

Madrid, 10 y 11 de diciembre 2013

Auditorio

Museo de la Fábrica Nacional de Moneda y Timbre  
Real Casa de la Moneda

Platinum

**Deloitte.**



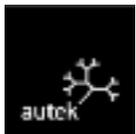
Gold



Entelgy



Silver



Organiza

[www.ccn.cni.es](http://www.ccn.cni.es)  
[www.ccn-cert.cni.es](http://www.ccn-cert.cni.es)  
[www.oc.ccn.cni.es](http://www.oc.ccn.cni.es)



Con la colaboración especial de la  
FNMT - RCM

[www.fnmt.es](http://www.fnmt.es)

La VII  
ciberseguridad,  
un factor  
estratégico  
nacional  
JORNADAS  
STIC  
CCN-CERT

<b>07:45 – 09:00 h</b>	Recepción de asistentes
<b>09:00 – 09:15 h</b>	Inauguración oficial a cargo del SED CNI
<b>09:15 – 11:10 h</b>	<b>PRIMER MÓDULO: Gestión de incidentes APT</b>
<b>09:15 – 09:40 h</b>	Novedades CCN-CERT. Gestión incidentes. Proyecto LUCIA (CCN)
<b>09:45 – 10:10 h</b>	Ataques dirigidos contra la Administración (CCN)
<b>10:15 – 10:40 h</b>	Ingeniería inversa a un APT (José M. Migoya y Francisco Oca, Innotec)
<b>10:45 – 11:10 h</b>	Campañas APT. ¿Quién nos ataca? (Vicente Díaz, Kaspersky)
<b>11:15 – 11:40 h</b>	Pausa café
<b>11:40 – 14:15 h</b>	<b>SEGUNDO MÓDULO: Ponencias tecnológicas</b>
<b>11:40 – 12:05 h</b>	Malware, evadiendo al vigilante (Javier Rascón, Hispasec)
<b>12:10 – 12:35 h</b>	Vectores de ataque: <i>Fake Access Point</i> - Demo (José Daniel Martínez, Deloitte)
<b>12:40 – 13:05 h</b>	Mecanismos de Protección Propios de Windows: ¿Estamos realmente protegidos? (Ricardo Rodríguez, UPM)
<b>13:10 – 13:35 h</b>	Anomalías HTTP (Antonio Villalón, S2Grupo)
<b>13:40 – 14:10 h</b>	Malware en GooglePlay (David Barroso, Eleven Paths)
<b>14:15 h</b>	Cierre de la sesión de mañana
<b>14:15 – 16:00 h</b>	Vino español – Entrega diplomas patrocinadores

**Los talleres se desarrollarán de 16 a 18 h.**

<b>Taller 1.</b> Destripando un troyano con objetivo "EL IOC". <i>Rafael Estevan, Incita Security</i>	Sala del Consejo (FNMT)
<b>Taller 2.</b> Análisis forense: ejemplos prácticos para responder ante incidentes en su organización. <i>Juan Antonio Calles, Flu-project</i>	Sala de Audición (FNMT)
<b>Taller 3.</b> Desconectando el malware ¿Es posible trabajar en una red aislada? <i>Miguel Ángel Martín y Manuel Sanz, Autek</i>	Auditorio FNMT

<b>08:30 – 09:00 h</b>	Recepción de asistentes
<b>09:00 – 09:05 h</b>	Bienvenida. Resumen de los módulos (S/G CCN)
<b>09:05 – 10:50 h</b>	<b>PRIMER MÓDULO: Implantación del ENS</b>
<b>09:05 – 09:30 h</b>	Modificación RD 3/2010 (Miguel Ángel Amutio, SEAP-MINHAP)
<b>09:35 – 09:55 h</b>	Evolución de la implantación del ENS (CCN y José Antonio Mañas, UPM)
<b>10:00 – 10:20 h</b>	Esquema de Certificación de Personas (CCN y Óscar Pastor, Isdefe)
<b>10:25 – 10:50 h</b>	Problemas del almacenamiento seguro (u otros usos) en nubes públicas y privadas (Jorge Dávila, UPM)
<b>10:55 – 11:20 h</b>	Pausa café
<b>11:20 – 14:40 h</b>	<b>SEGUNDO MÓDULO: Estrategia de Ciberseguridad</b>
<b>11:20 – 11:35 h</b>	Estrategia de Ciberseguridad Nacional (Joaquín Castellón, DSN)
<b>11:40 – 11:55 h</b>	Mando Conjunto de Ciberdefensa. Punto de situación (Cte. Salvador Llopis, MCCD)
<b>12:00 – 13:15 h</b>	Mesa redonda: Ciberseguridad Pública y Privada: Colaboración, Solapamiento y Competencia. Modera: José de la Peña, Revista SIC. Intervienen: Telefónica (Manuel Carpio), S21sec (J. Roberto Martín), MINETUR-SETSI (Juan Corro), DSN (Joaquín Castellón), CCN (Luis Jiménez), MCCD (Cte. Salvador Llopis), MINT-CNPI (Fernando Sánchez)
<b>13:20 – 13:45 h</b>	Plataforma de mensajería y riesgos asociados: caso WhatsApp (Jaime Sánchez, Seguridad Ofensiva)
<b>13:50 – 14:35 h</b>	Vulnerabilidades Wi-Fi de dispositivos móviles en redes empresariales 802.1x/EAP (Raúl Siles, DinoSec)
<b>14:40 h</b>	Clausura VII Jornadas STIC CCN-CERT