XII Jornadas STIC CCN-CERT

Ciberseguridad,

hacia una respuesta y disuasión efectiva

CCN-CERT
centro criptológico nacional

Ciberseguridad: hacia una respuesta y disuasión efectiva

Necesidad de implementar ciberseguridad

ENCS 2013. OBJETIVO GLOBAL: Lograr que España haga un uso seguro de los Sistemas de Información y Telecomunicaciones, fortaleciendo las capacidades de prevención, defensa, detección, y respuesta a los ciberataques.

Prevención

Detección

Respuesta

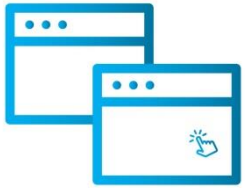
Normativa. LEGISLACIÓN.

Normativa. Guías CCN-STIC e Informes.

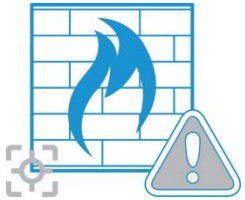
335 Guías CCN-STIC

53 Nuevas / Actualizadas

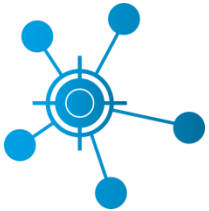
26 Informes de Código Dañino



72 Informes Técnicos



4 Informes de Buenas Prácticas



30 Informes de Amenazas

1.200.000 descargas IA / ID / BP en 2018

CIBER_ SEGURIDAD

Prevención

- Normativa
- Formación
- Auditorías
- Implantación ENS

Detección

Respuesta

335
Guías
CCN-STIC

Guía CCN-STIC 301

Guía CCN-STIC 303

Guía CCN-STIC 819

Guía CCN-STIC 834

ccn-cert centro criptológico nacional

Normativa. Guías CCN-STIC

Descargas:

- Serie 800 …….. 755.000
- Serie 500…….. 230.000
- CCN-STIC 460…. 16.000

Guía CCN-STIC 570

Windows Server 2016

- **Anexo + Script ENS**
- **Anexo + Script Info Clasificada**

Guía CCN-STIC 599

Windows 10

- **Anexo + Script ENS**
- **Anexo + Script Info Clasificada**

Implicar, Concienciar, Demostrar

Prevención

- Normativa
- Formación
- Auditorías
- Implantación ENS

Detección

Respuesta

3.958 (620)
alumnos en 2018

22
cursos presenciales

7
cursos online

</vanesa>

13
cursos a distancia

Novedades:

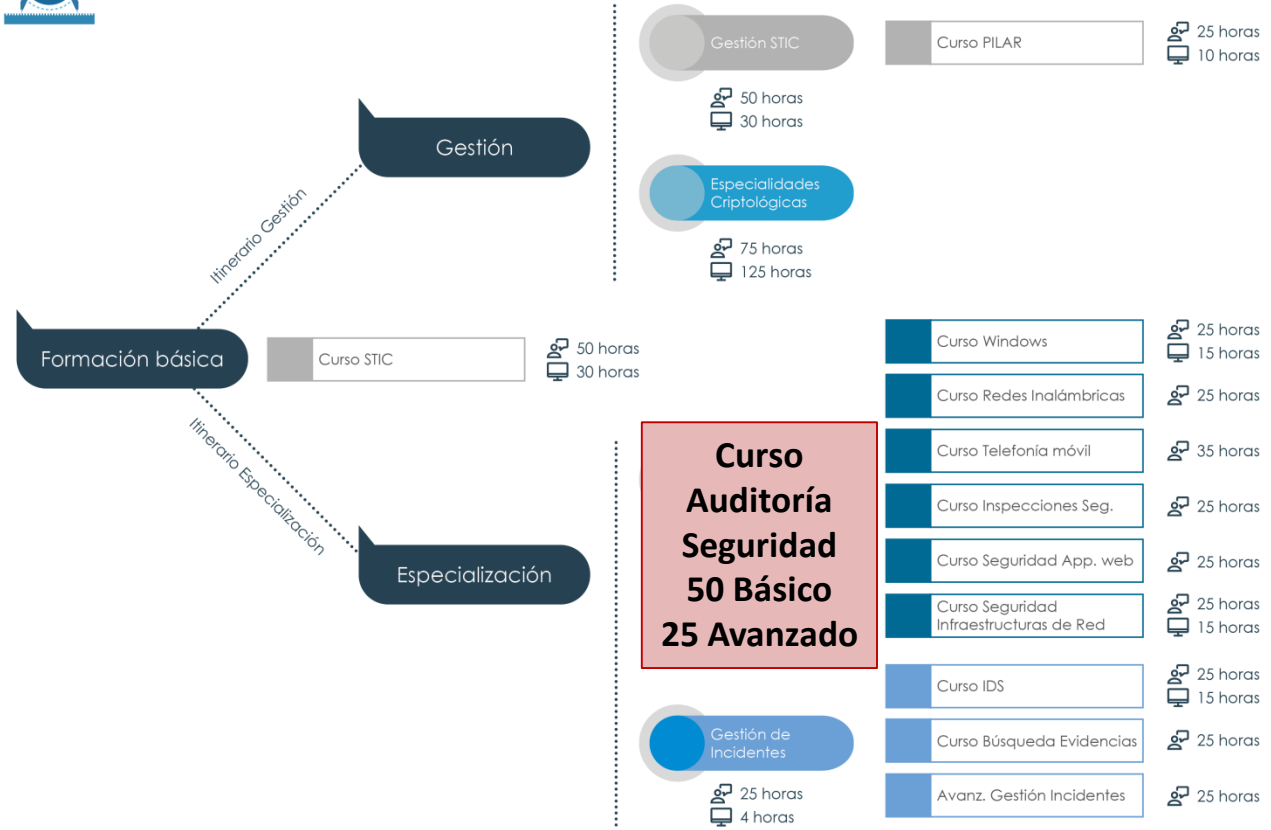
I Curso STIC Seguridad en Infraestructuras de Red

Curso piloto STIC de Auditorías de Seguridad

CCN 2019

Implicar, Concienciar, Demostrar

- Prevención
  - Normativa
  - Formación
  - Auditorías
  - Implantación ENS
- Detección
- Respuesta



Prevención

- Normativa
- Formación
- Auditorías
- Implantación ENS

Detección

Respuesta

ATENEA

Plataforma de desafíos de seguridad

+5.000
usuarios

+70
Retos de seguridad

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

ATENEA ESCUELA

+60
Retos de seguridad

https://atenea.ccn-cert.cni.es/escuela

Marco General de Auditoría

Prevención

- Normativa
- Formación
- Auditorías
- Implantación ENS

Detección

Respuesta

Auditorías de Seguridad

- Determinación del grado de conformidad frente a una política de seguridad establecida
- **Dictamen** final:
  - Favorable ✓
  - Favorable con NO conformidades (Plan de Acciones Correctivas) ✓
  - Desfavorable ✘
- Incluye una o varias **INSPECCIONES DE SEGURIDAD**

Inspecciones de Seguridad

- Verificación de la seguridad implementada
- Toma de evidencias
- **Dictamen** final:

Inspección de cumplimiento ***(NIVEL 1 y 2)***

- *No conformidad mayor*
- *No conformidad menor*
- *Observación*

Inspección técnica ***(NIVEL 3, 4 y 5)***

- *Criticidad Baja*
- *Criticidad Media*
- *Criticidad Alta*
- *Crítica*

	NIVEL 1	NIVEL 2	NIVEL 3*	NIVEL 4	NIVEL 5
ALCANCE	Conocimiento de la gobernanza de la seguridad del Sistema	Mejora en la gestión "global" de la seguridad	Reconocimiento objetivo de que el Sistema opera dentro del marco de seguridad definido	Conocimiento "real y completo" de la criticidad y riesgo del Sistema	Conocimiento "real y estimado" de la criticidad y riesgo del Sistema
ÁMBITO	Elemento (producto, servicio, dispositivo, aplicación,...) y Sistema	Elemento (producto, servicio, dispositivo, aplicación,...) y Sistema	Elemento (producto, servicio, dispositivo, aplicación,...), Sistema e Interconexión	Elemento (producto, servicio, dispositivo, aplicación,...), Sistema e Interconexión	Elemento (producto, servicio, dispositivo, aplicación,...), Sistema e Interconexión
OBJETIVO	Determinar los servicios proporcionados y arquitectura del Sistema	Determinar las propiedades y funciones de seguridad del Sistema	Determinar el nivel de seguridad de un Sistema y su grado de cumplimiento con la política de seguridad. Evaluación de la configuración del	Llegar a conocer la configuración del sistema, la superficie de exposición a vulnerabilidades y las amenazas	Llegar a conocer la superficie de exposición a vulnerabilidades y amenazas existentes

Auditoría ENS / Sist. Clasificados

Prevención

- Normativa
- Formación
- Auditorías
- Implantación ENS

Detección

Respuesta

Certificaciones de conformidad con el ENS

- Impulso notable en el volumen de certificaciones durante 2018.

78 SECTOR PRIVADO

21

AGE: 2

CC.AA: 4

EE.LL: 3

Universidades: 1

Sector Público Institucional: 11

Primer organismo público auditor del ENS: *Viceconsejería de Administración Local y Coordinación Administrativa JCCM*

Castilla-La Mancha

Nueva Guía: CCN-STIC-120

PROCEDIMIENTO DE ACREDITACIÓN DE ENTIDADES AUDITORAS PARA VERIFICAR REQUISITOS STIC EN SISTEMAS DIFUSIÓN LIMITADA

ACREDITACIÓN DE CONFORMIDAD

CCN centro criptológico nacional

Entidad capacitada para la realización de inspecciones STIC de sistemas que manejen información clasificada hasta el grado de DIFUSIÓN LIMITADA.

Certificación de Productos

Prevención

- Normativa
- Formación
- Auditorías
- Implantación ENS

Detección

Respuesta

Catálogo Productos Seguridad TIC (CPSTIC)

Guía CCN-STIC 105

70% Crecimiento de productos

Guía CCN-STIC 140

5 nuevas familias:

- VPN SSL.
- Plataformas de confianza.
- Copias de seguridad.
- **Comunicaciones móviles (2).**

Guía CCN-STIC 106

Inclusión de productos ENS MEDIO y BASICO bajo certificación **LINCE**

CPSTIC - Líneas futuras

Inclusión de servicios en la nube

ENS Cualificado

Nuevas familias de productos:

- VDI.
- Soluciones de hiper-convergencia.
- Gestión de vulnerabilidades.
- …

Intensificación en movilidad

Actualmente trabajando en la inclusión de **4** dispositivos

Certificación de Productos

Prevención

- Normativa
- Formación
- Auditorías
- Implantación ENS

Detección

Respuesta

Nuevas metodologías evaluación seguridad

- **Certificación Nacional Esencial de Seguridad (Metodología LINCE)**
  - LINCE esta basado en los principios de Common Criteria
  - Foco en el análisis de vulnerabilidades y tests de penetración
- **To learn more … → Presentación en la Sala 19**

Incremento capacidad evaluación seguridad

Despliegue de pilotos soluciones auditoría

Prevención

- Normativa
- Formación
- Auditorías
- Implantación ENS

Detección

Respuesta

pilar

- v7.2 Perfil RGPD
- Ejemplos EELL

rocio

- Tecnología FORTINET
- 2019 Allied Telesys y Aruba
- 58% Usuarios

clara

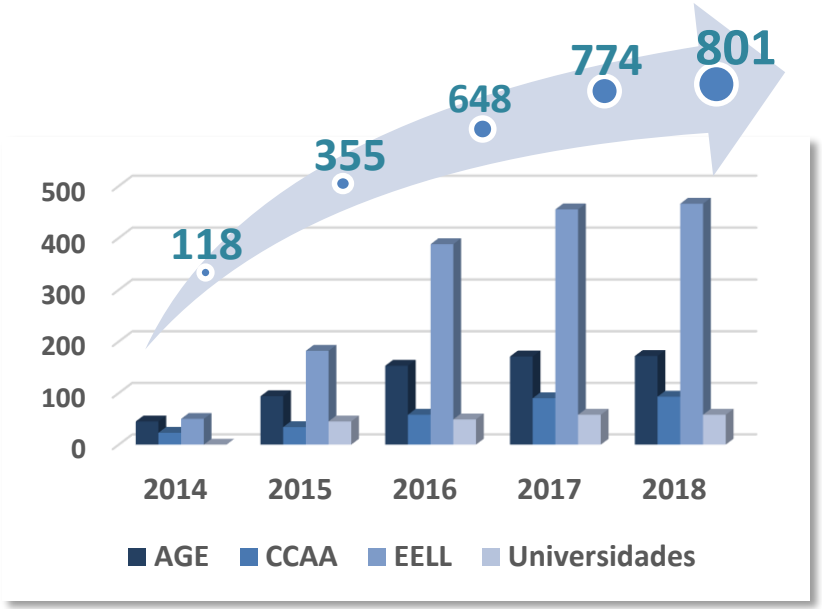
- V2.0 Gestión centralizada
- Integración ANA

ana

automatización y normalización de auditorías

- Elecciones Colombia
- Integración CVSS

Implantación ENS



Fichas registradas a 7 de diciembre de 2018

Campaña 2017

Número de sistemas: **19.135**

Número de usuarios: **4.261.078**

Indicador Global de Madurez (IM): **52%**

Indicador Global de Cumplimiento (IC): **64%**

7 Informes agregados:

- ✓ AA.PP
- ✓ AGE
- ✓ CC.AA.
- ✓ EE.LL.
- ✓ Universidades
- ✓ Autoridades Portuarias
- ✓ Confederaciones Hidrográficas

</inés> cc-cert 2.0

Prevención

- Normativa
- Formación
- Auditorías
- Implantación ENS

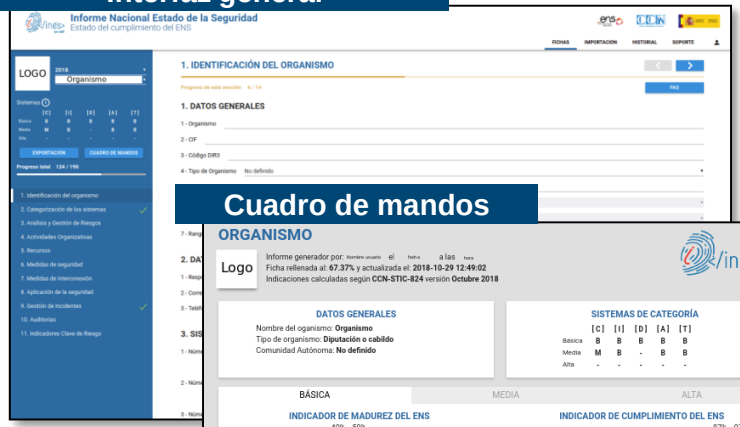
Detección

Respuesta

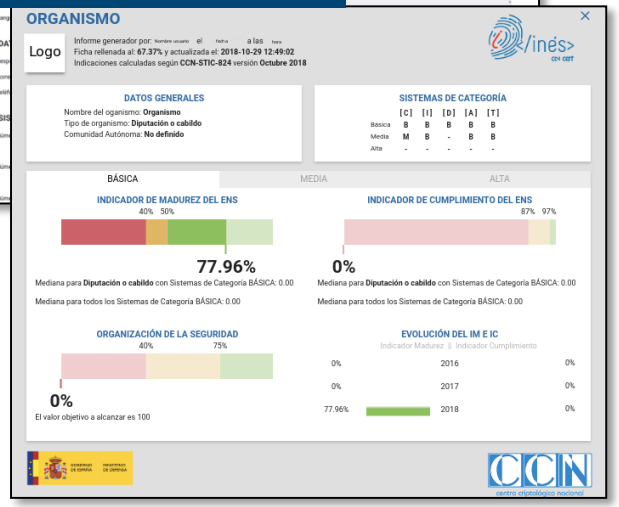
Nueva Plataforma **INES 2.0**

- Mejora en la interfaz de usuario.
- Mensajería interna de soporte.
- Carga individual de información por categoría de sistema.
- Existencia de usuarios supervisores
- Generación automática de información agregada.
- FAQ mejorada
- Solicitud de nueva información

Interfaz general



Cuadro de mandos



Implantación ENS. Certificación.

Prevención

- Normativa
- Formación
- Auditorías
- Implantación ENS

Detección

Respuesta

ENS: referencia a utilizar en la implementación de medidas de seguridad

ens Consejo de Certificación del Esquema Nacional de Seguridad + incrementales =

Filosofía: **una sola auditoría** para validar los requisitos del **ENS más aquellos determinados por los incrementales** que se indiquen, de tal manera, que aunque acudan expertos en diferentes esquemas al final se pueden **conceder diversas certificaciones**.

Posibilidad de **constituir órganos auditores en CCAA**

Cursos para 2019

Castilla-La Mancha

SECRETARÍA DE ESTADO DE PRESUPUESTOS Y GASTOS
IGAE
INTERVENCIÓN GENERAL DE LA ADMINISTRACIÓN DEL ESTADO

JUNTA DE ANDALUCIA

Sistemas de Alerta Temprana

Prevención

Detección

- SAT
- Análisis
- Carmen

Respuesta

</sat-inet>

192
organismos y empresas adscritos

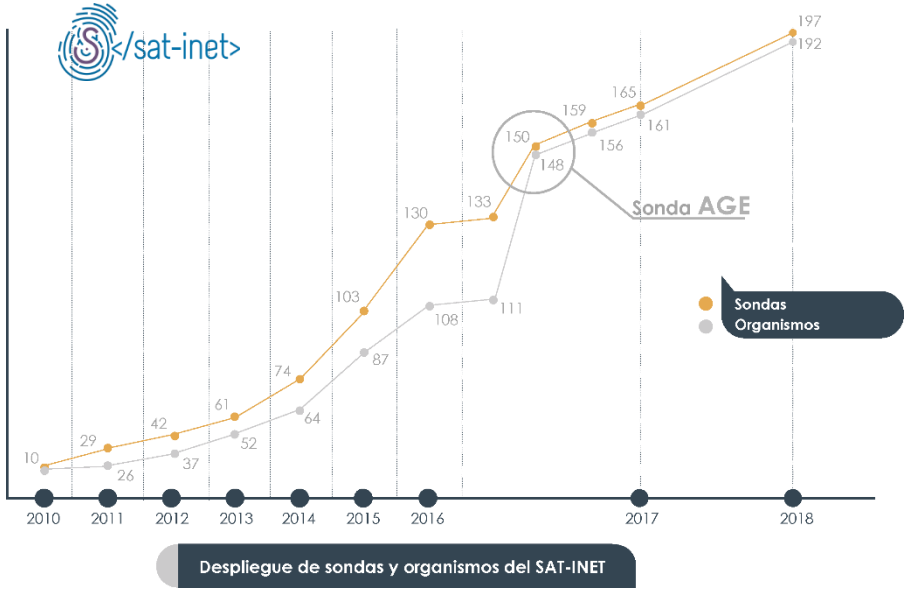
31
nuevos organismos adscritos en 2018

</sat-sara>

50
Áreas de conexión

</sat-ics>

8
entidades



Despliegue de sondas y organismos del SAT-INET

Herramientas de análisis

Prevención

Detección

- SAT
- Análisis
- Carmen

Respuesta

</marta> ccn-cert

</maría> ccn-cert

Total de binarios subidos

Total de análisis realizados

Total de usuarios

Total de análisis

Total de análisis positivos

Total de análisis negativos

Mejor ratio de detección

Peor ratio de detección

Prevención

Detección

- SAT
- Análisis
- Carmen

Respuesta

carmen Ciberinteligencia Avanzada

Detección de compromisos por APT

54

Implantaciones operativas en todo el mundo

28

Implantaciones en organismos y empresas

16

Integraciones con CARMEN Central

Integración con

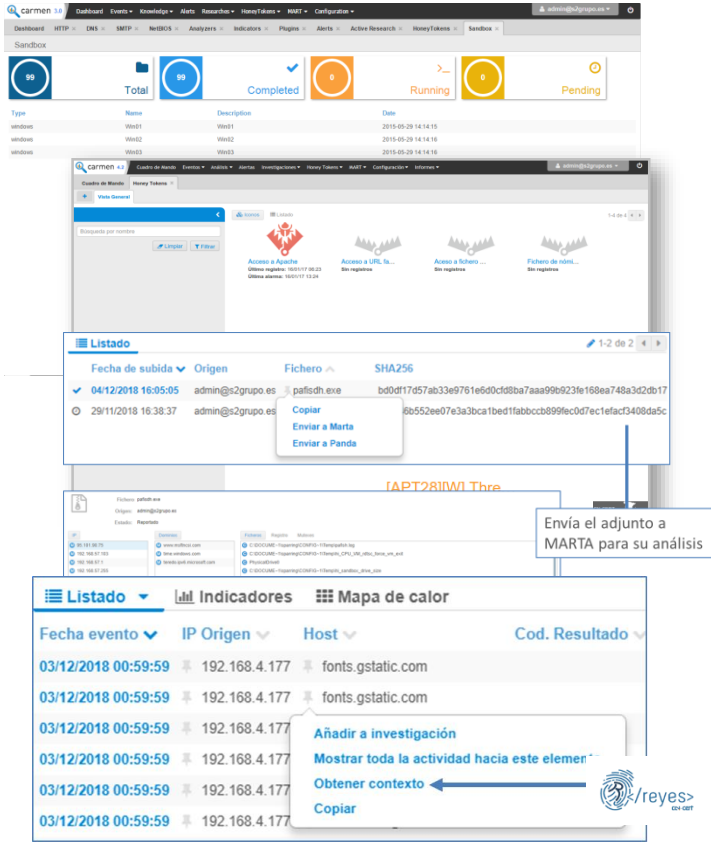
reyes · marta · panda · claudia

Cabeceras completas

HTTP

Subida de ficheros

PCAP



CIBER_ SEGURIDAD

Centro de Operaciones de Seguridad SGNTJ

ccn-cert centro criptológico nacional

SOC AGE

Prevención

Detección

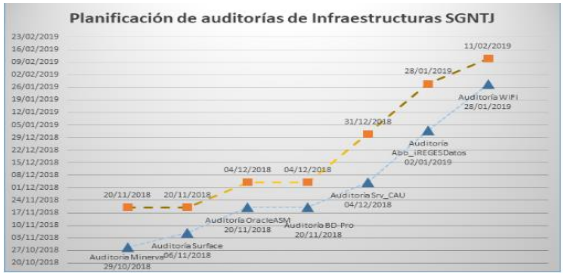
Respuesta

- SOC
- Evaluación continua
- Intercambio
  - REYES 3.0
  - LUCÍA
  - CSIRT.ES

- **Ser certificables en ENS**
  - Tener análisis de riesgos
  - Normativa común para justicia
- **Conocer exposición y salud SGNTJ**
  - Exposición de cara al exterior
  - Salud de los servicios internos y externos
  - Grado de seguridad de las aplicaciones existente y nuevas
- **Detección y respuesta a incidentes**

27

Analistas / operadores

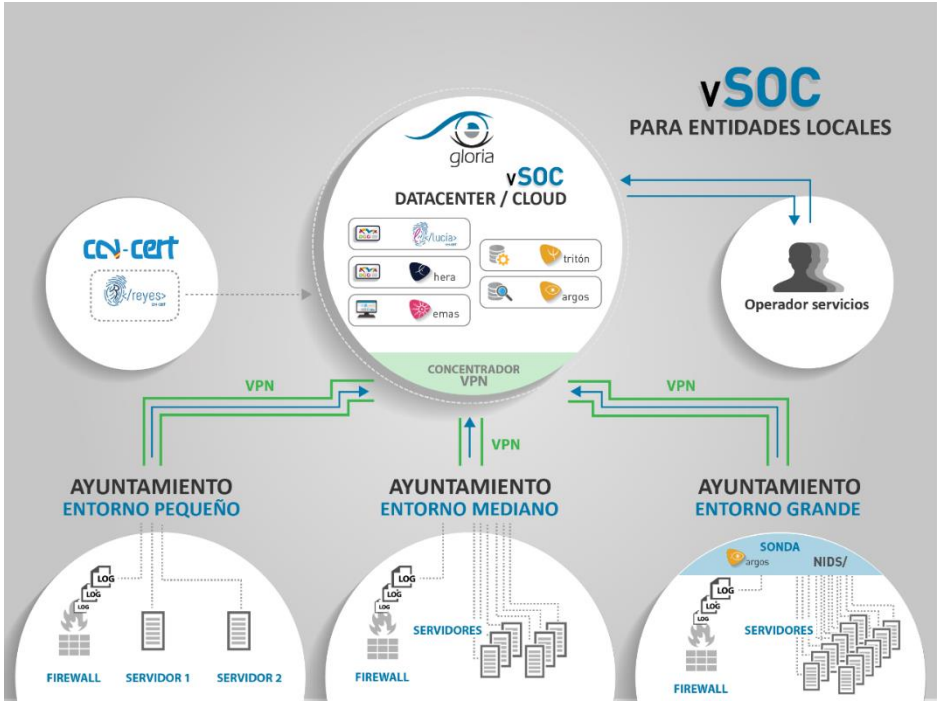


Prevención

Detección

Respuesta

- SOC
- Evaluación continua
- Intercambio
  - REYES 3.0
  - LUCÍA
  - CSIRT.ES



SOC,s VIRTUALES

3 + 3

Diputaciones / CCAA

vSOC para entidades locales está diseñado para ayudar a los ayuntamientos en el **cumplimiento del ENS. Proporcionando servicios:**

- **Vigilancia de la seguridad**
- **Gestión de Incidentes**
- **ANA (Auditoría continua)**
- **PILAR (Análisis Riesgos en Nube)**

Piloto a implantar:

- **Diputación de Zaragoza**
- **Diputación de Valencia**
- **Diputación de León**
- Región de Murcia
- Cabildo Insular Tenerife
- Diputación de Burgos

CIBER_ SEGURIDAD

@</ana> automatización y normalización de auditorías

ccn-cert centro criptológico nacional

Evaluación continua.

Capacidad de gestionar la seguridad priorizando los recursos disponibles, ayuda a reducir la superficie de exposición frente a posibles amenazas.

- Prevención
- Detección
- Respuesta
  - SOC
  - Evaluación continua
  - Intercambio
    - REYES 3.0
    - LUCÍA
    - CSIRT.ES

Gestión de seguridad

Intercambio. Reyes 3.0.

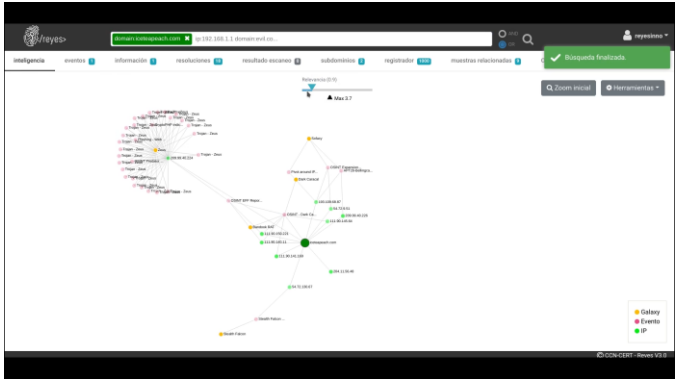
Prevención

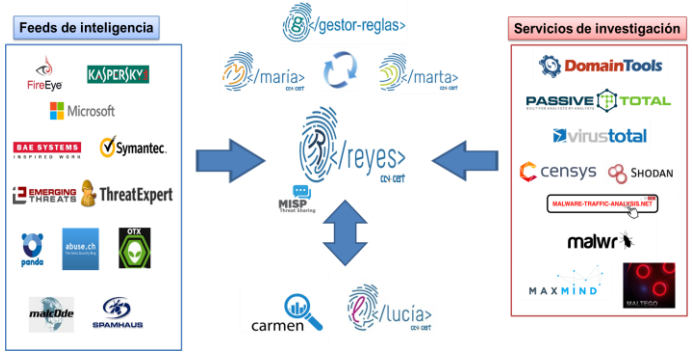
Detección

Respuesta

- SOC
- Evaluación continua
- Intercambio
  - REYES 3.0
  - LUCÍA
  - CSIRT.ES

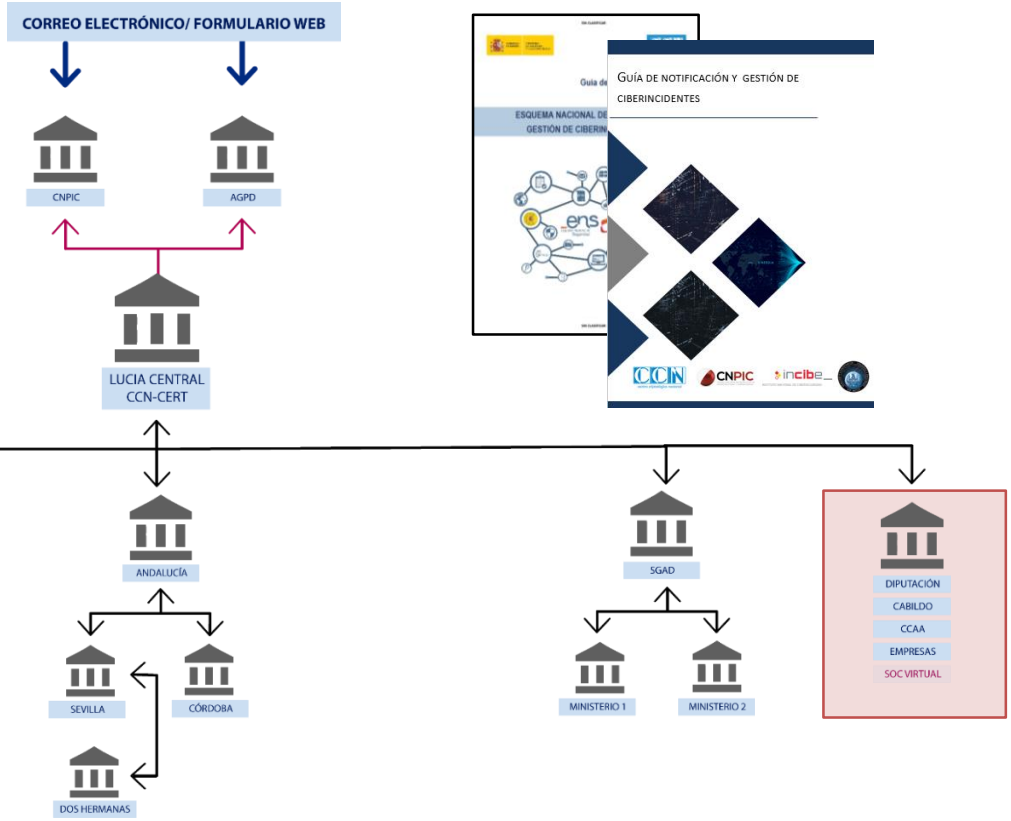
- Nueva interfaz
- Nuevo motor de inteligencia
- Nuevas fuentes de información
- Mapa de calor resoluciones DNS y avistamientos en VirusTotal
- Histórico de WhoIS
- Análisis de registradores de dominios
- Análisis en OSINT





Intercambio. Lucía.

- Prevención
- Detección
- Respuesta
  - SOC
  - Evaluación continua
  - Intercambio
    - REYES 3.0
    - LUCÍA
    - CSIRT.ES



CIBER_ SEGURIDAD

CSIRT.es

CCN-CERT centro criptológico nacional

Prevención

Detección

Respuesta

- SOC
- Evaluación continua
- Intercambio
  - REYES 3.0
  - LUCÍA
  - CSIRT.ES

Equipos de Seguridad y Gestión de Incidentes españoles

Objetivo: optimizar la cooperación entre los CSIRT de ámbito nacional para actuar frente a problemas de seguridad informática.

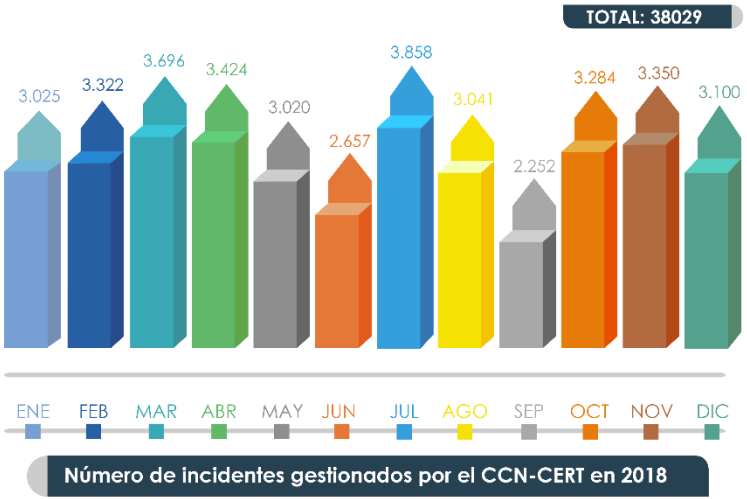
Compartir, Cooperar, Divulgar

Intercambio

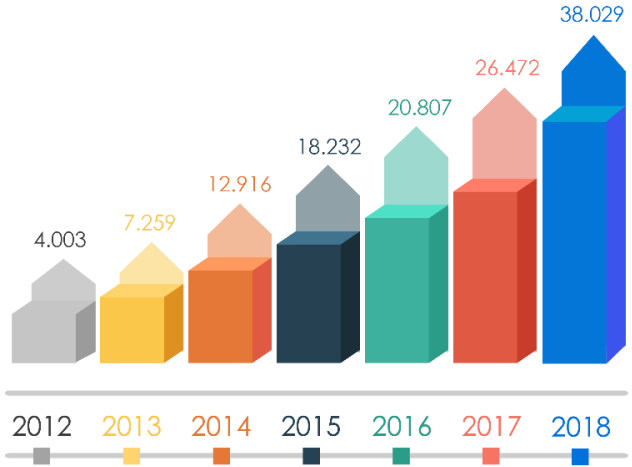
Coordinación

Ciberseguridad: hacia una respuesta y disuasión efectiva

A finales de 2018 se habrán resuelto más de **38.000 incidentes**



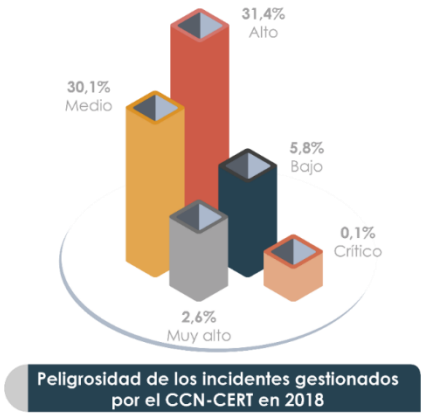
Número de incidentes gestionados por el CCN-CERT en 2018



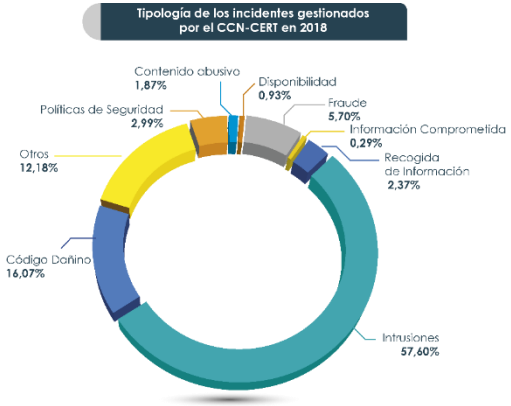
Total de incidentes gestionados por año

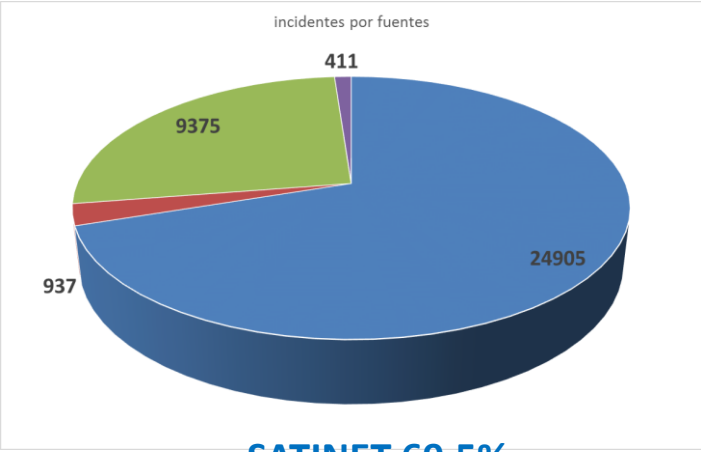
Ciberseguridad: hacia una respuesta y disuasión efectiva

El **2,7%** tiene una peligrosidad "**Muy Alta**" o "**Crítica**" (2,8 incidentes al día)



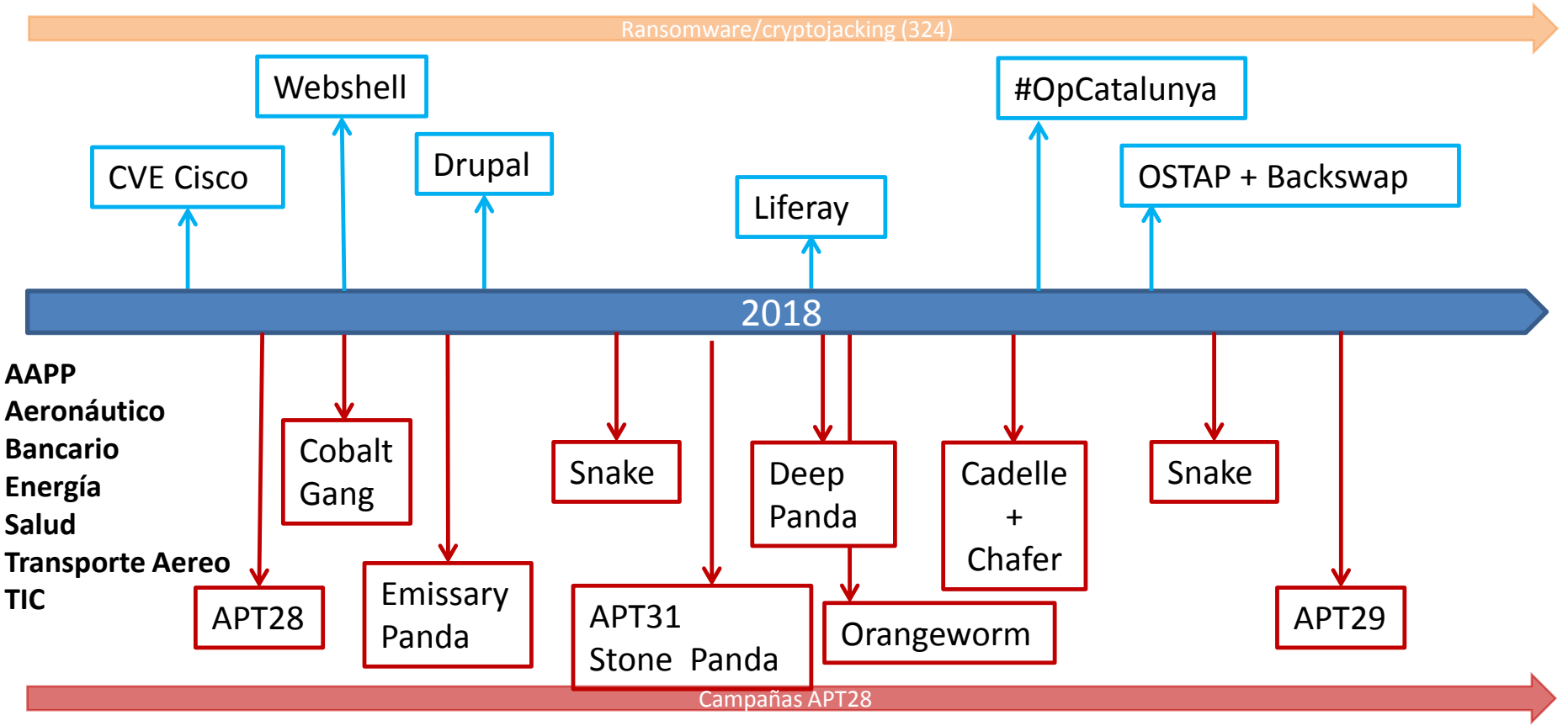
Peligrosidad de los incidentes gestionados por el CCN-CERT en 2018





SATINET 69.5%
LUCIA 27%
SATSARA 2.5%
CCN-CERT 1%

Ciberincidentes destacados en 2018

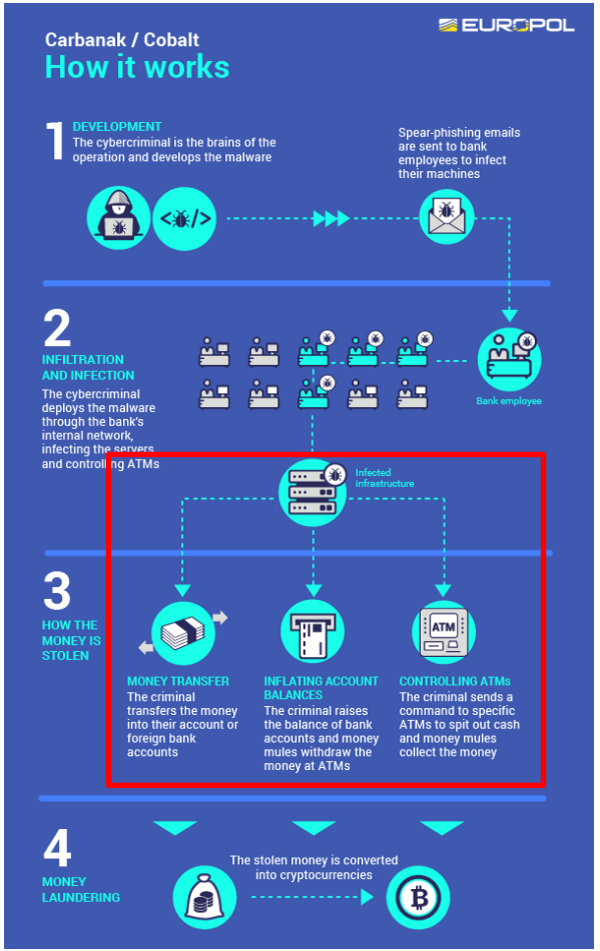


Actor: Cobalt Gang

- Grupo presentado en las VIII Jornadas por Kaspersky.
- Ataque estilo APT que busca el robo económico (1000M€ desde 2014)

Sector Bancario – marzo 2018

- Avisos de empresa de seguridad y CERT extranjero
- Actuación del CCN-CERT momentos previos al *cash-out*
- Vector de infección: *spear-phishing* con CVE no parcheados
- Progreso muy rápido dentro de la red (2 semanas)
- Uso de Powershell y *Cobalt Strike Beacon* – no *malware* propio



Actor: Emissary Panda

Sector Aeroespacial – abril 2018

- Intrusión antigua (>2 años).
  - Más de 200GB de información robados en los 3 primeros meses
- Vector de infección: servidor web abandonado, sin parchear, "en DMZ".
- Ataque "***malware-less***"
  - Acceso mediante *webshells* (China Chopper)
  - Robo de información vía peticiones HTTP

Actor: APT29

Sector Gobierno – noviembre 2018

- Campaña global (~3000 destinatarios)
- Uso de una funcionalidad del SO para la instalación del código dañino.
- *Cobalt Strike Beacon*, no malware propio.

OBJETIVOS 2019

- **Implantación del ENS Sector Público. Necesidad de certificación.**
  - Se establecerán de forma clara la necesidades adicionales para INF. CRITICAS, PROTECCIÓN DE DATOS, DIRECTIVA NIS …..
- **REFORZAR LA CAPACIDAD DE VIGILANCIA** Y **RESPUESTA …** Aumentar la disuasión… Impulso al despliegue de SOC,s VIRTUALES
- **Formación.** Integración formación presencial y a distancia. Definir el perfil de seguridad en los puestos de trabajo de las AAPP.
- **CSIRT.es**. Impulso de la **comunidad de CERT,s / ciberinteligencia** (generar confianza mutua para fortalecer el intercambio).
- **Mejorar el intercambio**
  - Patrones de detección en cualquier formato (Listas negras, IOC, reglas Yara, Reglas SIGMA etc.)
  - REYES 3.0 / LUCIA .
  - Experiencias CCN / Apoyo resolución incidentes

AUDITORÍA	DETECCIÓN	ANÁLISIS	INTERCAMBIO	FORMACIÓN
/inés	/sat-inet	/gloria	/lucía	/vanesa
/pilar	/sat-sara	/maría	/loreto	ATENEA
/clara	/sat-ics	/marta		
/rocio	carmen		/reyes	
/claudia				
/ana				

SOC AGE
SOC SGNTJ