

XIII JORNADAS STIC CCN-CERT



Información Administrativa

**COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD**

#XIIIJORNADASCCNCERT

XIII JORNADAS STIC CCN-CERT

COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD

#XIIIJORNADASCNCERT
#CCNCERT_Labs



ENTRADA

ROPERO
R

Acreditación

Amenazas, Ataques
y Retos Tecnológicos

SALA 15

Catering

Operaciones militares
en el ciberespacio

SALA 16
Ingenia



ATENEA

SALA 17
ATENEA
/RootedCOM

Catering

Prevención en Ciberseguridad
/ Soluciones Tecnológicas

SALA 18
CYTOMIC

Área Silver

15

11

7

Área de
Encuentro

SALA 22

Área
Facebook

SALA 21
e/Elisa

Observatorio Digital. ELISA

CNI

CCN

SALA 20
Microsoft

Redes Operacionales
/ Control Industrial

16

14

10

SALA 19
eset

ENS y Cumplimiento
Normativo

6

Catering

1

2

3

4

5

SALA 25

Entelgy
Innotec
SECURITY

Área
VIP

VIP

Set de
Prensa

Diamante

1 Entelgy Innotec Security

Estratégicos

2 Microsoft

3 Ingenia

4 Cytomic

5 ESET

VIP

VIP S2 Grupo

Platinum

6 CSA

7 Sophos

8 Grupo ICA

9 Proofpoint

10 Samsung

11 Opencloud factory

12 CheckPoint

13 Fortinet

14 IBM

15 Aruba

16 RSA

Gold

17 Sidertia

18 Tenable

19 Akamai

20 Cybereason

21 Netskope

22 Accenture Security

23 One Identity

24 S21sec

25 Radware

26 Microfocus

27 McAfee

28 Autek

29 Forcepoint

30 Thycotic

31 Kaspersky

32 Telefónica

MADRID
11 Y 12 DE DICIEMBRE

ccn-cert
centro criptológico nacional

WWW.CCN-CERT.CN.ES

WWW.CCN.CN.ES

OC.CCN.CN.ES



STREAMING EN ABIERTO - PLENARIAS

Plenarias 11 y 12 diciembre

ESPAÑOL: <https://www.ccn-cert.cni.es/xiii-jornadas-streaming.html>

INGLÉS: <https://www.ccn-cert.cni.es/en/xiii-conference-streaming.html>



#XIIIJornadasCCNCERT

COLABORACIONES MÓDULOS



/Rooted[®]CON



APP 13 JORNADAS CCN



- Agenda
- Mi propia agenda
- Ponentes
- Preguntas
- Encuesta
- Más información



PROGRAMA XIII JORNADAS STIC CCN-CERT

1º DÍA – 11 DE DICIEMBRE

07:15	Recogida de acreditaciones y recepción de autoridades Café						
SESIÓN PLENARIA (Sala Entelgy Innotec Security-25)							
09:00 09:35	Inauguración por autoridades						
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)						
	Módulo 1: Sala Entelgy Innotec Security-25 AMENAZAS, ATAQUES Y RETOS TECNOLÓGICOS	Módulo 2: Sala ESET-19 ENS y CUMPLIMIENTO NORMATIVO	Módulo 3: Sala Cytomic-18 PREVENCIÓN EN CIBERSEGURIDAD / SOLUCIONES TECNOLÓGICAS	Módulo 4: Sala 17 ATENEA	Módulo 5: Sala Ingenia-16 OPERACIONES MILITARES EN EL CIBERESPACIO	Módulo 6: Sala Microsoft-20 REDES OPERACIONALES / CONTROL INDUSTRIAL	Módulo 7: Sala 21 OBSERVATORIO DIGITAL. ELISA

	Módulo 1: Sala Entelgy Innotec Security-25 AMENAZAS, ATAQUES Y RETOS TECNOLÓGICOS	Módulo 2: Sala ESET-19 ENS y CUMPLIMIENTO NORMATIVO	Módulo 3: Sala Cytomic-18 PREVENCIÓN EN CIBERSEGURIDAD / SOLUCIONES TECNOLÓGICAS	Módulo 4: Sala 17 ATENEA	Módulo 5: Sala Ingenia-16 OPERACIONES MILITARES EN EL CIBERESPACIO	Módulo 6: Sala Microsoft-20 REDES OPERACIONALES / CONTROL INDUSTRIAL	Módulo 7: Sala 21 OBSERVATORIO DIGITAL. ELISA
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)	Peculiaridades del combate en el ciberespacio (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	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)		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	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)	Vientos remotos, tempestades locales: Análisis forense de incidentes con accesos remotos (Antonio Sanz, S2 Grupo)	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	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)		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)
14:00 15:30	Vino español						

14:00 15:30	Vino español						
	Módulo 1: Sala Entelgy Innotec Security-25 AMENAZAS, ATAQUES Y RETOS TECNOLÓGICOS	Módulo 2: Sala ESET-19 ENS y CUMPLIMIENTO NORMATIVO	Módulo 3: Sala Cytomic-18 PREVENCIÓN EN CIBERSEGURIDAD / SOLUCIONES TECNOLÓGICAS	Módulo 4: Sala 17 ATENEA	Módulo 5: Sala Ingenia-16 OPERACIONES MILITARES EN EL CIBERESPACIO	Módulo 6: Sala Microsoft-20 REDES OPERACIONALES / CONTROL INDUSTRIAL	Módulo 7: Sala 21 OBSERVATORIO DIGITAL. ELISA
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)	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: Revista SIC
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)		OrangeWorm: How I met your master... (Pablo Rincón, Cylera)	Ciberseguridad Industrial: errores cometidos y cambios a aplicar (Edorta Echave, Secure&IT)	

Fuera de programa

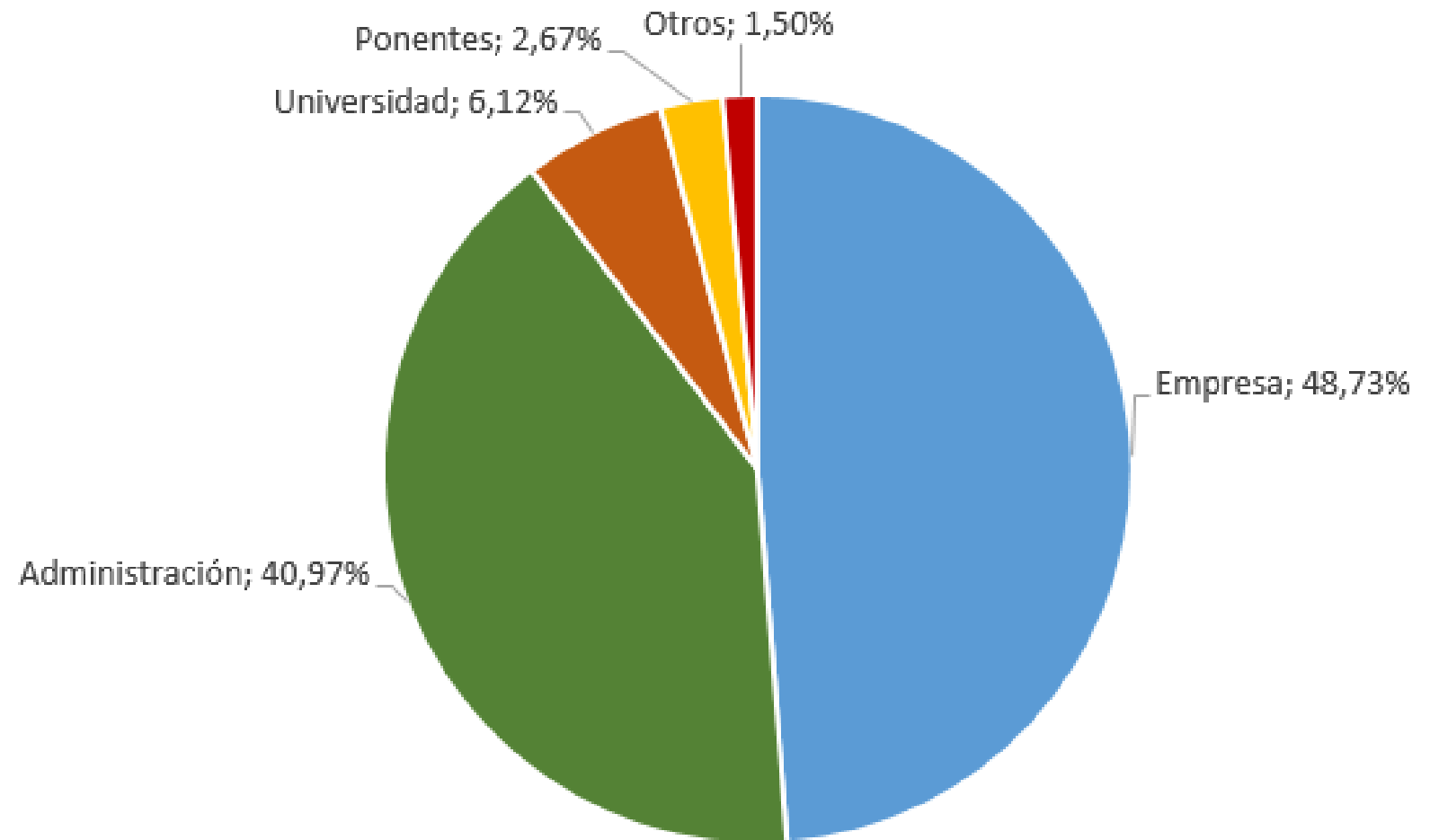
Sala Entelgy Innotec Security-25	Sala ESET-19	Sala Cytomic-18	Sala ATENEA-17	Sala Ingenia-16	Sala Microsoft-20	Sala 21
---	---------------------	------------------------	-----------------------	------------------------	--------------------------	----------------

	Sala Entelgy Innotec Security-25	Sala ESET-19	Sala Cytomic-18	Sala ATENEA-17	Sala Ingenia-16	Sala Microsoft-20	Sala 21
16:45 17:05	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, S2 Grupo)	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)
17:10 17:25	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)	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)
17:30 17:45	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)		¿Ahorrar y facilitar la vida del SOC es posible? RSA	

08:00 09:00	Recogida de acreditaciones Café						
	Módulo 1: Sala Entelgy Innotec Security-25 AMENAZAS, ATAQUES Y RETOS TECNOLÓGICOS	Módulo 2: Sala ESET-19 ENS y CUMPLIMIENTO NORMATIVO	Módulo 3: Sala Cytomic-18 PREVENCIÓN EN CIBERSEGURIDAD / SOLUCIONES TECNOLÓGICAS	Módulo 4: Sala 17 ATENEA	Módulo 5: Sala Ingenia-16 OPERACIONES MILITARES EN EL CIBERESPACIO	Módulo 6: Sala Microsoft-20 REDES OPERACIONALES / CONTROL INDUSTRIAL	Módulo 7: Sala 21 OBSERVATORIO DIGITAL. ELISA
09:00 09:30	Evolución del malware bancario y ataques dirigidos a usuarios en España (Josep Albors, ESET)	Framework auditoría - ANA Central (CCN-CERT)	La amenaza cuántica, ¿hay cripto después? (Luis Hernández y Víctor Gayoso, ITEFI - CSIC)	Remote Code Execution in restricted environments (Borja Merino, Tarlogic)	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	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=	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	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)		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	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)	Comunicaciones móviles para gestión de crisis. Caso ejército de Finlandia (Laura Casadevall, Bittium Wireless)		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)
11:15 11:45	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 (Álvaro y Carlos Abad , CCN-CERT)
13:35 13:45	Entrega premio a la trayectoria profesional en favor de la ciberseguridad del CCN
13:50 14:00	Clausura

ASISTENTES**SOLICITUDES****3800+****INSCRITOS****3593****ORGANIZACIONES
REPRESENTADAS****1053**

**XIII
JORNADAS
STIC
CCN-CERT**



RETOS 2020

**COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD**

#XIIIJORNADASCCNCERT

Retos 2020



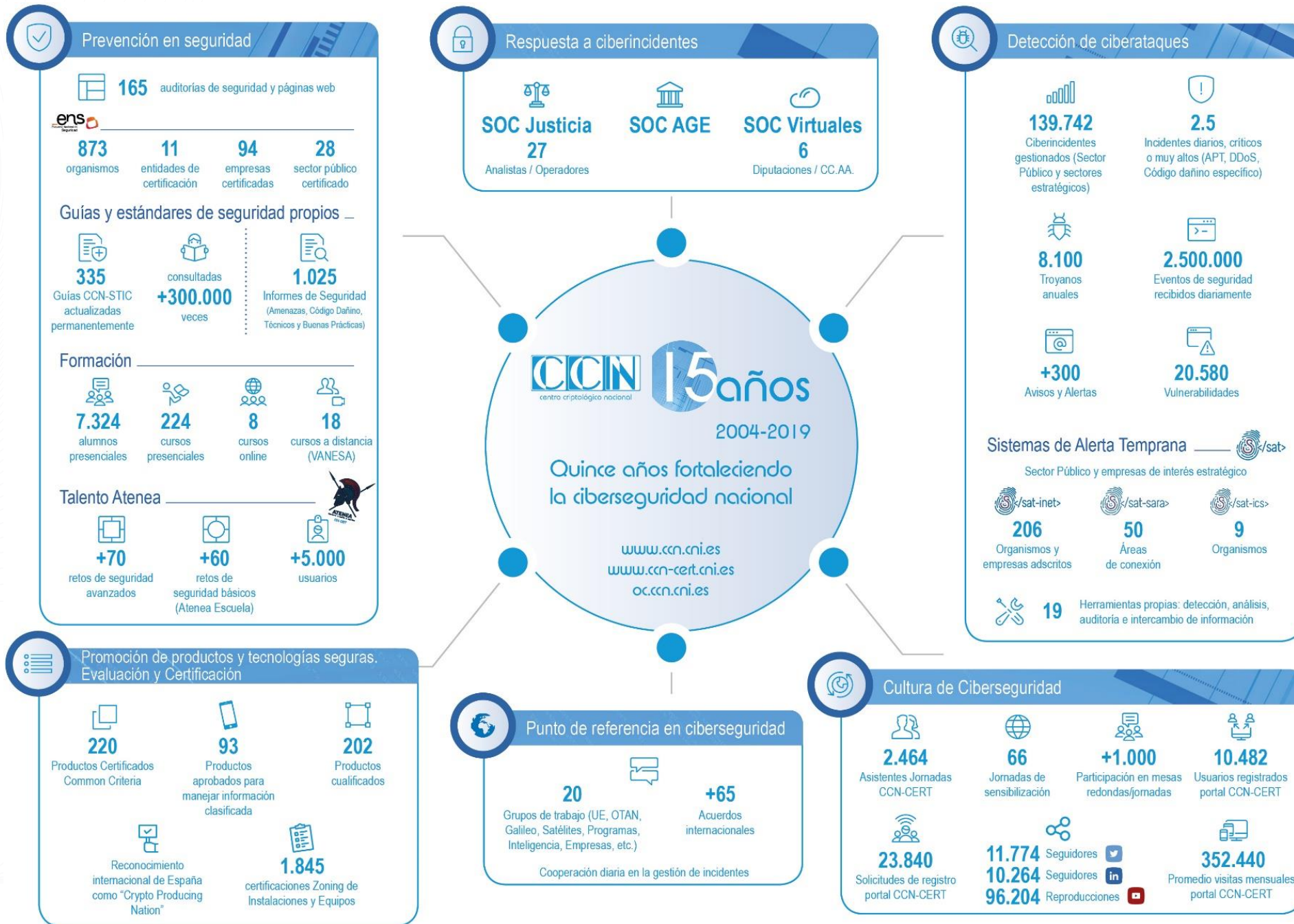
Javier Candau

Jefe Departamento
Ciberseguridad

Centro Criptológico
Nacional.



-  Mandar
-  Coordinar
-  Colaborar
-  Cooperar
-  Informar
Notificar



XIII JORNADAS STIC CCN-CERT

COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD
#XIIIJORNADASCNCERT

MADRID
11 Y 12 DE DICIEMBRE



WWW.CCN-CERT.CN.ES
WWW.CCN.CN.ES
OC.CCN.CN.ES

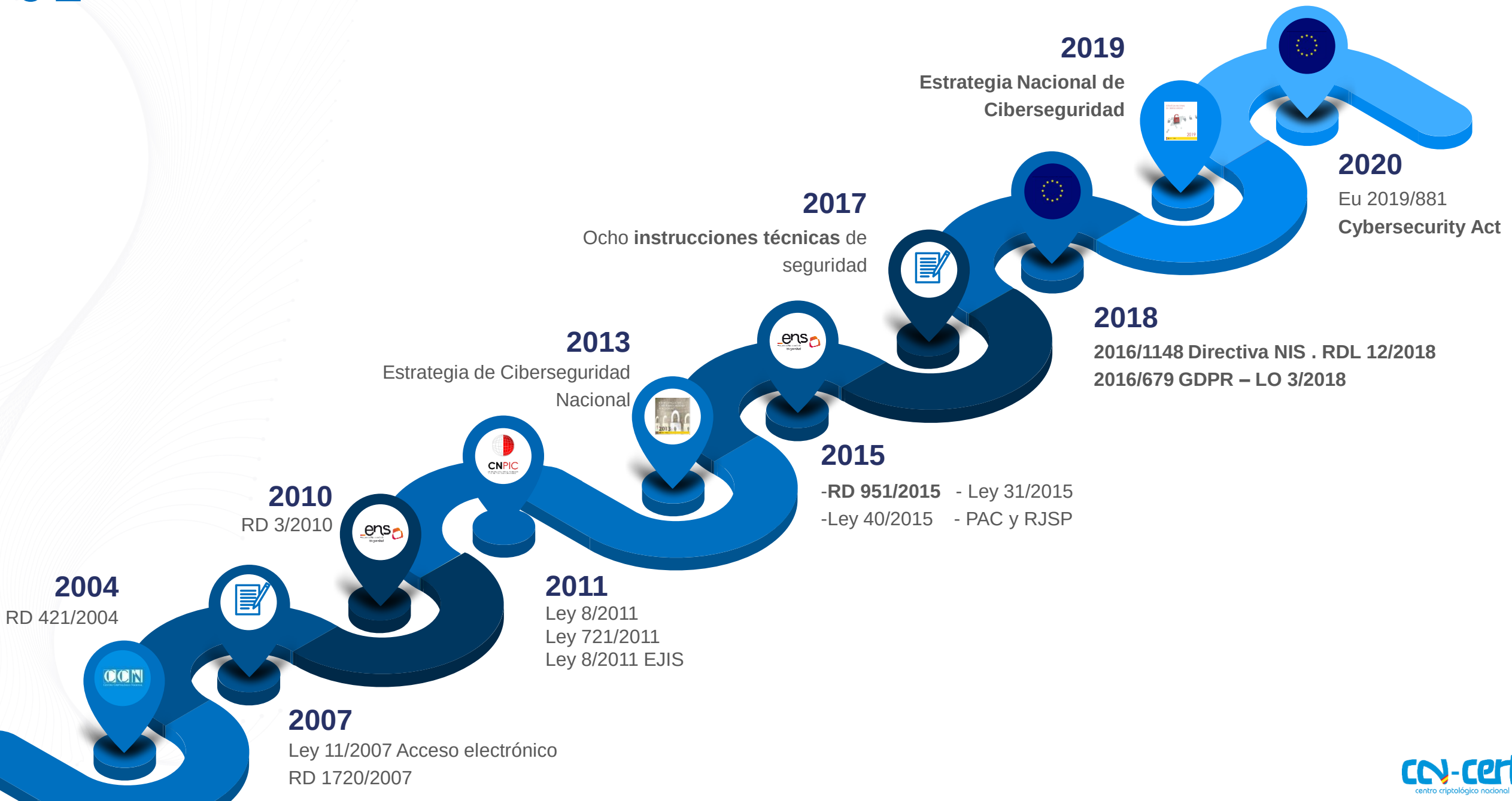


Índice

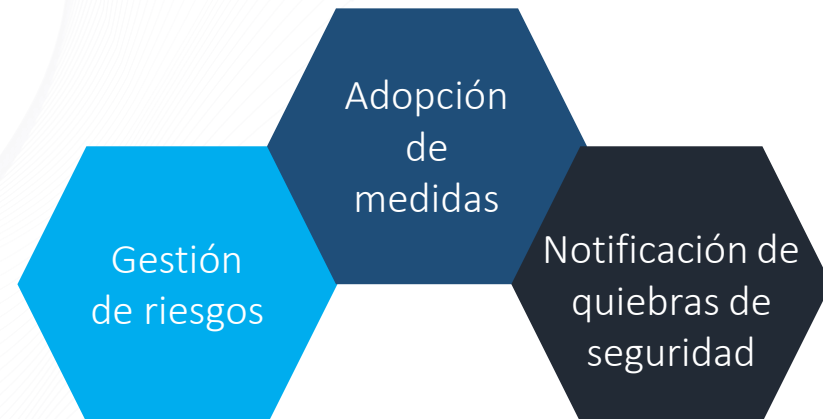
- 01 LEGISLACIÓN RELEVANTE
- 02 CCN. NUEVOS PROCEDIMIENTOS
- 03 REDUCIR LA SUPERFICIE DE EXPOSICIÓN
- 04 VIGILANCIA CONTINUA
- 05 RESPUESTA EFICIENTE
- 06 LECCIONES APRENDIDAS / APOYOS 2019
- 07 PRODUCTOS Y CATÁLOGO
- 08 RETOS 2020

01 Novedades Normativas

#XIIIJORNADASCCNCERT

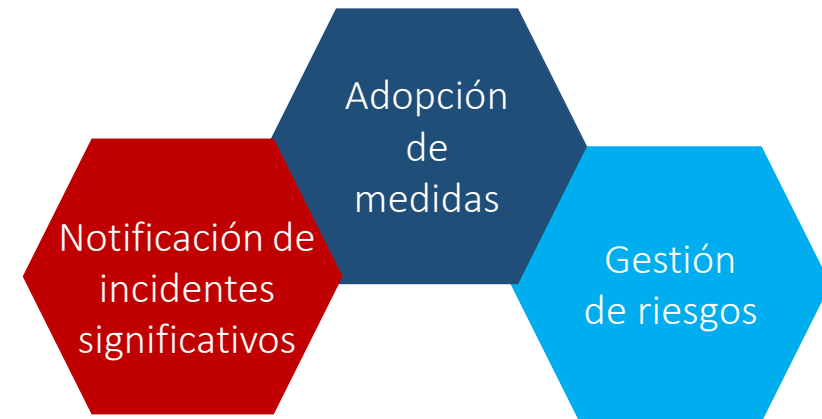


2016/679 GDPR –LO 3/2018



Disposición adicional primera.
Medidas de seguridad en el
ámbito del sector público.
APLICAR EL ENS

2016/1148 Directiva NIS – RDL 12/2018



ESTRATEGIA NACIONAL DE CIBERSEGURIDAD

CIBERSEGURIDAD



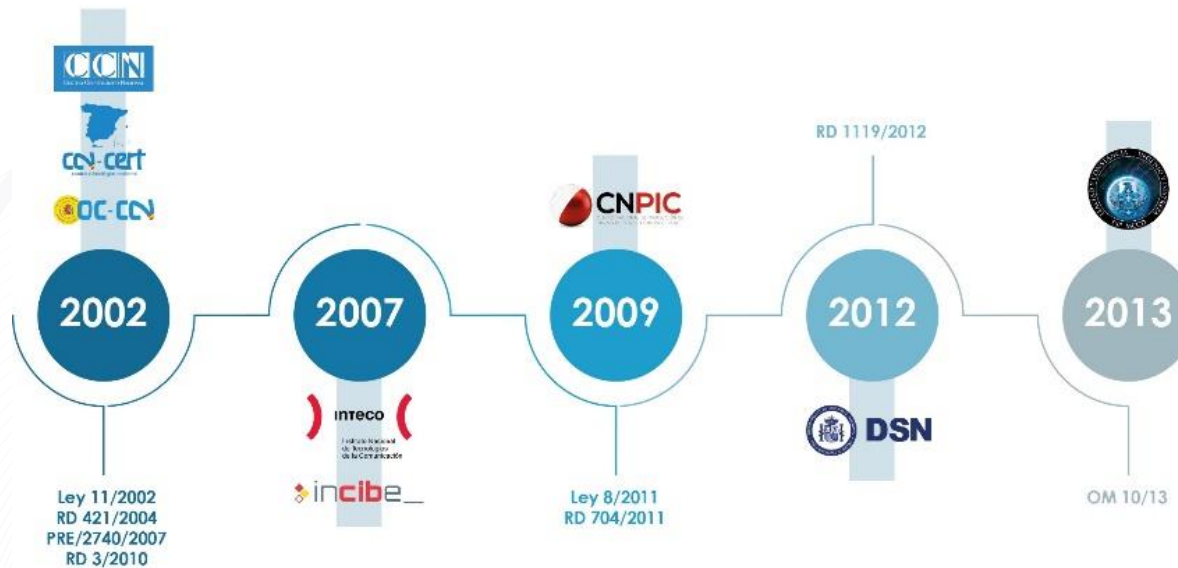
2019

ENCS 2019

- **Nuevos objetivos.** ¿Hemos cumplido con la ECSN 2013?
- Continuista en objetivos, líneas de acción y **modelo de gobernanza**
- Necesidad de fondos e impulso político para el sector público. **Medidas de Defensa ACTIVA**
- España, pionera en los campos de **gestión de riesgos, medidas de seguridad y notificación de incidentes.**
- La **desinformación** es el nuevo frente

Comisión permanente

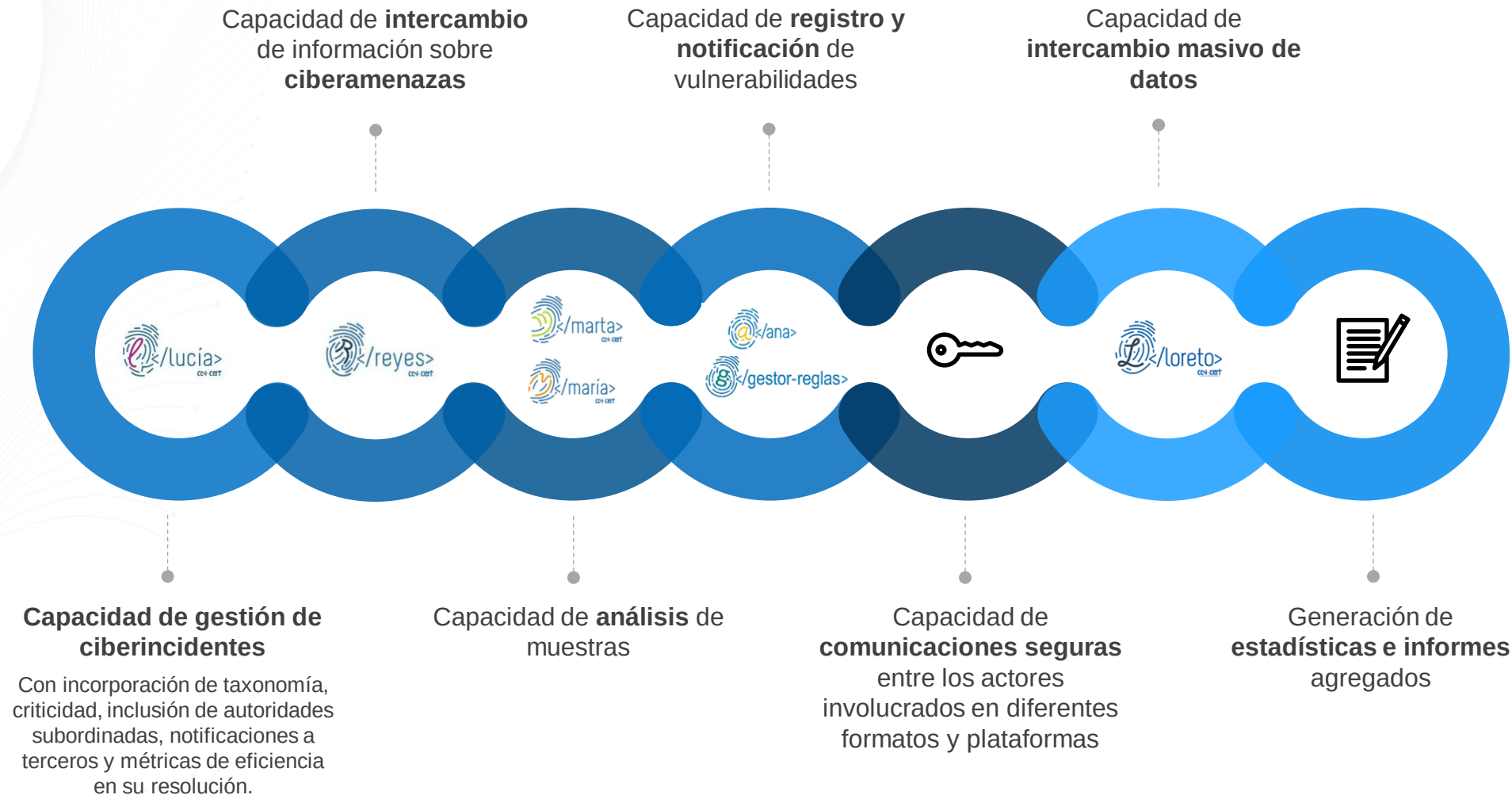
Actores en la Ciberseguridad Nacional



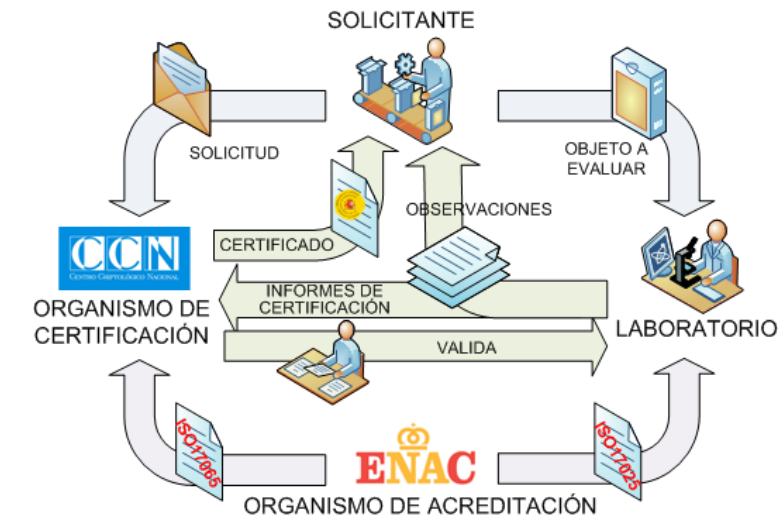
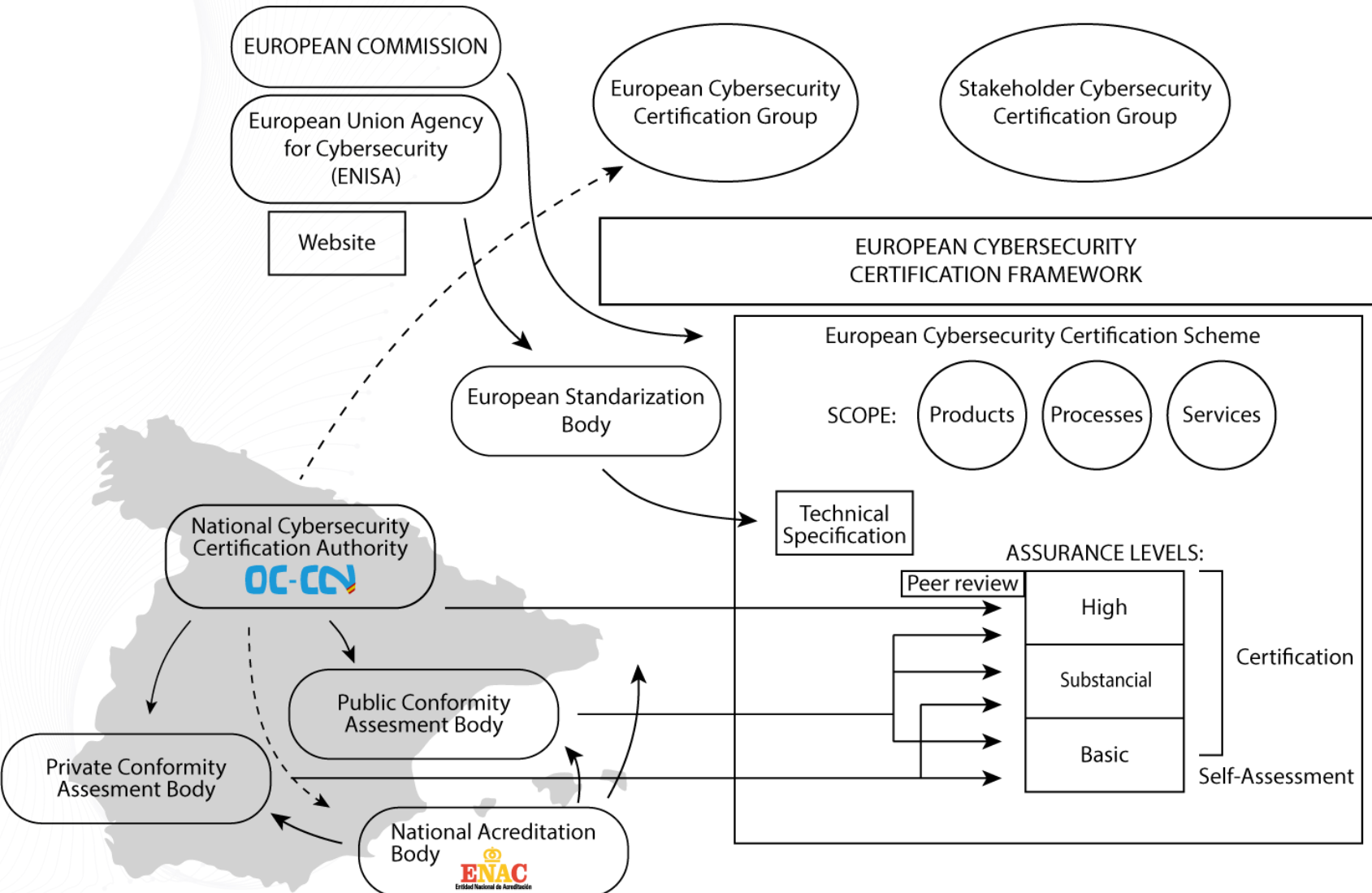
- **Flexible** en coordinación y organización
- Sin TOR claros, pero **integra capacidades**
- Definir **necesidades de información**
- Ha tratado **incidentes críticos** y **situaciones de alerta.**



incibe

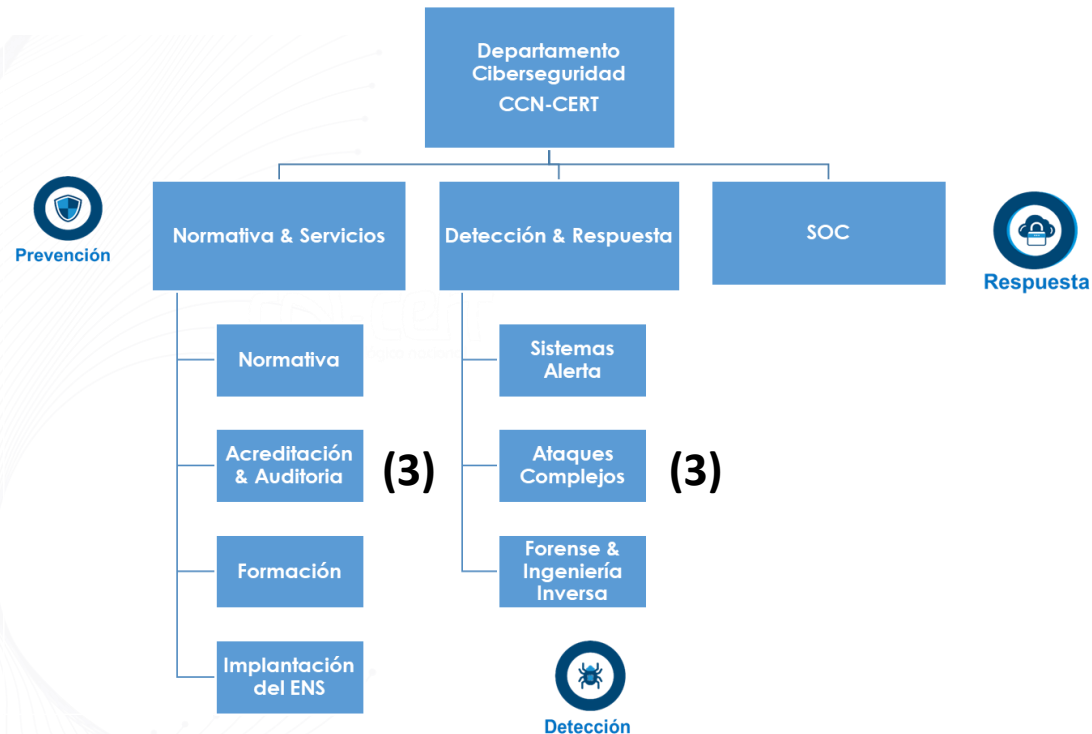


01 Marco Europeo de certificación



MISIÓN

Contribuir a la mejora de **la ciberseguridad española**, siendo el centro de alerta y respuesta a incidentes que coopere y ayude a responder de forma rápida y eficiente al sector público a afrontar de forma activa las nuevas ciberamenazas.



Necesidad de un modelo distribuido



Prevenición

Reducir la superficie de exposición



Detección

Vigilancia continua



Respuesta

Respuesta eficiente

02 Nueva soluciones

Auditoría



Detección



Intercambio



02 Nueva soluciones

#XIIIJORNADASCCNCERT



Vigilancia



Análisis



Formación





Medir y Determinar Superficie de Exposición

Logos: /ana>, /amparo>, /clara>, /rocío>, /emma>, /pilar>, and /lucía> (highlighted in red).

ES
ENTORNO DE SUPERFICIE DE EXPOSICIÓN

Medir y Explotar Información (Adecuación al ENS)

Logos: /inés>, /clara>, /pilar>, /ana>, /amparo>, /lucía> (highlighted in red), /rocío>, and /emma>. Includes the RGPD logo.

e-ens
ENTORNO DE VALIDACIÓN ENS

Logos: /pilar>, /gloria>, /lucía> (highlighted in red), /claudia>, /carmen>, /sat-ics>, /sat-inet>, /sat-sara>, /marta>, and /maria>.

SOC AGE SOC SGNTJ **vSOC**

Cyber situational Awareness

World map showing risk levels: High (40%), Medium (12), Low (04), and Commitments (07).

e-/elisa>
Estudio Simplificado de fuentes abiertas

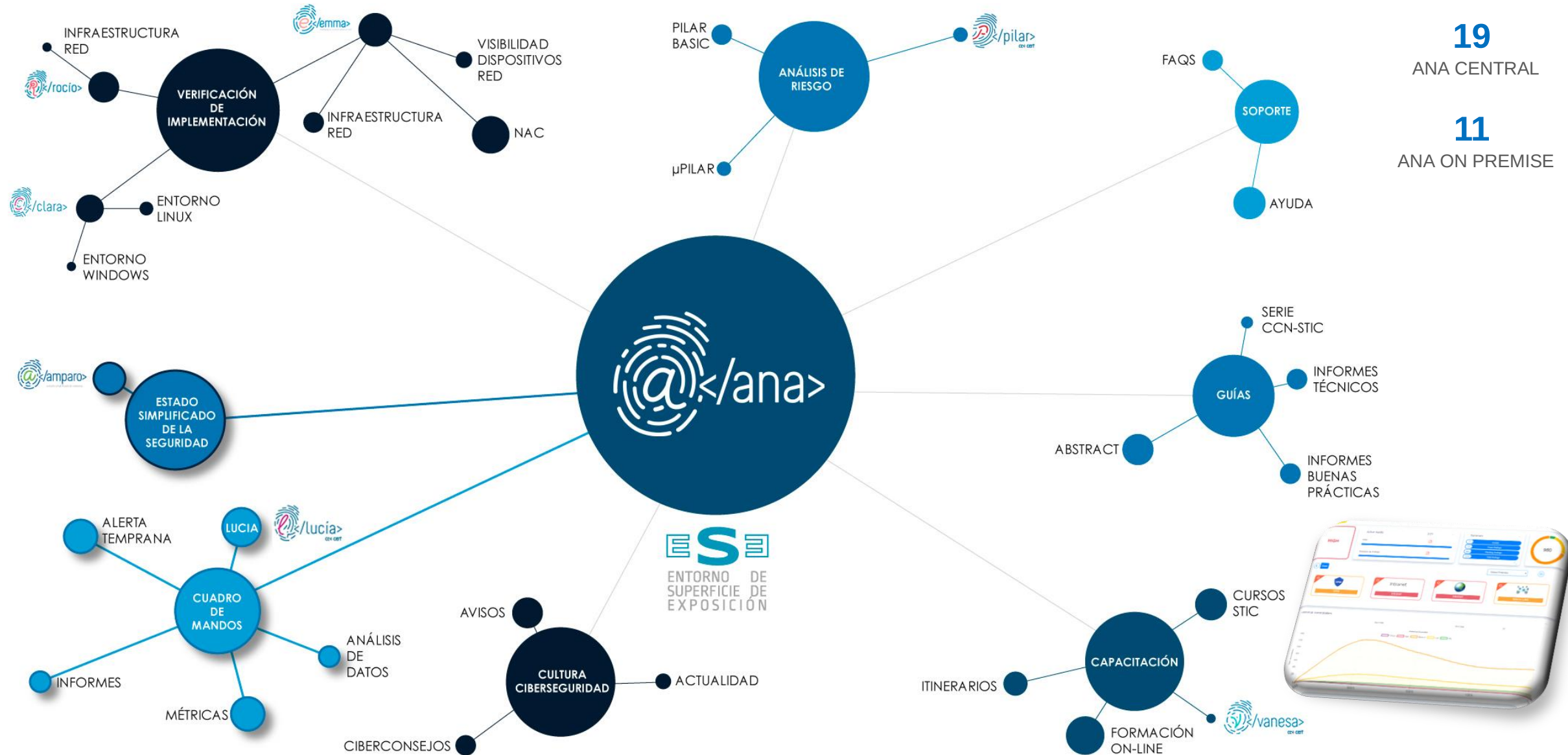
ESTUDIO SIMPLIFICADO DE FUENTES ABIERTAS

e-/elisa>
Estudio Simplificado de fuentes abiertas v0.5.1

Observatorio Digital

CEF 2019

03 Medir la superficie de exposición



19

ANA CENTRAL

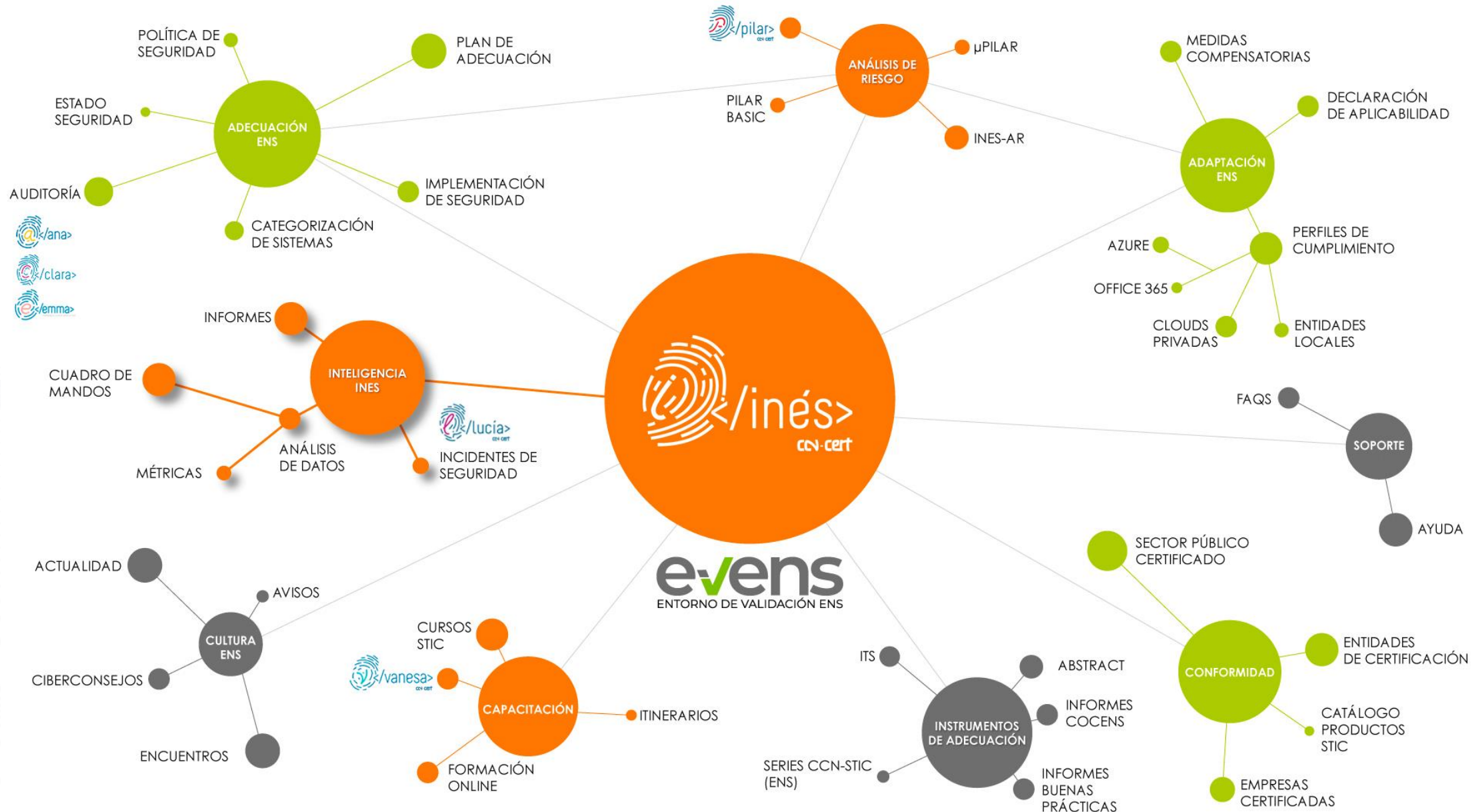
11

ANA ON PREMISE



03 Propiciar Cumplimiento del ENS

#XIIJORNADASCCNCERT



+950
ORGANISMOS

199
AGE

144
CCAA

557
EELL

61
UNIVERSIDADES

En 2018

51,1%
INDICE MADUREZ

68,9%
I. CUMPLIMIENTO

03 Reducir la superficie de exposición

Formación presencial



21 + 7 (600)
cursos presenciales

Formación online



21 (+4.000)
cursos a distancia

Informes elaborados

26
Informes de
Código Dañino

41
Guías Nuevas /
Actualizadas

6
Informes de
Buenas Prácticas

81
Informes
Técnicos

73
Informes de
Amenazas

Cifras totales informes

227
Informes elaborados

1.200.000
descargas

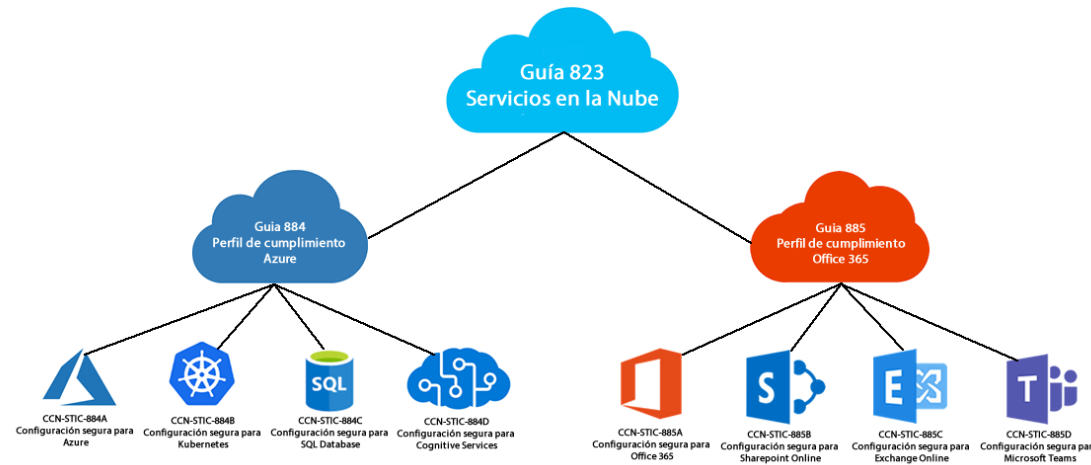
ATENEA



+9.200
usuarios

101
Retos de seguridad

Adaptación a los Servicios en Nube





228

organismos y
empresas adscritos

36

nuevos organismos
adscritos en 2019



50

Áreas de
conexión



12/15

entidades



carmen
Ciberinteligencia
Avanzada

42

Implantaciones en
organismos y empresas



carmen
central

27

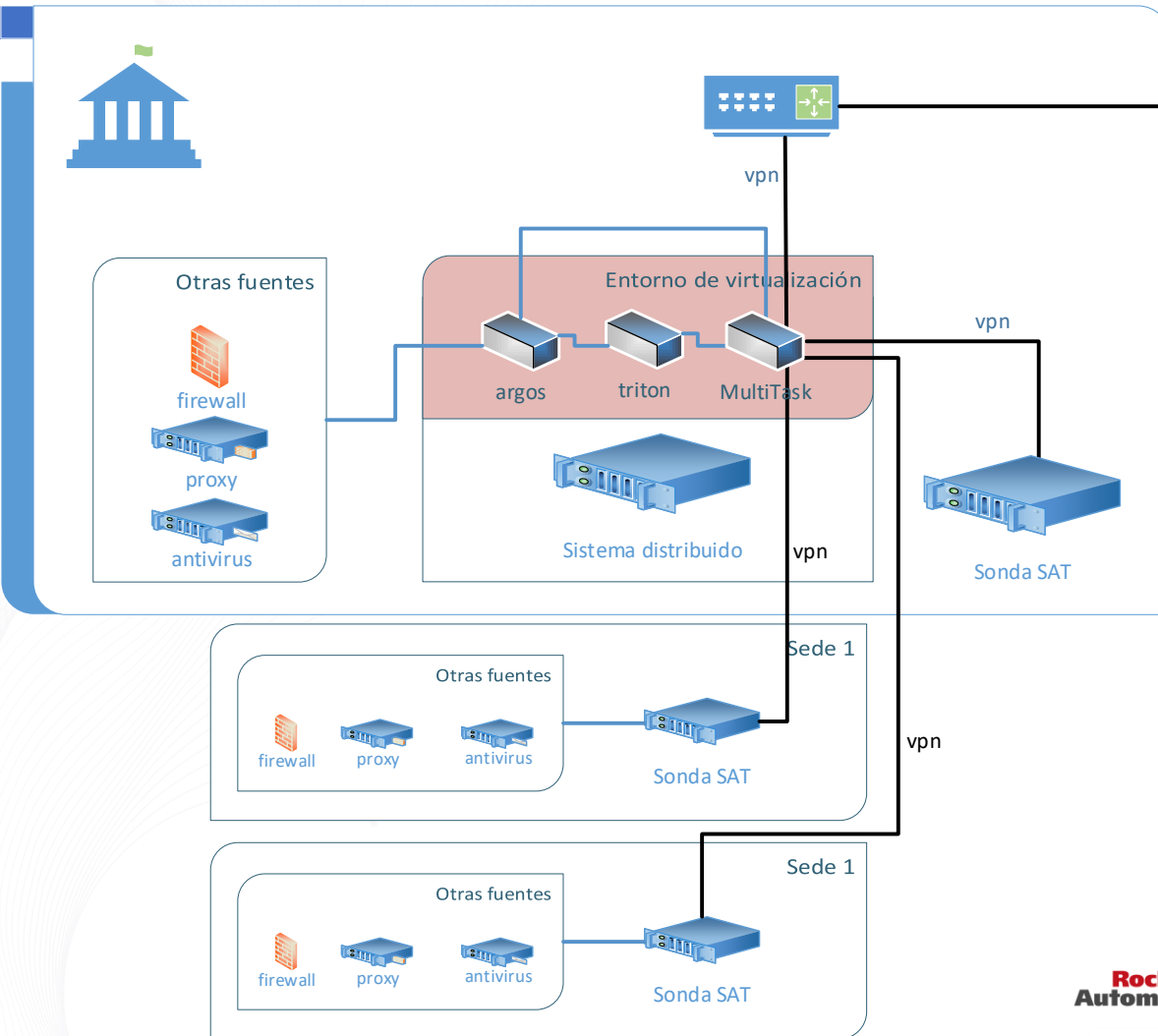
Integraciones con
CARMEN Central

12

Despliegues en
servidores y puestos
usuarios



04 Vigilancia continua. Sonda distribuida



Aumentar las capacidades de monitorización.
Incluir nuevas fuentes

Arquitectura multinivel y/o centralizada. Se adapta a las necesidades de la entidad.

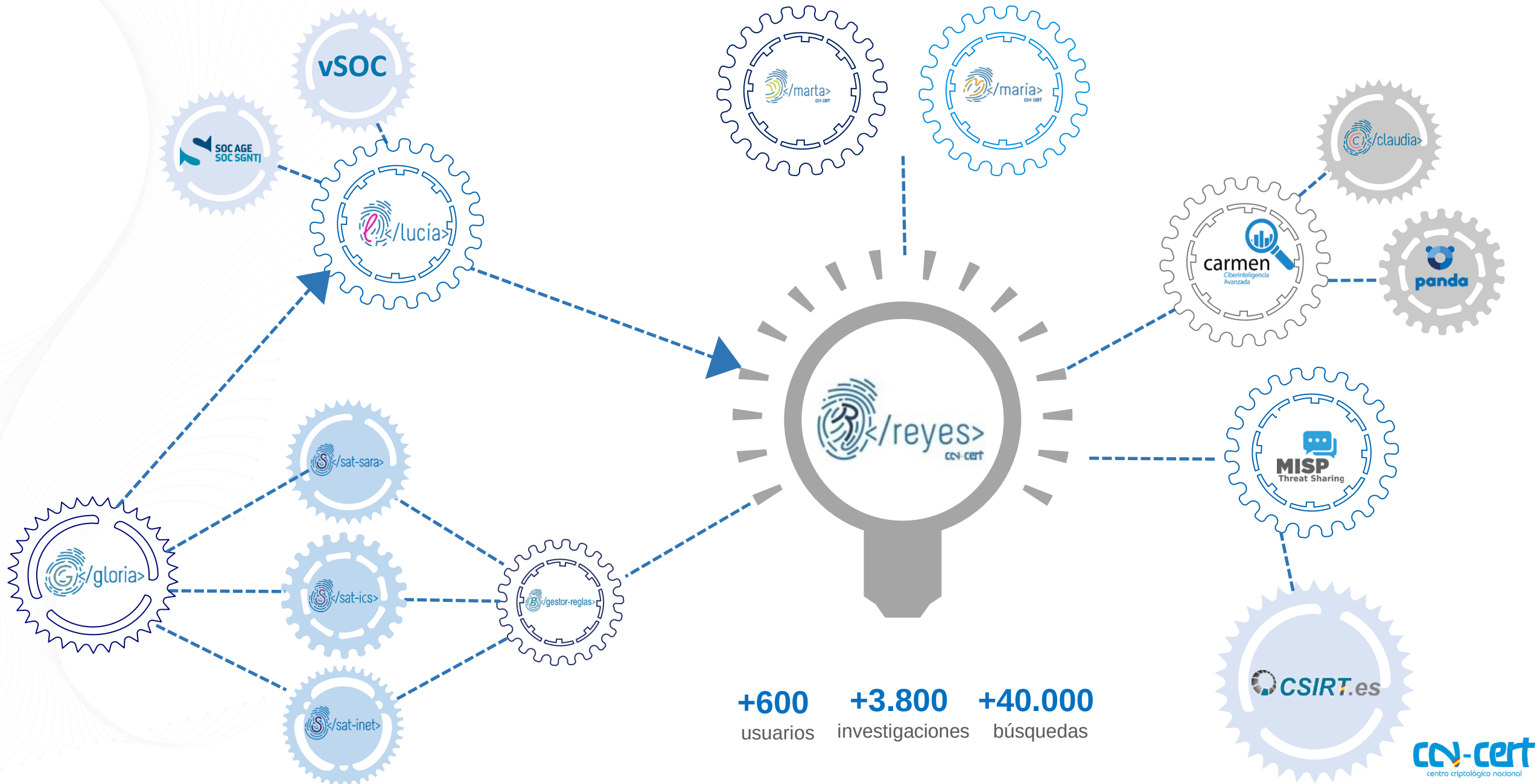
En 2020. Delegación de la gestión de la sonda



- Identificación activos
- Disección de protocolos (17)



04 Vigilancia continua. Sistema de trabajo



Cómo utilizar la matriz de clasificación

1. Evaluar el efecto conocido o probable del incidente:

- La naturaleza de lo que está ocurriendo y el efecto en el sistema o sistemas de destino
- Si los efectos son continuos, empeoran o se mueven lateralmente
- La importancia de los sistemas, servicios o datos de destino
- Considerar la atribución (capacidad e intención) o cualquier interés operativo

2. Evaluar la(s) víctima(s) del incidente:

- El número de víctimas
- La relevancia de la(s) víctima(s)
- Considerar tanto a las víctimas primarias como a las secundarias

3. En situaciones excepcionales, añade un indicador ALTO o CRÍTICO:

- Puede ser aplicado a cualquier categoría o incidente
- Se utiliza en circunstancias excepcionales cuando se requieren mayores recursos o una respuesta rápida de emergencia

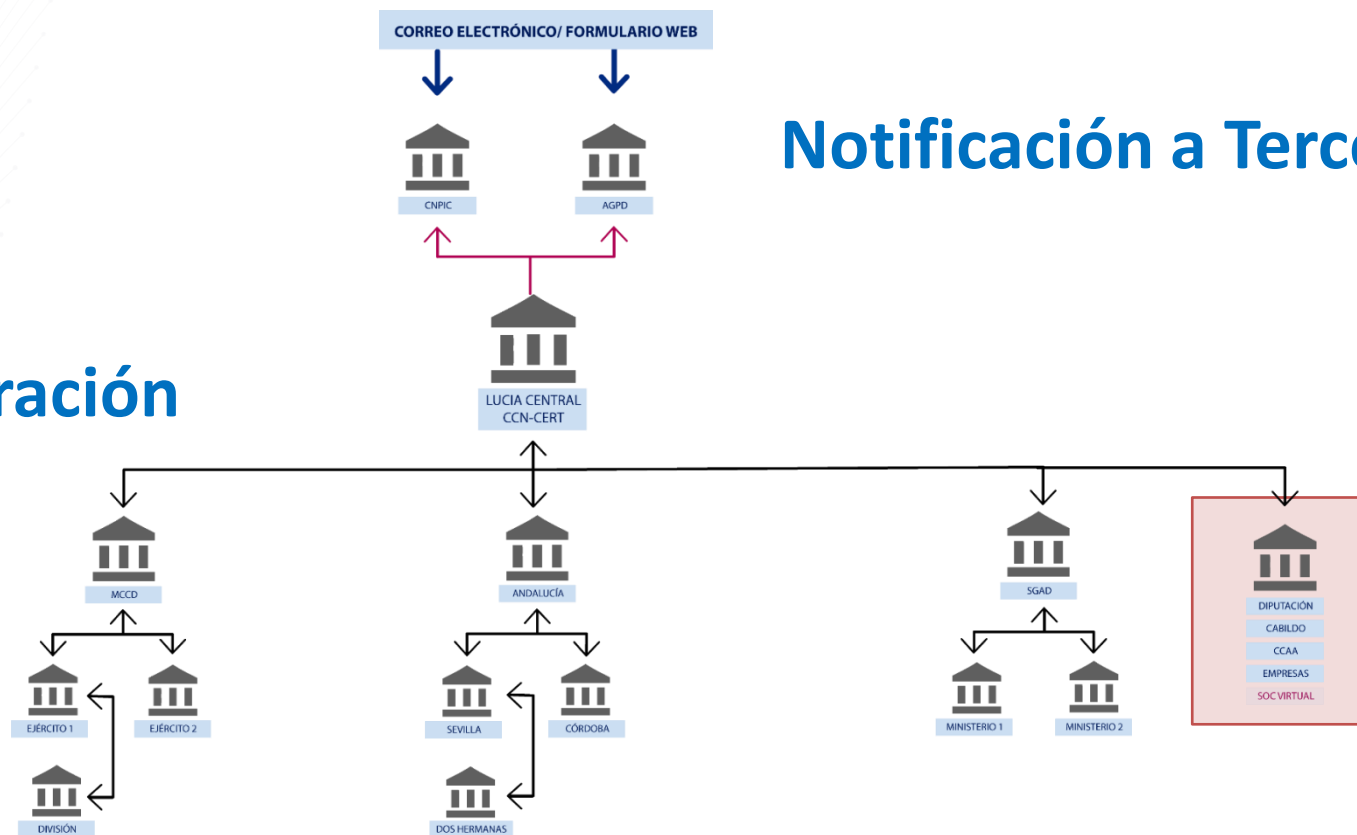


Cómo utilizar la matriz de clasificación

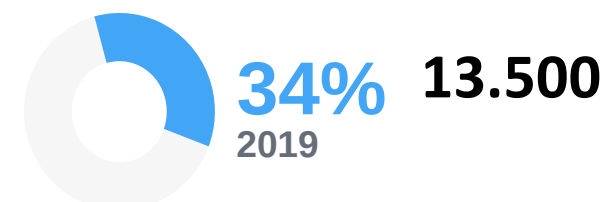
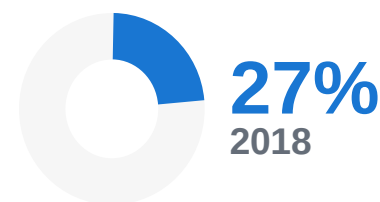
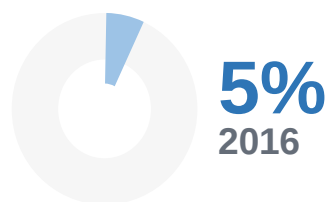
Federación

Notificación a Terceros

Multientidad



Evolución de incidentes
aportados por organismos



13.500

04 Vigilancia continua. Mejoras en Notificación



Mejora [01]

Remodelación del protocolo de sincronización

Segmentación del protocolo de comunicación y sincronización. **Tipología integrable en vSOCs.**



Mejora [02]

Modularización de LUCIA

Herramienta totalmente parametrizable e integrable en diferentes entornos, tanto de Administración Pública como empresariales.



Mejora [03]

Integración con SIEM



Mejora [04]

Mejoras en manejo de incidentes



Mejora [05]

Intercambio de información e integración con European Cybersecurity CSP



Mejora [06]

Interconexión con soluciones CCN-CERT INES, ANA, GLORIA



Organismos en
LUCÍA Central



Organismos Federados
a 31 diciembre

05 Respuesta eficiente. CEF 2019

#XIIJORNADASCNCERT



05 Respuesta eficiente. SOCs



Servicios de seguridad gestionada por empresas



Conexión a REYES y LUCIA



Concentrar el conocimiento

vSOC Inicial

- Notificación de incidentes.
- Avisos y alertas.

vSOC

- Actuación sobre el perímetro ante incidentes.
- Capacidad forense e investigación remota.
- Control de equipos infectados.

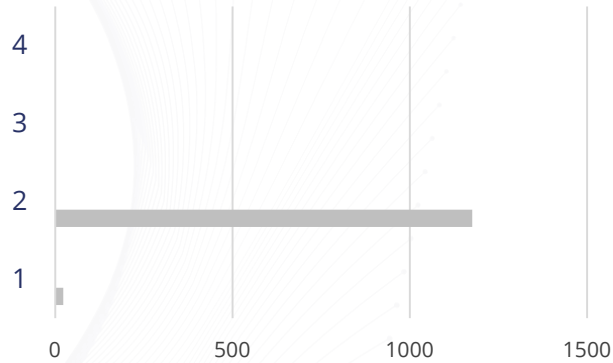
vSOC Avanzado

- Actuaciones / inspecciones técnicas.
- Evaluación y conocimiento del estado de seguridad.
- Valoración de la exposición.



06 Lecciones aprendidas

+37.000 Incidentes gestionados en 2019

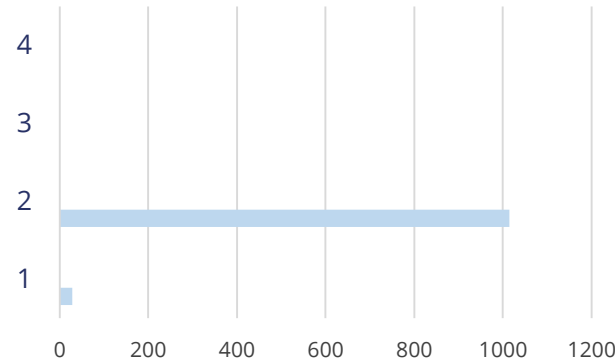


2017 —

24 incidentes Críticos

1.152 incidentes Muy altos

17 Intervenciones

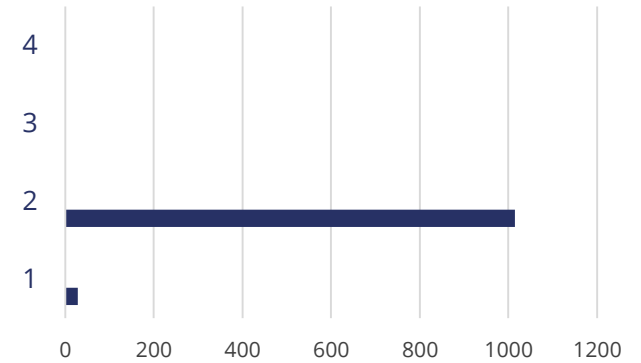


2018 —

29 incidentes Críticos

1.014 incidentes Muy Altos

21 Intervenciones



2019 —

36 incidentes Críticos

1.800 incidentes Muy Altos

37 Intervenciones



Lección [1]

Necesidad de despliegue de herramientas en incidentes Críticos y Muy Altos



Lección [2]

Mayor cantidad de solicitudes de apoyo presencial



Lección [3]

Técnicas de ataques complejos en cibercrimen



Lección [4]

El antivirus **NO** es suficiente

+30

Organismos afectados

Deficiencias encontradas

- Redes NO segmentadas
- Red interna sin vigilancia
- Reutilización de contraseñas
- Sistemas obsoletos
- Sin actualizaciones de seguridad
- Poco/Nulo personal de seguridad TIC
- Todo el back-up conectado a la red

Plan de recuperación

- Vacuna + Punto final
- Segmentar la red
- SAT INTERNET
- Servicio de seguridad gestionada




ALERTA

Campaña troyano EMOTET

Fecha de publicación: 07/10/2019
Nivel de peligrosidad: Muy alta

El Equipo de Respuesta a Incidentes del Centro Criptológico Nacional, **CCN-CERT**, alerta a su Comunidad de una campaña muy agresiva de ataques del troyano **EMOTET** contra los usuarios finales. Aunque EMOTET tiene diferentes módulos y funcionalidades, su objetivo en esta ocasión está siendo el robo de credenciales bancarias pero, por su funcionamiento, no se descarta que pudiera cambiar su finalidad.

La campaña comenzó a mediados de septiembre y se distribuye a través de correos electrónicos que tienen un documento ofimático (Word) con macros que, al ser activadas, infectan el equipo. Los correos electrónicos suelen llevar algún asunto genérico para evitar ser sospechosos: "Propuesta", "Respuesta", "Privacidad" o "Nueva Plantilla".

Sistemas afectados

Cualquier versión de Microsoft Windows.

Medidas de prevención

Para prevenir la infección para esta campaña concreta se pueden seguir las siguientes recomendaciones:

- Instalación de la herramienta EMOTET-stopper en todos los equipos Windows a proteger, disponible desde el siguiente enlace: <http://ccn-cert.net/emotet2019>. Se deberán habilitar los mecanismos necesarios para que se ejecute tras cada reinicio. En caso de que el Antivirus o Sistema Operativo detecten la herramienta como código dañino, se deberá excepcionar para evitar su eliminación. La herramienta se ejecuta en segundo plano por lo que solo se verá desde el Administrador de tareas.
- Dado que el vector principal de infección de esta campaña de EMOTET es el correo electrónico, recomendamos revisar la Guía de Buenas Prácticas del CCN-CERT sobre dicha temática: <http://ccn-cert.net/bpmail>.
- Dado que el vector principal de infección de esta campaña de EMOTET es el correo electrónico, recomendamos revisar la Guía de Buenas Prácticas del CCN-CERT sobre dicha temática.
- De la misma manera se recomienda deshabilitar Powershell en aquellos equipos en los que no sea necesaria la ejecución de comandos en dicho lenguaje.
- El CCN-CERT ha recopilado en 3 listas negras los indicadores que permiten la detección y bloqueo de gran parte de esta campaña: listas de IP, dominios y hashes de las muestras empleadas. Pueden descargar dichas listas aquí: <http://ccn-cert.net/emotet-ioc>.
- EMOTET puede desplegar el troyano bancario Trickbot para robo información, seguido en última instancia del ransomware Ryuk sobre los equipos infectados. Actualmente no existe forma de descifrar los ficheros afectados por esta familia. Recomendamos la lectura de la Guía de Buenas Prácticas sobre Ransomware que el CCN-CERT ha elaborado: <http://ccn-cert.net/bpransomware>.
- Mantener el Sistema Operativo, el antivirus actualizado y disponer de copias de seguridad *offline* (sin conexión con la red).

Medidas de detección

- Para contrarrestar los efectos de esta campaña, el CCN-CERT recomienda la búsqueda en la red de los Indicadores de Compromiso (IOC). Concretamente se debe realizar la búsqueda en los registros de conectividad (proxy/firewall/DNS) para comprobar si ha existido conectividad con los dominios o IP incluidos en las listas negras (<http://ccn-cert.net/emotet-ioc>).
- Para la detección en los equipos se puede utilizar las siguiente regla YARA: <http://ccn-cert.net/emotet-yara>

Medidas de mitigación

- Utilizar los indicadores proporcionados para identificar qué equipos se encuentran afectados por la campaña.
- Sobre dichos equipos se deberá realizar una copia de seguridad de la información, incluso



USO OFICIAL



Informe Código Dañino
CCN-CERT ID-24/19

TrickBot



USO OFICIAL



Informe Código Dañino
CCN-CERT ID-25/19

"Ryuk"



06 Apoyos relevantes

#XIIJORNADASCCNCERT



Apoyos Incidentes en
Iberoamérica



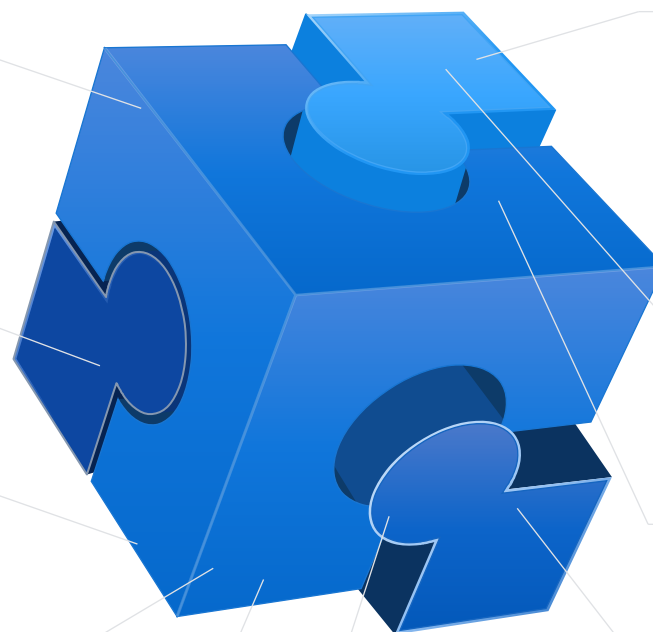
CSIRT de Chile.
Vigilancia Digital

Elecciones El Salvador



Apoyos CC.AA y AGE

Apoyos Empresas
Estratégicas



Difusión Cultura Ciberseguridad en
Iberoamérica y Norte de África



**Elecciones Generales.
Abril 2019**

**Elecciones Europeas
CC.AA. y locales.
Mayo 2019**

**Elecciones Generales
Noviembre 2019**

**Cumbre del Clima
Noviembre 2019**

2019



Nuevos
Requisitos fundamentales
de seguridad

ENS categoría media y básica



2020

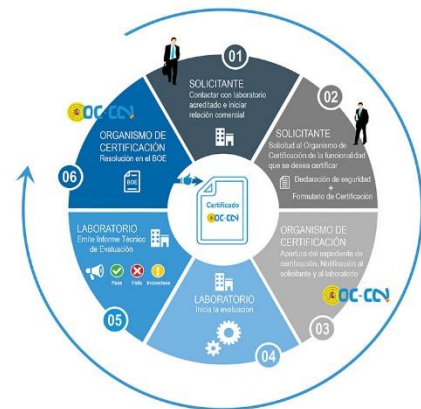


Cualificación de
Servicios en la nube

Incrementar número de
productos

nuevas **Familias de productos**

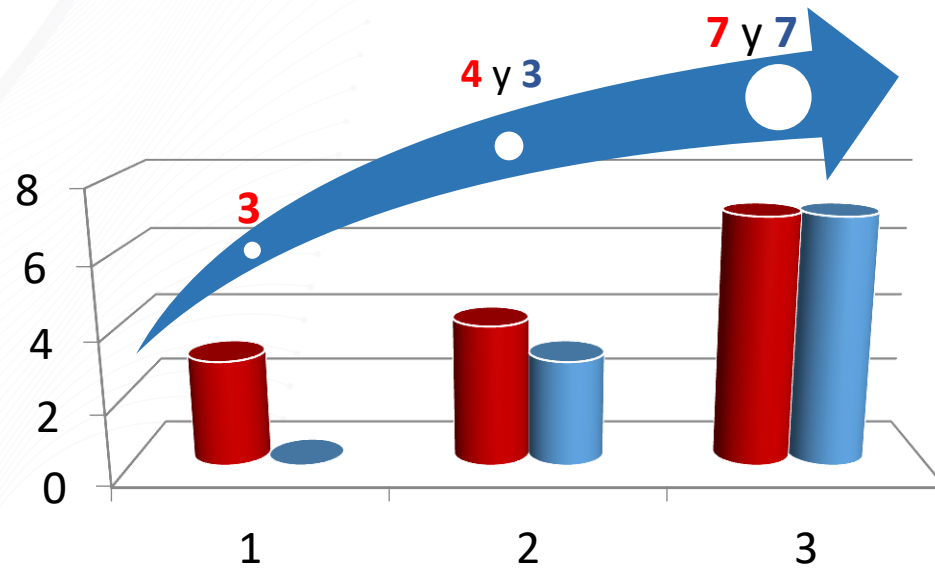




Proceso de Certificación: entre 3 y 18 meses



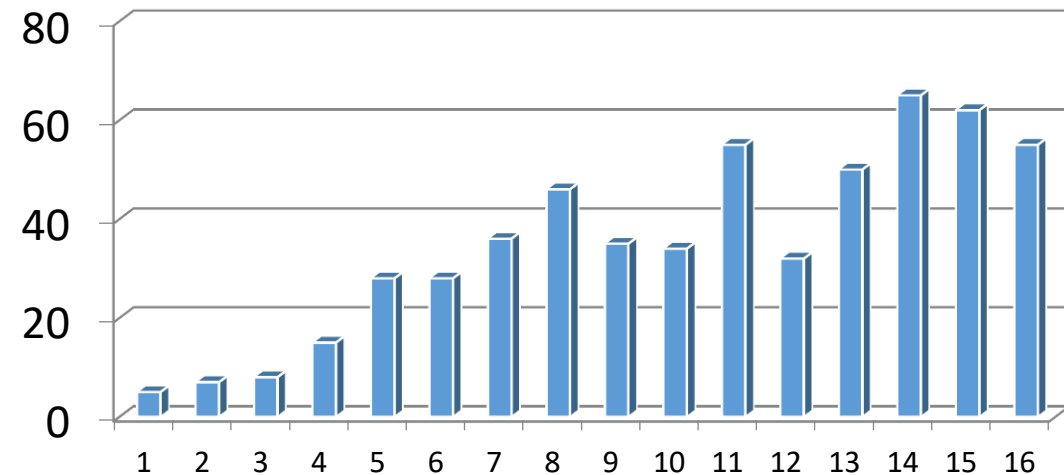
Laboratorios acreditados



Serie



Expedientes de evaluación



Reto 2020: adaptación al “*Cyber Security Act*”

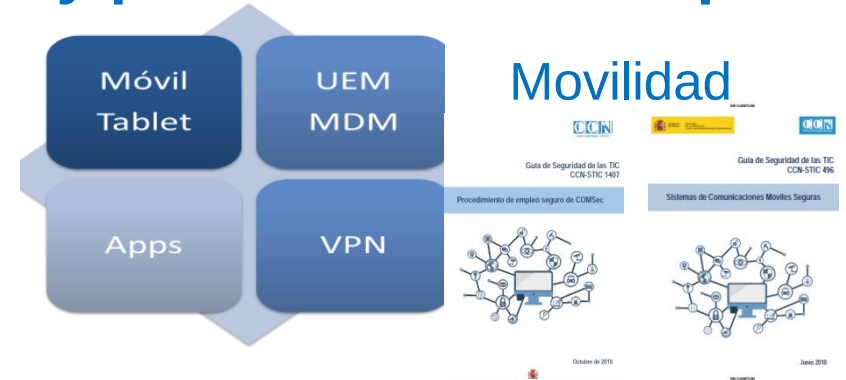
Seguridad en Movilidad

- Aprobación UE versión FM ESP
- Cualificación ENS Categoría Alta
 - MDM
 - Dispositivos móviles
 - *Tablets*



2019

Arquitecturas de referencia y procedimientos empleo



Comunicaciones Tácticas Seguras

- Primer cifrador táctico nacional
- Productos de cifra nacional en ET y Armada
- Evaluación de seguridad de nuevo equipamiento SDR
- WiFi y LTE seguro con ET



Sistemas seguros de navegación por satélite

- Prototipo de receptor GALILEO PRS
- Canal Secundario nacional para gestión de receptores PRS
- Desarrollo de cargador de claves dual UE y nacional



2020

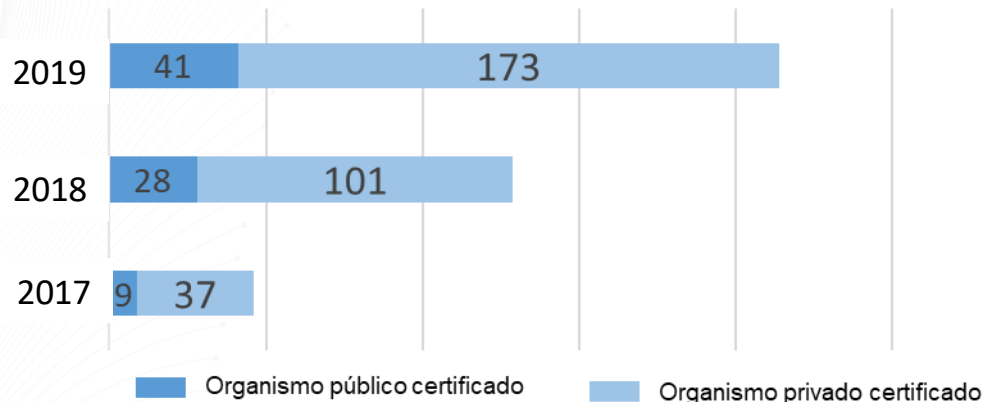
[Retos CCN]



[OB/01] ENS

Implantación del ENS en el sector público

Actualización del Esquema Nacional de Seguridad tras los 10 años de su publicación.



[OB/02] Evaluación continua

Reducir la superficie de exposición

Impulsar la realización auditorías regulares para verificar la exposición a vulnerabilidades y deficiencia de configuración



[OB/03] Capacitación

Diseño curricular

Definir el perfil de seguridad en los puestos de trabajo de la Administración Pública.



[OB/04] LUCÍA 3.0

Notificación de incidentes

Nueva versión de la solución que facilitará la cooperación en la notificación y respuesta a incidentes.



[OB/05] SOC

Despliegue del SOC de la AGE

Despliegue del SOC de la AGE y implementación de los SOC Virtuales en entidades locales.



[OB/06] Resolución de incidentes

Experiencia CCN

Despliegue de equipos en apoyo a la respuesta a incidentes. Nuestra experiencia marca la diferencia/valor añadido.



[OB/07] CSIRT.es

Agilizar el intercambio

Mejorar y adecuar el intercambio de información sobre incidentes entre “partners” y grupos de confianza.

08 Retos 2020. Productos y Catálogo



Modernización criptológica

- Amenaza computación cuántica
- Nueva generación algoritmos cripto
- Despliegue nuevos equipos cripto



Retos 2020

Arquitecturas de seguridad



Interconexión



Cloud



End Point

Comunicaciones Tácticas Seguras

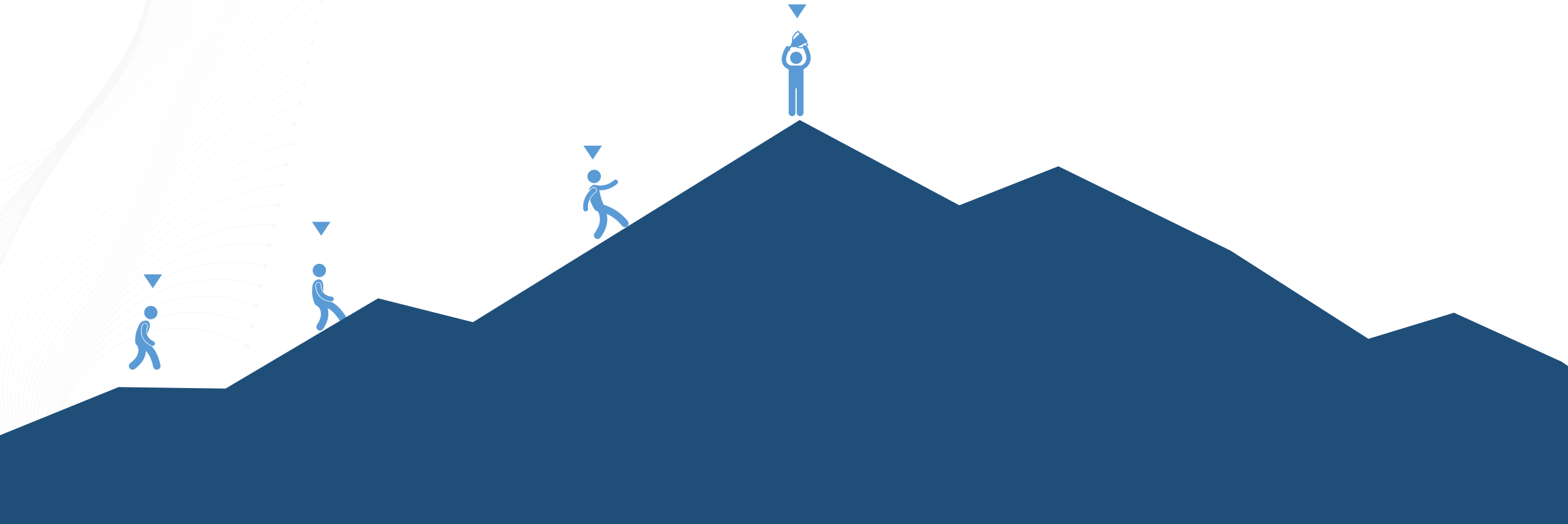
- Despliegue de cifra nacional en sistemas de las FAS
- Aprobación de primeras radios SDR
- Aprobación y despliegue WiFi y LTE seguro en unidades operativas
- Desarrollo de cifrador nacional para plataformas aéreas



Sistemas seguros de navegación por satélite

- Despliegue de primeros receptores PRS
- Capacidad operativa inicial del Canal Secundario
- Nuevos receptores de menor factor de forma

¿2025?



Prevención



Desarrollar

Capacidades Técnicas y Humanas

Detección



Defender

Medidas activas

Respuesta



Disuadir

COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD

#XIIIJORNADASCNCERT

OC.CCN.CNI.ES

WWW.CCN.CNI.ES

WWW.CCN-CERT.CNI.ES

XIII JORNADAS STIC CCN-CERT

ccn-cert
centro criptológico nacional