

XI
JORNADAS
STIC
CCN-CERT

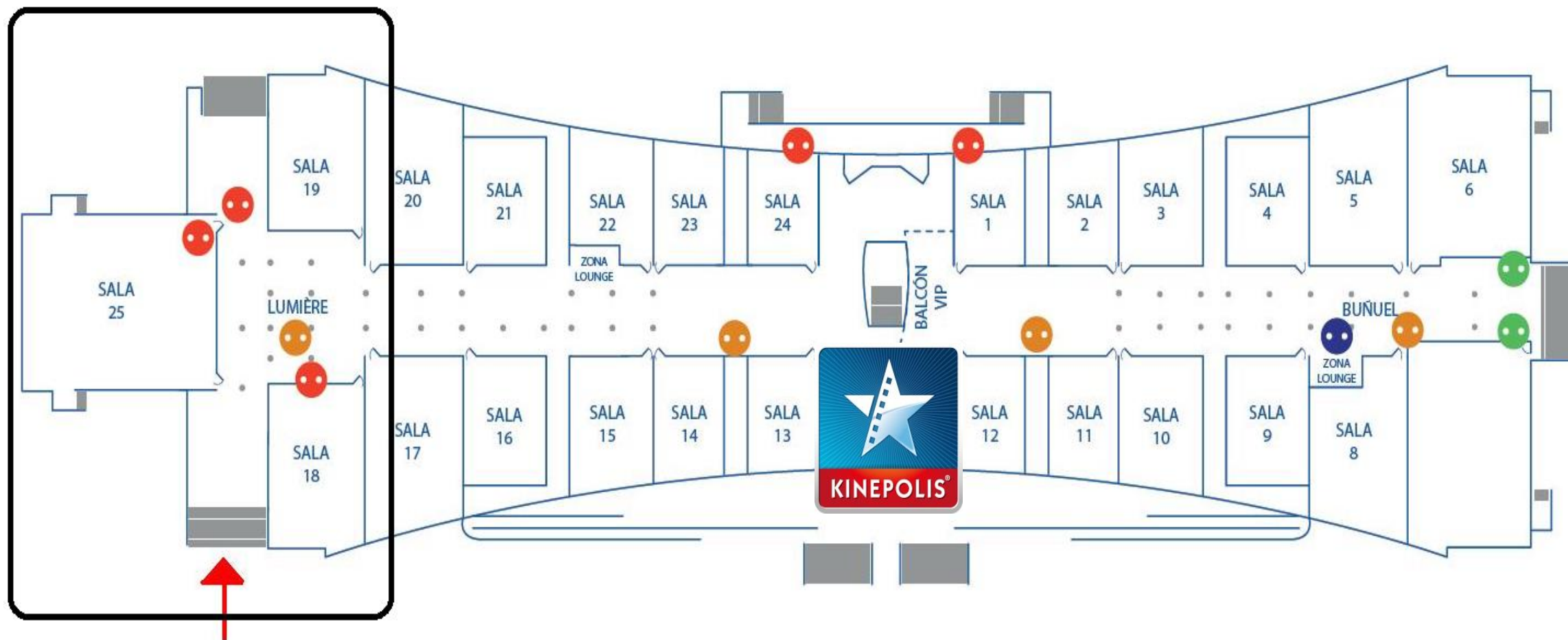
Ciberamenazas_
El reto de compartir

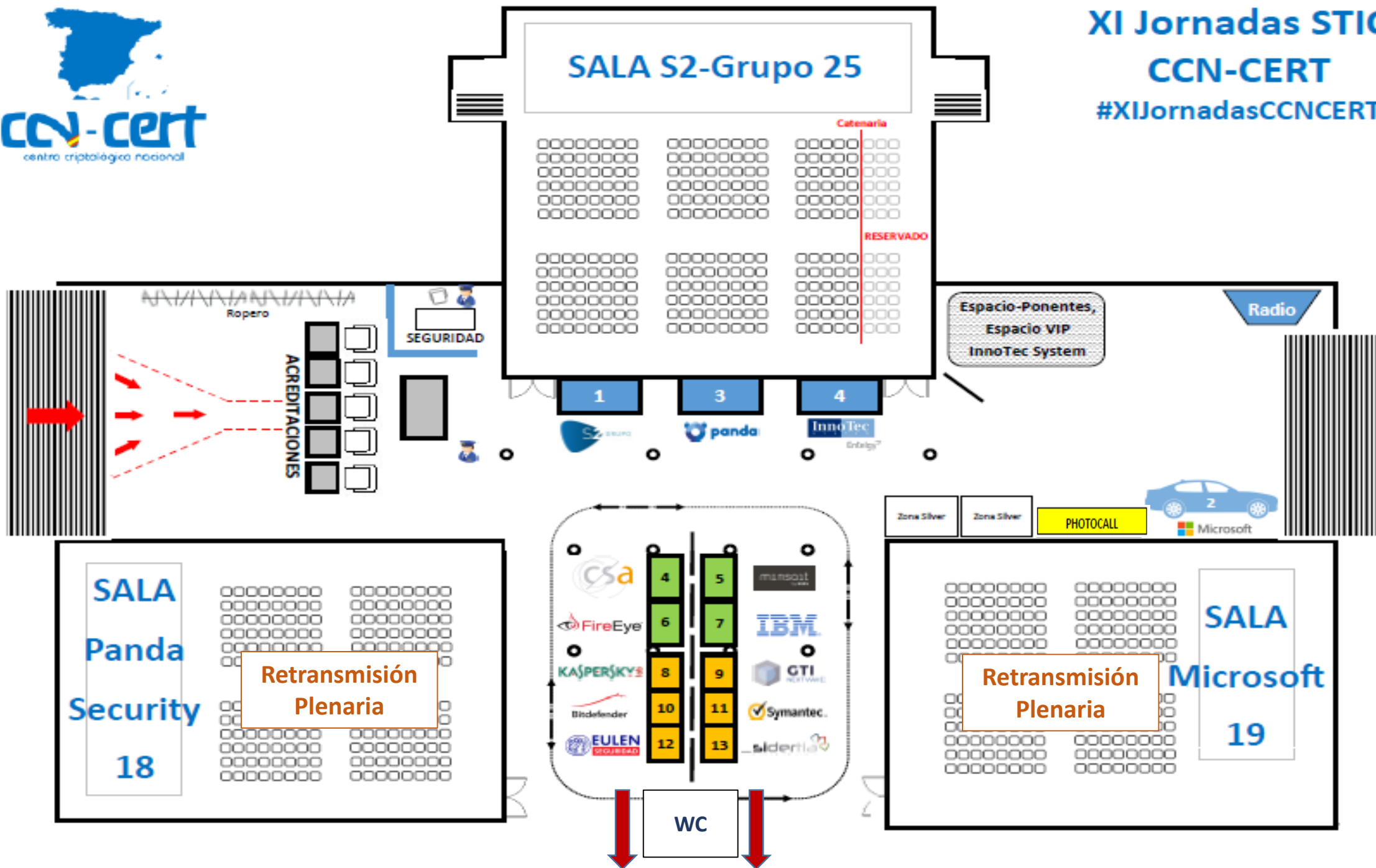
#XIJornadasCCNCERT

MADRID.
13 Y 14 DE DICIEMBRE
2017

BIENVENIDA

INFORMACIÓN ADMINISTRATIVA





XI JORNADAS STIC CCN-CERT	
DÍA 13 DE DICIEMBRE	
7:30	Recogida de acreditaciones
8:30	Recepción de autoridades
SESIÓN PLENARIA (SALA S2Grupo-25) (Retransmitida en Sala Panda Security-18) (Retransmitida en Sala Microsoft-19)	
09:00 09:25	INAUGURACIÓN (Vicepresidenta del Gobierno - D.ª Soraya Sáenz de Santamaría) (Secretario Estado Director del CNI - D.Félix Sanz Roldán)
09:30 10:00	Novedades CCN (Javier Candau, CCN-CERT - OC)
10:05 10:30	Un Año de Ataques (CCN)
10:35 11:00	Operaciones de falsa bandera: cuando las apariencias engañan (David Barroso, CounterCraft)
11:05 11:15	ENTREGA DE PREMIOS CCN
11:15 11:55	CAFÉ (Sala Lumière)

	Sala S2 Grupo-25	Sala Panda Security-18	Sala Microsoft-19
	MÓDULO 1: AMENAZAS/ATAQUES Y RETOS TECNOLÓGICOS	MÓDULO 2: ENS Y CUMPLIMIENTO NORMATIVO	MÓDULO 3: PREVENCIÓN EN CIBERSEGURIDAD
12:00 12:25	Quando el ciberespacio refleja el mundo real (Antonio Cañada, FireEye)	Un SOC para la AGE (Miguel Ángel Amutio, MINHAFP) (Pablo López, CCN)	Exchange Forensics: el caso del correo fantasma * (Antonio Sanz, S2Grupo)
12:30 12:55	Ciberdelincuencia Organizada, caso práctico: Inteligencia económica o como "perder" proyectos internacionales (Tcol. Jefe del Departamento de Delitos Telemáticos-UCO-, Guardia Civil)	El dilema de interpretación en el ciberespacio (Manuel R. Torres, Universidad Pablo Olavide)	Frente al computador cuántico, Criptografía postcuántica * (Luis Hernández y Victor Gayoso, CSIC)(David Arroyo, UAM)
13:00 13:25	KRACK Attacks (Deepak Daswani, Experto en Ciberseguridad)	Gestión de incidentes, tratamiento holístico (Ruth Sala Ordóñez, Legalconsultors) (Amador Aparicio, Profesor FP e Investigador en Ciberseguridad)	Hacking Hackers con Honeypots (Joaquín Molina-@kinomakino, ESET)
13:30 13:55	Hardware hacking: Obteniendo privilegios de administración * (Fran Quinto, RAQUINBER)	Mesa redonda: CISOs y DPOs de las AAPP: Retos y Desafíos Modera: José de la Peña (Revista SIC) Ponentes: Andrés Calvo (AGPD), Miguel Ángel Rodríguez (ASTIC), Miguel Ángel Amutio (MINHAFP)	UAC Bypass & Research with UAC-A-Mola * (Pablo González Pérez, ElevenPaths)(Santiago Hernández, Telefónica)
14:00 15:15	VINO ESPAÑOL (Sala Lumière) 14:10 Entrega Diploma Patrocinadores (Photocall)		
	Diplomas: SILVER		

	Sala S2 Grupo-25	Sala Panda Security-18	Sala Microsoft-19
15:20 15:45	Bots de Geolocalización de usuarios en Telegram (Eduardo Sánchez, onBRANDING)	Cine, cine, cine, más cine por favor... (Antonio Grimaltos, CH Júcar)	Busque, compare y compre algo cualificado. Ponga un #CATÁLOGO en su vida (CCN)
15:50 16:15	RockandROPeando: bypass DEP vía ROP * (Jesús Díaz, Palo Alto)	JCCL en adaptación al RGPD e integración ENS (Alicia Fernández-Torija, JCCL)	Ransomware: Los secuestradores van a la oficina (Fernando Rubio, Microsoft)
16:20 16:45	Radiografía de un ataque al suministro eléctrico * Demo (Manuel Bermúdez, ENAGAS)	Aplicación del ENS en las AA.PP. bajo un enfoque práctico: Menos es Más (Miguel A. Lubián, INSTITUTO CIES)	Cyber Situational Awareness. Retos e iniciativas (Cte. Mónica Mateos, Mando Conjunto de Ciberdefensa-MCCD)
	Fuera de programa		
	MÓDULO S2 GRUPO	MÓDULO PANDA SECURITY	MÓDULO MICROSOFT
16:50 17:45	Lo que realmente funciona en la Concienciación (Andrés Núñez)	Ciberguerra y el (des) control de los datos	Confiando información sensible a la nube. Azure Confidential Computing (Santiago Núñez)
	¿Quieres conocer a Gloria? (Daniel de los Reyes)		Cloud Services for GDPR compliance (Jaime Martín-Hinojal)
			Incident Response (Paloma Gómez Zamorano)
			Por un mundo sin contraseñas; pero mientras tanto, así las protegemos en Azure AD (Raúl Moros)

DÍA 14 DE DICIEMBRE

8:15 Recogida de acreditaciones

DNI Requerido
No olvidar Acreditación

SESIÓN PLENARIA

(SALA S2Grupo-25)
(Retransmitida en Sala Panda Security-18)
(Retransmitida en Sala Microsoft-19)

09:00 **Actúa y Baliza**
09:25 (Raúl Silas, Dinosec)

09:30 **Mitigación de riesgos en software de terceros en Google**
10:00 (Fermin Serna, Google)

Mesa redonda:
Ciberseguridad en el Sector público: aportaciones de la industria
Modera: Luis Fernández (Revista SIC)
Ponentes: Javier Cortés (CSA), Vesku Turtia (FIREEYE), Eduardo Argüeso (IBM), Félix Muñoz (INNOTECH), Héctor Sánchez (MICROSOFT), Jorge García (MINSAIT), José Rosell (S2GRUPO), Rosa Díaz (PANDA SECURITY), CCN

11:05 **CAFÉ (Sala Lumière)**
11:30 **Diplomas: GOLD y Superior**

Sala S2 Grupo-25

**MÓDULO 1:
AMENAZAS Y RETOS
TECNOLÓGICOS**

11:35 **Habías Tenido Tiempo para**
12:00 **Securizarlo...**
(Raúl Silas, Dinosec)
(CCN)

12:05 **Machine Learning, la re-evolución**
12:30 (Ramsés Gallego, Symantec)

Sala Panda Security-18

**MÓDULO 2:
ATAQUES**

11:35 **Descontrol industrial, el enemigo**
12:00 **invisible ***
(Aarón Flecha, S21sec)

12:05 **Mitos, debilidades y delitos**
12:30 **imperfectos en Tor**
(Manuel Guerra, Policía)
(Fco J. Rodríguez, INCIBE)

Sala Microsoft-19

**MÓDULO 3:
PREVENCIÓN EN
CIBERSEGURIDAD**

Nebularity Report, Anticipándonos
al Análisis de Malware *
(Fco. Javier Sucunza, InnoTec)
(Juan José Torres, Accenture)

Mirando dentro de tu dispositivo
móvil... ¿te puedes sentir seguro?
(Arneu Vives, APPLUS)

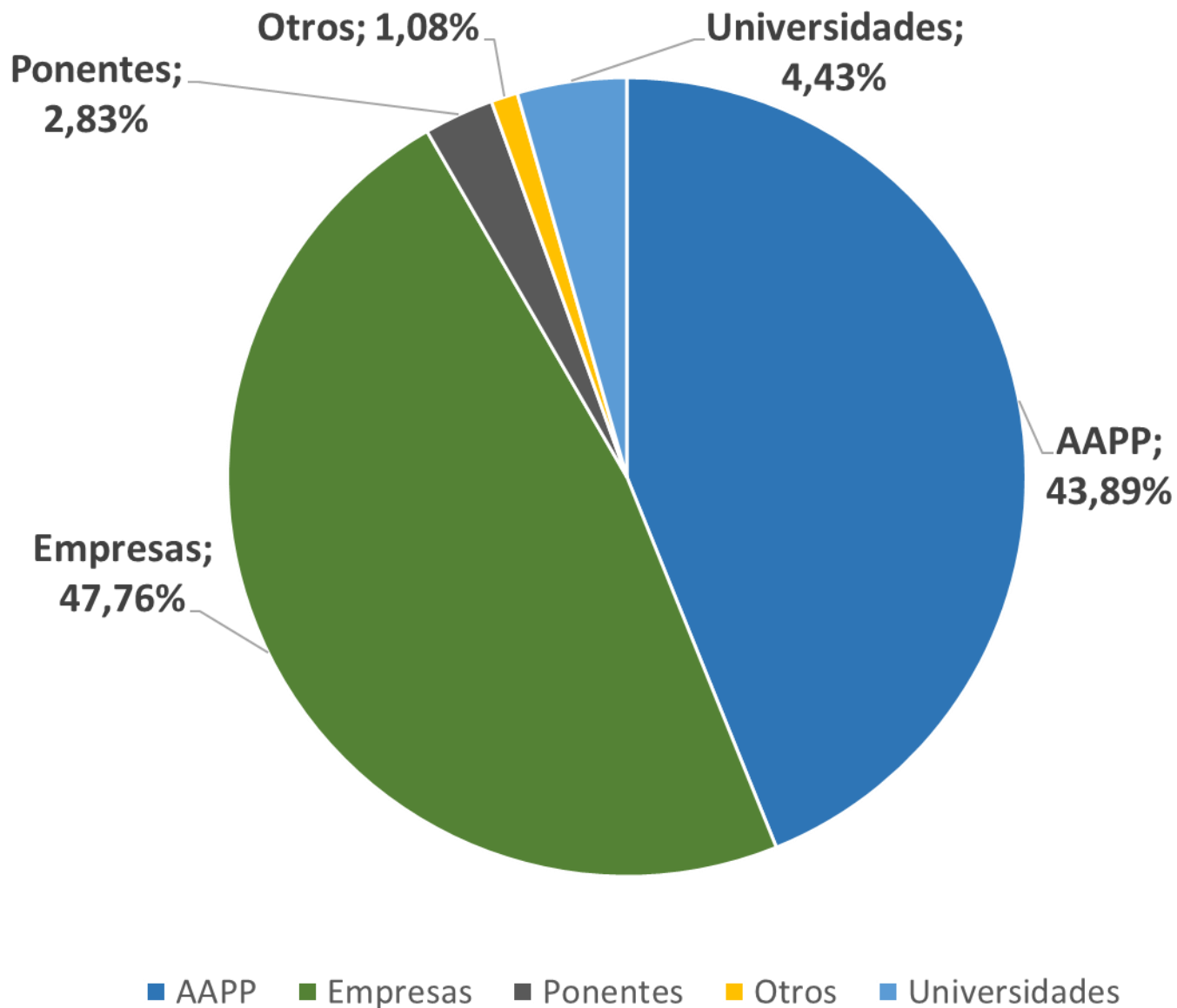
12:35 **NECURS: Estructura, Actividad y descripción en detalle**
13:05 (Jaeson Schultz, Líder Técnico de Cisco Talos Security Intelligence & Research Group)

13:10 **Smart Botnet. Porque no está la cosa como para denegar**
13:50 (Juan Garrido, Investigador en Ciberseguridad)

13:55 **CLAUSURA**
14:00 (Secretaría de Estado de Función Pública, MINHAFF – D.* Elena Collado)
(Secretario General de Administración Digital, MINHAFF – D. Domingo Molina)

(*) Ponencia con complejidad técnica

ASISTENTES
SOLICITUDES 2200+
INSCRITOS 1941
ORGANIZACIONES REPRESENTADAS 738



XI JORNADAS STIC CCN-CERT

Ciberamenazas_
El reto de compartir

#XIJornadasCCNCERT

MADRID.
13 Y 14 DE DICIEMBRE
2017

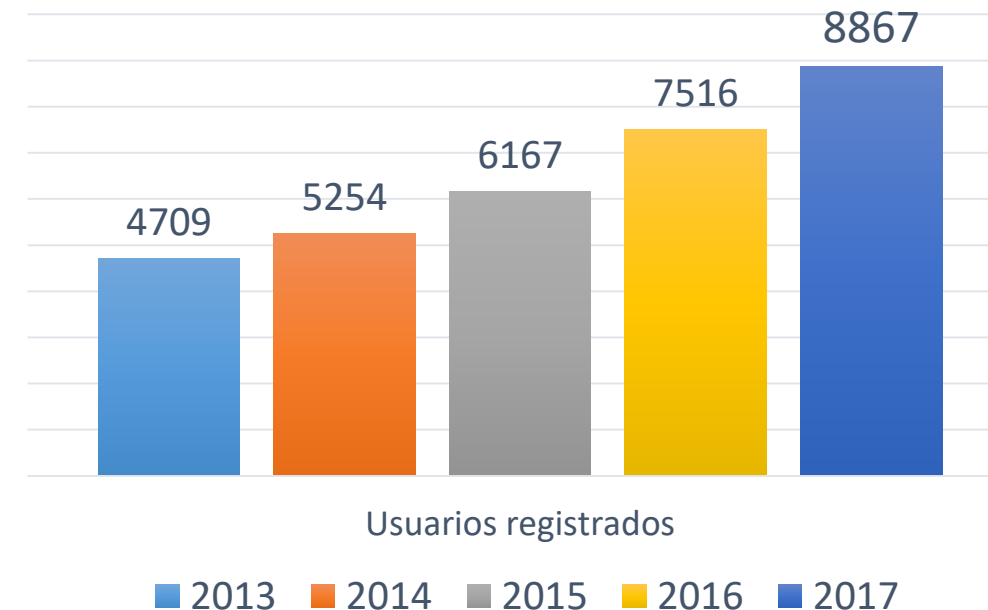
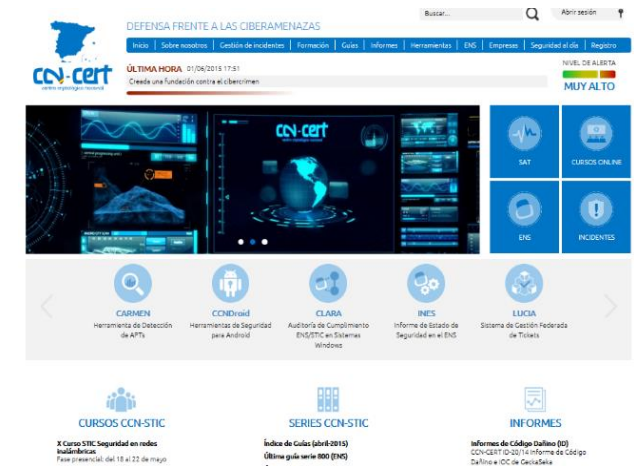
NOVEDADES CCN



- Javier Candau
- Jefe Departamento de Ciberseguridad
- Centro Criptológico Nacional
- ccn@cni.es

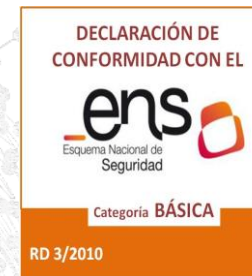
Índice

1. Cambios Legislativos. Directiva NIS
2. Formación y Concienciación
3. Buenas Prácticas. Guías e Informes
4. Sistemas de Alerta / Herramientas Detección
5. Herramientas de Auditoría
6. REYES y LUCIA
7. CSIRT.es
8. Plataforma de Retos
9. Objetivos / Conclusiones



Actualización Normativa

RD 951/2015, de 23 de octubre, Esquema Nacional de Seguridad
(fin de plazo 04.11.2017)



REGLAMENTO (UE) 2016/679, de 27 de abril de 2016.
Tratamiento y libre circulación de datos personales



**PILAR v7.0 con Perfil
GDPR**

DIRECTIVA (UE) 2016/1148, de 6 de julio de 2016. (Directiva NIS)
Garantizar un nivel común de seguridad en redes y sistemas.

Sector Público incluido
Identificación de OES (metodología)
Medidas de seguridad para OES
Autoridades Competentes (CCN)
Identificación de CSIRT de referencia
CCN-CERT y coordinación de respuesta técnica
Plataforma común de notificación incidentes
Subsanación de infracción antes que su castigo

Formación Presencial / On-line / A Distancia



2017

20 cursos presenciales + 13 sesiones VANESA

2691 solicitudes

574 alumnos presenciales + 1285 a distancia

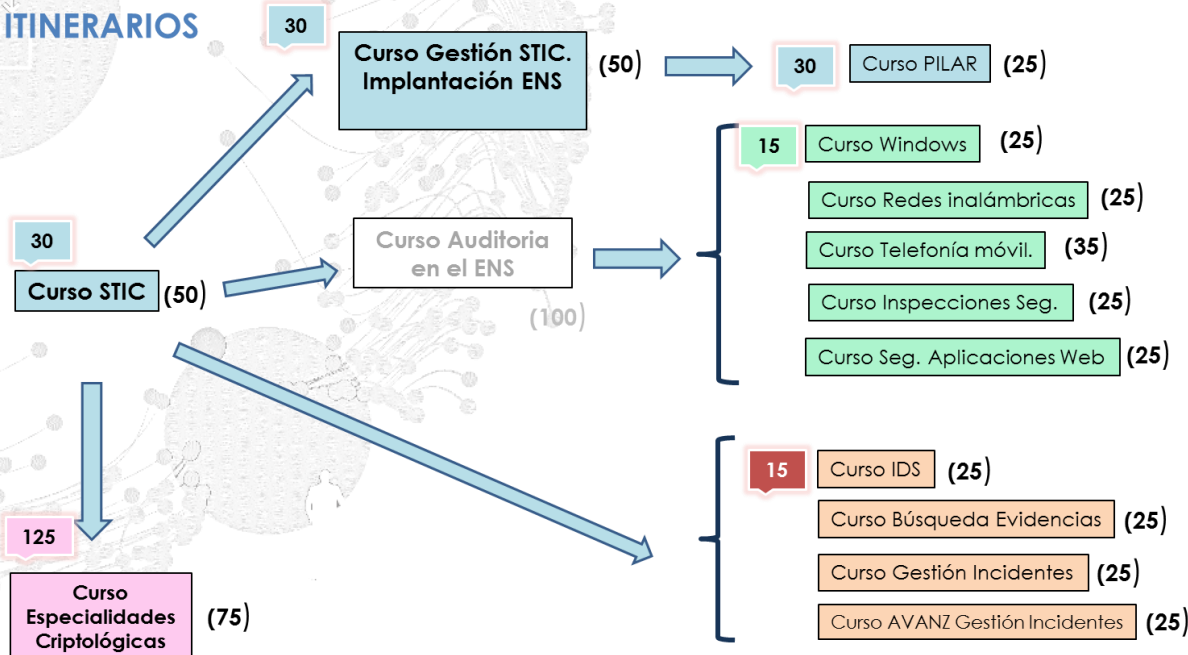
1295 horas lectivas

XIII Curso STIC
XI Curso Básico STIC Infraestructura Red
IX Curso STIC Búsqueda Evidencias
VIII Curso STIC Seguridad App Web
XI Curso STIC Inspecciones Seguridad
XIII Curso STIC Acreditación Windows
XI Curso Básico STIC BBDD
XXVII Curso Especialidades Criptológicas
I Curso STIC Gestión Incidentes
XIII Curso Gestión STIC
XII Curso STIC Detección Intrusos (IDS)
XI Curso STIC Seg. Redes Inalámbricas
VII Curso STIC Herramienta PILAR
V Curso STIC Dispositivos Móviles
II Curso STIC Gestión Incidentes

<i>Curso PILAR Ad-Hoc para el EA</i>
<i>Curso STIC Ad-Hoc para la DGP</i>
<i>Curso STIC Ad-Hoc para el CNI</i>
<i>Curso STIC Ad-Hoc República Dominicana</i>
<i>Curso Ad-Hoc Comunicaciones Seguras México</i>
<i>Curso Acreditación Empresas (ONS)</i>
13 sesiones teleformación plataforma VANESA

Cursos On-Line (Plataforma Web)
<i>Curso básico LINUX</i>
<i>Introducción al ENS</i>
<i>Curso INES</i>
<i>Curso básico WINDOWS</i>
<i>Curso STIC</i>
<i>Curso PILAR</i>

ITINERARIOS



Formación a distancia: Plataforma VANESA

FECHA	CURSO	USUARIOS REGISTRADOS	ACCESOS
17 mayo	Herramienta LUCIA	34	30
5 junio	Código Dañino	35	30
6 junio	Herramienta CLARA	33	30
11 julio	Herramienta PILAR	48	29
13 julio	Herramienta ROCIO	36	20
26 julio	HTTPS	197	150
27 julio	HTTPS	217	153
6 septiembre	Herramienta REYES	74	56
7 septiembre	Actualizaciones Seg. Windows	396	220
9 octubre	Actualizaciones Seg. Windows	391	100
10 octubre	Herramienta MARTA	96	60
11 octubre	Captura de Evidencias	474	132
7 noviembre	Big Data	489	275



Más de 1.200 alumnos

Sesiones de 4-5 horas

Mejor llegada a CCAA Y EELL

Integración con formación presencial

Información (Guías e Informes)

296 guías
441 documentos

2016

19 nuevas guías
12 actualizadas

2017

29 nuevas guías
22 actualizadas



154

Informes de Amenazas (IA) (28/**30**)
Informes de Código Dañino (ID) (29/**27**)
Informes Técnicos (IT) (92/**57**)
Buenas Prácticas (BP) (5/**3**)

Guía CCN-STIC
406

Guía CCN-STIC
652

Guía CCN-STIC
817

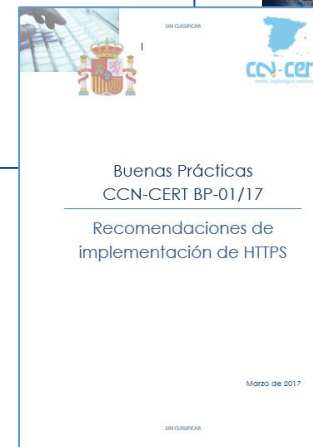
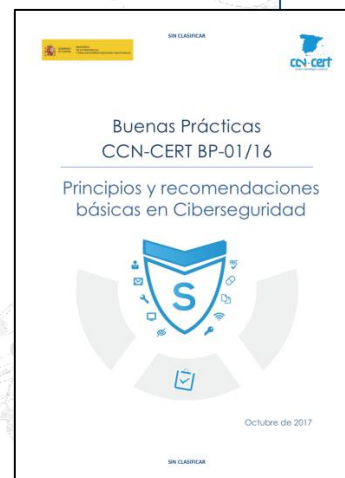
Guía CCN-STIC
811

Guía CCN-STIC
105

Guía CCN-STIC
106

Guía CCN-STIC
101

Guía CCN-STIC
301



Vulnerabilidades - Alertas - Avisos



Asunto de la Alerta	Fecha de envío
[CCN-CERT Alerta] Dos vulnerabilidades de EXIM permiten ejecutar código arbitrario o causar un ataque DoS	28/11/2017
[CCN-CERT Alerta] Vulnerabilidad en Microsoft Office	16/11/2017
[CCN-CERT Alerta] Campaña de ataques DDoS contra la Administración	23/10/2017
[CCN-CERT Alerta] Vulnerabilidades en WPA2 afectan a redes Wi-Fi	16/10/2017
[CCN-CERT Alerta] Vulnerabilidades críticas en Bluetooth	14/09/2017
[CCN-CERT Alerta] Vulnerabilidades en Apache Struts 2 afectan a múltiples productos Cisco	12/09/2017
[CCN-CERT Alerta] Vulnerabilidad crítica de Struts, actualización urgente	06/09/2017
[CCN-CERT Alerta] Actualizada la herramienta para prevenir la infección por el ransomware WannaCry	15/05/2017
[CCN-CERT Alerta] CCN-CERT's tool to prevent the execution of the ransomware WannaCry	13/05/2017
[CCN-CERT Alerta] Ransomware WannaCry-herramienta preventiva (6)	13/05/2017
[CCN-CERT Alerta] Herramienta de prevención del ransomware WannaCry (5)	12/05/2017
[CCN-CERT Alerta] Listado de ficheros, hash e IoCs del ataque de ransomware (4)	12/05/2017
[CCN-CERT Alerta] Ataque de ransomware que afecta a sistemas Windows	12/05/2017
[CCN-CERT Alerta] Medidas de mitigación contra el ataque masivo de ransomware	12/05/2017
[CCN-CERT Alerta] Ataque masivo de ransomware	12/05/2017
[CCN-CERT Alerta] Vulnerabilidad Crítica en IIS 6 y Windows Server 2003 R2	29/03/2017
[CCN-CERT Alerta] Vulnerabilidad Crítica en Apache (continuación)	13/03/2017
[CCN-CERT Alerta] Vulnerabilidad Crítica en Apache	10/03/2017
[CCN-CERT Alerta] Vulnerabilidad de los sistemas de protección de memoria	20/02/2017
[CCN-CERT Alerta] ANC, ataque que afecta al sistema de protección ASLR y cache	20/02/2017
[CCN-CERT Alerta] Explotación de la vulnerabilidad de WordPress en su Api Rest	06/02/2017

2017

20 Alertas

19 Avisos

Línea de tiempo:

- Apache - Struts
- Microsoft
- NotPetya
- WannaCry
- Bluetooth
- WPA2
- #OPCatalunya

Aproximación Práctica / Herramientas Ciberseguridad



Detección - Sistemas de Alerta



SAT INTERNET

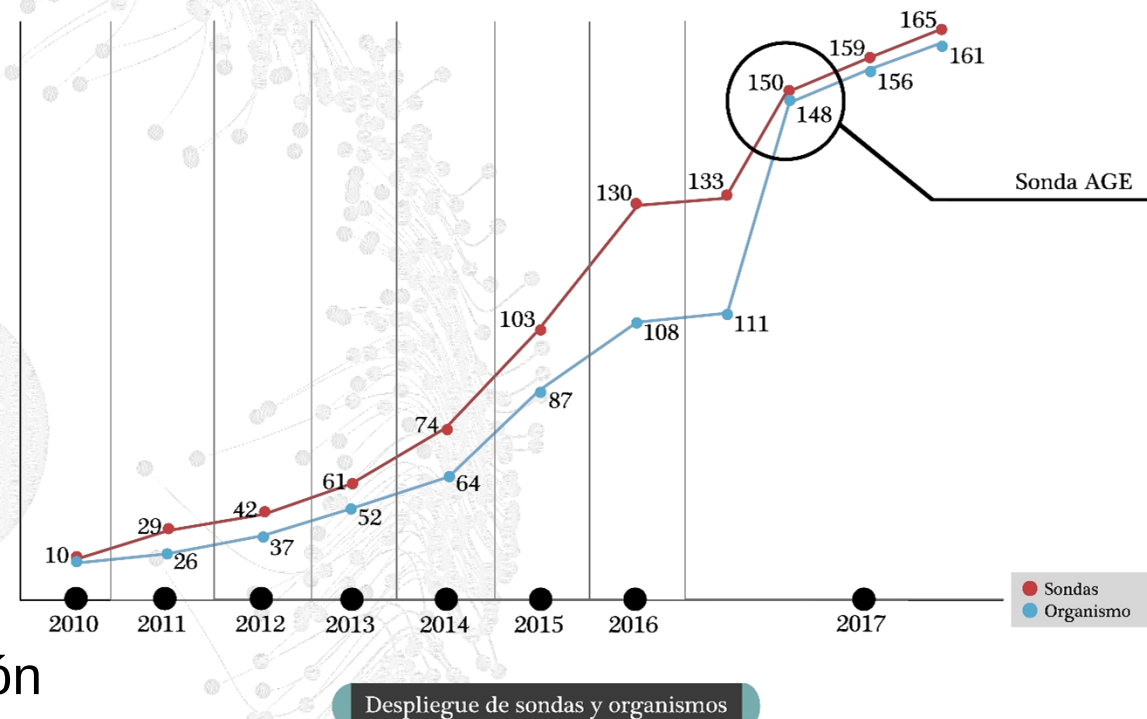
- Servicio por suscripción
- Despliegue de sondas
 - **161 Organismos**
 - **165 sondas**
- SAT v2.0 desplegado
- Correlación distribuida
- Automatización

Sonda AGE

- 2 tecnologías de detección

SAT SARA

- Plan renovación de hardware (CCN-CERT). **(21/49)**
- Sistema de análisis de vulnerabilidades
- Cambio de Correlador / Gestor eventos



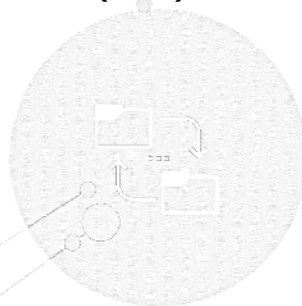
Detección - Sistemas de Alerta



- **Mínima intrusión** en el sistema monitorizado.
 - *Port Mirror.*
- **Análisis** del tráfico en las **redes operacionales** (OT).
- **Diferente aproximación...**
 - DPI de protocolos industriales
 - Reglas de comportamiento
 - IDS Reglas SNORT específicas

Sectores estratégicos:

- Aguas
- Puertos
- Confederaciones Hidrográficas
- Transporte



ENAIRe



CONFEDERACIÓN
HIDROGRÁFICA
DEL TAJO



Confederación Hidrográfica del Júcar



DIRECCIÓN GENERAL
DEL AGUA
CONFEDERACIÓN
HIDROGRÁFICA
DEL GUADALQUIVIR



**Bilbao Bizkaia
Ur Partzuergoa**
Consorcio de Aguas
Bilbao Bizkaia

Certificación EAL 2+



- **35 appliances** desplegados
- **7 appliances** en proceso de despliegue

Principales Novedades



6.0

- **Adquisición**
 - Cabeceras completas HTTP
 - Subida de ficheros PCAP
 - Análisis automático de código dañino en ficheros adjuntos
- **Investigación**
 - Integración con REYES
- **Mejoras en el interfaz**







Herramientas de Análisis

Total binarios subidos: 314

Total análisis realizados: 1796

Análisis solicitado por info@ccn-cert.cni

Fecha: 2017-05-12 17:00:36

Nombre: ed01ebfbc9eb5bbea545af4d01bf5f107166

Tamaño: 3514368 bytes

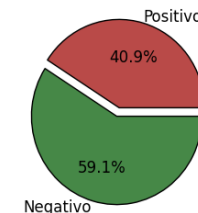
Tipo de fichero: PE32 executable (GUI) Intel 80386

Tipo MIME: application/x-dosexec

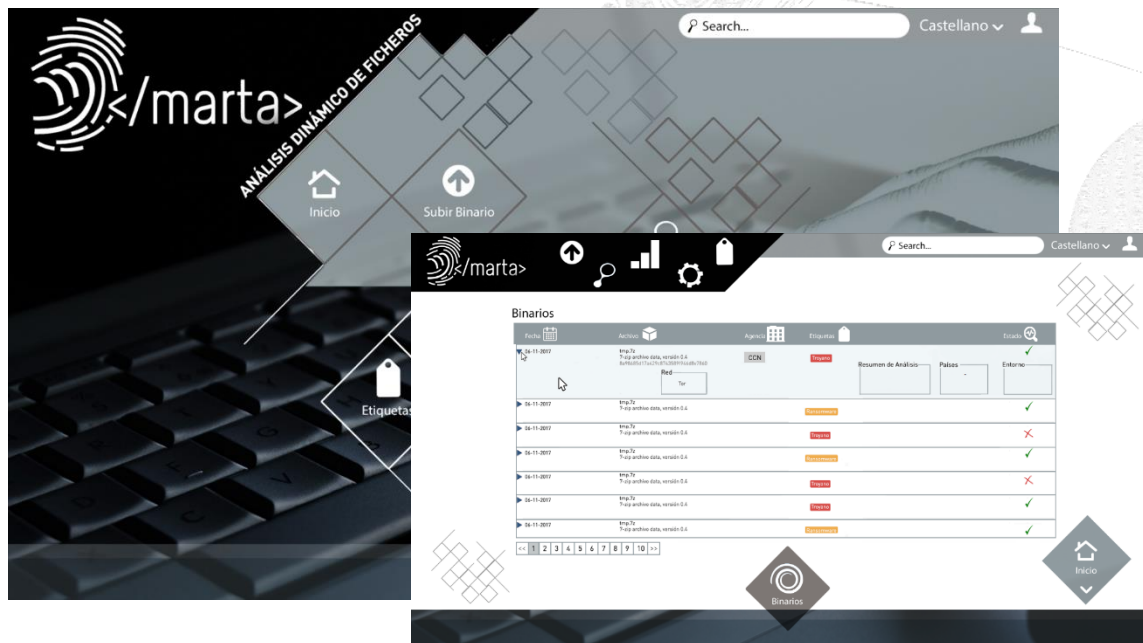
MD5: 84c82835a5d21bbcf75a61706d8ab549

SHA1: 5ff465afaabcbf0150d1a3ab2c2e74f3a44264

SHA256: ed01ebfbc9eb5bbea545af4d01bf5f107166



Resultado: POSITIVO



Antivirus	Resultado	Malware
NANO-Antivirus	NEGATIVO	
Symantec	NEGATIVO	
Zillya	NEGATIVO	
AVG	POSITIVO	Trojan horse Ransom_r.CFY
Arcabit	POSITIVO	Trojan.Graftor.D5A218
Quick Heal	NEGATIVO	
Avast	POSITIVO	OK
Ad-Aware	POSITIVO	Gen:Variant.Graftor.369176
Ikarus	NEGATIVO	
Nod32	POSITIVO	Win32/Filecoder.WannaCryptor.D trojan
Vba32	NEGATIVO	
Emsisoft	POSITIVO	Gen:Variant.Graftor.369176(B)
Mcafee	NEGATIVO	
Kaspersky	NEGATIVO	
Sophos	NEGATIVO	
ClamAV	NEGATIVO	
Zoner	NEGATIVO	
F-Prot	NEGATIVO	
Dr.Web	POSITIVO	BACKDOOR.Trojan
BitDefender	POSITIVO	Gen:Variant.Graftor.369176
eScan	POSITIVO	Gen:Variant.Graftor.369176(DB)
ClamAV	NEGATIVO	

CEF 2016: importante esfuerzo en el desarrollo de integración de herramientas con las que facilitar la labor de la comunidad en la mejor gestión de la ciberseguridad (MARTA y CARMEN)

Herramientas de Auditoría

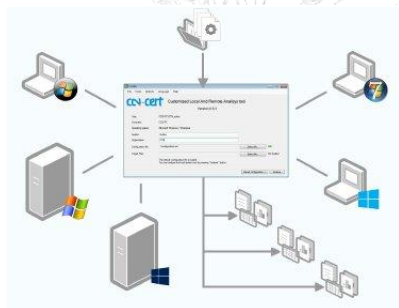


- Versión 7.0
- MicroPILAR Protección Datos
- **MicroPILAR Infraestructuras Críticas**
- **Realizar casos de uso con AEPD**
- Apoyo elaboración Documentación Seguridad



- Modelo distribuido
- Análisis de MS Windows 10 / **Serie 2016**
- Valoración continua nivel seguridad de Sistemas
- Aplicación de guías CCN-STIC
- Apoyo configuración de Seguridad de Sistemas

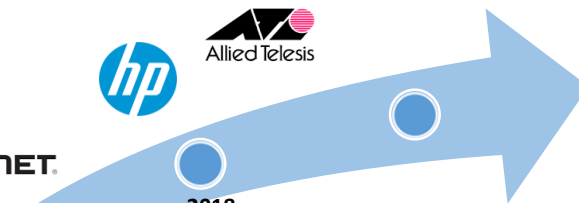
• Comprobación INTEGRIDAD sistemas



- Análisis equipos comunicaciones
- **Conexiones**
- **Firmware y sistema operativo**
- **Configuración**
- Apoyo configuración de Seguridad de Sistemas
- Contacto: rocio@ccn-cert.cni.es



- 2016
- Router y Switches Cisco
- Empleado por auditores CCN

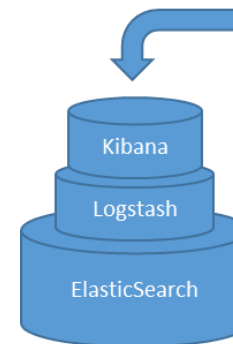


- 2017
- Fortigate
- Servicio ofrecido a la AGE

2018

- Instalación en Sistema Clasificado
- HP, Allied Telesys, Cisco Nexus

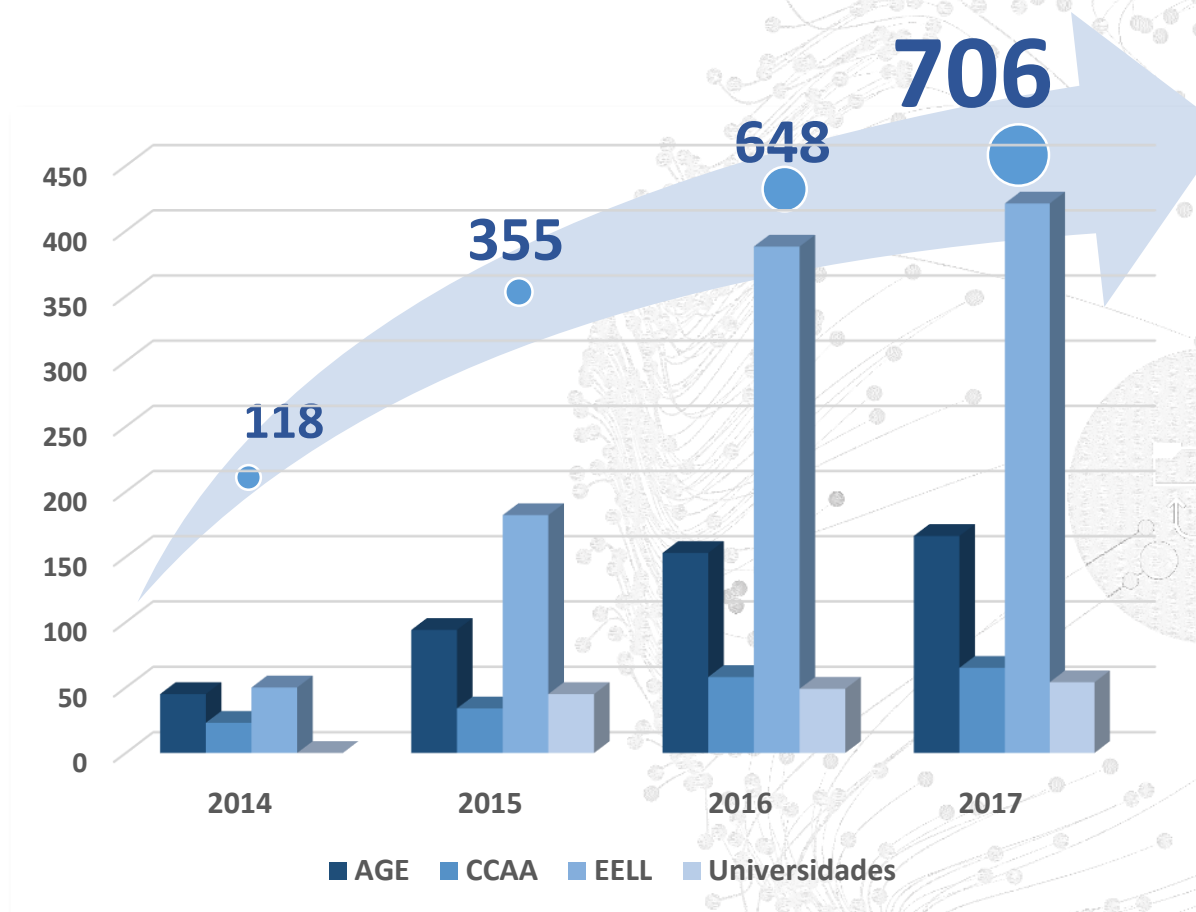
92 usuarios registrados
103 proyectos creados
314 informes generados



Recopilación centralizada de registros en todas las plataformas para cumplimiento de ENS/STIC

- Minería de registros
- Inventario de software
- Cuadros de mando para nivel de cumplimiento
- Alertas: anomalías, discrepancias, eventos predefinidos

Herramientas de Auditoría



	ALTA	MEDIA	BÁSICA
AGE	44	66	23
CCAA	29	14	5
EELL	101	167	25
UNIVERSIDADES	5	36	6
TOTAL	179	283	59

35%	54%	11%
------------	------------	------------

Hay algunos organismos que todavía no han registrado la categoría de sus sistemas



Número de sistemas: 16.544

Número de usuarios: 3.653.148



Ampliación del ámbito de aplicación del ENS con la entrada en vigor de la Ley 39/2015 y la Ley 40/2015

Auditoría / Inspección

El número de auditorías realizadas en 2017 ha aumentado notablemente en relación a años anteriores. En especial, las auditorías sobre páginas web de las AA.PP (**59 realizadas**)

• Ministerio de la Presidencia y para las Administraciones Territoriales

- 5 Fases / 14 Informes Técnicos
- Servicios Horizontales / BBDD / Redes Inalámbricas/ Aplicaciones Web

• Ministerio de Justicia



- 2 Fases / 20 Informes Técnicos
- Infraestructuras / Comunicaciones / Servicios Centrales / Delegaciones
- LEXNET / Justicia Digital

• Ministerio de Hacienda y Función Pública

- 4 Fases / 11 Informes Técnicos
- Cita Previa / Altos Cargos / Notifica / GEISER

• Ajuntament de Vinaròs

- 1 Fase / 7 Informes Técnicos
- Páginas Web / Volcado de datos

• Comunidad Autónoma de la Región de Murcia

- Fase inicial / 1 Informe Técnico (en revisión)
- Portal Web / Educación / Salud



	NIVEL 1	NIVEL 2	NIVEL 3	NIVEL 4	NIVEL 5
ÁMBITO	Elemento (producto, servicio, dispositivo, aplicación,...) y Sistema.	Elemento (producto, servicio, dispositivo, aplicación,...) y Sistema.	Elemento (producto, servicio, dispositivo, aplicación,...), Sistema e Interconexión.	Elemento (producto, servicio, dispositivo, aplicación,...), Sistema e Interconexión.	Elemento (producto, servicio, dispositivo, aplicación,...), Sistema e Interconexión.
OBJETIVO	Determinación de los servicios proporcionados y arquitectura del Sistema.	Análisis de riesgos para determinar las propiedades y funciones de seguridad del Sistema.	Búsqueda de vulnerabilidades para llegar a conocer las propiedades y funciones de seguridad del Sistema.	Determinar el nivel de seguridad de un Sistema y su grado de cumplimiento con la política de seguridad.	Determinar el nivel de seguridad de un Sistema y su grado de cumplimiento con la política de seguridad.
ACTIVIDADES	- Análisis.	- Análisis. - Verificación Manual.	- Análisis. - Verificación Manual. - Verificación Automática.	- Análisis. - Verificación Manual. - Verificación Automática. - Prueba Intrusión Caja Blanca.	- Análisis. - Verificación Manual. - Verificación Automática. - Prueba Intrusión Caja Negra.
MEDIOS Y TÉCNICAS	- Revisión Documentación.	- Revisión Documentación. - Gestión Configuración. - Cuestionarios (ST&E Plan ¹). - Entrevistas.	- Revisión Documentación. - Gestión Configuración. - Cuestionarios (ST&E Plan ¹). - Entrevistas. - Herramientas Seguridad.	Herramientas y técnicas de explotación de vulnerabilidades.	Herramientas y técnicas de explotación de vulnerabilidades.
REALIZACIÓN	Continua, especialmente tras la adición de un nuevo componente al Sistema.	Periódica y acorde con el Procedimiento de Acreditación.	Periódica y acorde con el Procedimiento de Acreditación. Se considera como el Nivel recomendado para superar un proceso de acreditación.	Con carácter excepcional dependiendo de la sensibilidad del Sistema.	Con carácter excepcional dependiendo de la sensibilidad del Sistema.
RESULTADO	Mejora en la gestión "global" de la seguridad.	Mejora en la gestión "global" de la seguridad.	Conocimiento "real" del riesgo del Sistema.	Reconocimiento objetivo de que el Sistema opera dentro del marco de seguridad definido.	Reconocimiento objetivo de que el Sistema opera dentro del marco de seguridad definido.

- ¿Este incidente se notifica?
- ¿Tiene relación con el ENS?
- ¿Es Infraestructura Crítica?
- ¿Es servicio esencial NIS?
- ¿Hay datos personales?
- ¿Cuándo notifico?
- ¿Imagen / sanciones?
- ¿Es delito?
- ¿Es necesaria una denuncia?

PERO YO LO QUE QUIERO ES AYUDAAAAAA



Empresa IC



Organismo



Proveedor
Serv. Esencial



Empresa
Pública



Empresa

LUCIA 3.0

**En 150 Organismos (LUCIA Central)
28 Organismos federados**

Diciembre 2016

**89 % SAT INTERNET
4 % SAT SARA
2 % OTROS
5 % LUCIA**

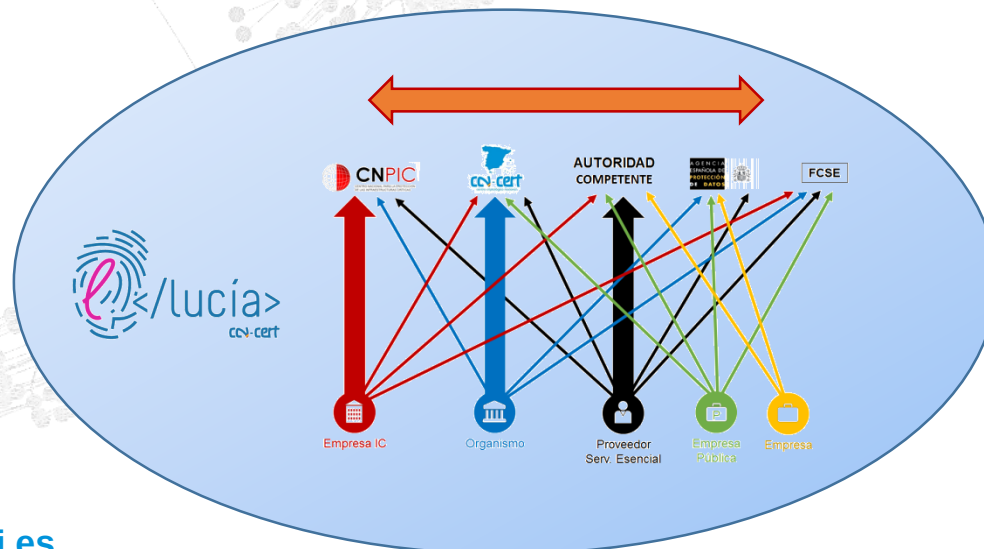
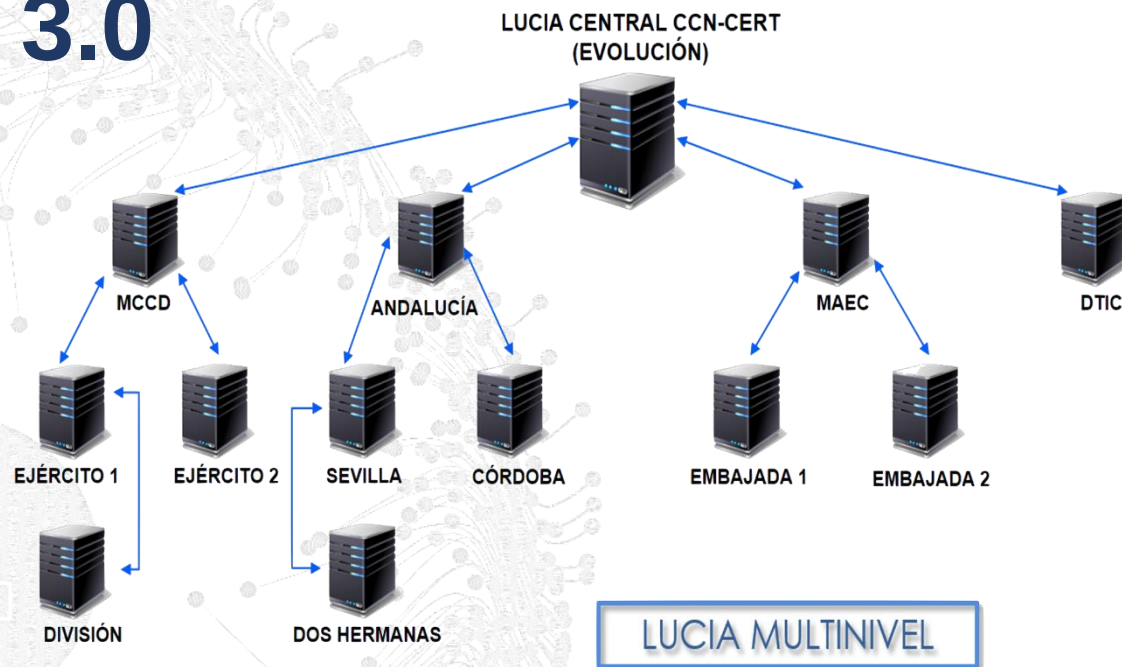


Diciembre 2017

**72 % SAT INTERNET
4 % SAT SARA
1 % OTROS
23 % LUCIA**

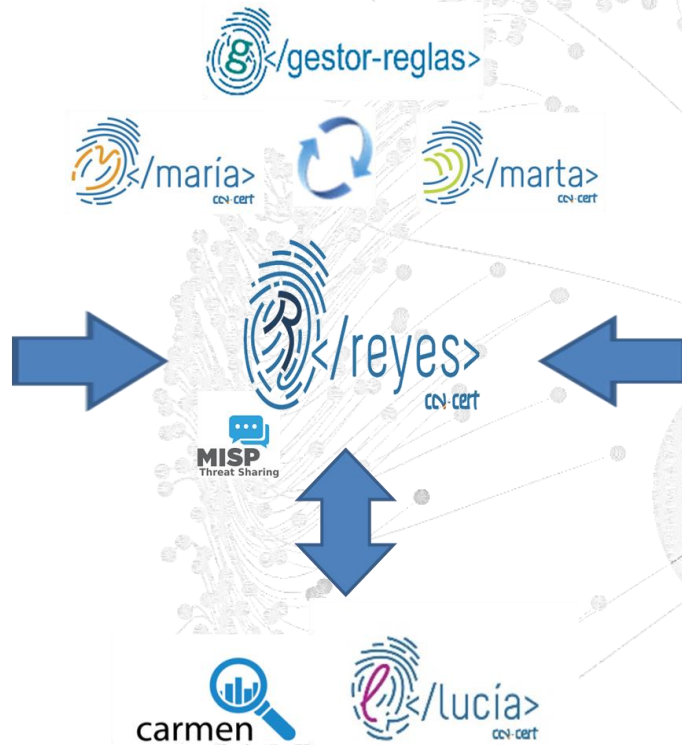


www.ccn-cert.cni.es

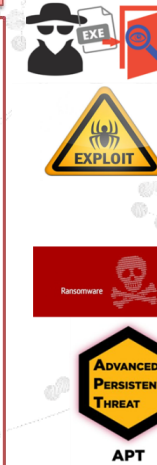


REYES 2.0

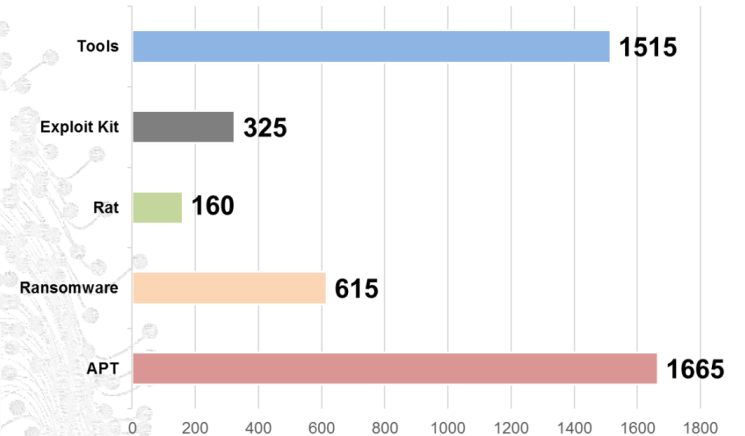
Feeds de inteligencia



Servicios de investigación

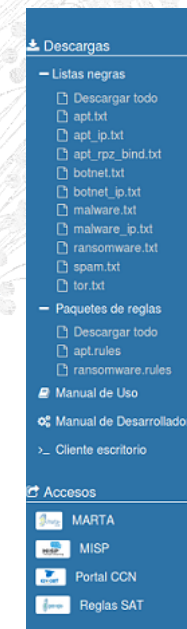


Eventos clasificados



Total búsquedas realizadas. 3742

Total indicadores buscados. 3513



PlaceholderBusqueda

Operador seleccionado:



CSIRT.es

Inicio Sobre CSIRT.es Objetivos Miembros FAQ Contacto Documentación

Coordinación ante ciberincidentes globales
Actuación rápida y simultánea ante un ciberataque

Equipos de Ciberseguridad y Gestión de Incidentes españoles

Proteger el ciberespacio español, intercambiando información sobre ciberseguridad y actuar de forma rápida y coordinada ante cualquier incidente que pueda afectar simultáneamente a distintas entidades en nuestro país, es el principal objetivo del Foro CSIRT.es

Este foro es una asociación independiente y sin ánimo de lucro compuesto por los equipos de respuesta a incidentes de seguridad CSIRT/CERT, sean públicos o privados, cuyo ámbito de actuación es el territorio español.

MIEMBROS **COORDINACIÓN DE INCIDENTES** **INTERCAMBIO DE INFORMACIÓN**

FIRST **TF-CSIRT**
Trusted Introducer

Aviso legal | Mapa web | Contactar

© 2017 - Equipos de Ciberseguridad y Gestión de Incidentes españoles - **CSIRT.es**

Iniciativa de CSIRT/CERT, públicos o privados, cuyo ámbito de actuación es el territorio español con el objetivo de compartir e intercambiar de una manera real

- Andalucía CERT
- BBVA CERT
- **Caixabank CSIRT**
- CCN-CERT
- CERTSI
- CertUC3M
- CESICAT-CERT
- CNPIC
- **CSIRT-CV**
- CSUC-CSIRT
- InnoTec-Entelgy-CSIRT
- esCERT-UPC
- ESP DEF CERT
- eSOC Ingenia
- Eulen-CCSI-CERT
- Guardia Civil
- MAPFRE-CCG-CERT
- Mº Interior
- Policía Nacional
- Prosegur CERT
- **RedIRIS**
- **S2 Grupo CERT**
- S21sec CERT
- Telefónica-CSIRT

¿Qué es?

- **ATENEA** es una plataforma de desafíos de **seguridad informática**
- Diversa temática: ciberseguridad básica, criptografía y esteganografía, exploiting, reversing, análisis de tráfico, forense, hacking web...

53 retos distinta dificultad
5.198 puntos

Objetivos

- **Involucrar** a todo aquél con experiencia en seguridad TIC.
- **Concienciar** al personal TIC sobre los riesgos de la seguridad informática.
- Mostrar a las personas con menos experiencia en la seguridad TIC que **los retos son divertidos** y que la seguridad no es una ciencia secreta que nunca entenderán.





ccn-cert centro criptológico nacional

6 5 5 5 6 9 0★

Básica Criptografía y esteganografía Exploiting Forense Hacking Web Networking Reversing

17 18 hours, 31 minutes, 19 seconds remaining

Hash 2 (1pts) 693 days, 1 hour, 58 minutes, 38 seconds remaining

Hash 3 (2pts) 693 days, 2 hours, 8 minutes, 53 seconds remaining

Base64 (3pts) 1055 days, 18 hours, 35 minutes, 50 seconds remaining

ASCII (3pts) 691 days, 16 hours, 59 minutes, 12 seconds remaining

Hex (3pts) 691 days, 17 hours, 9 minutes, 27 seconds remaining

XOR (4pts) 1055 days, 18 hours, 39 minutes, 25 seconds remaining

Entropía (5pts) 693 days, 2 hours, 17 minutes, 19 seconds remaining

Magic number (5pts) 693 days, 2 hours, 23 minutes, 28 seconds remaining

Strings (5pts) 711 days, 19 hours, 59 minutes, 14 seconds remaining

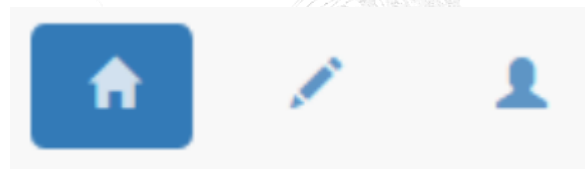
Metadatos (6pts) 711 days, 20 hours, 50 minutes, 25 seconds remaining

¿Quién puede registrarse?

Cualquiera, con una cuenta de correo electrónico.

Soporte limitado.

En esta primera fase, se limitará el **acceso a únicamente 1.500 usuarios.**



¿Cómo me registro?

Accediendo a la siguiente URL:

<https://atenea.ccn-cert.cni.es>

OBJETIVOS 2018

- **Implantación del ENS Sector Público. Necesidad de certificación.**
 - Se establecerán de forma clara la necesidades adicionales para INF. CRITICAS, PROTECCIÓN DE DATOS, DIRECTIVA NIS
- **REFORZAR LA CAPACIDAD DE VIGILANCIA Y RESPUESTA ...**
Aumentar la disuasión... Generar dudas coste/beneficio al ciberatacante
- **Formación.** Integración formación presencial y a distancia. Definir el perfil de seguridad en los puestos de trabajo de las AAPP.
- **CSIRT.es.** Impulso de la **comunidad de CERT,s / ciberinteligencia** (generar confianza mutua para fortalecer el intercambio).
- **Mejorar el intercambio**
 - Patrones de detección en cualquier formato (IOC, reglas Yara, etc.)
 - Herramientas que faciliten el **intercambio automático.**
 - Experiencias CCN / Apoyo resolución incidentes



XI
JORNADAS
STIC
CCN-CERT

Ciberamenazas_
El reto de compartir

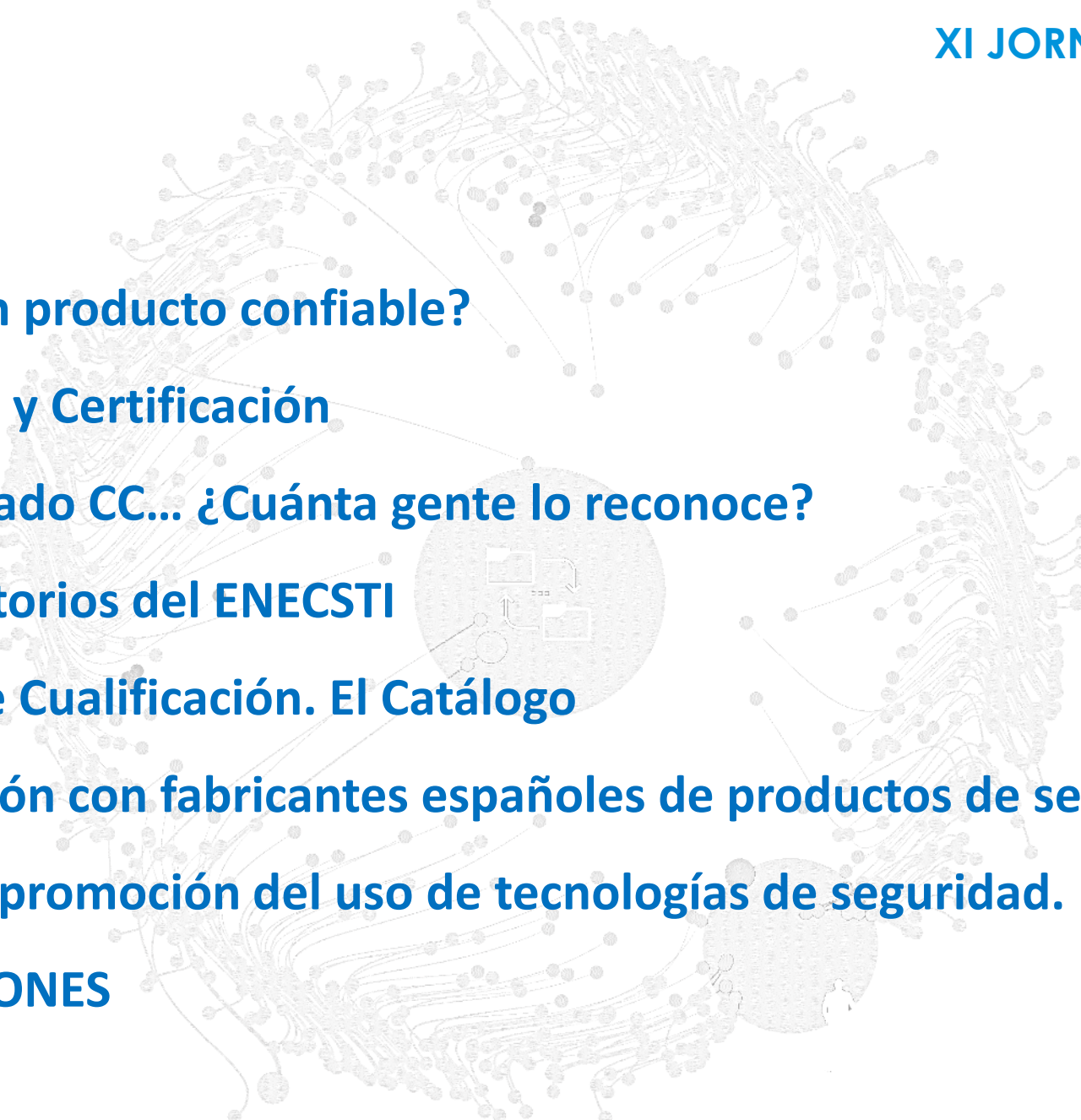
#XIJornadasCCNCERT

MADRID.
13 Y 14 DE DICIEMBRE
2017

**La importancia de usar
productos de seguridad confiables**



- Departamento de Productos y Tecnologías
- Centro Criptológico Nacional
- ccn@cni.es

- 
1. **¿Qué es un producto confiable?**
 2. **Evaluación y Certificación**
 3. **Un certificado CC... ¿Cuánta gente lo reconoce?**
 4. **Los laboratorios del ENECSTI**
 5. **Proceso de Cualificación. El Catálogo**
 6. **Colaboración con fabricantes españoles de productos de seguridad.**
 7. **Difusión y promoción del uso de tecnologías de seguridad.**
 8. **CONCLUSIONES**

1.-¿Qué es un producto confiable?

- Producto que ha sido sometido a un proceso de evaluación de seguridad independiente.



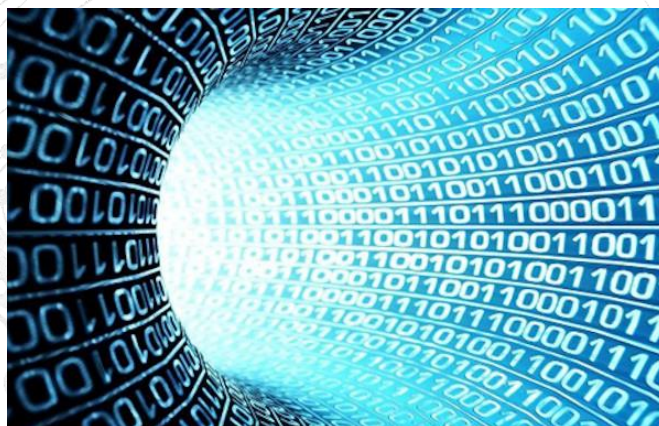
2.-Evaluación y Certificación.

NIVEL ALTO / MUY ALTO

**Certificación
Funcional**

**Certificación
Cripto**

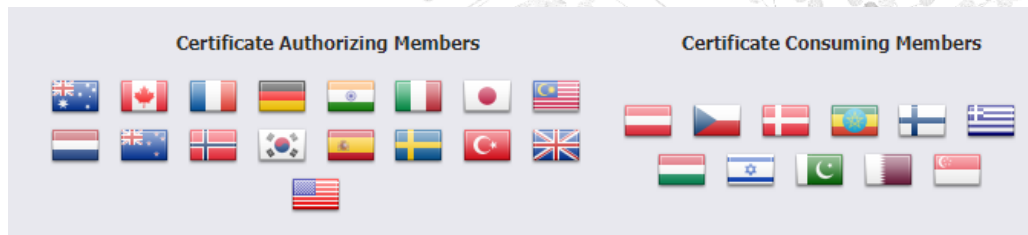
**Certificación
EMSEC**





3.-Un certificado CC... ¿Cuánta gente lo reconoce?

CCRA



28 países

SOGIS



- Austria, Bundeskanzleramt
- Croatia, Information Systems Security Bureau
- Estonia, RIA - Riigi Infosüsteemi Amet
- Finland, FICORA - Finnish Communications Regulatory Authority
- France, ANSSI - Agence Nationale de la Sécurité des Systèmes d'Information
- Germany, BSI - Bundesamt für Sicherheit in der Informationstechnik
- Italy, OCSI - Organismo di Certificazione della Sicurezza Informatica
- The Netherlands, NLNCSA - Netherlands National Communications Security Agency, Ministry of the Interior and Kingdom Relations
- Luxembourg, ANSSI.lu - Agence Nationale de la Sécurité des Systèmes d'Information Luxembourg
- Norway, SERTIT - Norwegian National Security Authority operates the Norwegian Certification Authority for IT Security
- Poland, NASK - Naukowa i Akademicka Sieć Komputerowa
- Spain, CCN - Centro Criptológico Nacional, Organismo de Certificación de la Seguridad de las Tecnologías de la Información
- Sweden, FMV - Försvarets Materielverk
- United Kingdom, NCSC - National Cyber Security Centre

14 países



EAL 2



EAL 4



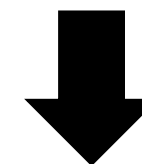
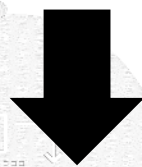
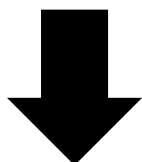
DOMINIO TECNICO

SmartCard

**HW
Devices**

EAL 7

4.-Los laboratorios del ENECSTI



EN PROCESO

5.-Proceso de Cualificación. El Catálogo

- ¿En qué me facilita la vida el catálogo?
- ¿Como pueden las empresas incluir sus productos en el catálogo?
- Siendo un usuario final... ¿Qué es lo que tengo que hacer?

La respuesta a todas esas preguntas y más...

HOY 13 DE DICIEMBRE
Sala Microsoft-19
15:20 a 15:45



**Busque, compare y compre algo
cualificado. Ponga un #Catalogo en su vida**

6.-Colaboración con fabricantes españoles de productos de seguridad.

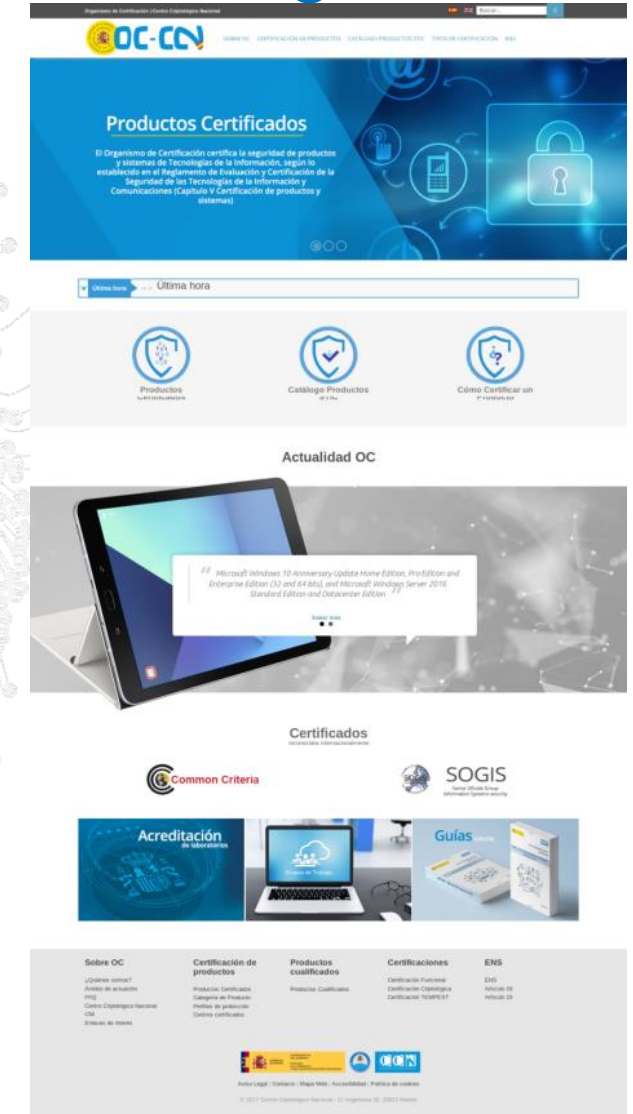
- Desarrollo de productos específicos.
- Seguimiento durante el desarrollo del producto.



7.-Difusión y promoción del uso de tecnologías de seguridad.

- Formación.
- Desarrollo de Normativa
- Arquitecturas de seguridad.
- Comunicación
 - Twitter
 - Nueva Web del OC
 - Boletines

<https://oc.ccn.cni.es>



8.- CONCLUSIONES

- Importancia del uso de productos certificados/cualificados
- Proceso de certificación validado mundialmente
- Te hacemos la vida más fácil. El Catálogo
- Trabajo continuo con las empresas del sector
- Nuevos medios de comunicación





E-Mails

- > info@ccn-cert.cni.es
- > ccn@cni.es
- > sat-inet@ccn-cert.cni.es
- > sat-sara@ccn-cert.cni.es
- > organismo.certificacion@cni.es
- > ccn-pytec@cni.es



Websites

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



Síguenos en

