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 Criticas
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 hibrido	Big Data Redes operacionales IoT

FUNCIONES CCN

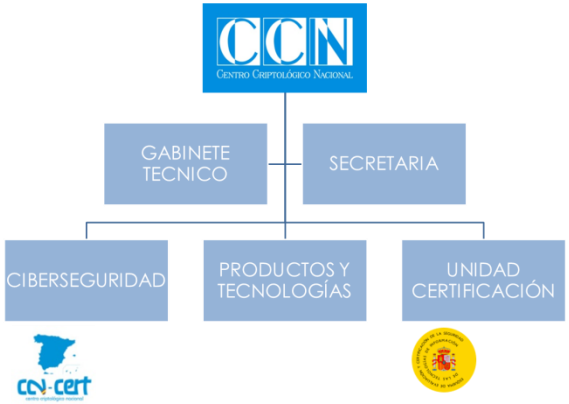
CCN-CERT. SERVICIOS

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)

MINISTERIO DE DEFENSA
DGAM
Dirección General de Armamento y Material

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

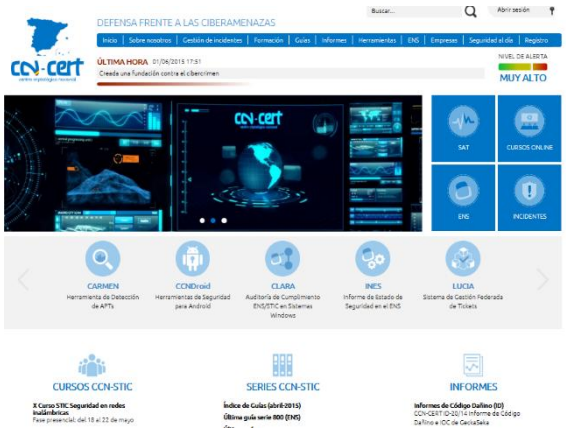
Contribuir a la mejora de la **ciberseguridad española**, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente al **Sector Público** a afrontar de forma activa las nuevas ciberamenazas.

COMUNIDAD

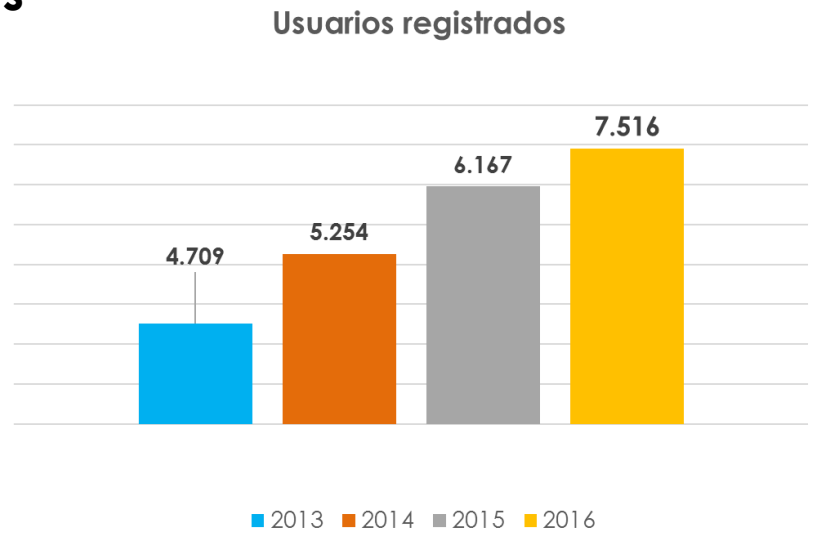
Responsabilidad en ciberataques sobre:

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

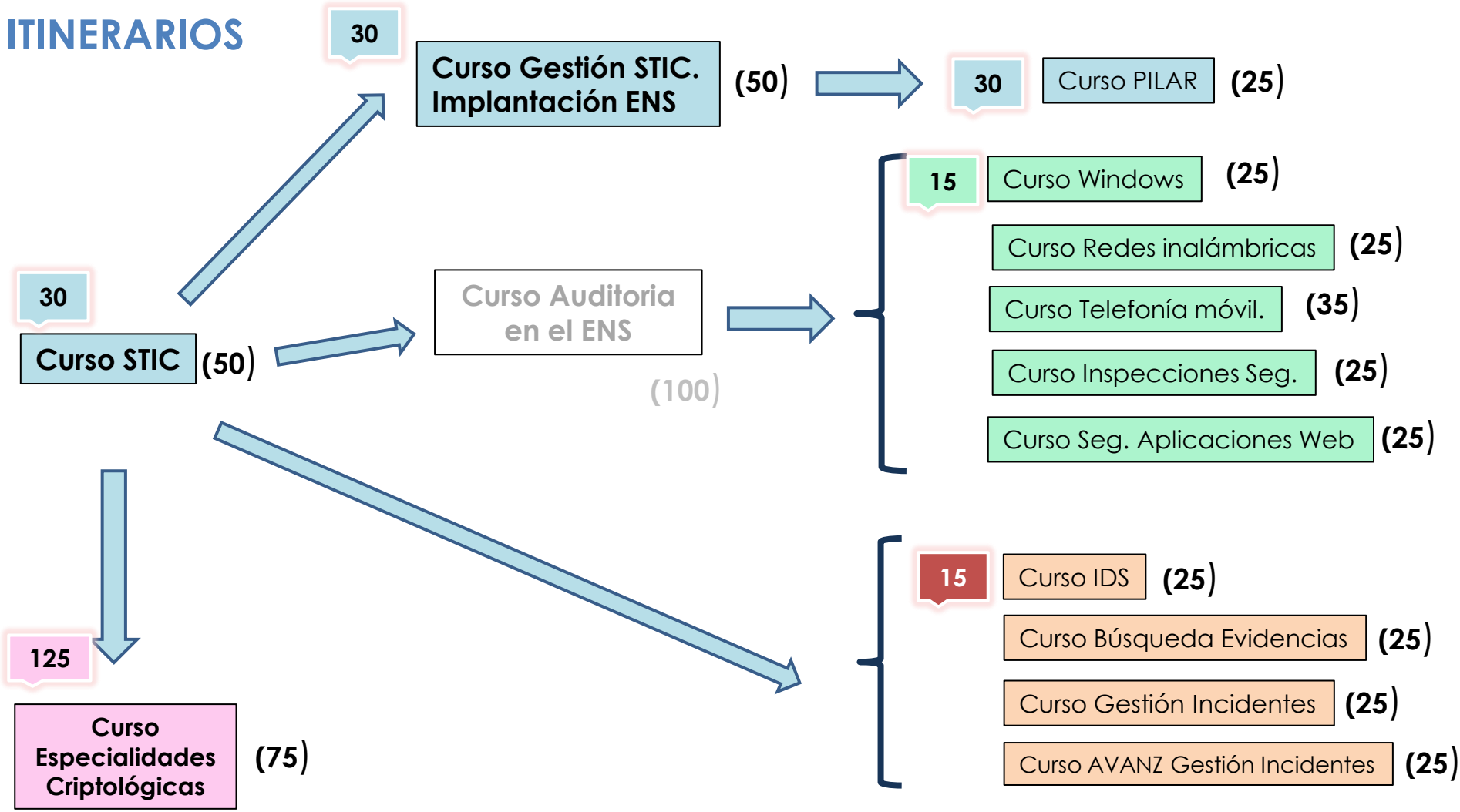
SERVICIOS



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**

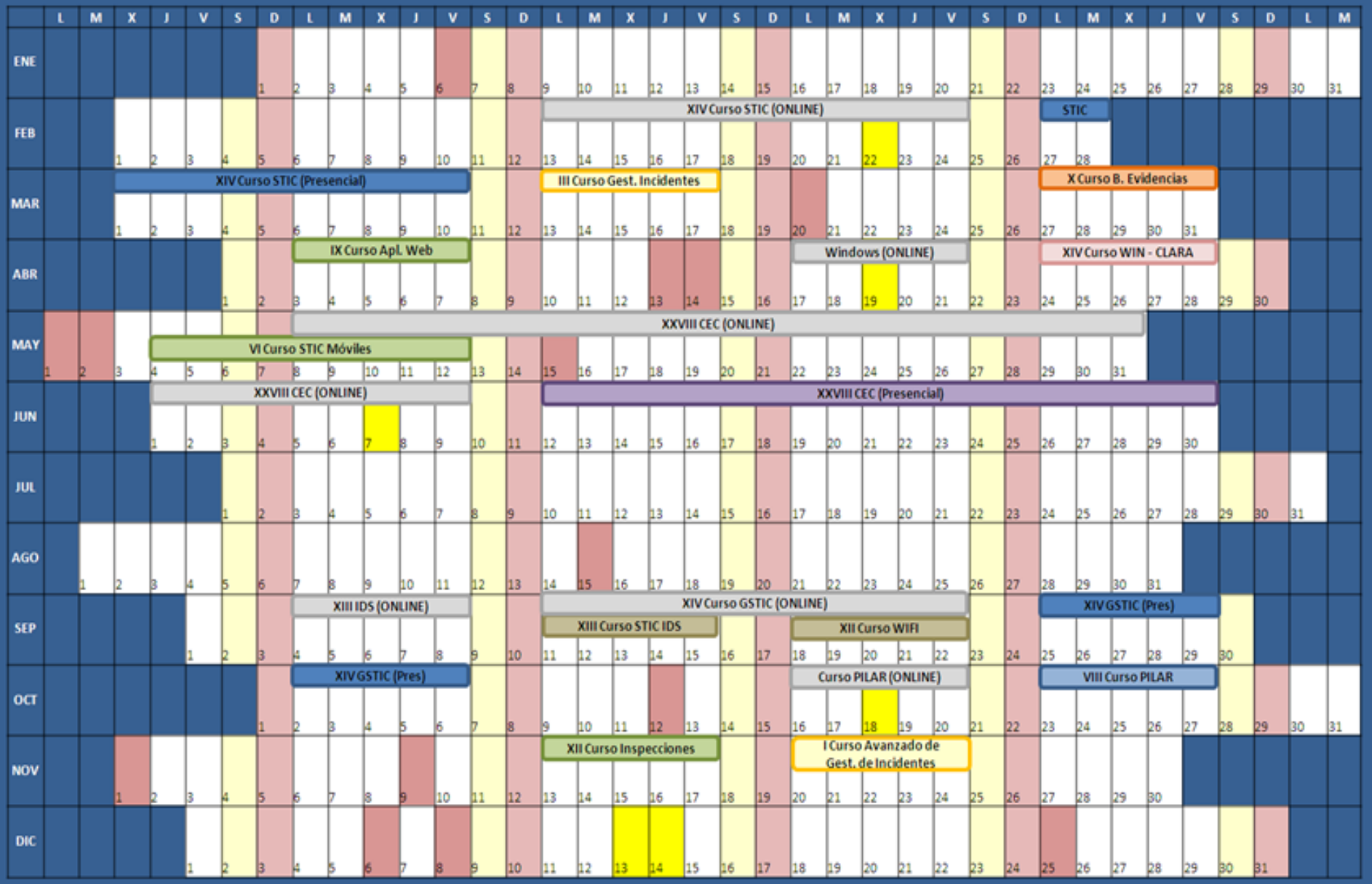


ITINERARIOS



PLAN DE FORMACIÓN

Centro Criptológico Nacional 2017



Plan 2016 / 2017

FORMACIÓN A DISTANCIA

Profesor con plataforma videoconferencia y chat de preguntas

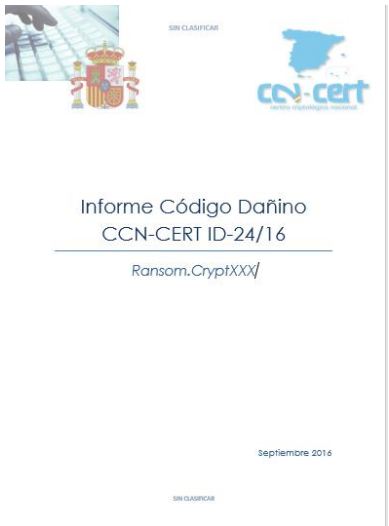
Formación a Distancia

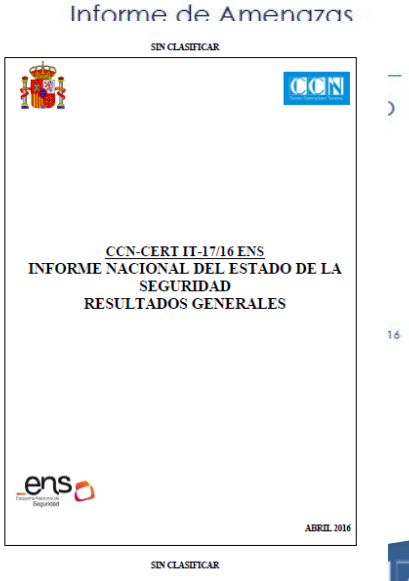
1. Actualización Esquema Nacional de Seguridad (4 horas) (Dic 16)
2. CCN-STIC 824 e INES (4 horas) (Dic 16)
3. LUCIA. Gestión de Incidentes (4 horas) (Mayo)
4. CLARA. Auditoria de sistemas Windows (4 horas)(Junio)
5. ROCIO. Auditoria de equipos de comunicaciones (4 horas) (Julio)
6. Análisis de Malware (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

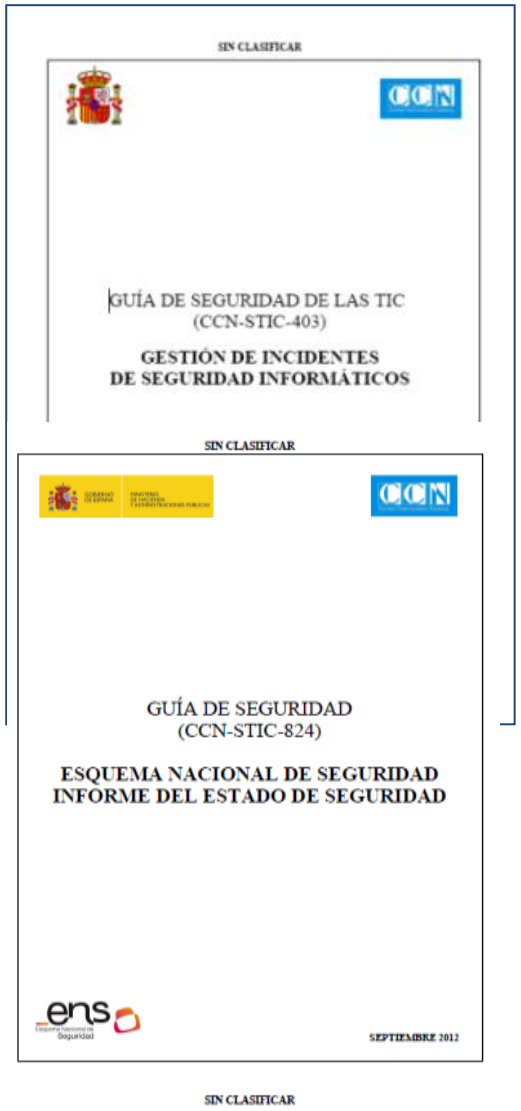
CCN-STIC 400: Guías Generales

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

- sat-inet
- sat-sara
- carmen

SONDA AGE

- sat-ics

ANÁLISIS

- marta
- maría

AUDITORÍA

- pilar
- clara
- inés
- rocio
- claudia

INTERCAMBIO

- lucía
- reyes
- loreto
- vanesa

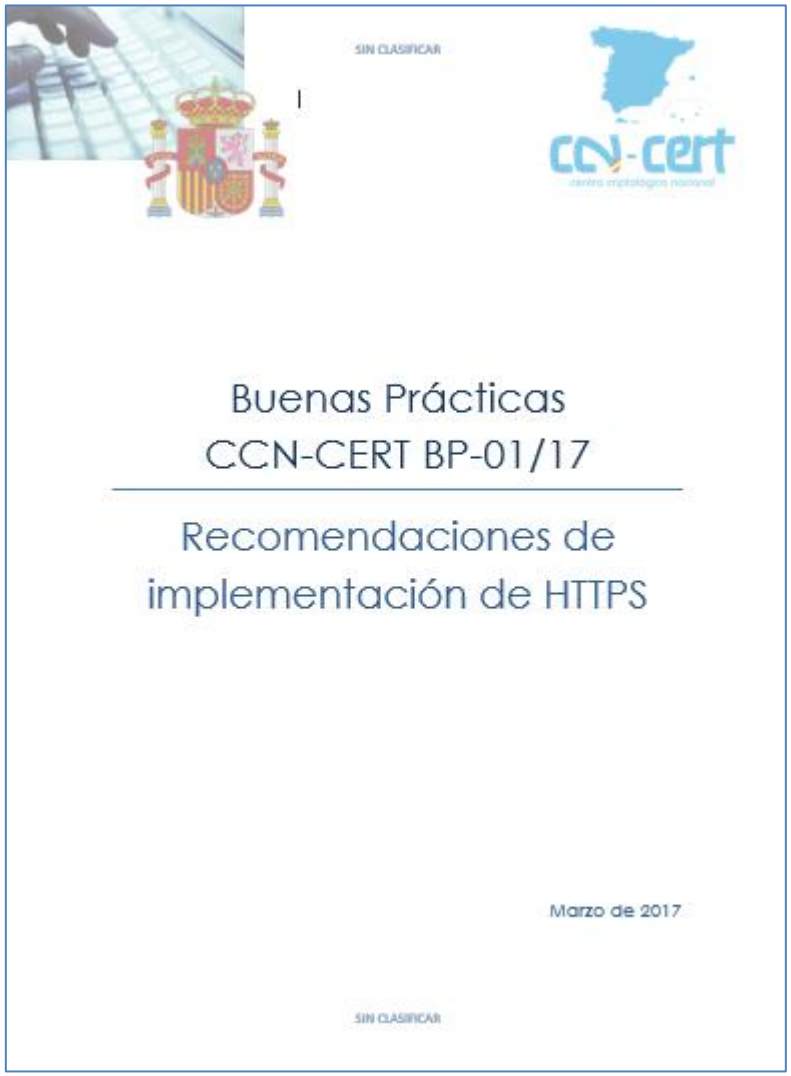
IMPLEMENTACIÓN HTTPS

IMPLEMENTACIÓN HTTPS

08.04.2017 Presentación solicitud
19.05.2017 Finalización solicitud
08.2017 Resultados 1ª vuelta
11.2017 Resultados 2ª vuelta

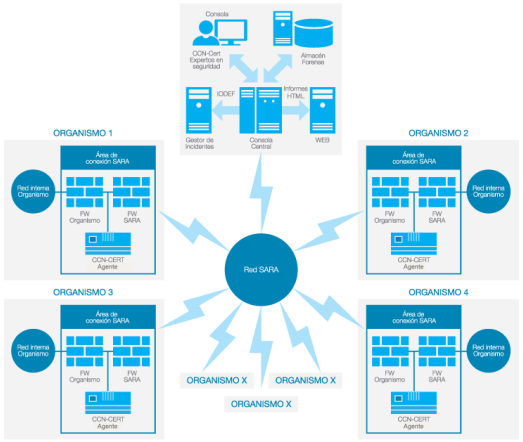
Portal web parte privada portal

estudiohttps@ccn-cert.cni.es

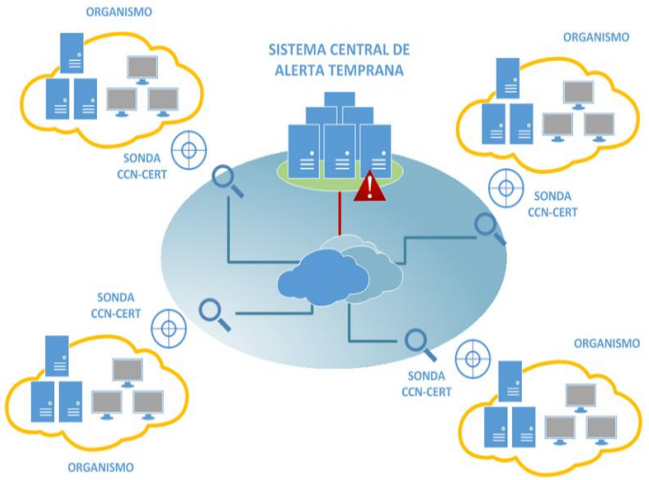


Sistemas de Alerta Temprana (SAT)

- **RED SARA [SAT- SARA]**
  - Servicio para la Intranet Administrativa
  - Coordinado con MINHFP-SGAD
  - **50 Áreas de Conexión**



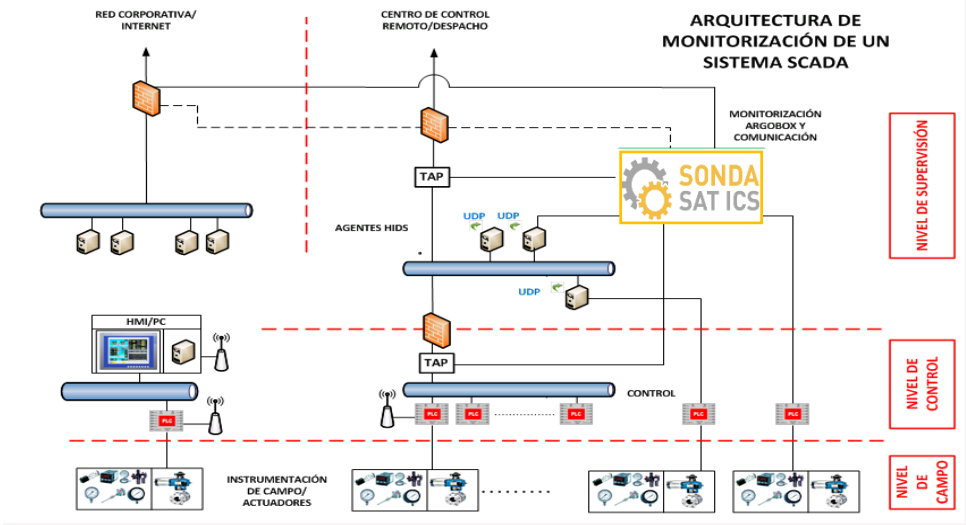
- **SALIDAS DE INTERNET [SAT INET]**
  - Servicio por suscripción
  - Basado en despliegue de sondas.
  - **156 Organismos / 157 sondas**
  - Últimas incorporaciones: **Región Murcia, Ayto. Valencia, C.A. Ceuta, Tribunal de Cuentas, Universidad Pablo Olavide, ICO, Junta Andalucía, Puerto Gijón, Parlamento 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)**



</sat-ics>

GOBIERNO DE ESPAÑA · MINISTERIO DE AGRICULTURA, ALIMENTACIÓN Y MEDIO AMBIENTE · CONFEDERACIÓN HIDROGRÁFICA DEL JÚCAR

EMASESA

valenciaport

GOBIERNO DE ESPAÑA · MINISTERIO DE AGRICULTURA Y PESCA, ALIMENTACIÓN Y MEDIO AMBIENTE · CONFEDERACIÓN HIDROGRÁFICA DEL TAJO

GOBIERNO DE ESPAÑA · MINISTERIO DE AGRICULTURA Y PESCA, ALIMENTACIÓN Y MEDIO AMBIENTE · CONFEDERACIÓN HIDROGRÁFICA DEL GUADALQUIVIR

GOBIERNO DE ESPAÑA · MINISTERIO DE FOMENTO · Puertos del Estado

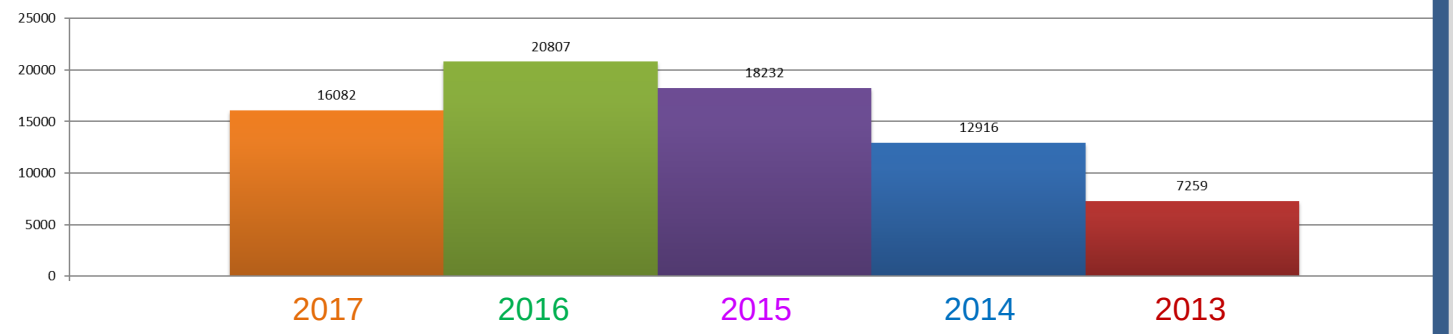
SECTOR PÚBLICO

CNPIC
CENTRO NACIONAL PARA LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS

PELIGROSIDAD DE LOS INCIDENTES

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

ESTADÍSTICAS GLOBALES



Acumulado Anual

2017 16082 (14%)

2016: 20.940 (15%)

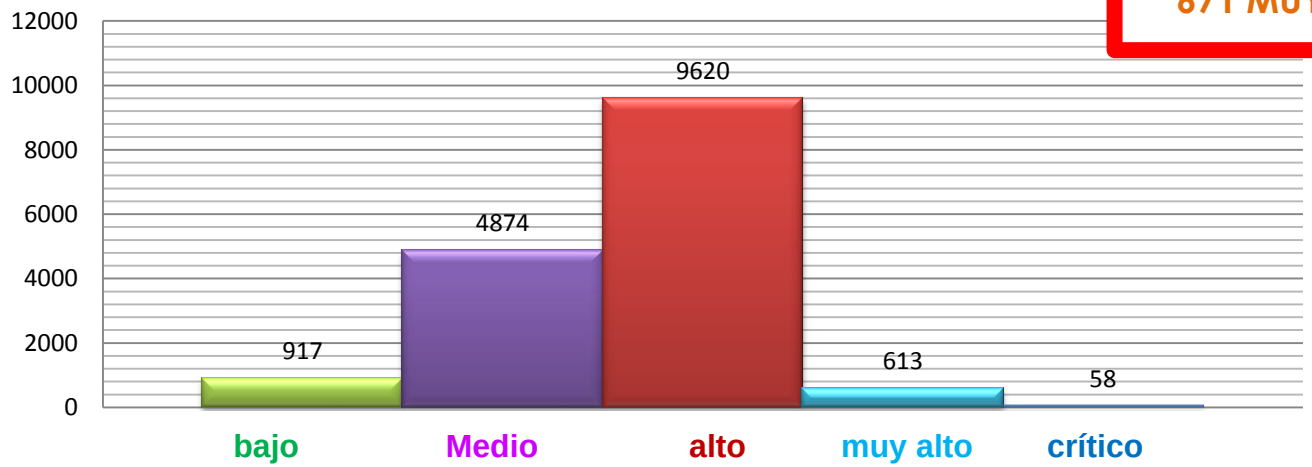
2015: 18.232 (41%)

2014: 12.916 (78%)

2013: 7.259

620 MUY ALTOS Y CRITICOS en 2016

671 MUY ALTOS Y CRITICOS en 2017

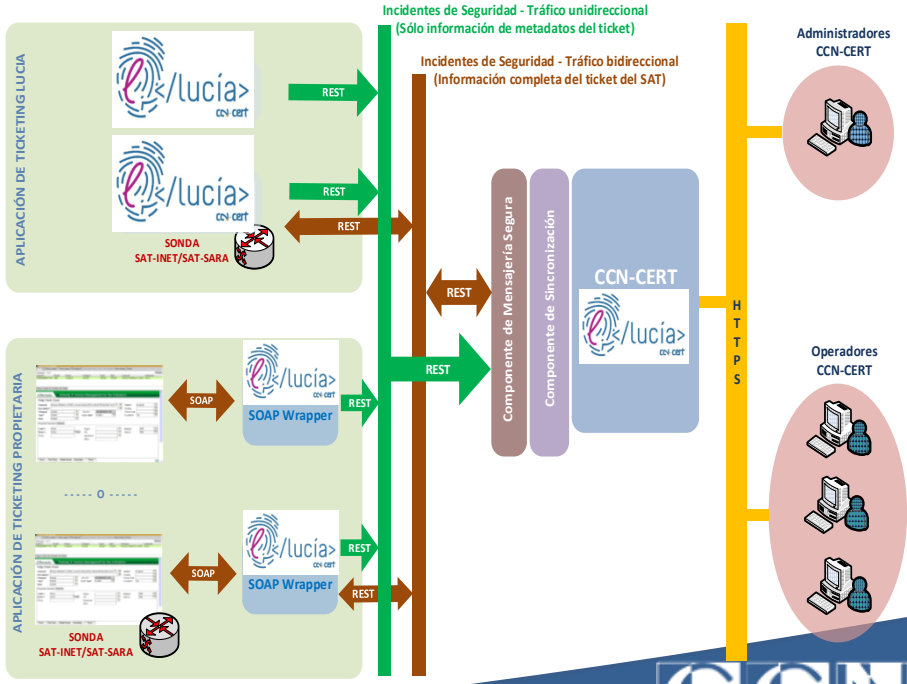


Listado Unificado de Coordinación de Incidentes y Amenazas

- 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
TOTAL	20940	18851	810	960	319

	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	84	383	31
MAYO	2017	1446	94	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
TOTAL	16082	11867	817	3197	201

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 común Y ESTructurado de amenazas y código dañino)

Servicios Inteligencia

SIGINT

CAPACIDADES FORENSES ING. INVERSA

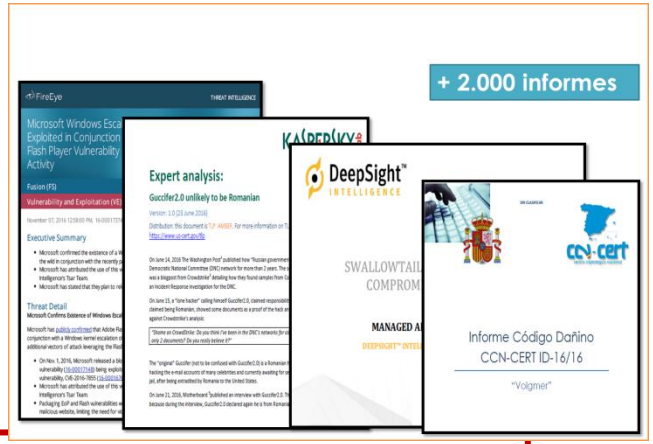
Elaboración

</lucia> CCN-CERT

</sat-inet>

carmen

</reyes> CCN-CERT



Federación feeds

KASPERSKY lab · Symantec · FireEye · Microsoft · S2 GRUPO · InnoTec System · Entelgy · CERT-EU · panda security

CCN-CERT centro criptológico nacional

CIBERAMENAZAS

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

Informe de Amenazas
CCN-CERT IA-16/16

Ciberespionaje

Informe de Amenazas
CCN-CERT IA-10/15

Campañas de
Ciberespionaje

Informe de Amenazas
CCN-CERT IA-04/17

Hacktivismo y
Ciberyihadismo
Informe Resumen 2016

Marzo de 2017

Informe de Amenazas
CCN-CERT IA-06/17

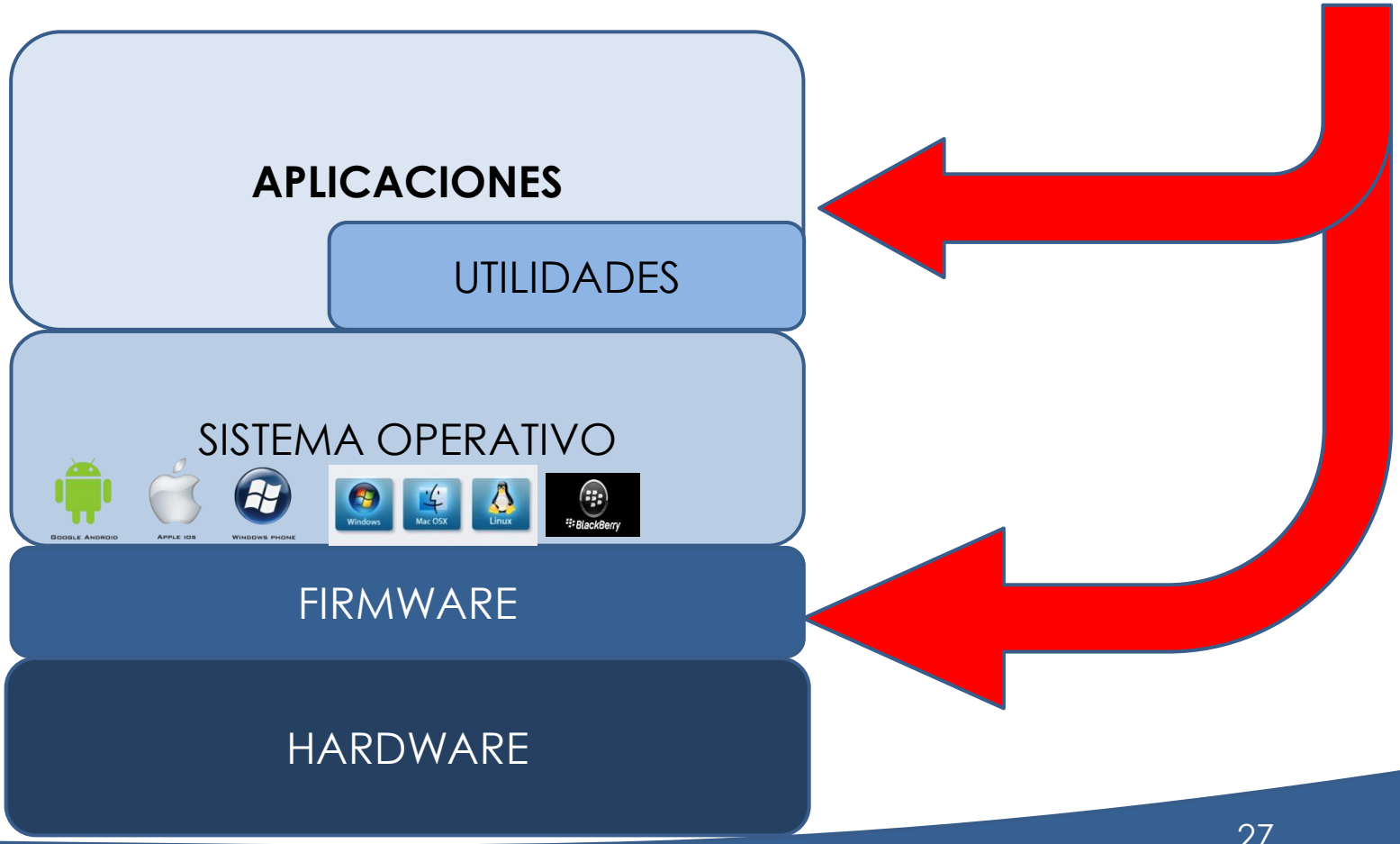
Dispositivos y
Comunicaciones Móviles
Informe Resumen 2016

Abril de 2017

¿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

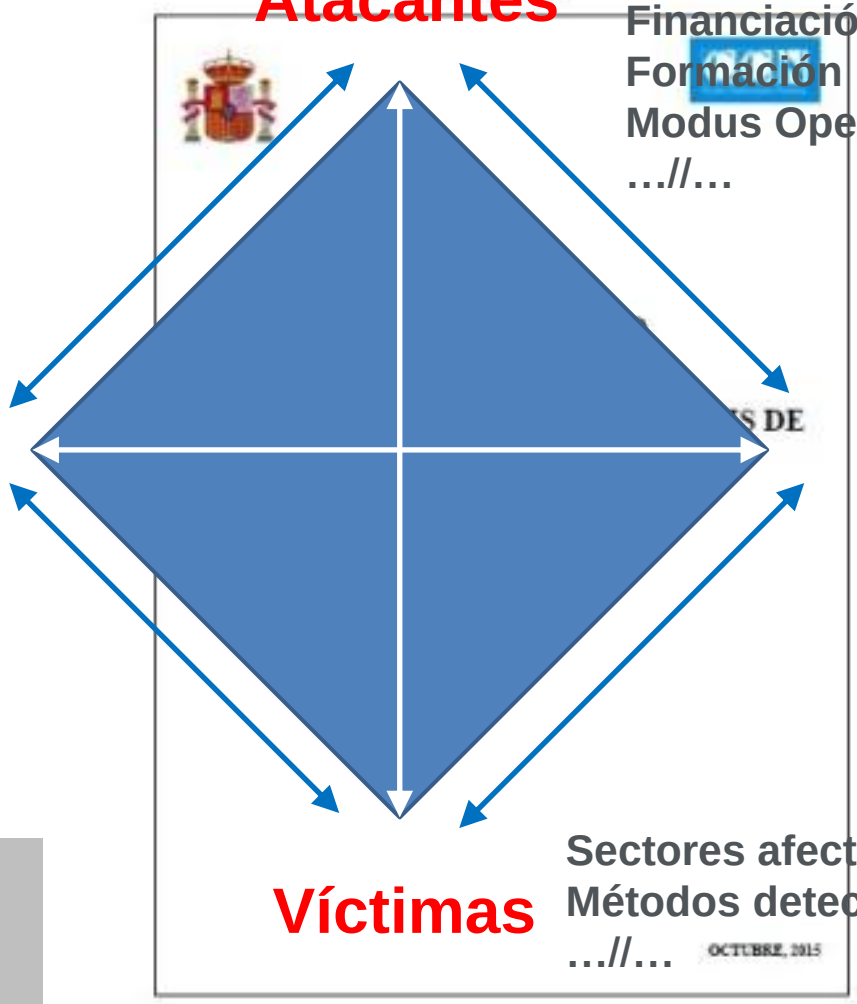
- **+ 75 organismos notificados**
- **+ 25 Incidentes / 4 críticos**

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.**

CCN-STIC 425



Estudio de Tácticas / Técnicas / Procedimientos (TTP)

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

Usuarios internos

=

3. Ciberactivismo
   - ANONYMOUS y otros grupos

+

4. Uso de INTERNET por terroristas
   - Objetivo : Comunicaciones , obtención de información, propaganda, **radicalización** o financiación

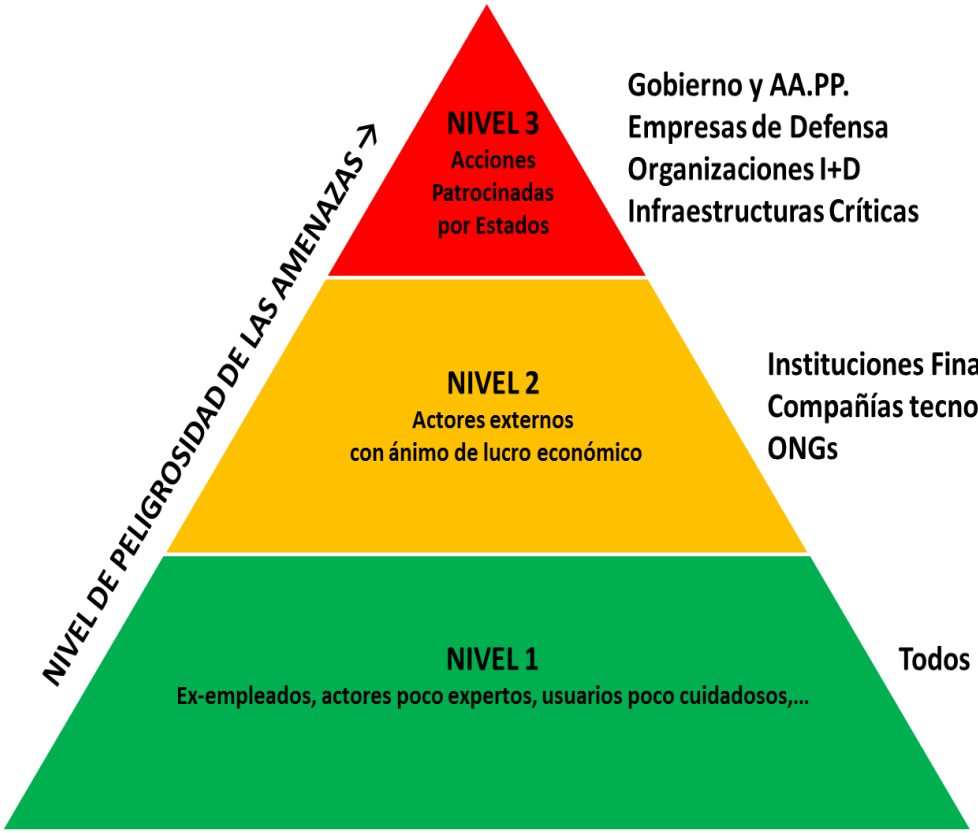
+

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

APT

Carbanak
AGENT BTZ
Octubre Rojo
RCS

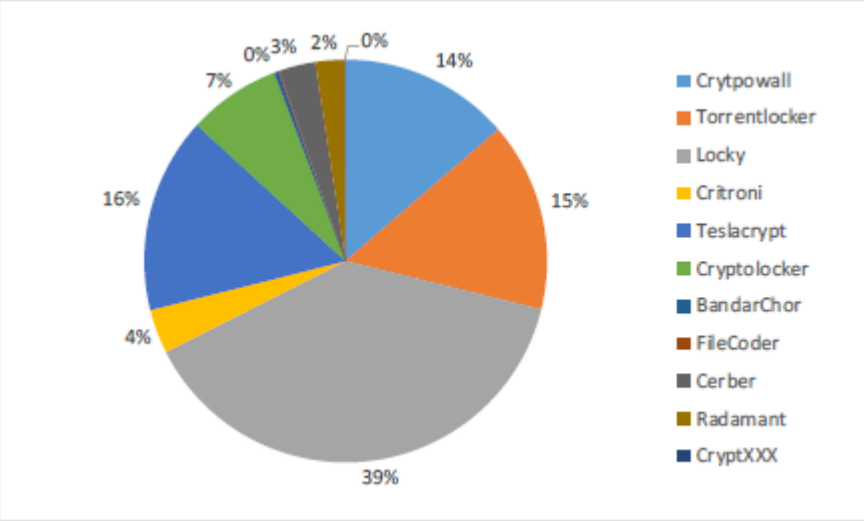
Ramsonware
Botnets
Otro Malware

Ransomware

2015

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

Total: 427

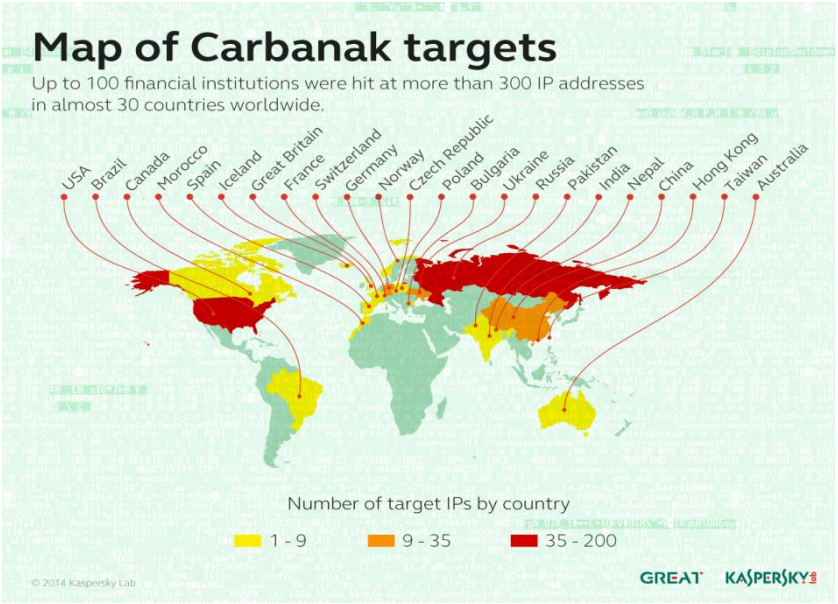


2016

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

CARBANAK



- 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**
  - 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

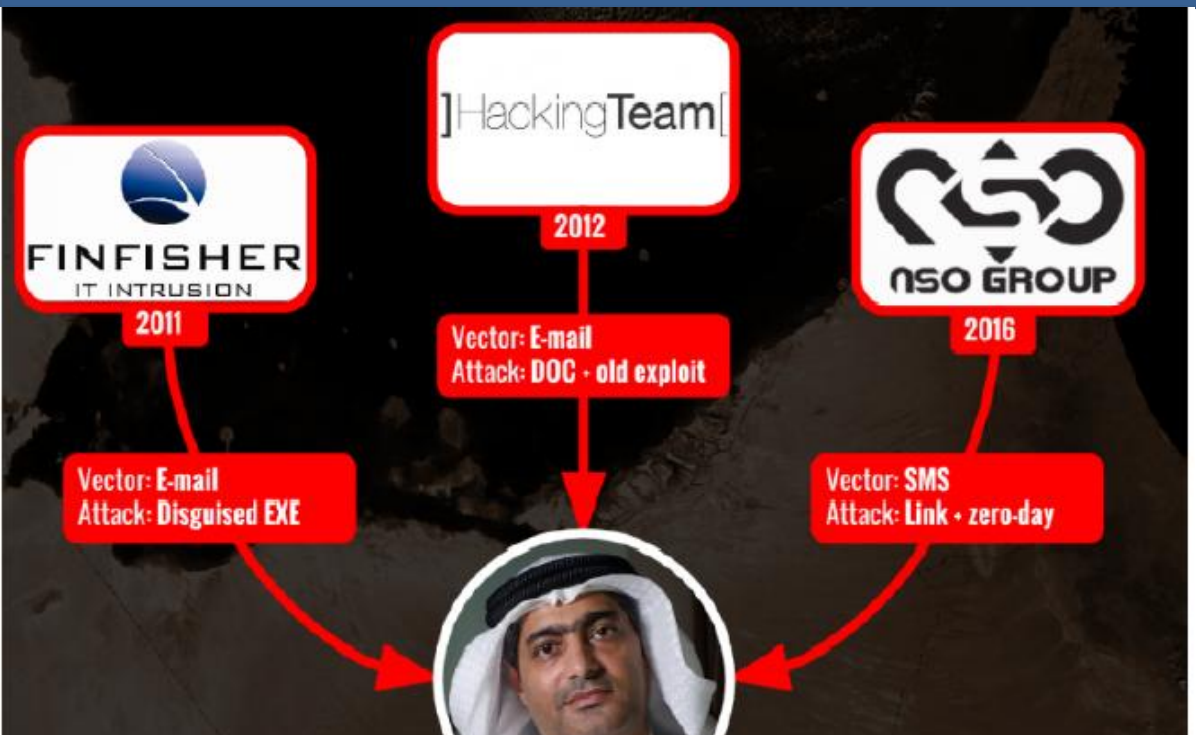
    tecnológicos, económicos, humanos

APT

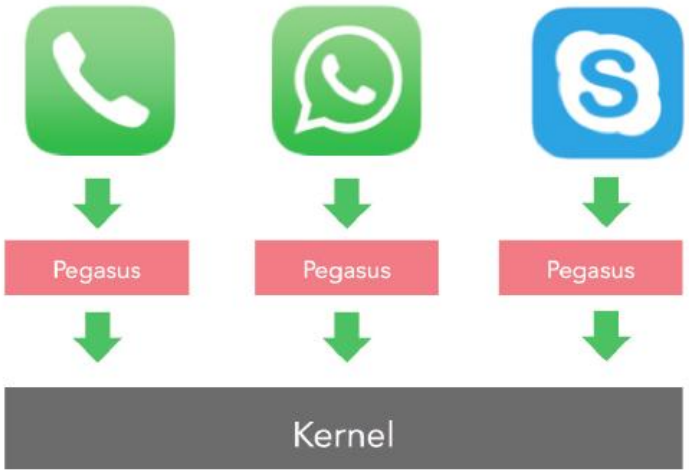

Goblin Panda
Vixen Panda
Deep Panda
Emissary Panda
Pirate Panda
Numbered Panda
Lotus Panda
Pitty Panda
Gothic Panda
Predator Panda
Dynamite Panda
Temper Panda
Pale Panda
Violin Panda
Hurricane Panda
Sabre Panda
Samurai Panda
Dagger Panda
Aurora Panda
Maverick Panda
Keyhole Panda
Stone Panda
Spicy Panda
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

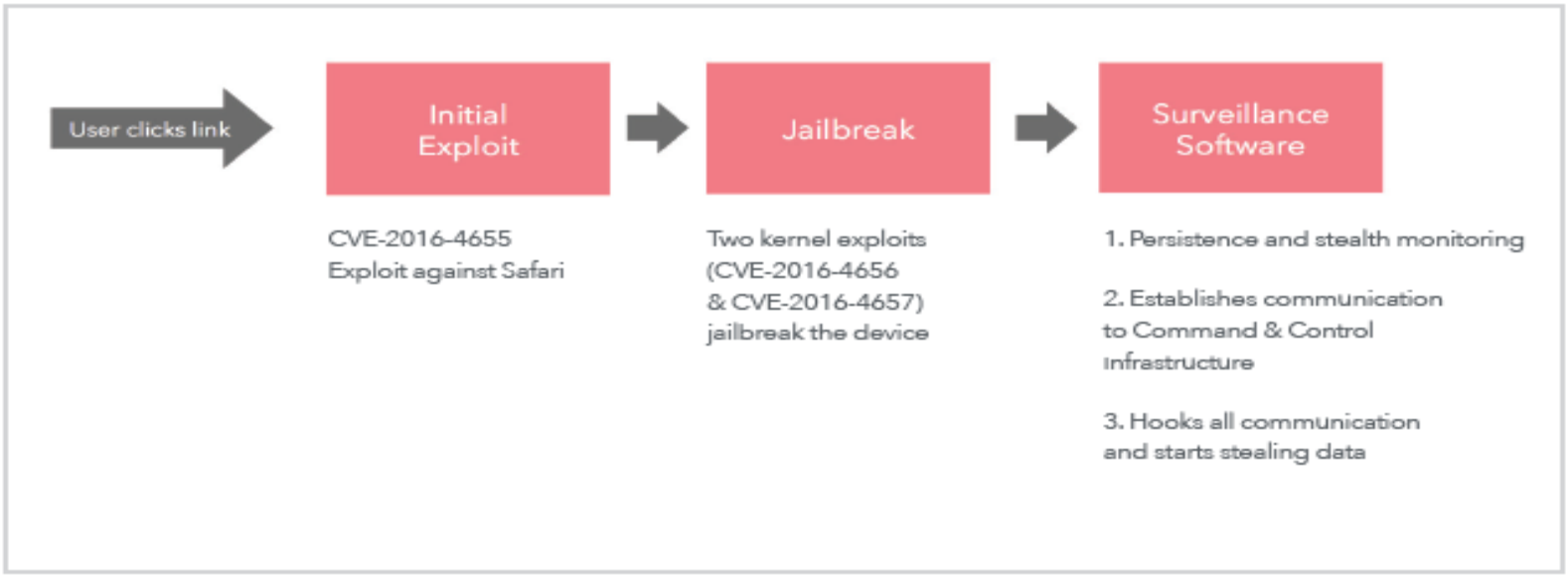
- Grupos más activos en España:



NSO GROUP PEGASUS



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



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

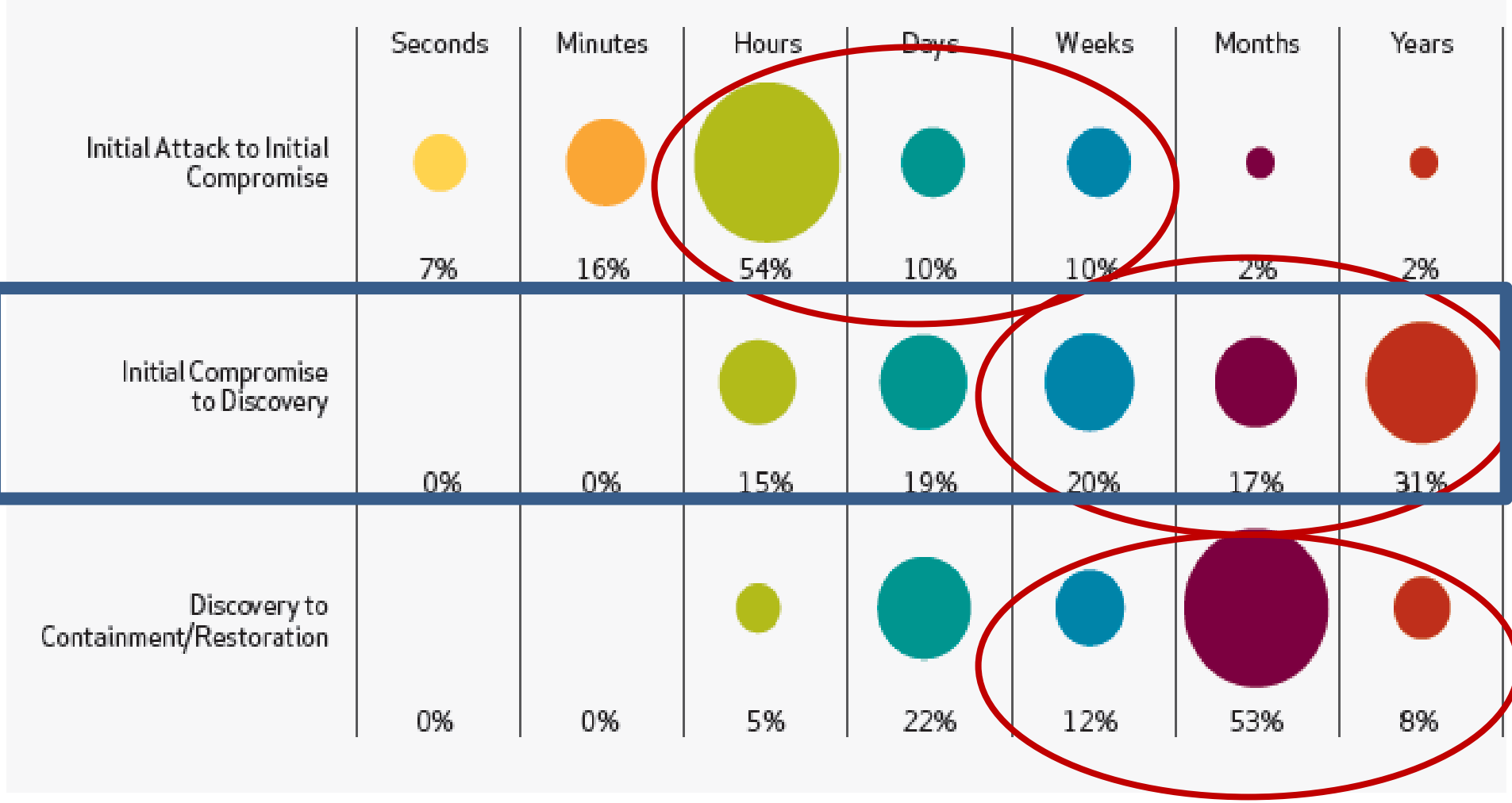
- Privilegios de usuarios
- Autenticación de usuario
- Redes sociales
- Telefonía móvil
- Servicios en nube
- Unidades de memoria

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

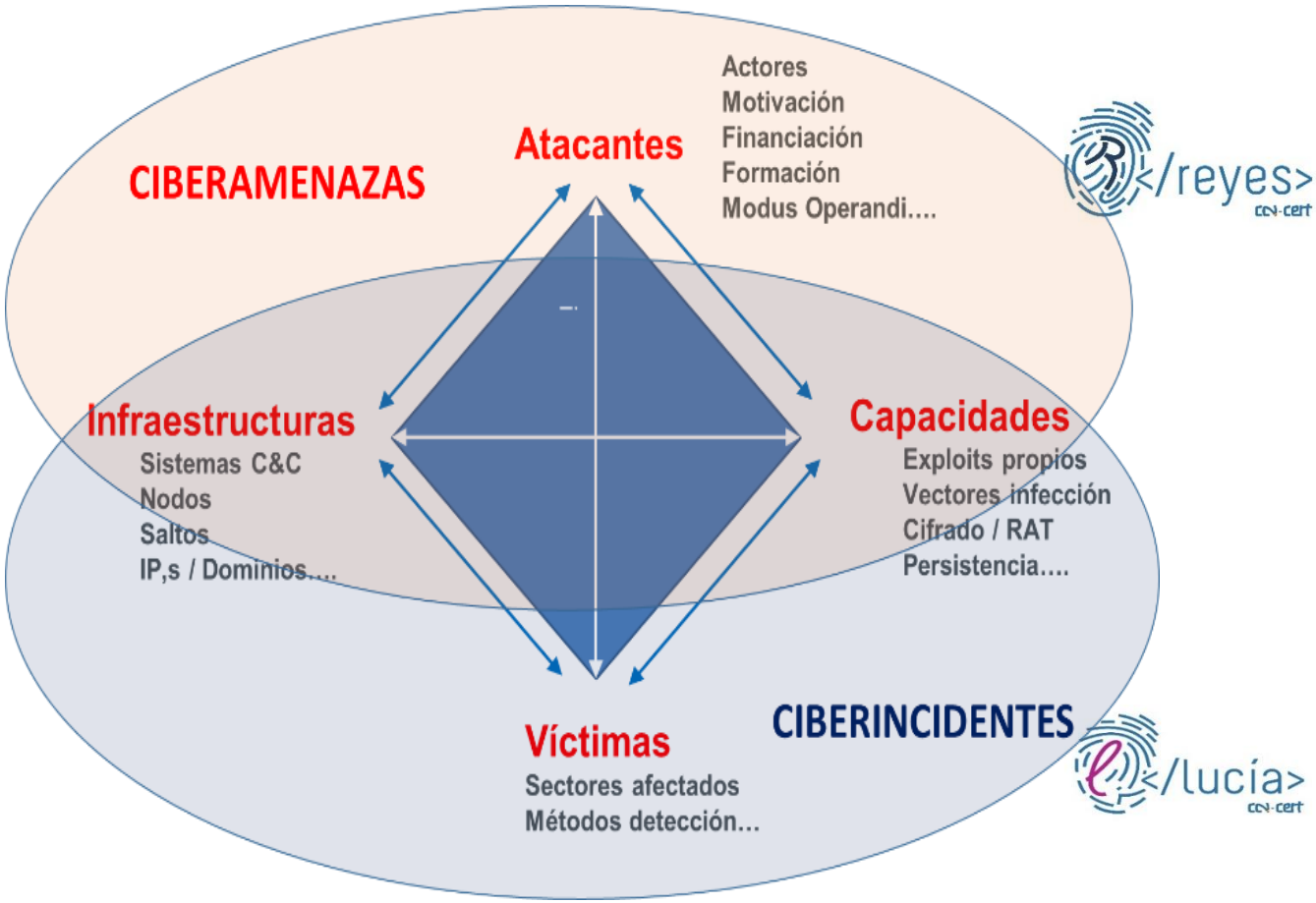


VERIZON rp_data-breach-investigations

DECALOGO

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.**

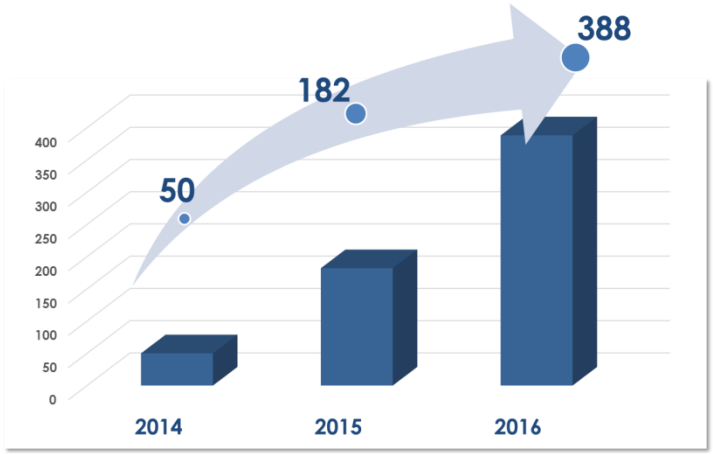
INTERCAMBIO Y CONOCIMIENTO DE LA AMENAZA



UNIVERSIDADES

RESULTADOS GENERALES

RESULTADOS SECTORIALES



Esquema Nacional de Seguridad

ens Esquema Nacional de Seguridad

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**.

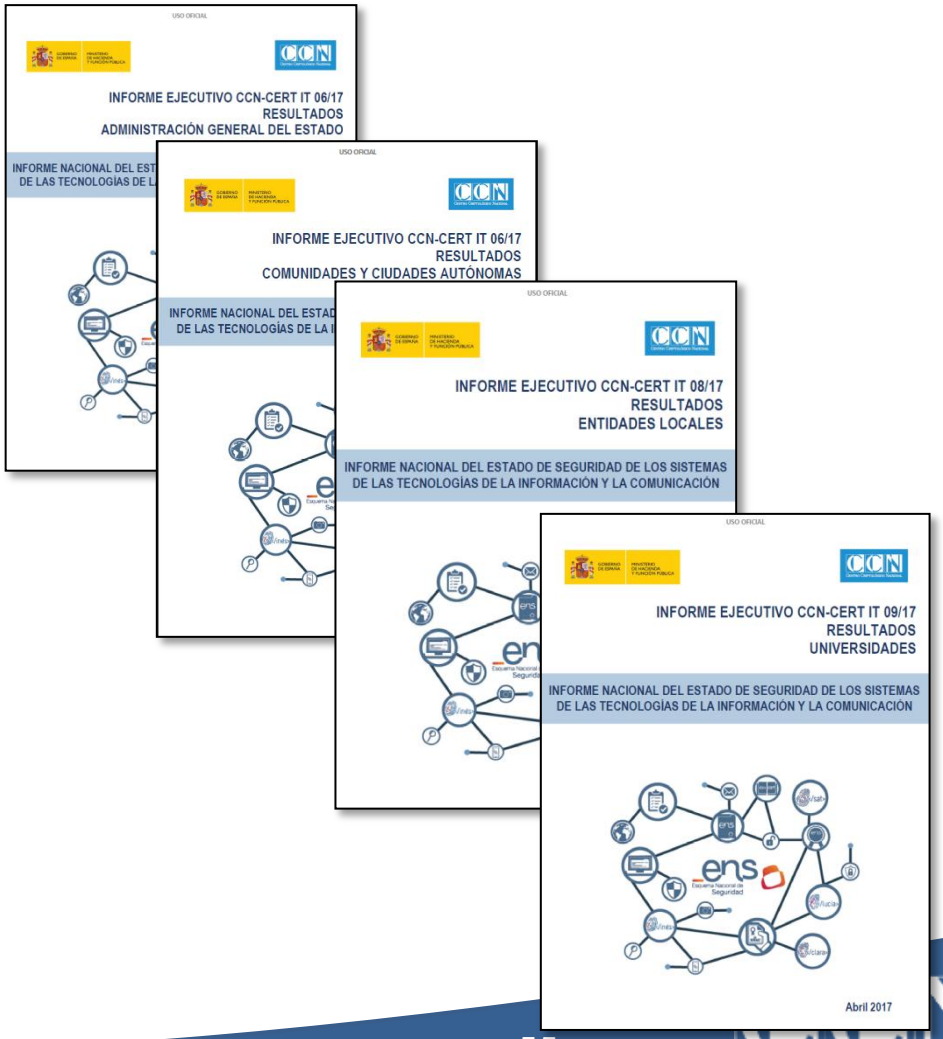
RESULTADOS INES 2016 – RESULTADOS MEDIDAS ANEXO II

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

RESULTADOS INES 2016 – INFORMES

RESULTADOS GENERALES

RESULTADOS SECTORIALES

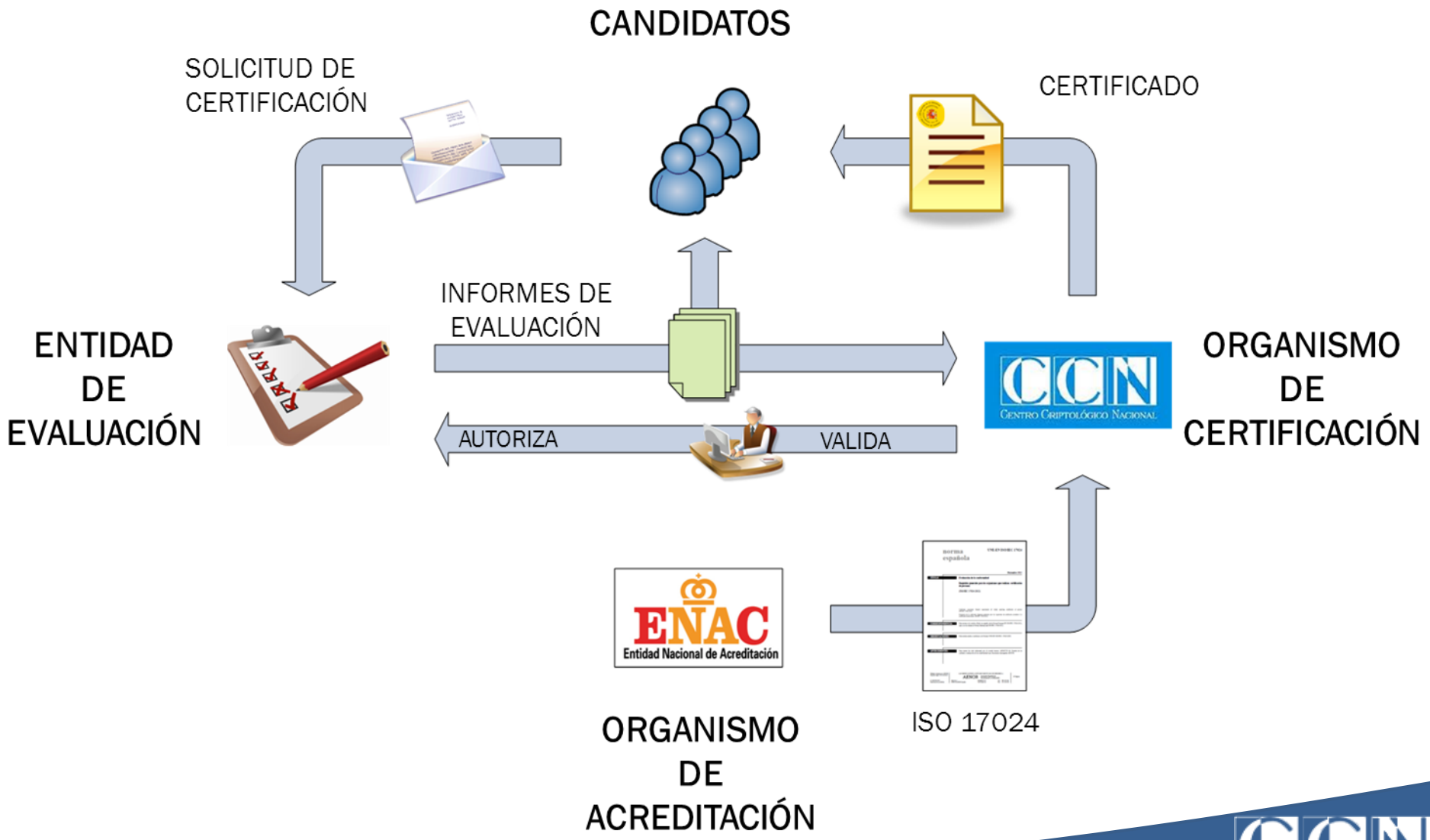


RESULTADOS INES 2016 – CONCLUSIONES

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
  - info@ccn-cert.cni.es
  - **ccn@cni.es**
  - Sat-inet@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

Gracias