El CCN-CERT es competente en la gestión de ciberincidentes que afecten a sistemas clasificados, de las AAPP y de empresas de interés estratégico

Gestión de Ciberincidentes, nueva Guía del CCN-CERT

- **Una tipificación clara de los distintos ciberincidentes, recomendaciones para determinar su peligrosidad, las pautas para ofrecer la respuesta más adecuada en cada caso y una metodología para notificar al CCN-CERT los ataques en función del momento y su tipología, principales aspectos de la Guía CCN-STIC 817, descargable desde la parte pública del portal www.ccn-cert.cni.es**

- **El propósito de esta Guía es ayudar a las entidades públicas del ámbito de aplicación del ENS al establecimiento de las capacidades de respuesta a ciberincidentes y su adecuado tratamiento, eficaz y eficiente para minimizar los daños de un ataque.**

Madrid, 16 de marzo de 2015.- Gestionar adecuadamente un ciberincidente constituye una actividad compleja, que requiere de metodologías para recopilar y analizar datos y eventos, realizar un seguimiento; o tener claro el grado de peligrosidad del mismo y su priorización (en función del tipo de amenaza, origen, perfil de usuario afectado, número o tipología de sistemas afectados, impacto…). Todo ello con el fin de minimizar la pérdida o exfiltración de información o la interrupción de los servicios que puede darse después de sufrir un ataque. Por este motivo, y en virtud de lo dispuesto en el **Esquema Nacional de Seguridad**, el **CCN-CERT,** del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI, ha hecho pública su **Guía CCN-STIC 817** sobre **Gestión de Ciberincidentes**. Con ella, el CERT Gubernamental Nacional pretende ayudar a las entidades públicas del ámbito de aplicación del ENS al establecimiento de las **capacidades de respuesta a ciberincidentes** y su adecuado tratamiento, eficaz y eficiente.

La Respuesta dependerá, entre otros, del tipo de amenaza, su origen, el perfil y el número de sistemas afectados, el impacto del incidente y los requerimientos legales y regulatorios

La Guía recoge una clasificación con **nueve tipos de ciberincidentes** distintos y 36 subcategorías, entre las que se incluyen algunos de los ataques y vulnerabilidades más detectados como Troyanos, Spyware, Cross-Site Scripting (XSS), Inyección SQL, DDoS, Exfiltración de Información, Phishing o Ransomware. Además, y en función de distintos parámetros (como la amenaza subyacente, el vector de ataque o las características potenciales del ciberincidente), se recoge una tabla para determinar la **peligrosidad** potencial y, de esta forma, poder asignar prioridades y recursos.

16 de marzo de 2015

Intercambio de información y Comunicación de Ciberincidentes

Además de la preceptiva notificación de los ciberincidentes al CCN-CERT, en ocasiones los organismos públicos necesitarán comunicarse con terceros (Fuerzas y Cuerpos de Seguridad y medios de comunicación social, específicamente). El resto de las comunicaciones con otros actores (proveedores de Internet, equipos CSIRT, vendedores de software, etc.) se desarrollarán a través del CCN-CERT, en su función de Nodo de Intercambio de Información de Ciberincidentes en los Sistema de Información de las AA.PP. (*véase Figura 1*).

La Guía recoge también la gestión y coordinación de incidentes para los organismos del sector público español, a través del Sistema de **Alerta Temprana de Red SARA (SAT-SARA)** y del **Sistema de Alerta Temprana de Internet (SAT-INET)**, así como su nueva herramienta, **LUCIA,** desarrollada para la Gestión de Ciberincidentes y puesta a disposición de los organismos del ámbito de aplicación del ENS.

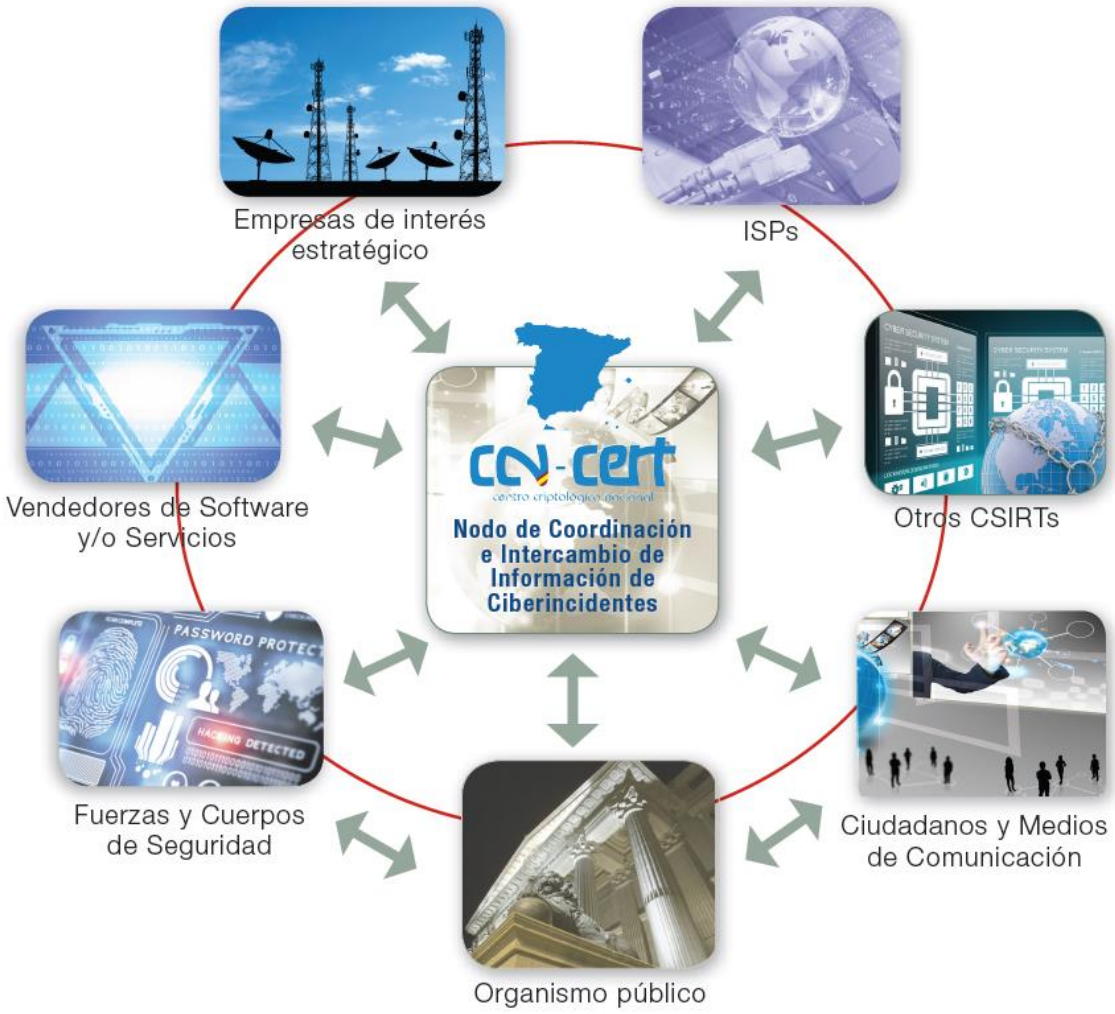

Figura 1. Comunicación a Terceros de Información de Ciberincidentes

Sobre CCN-CERT, CERT Gubernamental Nacional

El CCN-CERT (www.ccn-cert.cni.es) es la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN (www.ccn.cni.es). Este servicio se creó en el año 2006 como el **CERT Gubernamental Nacional** español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del ENS.

De acuerdo a todas ellas, es competencia del CCN-CERT la gestión de ciberincidentes que afecten a **sistemas clasificados**, a sistemas de las **Administraciones Públicas** y de **empresas y organizaciones de interés estratégico** para el país. Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas.

MÁS INFORMACIÓN

CCN-CERT
eventos@ccn-cert.cni.es
+34 670 29 20 05

Síguenos en
www.ccn-cert.cni.es/

@CcnCert

http://youtu.be/5XxS9mZZfKs