



El Real Decreto 421/2004, de 12 de marzo, vino a regular y definir el ámbito y funciones del CCN, adscrito al Centro Nacional de Inteligencia, CNI

Centro Criptológico Nacional, diez años trabajando por la ciberseguridad del país

- La intensidad y sofisticación de los ciberataques detectados diariamente por este organismo (7.263 en 2013), tanto a las Administraciones Públicas como a las empresas y organizaciones de interés estratégico para el país, así como las graves repercusiones de los mismos, hacen cada día más necesaria su actuación.
- El Secretario de Estado director del CNI, Félix Sanz, ejerce este año la presidencia del Consejo de Ciberseguridad Nacional, tal y como figura en la recientemente aprobada Estrategia de Ciberseguridad Nacional, que marca la necesidad de fortalecer las capacidades de prevención, defensa, detección, análisis, investigación, recuperación y respuesta a los ciberataques, tareas todas ellas realizadas por el CCN.

Madrid, 11 de marzo de 2014.- El 19 de marzo de 2002, se publicaba en el Boletín Oficial del Estado, el **Real Decreto 421/2004**, de 12 de marzo, por el que se regula el **Centro Criptológico Nacional (CCN)**, adscrito al **Centro Nacional de Inteligencia (CNI)**. Este RD venía a regular y definir el ámbito y funciones de este Organismo, cuya actividad venía recogida en la **Ley 11/2002**, de 6 de mayo, reguladora del **CNI**, y que venía ya operando como un departamento del Centro desde principios de los años 80 (principalmente

"En 2013, el CERT Gubernamental español gestionó 7.263 ciberincidentes (un 82% más que el ejercicio anterior) y notificó más de 11.370 vulnerabilidades"

proporcionando medios o procedimientos de cifra, para garantizar la seguridad de la información clasificada del país.)

El RD citado, señalaba entre otras funciones del CCN, actuar contra el ciberespionaje, neutralizando las actividades de inteligencia y mejorando la

11 de marzo de 2014

www.ccn.cni.es
www.ccn-cert.cni.es
www.oc.ccn.cni.es



seguridad de los sistemas de información del país, protegiendo su patrimonio tecnológico.

Desde su creación, el CCN ha ido adecuándose y, en la medida de lo posible, adelantándose a una realidad cambiante, en donde las amenazas se incrementan día a día favorecidas por la rentabilidad que se obtiene ya sea económica, política o de otro tipo; la facilidad y el bajo coste en el empleo de las herramientas utilizadas, así como el reducido riesgo para el atacante, que lo puede hacer de forma anónima y desde cualquier lugar del mundo, afectando transversalmente tanto al sector público, como al privado o a los ciudadanos. Ciberdelincuentes, crimen organizado, terroristas, hacktivistas o los propios estados, son capaces de explotar las vulnerabilidades tecnológicas con el objeto de recabar información, sustraer activos de gran valor y amenazar servicios básicos para el normal funcionamiento de nuestro país.

Funciones asignadas al CCN

Elaborar y difundir **normas, instrucciones, guías** y recomendaciones (cuenta con más de 200 documentos en este sentido); **formar** al personal de la Administración; constituir el **Organismo de Certificación** de la seguridad de los productos y sistemas utilizados en su ámbito; **valorar y acreditar** la capacidad de los productos de cifra y de los sistemas que incluyan medios de cifra, para procesar, almacenar o transmitir información de forma segura y velar por el cumplimiento de la normativa relativa a la **protección de la información clasificada**, son algunas de las funciones asignadas al CCN. Junto a ellas, el establecimiento de las necesarias relaciones y firma de acuerdos pertinentes con organizaciones similares de otros países y, a través del **CCN-CERT**, contribuir a la mejora de la ciberseguridad en España, con responsabilidad en los ciberataques sobre **sistemas clasificados** y sobre sistemas de la **Administración** y de **empresas y organizaciones de interés estratégico nacional**. De hecho, en el año 2013, el CERT Gubernamental español gestionó 7.263 ciberincidentes (un 82% más que el ejercicio anterior) y notificó más de 11.370 vulnerabilidades de hardware y software.

MÁS INFORMACIÓN

Centro Criptológico Nacional

Argenta, 20. 28023 Madrid

www.ccn-cert.cni.es





eventos@ccn-cert.cni.es

11 de marzo de 2014

www.ccn.cni.es
www.ccn-cert.cni.es
www.oc.ccn.cni.es



 CENTRO CRIPTOLÓGICO NACIONAL	Normas, instrucciones y Guías	<ul style="list-style-type: none"> • Más de 200 Guías CCN-STIC • Guías Herramienta PILAR de gestión de riesgos
	Formación	<ul style="list-style-type: none"> • Presencial (18 cursos STIC) • On-line (www.ccn-cert.cni.es)
	Esquema Nacional de Seguridad	<ul style="list-style-type: none"> • Seguimiento del cumplimiento y adecuación • Documentación, guías y formación
	Investigación y desarrollo de productos	<ul style="list-style-type: none"> • Sistemas de cifrado • Pasarelas seguras


 CENTRO CRIPTOLÓGICO NACIONAL	Gestión de Incidentes	<ul style="list-style-type: none"> • 7.2630 ciberataques a sistemas de la AAPP y empresas estratégicas.
	Sistema de Alerta Temprana (SAT) en Internet	<ul style="list-style-type: none"> • 55 organismos adscritos (todos los Ministerios incluidos) • Prevención, detección y reducción de impacto
	Sistema de Alerta Temprana (SAT) en la red SARA	<ul style="list-style-type: none"> • En colaboración con el M^o de Hacienda y AAPP . • 49 áreas de conexión (todos los Ministerios)
	Sistemas de Información, alertas, avisos y vulnerabilidades	<ul style="list-style-type: none"> • 11.370 vulnerabilidades notificadas en 2013 • 50 Informes de amenazas, actualidad y código dañino en 2013
	CARMEN	<ul style="list-style-type: none"> • Herramienta propia desarrollada para detectar APT en curso
	LUCIA	<ul style="list-style-type: none"> • Herramienta propia para la mejor gestión y coordinación de incidentes
	INES	<ul style="list-style-type: none"> • Herramienta para adecuación del Informe del Estado de Seguridad (ENS)

11 de marzo de 2014

www.ccn.cni.es
www.ccn-cert.cni.es
www.oc.ccn.cni.es



ORGANISMO DE CERTIFICACIÓN (OC)



Certificación funcional de productos y sistemas	<ul style="list-style-type: none"> • Normas Common Criteria • Acuerdo internacional CCRA
Certificación Criptológica	<ul style="list-style-type: none"> • Productos que protegen información clasificada
Certificación TEMPEST	<ul style="list-style-type: none"> • Equipos, sistemas e instalaciones, fijas o móviles, donde se genera información nacional clasificada

11 de marzo de 2014

www.ccn.cni.es
www.ccn-cert.cni.es
www.oc.ccn.cni.es

