## SERVICIOS CCN-CERT

**GESTIÓN DE INCIDENTES**
Cualquier organismo público que sufra un ataque en sus sistemas puede solicitar la colaboración del CCN-CERT para su resolución.

**INFORMACIÓN, ALERTAS, AVISOS Y VULNERABILIDADES**
El CCN-CERT ofrece diferente información a toda su Comunidad, entre la que destacan las vulnerabilidades, alertas y avisos de nuevas amenazas a los sistemas de información, basadas tanto en el trabajo de sus propios analistas como en las contribuciones procedentes de muy diversas fuentes de reconocido prestigio, nacionales e internacionales.

**AUDITORÍAS WEB**
El equipo CCN-CERT lleva a cabo auditorías a páginas web de distintos organismos de las administraciones públicas en busca de posibles vulnerabilidades críticas, con el fin de establecer las pautas adecuadas para reducirlas o eliminarlas.

**SISTEMA DE ALERTA TEMPRANA**
Sistema desarrollado para la detección rápida de incidentes y anomalías dentro del ámbito de la Administración, que permite realizar acciones preventivas, correctivas y de contención.

**SISTEMA MULTIANTIVIRUS / ANÁLISIS DE CÓDIGO DAÑINO**
El Sistema Multiantivirus (MAV) permite analizar todo tipo de código, haciendo uso de múltiples motores antivirus, actualizados en tiempo real.

## PATROCINADORES

PLATINUM

tb·security

GOLD

autek · hp · Microsoft

SILVER

alienvault · Check Point · Ingenia · Isdefe · S21sec · SafeNet · SIC · SOURCEfire · Telefónica · telindus

## LUGAR DE CELEBRACIÓN

Las V Jornadas STIC CCN-CERT se celebrarán en el Aula Magna del Centro Superior de Estudios de la Defensa Nacional, CESEDEN, situado en el Paseo de la Castellana nº 61 de Madrid.

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

# V JORNADAS STIC CCN-CERT

## LA CIBERSEGURIDAD: UN RETO PARA LAS ADMINISTRACIONES PÚBLICAS

13 Y 14 DE DICIEMBRE 2011

CCN-CERT

GOBIERNO DE ESPAÑA · MINISTERIO DE DEFENSA

CCN

# PROGRAMA

## Martes 13 de diciembre de 2011

| | | |
|---|---|---|
| **Módulo 1** | **Gestión de Incidentes (sólo Administración Pública)** | |
| 09.15-09.40h | Gestión de incidentes CCN-CERT | (CCN) |
| 09.40-10.00h | APT* en las Administraciones Públicas | (CCN) |
| 10.00-10.30h | Persistencia APT: Ocultación en las comunicaciones | (Emiliano Martínez - Hispasec) |
| 10.30.11.00h | Vulnerabilidades en aplicaciones web basadas en el DNIe en las AAPP | (Raúl Siles - Taddong) |
| 11.00-11.30h | Nuevos retos en detección de APT | (CCN) |
| 11.30-12.00h | Pausa - Café | |
| **Módulo 2** | **Gestión de Incidentes** | |
| 12.00-12.20h | Persistencia APT en los sistemas de la organización | (Óscar Rivillo) |
| 12.20-12.45h | Ataque a iPhone | (Alejandro Soler - TB-Security) |
| 12.45-13.10h | Estrategias de monitorización del uso de Internet para alerta temprana | (Antonio Villalón - S2 Grupo) |
| 13.15-14.30h | Mesa redonda: Panorama en la gestión de incidentes en las AAPP<br>Modera: José de la Peña (Revista SIC)<br>Tema: “Necesidad en la coordinación de gestión de incidentes" | (Andalucía-CERT / CCN-CERT<br>CESICAT / CSIRT-cv<br>INTECO-CERT / IRIS-CERT) |

** Advanced Persistent Threat - Amenaza Persistente Avanzada*

## Miércoles 14 de diciembre de 2011

| | | |
|---|---|---|
| **Módulo 1** | **Implantación del ENS** | |
| 09.05-09.30h | Retos en la implantación del ENS | (M.Ángel Amutio - MPTAP) |
| 09.30-09.45h | Novedades CCN-CERT | (CCN) |
| 09.45-10.10h | Métricas en el ENS | (José A. Mañas) |
| 10.10-10.35h | Cloud Computing y el ENS | (Ramsés Gallego - Quest Software) |
| 10.35-11.00h | El DNIe es seguro pero… ¿se usa de forma segura? | (Raúl Siles - Taddong) |
| 11.00-11.30h | El ENS y la seguridad en el intercambio de información | (CCN) |
| 11.30-12.00h | Pausa - Café | |
| **Módulo 2** | **Infraestructuras Críticas** | |
| 12.00-12.15h | Actualización sobre Infraestructuras Críticas | (M.Ángel Abad - CNPIC) |
| 12.15-12.40h | Ataque a protocolos de comunicaciones en Infraestructuras Críticas | (Leonardo Nve - S21Sec) |
| 12.40-13.05h | Lecciones aprendidas tras un ataque DDoS | (David Barroso / Raúl Bretón - Telefónica) |
| 13.05-13.30h | Ataque de una arquitectura SCADA para boicotear un proceso industrial | (ISDEFE) |
| 13.30-14.00h | Vulnerabilidades SCADA, un problema ¿con solución? | (CCN) |
| 14.00-14.30h | DNS Distribución de malware y compromiso de información | (F. Gómez / Carlos Díaz - Telefónica) |

## V JORNADAS STIC CCN-CERT

Con el desarrollo y uso masivo por todos los ámbitos de la sociedad de las Tecnologías de la Información y las Comunicaciones (TIC), se ha creado un nuevo espacio, el ciberespacio, donde no hay barreras de distancia y tiempo y donde las fronteras nacionales han quedado diluidas. Su defensa y protección, es decir, la ciberseguridad, ha pasado a considerarse un eje fundamental de nuestra sociedad y nuestro sistema económico. Y es que, el ciberespacio y las redes de información y comunicación son, al tiempo que una fuente constante de nuevas posibilidades (entre otras, un número cada vez mayor de servicios ofrecidos a todos los ciudadanos por las Administraciones Públicas), un objetivo creciente de ataques ilícitos de todo tipo.

La actividad del CCN ha ido adecuándose a estos nuevos riesgos, potenciando las acciones no sólo defensivas, sino primordialmente preventivas, correctivas y de contención. Sabedores de la importancia de adoptar medidas que sean capaces de reaccionar ante el constante incremento de incidentes y, sobre todo, que prevengan su propagación y atajen su impacto de la forma más rápida y eficaz posible. Así, y ante estas amenazas, se ha apostado por colaborar con todas las administraciones en la implantación del ENS (cuyo primer plazo de adecuación concluyó el 29 de enero de este 2011), en la potenciación de las capacidades de alerta temprana, en el fortalecimiento de la gestión y respuesta a incidentes y en la utilización de productos y sistemas seguros y certificados de acuerdo a las normas y estándares de mayor reconocimiento internacional.

Las Jornadas STIC CCN-CERT, que cumplen su quinta edición se han convertido en una cita ineludible del personal de la Administración para la puesta en común de conocimientos, el análisis de las amenazas y el estudio de las soluciones y tendencias con las que hacer frente a estos ciberataques.