



El Informe se inicia con una Carta del Secretario de Estado Director del CNI y Director del CCN, Félix Sanz Roldán

El Centro Criptológico Nacional presenta su Informe de Actividades 2008-2010

- **El Informe recoge la apuesta del CCN por la implantación del Esquema Nacional de Seguridad (ENS), la potenciación de las capacidades de alerta temprana y el fortalecimiento de la gestión y respuesta a incidentes (a través del CCN-CERT), y la utilización de productos y sistemas seguros y certificados de acuerdo a las normas y estándares internacionales (OC).**
- **Entre otra información, el documento recoge todos los Cursos STIC y on-line desarrollados por el CCN, junto con las Guías CCN-STIC, los productos de cifra desarrollados y certificados, así como los nuevos servicios ofrecidos por el propio Centro.**

Madrid, 23 de mayo de 2011. El Centro Criptológico Nacional (CCN), organismo adscrito al Centro Nacional de Inteligencia, responsable de coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, así como garantizar la seguridad de las TIC en ese ámbito, acaba de publicar su memoria de actividades de los últimos tres años.

Este documento recoge el trabajo y el esfuerzo realizado por este Organismo entre los años 2008 y 2010, actividad que ha ido adecuándose a los nuevos riesgos emergentes del ciberespacio ante los que se ha potenciado las acciones no sólo defensivas, sino primordialmente preventivas, correctivas y de contención, sabedores de la importancia de adoptar medidas que permitan reaccionar ante el constante incremento de incidentes de seguridad y, sobre todo, que prevengan su propagación y atajen su impacto de la forma más rápida y eficaz posible.

Así, tal y como señala el **Secretario de Estado Director del CNI y Director del CCN**, Félix Sanz Roldán, en el prólogo del Informe, el CCN ha apostado por *“colaborar con todas las administraciones en la implantación del Esquema Nacional de Seguridad (ENS), la potenciación de las capacidades de alerta temprana, el fortalecimiento de la gestión y respuesta a incidentes (a través del CCN-CERT) y en la utilización de productos y sistemas seguros y certificados de acuerdo a las normas y estándares de mayor reconocimiento internacional”*.

Formación y Guías CCN-STIC

Dentro del ámbito de actuación y funciones del CCN recogidas en este Informe, se señala su importante papel de formar al personal de la Administración, así como elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de sus sistemas de las TIC. En este sentido, cabe resaltar que más de 1.300 alumnos han pasado por los cursos presenciales ofertados por el Centro, a los que habría que sumar los cerca de 900 que han accedido a la formación on-line, a través del portal del CCN-CERT (www.ccn-cert.cni.es).

Por su parte, y en el capítulo de Guías CCN-STIC, el Informe resalta las 153 guías que ha elaborado, a las que hay que sumar 21 que están pendientes de publicar (65 de ellas nuevas o actualizadas).

Organismos y capacidades

Uno de los capítulos del Informe está centrado en el CCN-CERT, la Capacidad de Respuesta a Incidentes de Seguridad de la Información, del Centro Criptológico Nacional, creado a finales del año 2006 como CERT gubernamental español y cuyas funciones quedan recogidas en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad.

Junto a sus servicios tradicionales de Gestión de Incidentes, elaboración de alertas, avisos y vulnerabilidades o auditorías web a distintos organismos de la Administración, el Informe recoge los nuevos servicios ofrecidos por el CCN-CERT. El Sistema de Alerta Temprana (SAT), tanto de la Red SARA como de Internet, para la detección rápida de incidentes y anomalías es el más destacado. En este sentido, desde su puesta en marcha en 2008, en la red SARA se han desplegado 30 sondas de recolección en las áreas de conexión y se han integrado un gran número de fuentes de datos. De igual modo, el SAT de Internet tenía desplegadas hasta el 30 de marzo de 2011, un total de 14 sondas, que dan cobertura a varios Ministerios y Entidades del Estado (a finales de este año se prevé tener instaladas de 25 a 30 sondas). El número de incidentes recogidos por este sistema no ha parado de crecer en los últimos años (los más detectados son los relacionados con la violación de políticas de seguridad, escaneos, código dañino, spyware, troyanos o exploits).

Por último, el informe del CCN resalta el papel que cumple el Organismo de Certificación (OC) del Centro Criptológico Nacional, que viene operando con diversas normas de evaluación de la seguridad de las TIC, entre ellas la de mayor reconocimiento internacional, la denominada Common Criteria (ISO-15408).

Este informe expresa que mientras el CCRA limita el reconocimiento mutuo a niveles de evaluación intermedios (hasta EAL4), en Europa se desarrolló y firmó el llamado SOGIS MRA que busca el reconocimiento también para los más altos niveles de seguridad posibles (hasta EAL7). En él también se recoge una explicación del procedimiento de certificación de productos, y ofrece una completa relación de productos certificados entre 2008 y 2010.

Este documento concluye con información sobre la actividad del CCN en el ámbito nacional e internacional, que abarca su participación en organismos y foros tanto nacionales como internacionales, y con ocho páginas que ilustran la cronología de la Institución entre 2008 y 2010.

MÁS INFORMACIÓN

comunicacion@tb-security.com
TB·Security
(+34) 91 301 34 95

Centro Criptológico Nacional
Avda. del Padre Huidobro, Km. 8,500
28023 Madrid
www.ccn-cert.cni.es
info@ccn-cert.cni.es