

IX JORNADAS STIC CCN-CERT

DETECCIÓN E INTERCAMBIO, FACTORES CLAVE

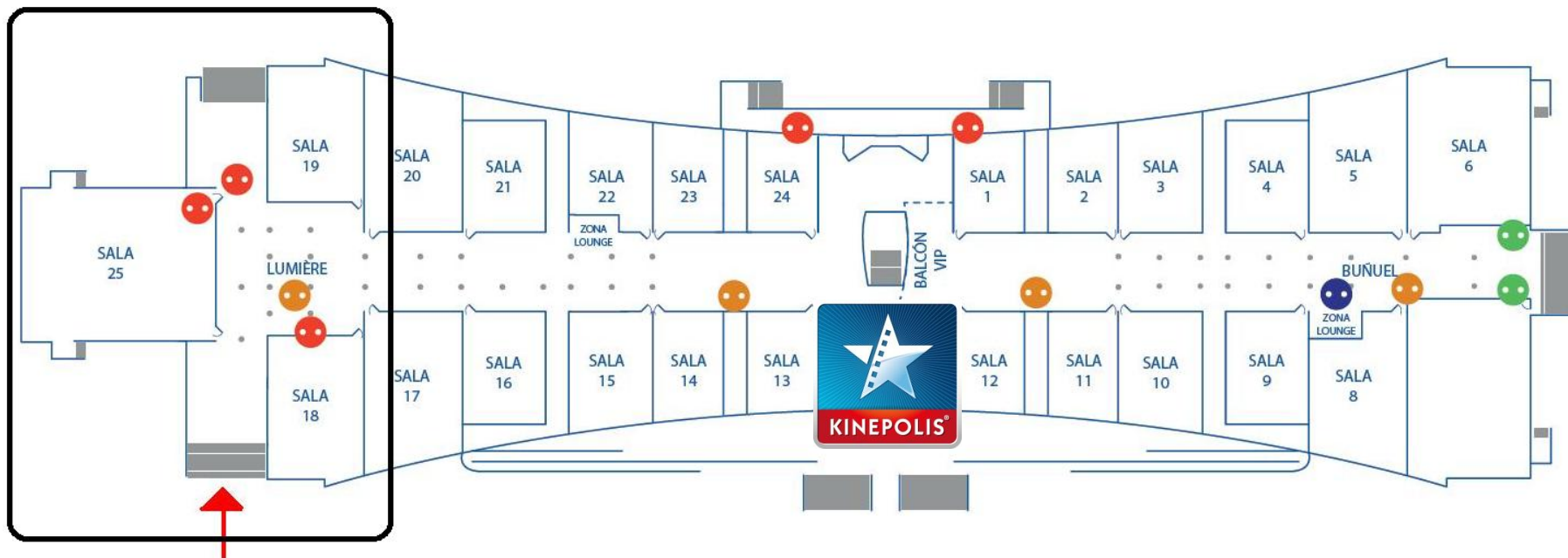
Madrid, 10 y 11 de diciembre 2015

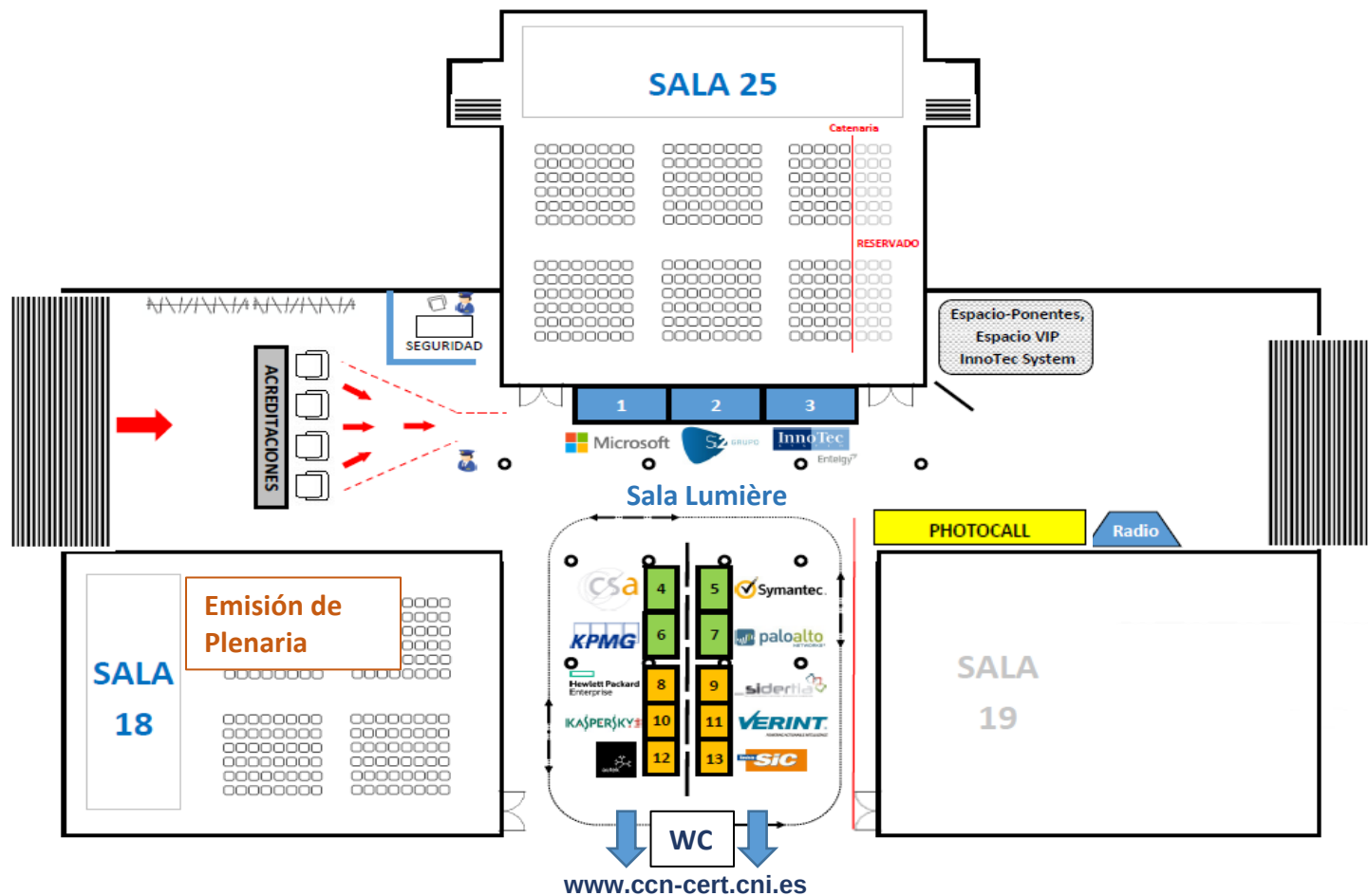
Bienvenida Información Administrativa



CENTRO CRIPTOLÓGICO NACIONAL







SESIÓN PLENARIA (SALA 25)	
09:00 - 09:25	INAUGURACIÓN SED-CNI
09:30 - 10:20	CCN-CERT / ¿Qué circula por nuestras redes? (CCN)
10:25 - 10:55	StageFright. Demo * Jaime Sánchez (TELEFÓNICA)
11:00 - 11:35	CAFÉ (Sala Lumière)
SALA 25	
MÓDULO 1: CIBERESPIONAJE/APTS/ AMENAZAS, HERRAMIENTAS Y TECNOLOGÍAS	
11:40 - 12:05	APT. Evolución de las tácticas. Situación de España en el panorama Europeo Álvaro García (FireEye)
12:10 - 12:35	APT: con P de Python * Vicente Díaz (Kaspersky)
SALA 18	
MÓDULO 2: ESTRATEGIA DE CIBERSEGURIDAD, ENS Y CUMPLIMIENTO NORMATIVO	
Acciones de la DTIC. Actualización del ENS y Nivel de cumplimiento . CCN y Miguel Ángel Amutio (MINHAP)	
ENS: enfoque práctico David López (Gobierno de Aragón)	

SALA 25

12:40 - 13:05 Bypassing trusted code:
Hacking GRUB * *
Héctor Marco-Gisbert e Ismael Ripoll
(Universitat Politècnica de València)

13:10 - 13:35 Cibercrimen en Rusia
Cte. Óscar de la Cruz (Grupo de
Delitos Telemáticos-Guardia Civil)

13:40 - 14:05 Controlando tu coche desde la nevera:
amenazas en el Internet de las cosas
(IoT)
José Albors (ESET)

SALA 18

Cómo conseguir la conformidad con el
ENS
Alicia Fernández (Junta de
Comunidades de Castilla-La Mancha)

Mesa redonda:
Implicaciones de un futuro desarrollo
reglamentario de la Ley de Seguridad
Privada en la contratación pública de
servicios de ciberseguridad
Moderador: José de la Peña,
(Director de la revista SIC)
Participantes:
CCN, Esteban Gándara (CNP),
Nacho García (HPE), C. Hortigüela (GISS)
Óscar Pastor (Isdefe),
Román Ramírez (Rooted CON)

14:10 - 15:40 VINO ESPAÑOL (Sala Lumière)
14.10 - Entrega Diploma Patrocinadores
PHOTOCALL

MÓDULO 1:
CIBERESPIONAJE/APTS/AMENAZAS,
HERRAMIENTAS Y TECNOLOGÍAS

15:45 - 16:10 Deconstruyendo la Estrella Roja:
el Linux de Corea del Norte *
Simón Roses (Vulnexus)

16:15 - 16:40 Construyendo un laboratorio de análisis
de aplicaciones Android * *
María Isabel Rojo (INDRA)

TALLER 1:
HERRAMIENTA DE DETECCIÓN
(Sala 25)

16:45 - 17:45 CARMEN *
(CCN, S2GRUPO)

17:50 - 18:50 Espacio Microsoft

- Auditoría de Office 365 y Microsoft Azure frente al Esquema Nacional de Seguridad
- Gestión de Identidades con Azure AD.
Azure Security Center
- Protección de la información con Office 365.
Advanced Threat Protection (ATP)
- Securitización del puesto de trabajo con Windows 10 y dispositivos

MÓDULO 2:
ESTRATEGIA DE CIBERSEGURIDAD,
ENS Y CUMPLIMIENTO NORMATIVO

Exfiltración por canal lateral.
¿Son las certificaciones la solución?
Luis Hernández y Agustín Martín (CSIC)

Detección en el ENS: HBOS IDS
("High Bandwidth Open Source IDS") *
Maite Moreno y José Vila (CSIRT-CV)

TALLER 2:
HERRAMIENTAS DE CUMPLIMIENTO
NORMATIVO E INTERCAMBIO DE
INFORMACIÓN (Sala 18)

LUCÍA * / REYES *
(CCN, CSA) / (CCN, InnoTec System)

Espacio S2 Grupo

Por determinar

¡Echémoslo a suertes!
Análisis de algunas de las principales capacidades hostiles. ¿Quién será el próximo?

DÍA 2 - 11 DE DICIEMBRE

08:30 Recogida de acreditaciones

SESIÓN PLENARIA (SALA 25)

09:00 - 09:25 Defensa Activa
David Barroso



09:30 - 09:55 Desactivación de infecciones, malware y cryptolockers: Prueba de Concepto *
Pablo San Emeterio (TELEFÓNICA)
Román Ramírez (Rooted CON)

10:00 - 10:55 Mesa redonda:
¿Qué está dispuesto a compartir el sector industrial de ciberseguridad privada con las estructuras oficiales de cibervigilancia del Estado?
Moderador: Luis Fernández (Editor de la revista SIC)
Participantes:
CCN, Jorge Uyá (InnoTec System), Héctor Sánchez (Microsoft),
José Miguel Rosell (S2 Grupo), Javier Santos (KPMG), Tony Hadzima (Palo Alto),
David Fernández (Symantec), Juan Luis García (Sidertia)

11:00 - 11:30 CAFÉ (Sala Lumière)

11:35 - 12:00 Ataques a sistemas de pago: pasado, presente y futuro *
Ricardo Rodríguez, (Universidad de Zaragoza)

12:05 - 12:45 Smart Cities *
Juan Garrido (InnoTec System)

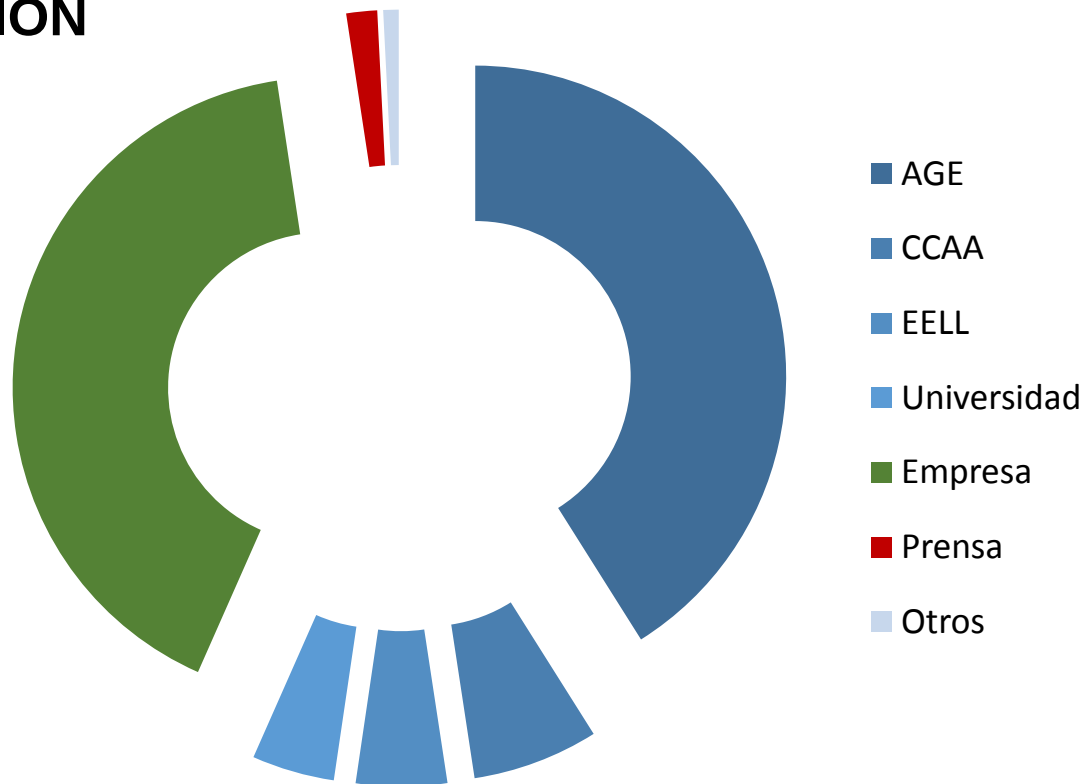
12:50 - 13:30 La cosecha de 2015 de Golden, Reineta y Gala *
Raúl Siles (Dinosec)

13:30 - 13:45 CLAUSURA

Acciones 2015/Objetivos 2016
Domingo Molina (Director TIC de la Administración General del Estado)

ASISTENTES - DISTRIBUCIÓN

TOTAL
1390
ORGANIZACIONES REPRESENTADAS
395



IX JORNADAS STIC CCN-CERT

DETECCIÓN E INTERCAMBIO, FACTORES CLAVE

Madrid, 10 y 11 de diciembre 2015

2015 EN CIFRAS

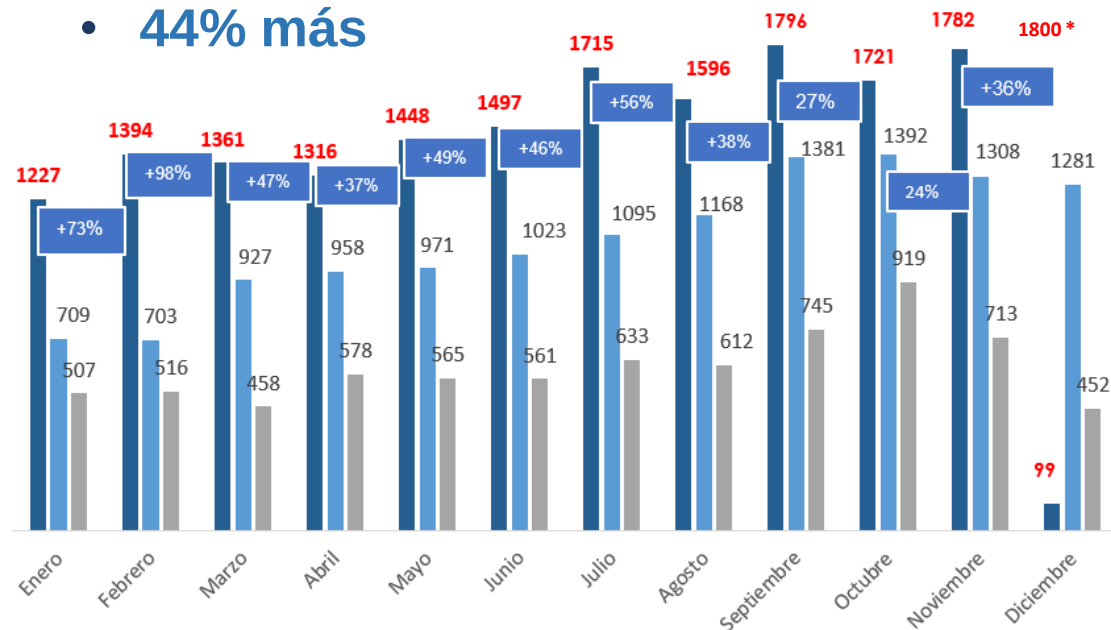


CENTRO CRIPTOLÓGICO NACIONAL

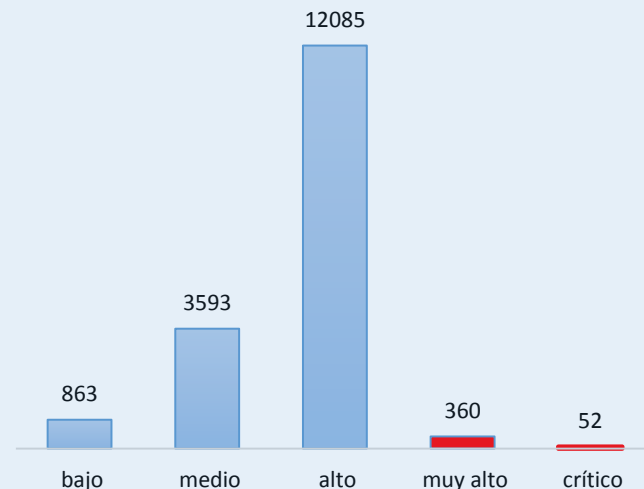


INCIDENTES

- 18.653 en 2015
- 44% más



Peligrosidad



* Previsión Diciembre

INFORMES DESTACADOS



CÓDIGO DAÑINO	
DOUBLE FANTASY	FANNY
AGENT.BTZ	RAMNIT
CRYPTTEAR.A	TORRENTLOCKER
KINS	SPYBOT
UPATRE	HYBRIDS
PAPRAS.EH	HOUDINI

400 Guías Generales

- 401 Glosario y Abreviaturas
- 423 Indicadores de Compromiso
- 424 Intercambio de Información de Ciberamenazas. STIX-TAXII
- 425 Ciclo de Inteligencia y Análisis de Intrusiones
- 453B Seguridad en Android 4.x
- 460 Seguridad en Wordpress

500 Guías Entornos Windows

- 520 IE 11 para W7 como miembro de dominio indep
- 529 Seguridad en MS Office 201
- 550 MS Exchange Server 2010 en Wserver 2008 R2
- 560A WServer 2012 R2 Instalación completa (DC o servidor miembro)
- 560B WServer 2012 R2 Instalación completa (servidor indep.)

600 Guías Otros Entornos

- 606 Seguridad en OS X Yosemite 10.10.x
- 643B Seguridad en Allied Telesis AT-8100S/AT8100L y FS970M
- 650 Seguridad en Cortafuegos Fortigate
- 651 Seguridad en Cisco ASA

800 Guías ENS

- 807 Criptología de empleo en el ENS
- 817 Gestión de Ciberincidentes
- 844 Manual Usuario de INES
- 859 Recolección y consolidación de eventos WServer 2008 R2
- 860 Seguridad OWA en MS Exchange Server 2010
- 869 Implementación AppLocker en el ENS
- 870A Implementación ENS en WServer 2012 R2 (DC y servidor miembro)
- 870B Implementación ENS WServer 2012 R2 (servidor indep.)

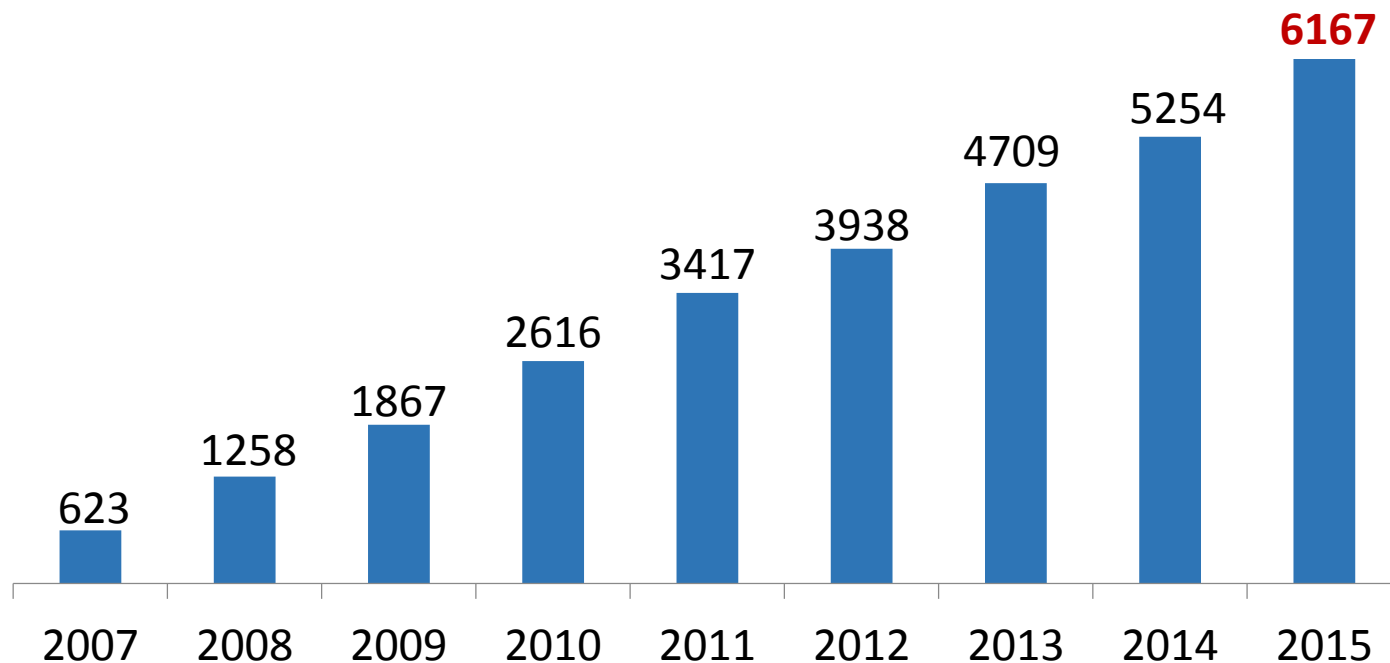
Pública / Privada



GUÍAS CCN-STIC
23 nuevas guías
5 actualizadas

246 guías 273 documentos

USUARIOS DEL PORTAL (a 7.12.2015)



Formación - Cursos STIC 2015



	2008	2009	2010	2011	2012	2013	2014	2015
Alumnos	380	450	510	500	500	500	525	580
Solicitudes	-	-	2119	2493	3090	4300	4850	-
Cursos presenciales	17	18	17	14	14	14	16	17
Horas lectivas	1200	1400	1200	900	900	1000	1100	1180
Cursos online	-	1	3	5	6	6	7	9
Participación en mesas / jornadas	10	14	18	57	73	103	114	129

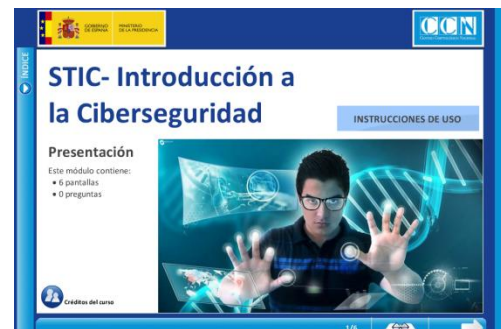
Formación - Cursos Online



1. Esquema Nacional de Seguridad (2) – Público y Fase Online
2. Análisis y Gestión de Riesgos de los Sistemas de Información (2) – Público y Fase Online
3. Curso de Seguridad de las Tecnologías de la Información y las Comunicaciones, STIC – Fase Online
4. Curso básico de Seguridad. Entorno Windows – Fase Online
5. Curso básico de Seguridad. Entorno Linux – Fase Online

6. Curso Cortafuegos
7. Curso Infraestructura de red
8. Curso IDS
9. Curso INES

10-15h



	2010	2011	2012	2013	2014	2015
Nº de accesos a los cursos online	5.430	13.876	11.735	16.261	46.763	47336
Nº de alumnos inscritos	891	1.511	1.887	2.224	4.688	-

HERRAMIENTAS

DETECCIÓN



ANÁLISIS



MÓNICA

**HERRAMIENTA
FORENSE**

AUDITORÍA



ROCÍO

INTERCAMBIO



GESTOR DE REGLAS

IX JORNADAS STIC CCN-CERT

DETECCIÓN E INTERCAMBIO, FACTORES CLAVE

Madrid, 10 y 11 de diciembre 2015

SAT 2.0



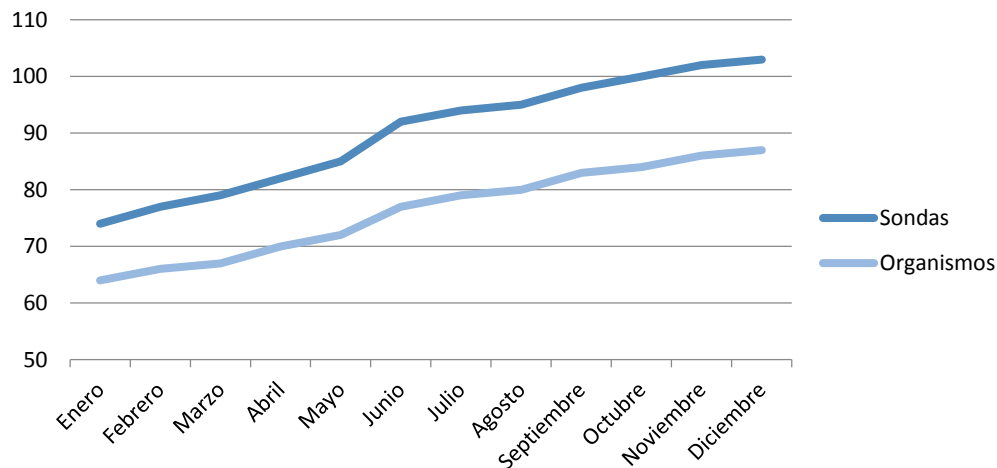
CENTRO CRIPTOLÓGICO NACIONAL



Sistema de Alerta Temprana (SAT) de Internet

Estado del despliegue en 2015

- Ampliación del servicio a nuevos Organismos
 - 87 Organismos (23 nuevos en 2015)
 - 103 Sondas (29 desplegadas en 2015)



Sistema de Alerta Temprana (SAT) de Internet

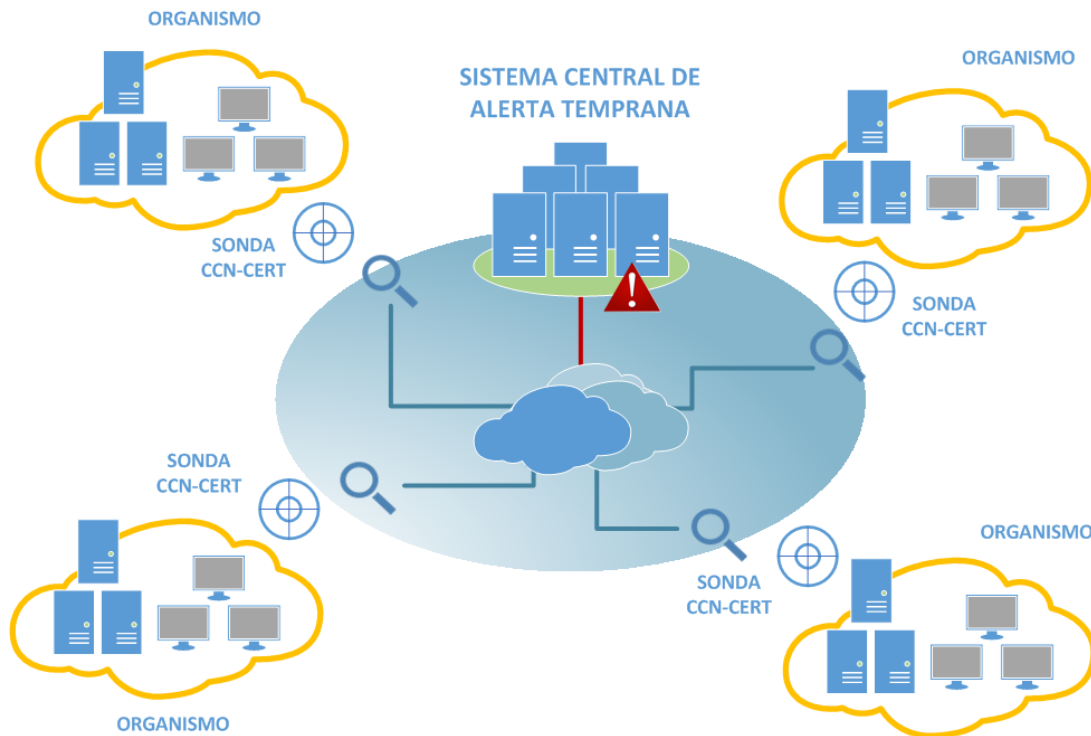
Despliegue para 2016

- Ampliación del servicio a nuevos Organismos
 - Organismos dependientes de algunos Ministerios
 - Continuar con el despliegue en la Administración Autonómica y Local
 - Continuar con el despliegue en los Puertos del Estado
 - Actualmente desplegado en Puerto de Valencia, Puerto de Barcelona, Puerto de Melilla
 - Continuar con el despliegue en las Universidades
 - Continuar con el despliegue en las Confederaciones Hidrográficas
 - Iniciar el despliegue en las Asociaciones Públicas de Abastecimiento y Saneamiento

Sistema de Alerta Temprana (SAT) de Internet

Actual SAT

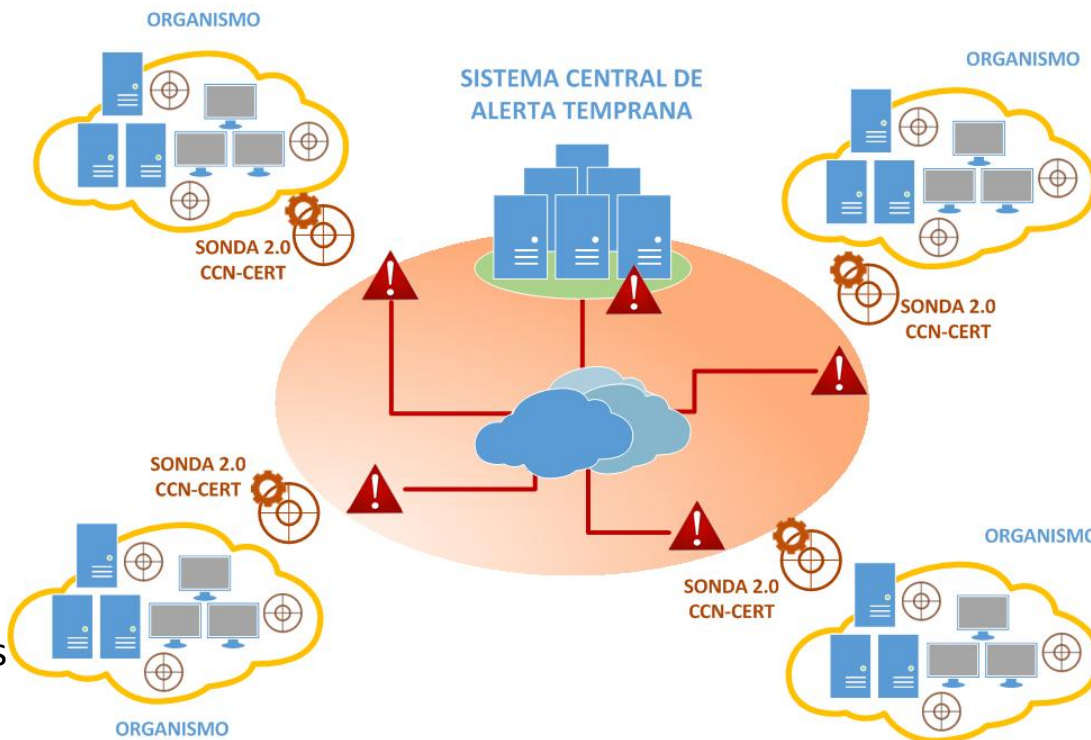
- Características
 - Despliegue distribuido
 - Sondas envían eventos que genera el IDS
 - Correlación de eventos en el sistema central
- Limitaciones
 - Envío de más fuentes de eventos al sistema central



Sistema de Alerta Temprana (SAT) de Internet

SAT 2.0

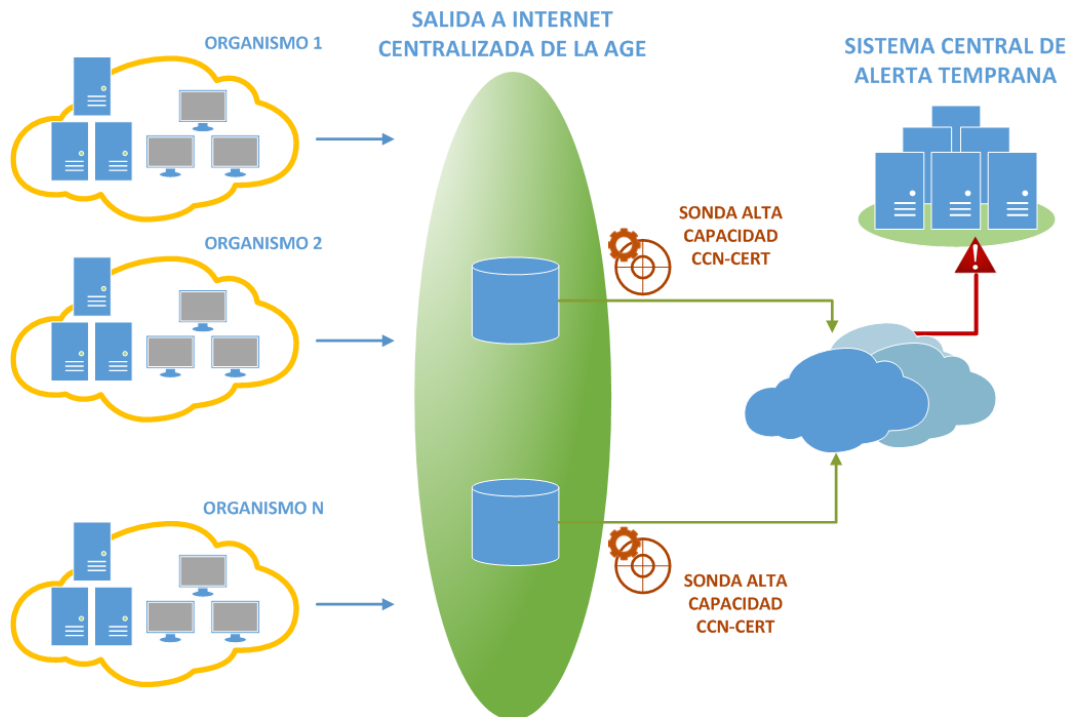
- Características
 - Despliegue multinivel
 - Correlación de eventos en las sondas
 - Envío de alarmas al sistema central
 - Mantiene compatibilidad con actual SAT
- Mejoras
 - Análisis de información de nuevas fuentes de eventos
 - Aumento de la capacidad de correlación



Sistema de Alerta Temprana (SAT) de Internet

SAT en la salida a Internet centralizada de la AGE

- 73 Organismos previstos en la fase 1
- Características
 - Sondas de alta capacidad
 - Análisis de 20Gbps simétricos de tráfico
 - Despliegue en los puntos de agregación
- Mejoras
 - Ampliación del servicio a Organismos que actualmente no se benefician del SAT



IX JORNADAS STIC CCN-CERT

DETECCIÓN E INTERCAMBIO, FACTORES CLAVE

Madrid, 10 y 11 de diciembre 2015

OBJETIVOS 2016



CENTRO CRIPTOLÓGICO NACIONAL



OBJETIVOS 2016

- 1. SAT Internet 2.0**
- 2. Monitorización salida agregada / integración SOC AGE**
- 3. ENS. Mejora y precisión en el conocimiento del nivel de seguridad.
Impulsar las certificaciones de cumplimiento.**
- 4. REYES / LUCIA. Intercambio real de amenazas / incidentes**
- 5. Formación online. Curso gestión incidentes**
- 6. Productos / Organismo de Certificación**
- 7. Seguimiento de incidentes con equipos dedicados**
- 8. Incrementar la actividad de Auditoria / Inspección**

ESQUEMA NACIONAL DE SEGURIDAD



De aplicación a todas las AA.PP

BOE BOLETÍN OFICIAL DEL ESTADO 

Núm. 25 Viernes 29 de enero de 2010 Sec. I. Pág. 8089

I. DISPOSICIONES GENERALES

MINISTERIO DE LA PRESIDENCIA

1330 *Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.*

RD 3/2010 (29.01.2010)

BOE BOLETÍN OFICIAL DEL ESTADO 

Núm. 264 Miércoles 4 de noviembre de 2015 Sec. I. Pág. 104246

I. DISPOSICIONES GENERALES

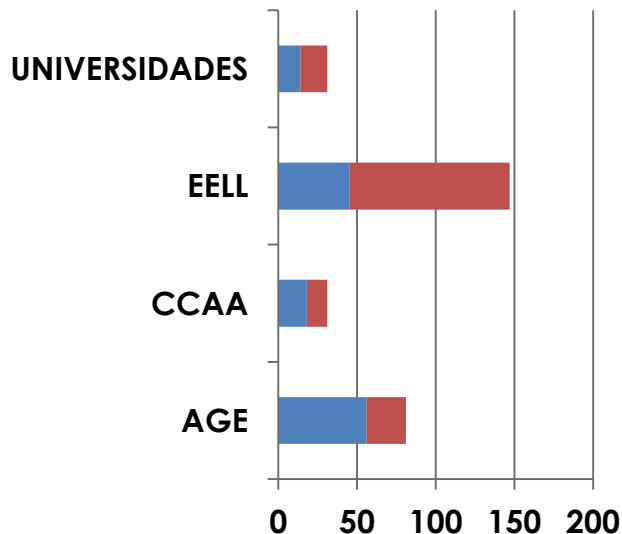
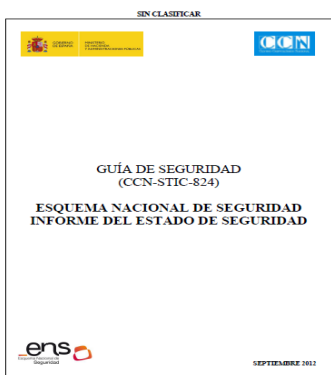
MINISTERIO DE LA PRESIDENCIA

11881 *Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.*

RD 951/2015 (04.11.2015)



119 en 2014

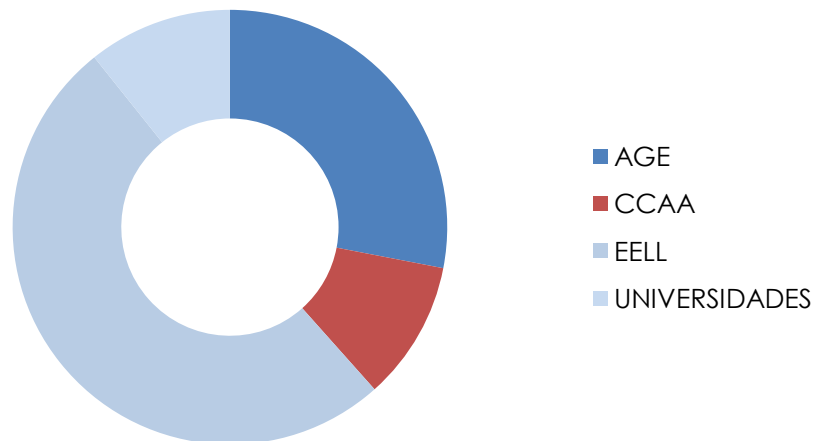


52%

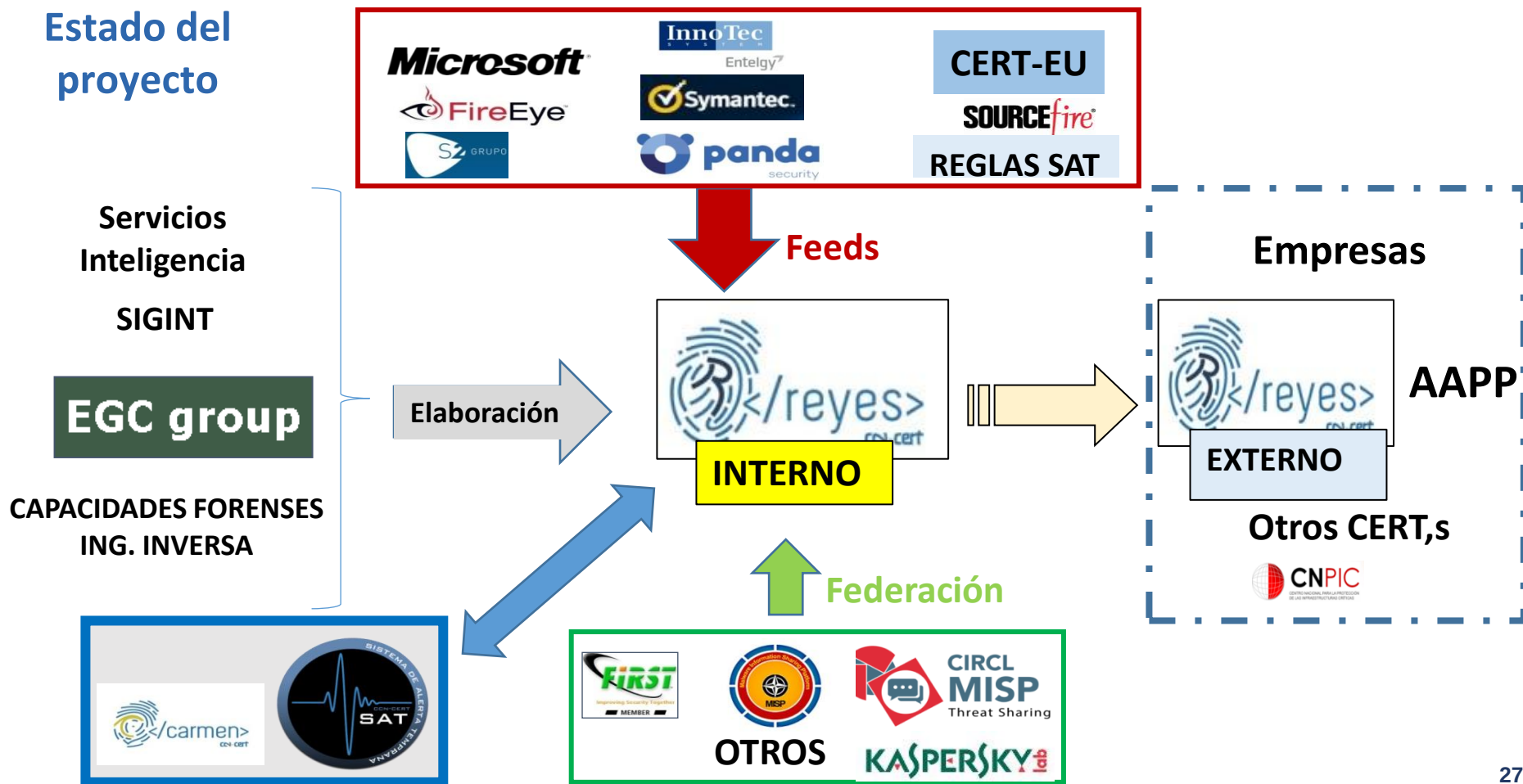
■ Nivel +75%

■ Nivel -75%

09.12.2015	
TIPO ORGANISMOS	Acceso INES
AGE	81
CCAA	31
EELL	147
UNIVERSIDADES	32
TOTAL	Acceso INES 291



Estado del proyecto



2015



EP 430T



EP430GN



CRIPTOPER SAT



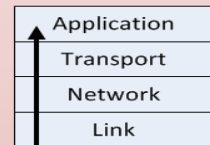
2016

EP430GU

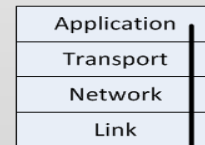


Pasarela

Unidad



Unidad



ESQUEMA NACIONAL DE EVALUACIÓN Y CERTIFICACIÓN DE LAS TI (ENECSTI) ORGANISMO DE CERTIFICACIÓN



CERTIFICACIÓN CRIPTOLÓGICA

Productos capaces de proteger la información clasificada Nacional



CERTIFICACIÓN FUNCIONAL

En base a criterios establecidos y reconocidos como estándar internacional (CC)



CERTIFICACIÓN TEMPEST

Equipos y sistemas protegidos frente a las emanaciones electromagnéticas.

13 expedientes
abiertos de
productos de cifra

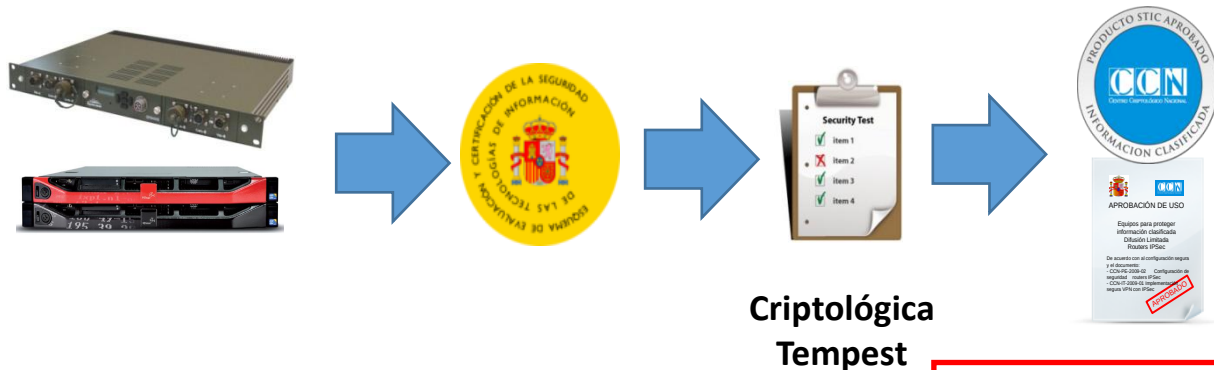
27 expedientes
abiertos de
productos TIC

3 expedientes
acreditación de
laboratorios

146 expedientes
abiertos para la
certificación
TEMPEST de locales
equipos y
plataformas móviles



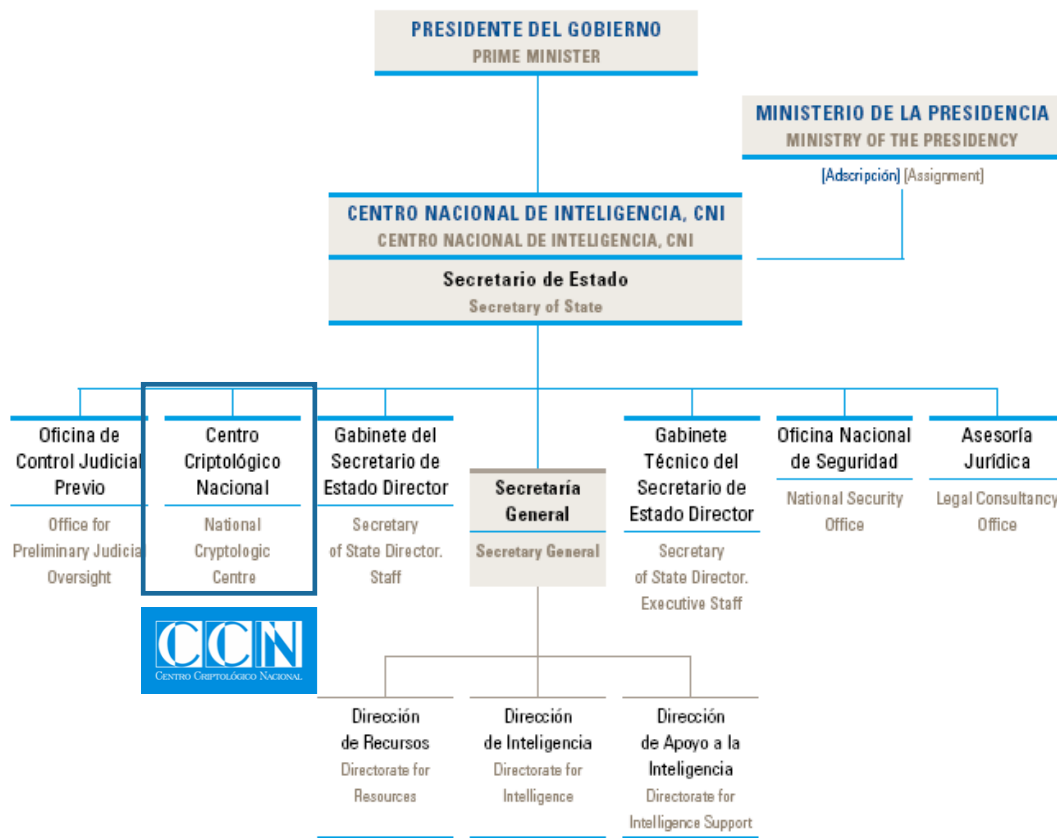
DESARROLLO. Con Tecnología Nacional + Sometidos a un riguroso proceso de evaluación y certificación:



Seguridad verificable

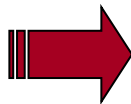
- ✓ Corrección y eficacia mecanismos de seguridad
- ✓ Fortaleza e implementación cifra
- ✓ Aleatoriedad y longitud claves

**Necesidad de utilizar
productos STIC
debidamente evaluados
y certificados**



⁽⁴⁶⁾ La estructura básica del CNI está definida en los Reales Decretos 436/2002, de 10 de mayo y 612/2006, de 19 de mayo.
The basic structure of the CNI is established by Royal Decree 436/2002 of May 10th, and 612/2006 of May 19th.

CIBERSEGURIDAD EN EL CNI



Objetivo Prioritario:

- Unidad ciberamenazas
- Integración SIGINT
- Integración Capacidades de Respuesta
- Potenciar Capacidad Defensa Redes



Subdirección
+ 35% Personal
+ 30% Presupuestos

➤ E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- sondas@ccn-cert.cni.es
- redsara@ccn-cert.cni.es
- organismo.certificacion@cni.es

➤ Websites

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



Síguenos en Linked in

