# El CCN-CERT, principal apoyo de los Ayuntamientos en la protección de sus sistemas informáticos

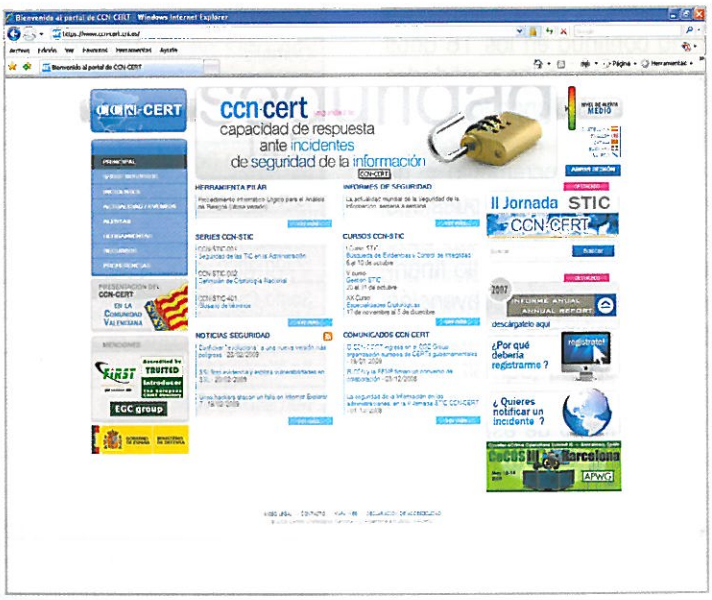
**Los crecientes ataques a los sistemas de la información de las Entidades Locales, pueden poner en peligro la integridad de los datos que gestionan los Ayuntamientos y su confidencialidad, así como la disponibilidad y el acceso a los servicios online que deben ofrecer las Administraciones, tal y como recoge la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.**

El Centro Criptológico Nacional, a través de su servicio de Respuesta ante Incidentes (CCN-CERT), precisamente tiene como principal objetivo ayudar y colaborar con los Ayuntamientos para prevenir los incidentes de seguridad y, llegado el caso, responder de forma rápida y eficiente ante cualquier ataque que puedan sufrir.

En enero del año pasado, un hacker accedió al servidor central de un Ayuntamiento español y borró toda la información municipal tramitada. Unos meses más tarde, en la primera quincena de agosto, otro Consistorio se vio afectado por un virus muy potente denominado "Gitano", que se propagó por toda la red informática municipal bloqueando el sistema operativo y colapsando la actividad municipal.

Estos son sólo algunos ejemplos de los riesgos y amenazas a los que están expuestos hoy en día los sistemas de información de cualquier organismo, capaces de afectar seriamente a su normal funcionamiento.

Con el fin de prevenir estos ataques, el Centro Criptológico Nacional (CCN), adscrito al Centro Nacional de Inteligencia (CNI), puso en marcha en el año 2007 el servicio de Respuesta a Incidentes de Seguridad (CCN-CERT). Además, el pasado mes de diciembre, la FEMP firmaba un acuerdo de colaboración con el CCN, por el cual ambas instituciones se comprometían a impulsar la seguridad de las Entidades Locales, mediante el intercambio de información, la formación especializada y el desarrollo de proyectos tecnológicos.




## ¿Qué es el CCN-CERT?

Ataques contra sitios web, fraude online, robo de información y datos sensibles... La extensión del uso de las Tecnologías de la Información y la Comunicación (TIC) y de Internet, así como la progresiva interconexión de los sistemas en un mundo cada vez más globalizado, han traído consigo nuevos retos a la hora de afrontar las amenazas que ponen en peligro los sistemas de la información de las Administraciones.

Desde esta perspectiva, era necesaria la creación de un Organismo especializado, encargado de velar por la seguridad de estos sistemas (máxime si se tienen en cuenta las previsiones para 2010, que señalan que más del 80% de los trámites administrativos se realizará por Internet). Este organismo, creado en el año 2004, lo constituye el Centro Criptológico Nacional, del cual depende el Equipo de Respuesta a Incidentes de Seguridad de la Información (CCN-CERT), un centro de alerta nacional creado a principios de 2007 que coopera y ayuda a todas las Administraciones a prevenir los incidentes de seguridad o, llegado el caso, a responder de forma rápida y eficiente ante cualquier ataque que puedan sufrir.

## Servicios del CCN-CERT para las Entidades Locales

Para hacer frente a estas amenazas, el CERT gubernamental pone a disposición de las Administraciones Locales una serie de recursos gratuitos con los que poder mejorar la seguridad de sus sistemas y, de esta forma, garantizar su funcionamiento eficaz al servicio del ciudadano.

El Centro Criptológico Nacional, a través de su servicio de Respuesta ante Incidentes (CCN-CERT), tiene como principal objetivo ayudar a los Ayuntamientos a prevenir los incidentes de seguridad

Estos servicios, recogidos todos ellos en el portal www.ccn-cert.cni.es, podrían dividirse en tres grandes grupos, en función del momento y la forma en que se actúe ante un incidente. Así nos encontramos con: servicios reactivos (destinados a responder a una amenaza o incidente que pueda haber sufrido un ordenador o un sistema de información de la Administración y a minimizar su impacto), servicios proactivos (aquéllos destinados a reducir los riesgos de seguridad a través de información e implantación de sistemas de protección y detección) y servicios de gestión (ofrecidos con el fin de mejorar los procesos de trabajo).

De entre todos ellos, los más destacados podrían ser:

• Gestión de incidentes. A través de su servicio de apoyo técnico, se ofrece soporte y coordinación para la resolución de incidentes. El CCN-CERT actúa rápidamente ante cualquier ataque recibido en los sistemas de información de cualquier sistema. Proporciona asistencia, señala documentos técnicos relevantes o sugiere medidas para restaurar la seguridad del sistema.

• Alertas y avisos. Información sobre vulnerabilidades (debilidad o falta de control que permitiría o facilitaría que una amenaza actuase contra un objetivo o recurso de un sistema), alertas y avisos de nuevas amenazas a los sistemas de información, basadas tanto en el trabajo de sus propios analistas como en las contribuciones procedentes de muy diversas fuentes de reconocido prestigio, nacionales e internacionales.

• Gestión de vulnerabilidades. Junto con la tarea de informar sobre las vulnerabilidades detectadas en los sistemas operativos y aplicaciones más conocidos (por ejemplo, Microsoft, Red Hat, Sun, HP, IBM, Oracle, etc....), el CCN-CERT colabora en la resolución de aquellas otras potenciales amenazas detectadas por los diferentes organismos de la Administración que así lo requieran.

• Análisis de código dañino. Supervisión de todo tipo de amenazas y agentes dañinos remitidos, con el fin último de prevenir cualquier incidente en los sistemas de información de los Entes Locales.

• Análisis de riesgos. Identificación sistemática de las amenazas y peligros que acechan a los distintos componentes pertenecientes o relacionados con el sistema de información, para determinar la vulnerabilidad del sistema ante esas amenazas y para estimar el impacto o grado de perjuicio que una seguridad insuficiente puede tener para la organización.

• Información sobre normas, instrucciones, guías y recomendaciones (Series CCN-STIC) para la implantación de proyectos de mejora de la Seguridad de la Información. En este apartado se enmarcan los documentos CCN-STIC, elaborados por el CCN y actualizados continuamente, para garantizar la seguridad de los Sistemas TIC. Este conjunto normativo tiene por objeto que los responsables de seguridad de la Administración dispongan de las necesarias referencias que les faciliten el cumplimiento de los requisitos de seguridad exigibles a sus sistemas.

• Formación y sensibilización. Uno de los pilares básicos de la Seguridad de la Información es la sensibilización de sus usuarios, así como la continua actualización de sus conocimientos. Por ello es imprescindible una formación del personal responsable de las TIC en todas las organizaciones, incluidas, por supuesto, la Administración Local. El CCN-CERT ofrece a lo largo de todo el año sus cursos gratuitos STIC de formación (presencial y a distancia) a través del INAP (Instituto Nacional de Administración Pública). Estos cursos están publicados además en su portal.

• Herramientas de seguridad. El CCN desarrolla distintas herramientas de apoyo a la gestión de la seguridad que facilita a todas los responsables TIC de los Ayuntamientos que así lo requieran. Entre ellas, la herramienta PILAR que soporta el análisis y la gestión de riesgos de un sistema de información, así como otras de análisis de vulnerabilidades, detección de software dañino, de análisis de contraseñas o anti-spam.

El éxito de estos servicios, desplegados durante estos dos años de intenso trabajo por el CERT gubernamental español, se refleja en la buena acogida por parte de las diferentes Administraciones (el portal del CCN-CERT cuenta con una media de visitas de 50.000 páginas cada mes), que gozan de más seguridad, más confidencialidad y mayores recursos para hacer frente a los crecientes ataques que se puedan producir ★