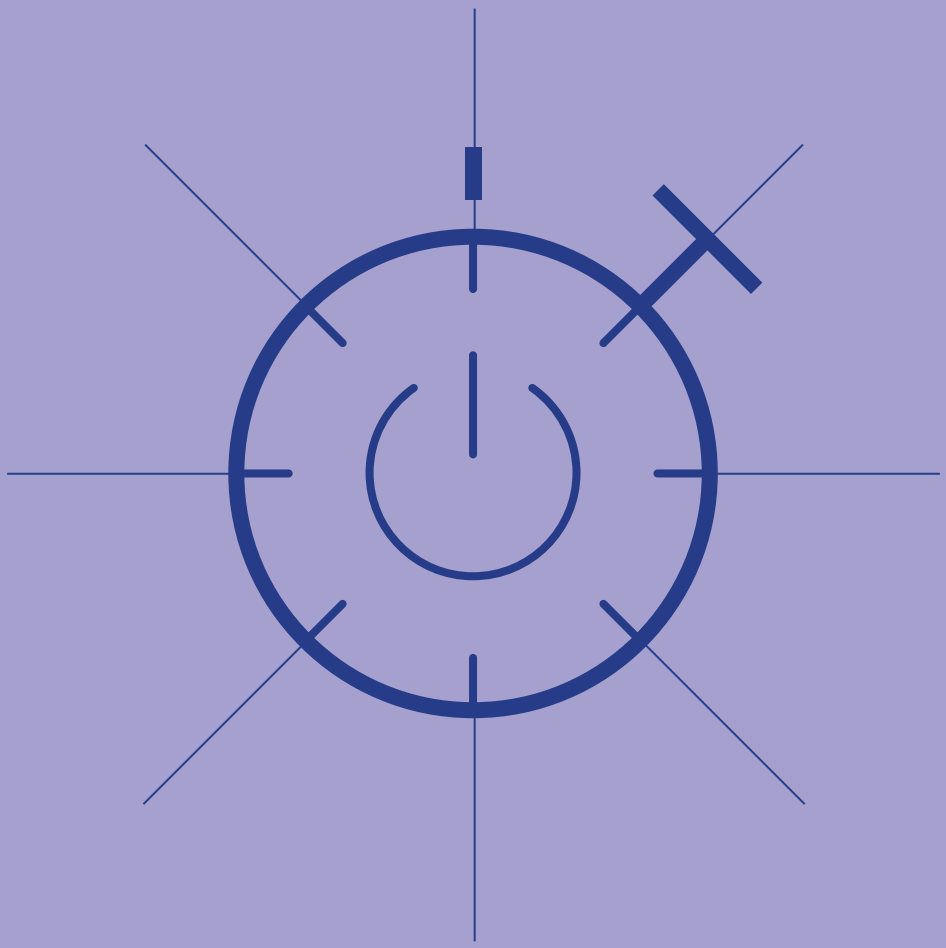
Puede leer el estudio completo aquí (Artículo en francés)

ÍNDICE

32
Consiguiendo que actores dispares trabajen juntos

36
Implementando las soluciones de seguridad apropiadas

38
Siguiendo las recomendaciones de las autoridades competentes



Autoridades locales y las ciudades inteligentes:

¿Cómo podemos apoyar la evolución hacia la transformación digital?

Mientras los ayuntamientos afrontan las crecientes incertidumbres sociales, económicas y climáticas, una cosa es segura: tarde o temprano sufrirán ciberataques. En este panorama urbano cada vez más digital, ¿por dónde deben empezar las autoridades locales en lo que a ciberseguridad se refiere?

02

Consiguiendo que actores dispares trabajen juntos

El panorama para las autoridades locales – y para las ciudades inteligentes en particular – se caracteriza por un mosaico de actores, lo que no está exento de problemas. Esta proliferación aumenta el número de conexiones que hay que proteger y puede llevar a una disminución de la responsabilidad en materia de ciberseguridad.

Por ejemplo, en una licitación dedicada a la comunidad conectada, el área metropolitana emisora indica su intención de conectar el equipamiento vial a un sistema de mantenimiento. **Esta licitación exigirá que varios actores se reúnan para responder a ella: un operador de telecomunicaciones que suministrará la tarjeta SIM integrada en el sensor IoT, un instalador, una empresa de mantenimiento, un fabricante de software, un proveedor de alojamiento, etc.** ¿Cuál de estos actores es responsable de la ciberseguridad? ¿Quién se encargará de la confidencialidad, integridad y disponibilidad de los datos? ¿El actor propietario de los datos? ¿O el que los recopila? ¿Los procesa? ¿Los agrega? ¿Todos? ¿Nadie? Es difícil responder, porque cada caso es diferente.

Y esta indefinición no se limita a los servicios externos, ya que muy pocas autoridades locales disponen de una gobernanza clara e interfuncional en materia de ciberseguridad.

Siguen existiendo grandes diferencias de madurez en ciberseguridad entre los grandes operadores nacionales de redes de agua – que están sujetos a la directiva NIS y disponen de departamentos especializados - y las estructuras de tamaño medio, como las autoridades locales, que explotan sus propias instalaciones".

Joël Rivallan,
Presidente, ASTEE
Bretagne-Pays de la Loire

La situación no es mejor en los municipios más pequeños. La gobernanza de la ciberseguridad es más fácil, pero el factor humano adquiere una dimensión totalmente nueva, porque muy a menudo una sola persona gestiona toda la cadena de aprobación. "*En los municipios más pequeños, nos limitamos a dar el visto bueno a un flujo de trabajo, en lugar de a facturas separadas. Así que no estamos tan atentos*", admitió Sylvain Le Chatton, alcalde de Liancourt-Saint-Pierre y vicepresidente de la federación de municipios Vexin Thelle (Francia), hablando de los nuevos procesos digitales de compras y pagos en una mesa redonda organizada por Cybermalveillance.gouv.fr. El funcionario también informó sobre las estafas de ayudas falsas a las que se había enfrentado el secretario de su ayuntamiento. Por último, admitió que no siempre sabía a quién dirigirse ante tal plétora de actores: ¿sugiere esto fusionar ciertos esquemas?

Esta diversidad de situaciones dificulta la aplicación de un método único. Sin embargo, en Francia, todos los ayuntamientos tienen las mismas responsabilidades y los mismos compromisos de servicio público, sea cual sea su tamaño.

Muchos casos de uso no se están desplegando porque la propia estructura de las autoridades locales está demasiado "aislada". La falta de una gestión global de nuestros sistemas urbanos hace que el proceso de intercambio de información y difusión de buenas prácticas sea complejo".

Rodolphe de Beaufort,
director general adjunto
Gimelec

Haciendo foco en las autoridades locales y en los actores de la ciberseguridad de las ciudades inteligentes



Cargos electos y administraciones locales: municipales o intermunicipales (área metropolitana, federación de municipios)

¿Su papel? Decidir sobre políticas públicas e inversiones.

Integradores

¿Su papel? Garantizar que la solución de seguridad esté integrada en el entorno de producción.

Operadores de red

¿Su papel? Gestionar la instalación y el funcionamiento de las redes de telecomunicaciones, los sistemas de seguridad informática y los sistemas telefónicos.

Fabricantes de software

¿Su papel? Crear y desarrollar soluciones de TI.

Fabricantes de hardware

¿Su papel? Fabricar los componentes de hardware que conforman las soluciones utilizadas (por ejemplo: sensores IoT).



Operadores públicos de servicios digitales

¿Su papel? Ayudar a las autoridades públicas porporcionando servicios de TI y de ciberseguridad.

Delegados del servicio público

¿Su papel? Estos actores privados son contratados para gestionar un servicio público.

Operadores

¿Su papel? Estas entidades explotan una infraestructura (por ejemplo, una red de agua), una autoridad local directamente o un tercero a través de una concesión o delegación de servicio público.

Central de compras

¿Su papel? Seleccionar proveedores de ciberseguridad de confianza.

Implementando las soluciones de seguridad apropiadas

¿Debemos resignarnos a desconectar las comunidades conectadas? ¿Dar marcha atrás en la transformación digital de los servicios al ciudadano? No, porque existen métodos de ciberprotección. Y aplicar estos métodos a las autoridades locales, avancen o no hacia una ciudad inteligente, les permitiría seguir disfrutando de los beneficios de los servicios públicos conectados.

Para garantizar la seguridad de los sistemas de información de una ciudad inteligente o de una autoridad local conectada, es necesario establecer una política de seguridad global y luego adaptarla a cada SI. Y ahí es donde a menudo se complican las cosas. Esto se debe a que, además de la amplia gama de actores implicados, **las autoridades locales tienen que combinar los retos de diferentes ámbitos de red, tanto de TI como de OT**. Y se trata de redes con prioridades divergentes y normas de seguridad diferentes.

¿QUÉ MÉTODOS PODEMOS UTILIZAR?

- ✓ Usar soluciones de confianza
- ✓ Pensar en la cibergobernanza global
- ✓ Mapear y segmentar las diferentes redes
- ✓ Implantar autenticación multifactor
- ✓ Elegir una arquitectura de confianza cero
- ✓ Focalizarse en la seguridad por diseño
- ✓ Considerar la escalabilidad de los SI y pensar en los retos del mañana y en las prácticas operativas en este momento
- ✓ Especificar cláusulas contractuales para establecer claramente áreas de responsabilidad

¿Le gustaría profundizar en el tema y ver cómo puede empezar a actuar? Nuestros expertos están a su disposición para ayudarle.



Para proteger a la comunidad conectada, no basta con garantizar que las nuevas prácticas de trabajo sean seguras: hay que tener en cuenta todos los sistemas de información existentes. Además de los aspectos técnicos y la implantación de herramientas de seguridad, los expertos en seguridad informática deben aprovechar las competencias de alcaldes, jefes de departamento y responsables de seguridad informática para concienciar al mayor número posible de personal, en función del contexto.

CIFRA CLAVE

EL 94% DE LAS AUTORIDADES LOCALES

encuestadas en el estudio francés de Cybermalveillance.gouv.fr 2023 están equipadas con al menos 1 dispositivo de ciberseguridad, pero sólo el 62% menciona el cortafuegos, el 10% la autenticación de dos factores y el 7% una solución de detección de ataques.

Siguiendo las recomendaciones de las autoridades competentes

Para facilitar la tarea de garantizar la seguridad, las autoridades han desarrollado una serie de mecanismos de apoyo y recursos para ayudar a las autoridades locales en su labor.

En Francia, la autoridad de ciberseguridad ANSSI enumera las medidas de apoyo disponibles para las autoridades locales en tres secciones: **concienciación, protección y respuesta frente a incidentes**. Esta organización ANSSI publica también guías de buenas prácticas que recomiendan el uso de productos de ciberseguridad certificados. La certificación acredita la solidez de un producto de seguridad y demuestra que su fabricante lo ha sometido a pruebas en un laboratorio independiente.



Al igual que en el caso de los robos, la presentación de una denuncia permite movilizar lo antes posible a un grupo de trabajo digital para obtener información útil para la investigación".

Christophe Husson,
Subcomandante
de la Gendarmería del
Ciberespacio ComCyberGend

Pero, al mismo tiempo, las administraciones públicas deben cumplir la normativa europea y nacional en materia de ciberseguridad, como el RGPD, la Ley de Ciberseguridad e incluso la clasificación de seguridad "EU Restricted" para Europa, y el Référentiel Général de Sécurité (RGS) o la Politique de Sécurité des Systèmes d'Information de l'État (PSSIE) en Francia. En determinadas situaciones, las autoridades locales necesitan acceder a soluciones de ciberseguridad calificadas. La calificación va más allá de la simple certificación: atestigua la confianza depositada en el producto de seguridad por el gobierno francés.

Además de las soluciones técnicas y prácticas aplicadas anteriormente, la respuesta a los incidentes está resultando ser un factor clave en la gestión de las crisis cibernéticas. Por ello, las autoridades locales francesas están obligadas a informar de los incidentes a las autoridades competentes: la CNIL y ANSSI. En el caso de un incidente de seguridad, se recomienda encarecidamente notificarlo formalmente a la gendarmería.

¿Cuál es la realidad cotidiana de las autoridades locales? ¿Cuál es su ámbito de actuación? ¿Qué tipo de estructura se está creando? Dos personas con una visión clara de los problemas de ciberseguridad en las autoridades locales arrojan algo de luz sobre el tema.

¿Cuál es la naturaleza y el alcance de su misión?

Yann A. Nuestro departamento se creó en 2018 para ocuparse del mantenimiento operativo de cuatro infraestructuras: los municipios de Brignais, Chaponost, Millery y las infraestructuras que cubren las necesidades propias de la CCVG. Los municipios de Montagny y Vourles, aunque forman parte de la federación de municipios, no benefician de esta puesta en común de recursos y competencias.

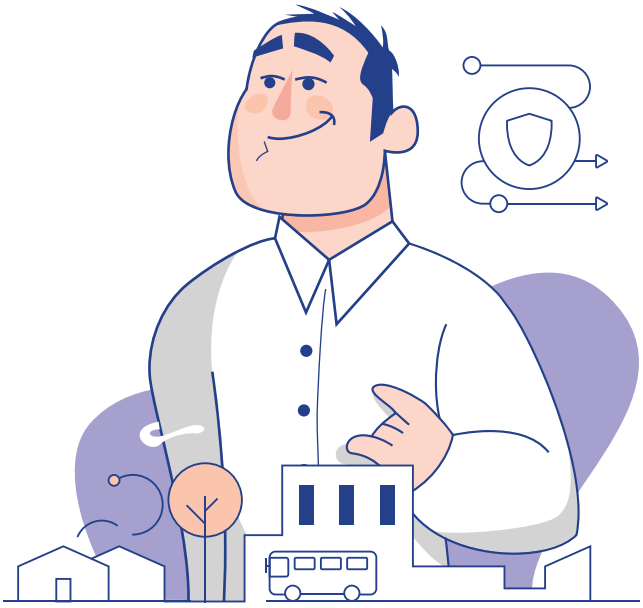
En la medida de lo posible, también nos encargamos del mantenimiento de la seguridad. Pero sólo somos cuatro, así que es difícil hacerlo todo. Gestionamos unos 1.400 terminales (estaciones de trabajo, teléfonos, tabletas) para 450 usuarios.

50 km²

más de 30.000
habitantes

200 km de carreteras

Cibersoluciones instaladas
Cortafuegos, EDR, protección del correo electrónico, copias de seguridad en la nube, DRP/BCP, virtualización.



Yann Ariza es CISO de la federación de municipios de Vallée du Garon (CCVG), en el departamento francés de Rhône.

¿Ofrece su federación local de municipios servicios a distancia? ¿Qué ha hecho para que sean seguros?

Y.A. El servicio a distancia más importante del CCGV es un portal familiar. Sirve para gestionar las inscripciones en los servicios de comedor y extraescolares y la información para el cálculo del impuesto sobre la renta. Se trata de un software comercial, porque no teníamos capacidad de desarrollo interno. Tras evaluar a varios proveedores, elegimos la herramienta que mejor se adaptaba a nuestras necesidades.

El proveedor es responsable de alojar y proteger los datos procesados, pero esta responsabilidad es compartida. A nosotros, como autoridades locales, nos corresponde hacerles preguntas y revisar el contrato para comprobar certificados, cumplimiento del RGPD, etc..

¿Qué obstáculos encuentra a la hora de tomar medidas de seguridad para las infraestructuras informáticas y operativas de su federación local de municipios?

Y.A. La comprensión de los problemas sigue siendo desigual. En general, los empleados de las autoridades locales conocen bien las ventajas de la autenticación en línea de dos factores, ya que coincide con su experiencia como particulares; por ejemplo, en el sitio web de su banco. Entienden menos el acceso remoto. A veces tienden a pensar que los datos públicos no son sensibles. Así que tenemos que seguir concienciándoles, sea cual sea su nivel de responsabilidad, para mejorar la seguridad general.

También está la cuestión de los costes. Por ejemplo, las suscripciones son una partida importante de los gastos de funcionamiento. Pero con un presupuesto cada vez mayor, lo que más nos falta son recursos humanos. Necesitamos más personal a nivel intermunicipal para cubrir todas nuestras necesidades. La respuesta suele ser la externalización, pero esto plantea problemas de gestión y gobernanza.



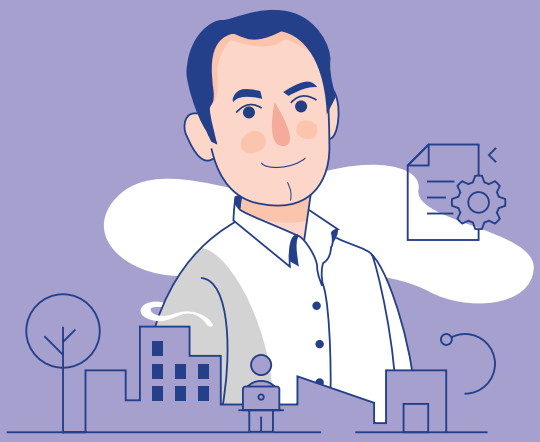


Estamos realizando una gran labor de concienciación entre los departamentos empresariales; comprenden los problemas, pero no siempre las implicaciones.
Y funciona.

Hemos elaborado un ciberformulario, que ahora se cumplimenta al inicio de cada proyecto, para identificar los problemas y el nivel de seguridad exigido a los proveedores de servicios, en función de la criticidad del proyecto.

La dificultad reside ahora principalmente en el desfase entre nuestros requisitos cibernéticos y el nivel de madurez de los fabricantes e instaladores de IoT. Todavía han recibido muy poca formación en estas cuestiones".

Testimonio del CIO de una ciudad de más de 150.000 habitantes.



ÍNDICE

46
Un marco regulatorio cada vez más estricto

50
El papel de los políticos

52
Ciberseguridad para autoridades locales:
no es (solo) una cuestión de dinero



Las autoridades locales y las ciudades inteligentes

un mundo propio, con una mezcla de consideraciones administrativas y políticas

Las cuestiones administrativas y regulatorias adquieren una dimensión específica en el sector público. Por definición, la política también desempeña aquí un papel importante. A medida que avanzan los proyectos experimentales, estos aspectos van configurando poco a poco el perfil ético y jurídico de la ciudad inteligente.

03

Un marco regulatorio cada vez más estricto

A lo largo de los años, el marco regulatorio de las comunidades conectadas se ha ido ampliando. ¿El objetivo? Reforzar la confianza de los usuarios en los servicios digitales y proporcionar un marco para la transformación digital de las administraciones, mejorando al mismo tiempo la seguridad de los datos personales.

El establecimiento de un marco regulatorio y jurídico pretende proteger los sistemas de información de las entidades locales inmersas en una transformación digital de mayor o menor calado.

En Europa, se basa en los tres principios fundamentales de **gobernanza, gestión de riesgos y mejora continua**, y su objetivo es garantizar la seguridad de las interacciones, los datos y los actores críticos.

Este marco regulatorio se explica detalladamente en la guía específica del ANSSI (Artículo en francés)



Seguridad para las interacciones

Todos los servicios a distancia en los que participen tanto usuarios como autoridades administrativas deben cumplir los requisitos de seguridad establecidos en el Référentiel général de sécurité (RGS) de la Administración francesa. Este marco define aspectos como el proceso de cualificación de los proveedores de servicios de confianza. El reglamento eIDAS también proporciona un marco complementario para las interacciones digitales entre el sector público y los ciudadanos (identificación electrónica, etc.). Estos dos textos se solapan a veces; por ejemplo, en materia de seguridad de las firmas electrónicas.

Dado que aumenta el riesgo legal, la normativa es un activo valioso para aumentar el nivel general de ciberseguridad de las autoridades locales".

Yann Ariza,
Director de seguridad de la información, federación de municipios de Vallée du Garon

Seguridad para los datos

Algunos de los datos recogidos por las ciudades conectadas son de carácter personal. Como tales, están cubiertos por el Reglamento General de Protección de Datos (RGPD). Algunas autoridades locales tratan datos sanitarios que deben estar cubiertos por medidas de alojamiento específicas, amparadas por la certificación HDS. Es el caso de los departamentos, con los datos de las Maisons Départementales pour les Personnes Handicapées (MDPH), residencias para personas discapacitadas, y también de los municipios, con los Centres Communaux d'Action Sociale (CCAS), centros de acción social. Jean-Michel Morer, alcalde de la ciudad francesa de Trilport (77) y representante de la Association des Petites Villes de France (APVF) (Asociación de Pequeñas Ciudades de Francia), señaló que "*a la hora de gestionar los riesgos, ahora hay que tener en cuenta la nube*".

Seguridad para los actores críticos

En Europa, la Directiva sobre Seguridad de las Redes y de la Información (NIS), adoptada el 6 de julio de 2016, establece normas de seguridad específicas para los operadores de servicios esenciales (ESO), de los que forman parte algunas autoridades locales. Así, estas entidades deben identificar sus sistemas de información esenciales (SIE) y mantener un análisis de riesgos actualizado para ellos. Otras normas observadas son las auditorías de seguridad periódicas, la compartimentación de cada SIE, la protección de los accesos remotos y la implantación de un servicio de tratamiento de las alertas transmitidas por la ANSSI.

La nueva versión de esta directiva europea, conocida como NIS2, se aprobó en noviembre de 2022. Actualmente se está transponiendo a las legislaciones nacionales de todos los países de la UE. En el marco de su transposición a la legislación francesa, ANSSI está trabajando con todas las asociaciones profesionales de los sectores afectados (agua, energía, sanidad, etc.) para adaptar la ley a los retos específicos a los que se enfrenta cada sector.

NIS2: trabajando para un mayor número de partes interesadas en Europa

La NIS2 ya prevé una ampliación sin precedentes del ámbito de aplicación. Un número significativo de autoridades locales se convertirán en Entidades Esenciales o Entidades Importantes, y los agentes de su cadena de suministro – en particular en los ámbitos de la gestión de residuos, el agua y la tecnología digital – estarán sujetos a los mismos requisitos. La nueva normativa también prevé un mecanismo sancionador reforzado para garantizar la aplicación de la ley.

Paralelamente a la NIS2, las infraestructuras clave gestionadas por las autoridades públicas francesas (energía, agua, transportes, etc.) están clasificadas muy a menudo como operadores de importancia vital (OIV) y, como tales, deben cumplir las obligaciones de ciberseguridad establecidas en la Ley de Planificación Militar (LPM) francesa.

¿Y dónde entran las normas de comercialización? Además de las normas puramente de ciberseguridad, varias normas técnicas – específicas de cada línea de negocio – incluyen un componente ciber. Pero son la excepción y no la regla.

Este conjunto de normas contribuye a reducir el riesgo de violaciones de la seguridad informática al aumentar el riesgo legal en caso de que no se protejan los datos de personales o de otro tipo.

La vigilancia es necesaria

A diferencia de otras legislaciones, las entidades sujetas a la NIS2 no recibirán ninguna notificación al respecto. Por tanto, corresponde a cada autoridad local ser proactiva y averiguar si está obligada o no a cumplirla.

¿Necesita más información sobre los aspectos regulatorios?
Nuestros expertos está aquí para ayudarle.



El sector del agua cuenta con poca legislación que aborde la cuestión de la ciberseguridad. Se mencionan algunos requisitos básicos, pero en lo que respecta a la seguridad de los dispositivos industriales, se trata de un área nueva para nosotros y nuestros marcos”.

Joël Rivallan,
Presidente, ASTEE Bretagne
Pays de la Loire

El papel de los políticos

La ciberseguridad en las organizaciones tiene siempre una dimensión humana, vinculada a las competencias y a la concienciación. En el caso de las autoridades locales, este aspecto se ve reforzado por la influencia de la política: ésta define las prioridades, pero los plazos electorales y los imperativos de ciberseguridad no siempre coinciden.

Trabajar en el sector público no está exento de peculiaridades: las prioridades pueden cambiar con los vaivenes de la vida política. En Estados Unidos, Sudamérica y Asia, los equipos municipales se eligen una vez cada 4 años; en Francia, cada 6 años. Sin embargo, la concienciación sobre los problemas de ciberseguridad varía a veces en función de las sensibilidades individuales, y puede afectar al nivel de prioridad concedido al tema. Esta dependencia conduce a una falta de claridad que puede comprometer la continuidad del trabajo de los expertos en ciberseguridad.

"A medida que las grandes ciudades recuperan el control de sus infraestructuras críticas, necesitan contratar ciberespecialistas en redes industriales y sus PLCs".

Vincent Nicaise,
Responsable de partners y ecosistemas industriales, Stormshield



"La adopción generalizada de buenas prácticas en materia de ciberseguridad en las autoridades locales requiere un compromiso político a largo plazo. Por eso es importante que estas cuestiones no se deleguen en el ámbito local".

Rodolphe de Beaufort,
Director general adjunto de Gimelec

La decisión de externalizar o internalizar competencias depende también de la voluntad política. En Francia, en 2020, la Autoridad Metropolitana de la ciudad de Lyon decidió asumir la gestión de la producción y distribución de agua potable. Esta decisión significa que ahora es responsable no solo de la seguridad del suministro de agua, sino también de la ciberseguridad de las redes operativas e informáticas implicadas en el proceso.

En el otro extremo, el 57% de los responsables informáticos de las entidades locales de menos de 3.500 habitantes declararon en 2021 no haber recibido formación en seguridad digital. Poner en común las competencias de varios entes locales – como hace el CCVG y recomienda el Senado francés – parece una solución más asequible que tener un CISO en cada ente local.

Ciberseguridad para autoridades locales: no es (solo) una cuestión de dinero

Aunque los presupuestos son la parte esencial de la guerra de ciberseguridad en todos los sectores, las autoridades y administraciones locales tienen procesos de compra muy específicos que las diferencian de otras organizaciones. La comunidad conectada y la ciudad inteligente tienen que formar parte de esto.

¿Se está quedando sin financiación la ciberseguridad de la comunidad conectada? Es difícil dar aquí una respuesta inequívoca, dado que la disparidad de los actores descrita en las páginas 26-27 se corresponde con las disparidades presupuestarias.

A pesar de ello, la mayoría de las autoridades locales dedican aparentemente menos del 10% de sus presupuestos de TI a la ciberseguridad, por debajo de la recomendación de la ANSSI. En el marco del componente de ciberseguridad del plan de recuperación de France Relance (2020), se ha confiado a la agencia la gestión de un fondo de 136 millones de euros. Estos recursos, a veces considerados insuficientes, están destinados a reforzar la seguridad de los sistemas de información utilizados por los organismos públicos, las autoridades locales, los ministerios y los establecimientos sanitarios.



El sector del agua, que tiene experiencia en realizar grandes inversiones para mejorar sus redes, necesita disponer de medios para invertir en equipos más avanzados para ponerse al día en materia de ciberseguridad".

Joël Rivallan,
Presidente, ASTEE Bretagne - Pays de la Loire

El principal obstáculo a la ciberseguridad para las autoridades locales son los recursos humanos: tienen dificultades para contratar a las personas adecuadas. No obstante, sigue habiendo mucho en juego desde el punto de vista financiero, y queda por ver cómo apoyarán las autoridades públicas la aplicación de los nuevos requisitos NIS2, especialmente en las organizaciones más pequeñas".

Sébastien Dagot,
Ingeniero de ventas en
Stormshield



Por desgracia, mantener el status quo no es una opción, dado el coste de la inacción. En febrero de 2021, por ejemplo, la ciudad francesa de Chalon-sur-Saône y el área metropolitana de Grand Chalon tuvieron que gastar 500.000 euros para volver a poner en marcha sus sistemas informáticos tras un ciberataque.

90.000 EUROS

Se trata del importe de la subvención recibida durante dos años por la CCVG en el marco del plan France Relance. "*Nuestro presupuesto informático aumenta: algo menos de 300.000 euros al año en inversión y mantenimiento informático, más algunas herramientas de ciberseguridad que cuestan unos 20.000 euros al año*", añade Yann Ariza.

> *"Para las pequeñas autoridades locales que no disponen de un ejército de compradores, recurrir a una central de compras reduce los riesgos asociados al proceso de licitación. De este modo se aseguran de que están dentro de los límites legales y de que sus gastos han sido aprobados en caso de auditoría por parte de la oficina regional de auditoría".*
>
> Vincent Nicaise, Responsable de partners y ecosistemas industriales, Stormshield

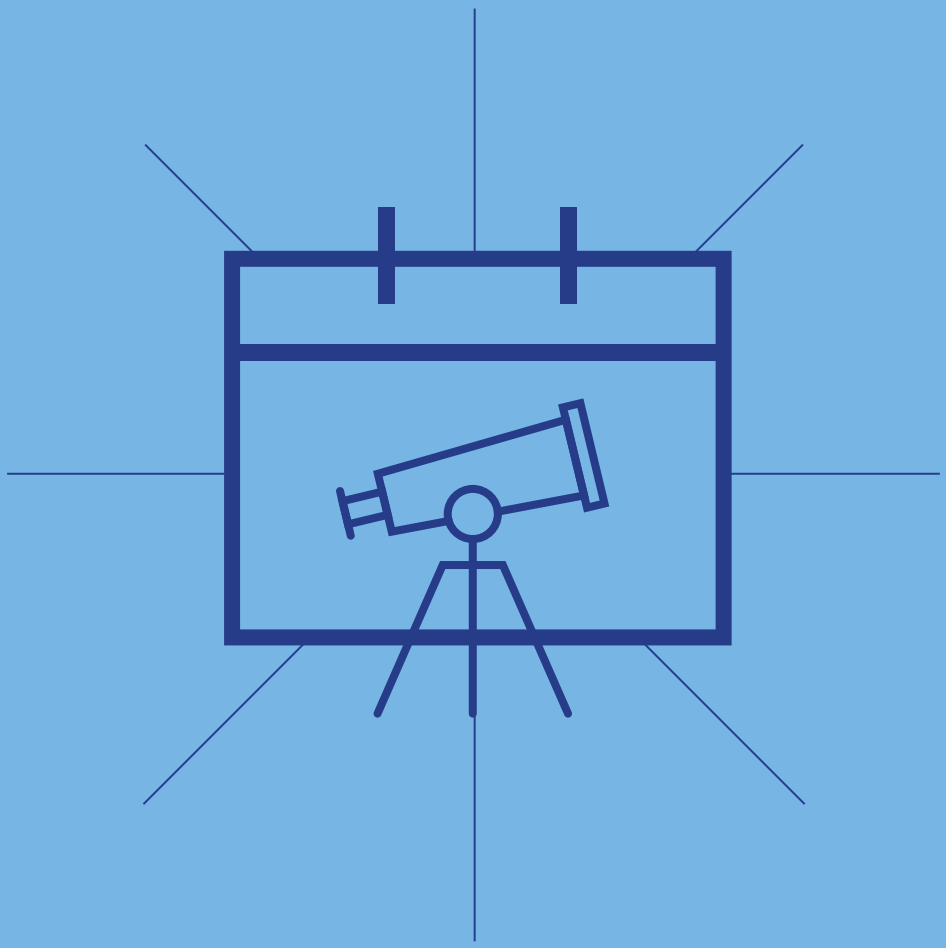
Pero donde el sector público difiere más significativamente de las organizaciones privadas es en los mecanismos establecidos para gastar este dinero.

¿Qué ocurre si una autoridad local quiere introducir un sistema de pago digital para los aparcamientos de su región geográfica? Según el código de contratación pública, debe organizar una licitación antes de poder adjudicar el contrato, a menos que el valor del mismo lo exima de publicidad y licitación competitiva.

Algunas ciudades y regiones conectadas prefieren recurrir a una central de compras, como la Union des groupements d'achats publics (UGAP). En este caso, la central de compras habrá sido la encargada de convocar la licitación, posiblemente en consulta con las oficinas de proyectos.

ÍNDICE

58
¿Qué nos deparará el futuro para el concepto de ciudad inteligente?
62
¿De qué soluciones técnicas y prácticas dispone la comunidad conectada?



Autoridades locales y ciudades inteligentes: **¿Qué nos deparará el futuro?**

Interconectividad galopante y nuevas prácticas de uso: ¿cómo serán nuestras ciudades del mañana? ¿Cuáles serán los ingredientes de su ciberseguridad? En los últimos quince años, la percepción de la ciudad inteligente ha cambiado, hasta el punto de que su estatus de "modelo" incuestionable está en entredicho. Entonces, el día de mañana, ¿estarán todas las autoridades locales conectadas y seguras?

04

¿Qué nos deparará el futuro para el concepto de ciudad inteligente?

¿Qué nuevas prácticas configurarán el futuro de nuestras ciudades? ¿Seguirán su camino hacia la interconectividad, acercándose al ideal de una ciudad inteligente segura y tecnológica?

Aunque los sensores de contaminación y los escúteres inteligentes son ya parte integrante del paisaje urbano, otras aplicaciones de la conectividad y el internet de las cosas poblarán sin duda nuestras ciudades "inteligentes" en el futuro.

Estas nuevas prácticas están surgiendo en todos los sectores: es muy posible que dentro de unos años la logística de última milla esté operada en su inmensa mayoría por pequeños robots autónomos... siempre que se disponga de la nueva infraestructura y el marco jurídico necesarios.

El paisaje que está tomando forma para las ciudades del futuro no será el mismo en los cuatro puntos cardinales del planeta. Mientras en Europa se tiende a una lenta reconversión de las ciudades más antiguas, en Estados Unidos se ha tomado el atajo de reconvertir barrios, en lugar de ciudades enteras. En otros lugares del mundo se están creando auténticas ciudades nuevas: en el desierto saudí, con The Line, y en la provincia china de Hebei, con la ciudad jardín de Xiong'an.

¿SEREMOS ALGUNA VEZ CAPACES DE PROTEGER LAS CIUDADES INTELIGENTES?

SI

Joël R. *La motivación está ahí, ¡y NIS2 nos animará a ponernos en marcha!*

Rodolphe dB. *La verdadera cuestión es la de una estrategia adecuada. En el sector de la energía, por ejemplo, ¿se confiará la cuestión a un actor público nacional, con el riesgo de crear toda una superficie de ataque, o a una multitud de actores privados que deberán realizar todos ellos importantes inversiones?*

NO

Noël C. *La protección al 100% no existe. El esfuerzo y los recursos que se ponen en juego a nivel estatal son tan grandes que estos ataques son difíciles de neutralizar... Sin embargo, es posible protegerse eficazmente contra la mayoría de las demás amenazas.*

Yann A. *La conexión y la superficie de ataque no tienen vuelta atrás, por lo que la seguridad es necesaria. Pero requiere la intervención del gobierno y una inversión sustancial.*

CIO anónimo. *Hasta que no dispongamos de una estandarización muy rígida, cada instalación de IoT representará un riesgo adicional para la seguridad. Hay mucho en juego a nivel social, pero la realidad sobre el terreno hace que el riesgo sea difícil de controlar.*

ENTREVISTA COMPARATIVA

Una ventana al mañana

Rodolphe de Beaufort y Joël Rivallan exponen sus puntos de vista sobre las prácticas que están llamadas a crecer en sus respectivos negocios de energía y agua.

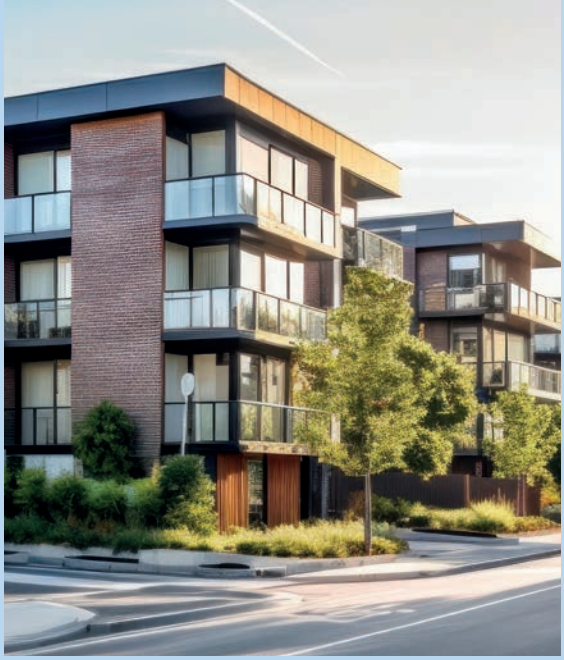


ELECTRICIDAD EN EL AIRE DE LA CIUDAD INTELIGENTE

R.dB. Apoyamos la introducción de vehículos eléctricos en el mercado. Esto significa, por ejemplo, equipar casi 250.000 edificios residenciales plurifamiliares con aparcamientos con infraestructura de recarga de vehículos (EVSE) para 2035 o 2040. La idea, por supuesto, es conectarlos a Internet, facilitando así su uso. También estamos planificando con antelación los problemas que surgirán cuando se conecten los 15 o 20 millones de vehículos en cuestión. Del mismo modo, la generalización de la calefacción eléctrica, que sustituirá a algunos sistemas de gas por bombas de calor, también dará lugar a la aparición de nuevos casos de uso: éstos se verán agilizados por los sistemas de gestión de edificios (BMS), que aportan flexibilidad en el consumo y cuya implantación en los edificios terciarios públicos y privados está prevista para 2027.

Nos anticipamos a los problemas que surgirán cuando se conecten los 15 o 20 millones de vehículos en cuestión”.

Rodolphe de Beaufort,
director general adjunto,
Gimelec



NO MÁS AGUA (RESIDUAL) DESPERDICIADA

J.R. Hasta hace poco, la reutilización de las aguas residuales estaba prohibida por la normativa francesa. Los nuevos decretos nos permitirán aumentar su proporción, paralelamente a nuestros esfuerzos de hidroeconomía.

SOLUCIONES INTELIGENTES QUE ESCALAN

R.dB. En cuanto a la producción de electricidad, también habrá cambios a medida que se generalicen los sistemas fotovoltaicos. El uso de la gestión local de la energía (microrredes) y el autoconsumo colectivo deberían extenderse al mismo tiempo.

¿Qué soluciones técnicas y prácticas están disponibles para la comunidad conectada?

La provisión de seguridad para las actividades y la infraestructura de las autoridades locales conectadas exige soluciones tanto técnicas como prácticas. ¿Surgirá en el futuro un ganador entre las soluciones autónomas o las gestionadas?

La descentralización se refiere a la transferencia de competencias y recursos del estado a las autoridades locales. Esta es también una de las características técnicas de la ciudad inteligente: un conjunto de sensores y equipos distribuidos por toda la región en cuestión. Basándose en este principio, los equipos de Stormshield diseñan una solución de seguridad en malla que garantiza la comunicación entre los distintos actores de la red, sea cual sea su punto de acceso. Esto se adapta especialmente bien a la diversidad de conexiones de red de una ciudad inteligente.

Al proporcionar protección de datos en las capas inferiores, la solución crea una red en malla de túneles de comunicación seguros entre distintos elementos de una red de confianza, sin tener que controlar la infraestructura.

PALABRA CLAVE

CAPAS INFERIORES

Expresión que hace referencia al modelo de Interconexión de Sistemas Abiertos (OSI). Desglosa el proceso de comunicación entre dos elementos de red en siete categorías, denominadas “capas”. Las capas inferiores son las capas 1 (activos críticos) y 2 (seguridad de los datos).

XDR es otra solución técnica que está llamada a ganar popularidad. Detrás de este acrónimo se esconde un nuevo paradigma de ciberseguridad: eXtended Detection & Response permite gestionar todos los incidentes de seguridad a través de una única plataforma. Este enfoque mejora la eficacia operativa y el nivel de protección de las organizaciones que lo aplican porque, además de las alertas, permite gestionar los elementos de respuesta y remediación.

Por último, la prospectiva tecnológica y los equipos de I+D están ideando sistemas de seguridad mejor adaptados a los entornos de las ciudades inteligentes y a sus infraestructuras distribuidas. Pero el reto de ofrecer seguridad a la ciudad inteligente y a las actividades conectadas de la ciudad del mañana no es sólo técnico. En términos de recursos humanos, la contratación es difícil porque estos entornos requieren conocimientos que pertenecen a dos mundos diferentes: TI y OT.



Noël Chazotte, jefe de producto en Stormshield

Instalar software de seguridad en equipos de tamaño modesto y capaces de realizar funciones informáticas: ése es el reto que nos impulsa a innovar para intercalarnos entre el sensor y el sistema de captación. Nuestro agente Stormshield estará disponible en las estaciones de trabajo, y esperamos trabajar con cada vez más fabricantes para integrarlo de forma nativa en los equipos del entorno OT. Nuestro objetivo es quitar la espina de la ciberseguridad a nuestros socios industriales, para que puedan concentrarse en sus protocolos de negocio”.

PROSPECTIVA

¿Quién ganará el ciberconcurso de ciudades inteligentes?

Escenario 1

LAS SOLUCIONES LISTAS PARA FUNCIONAR TRIUNFAN

Las soluciones más sencillas e integradas se imponen porque requieren menos configuración y mantenimiento y, por tanto, menos competencias.

Escenario 2

LA CAPACIDAD DE ADMINISTRACIÓN SALE VENCEDORA

El aspecto de “caja negra” de las soluciones “autónomas” es incompatible con las exigencias de determinados contextos operativos. Por eso es necesario desarrollar interfaces accesibles a los servicios de la empresa no especializados, que les permitan realizar ajustes.

La ambición al principio del mandato era claramente centrarse en la ciudad inteligente, pero la huella de carbono de los sistemas de información está siendo objeto de un escrutinio cada vez mayor. Esto influye en las decisiones de los representantes electos".

Yann Ariza, Director de seguridad de la información, de la federación de municipios de Vallée du Garon

"*La doctrina [de ciberseguridad] [para las autoridades locales] se está redactando actualmente*". Así se expresa Jean-Michel Morer, alcalde de Trilport y representante de la Asociación de Pequeñas Ciudades de Francia (APVF).

El dinamismo de los debates entre las autoridades locales sobre la creación de una certificación específica de ciberseguridad sugiere que se está produciendo un aumento global de las competencias.

Para seguir avanzando hacia la ciudad inteligente, las autoridades locales deben contar con el apoyo de una voluntad política sostenida, respaldada por recursos financieros suficientes.

Sin embargo, en los últimos años, la cuestión medioambiental ha pasado a formar parte del debate, incitando a los representantes electos a considerar el impacto medioambiental de tales prácticas más allá de los beneficios declarados; por ejemplo: en términos de reducción del consumo.

Sin llegar necesariamente a un rechazo total de la tecnología, estos debates están cambiando la propia definición de ciudad inteligente y sus representaciones: hoy, inteligente significa digital, pero también – y lo que es más importante – austera y responsable.

FUENTES

- Entrevistas
- **Olsztyn-Poland: primera ciudad inteligente en ser alcanzada por un ciberataque**, lemagit.fr
- **Organismos internacionales publican una guía de ciberseguridad para ciudades inteligentes**, cities-today.com
- **Cuanto más inteligente es la ciudad, más peligroso es el ciberriesgo**, emergingtechbrew.com
- **Angers abre un espacio público para hablar sobre su ciudad inteligente**, lesechos.fr
- **La ciudades inteligentes vulnerables a ciberataques**, independentaustralia.net
- **"Ciudades inteligente" desde la perspectiva del ciberriesgo,** club-ebios.org
- **Ciudades inteligentes 1-2 custiones de ciberseguridad** riskinsight-wavestone.com
- **Dallas gastó 4M en detección de amenazas después de un ataque de ransomware**, statescoop.com
- **Ciberseguriad IoT: cómo proteger la ciudad inteligente**, stormshield.com
- **San Francisco impulsa proyectos de transporte y aparcamiento inteligentes**, lemagit.fr
- **Ciberataques: cuando las autoridades locales buscan formas de contrarrestarlos**, stormshield.com
- **La ciudad inteligente: resumen de soluciones de software para la transformación digital de los entes locales,** ugap.fr
- **Contratación pública, regiones inteligentes: un catálogo,** ugap.fr
- **Ciberseguridad: el pariente pobre en los presupuestos de TI de las autoridades locales**, banquedesterritoires.fr
- **Mapa de ciberataques** konbriefing.com
- **Mes de la Ciberseguridad 2023: acto de presentación en el Ciber Campus**, cybermalveillance.gouv.fr

Ciberseguridad para autoridades locales
Un reto por el que no pueden esperar las ciudades inteligentes

STORMSHIELD
22, rue du Gouverneur Général Eboué
92130 Issy-les-Moulineaux, France

Contenido editorial: Ultramedia
Dirección artística, diseño, ilustraciones y maquetación: Studio Orkidées

LA ELECCIÓN EUROPEA DE CIBERSEGURIDAD

www.stormshield.com

Queda prohibida toda distribución, reproducción o representación, incluso parcial, de este libro blanco, para cualquier fin que no sea el uso privado, independientemente del soporte, pudiendo incurrir en responsabilidad civil y penal la persona que incumpla esta prohibición.

Copyright © 2023 Stormshield