ALBERTO SAIZ
SECRETARIO DE ESTADO DIRECTOR DEL CNI Y DIRECTOR DEL CCN

El reto de la seguridad en las Administraciones Públicas españolas

El Centro Criptológico Nacional (CCN), adscrito al Centro Nacional de Inteligencia (CNI), y su equipo de Respuesta a Incidentes (CCN-CERT), es el Organismo responsable de velar por la seguridad de las tecnologías de la información en la Administración Pública y formar a sus profesionales en este campo. En el presente artículo, Alberto Saiz, Secretario de Estado Director del CNI y Director del CCN desgrana alguna de las claves para comprender como se está trabajando desde el CCN-CERT para colaborar con todas las administraciones en la mejora de su seguridad.

Una de las características más destacadas del panorama nacional e internacional es, sin lugar a dudas, el desarrollo alcanzado por las Tecnologías de la Información y las Comunicaciones (TIC). La facilidad y la flexibilidad en la transmisión de información a través de diversos soportes; la generalización casi universal de su uso y el acceso global a las diversas herramientas y redes de comunicación son aspectos comunes en nuestras sociedades modernas que han abierto las puertas a nuevas formas de servir al ciudadano.

Por todo ello, prácticamente nadie cuestiona hoy en día el valor de estas nuevas tecnologías y las ventajas y posibilidades que ofrecen a la sociedad.

Sin embargo, el hecho de que gran parte de las actividades humanas sean cada vez más dependientes de las TIC

y la interconexión entre los sistemas y redes de todo el mundo, lleva aparejado una serie de riesgos y amenazas capaces de afectar seriamente al funcionamiento y al servicio que se presta a la ciudadanía.

La nota más preocupante es que estas amenazas, en un mundo globalizado como el actual, donde Internet se ha convertido en una herramienta de uso común y diario, pueden provenir desde cualquier parte del mundo, son cada vez más complejas y, desgraciadamente, más fáciles de llevar a cabo. Asimismo, su daño y la velocidad con la que se propagan se incrementan año tras año y no es previsible que mejoren en el futuro.

Ataques contra las redes o los sitios web de una Institución, el fraude online, el correo no deseado, la introducción de código dañino en los sistemas o el robo de información y datos sensibles son sólo algunos ejemplos de las amenazas que se ciernen sobre todos nosotros. No hay que olvidar que, incluso la mejor infraestructura de seguridad de la información no puede garantizar que una intrusión acabe por afectar a un equipo, incluidos, por supuesto, los de las administraciones públicas.

CCN-CERT, centro de alerta nacional

En esta tarea de garantizar la seguridad de las TIC en la Administración, a principios del año 2007, y tras dos años de intenso trabajo, el Centro Criptológico Nacional creó un nuevo servicio, el CCN-CERT, Equipo de Respuesta a Incidentes de Seguridad de la Información. Este CERT **(1)** gubernamental tiene como misión el convertirse en el centro de alerta nacional que coopere con todas las administraciones públicas (general, autonómica y local) y las ayude a responder de forma rápida y eficiente a los incidentes de seguridad que pudieran surgir y a afrontar las nuevas amenazas a las que hoy en día están expuestas.

Todo ello en un momento en el que, tal y como señala la Ley 11/2007, de 22 de junio, la Administración tiene que promover en beneficio de los ciudadanos el uso de las nuevas tecnologías y está obligada a transformarse en una administración electrónica, asegurando la "disponibilidad, el acceso, la integridad, la autenticidad, la confidencialidad y la conservación de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias" (Título Preliminar)

¿Y cómo se está trabajando desde el CCN-CERT para colaborar con todas las administraciones en la mejora de su seguridad?

A través de una amplia variedad de servicios, ampliados gradualmente, con los que prevenir los incidentes de seguridad o, llegado el caso, responder de forma rápida y eficiente ante cualquier ataque que puedan sufrir.

Para ello, y como principal herramienta, se cuenta con el portal *www.ccn-cert.cni.es*, desde donde se coordina »

> Nuestra política es mantener siempre la confidencialidad sobre cualquier información específica de la Administración solicitante de ayuda

FIGURA 1. Portal www.ccn-cert.cni.es

y da soporte a todos los responsables de seguridad, tanto con servicios de acceso público, como restringido.

Estos servicios pueden 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* (aquellos 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).

Entre los primeros, los servicios reactivos, se encuentra la gestión de incidentes (con especial atención a los reseñados en el cuadro adjunto, Figura 2), la información sobre vulnerabilidades, alertas y avisos de nuevas amenazas a los que están expuestos los sistemas de información, recopiladas de diversas fuentes de reconocido prestigio (incluidas las fuentes propias) y el análisis de código dañino remitido por las diferentes administraciones a través del portal o de una cuenta de correo creada a tal efecto

Nuestra política es mantener siempre la confidencialidad sobre cualquier información específica de la Administración solicitante de ayuda. En este sentido, hay que tener en cuenta que el Equipo recibe informes de incidentes de todas las partes del mundo que, en muchos casos tienen similares características o involucran a los mismos atacantes, por lo que, al centralizar la gestión, es mucho más rápida y eficaz su resolución.

En cuanto a los servicios proactivos, entre otros, ofrecemos *boletines de vulnerabilidades* e *informes restringidos*, actualización de firmas de código dañino, *auditorias y evaluaciones de seguridad* de los servicios web que así lo requieran (obligatorias en el caso de aquellos sistemas que manejan "Información Clasificada"), *desarrollo y evaluación de herramientas de seguridad*, como la herramienta de análisis de riesgos PILAR o las Series CCN-STIC (normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los Sistemas TIC en la Administración) y la detección *temprana de intrusiones*, lo que permite disminuir los tiempos de respuesta ante dichos problemas.

Por último, y dentro de los servicios de gestión, realizamos *análisis de riesgos*, adecuando la *Herramienta PILAR* a diferentes entornos (perfil de seguridad para sistemas clasificados, adaptación para cálculo del riesgo ante diferentes patrones de ataque y perfil de seguridad para Infraestructuras Críticas Nacionales o perfil de seguridad para la Administración) y contamos con una amplio programa de *formación y sensibilización* a través de los cursos STIC, ofrecidos a lo largo de todo el año a través del INAP y publicados en la parte restringida del portal. A estos cursos se añaden otros cursos complementarios, seminarios y jornadas de concienciación, encaminadas a formar y actualizar el conocimiento del personal de la Administración en materia de seguridad de la información. Así, desde el año 2006, hemos impartido cursos a más 1.200 funcionarios, procedentes de 110 organismos diferentes. Igualmente, »

Ataques contra las redes o los sitios web de una Institución, el fraude online, el correo no deseado, la introducción de código dañino en los sistemas o el robo de información y datos sensibles son sólo algunos ejemplos de las amenazas que se ciernen sobre todos nosotros

han tenido buena acogida las jornadas y seminarios de concienciación y sensibilización, así como las presentaciones del CCN-CERT realizadas por diversas autonomías (Madrid, Comunidad Valenciana, Aragón, Asturias, Cantabria o Castilla y León), a las que han asistido más de 700 responsables de seguridad de las distintas administraciones.

La labor desplegada por el equipo del CERT gubernamental español durante estos dos años de intenso trabajo ha sido muy bien acogida. Por de pronto, más de mil trescientos responsables TIC de toda la Administración pública española mantienen un contacto directo con el CCN-CERT a través de la parte restringida de su portal en Internet. Asimismo, existe una media de 50.000 visitas al portal. Esta receptividad hacia el trabajo del CCN-CERT nos confirma que estamos en el camino adecuado y nos da nuevas fuerzas para afrontar, junto con el resto de organismos, los nuevos retos que tenemos ante nosotros.

Coordinador de CERTs

En esta labor de fomentar y ayudar a toda la Administración en la seguridad de sus sistemas, el CCN-CERT ofrece información, formación y herramientas para que las distintas administraciones (sobre todo las autonómicas) puedan desarrollar sus propios CERTs, permitiendo al propio CCN-CERT actuar de catalizador y coordinador de CERTs gubernamentales. La voluntad del CCN-CERT es apoyar a todos ellos, colaborar en su formación (facilitando información, herramientas de seguridad...) y, llegado el caso, contribuir en la resolución de incidentes e, incluso, fomentar su participación en foros internacionales.

De hecho, el CCN-CERT firmó el pasado año un Convenio Marco de Colaboración con el CSIRT-CV, Centro de Seguridad de las TIC de la Comunitat Valenciana, primero de estas características constituido por una autonomía española, ha sido creado por la Conselleria de Justicia y Administraciones Públicas para hacer frente a estas mismas amenazas, no sólo en la AAPP sino también entre las empresas y los ciudadanos.

En virtud de dicho acuerdo se fijaron las bases de colaboración entre ambas instituciones para impulsar en España los aspectos de seguridad dentro del desarrollo de la Sociedad de la Información, mediante el intercambio de información, la formación especializada y el desarrollo de proyectos tecnológicos.

La apuesta por la creación de este tipo de equipos, en donde se centralicen las tareas de seguridad (independientemente de su definición como CERT, CSIRT, COS, etc.), se basa en el hecho de que un único centro no puede afrontar por sí sólo el número creciente de amenazas a los que hoy en día están expuestos los sistemas de información de un país o, en este caso, de toda la Administración pública. Así lo demuestra también la experiencia de otros países europeos como Alemania o Reino Unido, en los que el número de CERTs se eleva hasta los 19 y 17, respectivamente (incluidos equipos de organizaciones privadas). No obstante, es cierto que resulta imprescindible la cooperación entre los CERTs, no sólo a nivel estatal, sino también mundial.

Colaboración con instituciones estatales

Para el desarrollo de las funciones establecidas en el Real Decreto de su constitución (RD 421/2004), el

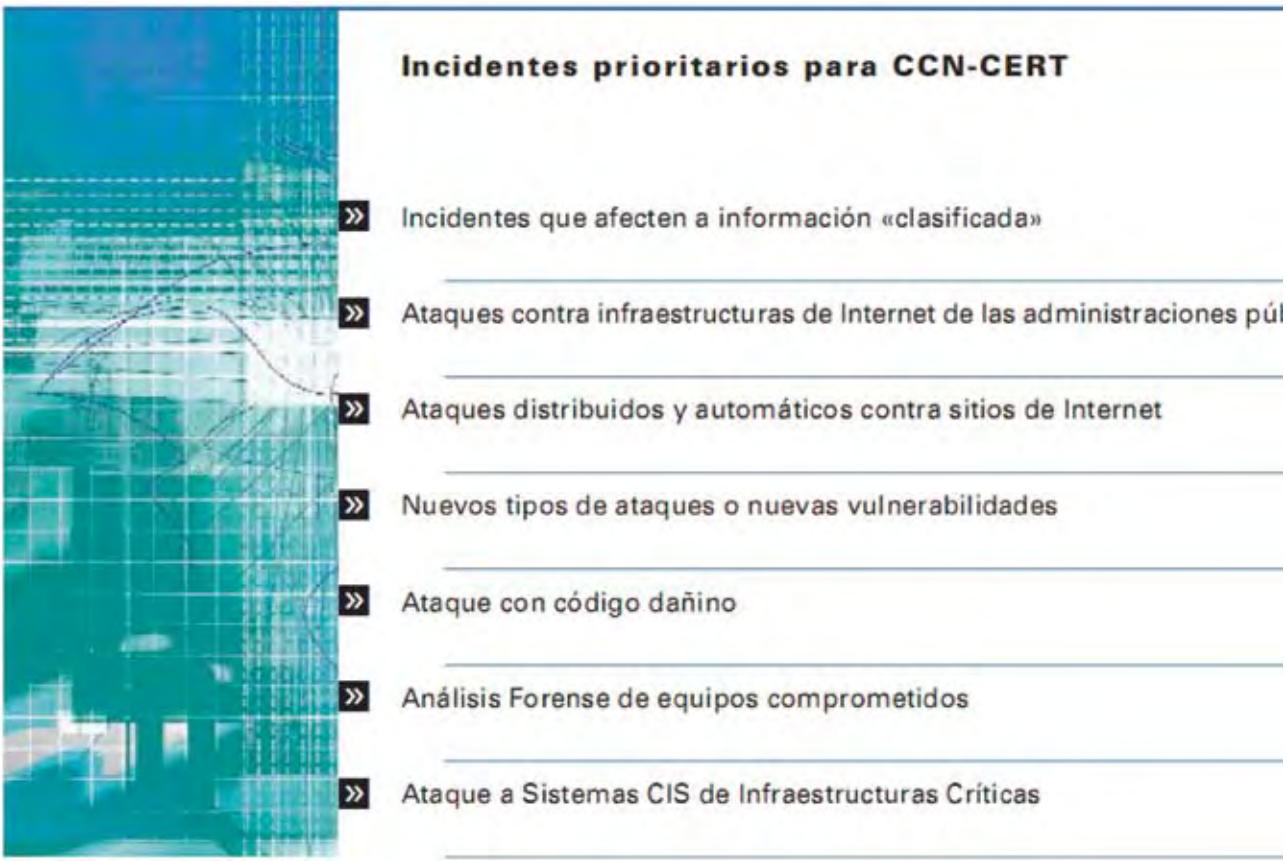

FIGURA 2. Incidentes prioritarios para el CCN-CERT

Centro Criptológico Nacional debe establecer la coordinación oportuna con las Comisiones nacionales a las que las leyes atribuyan responsabilidades en el ámbito de los sistemas de las Tecnologías de la Información y de las Comunicaciones. Esto implica mantener un contacto permanente con diversas instituciones y organismos implicados en la seguridad de la información.

Así, el CCN-CERT mantiene relación con otros CERTs, ISPs, empresas de hosting, registradores, etc. y forma parte del Grupo de CERTs españoles públicos y privados reconocidos (CSIRT.es) y del Foro ABUSES (equipos ABUSE de ISP españoles promovido por RedIRIS). Además, hemos venido firmando diversos acuerdos con distintos organismos con el fin de colaborar mutuamente.

Igualmente, prestamos especial atención a la protección de los sistemas de la información de las Infraestructuras Críticas (IC) y hemos venido apoyando al *Centro Nacional de Protección de Infraestructuras Críticas* (CNPIC), un organismo creado en 2007 para la prevención y gestión de incidentes relacionados con la seguridad de más de 3.500 infraestructuras críticas nacionales.

Uno de los casos recientes de establecimiento de acuerdos de colaboración por parte del CCN-CERT, es el suscrito con la *Federación Española de Municipios y Provincias* (FEMP), el pasado mes de diciembre, y que tiene por objeto impulsar la seguridad en el marco del desarrollo de la Sociedad de la Información, mediante el intercambio de información, la formación especializada y el desarrollo de proyectos tecnológicos.

Proyección internacional

Ante la proliferación de las amenazas cibernéticas (y la dificultad de detectar la procedencia del riesgo), los gobiernos de todo el mundo han ido adquiriendo una mayor conciencia sobre la necesidad de compartir objetivos, ideas e información sobre la seguridad de forma global. Y España no se ha mantenido al margen de esta tendencia.

Así, una importante parte del éxito del CCN-CERT radica en la colaboración »

FIGURA 3. Porcentaje de incidentes gestionados por el CCN-CERT en 2008

FIGURA 4. Sede del Centro Criptológico Nacional

con organismos europeos y mundiales, principalmente aquellos pertenecientes a la Unión Europea y a la OTAN. Este equipo, como CERT gubernamental español, está presente en los principales foros supranacionales en donde se comparten objetivos, ideas e información para abordar de forma conjunta cualquier posible amenaza.

Es miembro de pleno derecho del *Forum of Incident Response and Security Teams* (FIRST), principal organismo que aglutina a los CERTs de todo el mundo (alrededor de 200), está integrado en TERENA (*Trans-European Research and Education Networking Association*) y, recientemente, ha ingresado en el Grupo EGC (*European Government CERT*s), organización europea de CERTs gubernamentales en el que se incluyen los países nórdicos, Francia, Alemania, Hungría, Holanda y Reino Unido. Asimismo, pertenecemos al AntiPhishing WG y al Programa SCP de Microsoft.

A través de todas estas actividades, el CCN-CERT orienta sus esfuerzos, energías y recursos para continuar afrontando de manera eficaz los retos que plantea la Sociedad de la Información, contribuyendo así a la mejora de la seguridad de las tecnologías de la información en la Administración española, convencidos de que la seguridad de las tecnologías de la información y las comunicaciones es tan importante para la seguridad y el bienestar de los ciudadanos como lo es la protección de los propios ciudadanos, sus intereses y su sociedad.

(1) CERT: Computer Emergency Readiness/Response Team (marca registrada por CERT CC de la Universidad Carnegie Mellon de Estados Unidos)