XIII JORNADAS STIC CCN-CERT

COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD

#XIIIJORNADASCCNCERT

ccn-cert
centro criptológico nacional

COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD

La promoción de un ciberespacio más seguro y confiable es una tarea primordial. Es también un reto colectivo pues para fortalecer la ciberseguridad nacional se precisa del compromiso de toda la sociedad.

Por este motivo, el lema de las XIII Jornadas STIC CCN-CERT "Comunidad y confianza, bases de nuestra ciberseguridad", pretende servir de impulso y, al mismo tiempo, promover la colaboración entre todos los organismos implicados en la defensa y protección del ciberespacio español. En esta edición, en la que también conmemoramos el decimoquinto aniversario del Centro Criptológico Nacional, las Jornadas STIC se consolidan como el principal evento de ciberseguridad celebrado en España.

Desde su creación, hace ya quince años, el Centro Criptológico Nacional, organismo adscrito al Centro Nacional de Inteligencia, ha contribuido a la mejora de la ciberseguridad española, actuando como centro de alerta y respuesta nacional y como coordinador a nivel estatal de las distintas capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad. Todo ello, mediante la formación de personal experto, la aplicación de políticas y procedimientos de ciberseguridad y el empleo y desarrollo de las tecnologías más adecuadas.

A lo largo de estos 15 años, la actividad del Centro Criptológico Nacional ha ido adaptándose a una realidad cambiante como pocas. Su contribución ha sido fundamental para el desarrollo de la Estrategia de Ciberseguridad Nacional, la implantación del Esquema Nacional de Ciberseguridad o la creación del CERT Gubernamental español (CCN-CERT) para la gestión y resolución de los ciberataques dirigidos al sector público, empresas y organizaciones de interés estratégico por el país.

Este compromiso constante del CCN por fortalecer la ciberseguridad nacional seguirá guiando nuestros pasos en el futuro. Y lo hará de forma conjunta con otras instituciones públicas, universidades, empresas y ciudadanos, conscientes de que la ciberseguridad requiere del compromiso de todos. Nuestra seguridad nacional, el desarrollo de nuestro tejido empresarial y el bienestar de la ciudadanía, así lo requieren.

Hagámoslo posible.

#XIIIJORNADASCCNCERT

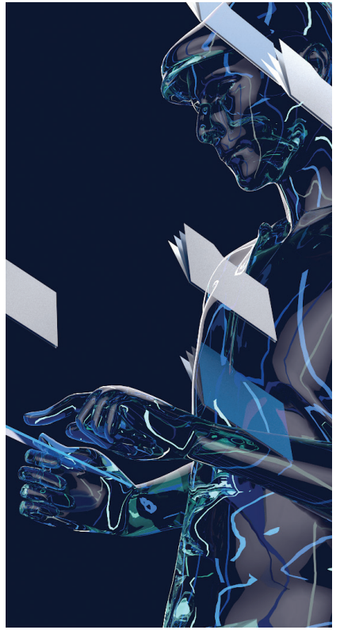
XIII JORNADAS STIC CCN-CERT

1º DÍA – 11 DE DICIEMBRE

07:15 09:00	**RECOGIDA DE ACREDITACIONES Y RECEPCIÓN DE AUTORIDADES** **CAFÉ**
	SESIÓN PLENARIA **(Sala Entelgy Innotec Security-25)**
09:00 09:45	**INAUGURACIÓN POR AUTORIDADES** Ministra de Defensa y de Asuntos Exteriores, D.ª Margarita Robles
09:50 10:25	**RETOS 2020** (Javier Candau, Jefe Departamento Ciberseguridad, CCN)
10:30 11:00	**FAKENEWS & FAKEPERSON: HERRAMIENTAS PARA MANIPULAR LA VERDAD** (Alejandro Martín y Juan Luis García, Sidertia)
11:00 11:35	**CAFÉ (SALA LUMIÈRE)**

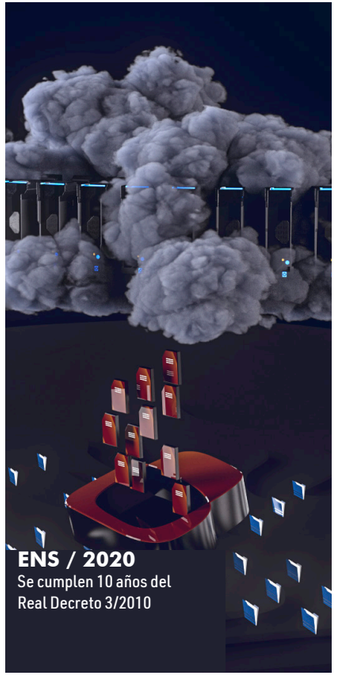
	SALA 25 ENTELGY INNOTEC	SALA 19 ESET	SALA 18 CYTOMIC	SALA 17 ATENEA
	MÓDULO 1:	MÓDULO 2:	MÓDULO 3:	MÓDULO 4:
	AMENAZAS, ATAQUES Y RETOS TECNOLÓGICOS	ENS Y CUMPLIMIENTO NORMATIVO	PREVENCIÓN EN CIBERSEGURIDAD / SOLUCIONES TECNOLÓGICAS	ATENEA
11:40 12:10	**I know your P4$$w0rd (and if i don´t, I will guess it)** (Jaime Sánchez y Pablo Jesús Caro, Telefónica)	**ENS 10 años. Framework ENS** (Miguel Ángel Amutio, Secretaría General de Administración Digital y Pablo López, CCN)	**Cybersecurity Act** (CCN)	**Resolución del reto Jörmundgander** (Germán Sánchez, Entelgy Innotec Security)
12:15 12:45	**5G: Mitos y leyendas** (José Pico y David Pérez, Layakk)	**El mito de la tecnología** (Raúl Morales y Jesús Angosto, Ingenia)	**Bypass of Air Gap Environments** (Joel Serna, Ferchau Engineering Spain)	**Vientos remotos, tempestades locales: Análisis forense de incidentes con accesos remotos** (Antonio Sanz, S2 Grupo)
12:50 13:20	**Cuando las apariencias engañan** (Delitos Telemáticos-UCO-, Guardia Civil)	**La incidencia del ENS en la contratación de servicios con terceros** (Miguel Ángel Lubián, Instituto CIES)	**La criptografía por las nubes** (Jorge Dávila, UPM)	
13:25 13:55	**Análisis de una APT: el caso BabyShark** (Óscar Luis García, Entelgy Innotec Security)	**Y la parte legal, ¿qué?** (Carlos Fernández, Guardia Civil)	**DualDAR encryption for the Samsung Knox Workspace** (José María Arroyo, Samsung)	
14:00 15:30	VINO ESPAÑOL			

	SALA 16 INGENIA	SALA 20 MICROSOFT	SALA 21
	MÓDULO 5:	MÓDULO 6:	MÓDULO 7:
	OPERACIONES MILITARES EN EL CIBERESPACIO	REDES OPERACIONALES / CONTROL INDUSTRIAL	OBSERVATORIO DIGITAL. ELISA
11:40 12:10	**Peculiaridades del combate en el cibersespacio** (CN Cubeiro Cabello, JEM MCCD)	**Caracterización de casos de uso de incidentes de ciberseguridad industrial** (Agustín Valencia y colaborador Francisco Rivero, Iberdrola)	**Características de las narrativas y los medios desinformativos** (Javier Lesaca, Columbia University)
12:15 12:45	**Planeamiento de Operaciones en el Ciberespacio I** (Capitán de Corbeta Santos Sande, MCCD)	**Los secretos de tu chip IoT** (Javier Tallón, jtsec Beyond IT Security)	**Vigilancia Digital de procesos electorales en fuentes abiertas** (Maite Moreno y Adrián Antón, CSIRT-CV)
12:50 13:20	**Planeamiento de Operaciones en el Ciberespacio II** (Comandante Laguna García, MCCD)	**Catching Mr Mime: Deception in an ICS environment** (Pedro Tubio y Alejandro Scatton, Deloitte)	**Desinformación 2.0** (Francisco José Carcaño, Ingenia)
13:25 13:55	**Inteligencia en apoyo al proceso de targeting ciber** (Cte. Ortega Medina, MCCD)	**Estrategias de ataque para el sector eléctrico** (Aarón Flecha y Jacinto Moral, S21sec)	**Automatizando la detección de contenido Deep Fake** (Alfonso Muñoz y Miguel Hernández, BBVA)
	VINO ESPAÑOL		



	SALA 25 ENTELGY INNOTEC	SALA 19 ESET	SALA 18 CYTOMIC	SALA 17 ATENEA
	MÓDULO 1:	**MÓDULO 2:**	**MÓDULO 3:**	**MÓDULO 4:**
	AMENAZAS, ATAQUES Y RETOS TECNOLÓGICOS	**ENS Y CUMPLIMIENTO NORMATIVO**	**PREVENCIÓN EN CIBERSEGURIDAD / SOLUCIONES TECNOLÓGICAS**	**ATENEA**
15:35 16:05	**Machine Learning para Defensa y Ataque** (José Selvi, NCC Group)	**Implantación del ENS por provincias** (David López, Cibergob)	**Por un puñado de bases de datos** (Simón Roses, VULNEX)	**Taller de Reversing Introducción a Ghidra** (Ricardo Rodríguez, UNIZAR)
16:10 16:40	**Anatomy of a real intrusion - APT and crimeware world, together for the same objective** (Marc Rivero, McAfee)	**Ya he certificado mi sistema del ENS, ¿y ahora qué?** (José Luis Colom, Audertis)	**Ciberseguridad vs la infraestructura abstracta: Microservicios, Docker y Kubernetes. No hay cuchara, Neo** (Alberto Cita, Symantec)	
	FUERA DE PROGRAMA			
17:00 17:20	**Servicio de Threat Hunting, aprendiendo del atacante para evolucionar las defensas** (Entelgy Innotec Security)	**ESET, solución frente a nuevas amenazas** (David Sánchez, ESET)	**Threat Hunting - Cómo responder a la profesionalización del cibercrimen** (María Campos, Cytomic)	**Nuevos Riesgos en Entornos Hospitalarios** (Óscar Navarro, S2Grupo)
17:25 17:40	**MrLooquer presenta el primer análisis de exposición y riesgo de entidades españolas que no querrás perderte** (Francisco Jesús Gómez y Leonardo Nve, CSA)	**Samsung Knox** (Santiago Izquierdo, Samsung)	**Del dato a la remediación. Destapando la ATP MuddyWater** (Alberto Cañadas, Grupo ICA y Michael Ramírez, Recorded Future)	**Parando Emotet y Ryuk** (Alberto R. Rodas, Sophos)
17:45 18:00	**El uso de machine learning en ciberseguridad** (CheckPoint)	**Seguridad en contenedores y Kubernetes** (David Castillo, Fortinet)	**Protegiendo el eslabón más débil: las Personas** (José Arias, Proofpoint)	**Implementando políticas del ENS ante ataques disruptivos** (Xavier González, Open Cloud Factory)

	SALA 16 INGENIA	SALA 20 MICROSOFT	SALA 21
	MÓDULO 5:	**MÓDULO 6:**	**MÓDULO 7:**
	OPERACIONES MILITARES EN EL CIBERESPACIO	**REDES OPERACIONALES / CONTROL INDUSTRIAL**	**OBSERVATORIO DIGITAL. ELISA**
15:35 16:05	**Ciberespaña: un modelo de criptored para la seguridad y la gobernanza de la soberanía nacional en el ciberespacio** (Andrés Montero, Fundación Concepto)	**Industrial IoT: librando la batalla en terreno** (Armand Pascual. S2 Grupo)	**Debate tecnológico: La desinformación como reto para la ciberseguridad** Modera: José de la Peña, Revista SIC Intervienen: Pablo López (CCN), Javier Lesaca (Columbia University), Nacho Buenavista (Antena 3 TV), Héctor Izquierdo (Instituto de Empresa)
16:10 16:40	**OrangeWorm: How I met your master...** (Pablo Rincón, Cylera)	**Ciberseguridad Industrial: errores cometidos y cambios a aplicar** (Edorta Echave, Secure&IT)	
	FUERA DE PROGRAMA		
17:00 17:20	**Darwin y la ciberseguridad** (Esteban Fernández, Ingenia)	**Cumplimiento del ENS en Azure y Office 365: guías técnicas y scripts oficiales para aplicación de la guía STIC-823** (Héctor Sánchez, Microsoft e Iván González, Plain Concepts)	**Protege tu Información Sensible** (Sidertia-Citrix)
17:25 17:40	**Conteniendo el caos desde la nube** (Emmanuel Roeseler, IBM Security)	**Despliegue de redes seguras desde el acceso: profiling y segmentación en base al comportamiento** (Rafael del Cerro, HPE-Aruba)	**IMDR: Intelligent Managed Detection and Response** (Miguel Sánchez, Accenture Security)
17:45 18:00		**¿Ahorrar y facilitar la vida del SOC es posible?** (RSA)	



2º DÍA – 12 DE DICIEMBRE

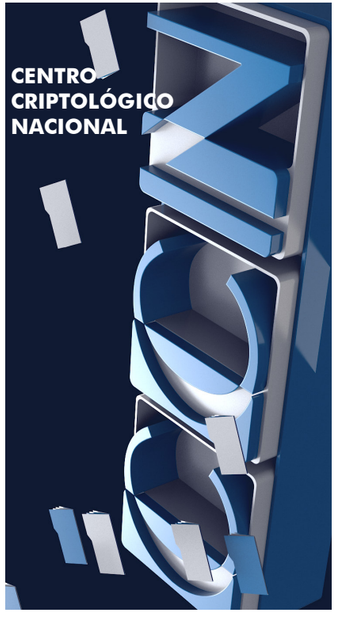
08:00 – 09:00 RECOGIDA DE ACREDITACIONES - CAFÉ

	SALA 25 ENTELGY INNOTEC	SALA 19 ESET	SALA 18 CYTOMIC	SALA 17 ATENEA
	MÓDULO 1:	**MÓDULO 2:**	**MÓDULO 3:**	**MÓDULO 4:**
	AMENAZAS, ATAQUES Y RETOS TECNOLÓGICOS	**ENS Y CUMPLIMIENTO NORMATIVO**	**PREVENCIÓN EN CIBERSEGURIDAD / SOLUCIONES TECNOLÓGICAS**	**ATENEA**
09:00 – 09:30	**Evolución del malware bancario y ataques dirigidos a usuarios en España** (Josep Albors, ESET)	**Framework Auditoría. Integración de Soluciones** (CCN-CERT)	**La amenaza cuántica, ¿hay cripto después?** (Luis Hernández y Víctor Gayoso, ITEFI - CSIC)	**Remote Code Execution in restricted environments** (Borja Merino, Tarlogic)
09:35 – 10:05	**OSINT – De la información a la inteligencia** (Carlos Seisdedos y Vicente Aguilera, ISEC Auditors)	**La certificación de personas: una herramienta eficaz para facilitar la implementación efectiva del ENS en las entidades públicas y sus proveedores** (Miguel Ángel Vila, IVAC)	**Visión práctica del catálogo de productos del CCN** (Fidel Paniagua y Miguel Viedma, Clover Technologies)	**HACKER ARENA** **100 vs 5** **¡ENFRÉNTATE A 5 RETOS EN DIRECTO!** **¡CONSIGUE TU PLAZA!** **DNHLQXFZVMK=**
10:10 – 10:40	**ThreatHunting práctico: no tengas miedo a Sigma y EQL** (David Barroso, CounterCraft)	**Cumplimiento conjunto del RGPD y ENS en la Universidad de Sevilla** (Julia Cortés y Francisco de Asís Gómez, Universidad de Sevilla CRUE TIC)	**El rol del ciber-integrador para esta ciber-época** (Ramsés Gallego, Grupo TRC)	
10:45 – 11:15	**Abusing - And protecting - Office 365** (Juan Garrido, NCC Group)	**vSOC para las EELL Valencianas: Proyecto piloto entre CSIRT-CV y la Diputación Provincial de Valencia para la mejora de la seguridad en la Administración Local** (Lourdes Herrero, CSIRT-CV)	**Comunicaciónes móviles para gestión de crisis. Caso ejército de Finlandia** (Laura Casadevall, Bittium Wireless)	

11:15 – 11:45 CAFÉ

	SALA 16 INGENIA	SALA 20 MICROSOFT	SALA 21
	6.0492	**MÓDULO 6:**	**MÓDULO 7:**
	OPERACIONES MILITARES EN EL CIBERESPACIO	**REDES OPERACIONALES / CONTROL INDUSTRIAL**	**OBSERVATORIO DIGITAL. ELISA**
09:00 – 09:30	**Cyber Situational Awareness y Cyber Operational Picture** (Teniente Coronel Mateos Calle, MCCD)	**Amenazas y soluciones de seguridad en entornos IoT: Sanidad e Industria** (Ricardo Borrajo. Extreme Networks)	**Análisis Forense de RPAs y su incidencia delictiva** (Casimiro Nevado, Víctor Tarazaga y Gabriel Cea, Escuela Nacional de Policía)
09:35 – 10:05	**Retos de la Ciberdefensa en el ámbito aeroespacial** (Coronel Acero Martín, Ejército del Aire)	**Cómo desplegar tecnologías en un entorno industrial** (Eduardo Di Monte, Oylo Trust Engineering)	**¿Se puede combatir el cibercrimen?** (Comisario D. Santiago Maroto, Unidad Central de Ciberdelincuencia)
10:10 – 10:40	**Concepto de "Ciberlitoral"** (CN Brandariz Calviño, Armada)	**Detección en sistemas de control industrial** (José Manuel Sacristán. Honeywell)	**Del crimen al cibercrimen** (Antonio López, Unidad Central de Ciberdelincuencia)
10:45 – 11:15	**Ciberejercicios en el ámbito militar** (TCol Palop Alcaide, MCCD)		**Campañas de desinformación a través de internet** (Inspector Jefe de la Unidad de Ciberterrorismo de la Comisaría General de Información)

CAFÉ



	SESIÓN PLENARIA (Sala Entelgy Innotec Security-25)
11:50 12:00	**ENTREGA PREMIOS ATENEA**
12:05 12:30	**PRIORIDADES DE LA POLÍTICA EUROPEA DE CIBERSEGURIDAD** (Miguel González Sancho, European Comission)
12:35 13:05	**PADRES NO HAY MÁS QUE DOS Y LOS MÍOS SON HACKERS (Y RECELAN DE LAS PLATAFORMAS TECNOLÓGICAS)** (Mónica Salas y Raul Siles, DinoSec)
13:10 13:30	**CCN-CERT UNCOVERED: DAVID CONTRA GOLIATH** (CCN-CERT)
13:35 13:45	**ENTREGA PREMIO A LA TRAYECTORIA PROFESIONAL EN FAVOR DE LA CIBERSEGURIDAD DEL CCN**
13:50 14:00	**CLAUSURA**

"SOLO A TRAVÉS DE LA CIBERSEGURIDAD SE PUEDE GENERAR LA CONFIANZA NECESARIA EN LA TECNOLOGÍA EN BENEFICIO DE LA SOCIEDAD."

#XIIIJORNADASCCNCERT

PATROCINADORES

VIP

S2 GRUPO
Anticipando un mundo ciberseguro

DIAMANTE

Entelgy Innotec SECURITY

ESTRATÉGICOS

Ingenia
CYTOMIC unit of Panda Security
eset ENJOY SAFER TECHNOLOGY™
Microsoft

CCN-CERT LABS

csa

PLATINUM

aruba a Hewlett Packard Enterprise company
Check Point SOFTWARE TECHNOLOGIES LTD.
FORTINET
grupo ICA Recorded Future
IBM
opencloud factory
proofpoint.
RSA
SAMSUNG
SOPHOS

ÁREA FACEBOOK

GOLD

accenturesecurity
Akamai Experience the Edge
autek
cybereason
FORCEPOINT
kaspersky
McAfee
MICRO FOCUS
netskope
ONE IDENTITY
radware
S21 SEC
Sidertia
Telefónica
tenable
thycotic

SILVER

a3sec
anadat technology
Applus
axians
Cipher
f5
gmv
iHackLabs
Isdefe su mejor aliado
MNEMO
oesia grupo
one cybersecurity
paloalto
realsec
redtrust a KEYPACTOR company
sia 30 años
Sidertia | citrix
SONICWALL
STORMSHIELD
TAISA
TARLOGIC
Telefónica
T-Systems
wisesecurity GLOBAL

ESPECIALES

udea
Entelgy Innotec SECURITY
eset ENJOY SAFER TECHNOLOGY™
GlobalSUITE
grupo ICA Recorded Future
TREND MICRO

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA

CCN centro criptológico nacional