Servicio de Respuesta a Incidentes de Seguridad para la Administración

EL CRECIMIENTO CONSTANTE DE LAS AMENAZAS Y VULNERABILIDADES SOBRE LOS SISTEMAS DE INFORMACIÓN, UN 55% EN LOS DOS ÚLTIMOS AÑOS, HACE IMPRESCINDIBLE LA CREACIÓN DE ESTE SERVICIO

CCN-CERT
Centro Criptológico Nacional

La sociedad española, tal y como recoge la exposición de motivos de la Ley 11/2002, de 6 de mayo, que regula las funciones del Centro Nacional de Inteligencia (CNI), demanda unos Servicios de Inteligencia eficaces, especializados y modernos, capaces de afrontar los nuevos retos del actual escenario nacional e internacional. Entre estos nuevos retos, sin lugar a dudas, se encuentran los denominados riesgos emergentes en donde la Seguridad de las Tecnologías de la Información y las Comunicaciones (STIC) y la protección de la información clasificada, ocupan un lugar destacado.

En este sentido, el Centro Criptológico Nacional (CCN), organismo público dependiente del CNI y cuya actividad está regulada a través del Real Decreto 421/2004, tiene, entre otras funciones, elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de las TIC en la Administración. De igual modo, el RD le asigna la formación del personal de la Administración especialista en el campo de la seguridad de las TIC, constitución del Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de aplicación a productos y sistemas de su ámbito; así como la coordinación, promoción, desarrollo, obtención, adquisición y utilización de la tecnología de seguridad de los Sistemas antes mencionados.

> El Centro Criptológico Nacional (CCN), organismo público dependiente del CNI

En este contexto se enmarca, precisamente, la reciente constitución del CCN-CERT; es decir, la Capacidad de Respuesta ante Incidentes de Seguridad de la Información para las Administraciones Públicas del Centro Criptológico Nacional (CCN-CERT).

El término CERT proviene de las siglas en inglés de *Computer Emergency Response Team* y viene a definir a una organización que estudia la seguridad de las redes y ordenadores para proporcionar servicios de respuesta ante incidentes a víctimas de ataques, publicar alertas relativas a amenazas y vulnerabilidades y para ofrecer información que ayude a mejorar la seguridad de estos sistemas. A estos servicios, y como valor añadido, suele unirse, bajo la denominación CSIRT *(Computer Security and Incident Response Team)* los servicios preventivos y de gestión de seguridad.

Objetivos

El CCN-CERT tiene como principal objetivo contribuir a la mejora del nivel de seguridad de los sistemas de información de las Administraciones Públicas de España. Para ello, su

misión es convertirse en el centro de alerta nacional que ayude a todas las AAPP (general, autonómica y local) a responder de forma rápida y eficiente a los incidentes de seguridad que pudieran surgir. Del mismo modo, el CCN-CERT se compromete a divulgar y asesorar a todas las Administraciones en la implantación de medidas tecnológicas que mitiguen el riesgo de sufrir cualquier ataque y puedan cumplir, de esta forma, con las elevadas exigencias de seguridad que hoy en día se requieren. Todo ello, en el convencimiento de que el desarrollo, la adquisición, conservación y utilización segura de las Tecnologías de la Información y las Comunicaciones (TIC) por parte de la Administración son imprescindibles para garantizar un funcionamiento eficaz al servicio del ciudadano y de los intereses nacionales.

Para contribuir a esta mejora del nivel de seguridad, el CCN-CERT ofrece sus servicios a todos los responsables TIC de las diferentes AAPP a través de tres grandes líneas de actuación:

- **Información sobre vulnerabilidades,** alertas y avisos de nuevas amenazas a los sistemas de información.
- **Investigación, formación y divulgación** de las mejores prácticas para la Seguridad de las Tecnologías de la Información y las Comunicaciones (STIC), con cursos de formación para el personal de las AAPP, desarrollo de las Series CCN-STIC (normas, instrucciones, guías y recomendaciones de configuración segura para diferentes tecnologías), desarrollo de herramientas de seguridad, auditorías o evaluaciones, detección de intrusiones en sistemas y divulgación de información.
- **Soporte ante incidentes y vulnerabilidades**, mediante servicios de apoyo técnico y coordinación.

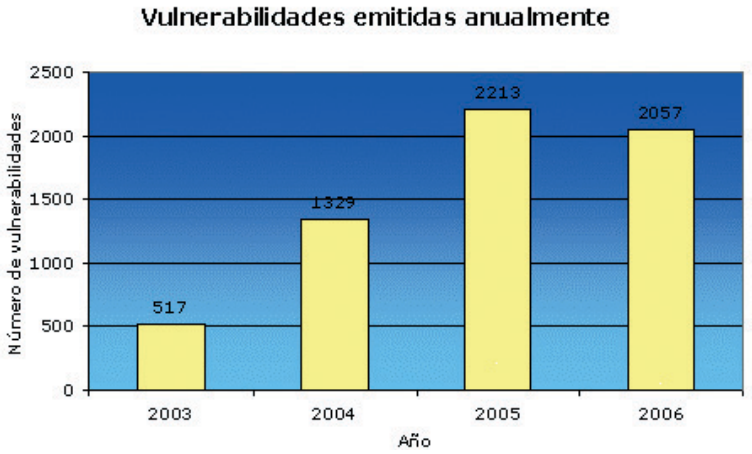
Para dar soporte a los servicios antes mencionados, el CCN-CERT cuenta con el apoyo de diversas instituciones y empresas, siendo TB-Security la contratista principal de la capacidad inicial.

Servicio imprescindible

La necesidad de este nuevo servicio queda patente al analizar las estadísticas de amenazas y vulnerabilidades registradas por el CCN-CERT. Éstas se incrementaron en un 55% en los dos últimos años. Así, de las 1.329 publicadas en 2004 (obviamente, no todas explotadas) se pasó a 2.057 en 2006, lo que representa un incremento del 54,7%.

Si bien es cierto que en 2006 se observa un leve descenso en el número de amenazas y/o vulnerabilidades registradas frente a 2005 (2.213), basta un repaso a la serie de datos de los últimos cuatro años para observar que el ritmo de crecimiento de las mismas que afectan a los Sistemas de Información ha sido prácticamente exponencial en este período de tiempo. De hecho, de estos intentos de ataques, un 20 % se materializaron.

La nota más preocupante es que estas amenazas son cada vez más complejas y difíciles de detectar. En este sentido, el Subdirector General Adjunto del CCN, Luis Jiménez, señala



que *"antes las técnicas de ataque estaban en manos de especialistas y ahora están pasando al gran público. Asimismo, el daño y la velocidad de los ataques se incrementan continuamente"*.

Dado el carácter de estas amenazas, se hace necesaria una formación del personal responsable de las TIC en todas las Organizaciones (incluidas, por supuesto, todas las Administraciones Públicas) para luchar contra la ingenuidad, la ignorancia de buenas prácticas y la falta de concienciación existente sobre la necesidad de preservar la seguridad de la información (STIC). Una seguridad que debe estar orientada a garantizar o mantener tres cualidades propias de esta última: disponibilidad, integridad y confidencialidad.

La Administración en su conjunto no puede ser ajena a este escenario y debe considerar el desarrollo, la adquisición, conservación y utilización segura de las TIC como algo imprescindible que garantice el funcionamiento eficaz al servicio del ciudadano y de los intereses nacionales. Sobre todo, teniendo en cuenta los nuevos retos a los que se enfrenta, procedentes de muy diversas fuentes: Servicios de Inteligencia, Grupos Organizados, Terroristas, *Hackers*, Grupos Criminales, Empleados deshonestos, etc.

Se hace imprescindible, por tanto, tomar conciencia de los riesgos a través de medidas a todos los niveles (legislativas, organizativas y técnicas) así como de la implementación de herramientas técnicas de seguridad (anti-virus, firewalls, software para autenticación de usuarios o para cifrado de la información) y del empleo de productos certificados, de inspecciones o auditorías de seguridad, etc.

Garantizar un funcionamiento eficaz al servicio del ciudadano y de los intereses nacionales

Del mismo modo, resulta esencial la gestión de incidentes a través de CERT dedicados a la implantación y gestión de medidas tecnológicas que prevengan, primero, y mitiguen, llegado el caso, el riesgo derivado de los ataques a los que están expuestos los sistemas de la comunidad a la que proporcionan el servicio.

La relación del CCN-CERT con el resto de la Administración será siempre de colaboración, y no se actuará nunca de forma jerárquica, salvo en el caso de información clasificada.

Incluso, desde el CCN se ofrecerá información, formación y herramientas para que la comunidad pueda desarrollar sus propios CERT, permitiendo al CCN-CERT actuar de catalizador y coordinador de CERTS gubernamental.

Portal www.ccn-cert.cni.es

Para una óptima coordinación, el CCN-CERT ha desarrollado un portal en Internet (www.ccn-cert.cni.es) con el que facilitar la comunicación con los responsables TIC de cada una de las Administraciones. A través de esta página web se ofrece información actualizada diariamente sobre amenazas, vulnerabilidades, guías de configuración, cursos de formación o formularios de comunicación de incidentes de seguridad.

De hecho, y dado el carácter crítico de algunos de los aspectos recogidos en el portal, existe una parte de acceso restringido que exige el registro previo de sus usuarios. Así, y una vez autorizada su alta, se puede realizar la descarga de documentos, herramientas de seguridad, metodologías o técnicas con las que contar ante un posible incidente.

Gracias a este registro, el CCN-CERT pretende conseguir una comunicación directa con su *comunidad* para poder actuar adecuada y rápidamente ante cualquier hipotético ataque.

Así pues, la creación por parte del Centro Criptológico Nacional del Equipo de Respuesta a Incidentes de Seguridad de la Información (CCN-CERT) viene a cubrir la necesidad y a contribuir a la mejora del nivel de seguridad de los sistemas de información en las Administraciones Públicas Españolas.