Servicios públicos locales seguros y confiables para todos

FEMP y CCN-CNI siguen afrontando el reto de la ciberseguridad de los Gobiernos Locales en el marco de la colaboración que mantienen ambas instituciones; la publicación de la "Guía para para la Gestión de Crisis para Ciberincidentes en las Entidades Locales", presentada en la FEMP en el marco de una jornada, fue una de las actuaciones más recientes para avanzar hacia servicios públicos seguros y confiables para todos los ciudadanos.

A. Junquera

Prevención y capacidad de reacción ante los ciberataques son las herramientas con las que cuentan tanto los Gobiernos Locales como el resto de las Administraciones a la hora de garantizar la prestación de servicios públicos y confiables para la ciudadanía. Así lo aseguraron el Secretario General de la FEMP, Carlos Daniel Casares, y la Secretaria de Estado Directora del Centro Nacional de Inteligencia, CNI, Esperanza Casteleiro, en sus intervenciones de apertura de la Jornada sobre Ciberseguridad en Entidades Locales, organizada por ambos organismos. En el marco de este encuentro se presentó la *"Guía para la Gestión de Crisis para Ciberincidentes en las Entidades Locales"*.

En su intervención, el Secretario General de la FEMP destacó los logros de la colaboración mantenida desde 2008 entre la Federación y el Centro Nacional de Inteligencia, CNI, y el Centro Criptológico Nacional, CCN. Y, según explicó, la importancia de esta relación a día de hoy, cuando *"se suceden los ataques cibernéticos"* en una Administración Local en la que la tecnología está cada día más presente tanto en su funcionamiento como en la prestación de servicios a la ciudadanía, está en *"disponer de un escudo permanente tanto para la prevención como para la resolución de incidentes"*. Poder contar con la colaboración del CNI supone *"la mejor garantía en el diseño y la implementación de las políticas de seguridad telemática"*.

En el marco de esta colaboración, destacó Casares, y ante una Administración que avanza hacia la digitalización plena, la fortaleza de la Federación está en la capacidad de llegar a todos los Ayuntamientos y en la posibilidad de concienciar a lo largo de todo el territorio: *"estamos impulsando una importante cantidad de actuaciones, en especial la difusión de alertas de seguridad y de documentos normativos e información de ayuda a la implantación"*, dijo, y se refirió a documentos como la Guía sobre el Esquema Nacional de Seguridad, ENS, entre otras muchas, y al extenso programa de formación en diferentes aspectos relacionados con la prevención y la seguridad en esta materia.

Para la Secretaria de Estado Directora del CNI, la principal responsabilidad del CCN es reducir el riesgo y las amenazas presentes en el ciberespacio y asegurar la seguridad de los sistemas de las Tecnologías de la Información en las Administraciones. *"No puede haber transformación digital sin ciberseguridad"*, y por ello es preciso *"construir entre todos un ciberescudo público para nuestro país"*, destacó coincidiendo con el Secretario General de la FEMP.

Esperanza Casteleiro también hizo referencia al convenio como *"un caso de éxito que muestra los beneficios de la colaboración entre ambas instituciones"* y subrayó que uno de los principales logros fue "l*a interpretación de forma práctica y homogénea*" en el conjunto de las Entidades Locales del Esquema Nacional de Seguridad, ENS, y su adecuación al mismo. En este punto, la Directora reafirmó el papel desarrollado por los Gobiernos Locales Intermedios a la hora de apoyar a los municipios más pequeños en la implantación del ENS y el fomento de la capacidad de detección y respuesta a incidentes.

Guía específica para Entidades Locales

En la jornada se presentó la *"Guía para para la Gestión de Crisis para Ciberincidentes en las Entidades Locales"*, un texto con el que se pretende facilitar herramientas para reforzar la ciberseguridad a los responsables de los Gobiernos Locales, a todos aquéllos *"sustentan la responsabilidad de hacer más segura y confiable la Administración Pública y más eficiente y eficaz la respuesta en caso de posibles ciberataques"*.

Según queda recogido en la introducción, con la publicación *"se espera contribuir a mejorar las capacidades de las Entidades Locales para responder ante un incidente de ciberseguridad relevante y de alto impacto, para gestionar una cibercrisis y volver a la normalidad con las menores consecuencias para las Entidades Locales, la ciudadanía y sus otros grupos de interés"*.

La Guía tiene dos partes. La primera propone un Modelo Básico de Organización para gestionar cibercrisis y sus elementos clave (comité de crisis, funciones de los distintos responsables, etc.). Y la segunda propone un Modelo de Protocolo de Actuación en caso de incidente que puede derivar en crisis (criterios de evaluación, acciones durante las diferentes fases del gobierno de la crisis). Los contenidos de la Guía se complementan con ejemplos, lecciones aprendidas y buenas prácticas en gestión de crisis, obtenidas a partir del trabajo de análisis de más de 100 casos reales en los ámbitos nacional e internacional, y también de la experiencia compartida por Entidades Locales que han vivido recientemente un ciberataque de nivel muy alto o crítico.

La Guía está disponible para su consulta y descarga en este QR

Reforzar la seguridad de las Entidades Locales

En el marco de la Jornada se celebró una mesa redonda en la que se abordó la necesidad de reforzar la ciberseguridad en las Entidades Locales. Tres participantes, Javier Candau, Jefe de Departamento en Centro Criptológico Nacional; Virginia Moreno, Directora General Nuevas Tecnologías e Innovación del Ayuntamiento de Leganés; y Javier de la Villa, Jefe de Explotación del Servicio TIC-Responsable de Seguridad de la Información de la Diputación Provincial de León, hicieron sus aportaciones:

Javier Candau puso de manifiesto los riesgos derivados del teletrabajo en pandemia: *"La pandemia nos hizo ir al teletrabajo. Hizo que todas nuestras Administraciones Públicas, también las Entidades Locales, dijeran a sus funcionarios que trabajaran en casa, pero no les dimos ordenadores, trabajaban con sus medios, con su conexión a Internet. Esto, que fue un éxito durante 2020, no estuvo seguido de las mejoras de ciberseguridad que necesitaban. Tenemos que fortalecer todas las capacidades de prevención, pasar auditorías, implantar el multifactor de autenticación, hacer mucha vigilancia e intercambiar mucha información entre todos"*.

Para **Virginia Moreno**, a estos efectos *"la Guía es importante porque van a venir muchos más ataques y tenemos que estar preparados. Por ello, es muy alentador que nos unamos y estemos con fuerza y con capacidad y, sobre todo, sepamos a que nos enfrentamos. En especial, por servir de referencia para los Ayuntamientos. La Guía va a ayudar a calmar, a poder acometer esas respuestas desde las Entidades Locales, enfrentarlo y poder levantarnos"*.

Javier de la Villa subrayó que *"en épocas pasadas, cuando todo era en papel"*, los habilitados nacionales tenían interiorizada su responsabilidad de protección de esa información, *"que ningún expediente se violara, que toda la documentación estuviera disponible, que no hubiera ningún problema con ningún expediente"*, pero en la época actual, *"estoy percibiendo que a determinados perfiles dentro de las organizaciones les cuesta involucrarse en todo lo que sea sinónimo de tecnología"*. A su juicio, hay que intentar que se involucren más y poner en valor dentro de las organizaciones esos perfiles.