VIII JORNADAS STIC CCN-CERT

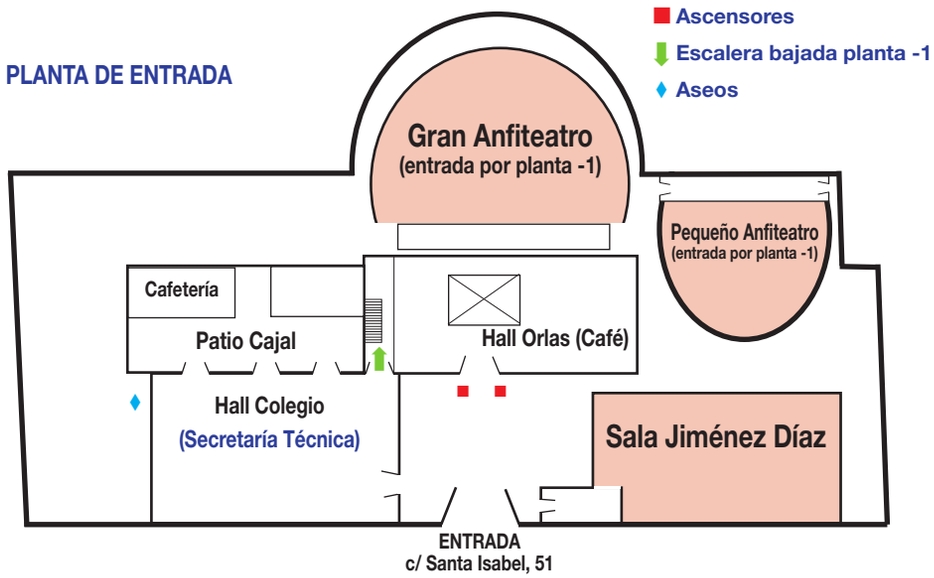
Lugar: **ILUSTRE COLEGIO OFICIAL DE MÉDICOS DE MADRID**

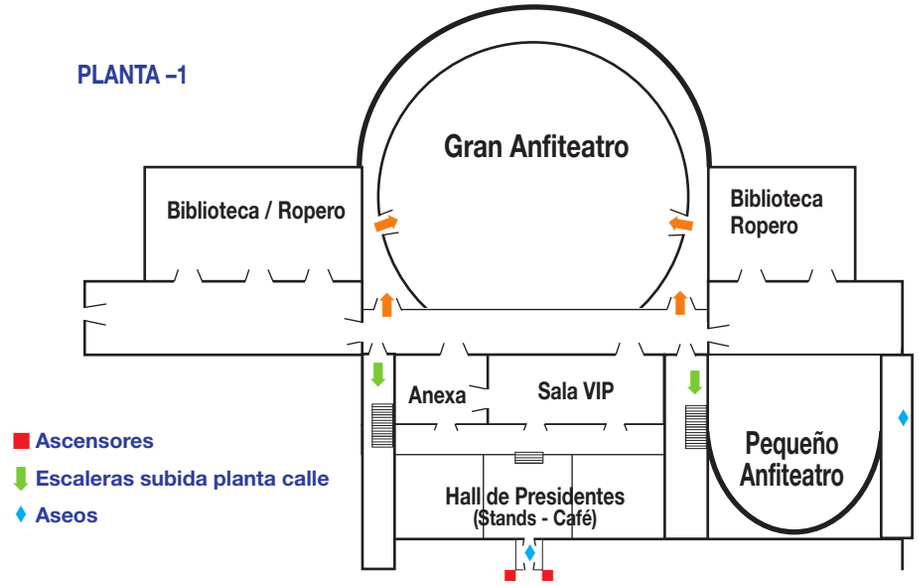
la defensa del patrimonio tecnológico frente a los ciberataques

Madrid 10/11 diciembre 2014

CCN-CERT
centro criptológico nacional

VIII JORNADAS STIC CCN-CERT





10 DE DICIEMBRE

07.45 – 09.00 ..... Recogida de acreditaciones *(Hall Colegio)*

09.00 – 09.25 ..... Inauguración

09.30 – 10.55 ..... Sesión plenaria *(Gran Anfiteatro)*

11.00 – 11.45 ..... Café y entrega de Diplomas a Patrocinadores

11.45 – 14.15 ..... Módulos 1, 2 y 3

14.15 – 16.00 ..... Vino español *(Hall Presidentes y Hall Orlas)*

16.00 – 18.00 ..... Talleres 1, 2 y 3

11 DE DICIEMBRE

08.00 – 09.00 ..... Recogida de acreditaciones *(Hall Colegio)*

09.00 – 11.15 ..... Módulos 1, 2 y 3

11.15 – 12.00 ..... Café

12.00 – 14.25 ..... Sesión plenaria *(Gran Anfiteatro)*

14.30 – 14.45 ..... Clausura

#8JornadasCCN_CERT

www.ccn-cert.cni.es

LinkedIn es.linkedin.com/in/ccncert/

SESIÓN PLENARIA *(Gran Anfiteatro)*

09.00 – 09.25 INAUGURACIÓN
(Félix Sanz, *Secretario de Estado Director del CNI-CCN*),
(Fernando García Sánchez, *Jefe de Estado Mayor de la Defensa*)

09.30 – 10:20 ***Novedades CCN-CERT.*** **Gestión de Incidentes en 2014** *(CCN)*

10.25 – 10.55 ***Persistencia en BIOS.*** **Estado del Arte** 🔥
(David Barroso, ELEVEN PATHS)

11.00 – 11.45 CAFÉ Y ENTREGA DE DIPLOMAS A PATROCINADORES

MÓDULO 1

CIBERESPIONAJE / APTs
(Gran Anfiteatro)

11.45 – 12.10
China y el ciberespionaje:
Sun Tzu, APT1 y los tiempos interesantes
(Antonio Sanz Alcober, S2GRUPO)

12.15 – 12.40
El APT de los 26 millones
(Vicente Díaz, KASPERSKY)

12.45 – 13.10
Ataques avanzados: **APT28**
(FIREEYE)

13.15 – 13.40
Experiencias y tendencias en investigaciones digitales de gran escala
(Carlos Fragoso ONE ESECURITY)

13.45 – 14.10
Rootkit**, quién te ha visto y quién te ve** 🔥
(Josechu Migoya y Francisco Oca, INNOTEC SYSTEM)

MÓDULO 2

NUEVAS AMENAZAS, HERRAMIENTAS Y TECNOLOGÍAS
(Sala Jiménez Díaz)

11.45 – 12.10
Ataques de *relay* en tarjetas EMV NFC con dispositivos Android. *Demo* 🔥🔥
(José Vila, ERNST & YOUNG)
(Ricardo Rodríguez, UNIVERSIDAD DE LEÓN)

12.15 – 12.40
Pre-fetching **of suspicious mobile apps based on Big Data techniques and correlation** 🔥
(Alfonso Muñoz, Sergio de los Santos, ELEVEN PATHS)

12.45 – 13.10
Ghost **in the Shell** 🔥
(Jaime Sánchez, TELEFÓNICA)

13.15 – 13.40
Desmitificando el AntiVirus 🔥🔥
(Abraham Pasamar, INCIDE)

13.45 – 14.10
UEFI Arma de doble filo. *Demo* 🔥🔥
(CCN)

MÓDULO 3

ESTRATEGIA DE CIBERSEGURIDAD. ENS Y CUMPLIMIENTO NORMATIVO
(Pequeño Anfiteatro)

11.45 – 12.10
Seguridad en *Cloud Computing*. Guía 823
(José A. Mañas, UPM)

12.15 – 12.40
Gestión de Incidentes. Visión del CSIRT-CV
(Lourdes Herrero, GVA)

12.45 – 13.10
Adecuación al ENS de la plataforma eAdministracion del Gobierno Vasco
(Jaime Domínguez-Macaya, GOBIERNO VASCO)

13.15 – 14.10
MESA REDONDA 1
Formación y certificaciones profesionales en ciberseguridad:
¿quiénes deben definir los perfiles?
Moderador:
Luis G. Fernández (Revista SIC)

14.15 – 16.00 VINO ESPAÑOL

La intensidad y sofisticación de los ciberataques dirigidos contra las Administraciones Públicas y contra las empresas y organizaciones de interés estratégico para el país, y cuyo principal objetivo es el robo de información y el ciberespionaje industrial, se incrementan día a día. Unas amenazas que se concretan a través de vulnerabilidades, exploits, código dañino, software potencialmente no deseado, amenazas contra el correo electrónico, sitios web dañinos, amenazas a dispositivos móviles o amenazas a bases de datos que no hacen sino poner en peligro el principal activo de cualquier organización: la información.

🔥 Grado de complejidad técnica

***Mesa redonda** Véase página siguiente*

TALLER 1

HERRAMIENTAS DETECCIÓN APTs

(Gran Anfiteatro)

16.00 – 16.55
CARMEN. Detectando lo desconocido… 🔥
(CCN y Daniel de los Reyes y Antonio Villaón, de S2 GRUPO)

17.00 – 18.00
MISP, MARTA y MARIA
(CCN y Fernando Muñoz y Myriam Sánchez, de INNOTEC SYSTEM)

TALLER 2

CONOCIENDO AL ATACANTE

(Sala Jiménez Díaz)

16.00 – 18.00
Desarrollo de Exploits en Win32 🔥🔥
(Ignacio Sorribas, WISE SECURITY)

TALLER 3

HERRAMIENTAS CUMPLIMIENTO NORMATIVO

(Pequeño Anfiteatro)

16.00 – 16.40
PILAR. Sendas de Ataque 🔥
(José A. Mañas, UPM)

16.45 – 17.20
LUCIA. *Demo*
(CCN y Joaquín Seco Martínez, CSA)

17.25 – 18.00
CLARA. *Demo* 🔥
(CCN y SIDERTIA)

🔥 Grado de complejidad técnica

1 MESA REDONDA

Formación y certificaciones profesionales en ciberseguridad:
¿quiénes deben definir los perfiles?

Moderador: Luis G. Fernández *(Revista SIC)*

- Javier Candau *(CCN)*
- Jorge Ramió Aguirre *(CRIPTORED-UPM)*
- Sergi Gil *(DELOITTE)*
- Marisol Serrano Alonso *(MINHAP-INAP)*
- Antonio Ramos García *(ISACA)*
- Elena de la Calle Vian *(MINETUR)*
- Jesús García *(SANS INSTITUTE en ESPAÑA)*

Ante esta situación, el CCN-CERT, con responsabilidad en ciberataques sobre sistemas clasificados y sobre sistemas de las Administraciones Públicas y de empresas y organizaciones de interés estratégico para el país, vuelca todos sus esfuerzos en contribuir a la mejora de la ciberseguridad española, cooperando y ayudando a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas.

08.30 Recogida de acreditaciones

MÓDULO 1

CIBERESPIONAJE / APTs
(Gran Anfiteatro)

09.00 – 09.25
Caso práctico APT: **Cuando las barbas de tu vecino veas pelar...** 🔥
(Antonio Sanz Alcober, S2GRUPO)

09.30 – 09.55
Abuso de la funcionalidad de los sistemas de control industrial. ***Demo*** 🔥
(Joel Sevilleja Febrer y Óscar Navarro Carrasco, S2GRUPO)

10.00 – 10.25
Medidadas fundamentales para mitigar el ciberespionaje. La Segmentación 🔥
(Miguel Sanz y Miguel Ángel Martín, AUTEK)

10.30 – 11.10
Are you the Weakest Link?
(Lorenzo Martínez, SECURÍZAME)

MÓDULO 2

NUEVAS AMENAZAS, HERRAMIENTAS Y TECNOLOGÍAS
(Sala Jiménez Díaz)

09.00 – 09.25
Wearables IT
(Jorge Dávila, UPM)

09.30 – 09.55
Desmitificando BAD USB 🔥
(Josep Albors, ESET)

10.00 – 10.25
Comunicaciones móviles seguras: **Selfies y Planes estratégicos**
(CCN)

10.30 – 11.10
Sistemas de mitigación DDoS coordinados con la operadora. Experiencia en un entorno universitario. ***Demo*** 🔥
(Alex López, Arbor Networks)

MÓDULO 3

ESTRATEGIA DE CIBERSEGURIDAD. ENS Y CUMPLIMIENTO NORMATIVO
(Pequeño Anfiteatro)

09.00 – 09.25
Actualización ENS y resultados INES
(CCN y Carlos F. Gómez, SEAP-MINHAP)

09.30 – 11.10
MESA REDONDA 2
Maniobras público-privadas orientadas a la ciberresiliencia sectorial
Moderador: José de la Peña (Revista SIC)

11.15 – 12.00 CAFÉ

12.00 – 12.40 SESIÓN PLENARIA ***(Gran Anfiteatro)***

12:00 – 12:40 **Homeland - el enemigo puede estar en casa** 🔥
(Juan Garrido, INNOTEC SYSTEM)

12:45 – 13:40 **MESA REDONDA 3 ¿Qué aportan los proveedores de servicios e integradores a la Ciberseguridad Nacional?**

13:45 – 14:25 **iOS: Regreso al futuro II** 🔥
(Raul Siles, DINOSEC)

14:30 – 14:45 **CLAUSURA**
Antonio Beteta, *Secretario de Estado de Administraciones Públicas*
Beatriz Méndez de Vigo, *Secretaria General del CNI*
Domingo Molina Moscoso, *Director TIC de la Administración General del Estado*

2 MESA REDONDA
Maniobras público-privadas orientadas a la ciberresiliencia sectorial

Moderador:
José de la Peña *(Revista SIC)*

- Luis Jiménez *(CCN)*
- Joaquín Álvarez *(ENDESA)*
- Francisco Javier Carmona *(IBERDROLA)*
- Alberto Hernández *(INCIBE)*
- Rafael Luis Santos *(Mº DE FOMENTO)*
- Francisco Lázaro *(RENFE)*

3 MESA REDONDA
¿Qué aportan los proveedores de servicios e integradores a la Ciberseguridad Nacional?

Moderador:
Domingo Molina
(Director TIC AGE)

- David Fernández *(SYMANTEC)*
- José Pereiro *(BT)*
- Félix Martín *(HP)*
- Jorge Uyá *(INNOTEC SYSTEM)*
- Óscar Pastor *(ISDEFE)*
- José Miguel Rosell *(S2 GRUPO)*

🔥 *Grado de complejidad técnica*

Platinum

InnoTec System Entelgy

S2 Grupo

Symantec.

Módulo 1

indra

Módulo 2

PANDA SECURITY

Gold

ARBOR NETWORKS

CSA

opens Open Source & Security Services

SIC

sidertia

TAISA

Silver

Deloitte.

FORTINET

Global CYBERSEC

Isdefe

realsec

TECNOBIT

Telefónica

WISE SECURITY

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