



# UNIVERSIDADES Y CIBERSEGURIDAD

**SIN CLASIFICAR**

Año	Concepto Seguridad	Amenaza	Cambios Tecnológicos
1980-1990	Compusec Netsec Transec	Naturales	Telecomunicaciones Sistemas Clasificados
1990-2004	Infosec Info. Assurance	Intencionadas	Redes corporativas Sist. Control industrial Infraestructuras Críticas
2005-2010	Ciberseguridad Ciberdefensa	Ciberespionaje Ciberterrorismo	Telefonía móvil Redes sociales Servicios en Cloud
2010-2015	Ciberresiliencia Seg. Transparente	APT Hacktivismo	BYOD Shadow IT
2015-2017	Defensa activa Ciberinteligencia	Ciberguerra Conflicto híbrido	Big Data Redes operacionales IoT

FUNCIONES CCN

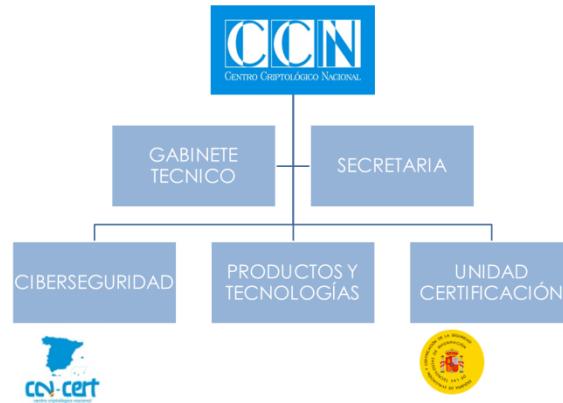
CCN-CERT. SERVICIOS

AMENAZAS 2016 / TENDENCIAS 2017

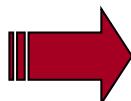
PARTE DEFENSIVA

UNIVERSIDADES

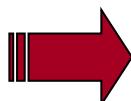
## FUNCIONES CCN



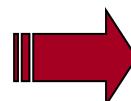
## El CCN actúa según el siguiente marco legal:



Ley 11/2002, 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), que incluye al Centro Criptológico Nacional (CCN)



Real Decreto 421/2004, 12 de marzo, que regula y define el ámbito y funciones del CCN.



Orden Ministerio Presidencia PRE/2740/2007, de 19 de septiembre, que regula el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información



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

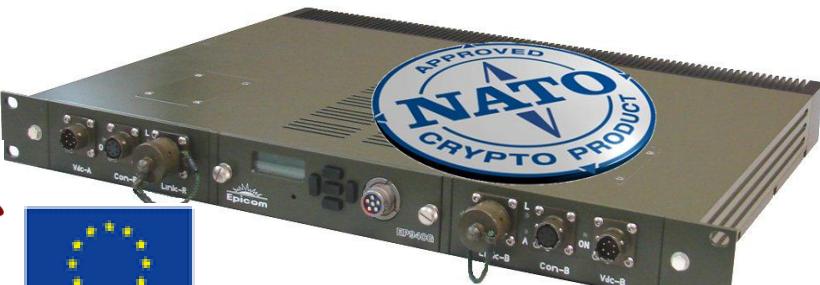
**RD 951/2015, 4 de Noviembre. Actualización.  
Ley 40/2015 Régimen Jurídico Sector Público**



# Productos de cifra nacionales

2016

- Cifrador IP alta velocidad EP430GN
- Cifrador IP táctico EP430T
- Cifrador SCIP Satélite (CRIPTOPER SAT)
- Terminales Móviles Seguros
- Terminal de voz y video SCIP (EP641)



## CCN-CERT SERVICIOS



- Ley 11/2002 reguladora del **Centro Nacional de Inteligencia**.
- Real Decreto 421/2004, 12 de Marzo, que regula y define el ámbito y funciones del **CCN**.
- Real Decreto 3/2010, 8 de Enero, que define el **Esquema Nacional de Seguridad** para la Administración Electrónica, modificado por el **RD 951/2015, de 23 de octubre**. Ampliación del ámbito de actuación con Ley 39/2015 Procedimiento Administrativo común de las AAPP y Ley **40/2015** Régimen Jurídico del Sector Público



## Establece al CCN-CERT como CERT Gubernamental/Nacional competente

### MISIÓN

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

### COMUNIDAD

Responsabilidad en ciberataques sobre:

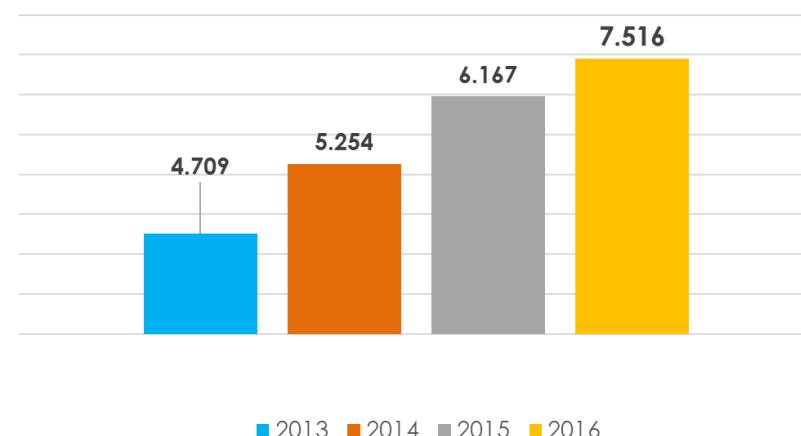
- **Sistemas clasificados**
- **Sistemas del Sector Público**
- Empresas y organizaciones de **sectores estratégicos (en coordinación con CNPIC)**.

# SERVICIOS

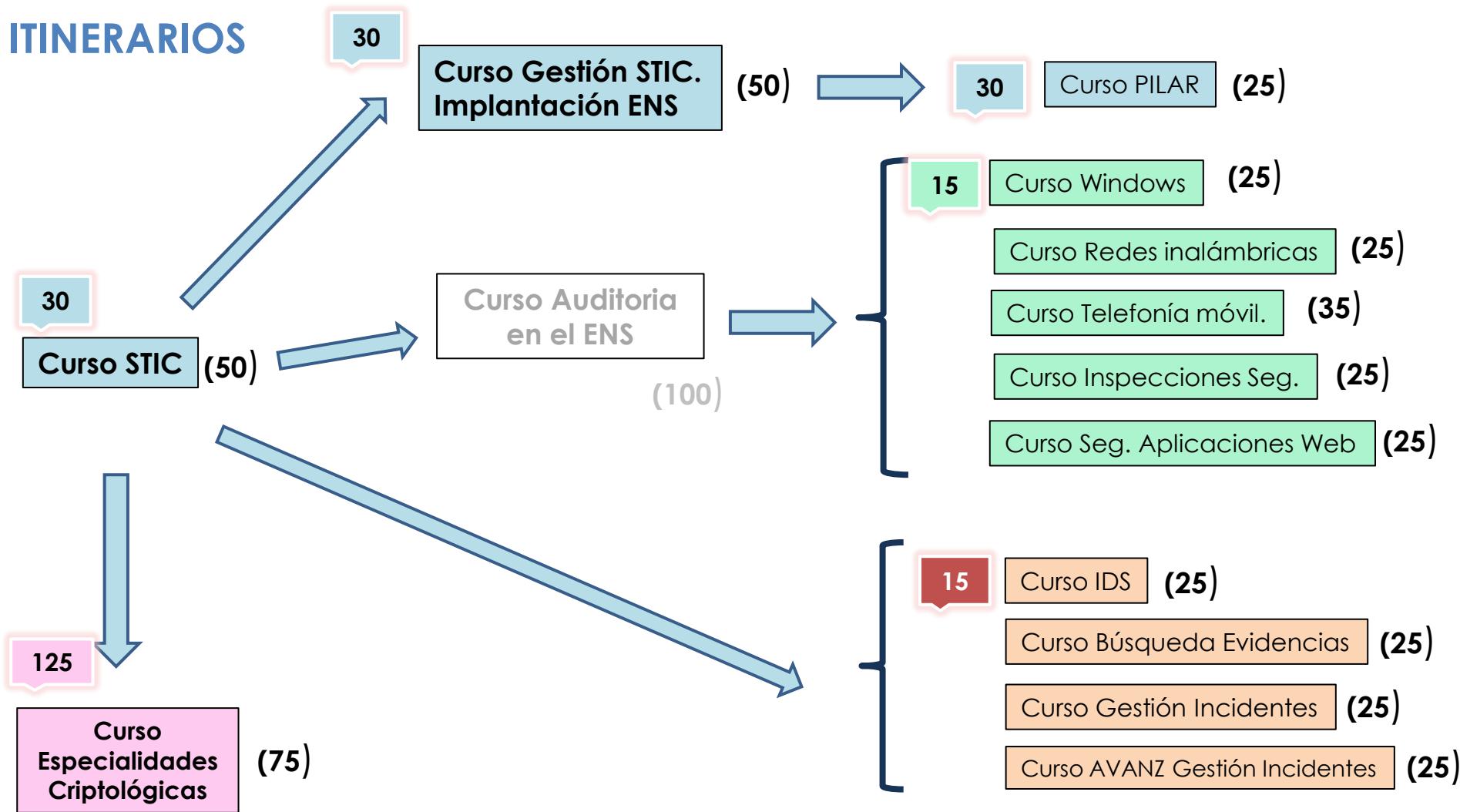
1. Proporcionar guías y estándares de seguridad
  - **Configuración segura de los sistemas**
2. Avisos y vulnerabilidades
  - **Amenazas / Malware / Mejores prácticas**
3. Formación
4. **Respuesta rápida ante ciberataques**
5. **Intercambio de información**
  - **Incidentes**
  - **Ciberamenazas**
6. **Auditorias / Inspecciones**

The screenshot shows the homepage of the CCN-CERT website. At the top, there is a navigation bar with links to 'Inicio', 'Sobre nosotros', 'Gestión de incidentes', 'Formación', 'Guías', 'Informes', 'Herramientas', 'ENS', 'Empresas', 'Seguridad el día', and 'Reportes'. A search bar and a 'Abrir sesión' button are also present. The main content area is titled 'DEFENSA FRENTA LAS CIBERAMENAZAS' and features a 'ÚLTIMA HORA' section with the date '21/06/2018 17:51' and the text 'Crea una fundación contra el cibercrimen'. A 'NIVEL DE ALERTA' indicator shows 'MUY ALTO'. Below this, there are several sections: 'CURSOS ONLINE' (with icons for SAT, ENS, and INCIDENTES), 'CARMEN' (Herramienta de Detección de APTs), 'CCNMobile' (Herramientas de Seguridad para Android), 'CLARA' (Auditoría EN/STIC en Sistemas Windows), 'INES' (Informe de Estado de Seguridad en el ENS), 'LUXIA' (Sistema de Gestión Federada de Tickets), 'CURSOS CON-STIC' (with a link to 'X Curso STIC Seguridad en redes sociales'), 'SERIES CCN-STIC' (with a link to 'Índice de Guías (abril 2015) Última guía serie 800 (EN)'), and 'INFORMES' (with a link to 'Informes de Código Único (IU) CCN-CERT/2018/14 Informe de Código Único a CCN de Gestión').

## Usuarios registrados



## ITINERARIOS



# Centro Criptológico Nacional 2017

	L	M	X	J	V	S	D	L	M	X	J	V	S	D	L	M	X	J	V	S	D	L	M	X	J	V	S	D	L	M												
ENE							1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31					
FEB							1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28								
MAR							XIV Curso STIC (Presencial)						III Curso Gest. Incidentes						XIV Curso STIC (ONLINE)						STIC						X Curso B. Evidencias											
ABR							1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31					
MAY	1	2	3	4	5	6	7	8	9	10	11	12	IX Curso ApL Web						Windows (ONLINE)						XIV Curso WIN - CLARA						XXVIII CEC (ONLINE)						VI Curso STIC Móviles					
JUN							XXVIII CEC (ONLINE)						XXVIII CEC (Presencial)																													
JUL							1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31					
AGO							1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31					
SEP							1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31					
OCT							XIII IDS (ONLINE)						XIV Curso GSTIC (ONLINE)						XIII Curso STIC IDS						XII Curso WIFI						XIV GSTIC (Pres)						XIV GSTIC (Pres)					
NOV							1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31					
DIC							1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31					

# FORMACIÓN A DISTANCIA

Profesor con plataforma videoconferencia y chat de preguntas



## Formación a Distancia

1. Actualización Esquema Nacional de Seguridad (4 horas) (Dic 16)
2. CCN-STIC 824 e INES (4 horas) (Dic 16)
3. LUCIA. Gestión de Incidentes (4 horas) (Mayo)
4. CLARA. Auditoria de sistemas Windows (4 horas) (Junio)
5. ROCIO. Auditoria de equipos de comunicaciones (4 horas) (Julio)
6. Análisis de Malware (2,5 horas) (Junio)
7. MARTA. Análisis dinámico de ficheros (4 horas) (Sept)
8. PILAR. ENS y Protección de datos (4 horas) (Julio / Septiembre)
9. Implementación HTTPS (4 horas) (Julio)
10. **Curso Actualizaciones Windows (5 horas) (Sept-Oct)**
11. **Incidentes complejos. Captura de evidencias básicas (4 horas) (Nov)**
12. REYES. Empleo y capacidades de intercambio (5 horas) (Sept)
13. **Big Data y la seguridad (2,5 horas) (Nov)**
14. Servicios externalizados en el ENS (4 horas)
15. Interconexión en el ENS (4 horas)

# INFORMES DESTACADOS 2016



## Informes en 2016

Informes de Amenazas (IA) (30)  
 Informes de Código Dañino (ID) (27)  
 Informes Técnicos (IT) (56)  
 Buenas Prácticas (BP) (4)



## SERIES CCN-STIC

**CCN-STIC 000:** Políticas STIC

**CCN-STIC 100:** Procedimientos

**CCN-STIC 200:** Normas

**CCN-STIC 300:** Instrucciones Técnicas

**CCN-STIC 400:** Guías Generales

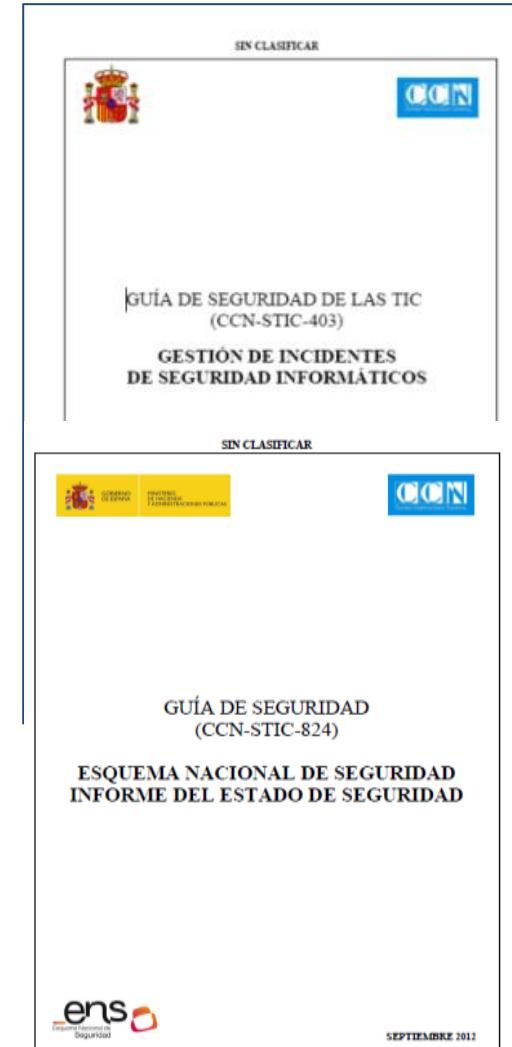
**CCN-STIC 500:** Guías Entornos Windows

**CCN-STIC 600:** Guías Otros Entornos

**CCN-STIC 800: Desarrollo ENS (50)**

**CCN-STIC 900:** Informes Técnicos

**289 guías / 405 documentos**



## Nuevas Guías 2016

- CCN-STIC-462 Seguridad en Joomla
- CCN-STIC-495 Seguridad en IPv6
- CCN-STIC-461 Seguridad en Drupal
- CCN-STIC-426 REYES. Manual de Usuario
- CCN-STIC-597 Entidad de Certificación en Windows Server 2012 R2
- CCN-STIC-567 Implement Hyper-V Windows Server 2012 R2 Core
- CCN-STIC-560C Windows Server 2012 R2 Instalación Core (controlador de dominio o servidor miembro)
- CCN-STIC-568 Windows Server Update Services (WSUS)
- CCN-STIC-563 Implementación de IIS 8.5 sobre Windows Server 2012 R2 en Servidor Miembro de Dominio
- CCN-STIC-552 MS Exchange Server 2013 en Windows Server 2012 R2
- CCN-STIC-561 Servidor impresión de MS sobre Windows Server 2012 R2
- CCN-STIC-562 Servidor ficheros de MS sobre Windows Server 2012 R2
- CCN-STIC-599A Seguridad en Wi10 Enterprise LTSB (cliente miembro dominio)
- CCN-STIC-599B Seguridad en W 10 Enterprise LTSB (cliente independiente)
- CCN-STIC-596 Protección de sistemas con AppLocker
- CCN-STIC-595 Entidad de Certificación en Windows 2008 R2
- CCN-STIC-515 Servidor de Impresión Windows 2008 R2
- CCN-STIC-647 Seguridad en Switches HP Comware
- CCN-STIC-873 Implementación del ENS IIS 8 5 sobre Windows Server 2012 R2
- CCN-STIC-899B Implementación ENS en Windows 10 independiente
- CCN-STIC-899A Implementación ENS en Windows 10 miembro de un dominio
- CCN-STIC-880 Implement ENS en Exchange 2013 sobre Windows SV 2012 R2
- CCN-STIC-830 Ámbito de aplicación del Esquema Nacional de Seguridad
- CCN-STIC-817 ENS Cyber Incident Management
- CCN-STIC-845C LUCIA. Manual Instalación Organismo
- CCN-STIC-845D LUCIA. Manual de Administrador
- CCN-STIC-845A LUCIA. Manual de Usuario
- CCN-STIC-845B LUCIA. Manual de Usuario Sistema de Alerta Temprana (SAT)

## Guías actualizadas 2016

- CCN-STIC-001 Información clasificada en la Administración
- CCN-STIC-101 Acreditación de sistemas de las TIC que manejan información clasificada
- CCN-STIC-103 Catálogo de Productos Certificados (DL)
- CCN-STIC-844 Manual de usuario de INES
- CCN-STIC-845D LUCIA. Manual de Administrador
- CCN-STIC-824 Información del Estado de Seguridad
- CCN-STIC-817 Gestión de Ciberincidentes
- CCN-STIC-809 Declaración de conformidad con el ENS
- CCN-STIC-845A LUCIA. Manual de Usuario
- CCN-STIC-800 Glosario de términos y abreviaturas del ENS

**273 guías  
374 documentos**

## HERRAMIENTAS CIBERSEGURIDAD

### DETECCIÓN



### SONDA AGE



### ANÁLISIS



### AUDITORÍA



### INTERCAMBIO



### IMPLEMENTACIÓN HTTPS

## IMPLEMENTACIÓN HTTPS

**08.04.2017 Presentación solicitud**

**19.05.2017 Finalización solicitud**

**08.2017 Resultados 1ª vuelta**

**11.2017 Resultados 2ª vuelta**

**Portal web parte privada portal**

**estudiohttps@ccn-cert.cni.es**



SIN CLASIFICAR



Buenas Prácticas  
CCN-CERT BP-01/17

Recomendaciones de  
implementación de HTTPS

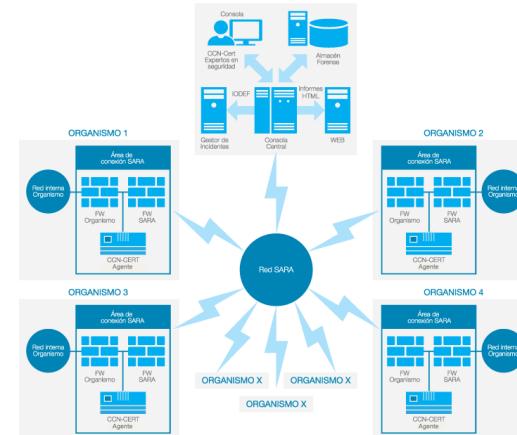
Marzo de 2017

SIN CLASIFICAR

# Sistemas de Alerta Temprana (SAT)

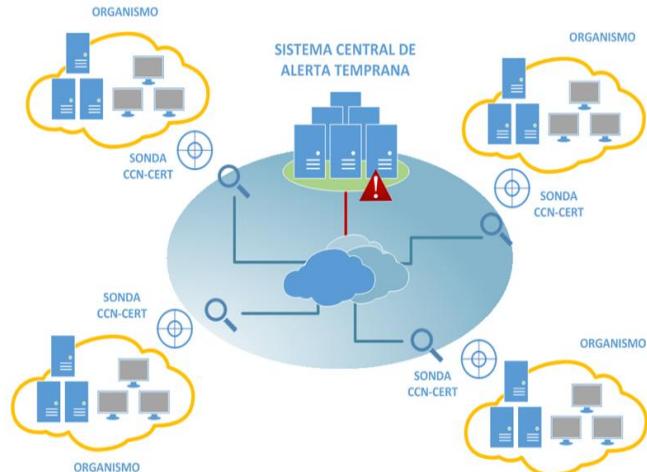
## RED SARA [SAT- SARA]

- Servicio para la Intranet Administrativa
- Coordinado con MINHFP-SGAD
- **50 Áreas de Conexión**



## SALIDAS DE INTERNET [SAT INET]

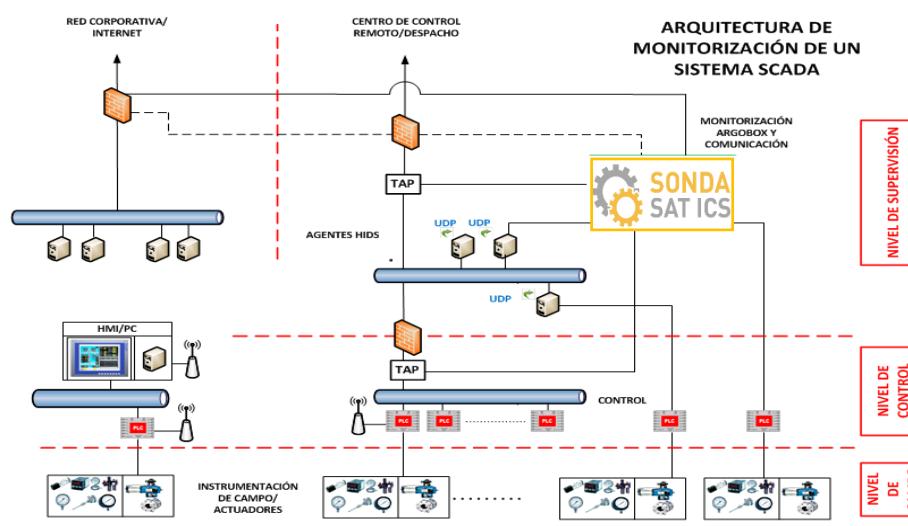
- Servicio por suscripción
- Basado en despliegue de sondas.
- **156 Organismos / 157 sondas**
- Últimas incorporaciones: **Región Murcia, Ayto. Valencia, C.A. Ceuta, Tribunal de Cuentas, Universidad Pablo Olavide, ICO, Junta Andalucía, Puerto Gijón, Parlamento de Galicia, Congreso de los Diputados...**



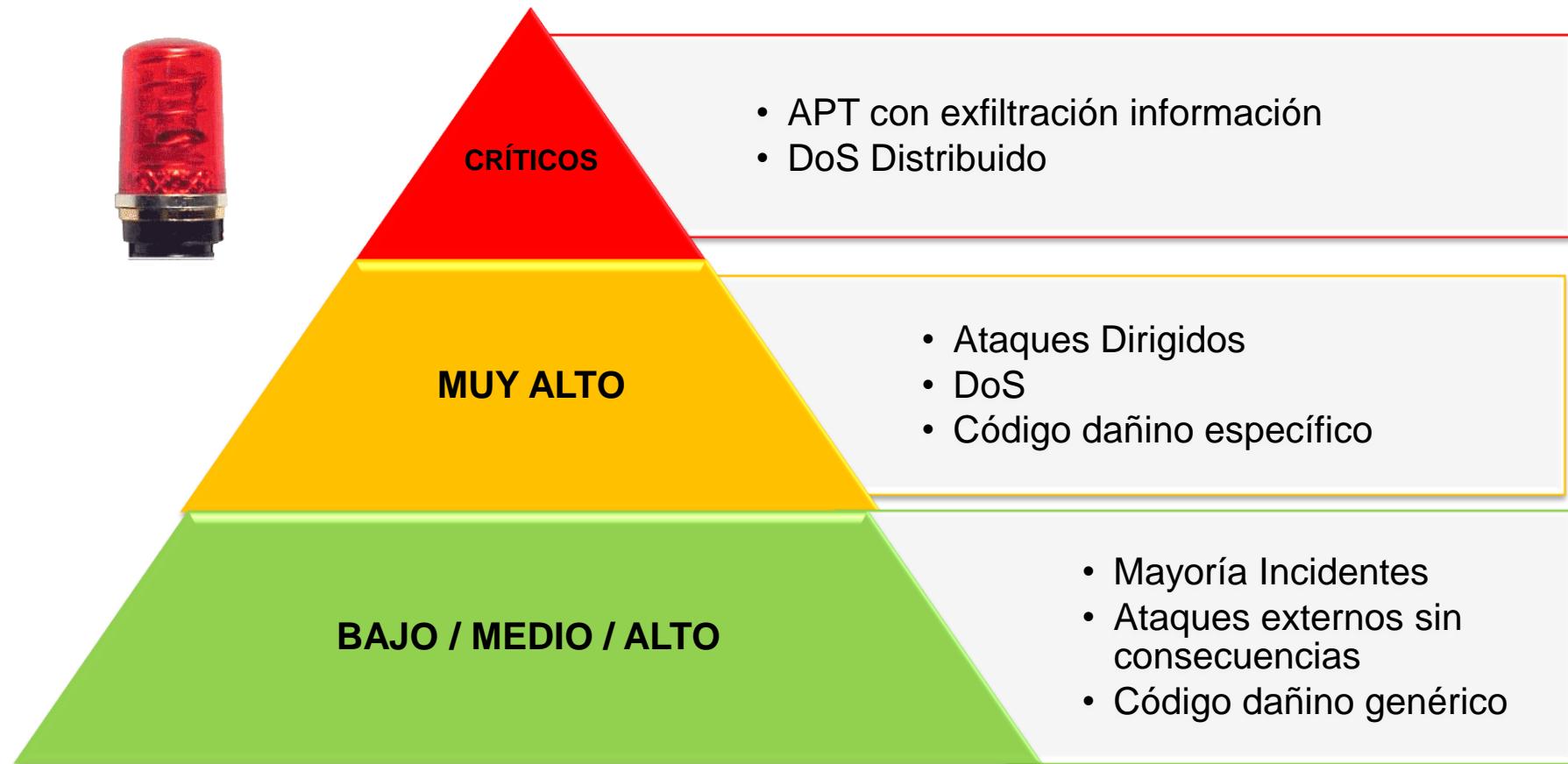
## SONDA AGE (23 Organismos )

## Sistemas Control Industrial

1. La sonda SAT ICS permite monitorizar la actividad en los sistemas de control industrial y SCADA de los Organismos.
2. Detección de acciones anómalas contra los procesos industriales basadas en el análisis del contexto.
3. Disectores específicos de protocolos industriales y motor de correlación local.
  - **EthernetIP (ya desarrollado y probado)**
  - **S7Com (Siemens)**
  - **FINS (Omron)**
  - **Modbus TCP (Estándar)**



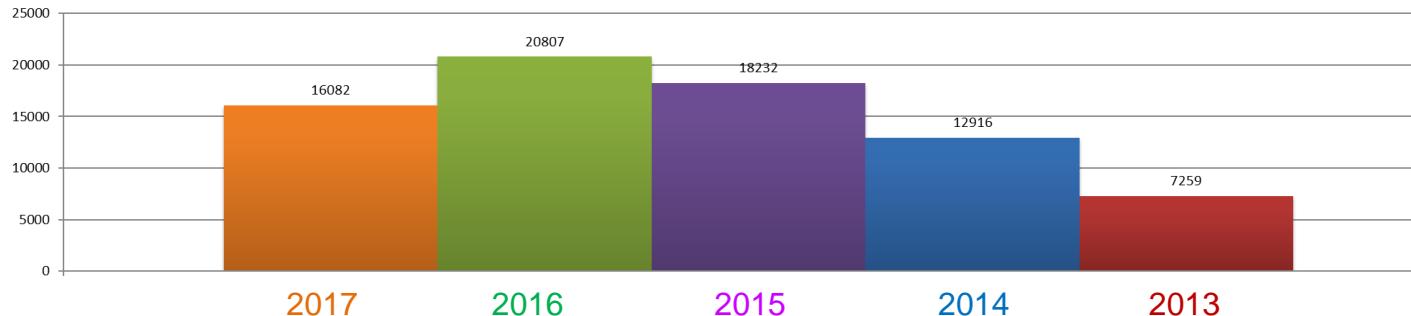
# PELIGROSIDAD DE LOS INCIDENTES



## Guía CCN-STIC-817– Criterios Comunes y Gestión de Incidentes

## ESTADÍSTICAS GLOBALES

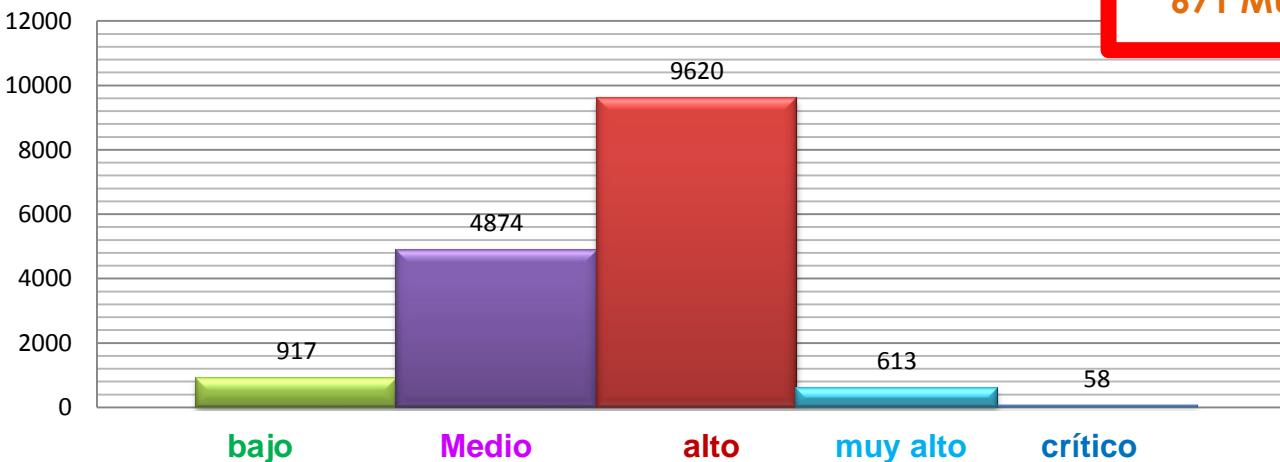
## Total de incidentes por Año



Acumulado Anual

- 2017 16082 (14%)
- 2016: 20.940 (15%)
- 2015: 18.232 (41%)
- 2014: 12.916 (78%)
- 2013: 7.259

## TOTAL 2017 - PELIGROSIDAD



620 MUY ALTOS Y CRITICOS en 2016  
671 MUY ALTOS Y CRITICOS en 2017



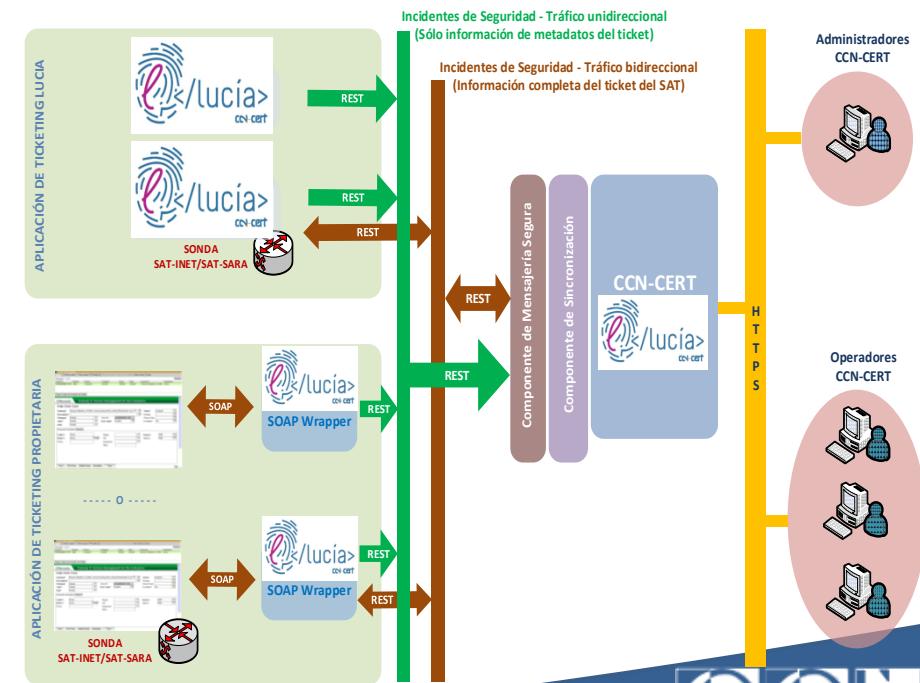


# Listado Unificado de Coordinación de Incidentes y Amenazas

- Cumplir los requisitos del ENS.
- Mejorar la coordinación entre CCN-CERT y los organismos
  - **(Mejorar intercambio de incidentes)**
- Lenguaje común de **peligrosidad y clasificación del incidente**
- Mantener la **trazabilidad y seguimiento del incidente**
- Automatizar tareas
- **Federar Sistemas**
- Permitir integrar otros sistemas
- REYES / MARTA / MARIA

## CCN-STIC 817

Basada en sistema de incidencias Request Tracker (RT)  
 Incluye extensión para CERT Request Tracker for Incident Response (RT-IR)



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



	TOTAL 2016	SAT INET	SAT SARA	REST	INCIDENTS
ENERO	1564	1505	36	0	23
FEBRERO	1761	1684	49	0	28
MARZO	1860	1797	49	0	14
ABRIL	1785	1728	43	0	14
MAYO	1737	1655	67	0	15
JUNIO	1694	1610	76	0	8
JULIO	1601	1480	98	2	21
AGOSTO	1632	1545	60	7	20
SEPTIEMBRE	1924	1732	98	53	41
OCTUBRE	2008	1506	72	391	39
NOVIEMBRE	1785	1362	105	278	40
DICIEMBRE	1589	1247	57	229	56
<b>TOTAL</b>	<b>20940</b>	<b>18851</b>	<b>810</b>	<b>960</b>	<b>319</b>

	TOTAL 2017	SAT INET	SAT SARA	REST	INCIDENTS
ENERO	1726	1385	72	248	21
FEBRERO	1791	1396	75	267	53
MARZO	2303	1648	114	520	21
ABRIL	1812	1314	8	383	31
MAYO	2017	1446	9	456	21
JUNIO	1992	1535	92	354	11
JULIO	1831	1333	117	363	18
AGOSTO	2205	1549	139	494	23
SEPTIEMBRE	405	261	30	112	2
OCTUBRE	0	0	0	0	0
NOVIEMBRE	0	0	0	0	0
DICIEMBRE	0	0	0	0	0
<b>TOTAL</b>	<b>16082</b>	<b>11867</b>	<b>817</b>	<b>3197</b>	<b>201</b>

Diciembre 2016

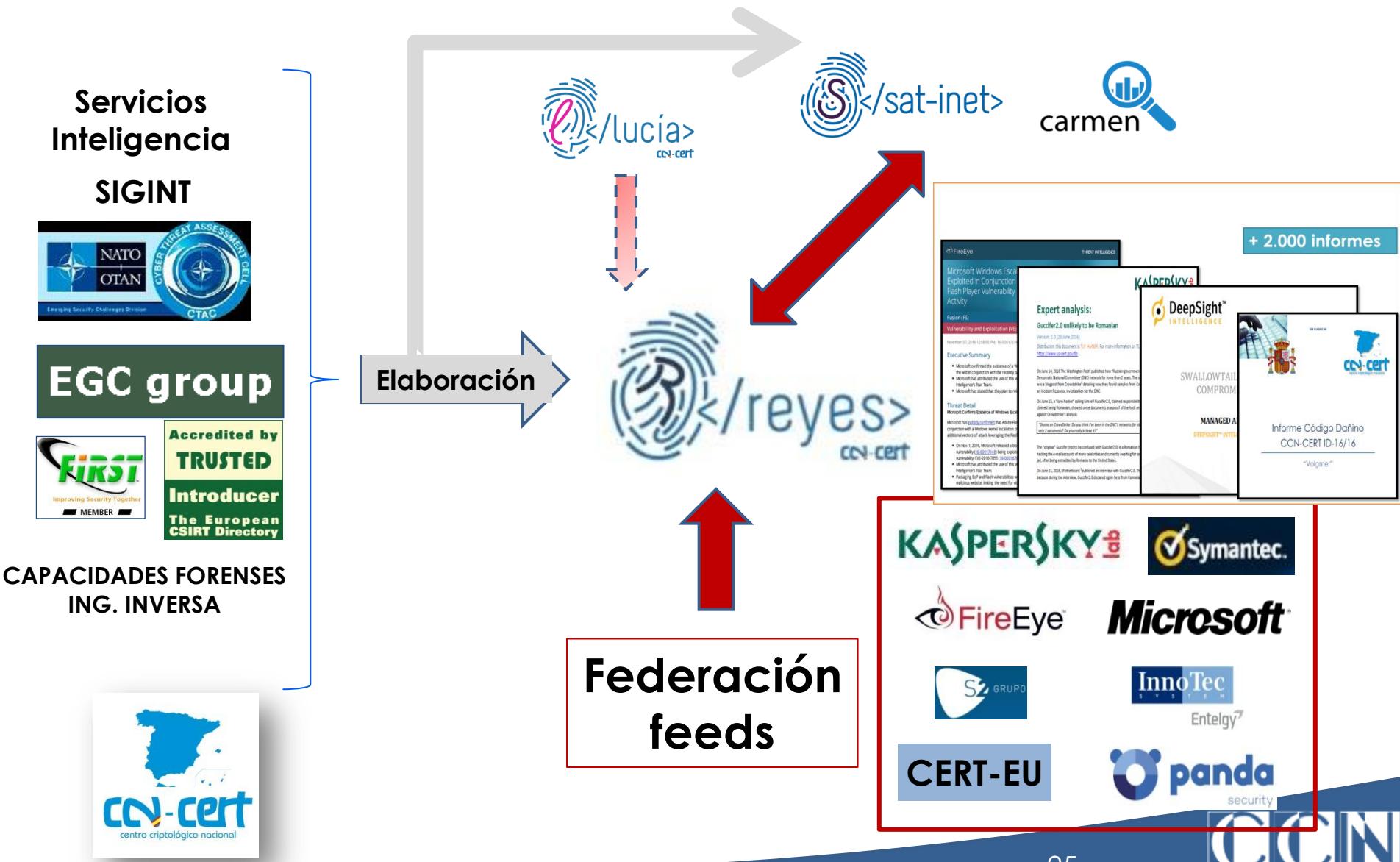
89 % SAT INTERNET  
4 % SAT SARA  
2 % OTROS  
5 % LUCIA



Septiembre 2017

74 % SAT INTERNET  
5 % SAT SARA  
1 % OTROS  
20 % LUCIA

## REYES (REpositorio comn Y Estructurado de amenazas y cdigo daino)



# CIBERAMENAZAS



Informe de Amenazas  
CCN-CERT IA-04/17  
Hacktivismo y  
Ciberyihadismo  
Informe Resumen 2016



Ciberamenazas y Tendencias  
Edición 2017  
CCN-CERT IA-16/17



CCN-CERT IA-09/16  
Ciberamenazas 2015  
Informe anual  
Tendencias 2016



Informe de Amenazas  
CCN-CERT IA-16/16

Ciberespionaje



Julio de 2016  
Informe de Amenazas  
CCN-CERT IA-10/15  
Campañas de  
Ciberespionaje

Agosto de 2016



Informe de Amenazas  
CCN-CERT IA-06/17  
Dispositivos y  
Comunicaciones Móviles  
Informe Resumen 2016

Marzo de 2017

SIN CLASIFICAR

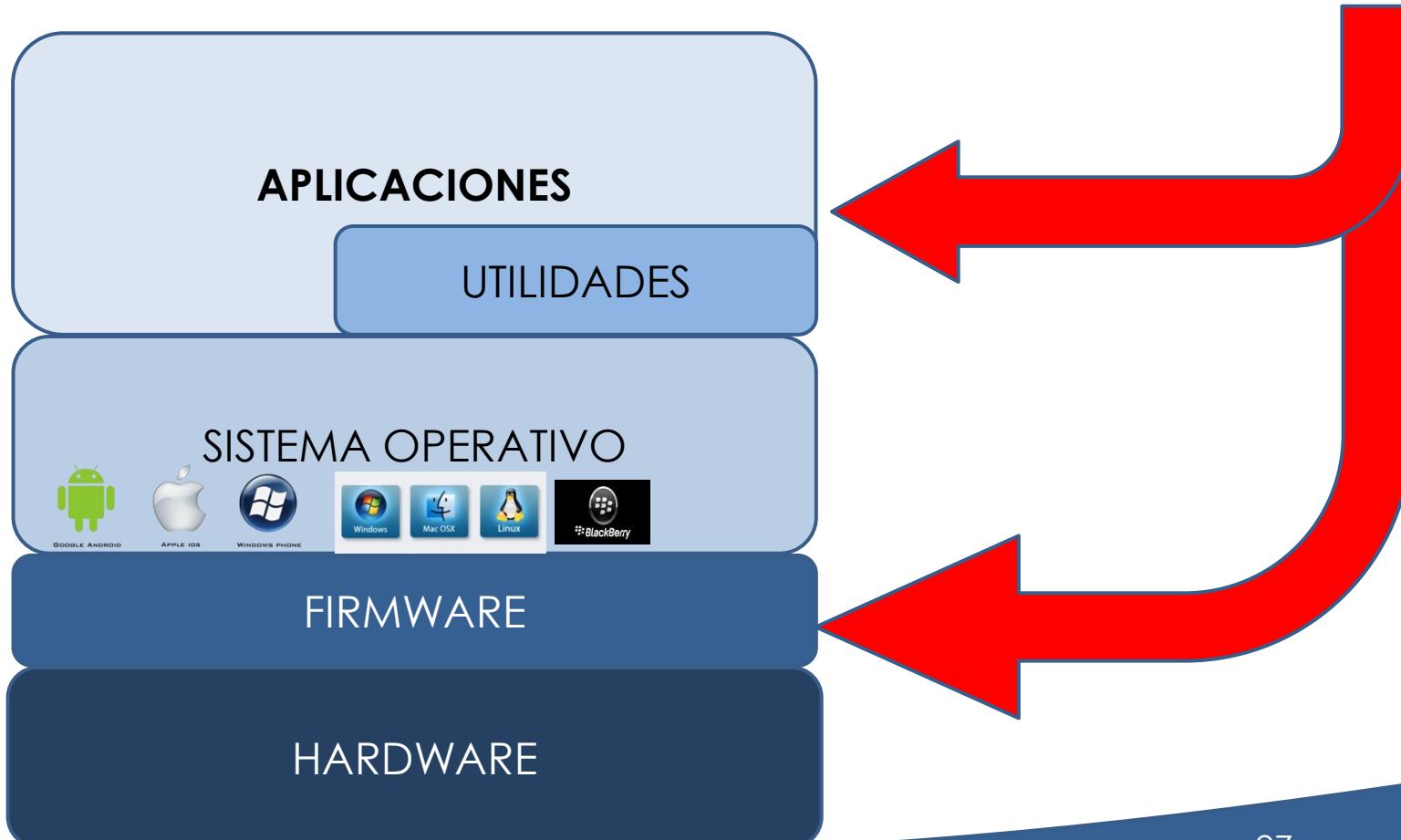
Abri de 2017

SIN CLASIFICAR

# ¿Qué se necesita para que un Ciberataque tenga éxito?

**Vulnerabilidad + exploit**

**+ ingeniería social = Vector de infección**



## Vulnerabilidades. Precios

- Criticidad ALTA = Ejecución de código
- Desmotivación de los investigadores de seguridad
- ◆ Vulnerabilidades DIA CERO
  - ◆ Mercado Negro
  - ◆ Mercado Gris



TARGET PLATFORM	PRICE
Adobe Reader	\$5,000-\$30,000
Mac OS X	\$20,000-\$50,000
Android	\$30,000-\$60,000
Flash or Java browser plug-ins	\$40,000-\$100,000
Microsoft Word	\$50,000-\$100,000
Microsoft Windows	\$60,000-\$120,000
Firefox or Safari browsers	\$60,000-\$150,000
Chrome or Internet Explorer browsers	\$80,000-\$200,000
Apple iOS	\$100,000-\$250,000

x5

## Ejemplo: Vulnerabilidad APACHE STRUTS

2017.01.29 Vulnerabilidad publicada. Se asigna CVE (Mitre)

- **CVE-2017-5638 Permite ejecución remota de código**
- **Comentada en muchos blog**
- **Se soluciona con una actualización**

2017.03.08 Publicación de exploit

- **Toda la info en blog. Afecta 35 millones de servidores**

2017.03.10 Alerta CCN-CERT

2017.03.11 Ataques a Web AAPP

- **+ 75 organismos notificados**
- **+ 25 Incidentes / 4 críticos**

2017.03.13 Impacto:

- **Denegación de servicio**
- **Compromiso de información ???**
- **Cambio de certificados**
- **Bloqueo de la actividad de los Administradores**
- **2017.09.06 Vulnerabilidad publicada.**



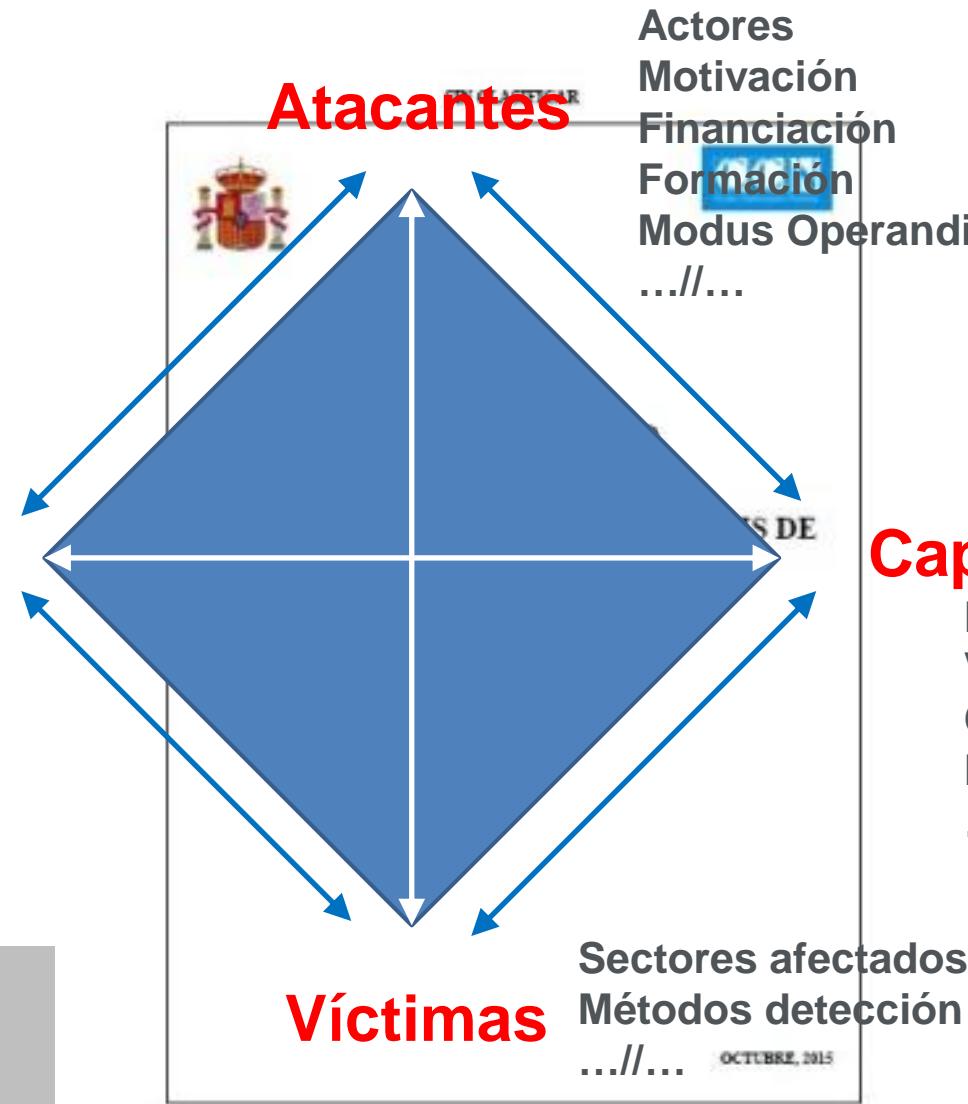
(CVE-2017-5638, S2-045)

CCN-STIC 425

## Infraestructuras

Sistemas C&C  
Nodos  
Saltos  
IP,s / Dominios  
...//...

Estudio de Tácticas /  
Técnicas /  
Procedimientos (TTP)



## Capacidades

Exploits propios  
Vectores infección  
Cifrado / RAT  
Persistencia  
...//...

## Definiciones. Agentes de la amenaza

### CIBERSEGURIDAD

La habilidad de proteger y defender las redes o sistemas de los **ciberataques**. Estos según su motivación pueden ser:

#### CIBERESPIONAJE

Ciberataques realizados para obtener secretos de estado, propiedad industrial, propiedad intelectual, información comercial sensible o datos de carácter personal.

#### CIBERDELITO / CIBERCRIMEN

Actividad que emplea las redes y sistemas como medio, objetivo o lugar del delito.

#### CIBERACTIVISMO

Activismo digital antisocial. Sus practicantes persiguen el control de redes o sistemas (sitios web) para promover su causa o defender su posicionamiento político o social.

#### CIBERTERRORISMO

Actividades dirigidas a causar pánico o catástrofes realizadas en las redes y sistemas o utilizando éstas como medio.

#### CIBERCONFLICTO / CIBERGUERRA / GUERRA HIBRIDA

Operación dirigida por un Estado que utiliza tácticas abiertas y encubiertas con el objetivo de desestabilizar otros Estados y polarizar a la población civil. Incluye una gran variedad de herramientas como diplomacia y acciones de inteligencia tradicional, actos subversivos y de sabotaje, influencia política y económica, instrumentalización del crimen organizado, operaciones psicológicas, propaganda y desinformación y ciberataques

#### **CIBERATAQUE**

*Uso de redes y comunicaciones para acceder a información y servicios sin autorización con el ánimo de robar, abusar o destruir.*

# Ciberamenazas. Agentes. Conclusiones 2016



## 1. Ciberespionaje / Robo patrimonio tecnológico, propiedad intelectual

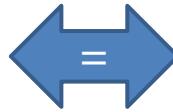
- ◆ China, Rusia, Irán, otros...

Servicios de Inteligencia / Fuerzas Armadas / Otras empresas



## 2. Ciberdelito / cibercrimen

- ◆ HACKERS y crimen organizado



## 3. Ciberactivismo

- ◆ ANONYMOUS y otros grupos



Usuarios internos



## 4. Uso de INTERNET por terroristas

- ◆ Objetivo : Comunicaciones , obtención de información, propaganda, radicalización o financiación



## 5. Ciberguerra / ciberconflicto

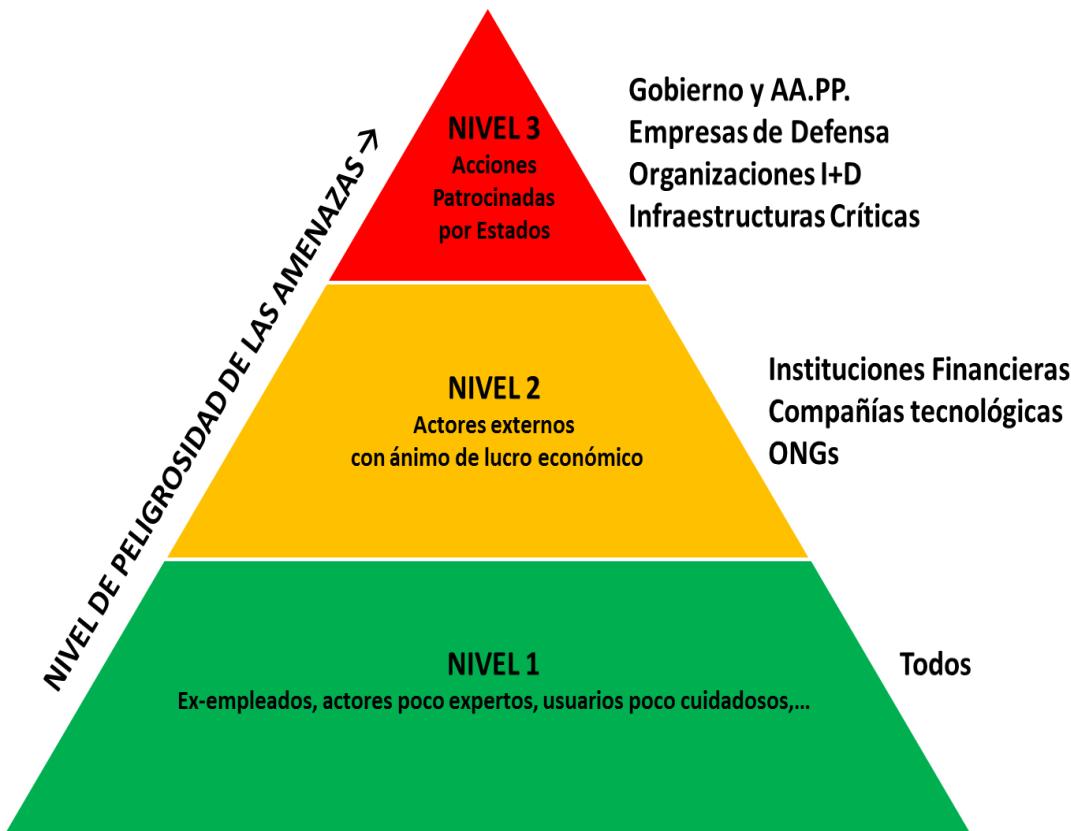
- ◆ Ataque a Infraestructuras críticas y otros servicios



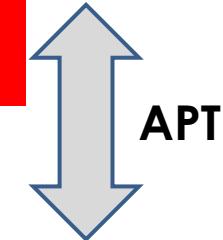
## 6. Ciberterrorismo

- ◆ Ataque a Infraestructuras críticas y otros servicios

# PELIGROSIDAD DE LAS AMENAZAS



**EQUATION GROUP  
SNAKE  
APT28  
REGIN**



**Carbanak  
AGENT BTZ  
Octubre Rojo  
RCS**

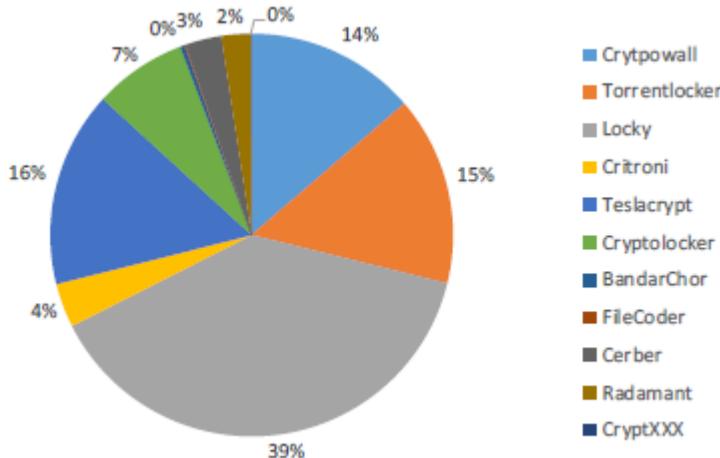
**Ramsonware  
Botnets  
Otro Malware**

# Ransomware

2015

Tipo	Nº incidentes
Cryptolocker	93
Torrentlocker	89
Teslacrypt	73
Cryptowall	109
Otros	73

Total: 427



2016

Tipo	Nº Incidentes
Crytpowall	278
Torrentlocker	308
Locky	785
Critroni	72
Teslacrypt	319
Cryptolocker	151
BandarChor	7
FileCoder	2
Cerber	59
Radamant	48
CryptXXX	1

Total: 2030

SIN CLASIFICAR

CCN-CERT

Informe de Amenazas  
CCN-CERT IA-21/14

Medidas de seguridad  
contra ransomware

FEBRERO 2017

14/09/2017

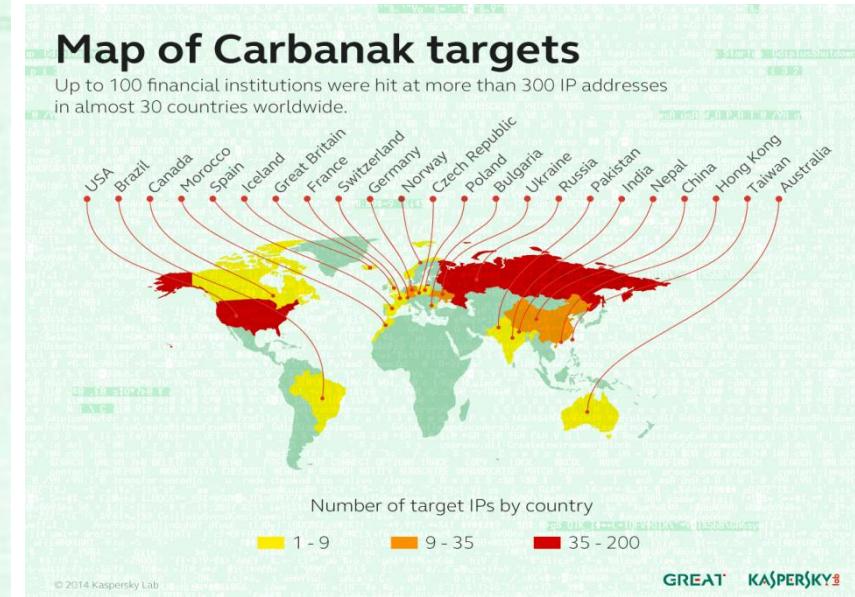
www.ccn-cert.cni.es

24 de Noviembre de 2014

## CARBANAK

## Carbanak: un robo de 1.000 millones de dólares

### Un ataque dirigido contra un banco



- Carbanak ejemplo claro del cibercrimen utilizando técnicas APT.
- “Spear phishing” simulando comunicaciones bancarias.
- Movimientos laterales: Ammyy RAT y comprometimiento de servidores SSH.
- Grabaciones vídeo de empleados (particularmente administradores).
- Utilización de red SWIFT, actualización balances y mecanismos de desembolso (ATM).
- Fondos transferidos a cuentas bancarias de USA y China.

## Advanced Persistent Threat

### -Ataque Dirigido

- ◆ Ciber Ataque “a medida” contra un objetivo concreto (administración, empresa, red, sistema)

### -Threat

APT

- ◆ El atacante tiene la intención y capacidades para ganar acceso a información sensible almacenada electrónicamente

### -Persistent

- ◆ Una vez infectado, se mantiene el acceso a la red/sistema durante un largo periodo de tiempo
- ◆ Muy difícil de eliminar

### -Advanced

- ◆ Habilidad de evitar la detección
- ◆ Se adapta al objetivo
- ◆ Disponibilidad de recursos tecnológicos, económicos, humanos





**Goblin Panda**

**Vixen Panda**

**Deep Panda**

**Emissary Panda**

**Pirate Panda**

**Numbered Panda**

**Lotus Panda**

**Pitty Panda**

**Gothic Panda**

**Predator Panda**

**Dynamite Panda**

**Temper Panda**



**Pale Panda**

**Violin Panda**

**Hurricane Panda**

**Sabre Panda**

**Samurai Panda**

**Dagger Panda**

**Aurora Panda**

**Maverick Panda**

**Keyhole Panda**

**Stone Panda**

**Spicy Panda**

**Comment Panda ...**



**Energetic Bear**

**Snake**

**Octubre Rojo**

**Agent BTZ**

**Inception**

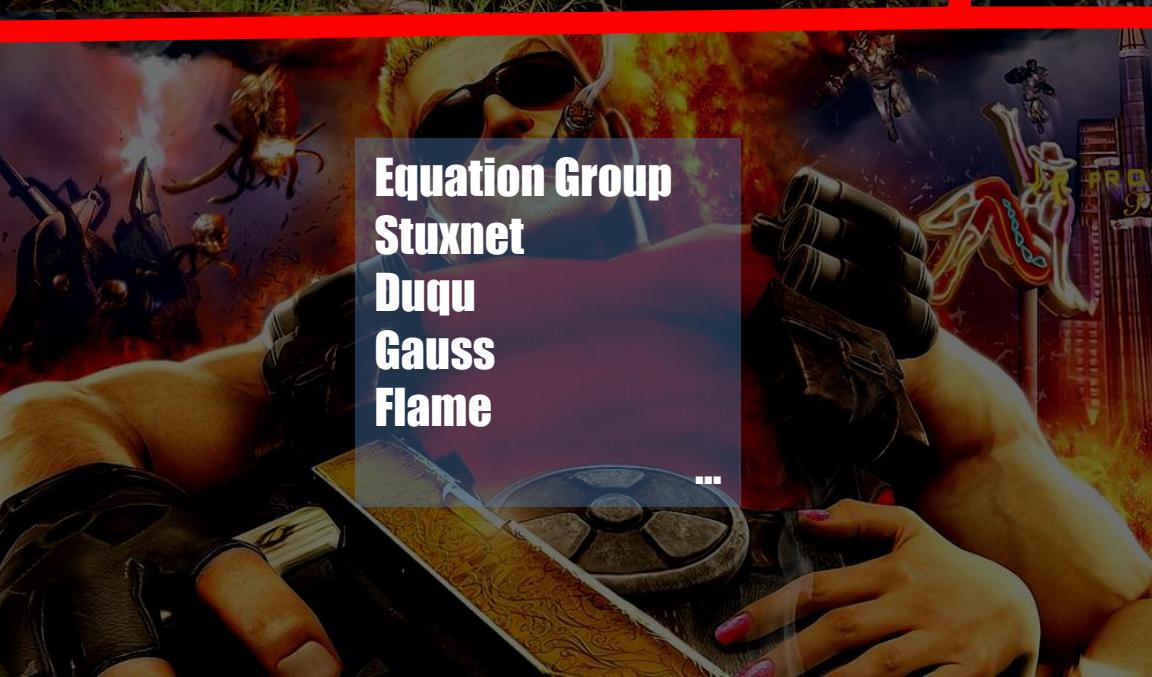
**APT28**

**Cosmic Duke**

**Monkey Duke**

**Cozyduke**

...



**Equation Group**

**Stuxnet**

**Duqu**

**Gauss**

**Flame**

...



**RCS**

**NSO-Pegasus**

**Machete**

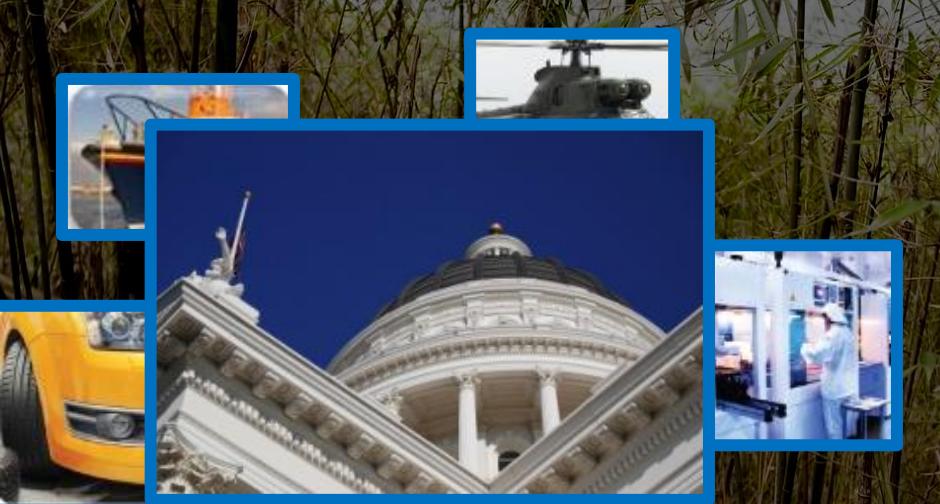
**Siesta**

**The Mask**

**Animal Farm**

**Regin**

**Desert Falcons**

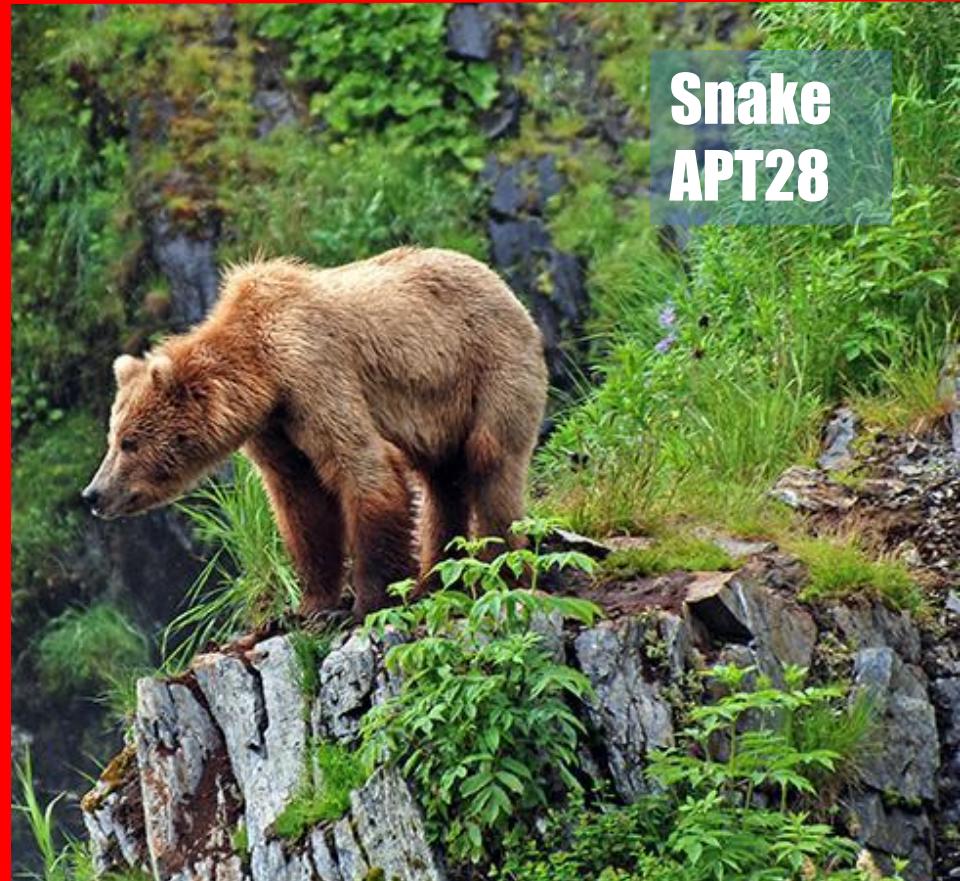


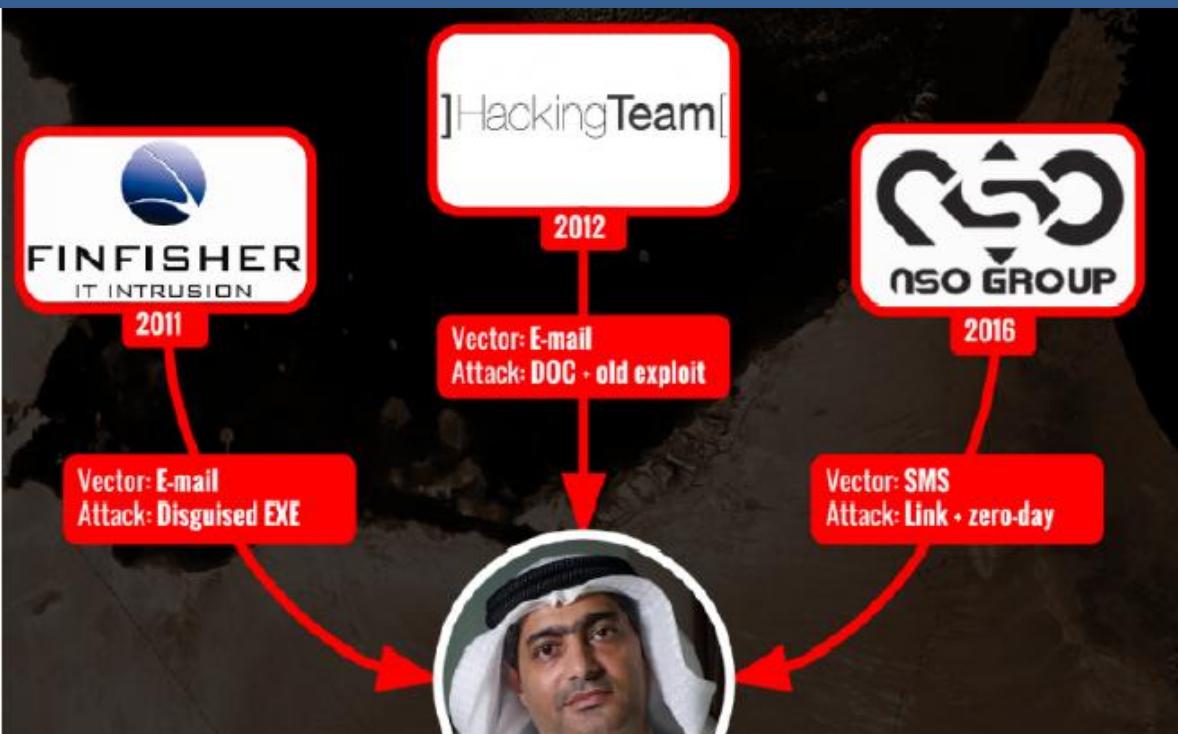
# Ciberespionaje

- Grupos más activos en España:

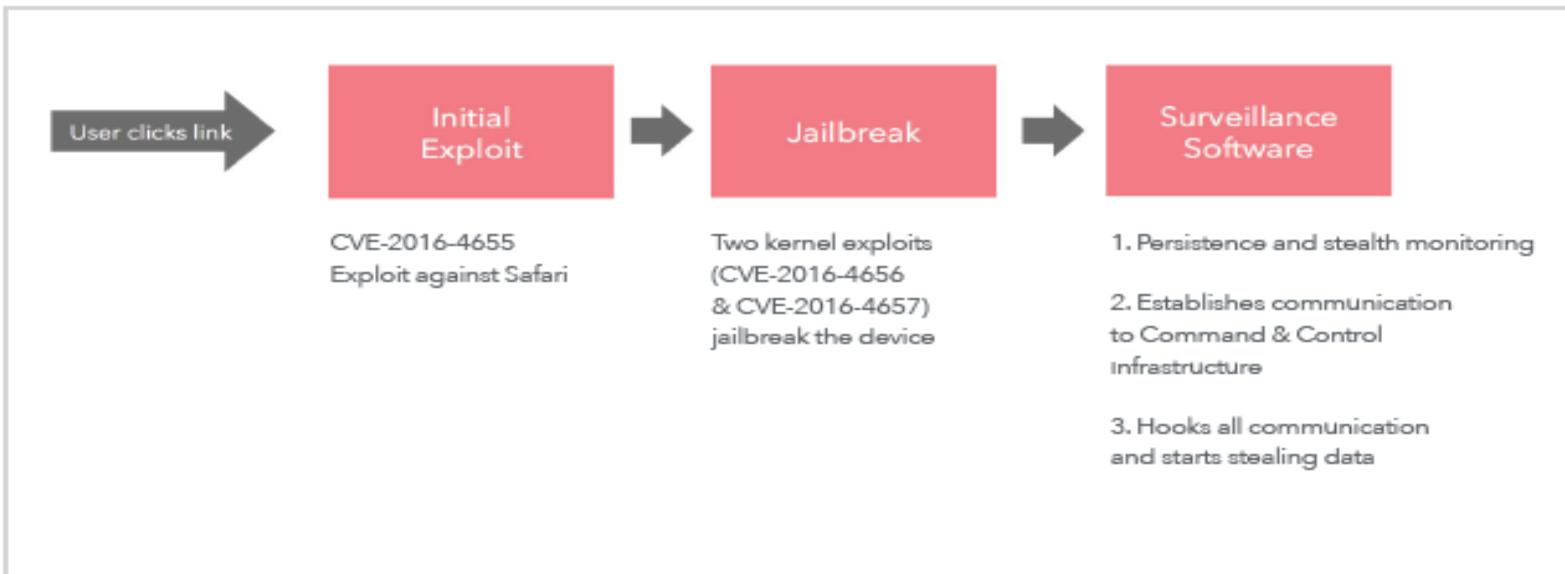


**APT3  
APT27**

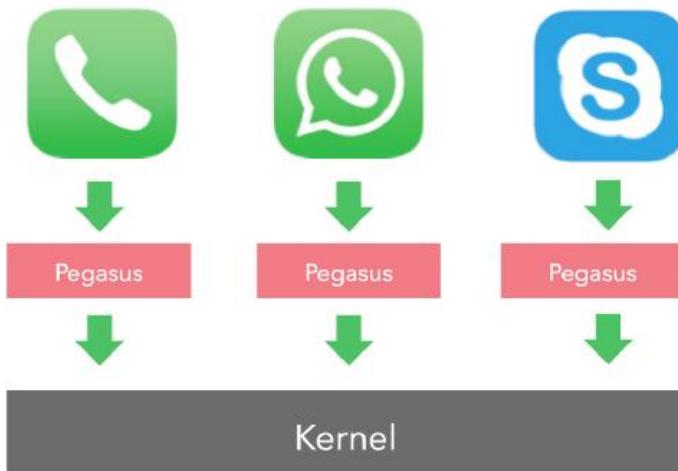




- Gmail
- Facetime
- Facebook
- Line
- Mail.Ru
- Calendar
- WeChat
- Surespot
- Tango
- WhatsApp
- Viber
- Skype
- Telegram
- KakaoTalk



## NSO GROUP PEGASUS



# Tendencias a considerar en 2017

## ❖ **Ciberespionaje**: incremento de actividad

- Actores esponsorizados por estados.
- Se espera mayor variedad de ataques sobre plataformas móviles de personas clave en las organizaciones.

## ❖ **Cibercrimen**: se espera que incremente su actividad y selectividad hacia objetivos más rentables en la infección.

- Variantes de ransomware.
- Código dañino para medios de pago.
- Ataques complejos al sector financiero.
- Denegaciones de servicio distribuidas usando internet de las cosas y venta de servicios a terceros (redes de botnets, herramientas de ataque,...)

## ❖ **Ciberactivismo**: tanto de origen nacional como internacional, continuarán los ataques por denegación de servicio y las desfiguraciones.

- Permanencia/aparición de identidades con elevadas capacidades técnicas.

## ❖ **Ciberyihadismo**: se mantendrá limitado a la propaganda y a la presencia de identidades en redes sociales, así como la realización de ataques no complejos contra objetivos de bajo perfil.

- Asociación o contratación de capacidades relacionadas con el cibercrimen.

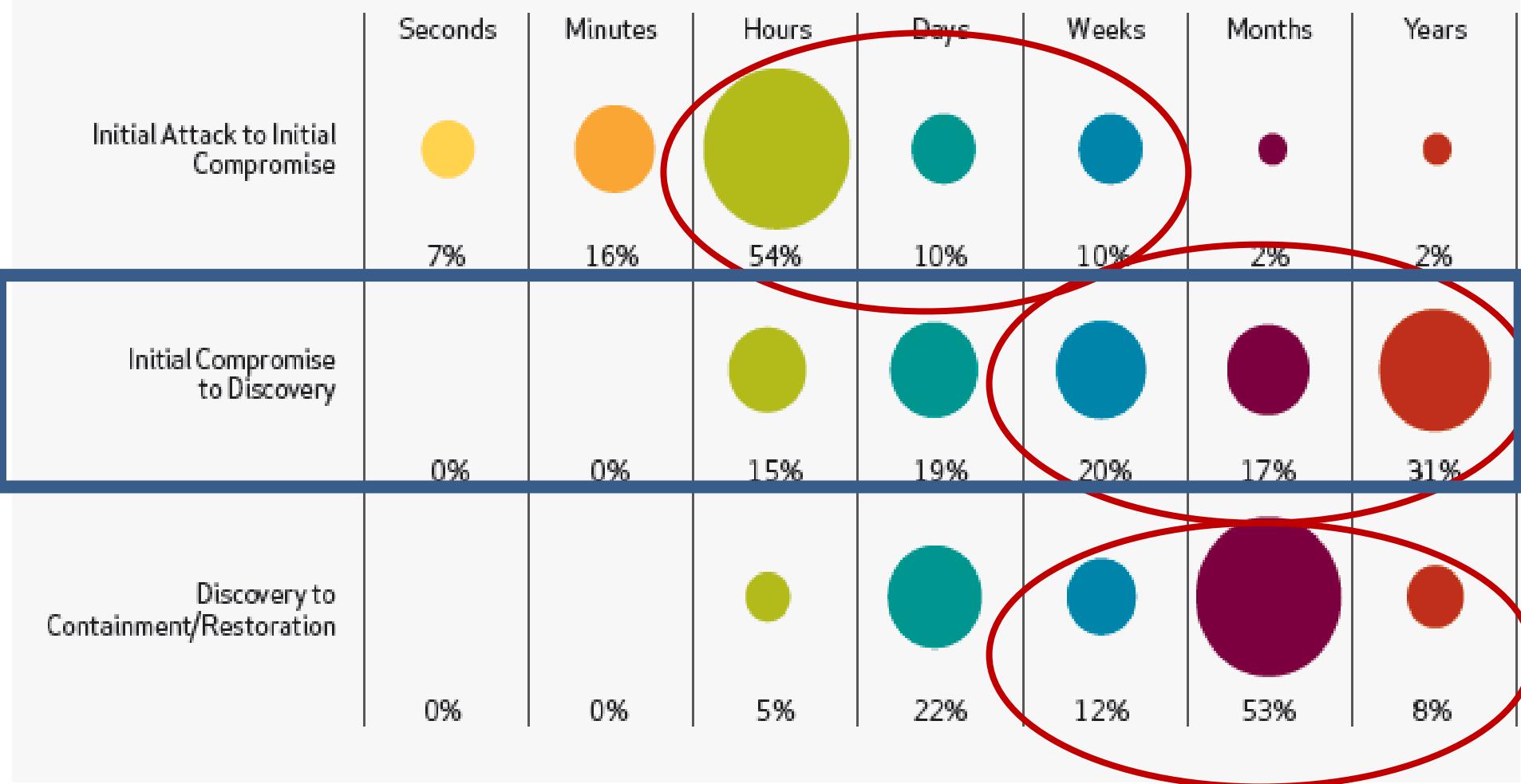
## PARTE DEFENSIVA



- **Privilegios de usuarios**
- **Autenticación de usuario**
- **Redes sociales**
- **Telefonía móvil**
- **Servicios en nube**
- **Unidades de memoria**

# Debilidades de Nuestros Sistemas de Protección

- ✓ Falta de concienciación y desconocimiento del riesgo
- ✓ Sistemas con Vulnerabilidades, escasas configuraciones de seguridad y Seguridad Reactiva. (OBJETIVOS BLANDOS)
- ✓ Poco personal de seguridad y escasa vigilancia
  - ✓ Ausencia herramientas faciliten investigación
- ✓ Mayor superficie de exposición (Redes sociales, Telefonía móvil (BYOD) y Servicios en nube)
- ✓ Afectados NO comparten información. NO comunican incidentes



VERIZON rp\_data-breach-investigations

## DECALOGO

## - DECALELOGO DE CIBERSEGURIDAD -

**01** > Aumentar la capacidad de vigilancia de las redes y los sistemas.  
Es indispensable contar con el adecuado equipo de ciberseguridad.

## Monitorización y correlación de eventos.

Uso de herramientas capaces de monitorizar el tráfico de red, usuarios remotos, contraseñas de administración, etc.

02

**03** > Política de Seguridad Corporativa restrictiva.  
Adecuación progresiva de los permisos de usuario, servicios en la "nube" y la utilización de dispositivos y equipos propiedad del usuario (BYOD).

## Configuraciones de seguridad en todos los componentes de la red corporativa.

Se incluirán los equipos móviles y portátiles.

04

**05** > Uso de productos, equipos y servicios confiables y certificados.  
Redes y sistemas acreditados para información sensible o clasificada

## Automatizar e incrementar el intercambio de información.

Reciprocidad con otras organizaciones y Equipos de Respuesta a Incidentes de Seguridad de la Información (CERTs).

06

**07** > Compromiso de la Dirección con la ciberseguridad.  
Los cargos directivos deben ser los primeros en aceptar que existen riesgos y promover las políticas de seguridad.

## Formación y la Sensibilización de usuarios (eslabón más débil de la cadena).

Todos y cada uno de los niveles de la organización (dirección, gestión e implantación) deben ser conscientes de los riesgos y actuar en consecuencia

08

**09** > Atenerse a la legislación y buenas prácticas.  
Adecuación a los distintos estándares (en el caso de las Administraciones Públicas al Esquema Nacional de Seguridad -ENS-).

## Trabajar como si se estuviese comprometido.

Suponer que los sistemas están ya comprometidos o lo estarán pronto y proteger los activos fundamentales.

10

**1. Aumentar la capacidad de Vigilancia.**

**2. Herramientas de Gestión Centralizada.**

3. Política de seguridad.

4. Aplicar configuraciones de seguridad.

5. Empleo de productos confiables y certificados.

6. Concienciación de usuarios.

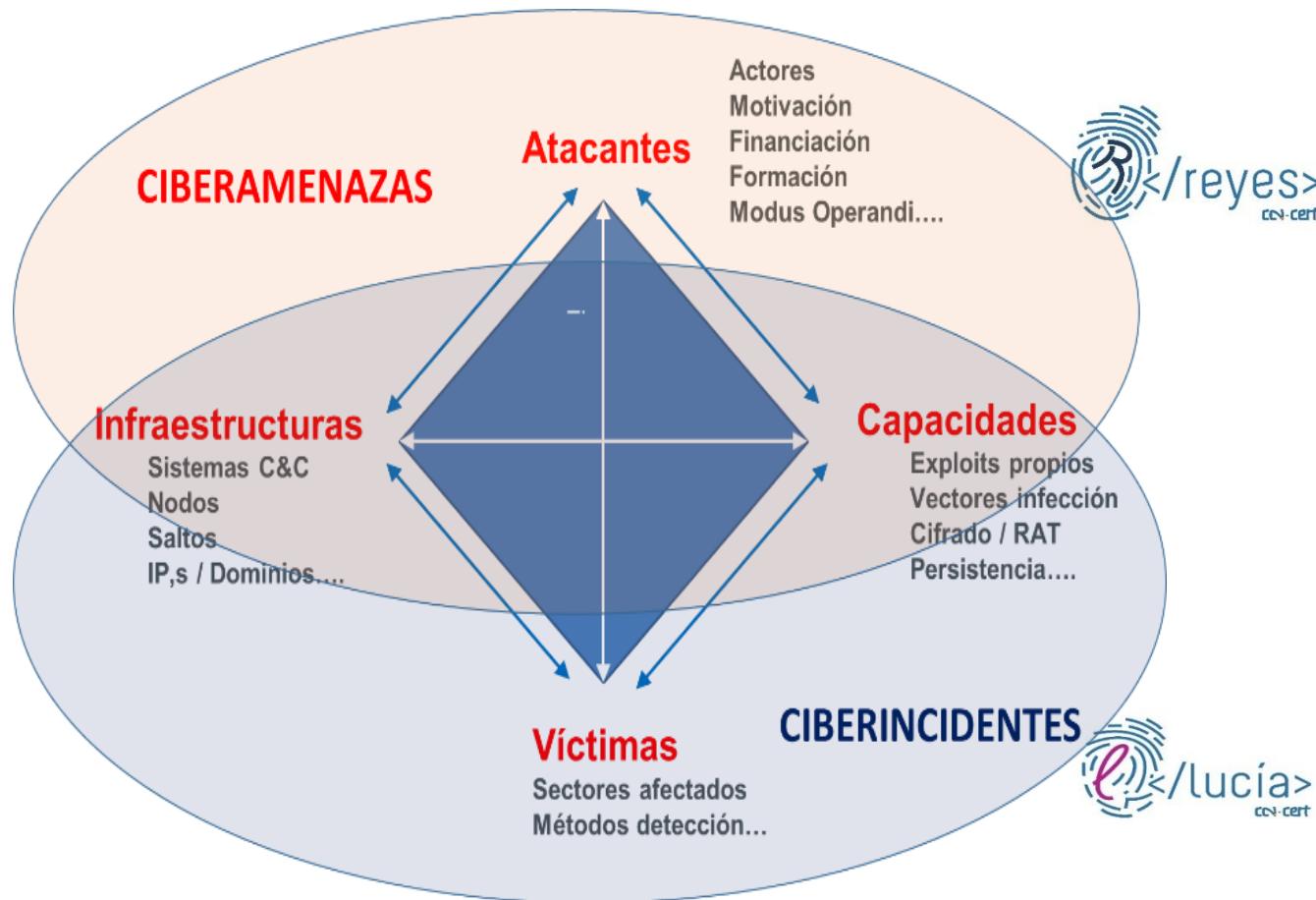
7. Compromiso de dirección (Aceptación Riesgo)

8. Legislación y Buenas Prácticas.

**9. Intercambio de Información.**

**10. Trabajar como si se estuviera comprometido.**

## INTERCAMBIO Y CONOCIMIENTO DE LA AMENAZA



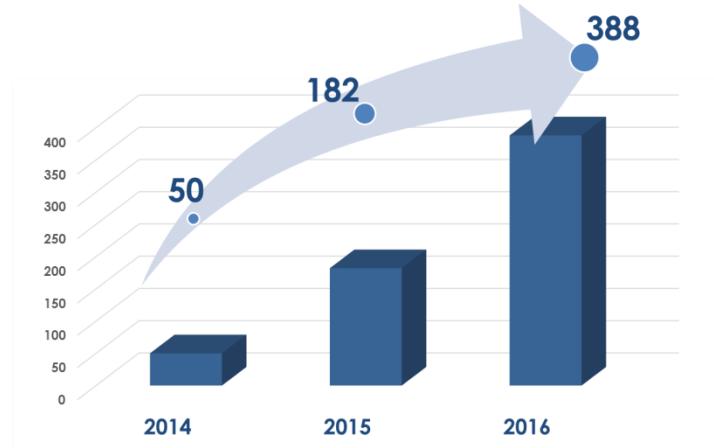
# UNIVERSIDADES



## RESULTADOS GENERALES

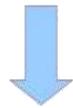


## RESULTADOS SECTORIALES



# Esquema Nacional de Seguridad

Principios básicos



Requisitos mínimos:



Medidas de seguridad

(Protección adecuada de la información)

- a) Seguridad integral
- b) Gestión de riesgos
- c) Prevención, reacción y recuperación
- d) Líneas de defensa
- e) Reevaluación periódica
- f) La seguridad como función diferenciada

6

- a) Organización e implantación del proceso de seguridad.
- b) Análisis y gestión de los riesgos.
- c) Gestión de personal.
- d) Profesionalidad.
- e) Autorización y control de los accesos.
- f) Protección de las instalaciones.
- g) Adquisición de productos.
- h) Seguridad por defecto.
- i) Integridad y actualización del sistema.
- j) Protección de la información almacenada y en tránsito.
- k) Prevención ante otros sistemas de información interconectados.
- l) Registro de actividad.
- m) Incidentes de seguridad.
- n) Continuidad de la actividad.
- o) Mejora continua del proceso de seguridad.

15

- a) Marco organizativo.
- b) Marco operacional.
- c) Medidas de protección.

75



1. Los **Principios básicos**, que sirven de guía.
2. Los **Requisitos mínimos**, de obligado cumplimiento.
3. La **Categorización de los sistemas** para la adopción de **medidas de seguridad** proporcionadas.
4. La **auditoría de la seguridad** que verifique el cumplimiento del ENS.
5. La **respuesta a incidentes de seguridad**. Papel del CCN- CERT.
6. El uso de **productos certificados**. Papel del Organismo de Certificación (CCN).
7. La **formación y concienciación**.



## RESULTADOS INES 2016 – RESULTADOS MEDIDAS ANEXO II

ESQUEMA NACIONAL DE SEGURIDAD  
75 MEDIDAS DE SEGURIDAD**MARCO ORGANIZATIVO**

El marco organizativo está constituido por un conjunto de medidas relacionadas con la organización global de la seguridad

4

POLÍTICA DE SEGURIDAD  
NORMATIVA DE SEGURIDAD  
PROCEDIMIENTOS DE SEGURIDAD  
PROCESO DE AUTORIZACIÓN

**MARCO OPERACIONAL**

El marco operacional está constituido por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin

31

PLANIFICACIÓN  
CONTROL DE ACCESO  
EXPLOTACIÓN  
SERVICIOS EXTERNOS  
CONTINUIDAD DEL SERVICIO  
MONITORIZACIÓN DEL SISTEMA

**MEDIDAS DE PROTECCIÓN**

Las medidas de protección, se centrarán en proteger activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad.

40

INSTALACIONES E INFRAESTRUCTURAS  
GESTIÓN DEL PERSONAL  
PROTECCIÓN DE LOS EQUIPOS  
PROTECCIÓN DE LAS COMUNICACIONES  
PROTECCIÓN SOPORTES DE INFORMACIÓN  
PROTECCIÓN APLICACIONES INFORMÁTICAS  
PROTECCIÓN DE LA INFORMACIÓN  
PROTECCIÓN DE LOS SERVICIOS

Los resultados abarcan 42 Universidades **504 sistemas TIC**  
que dan servicio a **602.337 usuarios**.

# RESULTADOS INES 2016 – INFORMES

## RESULTADOS GENERALES

USO OFICIAL

GOBIERNO DE ESPAÑA MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA

CCN Centro Criptológico Nacional

INFORME EJECUTIVO CCN-CERT IT 05/17  
RESULTADOS GENERALES

INFORME NACIONAL DEL ESTADO DE SEGURIDAD DE LOS SISTEMAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN



Abril 2017

## RESULTADOS SECTORIALES

USO OFICIAL

INFORME EJECUTIVO CCN-CERT IT 06/17  
RESULTADOS  
ADMINISTRACIÓN GENERAL DEL ESTADO

INFORME NACIONAL DEL ESTADO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

INFORME EJECUTIVO CCN-CERT IT 06/17  
RESULTADOS  
COMUNIDADES Y CIUDADES AUTONOMAS

INFORME NACIONAL DEL ESTADO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

INFORME EJECUTIVO CCN-CERT IT 08/17  
RESULTADOS  
ENTIDADES LOCALES

INFORME NACIONAL DEL ESTADO DE SEGURIDAD DE LOS SISTEMAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

INFORME EJECUTIVO CCN-CERT IT 09/17  
RESULTADOS  
UNIVERSIDADES

INFORME NACIONAL DEL ESTADO DE SEGURIDAD DE LOS SISTEMAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN



Abril 2017

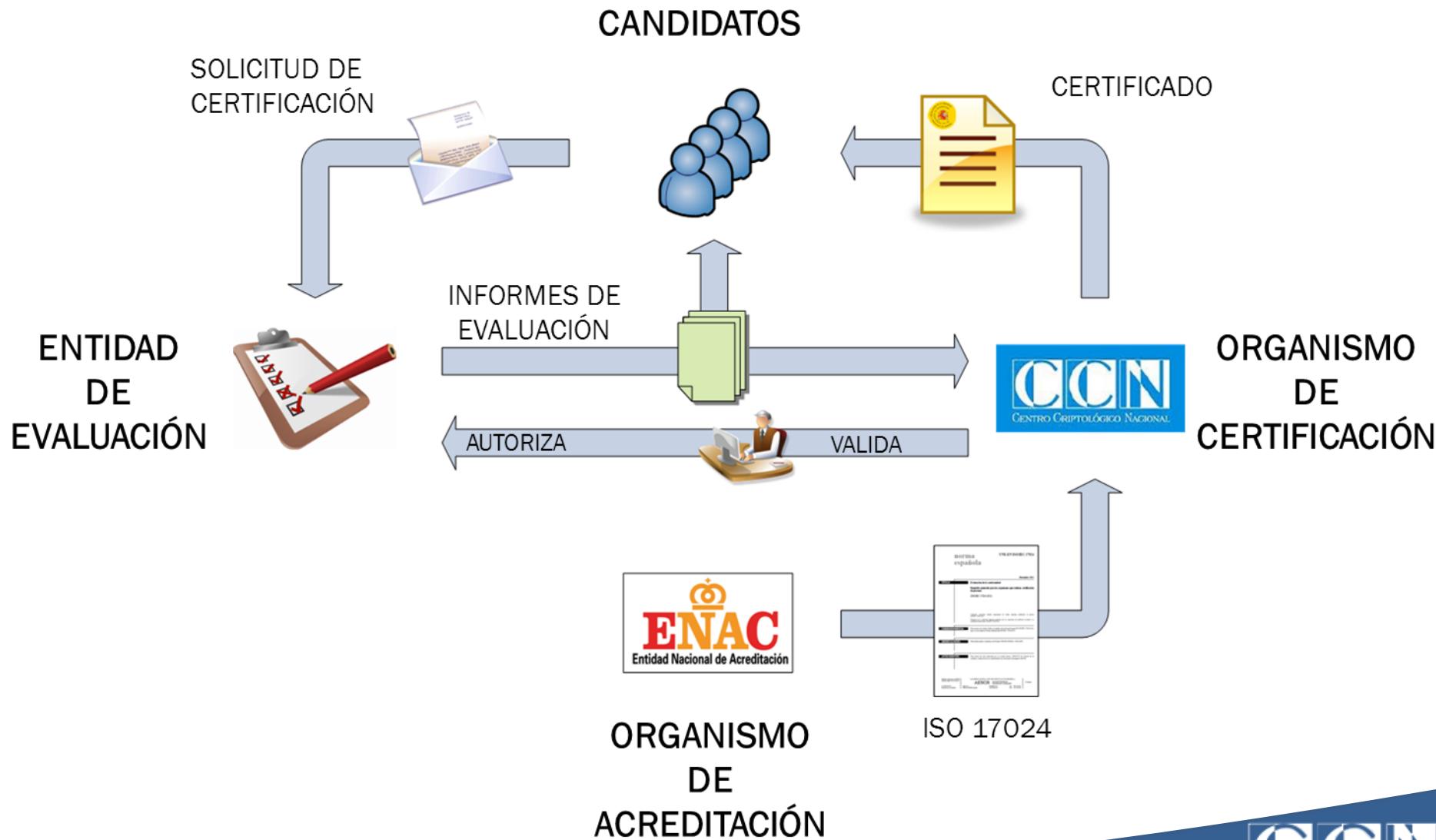
## RESULTADOS INES 2016 – CONCLUSIONES

- 1. Nivel de cumplimiento 2016 en las EE.LL. es BAJO (56%).** Retraso en la implementación.
- 2. Las EE.LL. tienen mucho recorrido pendiente en el proceso de adecuación al ENS,** siendo la certificación del cumplimiento del ENS el aspecto más significativo al respecto.
- 3. Es necesario mejorar algunos indicadores:**
  - Concienciación y Formación
  - Recursos
  - Mecanismos de Continuidad
- 4. Responsable de seguridad no es suficiente.**
  - Necesidad de equipos de seguridad
- 5. Pocas tareas de vigilancia de la red.**
  - No revisión de logs / No hay monitorización real.

# Invertir en CIBERSEGURIDAD al menos una cantidad equivalente que en SEGURIDAD FÍSICA.



# Esquema Nacional de Certificación de Profesionales en Ciberseguridad



## ➤ E-Mails

- [ccn-cert@cni.es](mailto:ccn-cert@cni.es)
- [info@ccn-cert.cni.es](mailto:info@ccn-cert.cni.es)
- **[ccn@cni.es](mailto:ccn@cni.es)**
- [Sat-inet@ccn-cert.cni.es](mailto:Sat-inet@ccn-cert.cni.es)
- [redsara@ccn-cert.cni.es](mailto:redsara@ccn-cert.cni.es)
- [organismo.certificacion@cni.es](mailto:organismo.certificacion@cni.es)

## ➤ Websites

- [www.ccn.cni.es](http://www.ccn.cni.es)
- [www.ccn-cert.cni.es](http://www.ccn-cert.cni.es)
- [www.oc.ccn.cni.es](http://www.oc.ccn.cni.es)



# Gracias