CAPÍTULO VIII

Actuaciones a seguir frente a un ciberataque a una entidad local

Fernando Suárez Lorenzo
Ingeniero en Informática.
Presidente del Colexio Profesional de Enxeñaría en Informática de Galicia (CPEIG) y del Consejo General de Ingeniería Informática (CCII)

SUMARIO. 1. Introducción. 2. Marco general de respuesta ante ciberataques. 2.1. La importancia de la preparación previa. 2.2. Políticas de ciberseguridad municipal. 2.3. Infraestructuras críticas en el ámbito local. 2.4. Colaboración con actores externos. **3. Fases de actuación frente a un ciberataque.** 3.1. Detección y respuesta inicial. 3.2. Contención del ataque. 3.3. Investigación y análisis forense. 3.4. Recuperación y restablecimiento. 3.5. Lecciones aprendidas y plan de mejora continua. **4. La política de ciberseguridad municipal.** 4.1. Gestión de riesgos. 4.2. Roles y responsabilidades. 4.3. Formación y sensibilización. 4.4. Implementación y monitorización. **5. Análisis DAFO. 6. Conclusiones. 7. Bibliografía.**

1. Introducción

El auge de la digitalización ha transformado significativamente la manera en que las entidades locales gestionan sus servicios. La incorporación de tecnologías como los sistemas de gestión electrónica, las plataformas de participación ciudadana y las infraestructuras críticas digitalizadas ha traído consigo ventajas indiscutibles, como la mejora en la eficiencia y la

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

accesibilidad. Sin embargo, esta dependencia tecnológica también expone a los municipios a nuevos y complejos riesgos de ciberseguridad.

Estudios recientes destacan que más del 70 % de las entidades locales europeas han reportado al menos un incidente de ciberseguridad en los últimos tres años. Estos ataques van desde *ransomware* y *phishing* hasta accesos no autorizados a datos personales de los ciudadanos. En muchos casos, las entidades locales carecen de los recursos humanos, financieros y técnicos para enfrentar estas amenazas de manera efectiva, situándolas en una posición de vulnerabilidad crítica.

Los ciberataques a nivel local pueden tener un impacto desproporcionado, dado que afectan directamente a servicios esenciales como:

- la gestión del agua potable y el saneamiento;
- la emisión de certificados y permisos;
- la recaudación de impuestos municipales;
- los sistemas de seguridad ciudadana, como cámaras de vigilancia o sistemas de alarmas.

Además del impacto operativo, estos incidentes erosionan la confianza pública y generan altos costos económicos. Un informe de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) estima que el coste promedio de un ciberataque a una entidad local puede superar los 300 000 euros, sin contar las posibles sanciones derivadas del incumplimiento normativo.

El marco normativo europeo, liderado por la Directiva NIS II y el Esquema Nacional de Seguridad en España, establece obligaciones claras para proteger las infraestructuras críticas. Sin embargo, la implementación de estas medidas a nivel local sigue siendo desigual. Este capítulo pretende conectar la teoría normativa con la práctica, brindando una guía paso a paso adaptada a las características y limitaciones de las Administraciones locales.

Este capítulo tiene tres objetivos principales:

- proporcionar un marco estructurado para responder a ciberataques en el ámbito local;

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

- establecer las responsabilidades y los roles necesarios para una respuesta efectiva;

- ofrecer herramientas prácticas que permitan a los municipios mejorar su resiliencia frente a amenazas cibernéticas.

En las secciones siguientes se abordará cómo las entidades locales pueden organizar su respuesta a un incidente desde una perspectiva técnica y de gestión, destacando la importancia de la cooperación interinstitucional, la capacitación continua y el aprendizaje posincidente.

2. Marco general de respuesta ante ciberataques

2.1. La importancia de la preparación previa

La preparación previa es el cimiento de una respuesta efectiva ante ciberataques. En el ámbito de las entidades locales, donde los recursos pueden ser limitados y la dependencia de sistemas tecnológicos es alta, contar con medidas proactivas puede marcar la diferencia entre una interrupción temporal y un colapso prolongado de servicios esenciales.

La ciberseguridad debe abordarse como un proceso continuo y cíclico. El marco del ciclo de vida de la ciberseguridad, que comprende las fases de identificar, proteger, detectar, responder y recuperar, proporciona una guía estructurada para las entidades locales:

1. Identificar: Esta etapa implica mapear los activos críticos de la organización, evaluar sus vulnerabilidades y entender las amenazas específicas del entorno. Por ejemplo, un pequeño ayuntamiento podría priorizar la protección de sus sistemas de recaudación de impuestos y expedición de certificados.

2. Proteger: Una vez identificados los activos, es esencial implementar controles técnicos, administrativos y físicos que reduzcan el riesgo de ataques. Esto incluye medidas como el uso de *firewalls*, políticas de contraseñas robustas y segmentación de redes.

3. Detectar: La capacidad de detectar amenazas de forma temprana es crucial para minimizar el impacto de un ataque. Las entidades locales pueden recurrir a soluciones como sistemas de detección

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

de intrusos (IDS) o colaborar con centros de respuesta a incidentes de seguridad (CSIRT).

4. Responder: Un plan claro y bien practicado para reaccionar ante un incidente es esencial. Esto incluye identificar responsables, comunicar el incidente a las partes relevantes y ejecutar medidas de contención.

5. Recuperar: Finalmente, la recuperación se centra en restaurar los servicios afectados y analizar el incidente para evitar futuras recurrencias. Esto también incluye la comunicación a los ciudadanos sobre las medidas adoptadas para garantizar la continuidad de los servicios.

Planes de contingencia y continuidad operativa

Un plan de contingencia bien diseñado asegura que las entidades locales puedan mantener sus servicios esenciales incluso durante un ciberataque. Este plan debe incluir:

- Inventarios de activos y servicios críticos: ¿qué sistemas deben restaurarse primero?; ¿cuáles son las dependencias clave?

- Planes de recuperación ante desastres (DRP): procedimientos técnicos para recuperar sistemas y datos en caso de ataque.

- Pruebas regulares y simulaciones: validar los planes mediante ejercicios prácticos como simulacros de *ransomware*.

Por ejemplo, un ayuntamiento podría realizar una simulación en la que se bloquea el acceso a su sistema de emisión de certificados, verificando la capacidad de restaurar el servicio dentro del tiempo objetivo definido.

Evaluación de riesgos periódica

Una evaluación regular de riesgos permite a las entidades locales adaptarse a nuevas amenazas. Este proceso incluye:

- Identificación de amenazas emergentes: por ejemplo, un incremento en ataques de *phishing* dirigidos a empleados municipales.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

- Clasificación de activos según criticidad: un análisis que priorice la protección de datos ciudadanos frente a sistemas de menor relevancia.

- Priorización de inversiones: asegurar que los recursos limitados se asignen de forma estratégica.

Además, esta evaluación debe estar alineada con las normativas nacionales y europeas, como el Esquema Nacional de Seguridad, para garantizar el cumplimiento regulatorio.

Cultura organizativa: la clave para la preparación

La ciberseguridad no es solo responsabilidad del equipo técnico; debe involucrar a toda la organización. Esto incluye:

- Capacitación del personal: Desde los altos cargos hasta los operativos, todos deben ser conscientes de los riesgos y las mejores prácticas.

- Sensibilización a nivel político: Los responsables municipales deben entender la importancia de priorizar la ciberseguridad en sus agendas.

- Definición de roles y responsabilidades: Asegurar que cada empleado sepa cómo actuar en caso de un incidente.

2.2. Políticas de ciberseguridad municipal

Las políticas de ciberseguridad son documentos estratégicos que establecen las directrices, procedimientos y responsabilidades necesarias para proteger los activos digitales de una organización. En el contexto de las entidades locales, estas políticas no solo deben adaptarse a la normativa vigente, sino también considerar las particularidades de los recursos y las infraestructuras de los municipios.

Una política de ciberseguridad municipal es un marco de trabajo diseñado para proteger los sistemas de información, los datos de los ciudadanos y los servicios públicos locales. Este documento tiene como objetivo:

- establecer directrices claras para la gestión de riesgos de ciberseguridad;

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

- definir roles y responsabilidades específicas dentro de la organización;
- describir los procedimientos para prevenir, detectar y responder a incidentes de ciberseguridad;
- fomentar una cultura organizativa de ciberseguridad que trascienda las áreas técnicas.

El diseño y la implementación de esta política deben ser liderados por los responsables técnicos, pero con un fuerte compromiso de los equipos políticos y administrativos.

Elementos clave de una política de ciberseguridad

Una política efectiva debe contener, al menos, los siguientes apartados:

1. Declaración de objetivos: una declaración que exprese el compromiso de la entidad local con la protección de los datos y servicios digitales.
2. Gestión de riesgos: incluir un enfoque sistemático para identificar, evaluar y mitigar riesgos. Esto puede involucrar matrices de riesgos y planes de acción específicos.
3. Roles y responsabilidades: especificar quién es responsable de cada aspecto de la ciberseguridad, desde el responsable político hasta los técnicos y personal operativo.
4. Formación y sensibilización: establecer programas regulares para educar al personal sobre prácticas seguras, como evitar el *phishing* y gestionar contraseñas de manera adecuada.
5. Procedimientos de respuesta a incidentes: un conjunto de pasos que detallen cómo actuar ante un ciberataque, desde la detección inicial hasta la recuperación completa.
6. Revisión y mejora continua: incluir mecanismos para evaluar y actualizar la política de forma periódica, adaptándose a nuevos riesgos y tecnologías.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

La colaboración interinstitucional

Muchas entidades locales, especialmente los pequeños municipios, enfrentan limitaciones en recursos técnicos y humanos. En este contexto, la colaboración con otras Administraciones y organismos especializados es crucial. Ejemplos de esta colaboración incluyen:

- Diputaciones provinciales: Estas instituciones pueden actuar como nodos de ciberseguridad, ofreciendo soporte técnico y asesoramiento a los municipios de menor tamaño.
- CSIRT regionales y nacionales: Proporcionan orientación y apoyo técnico en la gestión de incidentes.
- Instituto Nacional de Ciberseguridad (INCIBE) y Centro Criptológico Nacional (CCN): Organismos que ofrecen formación, herramientas y recursos específicos para entidades locales.

Beneficios de una política de ciberseguridad municipal

Implementar una política de ciberseguridad aporta ventajas tangibles, como:

- reducción de riesgos asociados a ciberataques;
- cumplimiento normativo con marcos como el ENS o la Directiva NIS II;
- mejora de la confianza de los ciudadanos en los servicios municipales;
- ahorro de costos a largo plazo, al prevenir incidentes y sus consecuencias económicas.

2.3. Infraestructuras críticas en el ámbito local

Las infraestructuras críticas constituyen el corazón operativo de las entidades locales, ya que soportan servicios esenciales que afectan directamente a la calidad de vida de los ciudadanos. En el ámbito municipal, estas infraestructuras incluyen sistemas de abastecimiento de agua, gestión de residuos, transporte público, alumbrado y comunicaciones, entre otros. La creciente digitalización de estos sistemas los hace más eficientes, pero

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

también más vulnerables a ciberataques que pueden generar graves consecuencias económicas, sociales y políticas.

Un ejemplo paradigmático de la vulnerabilidad de estas infraestructuras ocurrió en Baltimore (EE. UU.) en 2019, cuando un ataque de *ransomware* paralizó los sistemas municipales durante semanas. La ciudad sufrió pérdidas millonarias no solo por el rescate exigido, que no se pagó, sino también por los costes asociados a la interrupción de servicios, como la recaudación de impuestos y la emisión de licencias. Este caso evidencia cómo un ciberataque puede sobrepasar las barreras tecnológicas y afectar directamente al tejido social y económico.

Identificación y protección de infraestructuras críticas

En el caso de las entidades locales, la identificación de infraestructuras críticas debe ser una prioridad. Aunque estas varían dependiendo del tamaño y de las competencias de cada municipio, ciertos sistemas suelen ser considerados críticos en la mayoría de los casos, como los sistemas de gestión de emergencias o las redes de suministro eléctrico. Identificar estas infraestructuras requiere un análisis exhaustivo de los servicios prestados y de las posibles consecuencias de su interrupción.

Una vez identificadas, el siguiente paso es asegurar su protección. En el marco del Esquema Nacional de Seguridad, las entidades locales tienen la obligación de garantizar la seguridad de los sistemas que soportan sus servicios esenciales. Esto implica implementar medidas técnicas y organizativas específicas, como la segmentación de redes, el cifrado de datos sensibles y la adopción de estándares de ciberseguridad reconocidos.

En España, los ayuntamientos tienen acceso a herramientas y recursos proporcionados por organismos nacionales como el CCN y el INCIBE. Estos organismos ofrecen guías, formación y soporte técnico para fortalecer la seguridad de las infraestructuras locales. Sin embargo, la implementación efectiva de estas medidas depende en gran medida de la voluntad política y de la asignación de recursos adecuados a nivel municipal.

Retos específicos de las infraestructuras críticas locales

Uno de los mayores desafíos que enfrentan las entidades locales es la falta de recursos humanos y financieros especializados en ciberseguridad. Mientras que grandes ciudades como Madrid o Barcelona cuentan con

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

departamentos dedicados a la seguridad digital, muchos pequeños municipios dependen de un único técnico de sistemas para gestionar toda su infraestructura tecnológica. Esta brecha de capacidades puede ser abordada mediante la colaboración interinstitucional, como la ofrecida por las diputaciones provinciales o los Gobiernos autonómicos.

Además, las infraestructuras locales suelen estar integradas por sistemas heterogéneos y, en ocasiones, obsoletos, lo que dificulta su protección. Por ejemplo, sistemas *Supervisory Control and Data Acquisition* (SCADA) utilizados para el control del suministro de agua en algunos municipios han sido diseñados sin considerar las amenazas cibernéticas modernas, lo que los convierte en blancos fáciles para los atacantes. La modernización de estos sistemas requiere no solo inversiones económicas, sino también la adopción de una estrategia integral de ciberseguridad que priorice la prevención sobre la reacción.

El papel del Esquema Nacional de Seguridad

El ENS establece un marco común para garantizar la protección de los sistemas de información en las Administraciones públicas, incluyendo las locales. Aunque su implementación ha avanzado significativamente en los últimos años, aún existen retos en su aplicación práctica, especialmente en municipios pequeños y medianos. Una de las soluciones más efectivas ha sido la creación de perfiles de cumplimiento específicos para entidades locales, que adaptan las exigencias del ENS a las realidades de estas Administraciones.

Por ejemplo, los perfiles de cumplimiento distinguen entre grandes municipios, que deben cumplir con todas las medidas del ENS, y pequeños municipios, a los que se permite priorizar ciertas acciones esenciales. Esta flexibilidad ha facilitado que más entidades locales inicien el proceso de certificación, lo que a su vez mejora la seguridad de sus infraestructuras críticas.

En definitiva, las infraestructuras críticas en el ámbito local representan un punto neurálgico de la ciberseguridad municipal. Su protección no solo asegura la continuidad de los servicios esenciales, sino que también refuerza la confianza de los ciudadanos en sus instituciones. Sin embargo, lograr una protección efectiva requiere un enfoque multidimensional que combine recursos técnicos, formación especializada, colaboración interinstitucional y compromiso político. Solo a través de este enfoque integral será

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

posible garantizar la resiliencia de las infraestructuras críticas locales frente a las amenazas cibernéticas actuales y futuras.

2.4. Colaboración con actores externos

La colaboración con actores externos es un elemento esencial en la estrategia de ciberseguridad de cualquier entidad local. Dada la limitada capacidad técnica y financiera de muchos municipios, establecer alianzas con organismos especializados, proveedores tecnológicos y otras Administraciones es crucial para garantizar una respuesta efectiva frente a ciberataques. Este enfoque colaborativo permite compartir conocimientos, acceder a recursos avanzados y optimizar la gestión de riesgos.

Uno de los actores clave en la colaboración externa son los centros de respuesta a incidentes de seguridad informática (CSIRT) y los centros de operaciones de ciberseguridad (SOC). En España, el CCN-CERT y el INCIBE-CERT lideran la gestión de incidentes a nivel nacional y ofrecen soporte directo a las Administraciones públicas, incluidas las locales.

Estos centros proporcionan una variedad de servicios, como:

- la detección y análisis de amenazas emergentes;
- el apoyo técnico en la mitigación y recuperación de ciberataques;
- la capacitación de personal técnico a través de talleres y simulacros;
- la distribución de guías y herramientas específicas para proteger infraestructuras críticas.

Por ejemplo, durante la pandemia de COVID-19, el CCN-CERT intensificó su colaboración con las Administraciones locales para proteger las plataformas de teletrabajo y los sistemas de atención al ciudadano, que se convirtieron en objetivos frecuentes de ataques.

Ciber.gal: un modelo de colaboración regional en ciberseguridad

En Galicia, la Axencia para a Modernización Tecnolóxica de Galicia (AMTEGA) lidera un modelo ejemplar de colaboración interinstitucional en ciberseguridad, especialmente a través de su iniciativa Ciber.gal. Esta alianza estratégica reúne a Administraciones públicas, empresas tecnológicas, centros de

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

conocimiento y otros actores relevantes para fortalecer las capacidades de ciberseguridad en todos los niveles.

La AMTEGA no solo proporciona herramientas y servicios específicos a los ayuntamientos, sino que también promueve la sensibilización, formación y cooperación a través de iniciativas como el Encuentro Cibergal. Este evento anual se ha consolidado como un referente en el ámbito de la ciberseguridad, sirviendo como punto de encuentro para compartir experiencias, identificar buenas prácticas y fomentar la innovación en la protección de infraestructuras críticas locales.

Entre las acciones impulsadas por la AMTEGA se incluyen:

- Servicios tecnológicos compartidos: soluciones avanzadas de protección para los sistemas municipales, como *firewalls* y herramientas de monitorización en tiempo real.

- Capacitación del personal técnico: programas formativos diseñados para dotar a los responsables municipales de las competencias necesarias para gestionar riesgos cibernéticos.

- Simulacros de ciberseguridad: ejercicios prácticos que permiten a los ayuntamientos evaluar y mejorar su capacidad de respuesta ante incidentes.

- Fomento de la colaboración público-privada: integración de empresas tecnológicas en proyectos que refuercen las capacidades locales, como la implementación de soluciones basadas en inteligencia artificial para la detección de amenazas.

El Encuentro Cibergal, además, facilita el acceso de los municipios a redes de expertos y recursos avanzados, consolidando a Galicia como un modelo de referencia en la construcción de un ecosistema de ciberseguridad regional.

Colaboración con proveedores tecnológicos

Los proveedores tecnológicos desempeñan un papel doblemente relevante, tanto como aliados estratégicos en la protección de sistemas como posibles puntos vulnerables en la cadena de suministro. Es fundamental que las entidades locales establezcan relaciones claras y bien definidas con sus

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

proveedores, asegurando que estos cumplan con los estándares de ciberseguridad requeridos.

Un aspecto clave es la revisión de los acuerdos de nivel de servicio (SLA) para incluir cláusulas específicas sobre tiempos de respuesta ante incidentes, auditorías de seguridad y responsabilidad en caso de brechas de datos. Además, los proveedores pueden ser aliados en la capacitación del personal técnico, ofreciendo formaciones específicas sobre el uso seguro de sus plataformas y herramientas.

Casos de éxito en la cooperación público-privada

La colaboración público-privada es otro componente fundamental en la estrategia de ciberseguridad. Iniciativas como los foros de ciberseguridad organizados por INCIBE han facilitado la creación de alianzas entre Administraciones públicas y empresas del sector tecnológico. Estas alianzas no solo fortalecen las capacidades técnicas de las entidades locales, sino que también promueven la innovación en herramientas de protección.

Un caso exitoso es el proyecto CIBERLOCAL, desarrollado en colaboración con empresas tecnológicas y ayuntamientos piloto, que busca implementar soluciones de ciberseguridad adaptadas a las necesidades de municipios pequeños y medianos. Este proyecto incluye la creación de manuales prácticos, talleres de formación y la implementación de tecnologías avanzadas como sistemas de inteligencia artificial para la detección de amenazas.

La colaboración con actores externos amplía significativamente las capacidades de las entidades locales para enfrentar ciberataques, especialmente en un contexto de recursos limitados. La experiencia de iniciativas como Ciber.gal demuestra que, con una estrategia adecuada, es posible crear un ecosistema colaborativo que fortalezca la resiliencia de los municipios frente a las amenazas cibernéticas actuales y futuras.

3. Fases de actuación frente a un ciberataque

Responder de manera efectiva a un ciberataque requiere un enfoque estructurado que permita minimizar el impacto, proteger los activos críticos y restaurar los servicios afectados. Para las entidades locales, que gestionan sistemas esenciales y datos sensibles, este desafío es aún más complejo debido a las limitaciones de recursos y capacidades técnicas.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

El proceso de gestión de un ciberataque no puede ser improvisado. Desde el momento en que se detecta un incidente hasta la recuperación completa, cada acción debe estar guiada por protocolos predefinidos y ejecutada con precisión. Estas fases no solo garantizan una respuesta ordenada, sino que también maximizan las posibilidades de contener el daño, identificar las vulnerabilidades explotadas y aprender de la experiencia para evitar incidentes futuros.

En este apartado, se describen las cinco fases fundamentales para actuar frente a un ciberataque:

1. Detección y respuesta inicial: La capacidad de identificar y evaluar rápidamente un incidente es clave para activar una respuesta eficaz.

2. Contención del ataque: Evitar que el ataque se propague o cause mayores daños es una prioridad en las primeras horas del incidente.

3. Investigación y análisis forense: Comprender cómo ocurrió el ataque y cuál fue su alcance permite tomar decisiones informadas para mitigar su impacto.

4. Recuperación y restablecimiento: Restaurar los sistemas afectados de manera segura y garantizar la continuidad de los servicios es el objetivo principal tras la contención.

5. Lecciones aprendidas y plan de mejora continua: Analizar el incidente permite identificar áreas de mejora y ajustar las políticas y los procedimientos para fortalecer la resiliencia.

Cada una de estas fases será abordada en detalle, proporcionando pautas prácticas para que las entidades locales enfrenten los ciberataques de manera efectiva y profesional.

3.1. Detección y respuesta inicial

La detección temprana y la respuesta inicial son etapas críticas en la gestión de un ciberataque. Estas fases determinan, en gran medida, el impacto del incidente en los servicios y sistemas de la entidad local. Una detección oportuna permite activar protocolos que limitan la extensión del ataque, minimizan daños y protegen los datos sensibles de los ciudadanos.

Herramientas y mecanismos de detección

En el contexto de las entidades locales, donde los recursos técnicos pueden ser limitados, la detección de un ciberataque puede depender tanto de herramientas automatizadas como de la intervención humana. Entre los mecanismos más comunes para identificar incidentes se encuentran:

- Sistemas de detección de intrusos (IDS): Tecnologías que monitorizan el tráfico de red en busca de comportamientos anómalos o patrones conocidos de ataque.

- Alertas de *software* de seguridad: Herramientas como antivirus o *firewalls* que detectan y bloquean actividades sospechosas.

- Informes de usuarios: En muchos casos, los primeros indicios de un ataque son reportados por empleados municipales que experimentan fallos inusuales en sus sistemas.

Un ejemplo ilustrativo es un incidente de ransomware en un pequeño municipio donde el ataque fue detectado cuando varios empleados no pudieron acceder a sus documentos, y sus pantallas mostraron un mensaje exigiendo el pago de un rescate. Este tipo de detección, aunque reactiva, es común en entidades sin soluciones avanzadas de monitorización.

Acciones inmediatas tras la detección

Una vez que se identifica un posible incidente, la respuesta inicial debe centrarse en confirmar su naturaleza y activar los protocolos adecuados. Este proceso incluye:

1. Confirmación del incidente: Es crucial determinar si se trata de un ataque real o un falso positivo. Esto puede implicar la revisión de los logs del sistema y la consulta con expertos técnicos internos o externos.

2. Notificación interna: Inmediatamente después de confirmar el incidente, debe informarse al equipo de respuesta a incidentes, que puede incluir tanto personal técnico municipal como organismos externos, como un CSIRT regional.

3. Establecimiento de prioridades: Evaluar rápidamente qué sistemas y datos están en riesgo para priorizar las acciones. Por ejemplo, si el

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

sistema afectado gestiona la emisión de certificados, podría considerarse crítico para la continuidad operativa del municipio.

Comunicación temprana y control de la información

La gestión adecuada de la comunicación interna y externa en esta etapa es esencial para evitar la desinformación y mantener el control del incidente. A nivel interno, se debe garantizar que todos los empleados municipales estén al tanto de las instrucciones clave, como no intentar acceder a sistemas comprometidos o no desconectar dispositivos sin autorización.

En cuanto a la comunicación externa, especialmente si el incidente afecta servicios públicos visibles para la ciudadanía, debe manejarse con cuidado para evitar alarmas innecesarias. Esto podría incluir:

- emitir un comunicado breve que informe del problema de manera general, asegurando que se están tomando medidas para solucionarlo;

- designar un portavoz que centralice todas las comunicaciones para evitar mensajes contradictorios.

Comunicación en caso de filtración de datos personales

La comunicación con los ciudadanos tras un ciberataque, especialmente en casos de filtración de datos personales, requiere una estrategia bien estructurada que combine transparencia, sensibilidad y cumplimiento normativo. Además de informar sobre el restablecimiento de servicios, las entidades locales tienen la responsabilidad legal y moral de comunicar adecuadamente las posibles afectaciones a la privacidad de los ciudadanos.

Los elementos clave de la comunicación en caso de filtración de datos personales son los siguientes:

1. Notificación inmediata y transparente:

    - Según el Reglamento General de Protección de Datos (RGPD), si una brecha de datos supone un riesgo para los derechos y libertades de las personas afectadas, la entidad local debe notificarlo de manera inmediata tanto a los afectados como a la Agencia Española de Protección de Datos (AEPD).

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

- La notificación debe incluir información clara sobre:
  - qué datos se han visto comprometidos (por ejemplo: nombres, direcciones, datos financieros);
  - cómo ocurrió la filtración;
  - las medidas adoptadas para mitigar los daños.

2. Establecimiento de un canal de atención directa:
   - crear un punto de contacto específico, como una línea telefónica o un correo electrónico, para responder a las dudas y preocupaciones de los ciudadanos;
   - designar a un responsable (posiblemente el delegado de protección de datos) que coordine las respuestas y garantice la coherencia en la información proporcionada.
3. Proporcionar orientación a los afectados:
   - Recomendar acciones concretas para minimizar posibles impactos, como:
     - cambiar contraseñas comprometidas;
     - monitorizar actividades inusuales en cuentas bancarias o de correo;
     - estar atentos a intentos de fraude relacionados con la filtración.
4. Reconocer la gravedad del incidente con profesionalismo:
   - reconocer públicamente el incidente y explicar las acciones tomadas para proteger los datos de los ciudadanos en el futuro;
   - evitar actitudes defensivas o culpar a terceros, ya que esto puede erosionar aún más la confianza pública.
5. Cumplimiento normativo:
   - además de notificar a la AEPD, documentar todas las acciones realizadas para gestionar la brecha de datos;

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

- mantener registros detallados del incidente para posibles auditorías o investigaciones posteriores.

Una buena estrategia de comunicación tiene una serie de beneficios claros y directos:

- Confianza ciudadana: La transparencia demuestra que la entidad local está actuando de manera responsable, incluso en situaciones críticas.

- Cumplimiento legal: Garantiza que la Administración cumple con las obligaciones establecidas por el RGPD y otras normativas aplicables.

- Reducción del impacto reputacional: Una respuesta clara y profesional puede minimizar las críticas y reforzar la percepción de compromiso con la seguridad.

La importancia de los planes preestablecidos

El éxito de esta fase depende en gran medida de la existencia y del conocimiento de un plan de respuesta a incidentes previamente definido. Este plan debe incluir:

- Roles y responsabilidades claras: saber quién debe ser contactado y qué decisiones deben tomarse en los primeros minutos tras la detección.

- Protocolos de escalado: definir en qué momento se requiere la intervención de actores externos, como un CSIRT o el proveedor del sistema afectado.

Un caso de referencia es el ataque sufrido por el Ayuntamiento de Castellón en 2022, donde la rápida activación del plan de contingencia permitió contener el incidente y evitar la pérdida de datos críticos. Este ejemplo destaca la importancia de estar preparado incluso con recursos limitados.

3.2. Contención del ataque

Una vez detectado y confirmado un ciberataque, la contención se convierte en la prioridad principal. Esta fase busca limitar el alcance del ataque,

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

evitar que se extienda a otros sistemas y proteger los activos críticos de la entidad local. La contención, aunque temporal, es clave para estabilizar la situación antes de avanzar hacia la investigación y la recuperación.

Estrategias de contención

La contención debe ser cuidadosamente planificada y ejecutada para no comprometer la evidencia necesaria para una posterior investigación. Algunas estrategias comunes incluyen:

- Aislamiento de sistemas comprometidos: Si un ataque afecta a un servidor o dispositivo específico, desconectarlo de la red puede evitar que el ataque se propague. Por ejemplo, en un caso de *ransomware*, desconectar inmediatamente las estaciones de trabajo infectadas puede proteger el resto de la red.

- Restricción de accesos: Imponer restricciones temporales a usuarios y dispositivos mientras se investiga el incidente. Esto puede incluir bloquear cuentas comprometidas o limitar los privilegios de administrador.

- Monitorización activa: Implementar una vigilancia más rigurosa de los sistemas no afectados para detectar señales de que el ataque intenta moverse lateralmente dentro de la red.

Un ejemplo práctico de esta estrategia ocurrió durante el ataque de *ransomware* WannaCry en 2017. Organizaciones que aislaron rápidamente los sistemas infectados lograron minimizar el impacto, mientras que otras que no tomaron medidas inmediatas enfrentaron una propagación masiva del *malware*.

Uso de herramientas y apoyo externo

Para muchas entidades locales, la contención efectiva puede requerir la ayuda de herramientas avanzadas o de actores externos. Por ejemplo:

- Herramientas de respuesta automatizada: sistemas de *Endpoint Detection and Response* (EDR) que permiten aislar dispositivos afectados con un solo clic.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

- Apoyo de CSIRT o SOC regionales: expertos en ciberseguridad que pueden proporcionar análisis en tiempo real y asesorar sobre las mejores prácticas de contención.

- Colaboración con proveedores tecnológicos: especialmente si el ataque afecta a un sistema proporcionado por un tercero, como una plataforma de gestión de servicios municipales.

En Galicia, la colaboración a través de la red Ciber.gal ha demostrado ser un modelo efectivo de apoyo interinstitucional, donde los ayuntamientos afectados por incidentes de ciberseguridad pueden contar con asistencia técnica inmediata de la AMTEGA y sus aliados.

Consideraciones específicas en infraestructuras críticas

Cuando el ataque afecta a infraestructuras críticas locales, como sistemas SCADA para el suministro de agua o electricidad, la contención requiere un enfoque aún más delicado. En estos casos, es esencial:

- Priorizar la continuidad del servicio: Si desconectar un sistema puede causar un impacto significativo en la ciudadanía, deben evaluarse medidas alternativas de contención que minimicen la interrupción.

- Evitar daños colaterales: Las acciones deben ejecutarse de manera que no afecten a servicios interdependientes. Por ejemplo, al contener un ataque en un sistema de transporte público, es importante asegurarse de que las plataformas de pago no queden inutilizables.

Un caso notable es el ataque al sistema de agua de Oldsmar, Florida, en 2021, donde un atacante intentó modificar químicamente los niveles de tratamiento del agua. La contención inmediata del sistema comprometido evitó un desastre potencial, demostrando la importancia de protocolos claros y la capacidad de reacción rápida.

La importancia de los procedimientos establecidos

Para que la contención sea efectiva, debe apoyarse en procedimientos predefinidos y bien practicados. Estos procedimientos deben incluir:

- Pasos específicos para diferentes tipos de ataques: desde *phishing* hasta *ransomware* o accesos no autorizados.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

- Coordinación clara: asegurarse de que todos los involucrados, desde técnicos hasta responsables políticos, comprendan su rol en la contención.

- Pruebas regulares: simulacros y ejercicios prácticos que preparen al personal para actuar con rapidez y confianza.

Equilibrio entre contención y preservación de evidencias

Una de las mayores dificultades en esta fase es equilibrar la necesidad de detener el ataque con la preservación de evidencias que puedan ser cruciales para la investigación forense. Tomar decisiones precipitadas, como apagar sistemas sin realizar una copia forense, puede dificultar la identificación del vector de ataque o los métodos utilizados por los ciberdelincuentes.

Por ello, se recomienda trabajar con herramientas y procedimientos que permitan:

- crear instantáneas de los sistemas afectados antes de aislarlos;

- registrar todas las acciones realizadas durante la contención para garantizar la trazabilidad.

La contención no es una solución definitiva, pero establece una barrera esencial que permite ganar tiempo para preparar la recuperación y el análisis posterior. En el caso de las entidades locales, donde los recursos son limitados, disponer de una estrategia clara de contención puede marcar la diferencia entre un incidente manejable y un desastre que paralice los servicios esenciales.

3.3. Investigación y análisis forense

Tras contener un ciberataque, la etapa de investigación y análisis forense se centra en comprender la naturaleza, el alcance y las implicaciones del incidente. Este proceso es esencial para identificar vulnerabilidades, aprender de la experiencia y tomar medidas que refuercen la seguridad futura de la entidad local.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

Objetivos de la investigación forense

La investigación forense tiene varios objetivos fundamentales:

- Identificar el punto de entrada del ataque: determinar cómo los atacantes accedieron al sistema, ya sea a través de un fallo en la configuración, una vulnerabilidad en el *software* o un error humano, como un clic en un correo malicioso;

- Evaluar el alcance del daño: detectar qué sistemas y datos han sido comprometidos, incluidos los que pueden haber sido exfiltrados o manipulados;

- Recolectar evidencias: recopilar datos que puedan ser utilizados para análisis internos, prevención de futuros incidentes o, en casos específicos, procedimientos legales.

Este proceso debe realizarse de manera meticulosa y documentada, siguiendo estándares de buenas prácticas en ciberseguridad y en cumplimiento de las normativas aplicables, como el Reglamento General de Protección de Datos (RGPD), si el incidente afecta a datos personales.

Metodología del análisis forense

El análisis forense en ciberseguridad sigue un enfoque sistemático que incluye varias etapas:

1. Adquisición de evidencias digitales:

    - Se realiza una copia forense de los sistemas afectados, asegurando la integridad de los datos mediante técnicas de *hash*. Esto evita que las evidencias sean manipuladas o cuestionadas. Ejemplo: Si un servidor es infectado por *ransomware*, se copia todo su contenido para su análisis, dejando el sistema original intacto.

2. Preservación del entorno afectado:

    - Mantener el estado de los sistemas tal como fueron encontrados en el momento del ataque. Esto incluye evitar reinicios o desconexiones innecesarias que puedan alterar las evidencias.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

3. Análisis detallado:

    - Identificar los patrones de comportamiento del atacante, los archivos o procesos sospechosos y los vectores de ataque utilizados. Por ejemplo, analizar *logs* de acceso, conexiones remotas y cambios realizados en el sistema.

4. Correlación de datos:

    - Cruzar información con bases de datos de amenazas conocidas (como indicadores de compromiso) para identificar herramientas o técnicas empleadas por los atacantes.

Herramientas y recursos para el análisis

En el ámbito local, muchas entidades no cuentan con equipos especializados en análisis forense, lo que hace necesario recurrir a herramientas específicas o a la colaboración con expertos externos. Algunas herramientas comúnmente utilizadas incluyen:

- Autopsy y EnCase: para análisis de discos duros y recuperación de datos.
- Wireshark: para examinar tráfico de red sospechoso.
- Volatility: para análisis de memoria y detección de *malware* en sistemas en ejecución.

Adicionalmente, organismos como el CCN-CERT, INCIBE o Ciber.gal ofrecen servicios de soporte y asesoramiento en análisis forense, permitiendo que incluso los pequeños municipios accedan a recursos avanzados.

Preservación de evidencias para acciones legales

Si existe la posibilidad de emprender acciones legales contra los responsables del ataque, es crucial que las evidencias recopiladas cumplan con los requisitos legales de admisibilidad. Esto incluye:

- Registrar la cadena de custodia: documentar quién tuvo acceso a las evidencias en cada momento.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

- Garantizar la integridad de los datos: utilizar técnicas de *hash* para certificar que los archivos analizados no han sido alterados.

Un caso relevante es el ataque a la ciudad de Atlanta en 2018, donde las autoridades locales trabajaron en estrecha colaboración con expertos forenses y fuerzas del orden para rastrear a los responsables, lo que resultó en arrestos y procesamientos.

Evaluación del impacto del ataque

La investigación también debe centrarse en medir el impacto real del ataque, considerando:

- Impacto operacional: servicios que fueron interrumpidos y tiempo necesario para su recuperación.
- Impacto económico: costes directos de la respuesta y la recuperación, así como posibles sanciones por incumplimiento normativo.
- Impacto reputacional: nivel de confianza ciudadana afectado por el incidente y cómo mitigarlo a través de la comunicación adecuada.

Por ejemplo, un ataque de *ransomware* en un ayuntamiento que gestione datos de ciudadanos puede tener implicaciones legales y financieras significativas si los datos afectados incluyen información personal sensible.

Incorporación de los resultados en las estrategias de seguridad

Los hallazgos del análisis forense no solo deben documentarse, sino también integrarse en las estrategias de ciberseguridad del municipio. Esto puede incluir:

- revisar y fortalecer las políticas de acceso a sistemas;
- actualizar herramientas de seguridad para prevenir vectores de ataque similares;
- implementar procesos de formación basados en los errores detectados durante el incidente.

La investigación y el análisis forense son más que una reacción al ataque; representan una oportunidad para fortalecer la ciberseguridad muni-

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

cipal y convertir una crisis en aprendizaje. Al comprender cómo y por qué ocurrió el incidente, las entidades locales pueden prepararse mejor para evitar recurrencias y responder con mayor eficacia en el futuro.

3.4. Recuperación y restablecimiento

La recuperación es una de las fases más críticas tras un ciberataque, ya que su objetivo es restablecer la funcionalidad de los sistemas afectados y garantizar que puedan operar de manera segura. Para las entidades locales, que suelen gestionar servicios esenciales, una recuperación exitosa es fundamental para minimizar el impacto en la ciudadanía y restaurar la confianza pública.

El primer paso en la recuperación es restaurar los sistemas afectados, priorizando aquellos que soportan servicios críticos. Este proceso implica:

- Validar las copias de seguridad: Antes de proceder a la restauración, es necesario garantizar que las copias de seguridad no estén comprometidas. En ataques de *ransomware*, por ejemplo, las copias conectadas a los sistemas infectados podrían haber sido cifradas.

- Restaurar los servicios prioritarios: La recuperación debe seguir un orden establecido en el plan de continuidad operativa, asegurando que los servicios más críticos sean los primeros en ser restablecidos. Por ejemplo, un ayuntamiento podría priorizar el sistema de emisión de certificados frente a otros menos esenciales.

- Realizar pruebas de integridad: Una vez restaurados, los sistemas deben ser sometidos a pruebas exhaustivas para confirmar que funcionan correctamente y no contienen elementos maliciosos residuales.

Un ejemplo práctico es el ataque sufrido por el Ayuntamiento de Jerez de la Frontera en 2020. La Administración utilizó copias de seguridad para restablecer sus sistemas, priorizando aquellos necesarios para atender a la ciudadanía. Sin embargo, la falta de pruebas iniciales causó problemas en algunos servicios secundarios, lo que subraya la importancia de la validación previa.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

Implementación de medidas preventivas

Una vez restaurados los sistemas, es crucial implementar medidas que prevengan recurrencias del ataque. Estas acciones incluyen:

- Actualizar y parchear sistemas: Muchas brechas de seguridad ocurren debido a vulnerabilidades conocidas en *software* desactualizado. Es fundamental aplicar parches de seguridad a todos los sistemas restaurados.

- Reforzar controles de acceso: Esto puede incluir la implementación de autenticación multifactor para usuarios y sistemas sensibles.

- Actualizar configuraciones de seguridad: Revisar y mejorar configuraciones de *firewalls*, antivirus y otros mecanismos de protección.

Comunicación con los ciudadanos

En los casos en que un ciberataque afecte servicios visibles para la ciudadanía, la recuperación debe ir acompañada de una estrategia de comunicación clara y transparente. Esto incluye:

- Informar sobre el restablecimiento de servicios: comunicar cuándo y cómo los servicios afectados estarán disponibles nuevamente.

- Explicar las medidas tomadas: detallar las acciones realizadas para garantizar la seguridad de los sistemas y la protección de los datos de los ciudadanos.

- Reforzar la confianza pública: reconocer el incidente de manera profesional y destacar los esfuerzos realizados para evitar futuros problemas.

Colaboración durante la recuperación

En esta fase, la colaboración con actores externos puede ser determinante. Las entidades locales pueden apoyarse en:

- CSIRT y SOC: Estos equipos proporcionan herramientas y conocimientos para garantizar una recuperación segura.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

- Proveedores tecnológicos: Ayudan en la restauración de servicios específicos, como plataformas de gestión municipal.

- Otras Administraciones: En casos de ataques que afectan a múltiples municipios, la cooperación interinstitucional permite compartir recursos y acelerar el proceso de recuperación.

3.5. Lecciones aprendidas y plan de mejora continua

La fase final tras un ciberataque, aunque a menudo subestimada, es una de las más valiosas para fortalecer la ciberseguridad de una entidad local. Este momento ofrece la oportunidad de reflexionar sobre lo sucedido, identificar áreas de mejora y establecer un plan de acción que minimice el riesgo de futuros incidentes. Una gestión adecuada de las lecciones aprendidas puede convertir un evento crítico en un punto de inflexión hacia una mayor resiliencia organizativa.

Evaluación posincidente

La evaluación posincidente es un análisis exhaustivo que busca responder a preguntas clave sobre el ataque y la respuesta adoptada. Este proceso debe ser sistemático e incluir:

1. Revisión de los eventos: Reconstruir cronológicamente lo sucedido, desde el momento en que se detectó el ataque hasta la restauración completa de los sistemas.

2. Identificación de debilidades: Evaluar qué aspectos fallaron, ya sean técnicos, organizativos o de comunicación. Por ejemplo, un análisis podría revelar que el ataque fue posible debido a una configuración incorrecta del *firewall* o a la falta de formación del personal.

3. Documentación de fortalezas: Identificar qué elementos de la respuesta funcionaron bien y cómo podrían replicarse en el futuro.

Este análisis debe involucrar a todos los actores que participaron en la gestión del incidente, desde técnicos hasta responsables políticos, para obtener una visión integral.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

Ajuste de políticas y procedimientos

Los hallazgos de la evaluación deben traducirse en ajustes concretos en las políticas y los procedimientos de ciberseguridad. Esto incluye:

- Actualización de los planes de respuesta a incidentes: incorporar lecciones aprendidas para mejorar la rapidez y eficacia de las acciones futuras.
- Revisión de la política de ciberseguridad municipal: ajustar directrices, roles y responsabilidades según los problemas identificados durante el incidente.
- Optimización del plan de continuidad operativa: modificar las prioridades de restauración de servicios basándose en la experiencia adquirida.

Por ejemplo, tras un ataque en un ayuntamiento español, se detectó que el plan de contingencia no cubría el acceso remoto de los empleados municipales, lo que retrasó la recuperación. Como resultado, el plan fue ampliado para incluir protocolos específicos para teletrabajo.

Formación y sensibilización del personal

Uno de los factores más comunes detrás de los ciberataques exitosos es el error humano. Por ello, tras un incidente, es fundamental reforzar la formación y sensibilización del personal. Esto incluye:

- Capacitación específica: enseñar a los empleados cómo identificar y responder a tácticas comunes, como *phishing* o *malware*.
- Simulacros regulares: realizar ejercicios prácticos que permitan al personal practicar la respuesta a diferentes tipos de ataques.
- Sensibilización a nivel político: involucrar a los responsables municipales en la formación, para garantizar su apoyo y comprensión de la importancia de la ciberseguridad.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

Implementación de mejoras tecnológicas

El análisis posincidente suele revelar deficiencias en las herramientas tecnológicas utilizadas. Las mejoras en este ámbito pueden incluir:

- Adopción de nuevas tecnologías: como sistemas de detección de amenazas basados en inteligencia artificial o soluciones avanzadas de monitorización de red.
- Actualización de *hardware* y *software*: reemplazar sistemas obsoletos que representan un riesgo para la seguridad.
- Fortalecimiento de la infraestructura tecnológica: mejorar la segmentación de redes, el cifrado de datos y los controles de acceso.

Un ejemplo es el ataque de *ransomware* a Baltimore en 2019, donde la falta de copias de seguridad adecuadas agravó el impacto. Tras el incidente, la ciudad invirtió en soluciones avanzadas de *backup* y recuperación.

Establecimiento de métricas de rendimiento

Para garantizar la mejora continua, es esencial establecer métricas que permitan medir el desempeño de la ciberseguridad en la entidad local. Estas métricas pueden incluir:

- tiempo promedio de detección de incidentes;
- tiempo de respuesta y recuperación;
- número de incidentes detectados y resueltos;
- grado de cumplimiento de normativas como el Esquema Nacional de Seguridad.

La monitorización regular de estas métricas permite evaluar la efectividad de las medidas implementadas y ajustar las estrategias según sea necesario.

Promoción de una cultura de resiliencia

Finalmente, una lección clave que debe surgir de cualquier ciberataque es la importancia de construir una cultura organizativa orientada a la resiliencia. Esto implica:

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

- Compromiso a todos los niveles: desde los responsables políticos hasta el personal técnico y operativo.

- Fomento de la colaboración: establecer alianzas con otros municipios, organizaciones y expertos en ciberseguridad.

- Comunicación abierta y transparente: informar a los ciudadanos sobre las acciones tomadas y su impacto positivo en la seguridad de los servicios públicos.

La fase de lecciones aprendidas y mejora continua cierra el ciclo de gestión del incidente y abre la puerta a un futuro más seguro. Para las entidades locales, que suelen operar bajo restricciones presupuestarias y de personal, este proceso representa una oportunidad única para maximizar el valor de cada experiencia, convirtiendo un desafío en una fortaleza organizativa.

4. La política de ciberseguridad municipal

La política de ciberseguridad municipal es un documento estratégico que establece las directrices, los principios y los procedimientos necesarios para garantizar la protección de los sistemas, datos y servicios digitales de una entidad local. Más que una declaración de intenciones, es una herramienta operativa que guía tanto las acciones preventivas como las reactivas ante incidentes de ciberseguridad.

Los objetivos principales de una política de ciberseguridad municipal son:

- Proteger los activos digitales: asegurar la integridad, disponibilidad y confidencialidad de la información y los sistemas.

- Garantizar la continuidad operativa: minimizar el impacto de los incidentes de ciberseguridad en los servicios esenciales.

- Cumplir con las normativas aplicables: adaptarse a marcos como el Esquema Nacional de Seguridad (ENS) y el Reglamento General de Protección de Datos (RGPD).

- Fomentar una cultura de seguridad: promover prácticas responsables entre empleados y colaboradores municipales.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

Una política de ciberseguridad municipal eficaz debe incluir componentes esenciales que aseguren la protección integral de los sistemas, datos y servicios. Estos componentes abarcan desde la identificación y gestión de riesgos hasta la capacitación del personal y el monitoreo continuo de la infraestructura tecnológica.

4.1. Gestión de riesgos

La gestión de riesgos es el pilar fundamental de cualquier política de ciberseguridad municipal. Este proceso permite a las entidades locales identificar y mitigar de manera proactiva las amenazas que puedan comprometer sus sistemas, datos y servicios. Dado que los recursos de los municipios son a menudo limitados, una gestión de riesgos efectiva ayuda a priorizar las inversiones y los esfuerzos en ciberseguridad.

La gestión de riesgos permite a las entidades locales adoptar un enfoque proactivo frente a las amenazas cibernéticas. Al identificar y abordar los puntos débiles antes de que sean explotados, los municipios no solo minimizan el impacto de los incidentes, sino que también optimizan el uso de sus recursos, enfocándolos en las áreas más críticas.

Inventario de activos críticos

Un paso inicial y esencial en la gestión de riesgos es realizar un inventario exhaustivo de los activos digitales del municipio. Esto incluye:

- Sistemas de información: plataformas de recaudación de impuestos, registros civiles, portales web municipales y otros sistemas críticos.
- Infraestructuras tecnológicas: servidores, redes, dispositivos de almacenamiento y sistemas SCADA utilizados en infraestructuras críticas como el suministro de agua o energía.
- Datos sensibles: información personal de los ciudadanos, datos financieros y otros registros confidenciales que deben protegerse.

El inventario debe clasificar estos activos según su importancia para la continuidad operativa y el impacto que tendría un incidente en cada uno. Por ejemplo, la base de datos de contribuyentes puede considerarse más crítica que un sistema de reservas para instalaciones deportivas.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

Evaluaciones periódicas de riesgos

Una vez identificados los activos críticos, es necesario evaluar regularmente los riesgos asociados. Esta evaluación debe considerar:

- Amenazas externas: ataques de *ransomware*, intentos de *phishing*, accesos no autorizados desde el exterior o interrupciones por ataque de denegación de servicio distribuido (*Distributed Denial-of-Service*, DDoS).
- Vulnerabilidades internas: configuraciones incorrectas, *software* obsoleto o credenciales débiles.
- Impacto potencial: consecuencias económicas, operativas y reputacionales que podría tener un incidente.

Las herramientas de evaluación de riesgos, como matrices de probabilidad e impacto, ayudan a priorizar los problemas más urgentes. Por ejemplo, un análisis podría identificar que un servidor clave, aún operativo con un sistema operativo sin soporte, representa un riesgo crítico que debe abordarse de inmediato.

Planes de mitigación

Basándose en los resultados de la evaluación, los municipios deben desarrollar planes específicos para reducir los riesgos detectados. Estos planes incluyen:

- Actualización de sistemas: garantizar que el *software* y el *hardware* utilizados estén actualizados con los últimos parches de seguridad.
- Segmentación de redes: separar las redes críticas de los sistemas menos sensibles para limitar la propagación de ataques.
- Controles de acceso: implementar políticas de acceso restringido, asegurando que solo el personal autorizado pueda interactuar con sistemas críticos.
- Uso de herramientas de monitorización: implementar sistemas de detección de intrusos (IDS) o herramientas avanzadas de análisis de tráfico para identificar comportamientos anómalos.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

Por ejemplo, tras evaluar el riesgo de un ataque de *ransomware*, un municipio podría priorizar la implementación de una política de copias de seguridad automatizadas, asegurándose de que los datos críticos puedan restaurarse rápidamente en caso de un ataque.

Gestión de riesgos como proceso continuo

La gestión de riesgos no es un ejercicio puntual, sino un proceso dinámico y continuo. Esto implica:

- Reevaluaciones periódicas: repetir el análisis a intervalos regulares o tras cambios significativos en la infraestructura, como la adopción de nuevas tecnologías.
- Adaptación a nuevas amenazas: mantenerse actualizado sobre las tendencias en ciberataques y ajustar los planes de mitigación según sea necesario.
- Integración con planes de contingencia: asegurar que las estrategias de gestión de riesgos estén alineadas con los procedimientos de respuesta a incidentes.

Un ejemplo práctico es la revisión anual de riesgos que realiza un municipio para actualizar su inventario de activos y ajustar sus prioridades de ciberseguridad en función de nuevos proyectos, como la digitalización de servicios ciudadanos.

4.2. Roles y responsabilidades

Una política de ciberseguridad municipal efectiva debe establecer claramente quién es responsable de cada aspecto de la seguridad, desde la planificación hasta la respuesta a incidentes. La claridad en los roles y responsabilidades no solo mejora la coordinación, sino que también asegura que todos los actores involucrados comprendan sus funciones y contribuyan a la protección de los activos digitales.

Responsables políticos

Los líderes políticos, como el alcalde y los concejales responsables de áreas tecnológicas, desempeñan un papel fundamental en la ciberseguridad municipal. Sus principales responsabilidades incluyen:

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

- Compromiso institucional: asegurar que la ciberseguridad sea una prioridad estratégica, destinando recursos adecuados y estableciendo políticas claras.

- Supervisión y aprobación: revisar y aprobar la política de ciberseguridad, así como los planes de contingencia y respuesta.

- Comunicación: informar de manera transparente a los ciudadanos sobre incidentes significativos, y las medidas adoptadas para resolverlos y prevenirlos.

Por ejemplo, el alcalde de un municipio podría liderar una iniciativa para certificar el cumplimiento del Esquema Nacional de Seguridad (ENS) y presentar los resultados en un pleno municipal.

Responsable de ciberseguridad (CISO)

El *Chief Information Security Officer* (CISO) o responsable de ciberseguridad es el encargado de implementar y supervisar la política de ciberseguridad. En los municipios más pequeños, esta función puede recaer en un técnico municipal con conocimientos específicos en seguridad digital. Sus funciones incluyen:

- Diseño e implementación: desarrollar y aplicar medidas técnicas y organizativas para proteger los sistemas y datos.

- Supervisión continua: monitorizar los sistemas para detectar y prevenir posibles amenazas.

- Gestión de incidentes: coordinar la respuesta ante ciberataques, incluyendo la comunicación con actores externos como CSIRT o proveedores tecnológicos.

- Capacitación del personal: liderar programas de formación y simulacros para preparar a los empleados ante posibles incidentes.

Un CISO en un municipio mediano, por ejemplo, podría liderar la instalación de herramientas de monitorización automatizada y garantizar que todos los empleados estén capacitados en las prácticas básicas de ciberseguridad.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

Técnicos municipales

Los técnicos municipales desempeñan un papel operativo en la implementación de medidas de ciberseguridad y en la gestión de sistemas tecnológicos. Sus responsabilidades incluyen:

- Gestión de infraestructura: mantener los sistemas actualizados, aplicar parches de seguridad y gestionar las configuraciones de red.
- Monitorización activa: utilizar herramientas de detección para identificar actividades sospechosas.
- Soporte en incidentes: actuar como el primer nivel de respuesta técnica en caso de ciberataque.

Por ejemplo, un técnico municipal podría ser el encargado de restaurar un sistema comprometido utilizando copias de seguridad validadas.

Empleados municipales

Todos los empleados municipales tienen un rol en la ciberseguridad, incluso si no trabajan directamente con tecnologías, ya que sus acciones individuales pueden influir significativamente en la protección de los sistemas. Sus responsabilidades incluyen:

- Cumplimiento de políticas: seguir las directrices establecidas, como el uso de contraseñas seguras y la autenticación multifactor.
- Notificación de anomalías: informar de correos sospechosos, actividades inusuales o posibles brechas de seguridad.
- Formación continua: participar en talleres y simulacros organizados para mejorar su conocimiento y sus habilidades en ciberseguridad.

Un empleado que detecte un correo sospechoso de *phishing* y lo reporte de inmediato podría evitar que el incidente se convierta en un ataque mayor.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

Colaboradores y proveedores externos

Los contratos con proveedores tecnológicos deben incluir cláusulas específicas de ciberseguridad para garantizar que estos cumplan con los estándares necesarios. Sus responsabilidades incluyen:

- Cumplimiento normativo: garantizar que los sistemas y servicios que proporcionan cumplen con el ENS y otras regulaciones aplicables.

- Soporte técnico: proporcionar asistencia en la configuración, el mantenimiento y la recuperación de sistemas críticos.

- Garantía de seguridad en la cadena de suministro: proteger sus propios sistemas para evitar que sean utilizados como vectores de ataque.

La seguridad en la cadena de suministro es fundamental para prevenir que las vulnerabilidades de los proveedores tecnológicos se conviertan en puntos de entrada para ciberataques, protegiendo así la integridad de los sistemas municipales y los datos sensibles que gestionan.

Un ejemplo reciente que ilustra la importancia de la seguridad en la cadena de suministro es el supuesto ciberataque a la Agencia Tributaria de España en diciembre de 2024. El grupo de piratas informáticos (no confundir con *hackers*) conocido como Trinity afirmó haber sustraído 560 GB de datos confidenciales de la Agencia, incluyendo información de contribuyentes, y exigió un rescate de 38 millones de dólares para no divulgar la información.

Sin embargo, la Agencia Tributaria negó haber detectado brechas de seguridad en sus sistemas y aseguró que todos sus servicios operaban con normalidad. Posteriormente, se indicó que una empresa privada externa, especializada en asesoría fiscal y laboral, podría haber sido la afectada, lo que sugiere que el ataque pudo haberse originado a través de un proveedor en la cadena de suministro.

Este incidente destaca la necesidad de que las entidades públicas y privadas garanticen que sus proveedores tecnológicos cumplan con estrictos estándares de ciberseguridad. La falta de medidas adecuadas en una empresa asociada puede convertirse en un punto de entrada para ciberataques que comprometan datos sensibles y afecten la integridad de los sistemas de la entidad principal.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

Por lo tanto, es esencial que los contratos con proveedores incluyan cláusulas específicas de ciberseguridad y que se realicen auditorías periódicas para asegurar el cumplimiento de las normativas y la protección de la información en toda la cadena de suministro.

La colaboración entre estos actores es fundamental para una ciberseguridad efectiva. Por ejemplo, en caso de un incidente, el técnico municipal podría identificar el problema inicial, el CISO coordinaría la respuesta técnica y el alcalde informaría a los ciudadanos sobre las medidas adoptadas. Esta coordinación debe estar respaldada por protocolos claros que definan cómo interactúan los diferentes roles en situaciones normales y de emergencia.

La asignación clara de roles y responsabilidades no solo fortalece la capacidad de respuesta ante incidentes, sino que también fomenta una cultura organizativa orientada a la ciberseguridad. Cada actor, desde el responsable político hasta el proveedor externo, juega un papel indispensable en la protección de los sistemas y datos municipales, convirtiendo la ciberseguridad en un esfuerzo compartido.

4.3. Formación y sensibilización

El factor humano es considerado uno de los eslabones más vulnerables en la ciberseguridad. Por ello, la formación y la sensibilización de los empleados municipales y responsables políticos son componentes esenciales de cualquier política de ciberseguridad. Estas acciones ayudan a reducir los riesgos asociados con errores humanos y a fortalecer la cultura organizativa orientada a la protección de los sistemas y datos.

Invertir en la formación y sensibilización del personal no solo reduce los riesgos de ciberataques exitosos, sino que también promueve una cultura organizativa donde la seguridad es una responsabilidad compartida. Al combinar talleres, simulacros y campañas de concienciación, los municipios pueden convertir a sus empleados en una primera línea de defensa eficaz frente a las amenazas digitales.

Objetivos de la formación y sensibilización

La capacitación en ciberseguridad debe estar diseñada para lograr los siguientes objetivos:

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

- Incrementar la conciencia sobre las amenazas: ayudar a los empleados a identificar y comprender los riesgos asociados con prácticas inseguras.

- Promover comportamientos seguros: fomentar el uso de contraseñas robustas, la autenticación multifactor y el manejo adecuado de la información sensible.

- Facilitar una respuesta eficaz ante incidentes: asegurar que todos los empleados sepan cómo actuar en caso de un ciberataque, reduciendo el impacto y facilitando la recuperación.

- Fortalecer el compromiso de los responsables políticos: garantizar que los líderes municipales entiendan la importancia estratégica de la ciberseguridad y respalden las iniciativas necesarias.

Programas de formación continuos

La formación debe ser accesible, regular y adaptada a las funciones de los distintos empleados municipales. Algunos enfoques clave incluyen:

- Talleres básicos de ciberseguridad: Dirigidos a todos los empleados, estos talleres pueden cubrir temas como:

  - cómo detectar correos de *phishing*;

  - manejo seguro de contraseñas;

  - prácticas seguras en el uso del correo electrónico y de dispositivos conectados.

- Capacitación avanzada para técnicos municipales: Incluir temas como:

  - análisis de incidentes de seguridad;

  - configuración segura de redes y sistemas;

  - uso de herramientas de detección de intrusos y respuesta a incidentes.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

- Sesiones específicas para responsables políticos: Asegurar que comprendan:
  - el impacto económico y reputacional de los ciberataques;
  - la importancia de destinar recursos adecuados a la ciberseguridad;
  - su rol en la comunicación con los ciudadanos en caso de incidentes.

Simulacros y ejercicios prácticos

Los simulacros son una herramienta poderosa para evaluar y mejorar la preparación del personal ante incidentes reales. Estos ejercicios deben incluir:

- Simulaciones de *phishing*: enviar correos falsos para medir cuántos empleados caen en el engaño y utilizar los resultados para reforzar la capacitación.
- Simulacros de ataques de *ransomware*: evaluar la capacidad del equipo técnico y de los empleados para contener el ataque y restaurar los sistemas.
- Ejercicios de respuesta en equipos interdisciplinarios: integrar a los responsables políticos, técnicos y administrativos en un escenario simulado para mejorar la coordinación y la toma de decisiones.

Un ejemplo exitoso es el de un municipio que, tras realizar un simulacro de *phishing*, detectó que más del 30 % de los empleados había hecho clic en un enlace sospechoso. Esto llevó a un refuerzo inmediato de la formación, reduciendo el porcentaje a menos del 10 % en un segundo ejercicio.

Campañas de concienciación

Además de la formación formal, las campañas de concienciación pueden mantener a los empleados alerta frente a las amenazas diarias. Estas campañas pueden incluir:

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

- Boletines informativos: enviar recordatorios periódicos con consejos de ciberseguridad, como “no compartas contraseñas” o “verifica los remitentes de correos electrónicos”.

- Material visual: colocar carteles en áreas comunes con mensajes clave, como “piensa antes de hacer clic”.

- Reconocimientos: premiar a los empleados que demuestren buenas prácticas de ciberseguridad, fomentando comportamientos positivos.

Personalización según roles

No todos los empleados municipales enfrentan los mismos riesgos o manejan información del mismo nivel de sensibilidad. Por ello, la formación debe adaptarse a las responsabilidades específicas de cada rol:

- Administrativos: centrarse en el manejo seguro de datos personales y cómo proteger documentos confidenciales.

- Técnicos: enfocarse en la configuración segura de sistemas y la gestión de incidentes.

- Directivos: enseñar la toma de decisiones estratégicas y la gestión de la comunicación ante incidentes.

Evaluación de impacto y mejora continua

Para garantizar la efectividad de la formación y sensibilización, es necesario medir su impacto y ajustarla según sea necesario. Esto puede incluir:

- Encuestas de conocimiento: evaluar periódicamente el nivel de conciencia sobre ciberseguridad entre los empleados.

- Análisis de incidentes: revisar cuántos incidentes han sido causados por errores humanos y ajustar la capacitación en consecuencia.

- Revisión de simulacros: identificar debilidades observadas durante los ejercicios y reforzar esas áreas específicas.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

4.4. Implementación y monitorización

La implementación y la monitorización son los pilares que aseguran que la política de ciberseguridad municipal no solo quede como un documento formal, sino que también se traduzca en acciones concretas y efectivas. Este componente esencial abarca desde la planificación inicial hasta la supervisión continua, permitiendo ajustar estrategias según cambien las circunstancias o evolucionen las amenazas.

La implementación y la monitorización continua aseguran que la política de ciberseguridad sea más que un documento formal, convirtiéndola en una herramienta activa de protección. Al priorizar acciones, supervisar su cumplimiento y adaptarse a un entorno cambiante, los municipios pueden garantizar una protección sostenible y efectiva para sus sistemas y servicios.

Implementación estructurada

La implementación de la política de ciberseguridad debe ser un proceso planificado y estructurado que garantice su adopción efectiva en toda la organización. Los pasos clave incluyen:

1. Aprobación institucional:

    - La política debe ser aprobada por el órgano correspondiente (pleno municipal, junta de gobierno, etc.), asegurando su legitimidad y respaldo institucional.

    - Este proceso debe incluir una presentación clara de los objetivos y beneficios de la política para todos los actores implicados, desde responsables políticos hasta empleados.

2. Asignación de recursos:

    - Presupuesto: garantizar que se disponga de recursos financieros suficientes para implementar las medidas necesarias, como la adquisición de herramientas de ciberseguridad o la contratación de formación externa.

    - Personal: designar a un equipo o responsable técnico que lidere el proceso de implementación, asegurando que los roles y responsabilidades estén claramente definidos.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

3. Priorización de acciones:

    - Comenzar por las medidas más críticas, como la actualización de sistemas, la implementación de controles de acceso y la formación inicial del personal.

    - Establecer un calendario realista que permita implementar la política en fases, reduciendo la presión sobre recursos limitados.

Monitorización continua

La monitorización es una actividad permanente que garantiza que las medidas implementadas se mantengan efectivas frente a nuevas amenazas o cambios en la infraestructura tecnológica. Los elementos clave de la monitorización incluyen:

1. Supervisión técnica:

    - Sistemas de detección de intrusos (IDS): herramientas que analizan el tráfico de red en tiempo real para identificar comportamientos anómalos o posibles intentos de ataque.

    - Monitorización de eventos: revisar los logs generados por sistemas críticos para detectar patrones sospechosos, como intentos de acceso fallidos o cambios no autorizados en configuraciones.

2. Auditorías periódicas:

    - Realizar auditorías internas o externas que evalúen el cumplimiento de la política y la efectividad de las medidas implementadas.

    - Estas auditorías pueden incluir simulacros de ciberataques, pruebas de penetración (*pentesting*) y revisiones de la infraestructura tecnológica.

3. Indicadores clave de desempeño (KPI):

    - Definir métricas para evaluar el éxito de la política, como:

        o tiempo promedio de detección de incidentes;

        o número de vulnerabilidades corregidas en cada revisión;

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

  - o porcentaje de empleados capacitados en prácticas de ciberseguridad.

- Utilizar estos indicadores para identificar áreas de mejora y justificar nuevas inversiones.

Actualización y adaptabilidad

El entorno de ciberseguridad es dinámico, con amenazas que evolucionan constantemente. Por ello, la política debe ser revisada y actualizada regularmente para reflejar:

- Cambios normativos: adaptarse a actualizaciones en el Esquema Nacional de Seguridad o nuevas regulaciones, como directivas europeas.

- Innovaciones tecnológicas: incorporar tecnologías emergentes que refuercen la seguridad, como herramientas de inteligencia artificial para la detección de amenazas.

- Lecciones aprendidas: ajustar estrategias tras la gestión de incidentes o los resultados de auditorías.

Un ejemplo práctico es la revisión anual que algunos municipios realizan de su política de ciberseguridad, incorporando hallazgos de simulacros o cambios en su infraestructura tecnológica, como la adopción de sistemas de teletrabajo.

Comunicación y transparencia

La implementación y la monitorización deben ir acompañadas de una comunicación efectiva que:

- informe regularmente a los responsables políticos sobre el estado de la ciberseguridad municipal, incluyendo logros, retos y necesidades;

- mantenga a los empleados al tanto de nuevas medidas o cambios en la política;

- en casos de incidentes, proporcione a los ciudadanos información clara sobre las acciones tomadas para resolver el problema y prevenir futuros ataques.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

Buenas prácticas en implementación y monitorización

Algunos municipios han demostrado enfoques exitosos en este componente:

- Centralización de recursos: utilizar SOC regionales para monitorizar actividades y gestionar incidentes, optimizando recursos limitados.
- Integración con servicios externos: contratar servicios gestionados de seguridad que ofrezcan monitorización continua y respuestas rápidas a incidentes.
- Auditorías compartidas: participar en programas de revisión conjunta con otras entidades locales o Administraciones superiores para reducir costes y mejorar la eficacia.

5. Análisis DAFO

El análisis DAFO (debilidades, amenazas, fortalezas y oportunidades) es una herramienta estratégica ampliamente utilizada en la gestión organizativa, y en el ámbito de la ciberseguridad municipal resulta especialmente útil. Esta metodología permite a las entidades locales identificar y priorizar los factores internos y externos que afectan a su capacidad para prevenir, gestionar y responder a ciberataques. Además, el DAFO ofrece una visión clara y estructurada para tomar decisiones informadas y desarrollar políticas eficaces de ciberseguridad.

Debilidades

Las debilidades representan los factores internos que limitan la capacidad de una entidad local para protegerse contra ciberataques. Entre las más comunes destacan:

- Recursos humanos insuficientes: Muchas entidades locales, especialmente las más pequeñas, carecen de personal técnico especializado en ciberseguridad.
- Sistemas obsoletos: La falta de presupuesto para renovar infraestructuras tecnológicas deja a los municipios expuestos a vulnerabilidades conocidas.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

- Falta de planes de contingencia: La ausencia de procedimientos claros para gestionar ciberataques dificulta la respuesta organizada ante incidentes.

- Baja formación del personal: Empleados municipales no capacitados pueden ser un punto de entrada para atacantes, especialmente a través de técnicas como el *phishing*.

- Dependencia de proveedores externos: La gestión delegada de sistemas críticos sin supervisión adecuada puede aumentar el riesgo.

Amenazas

Las amenazas representan los factores externos que pueden afectar negativamente la ciberseguridad de las entidades locales. Algunas de las más relevantes incluyen:

- Incremento en la sofisticación de los ataques: Los ciberdelincuentes utilizan herramientas avanzadas, como *ransomware* personalizado o ataques dirigidos (*spear phishing*), que son difíciles de detectar con sistemas tradicionales.

- Falta de coordinación interinstitucional: En algunos casos, la falta de colaboración entre Administraciones dificulta una respuesta rápida y efectiva a incidentes de gran magnitud.

- Regulación estricta y sanciones: El incumplimiento del Reglamento General de Protección de Datos o del Esquema Nacional de Seguridad puede derivar en sanciones económicas significativas tras un incidente.

- Escasez de soluciones tecnológicas accesibles: Las entidades pequeñas a menudo no tienen acceso a herramientas avanzadas de ciberseguridad, debido a sus costes.

Fortalezas

Las fortalezas son los elementos internos que aportan ventaja competitiva y pueden ser aprovechados para mejorar la ciberseguridad. En el caso de las entidades locales, algunas de las principales fortalezas incluyen:

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

- Proximidad a la ciudadanía: Permite una comunicación rápida y directa para gestionar incidentes y generar confianza en la respuesta adoptada.

- Colaboración interadministrativa: El proyecto RED ARGOS, en el que participan las comunidades de Andalucía, Castilla y León y País Vasco, tiene como principal objetivo contribuir a impulsar y fortalecer el ecosistema nacional de ciberseguridad y aumentar la adopción global de la misma, principalmente por empresas, basándose en la generación de capacidades especializadas, el trabajo en red de diferentes nodos de ciberseguridad regionales y la puesta en marcha de diferentes instrumentos de apoyo directo a las empresas.

- Acceso a subvenciones públicas: Programas de financiación específicos pueden facilitar la adquisición de herramientas y formación en ciberseguridad.

- Personal comprometido: Aunque falte especialización, muchos empleados muestran una gran disposición para adaptarse y mejorar sus competencias si reciben la formación adecuada.

Oportunidades

Las oportunidades son factores externos positivos que las entidades locales pueden aprovechar para mejorar su postura de ciberseguridad. Entre las más destacadas se encuentran:

- Avances tecnológicos: Soluciones basadas en inteligencia artificial y aprendizaje automático están haciendo más accesible la detección y respuesta a amenazas.

- Apoyo de organismos especializados: Entidades como INCIBE, CCN-CERT o iniciativas regionales proporcionan recursos técnicos y capacitación.

- Aumento de la sensibilización pública: Los ciudadanos son cada vez más conscientes de la importancia de la ciberseguridad, lo que facilita la implementación de medidas a nivel local.

- Programas europeos de ciberseguridad: La Unión Europea impulsa iniciativas y fondos para mejorar la ciberseguridad en Administraciones públicas.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

Integración del DAFO en la planificación estratégica

El análisis DAFO no es un fin en sí mismo, sino una herramienta para orientar decisiones estratégicas. Una vez identificado el panorama interno y externo, las entidades locales deben:

1. Priorizar las áreas críticas: centrarse en abordar debilidades clave y contrarrestar las amenazas más inmediatas, como la actualización de sistemas o la formación del personal.

2. Explotar fortalezas y oportunidades: ampliar la colaboración con organismos especializados o participar en programas de financiación para implementar soluciones avanzadas.

3. Desarrollar planes de acción basados en el DAFO: integrar los resultados del análisis en políticas de ciberseguridad municipales y planes de contingencia.

Por ejemplo, un pequeño municipio que identifique como debilidad su falta de recursos técnicos podría priorizar acuerdos con su diputación provincial para acceder a servicios compartidos. Al mismo tiempo, podría aprovechar oportunidades como subvenciones autonómicas para financiar la capacitación de su personal.

El análisis DAFO permite a las entidades locales comprender su situación actual en materia de ciberseguridad y diseñar estrategias realistas y efectivas para mejorar su resiliencia. Al integrar esta herramienta en la planificación estratégica, los municipios no solo estarán mejor preparados para enfrentar ciberataques, sino que también podrán optimizar sus recursos y generar mayor confianza entre los ciudadanos y actores externos.

6. Conclusiones

Las entidades locales se enfrentan a un entorno cada vez más desafiante en términos de ciberseguridad. Su dependencia de infraestructuras tecnológicas, combinada con la responsabilidad de proteger datos sensibles y garantizar la continuidad de servicios esenciales, las coloca en una posición de riesgo elevado frente a ciberataques. Este capítulo ha proporcionado un marco integral para abordar estas amenazas, destacando tanto las acciones inmediatas como los elementos estratégicos necesarios para fortalecer la resiliencia.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

Un resumen de los puntos clave para afrontar estos desafíos sería:

1. La importancia de la preparación y la planificación: La ciberseguridad debe ser vista como un proceso continuo que involucra no solo tecnología, sino también políticas claras, formación del personal y análisis estratégico. Contar con un plan de contingencia y continuidad operativa es fundamental para minimizar el impacto de cualquier incidente.

2. Pasos a seguir frente a un ciberataque: Desde la detección temprana hasta la recuperación, cada fase requiere protocolos bien definidos y una coordinación eficiente entre los actores implicados. La capacidad de aprender de cada incidente y ajustar las estrategias es clave para una mejora continua.

3. La política de ciberseguridad municipal como pilar estratégico: Este documento no solo guía las acciones preventivas y de respuesta, sino que también define responsabilidades, establece prioridades y asegura el cumplimiento normativo. Adaptar estas políticas a las características y los recursos de cada municipio es esencial.

4. El valor del análisis DAFO: Esta herramienta ofrece una visión clara de las debilidades y amenazas, pero también permite identificar fortalezas y oportunidades que pueden ser aprovechadas para mejorar la ciberseguridad municipal de manera realista y sostenible.

A la luz de los desafíos y soluciones presentados, se destacan las siguientes recomendaciones para las entidades locales:

- priorizar la formación y sensibilización del personal como elemento esencial para prevenir incidentes;

- fomentar la colaboración con organismos especializados y aprovechar los recursos disponibles a nivel regional y nacional;

- realizar evaluaciones periódicas de ciberseguridad mediante análisis DAFO para ajustar estrategias y priorizar inversiones;

- adoptar tecnologías avanzadas, como sistemas de detección automatizada, en función de las capacidades y necesidades específicas de cada municipio.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

7. Bibliografía

Centro Criptológico Nacional y Federación Española de Municipios y Provincias. (2022). *Prontuario de ciberseguridad para entidades locales*. Disponible en https://ens.ccn.cni.es/es/docman/documentos-publicos/25-ccn-cert-prontuario-ciberseguridad/file.

Cotino, L. y Sánchez, M. (2021). *Guía de ciberseguridad para ciudades inteligentes*. Washington: BID.

Vila Avendaño, P. (2018). *Técnicas de análisis forense informático para peritos judiciales profesionales*. Madrid: OxWord.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6