CCN
CENTRO CRIPTOLÓGICO NACIONAL

CCN-CERT
centro criptológico nacional

DIPUTACIÓN DE BURGOS

LA SEGURIDAD DE LA INFORMACIÓN EN TU AYUNTAMIENTO

SIN CLASIFICAR

CCN-CERT
centro criptológico nacional

CCN
Centro Criptológico Nacional

CCN-CERT
"Servicios y herramientas para garantizar la seguridad de la información de los ayuntamientos"

SIN CLASIFICAR

ÍNDICE

- 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, en respuesta a la evolución del entorno regulatorio, las tecnologías de la información y experiencia de implantación.

Establece al CCN-CERT como CERT Gubernamental/Nacional competente

HISTORIA

- 2006 Constitución en el seno del CCN
- 2007 Reconocimiento internacional
- 2008 Sistema Alerta Temprana SAT SARA
- 2009 EGC (CERT Gubernamentales Europeos)
- 2010 ENS y SAT Internet
- 2011 Acuerdos con CCAA
- 2012 CARMEN
- 2013 Relación con empresas
- 2014 LUCÍA e INES
- 2015 Ampliación SAT Internet EELL
- 2016 REYES, MARTA y ROCIO

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 a las **Administraciones Públicas** y a las **empresas estratégicas**, y afrontar de forma activa las nuevas ciberamenazas.

COMUNIDAD

Responsabilidad en ciberataques sobre **sistemas clasificados** y sobre **sistemas de la Administración** y de empresas pertenecientes a **sectores** designados como **estratégicos.**

SERVICIOS DE INFORMACIÓN

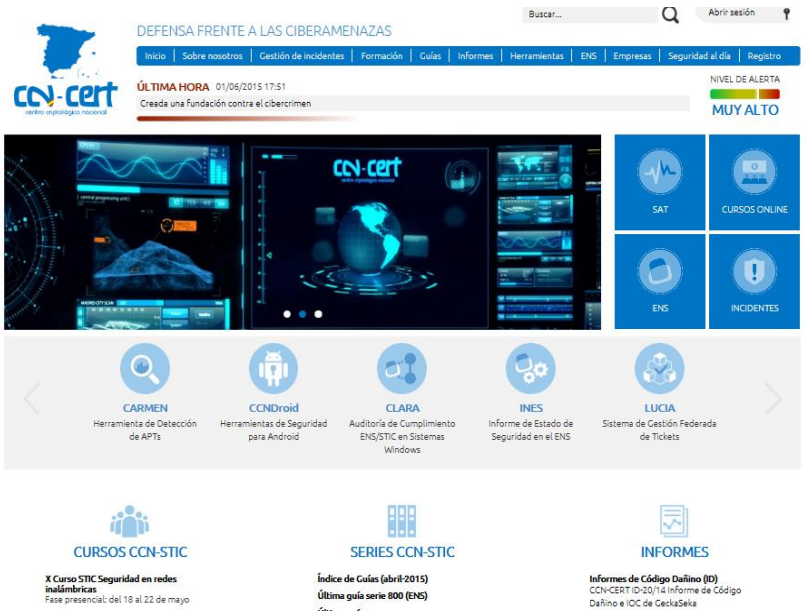
PORTAL CCN-CERT

Formación

Vulnerabilidades y Amenazas

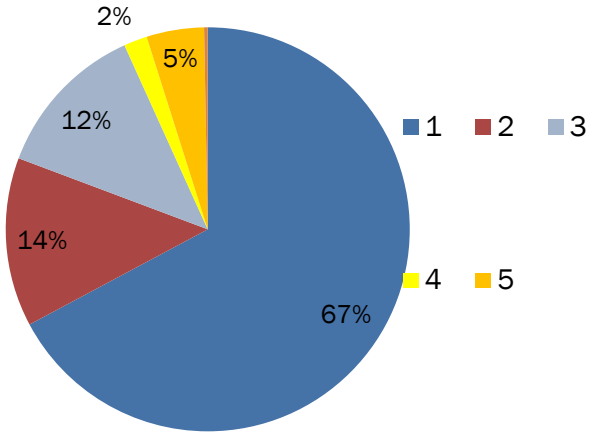
Guías CCN-STIC

Herramienta PILAR



Usuarios Portal CCN-CERT (a septiembre 2016)

Usuarios registrados por origen

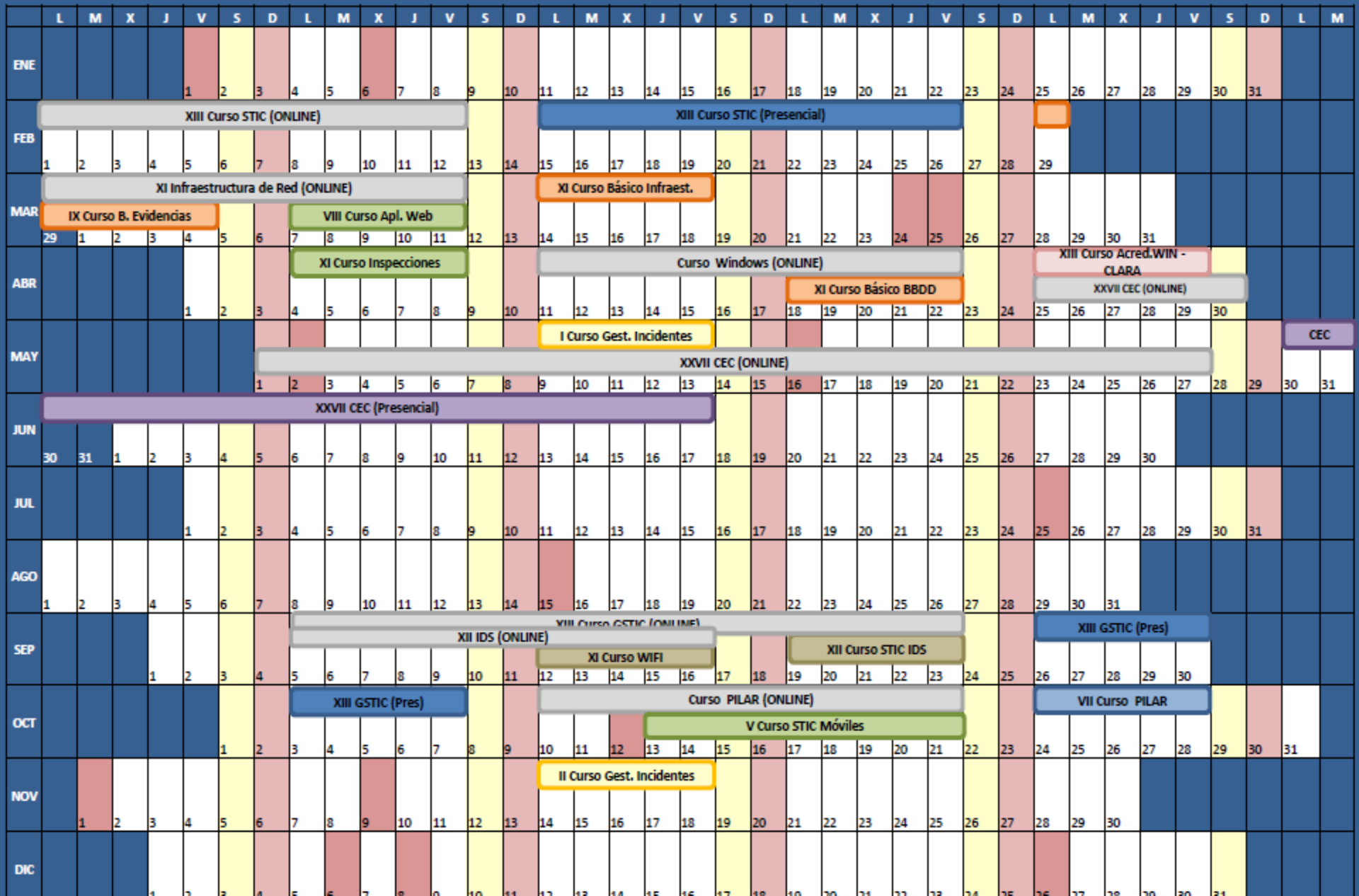


6810 (sep. 16)

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

Centro Criptológico Nacional 2016

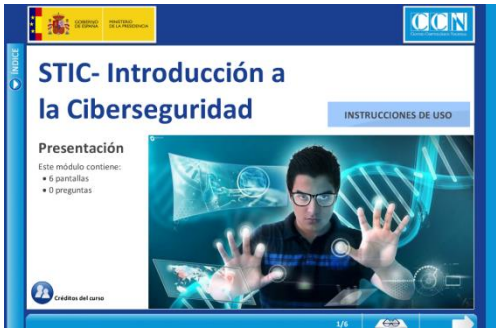


Cursos on-line de Seguridad de la Información

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 Common Criteria

10-15 horas

7. Curso cortafuegos
8. Curso Infraestructura de red
9. Curso IDS.
10. Curso INES



	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**	**-**

Vulnerabilidades. Precios

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

Producto	Rango de precios
Adode Reader	3.800 – 23.000€
Mac OS X	15.300 – 38.300 €
Android	23.000 – 46.000 €
Plug-ins Java para navegador	30.600 – 76.700 €
Plug-ins Flash para navegador	30.600 – 76.700 €
Microsoft Word	38.300 – 76.700 €
Windows	46.000 – 92.000 €
Firefox	46.000 – 122.600 €
Safari	46.000 – 225.000 €
Chrome	61.300 – 153.000 €
Internet Explorer	61.300 – 153.000 €
iOS	76.700 – 191.600 €

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

INFORMES DESTACADOS 2016

2016.10.05

Informes de Amenazas (IA) (22)
Informes de Código Dañino (ID) (25)
Informes Técnicos (IT) (52)
Buenas Prácticas (BP) (1)

262 guías 351 documentos

04.10.2016

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 (40)

CCN-STIC 900: Informes Técnicos

15 nuevas guías
8 actualizadas

453 B Seguridad en Android (Abril 2015)

HERRAMIENTAS

DETECCIÓN

carmen

ANÁLISIS

</marta>
CCN-CERT

</maría>
CCN-CERT

AUDITORÍA

</pilar>
CCN-CERT

</clara>
CCN-CERT

</inés>
CCN-CERT

ROCÍO

INTERCAMBIO

</lucía>
CCN-CERT

</reyes>
CCN-CERT

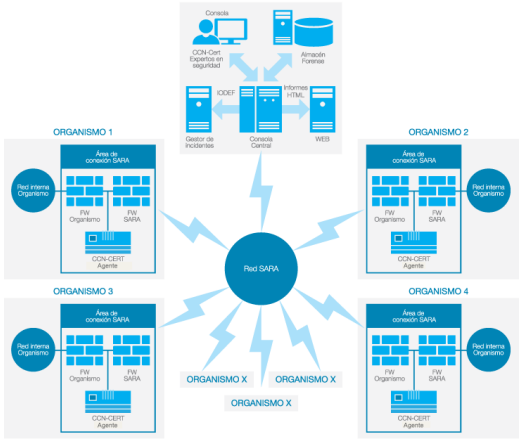
GESTOR DE REGLAS

SONDA AGE

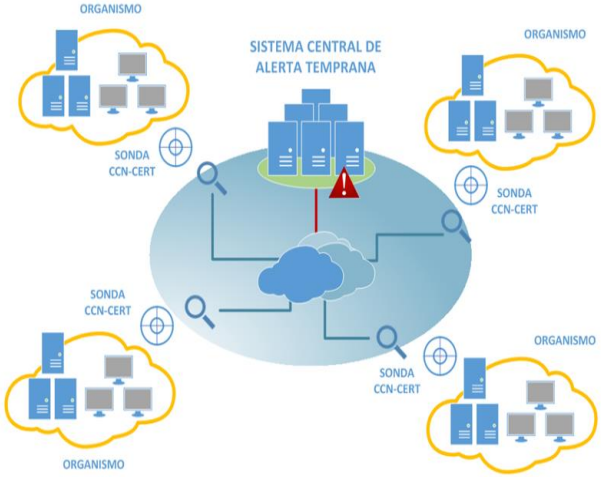
Sistemas de Alerta temprana

Sistemas de Alerta Temprana (SAT) (sep.16)

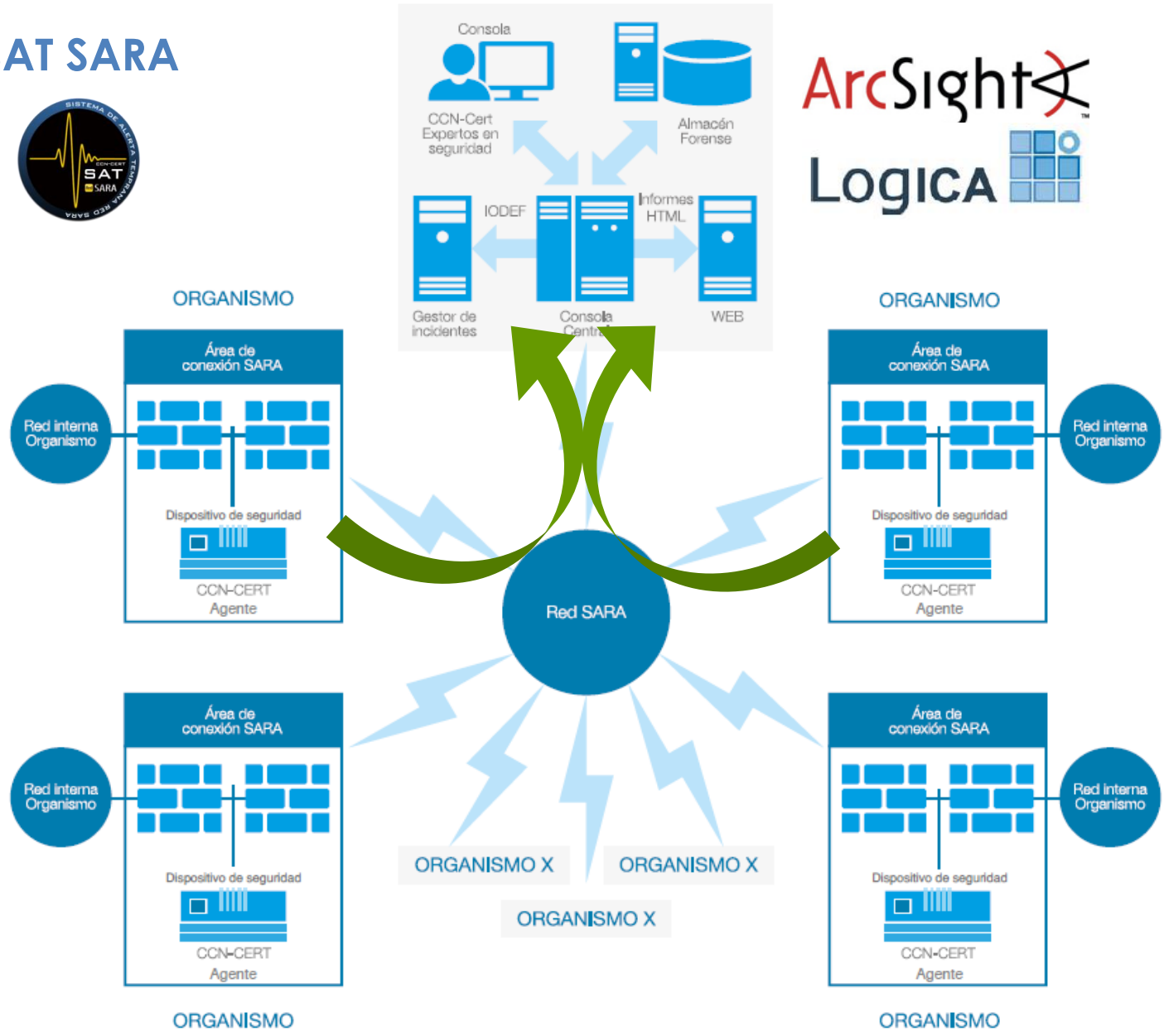
- **RED SARA [SAT- SARA]**
  - Servicio para la Intranet Administrativa
  - Coordinado con MINHAP-SEAP
  - **50/54 Áreas de Conexión**



- **SALIDAS DE INTERNET [SAT INET]**
  - Servicio por suscripción
  - Basado en despliegue de sondas.
  - **101 Organismos / 121 sondas**
  - Últimas incorporaciones: **Museo Reina Sofia, Confederación Hidrográfica Júcar, Región Murcia …**

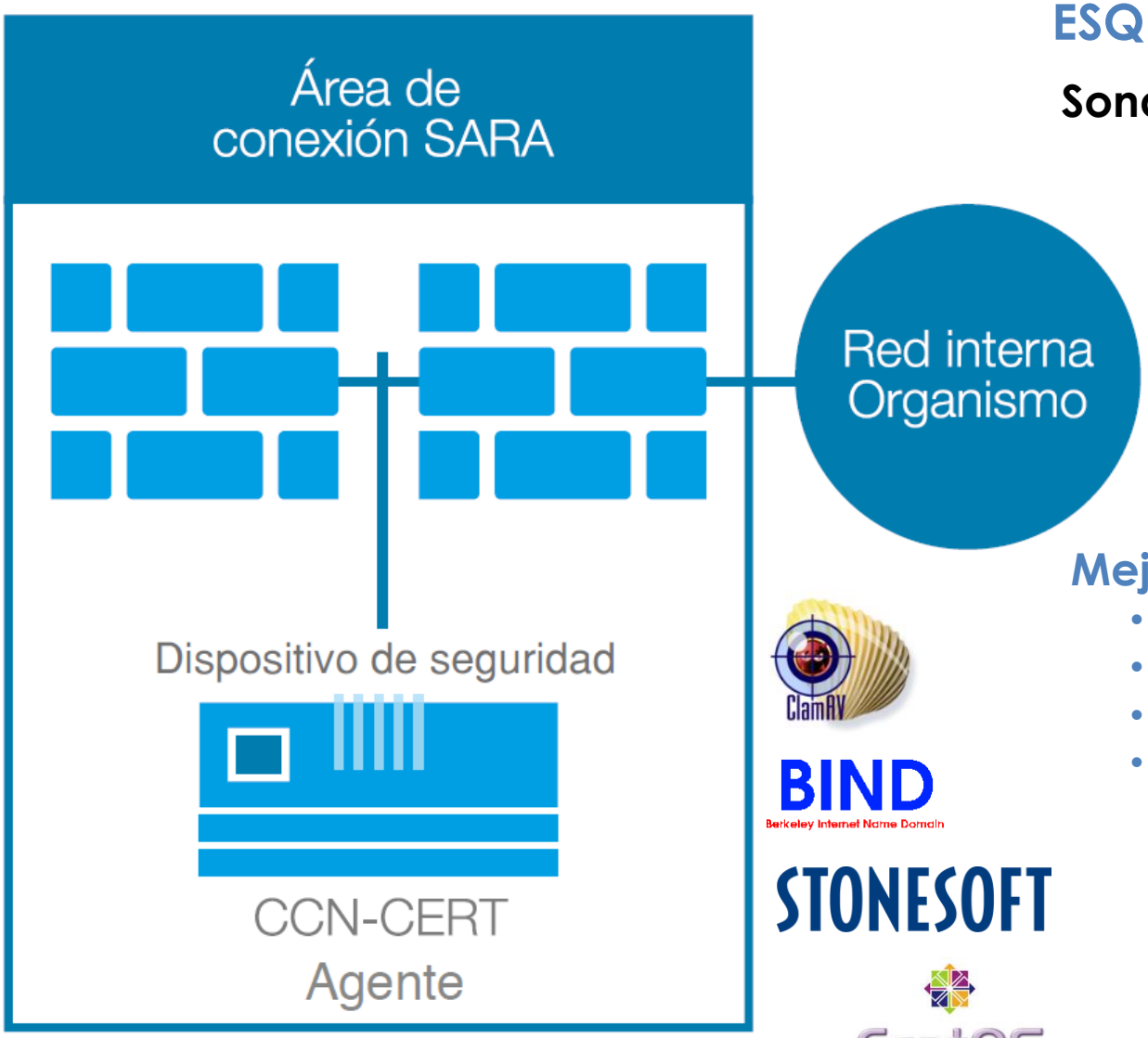


SAT SARA


Consola
CCN-Cert
Expertos en
seguridad
Almacén
Forense
IODEF
Informes
HTML
Gestor de
incidentes
Consola
Central
WEB
ArcSight
Logica
ORGANISMO
Área de
conexión SARA
Red interna
Organismo
Dispositivo de seguridad
CCN-CERT
Agente
Red SARA
ORGANISMO X
ORGANISMO X
ORGANISMO X
ORGANISMO

ESQUEMA ÁREA CONEXIÓN

Sondas desplegadas: **50/ 54**

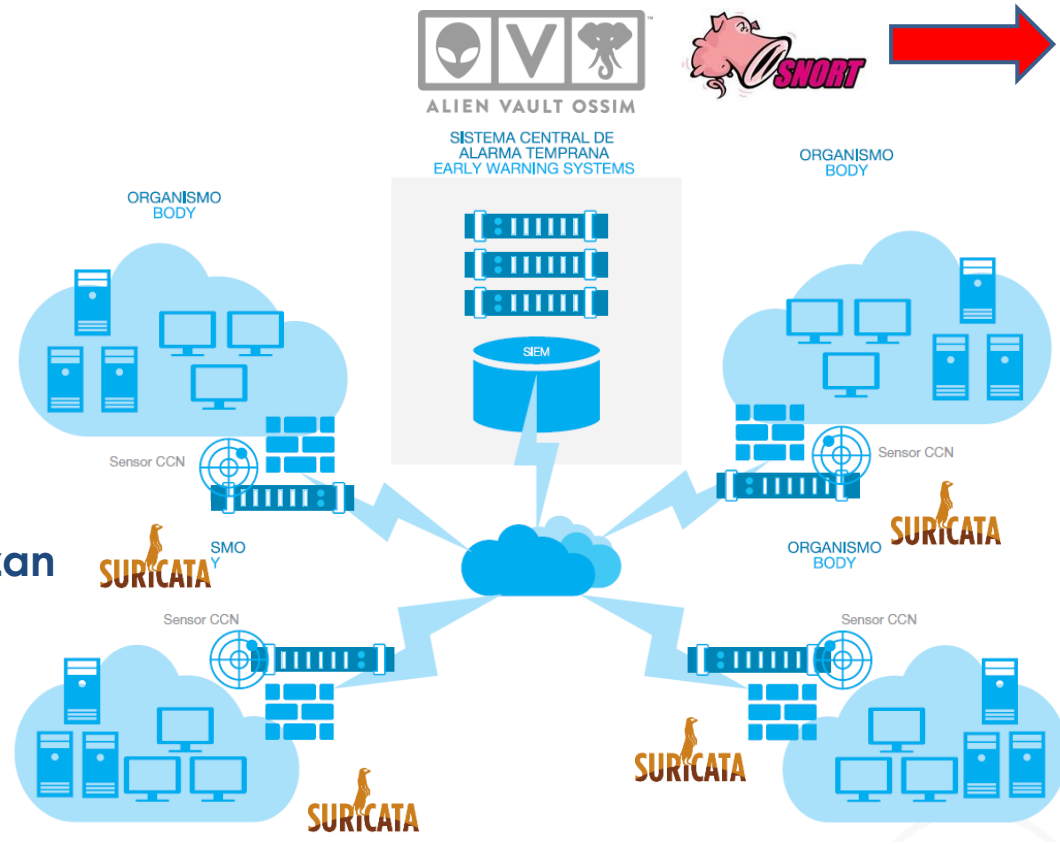


Mejoras 2016:

- Portal de informes
- Auditorias automatizadas
- Mejoras HW / Memoria IDS
- Mejoras en la correlación

Sistema de Alerta Temprana de sondas de Internet

- **Especificaciones de la sonda**
  - SO Debian 64 bits
    - Guías CCN-STIC
  - Aplicaciones Open Source
    - OSSIM: Open Source SIEM
    - Suricata
- **Fuentes de eventos que se analizan**
  - Eventos de SNORT
  - Eventos de Netflow



- **ORGANISMO PROPORCIONA EL HARDWARE Y EL CCN-CERT CONFIGURA Y ADMINISTRA EL EQUIPO DANDO EL SERVICIO.**

CCN-CERT. SERVICIOS

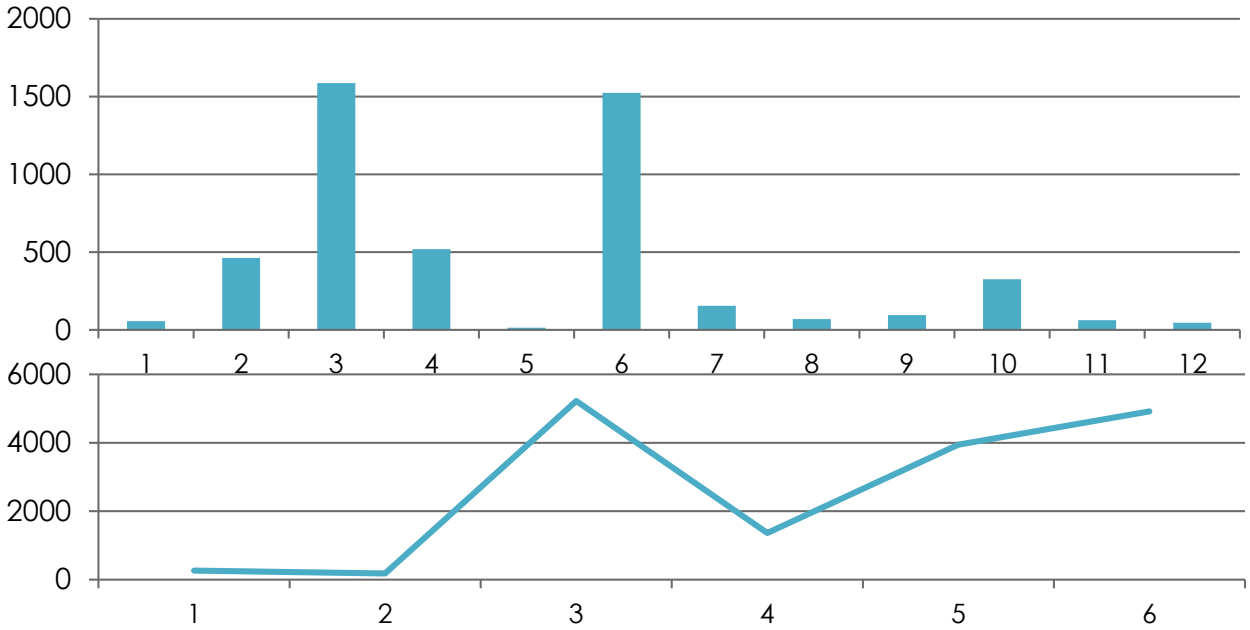
SIN CLASIFICAR

17 COMPAÑÍAS ESTRATÉGICAS

https://portalsat-inet.ccn-cert.es

Reglas de detección

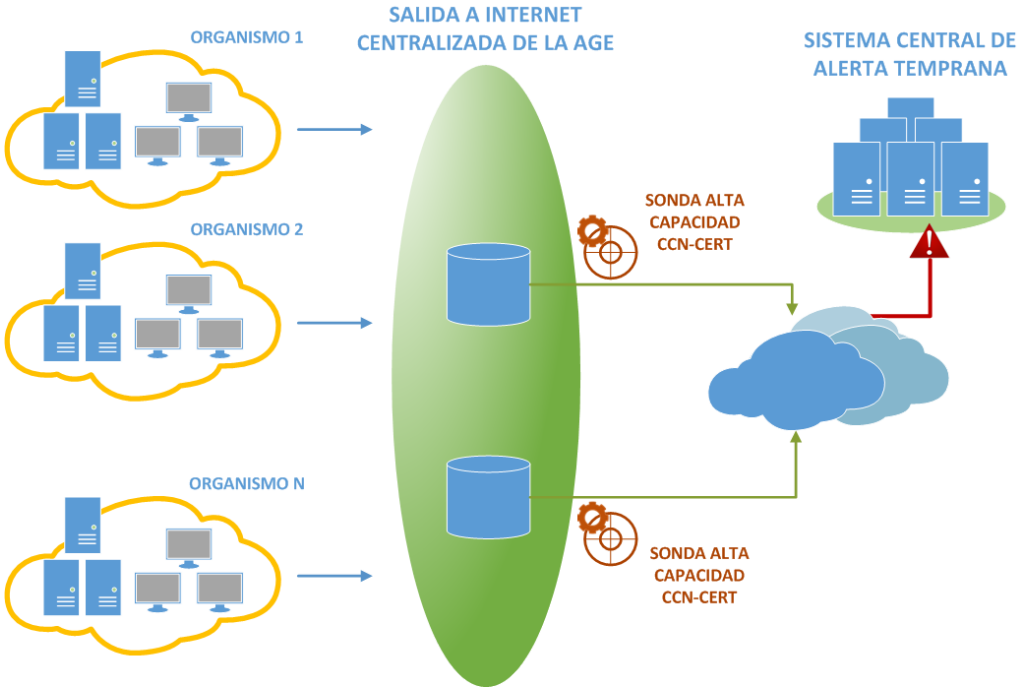
- Reglas de detección propias para su inclusión en el SAT que provienen de:
  - Investigación de incidentes por parte del CCN-CERT
  - Fuentes privadas
  - Intercambio con **Servicios de Inteligencia**
- En 2015 si incluyeron un total de 4.915 reglas propias nuevas



+ 50.000 REGLAS

SAT en la salida a Internet centralizada de la AGE

- Despliegue de dos sondas en los dos puntos de agregación (solución de Verint)
  - Instalación de sonda en Tecnoalcalá (Telefónica) y en el CPD del MEYSS
  - Envío de eventos al Sistema Central del SAT de Internet



  - Ampliación del servicio a organismos que no están en el SAT actualmente.

CLASIFICACIÓN DE LOS INCIDENTES

CRÍTICOS

- APT con exfiltración información
- DDoS (Denegación de Servicio Distribuido)

MUY ALTO

- Ataques Dirigidos
- DoS
- Código dañino específico

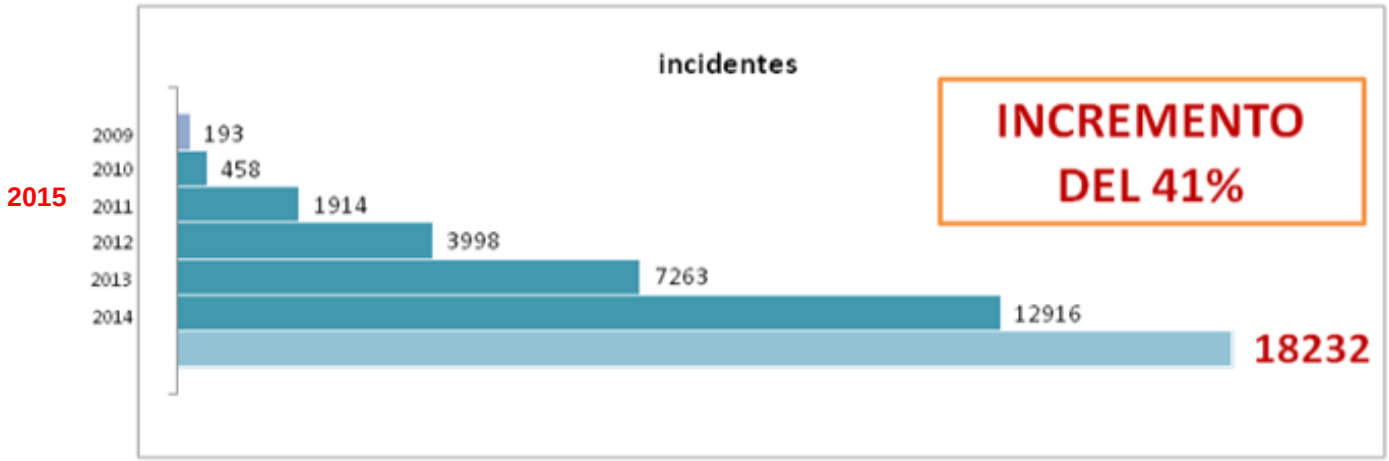
BAJO / MEDIO / ALTO

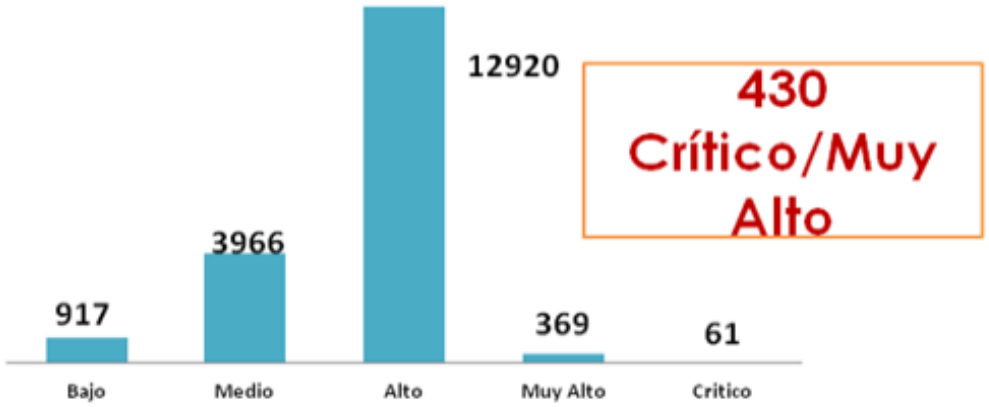
- Mayoría Incidentes
- Ataques externos sin consecuencias
- Código dañino genérico

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

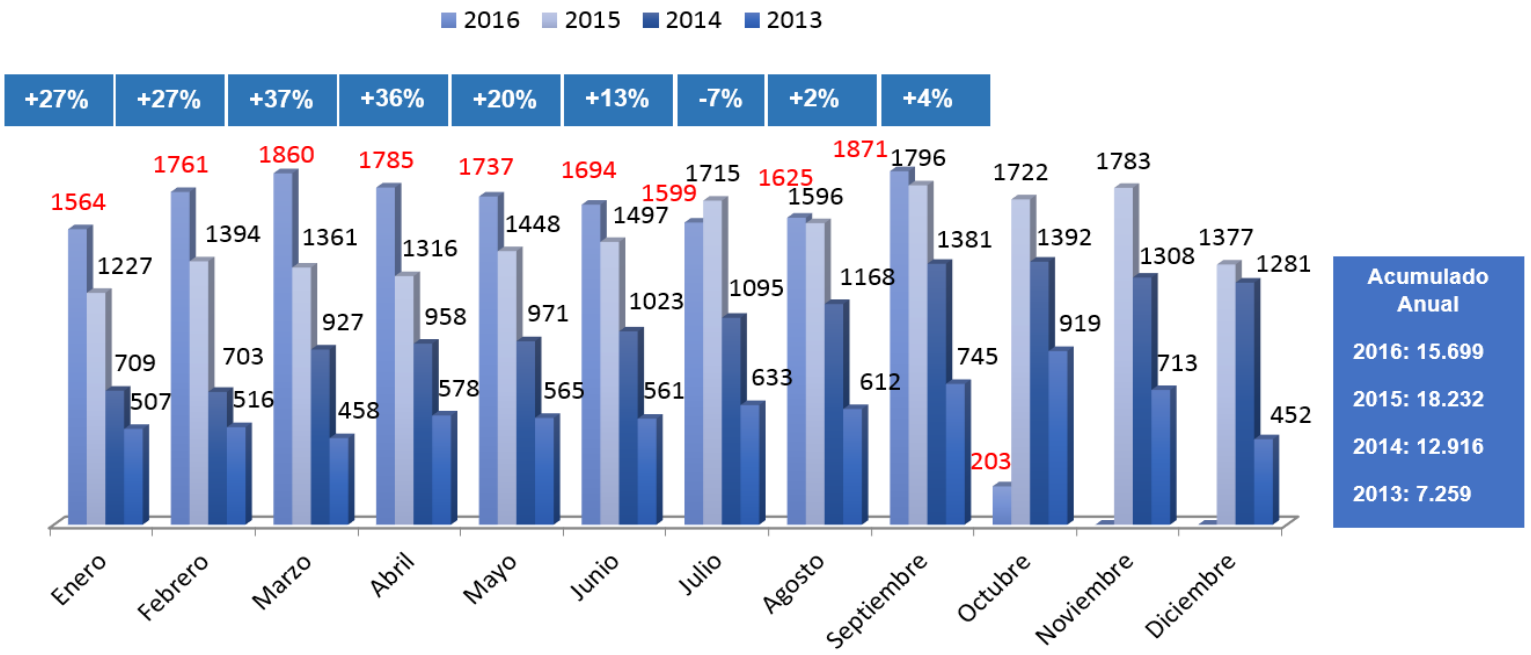
Incidentes detectados por los sistemas de alerta temprana del CCN-CERT

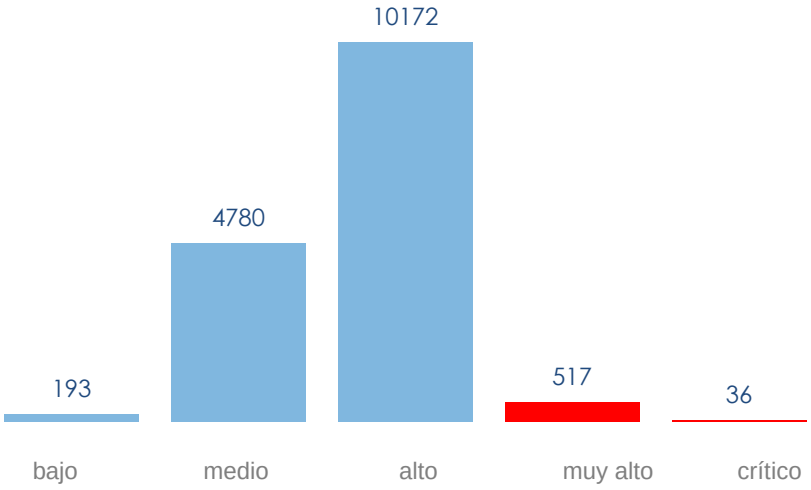
Total de incidentes gestionados por año





05.10.2016
15.700 INC.

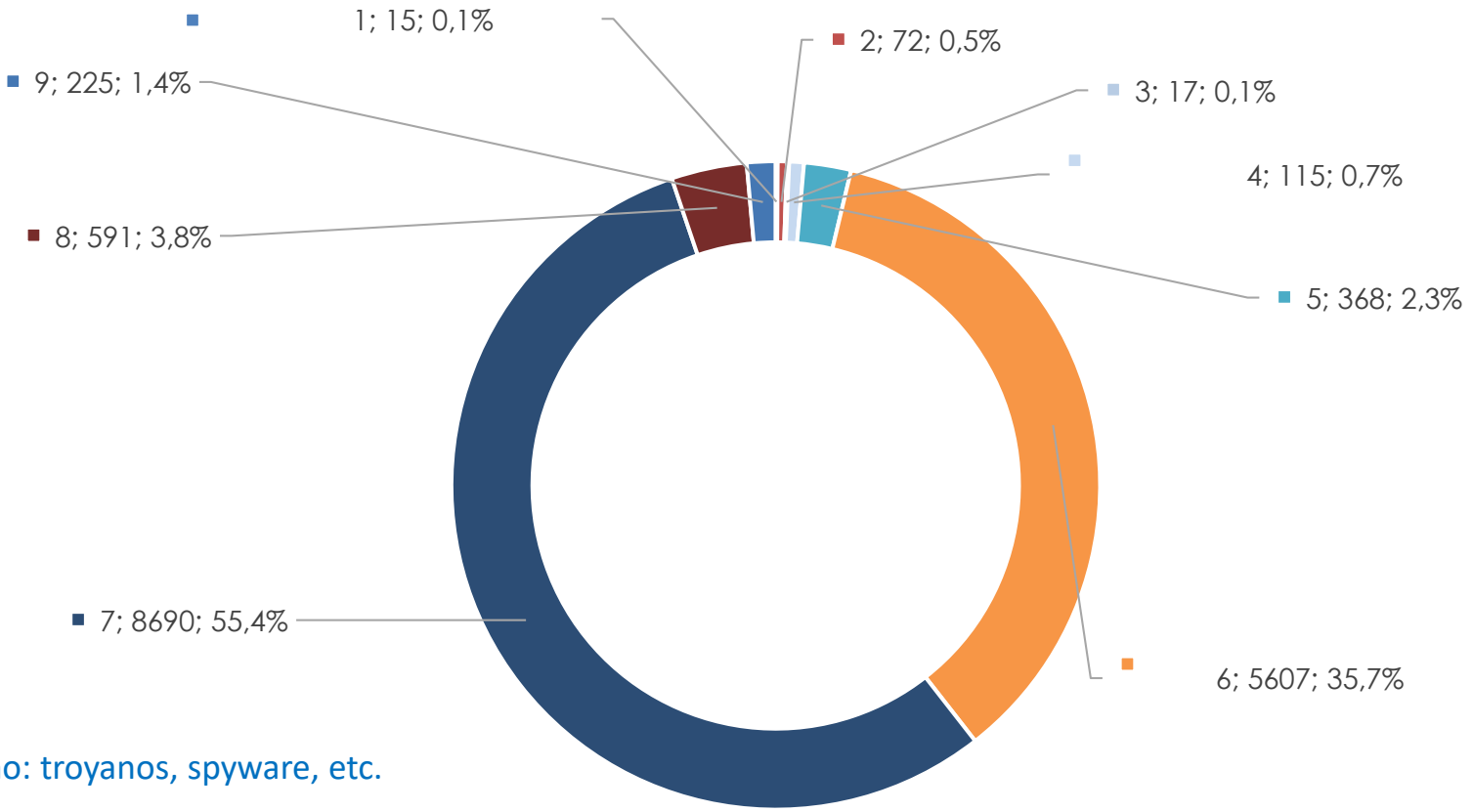




553 críticos
y muy altos

75 % SAT INTERNET
15 % SAT SARA
10 % OTROS

TIPOS DE INCIDENTES



1) Código Dañino: troyanos, spyware, etc.

2) Intrusiones: ataques dirigidos a explotar vulnerabilidades e introducirse

3) Recogida de información: primeros pasos para una campaña mayor (vulnerabilidades, ingeniería social)

4) Seguridad de la información: violaciones de políticas de seguridad

5) Contenido abusivo: contra la imagen

6) Disponibilidad: daños de imagen y productividad (rendimiento)

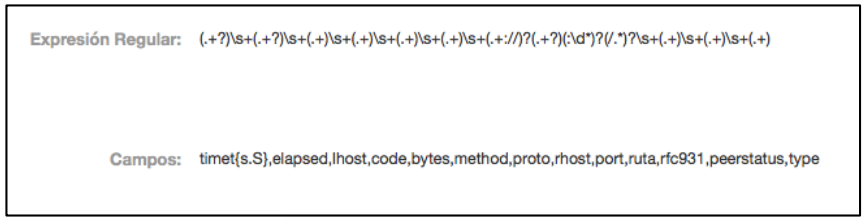
7) Fraude: propiedad intelectual, protección de datos o suplantación de identidad (phishing)

carmen

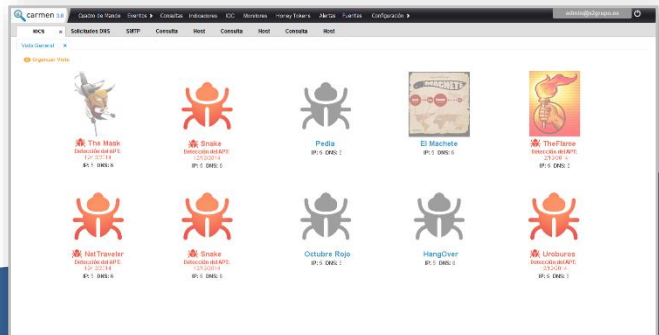
Usuarios: 10K
I/O: 100 Mbps
Datos:
SMTP: 150K hits/day
HTTP: 5M hits/day
DNS: 4M hits/day

S2 GRUPO

- Permite el estudio estadístico del tráfico de red de los siguientes protocolos:
  - HTTP (páginas web)
  - DNS (sistema de nombre de dominio)
  - SMTP (correo electrónico9
  - NetBIOS



- Puede **capturar tráfico directamente** o recibir logs (registros) mediante syslog.



- **Puesto de usuario**
  - Windows Carmen Agent
  - Anomalías en puesto de usuario
- **Elastic Search**
  - **Migración analizadores**
  - **Proceso Python plugins**
  - **Almacenamiento eventos**
- **Detección Intrusión**
  - Triage previo sandboxing.
  - Configuración proceso detección
  - Appliance Carmen intrusión
- **Nuevas capacidades de detección**
  - Integración Bot-Killer
  - Adquisición de peticiones HTTPS
  - Nuevos analizadores e indicadores
- **Reporting**
  - Informes de actividad de usuarios
- **Certificación**
  - Inicio certificación Common Criteria

Calendario de versiones 2016

- Escalabilidad
- Más cabeceras HTTP
- **Integración con LUCIA**
- Múltiples investigaciones

carmen Ciberinteligencia Avanzada
versión 4.2

Ene | Feb | Mar | Abr | May | Jun | Jul | Ago | Sep | Oct | Nov | Dic

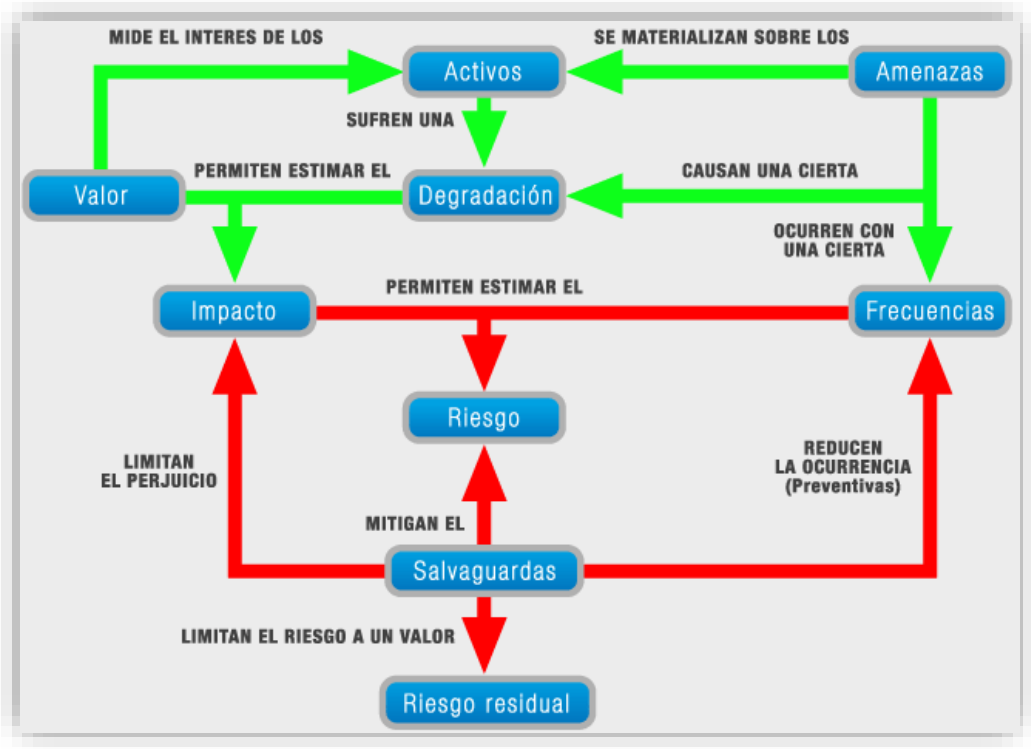
versión 4.0
carmen Ciberinteligencia Avanzada

- **Integración con REYES**
- Uso de datos privados
- Integración con otras fuentes (i.e. SIEM)

versión 5.0
carmen Ciberinteligencia Avanzada

Herramienta PILAR

- **PILAR 5.4**
- **PILAR Basic 5.4**
- **RMAT 5.4**
- **µPILAR 5.4**



CCN-STIC 470G/1 Manual Usuario PILAR 5.4– Análisis y Gestión de Riesgos

CCN-STIC 470G/2 Manual Usuario PILAR 5.34– Análisis de Impacto. Continuidad de Operaciones

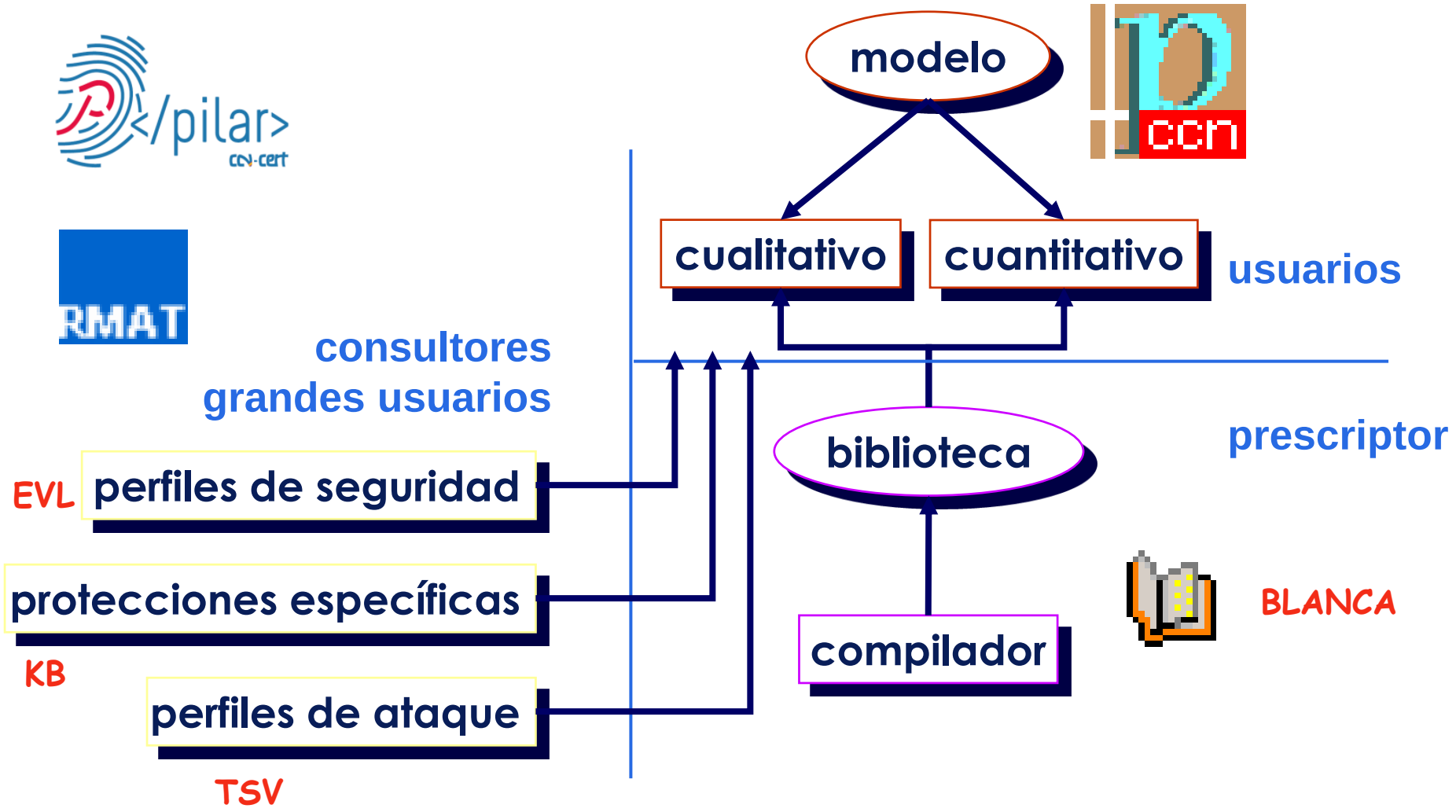
CCN.-STIC 471/D Manual Usuario RMAT.

CCN-STIC 472E Manual Usuario PILAR Basic 5.4

CCN-STIC 473D Manual Usuario µPILAR 5.4

MAGERIT versión 3

Diseño EAR / PILAR



Listado Unificado de Coordinación de Incidentes y Amenazas

LUCIA

/lucía>
CCN-CERT

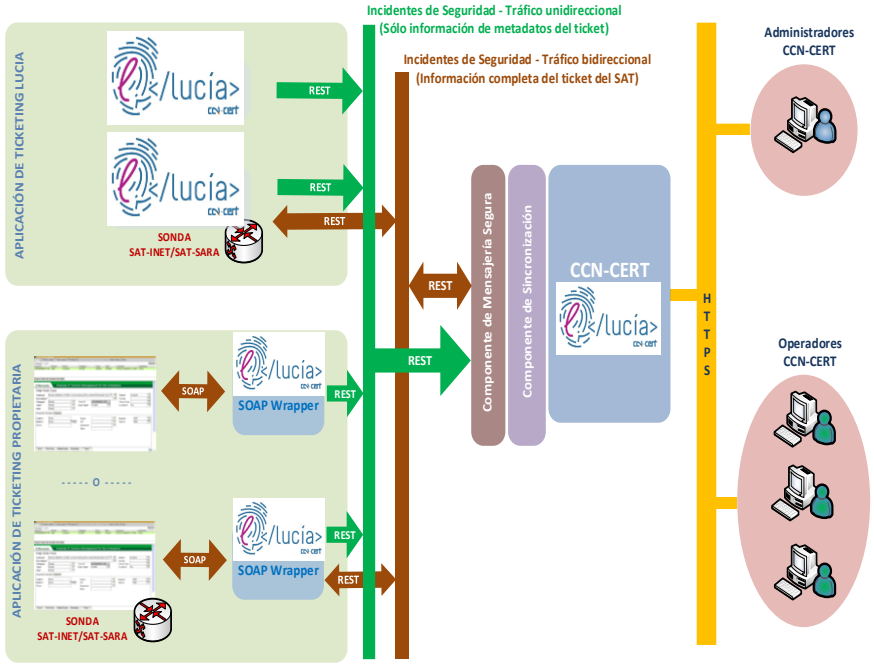
- Cumplir los requisitos del ENS.
- Mejorar la coordinación entre CCN-CERT y los organismos (Mejorar intercambio de incidentes)
- Lenguaje común de **criticidad** y **clasificación del incidente**
- Mantener la **trazabilidad y seguimiento del incidente**
- Automatizar tareas
- **Federar Sistemas**
- 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)

Listado Unificado de Coordinación de Incidentes y Amenazas

- LUCIA Rev2.0 (Septiembre 2015)
- LUCIA Rev2.1 (Diciembre 2015)
- *En producción en el CCN-CERT (1 enero 2016)*
- LUCIA Rev2.2 (Enero 2016)
- LUCIA Rev2.3 (Abril 2016)
- LUCIA Rev2.4 (Mayo 2016)
- *Federación de instancias de organismos*
- LUCIA Rev3.0 (Finales 2016)
  - *LUCIA Multinivel*



Listado Unificado de Coordinación de Incidentes y Amenazas

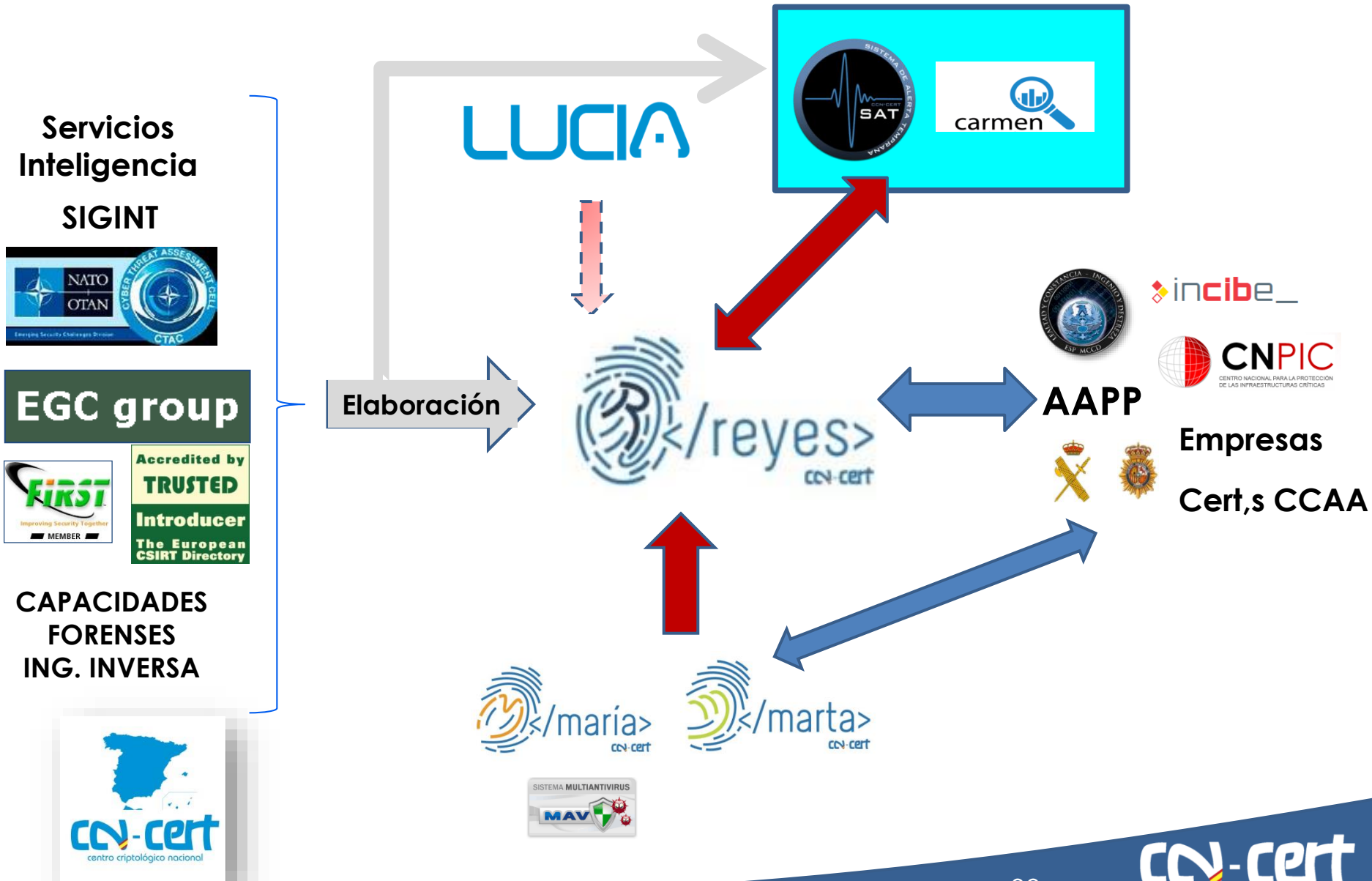
100 Organismos de forma centralizada

- Junta de Castilla y León
- MINECO. Ministerio de Economía y Competitividad
- MINECO-SEC
- MSSSI
- Universidad del País Vasco
- Universidad Politécnica de Cartagena
- Gobierno Balear
- Junta de Andalucía
- Gobierno de Canarias
- Ayuntamiento de Córdoba.
- Correos
- MPR.
- DGT.
- Gobierno de Aragón.
- Junta de Extremadura.
- MEYSS
- MINHAP-SEAP
- MECD
- Ayuntamiento de Málaga
- Melilla
- Consorcio de aguas Bilbao Bizkaia
- EMASESA
- CERT-MX Policía Federal de México
- INE

CAPACIDADES INTERNAS

- **ANÁLISIS FORENSE**
  - Recuperación de información como Perito Judicial
  - Análisis de registros de auditorias de diferentes dispositivos:
    - Firewall / Detectores de intrusos / Registros Proxies / Resoluciones DNS
    - Registros de estaciones trabajo / servidores
  - Análisis e interpretación de tráfico entre equipos / sistemas.
  - Búsqueda de evidencias ante fugas de información clasificada / sensible
- **INGENIERIA INVERSA**
  - Desensamblado de código
  - Análisis estático / dinámico
  - Interpretación de funcionalidades
- **AUDITORIAS WEB**
  - Bajo Demanda

REYES (REpositorio común Y EStructurado de amenazas y código dañino)

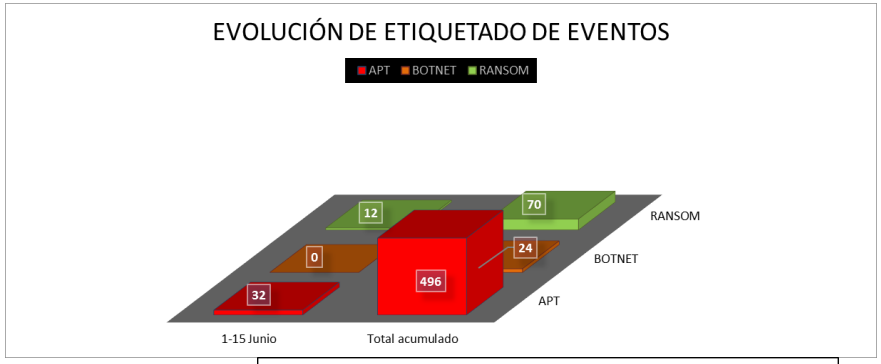


INTEGRACIÓN DE FUENTES

Symantec · panda · EMERGING THREATS · KASPERSKY lab

FireEye · Microsoft

</reyes> ccn-cert ⟷ MISP Threat Sharing



FEDERACIÓN CON OTROS MISP

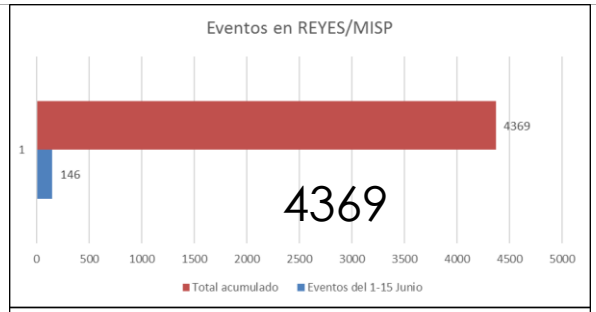
Federación

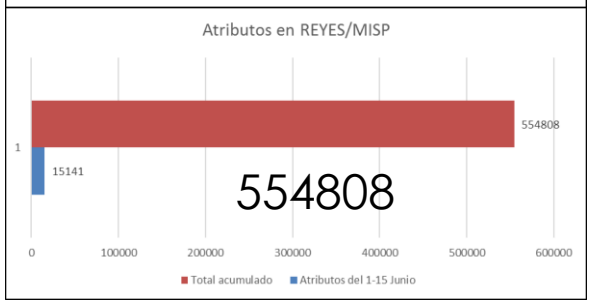
INTERNO

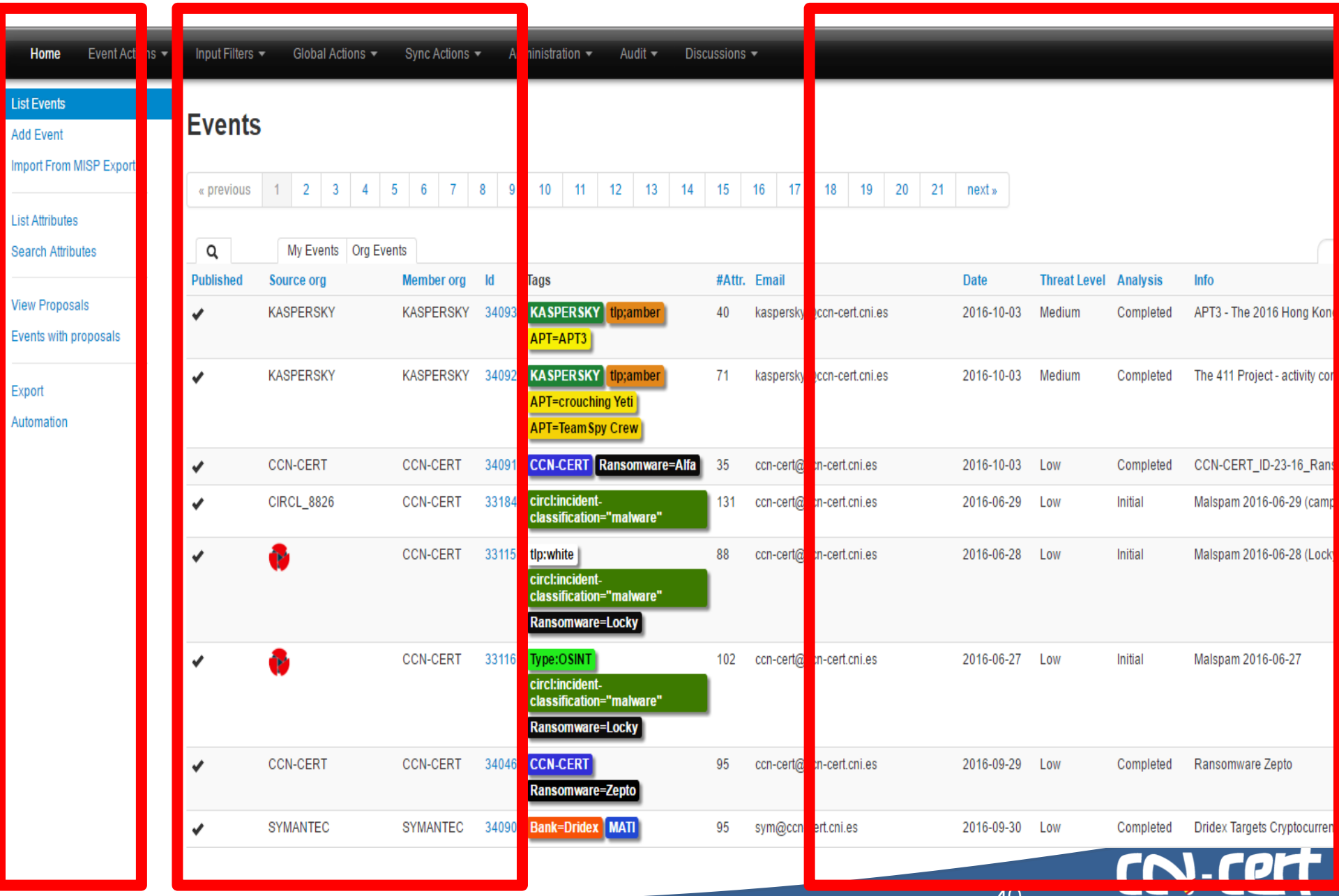
</reyes> ccn-cert

OTROS

FIRST Improving Security Together MEMBER · MISP · CIRCL MISP Threat Sharing · KASPERSKY lab







Home | Event Actions | Input Filters | Global Actions | Sync Actions | Administration | Audit | Discussions

List Events
Add Event
Import From MISP Export
List Attributes
Search Attributes
View Proposals
Events with proposals
Export
Automation

Events

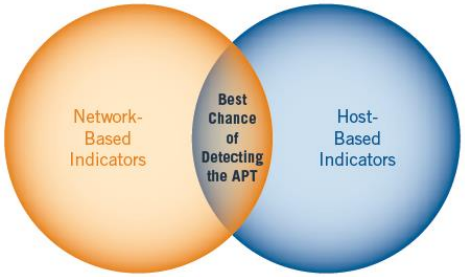
« previous 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 next »

My Events | Org Events

Published	Source org	Member org	Id	Tags	#Attr.	Email	Date	Threat Level	Analysis	Info
✔	KASPERSKY	KASPERSKY	34093	KASPERSKY, tlp:amber, APT=APT3	40	kaspersky ccn-cert.cni.es	2016-10-03	Medium	Completed	APT3 - The 2016 Hong Kon
✔	KASPERSKY	KASPERSKY	34092	KASPERSKY, tlp:amber, APT=crouching Yeti, APT=Team Spy Crew	71	kaspersky ccn-cert.cni.es	2016-10-03	Medium	Completed	The 411 Project - activity cor
✔	CCN-CERT	CCN-CERT	34091	CCN-CERT, Ransomware=Alfa	35	ccn-cert@ n-cert.cni.es	2016-10-03	Low	Completed	CCN-CERT_ID-23-16_Rans
✔	CIRCL_8826	CCN-CERT	33184	circl:incident-classification="malware"	131	ccn-cert@ n-cert.cni.es	2016-06-29	Low	Initial	Malspam 2016-06-29 (camp
✔		CCN-CERT	33115	tlp:white, circl:incident-classification="malware", Ransomware=Locky	88	ccn-cert@ n-cert.cni.es	2016-06-28	Low	Initial	Malspam 2016-06-28 (Lock
✔		CCN-CERT	33116	Type:OSINT, circl:incident-classification="malware", Ransomware=Locky	102	ccn-cert@ n-cert.cni.es	2016-06-27	Low	Initial	Malspam 2016-06-27
✔	CCN-CERT	CCN-CERT	34046	CCN-CERT, Ransomware=Zepto	95	ccn-cert@ n-cert.cni.es	2016-09-29	Low	Completed	Ransomware Zepto
✔	SYMANTEC	SYMANTEC	34090	Bank=Dridex, MATI	95	sym@ccn ert.cni.es	2016-09-30	Low	Completed	Dridex Targets Cryptocurren

DISTRIBUCIÓN DE REGLAS / IOCs

- Reglas **Públicas / Privadas** para la comunidad SAT-INET / Empresas (60.000)
  - ***https://portalsat-inet.ccn-cert.es***
  - Personalización de reglas para cada Organismo
  - Incorporación de diversas fuentes de reglas. Numerosas **firmas de IDS propias (CCN y fuentes privadas)**
- Reglas **Propias / Clasificadas** para uso interno del CCN-CERT (8.000)
  - Intercambio INTELIGENCIA / EGC
  - Relativas a Investigaciones en curso. Se hacen públicas a posteriori
- **Indicadores de Compromiso (CCN-STIC 423)**
  - Facilitar detección
  - Lucha contra APT,S



INTERCAMBIAR = CONFIANZA

¿PREGUNTAS?

- **E-Mails**
  - **ccn-cert@cni.es**
  - **info@ccn-cert.cni.es**
  - **ccn@cni.es**
  - sat-inet@ccn-cert.cni.es
  - sat-sara@ccn-cert.cni.es
  - **incidentes@ccn-cert.cni.es**
  - organismo.certificacion@cni.es
- **Websites**
  - www.ccn.cni.es
  - **www.ccn-cert.cni.es**
  - www.oc.ccn.cni.es

Gracias

Nivel	Cuándo debe emplearse	Con quién se puede compartir la información
TLP:RED	Las fuentes lo emplearán cuando el mal uso de la información pueda impactar en la privacidad, reputación u operaciones	Los receptores **no pueden divulgar la información con otras partes** fuera del ámbito en que se divulgó la información.
TLP:AMBER	Las fuentes lo emplearán cuando es necesario divulgar una información para dar respuesta a ella pero implica riesgos para la privacidad, reputación u operaciones si se divulga fuera de las partes involucradas en la divulgación.	Los recetores **sólo pueden compartir la información con miembros de su propia organización** que necesiten conocer la información y sólo hasta el límite de lo que sea necesario para dar respuesta a esa información.
TLP:GREEN	Las fuentes lo emplearán cuando la información es útil para concienciar o formar a las partes participantes del grupo de intercambio de información así como para otros interesados dentro de las organizaciones participantes o del sector en el que desarrollan su actividad.	Los receptores pueden **divulgar la información en el ámbito interno de sus organizaciones o sector** en el que desarrollen su actividad aunque no abiertamente por canales públicos.
TLP:WHITE	Las fuentes lo emplearán cuando la información conlleva un riesgo de mal uso mínimo o despreciable, de acuerdo con las prácticas y procedimientos propios del a organización referentes a la publicación de información	La información puede ser **redistribuida sin limitaciones**, siempre sujeto a restricciones legales (privacidad y/o derechos de propiedad intelectual).

Sectores que reciben más ataques en ESPAÑA

Disponibilidad

Energético

Industria Nuclea

Administración

Espacio

Financiero

Hídrico

Al on

Transporte

Sanid ndustria Química

ones de Investigación

Tecnologías de la Información

Infraestructuras Críticas

CNPIC
CENTRO NACIONAL PARA LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS

Confidencialidad
Protección del Patrimonio

Energético

Ae al

Administración

Defensa

armacéutico

Minería

Financi

Marítimo

Qu

Ingeniería

aciones

Derechos Humanos

Sectores Más atacados

Conjunto de Herramientas

- **PILAR**
  - Análisis de Riesgos cualitativo / cuantitativo
  - Análisis de impacto-continuidad de negocio cuantitativo / cualitativo
- **Pilar BASIC**
  - Análisis de riesgos para PYMES / Sistemas pequeños.
- Herramientas de personalización (RMAT)

  EVL: perfiles de seguridad

  TSV: threat profiles

  KB: protecciones adicionales por activo
- **Pilar MICRO**
- Pilar BATCH
- Creación de nuevas bibliotecas

  BLANCA: compilador de bibliotecas (no se distribuye)