Associació Catalana de Municipis

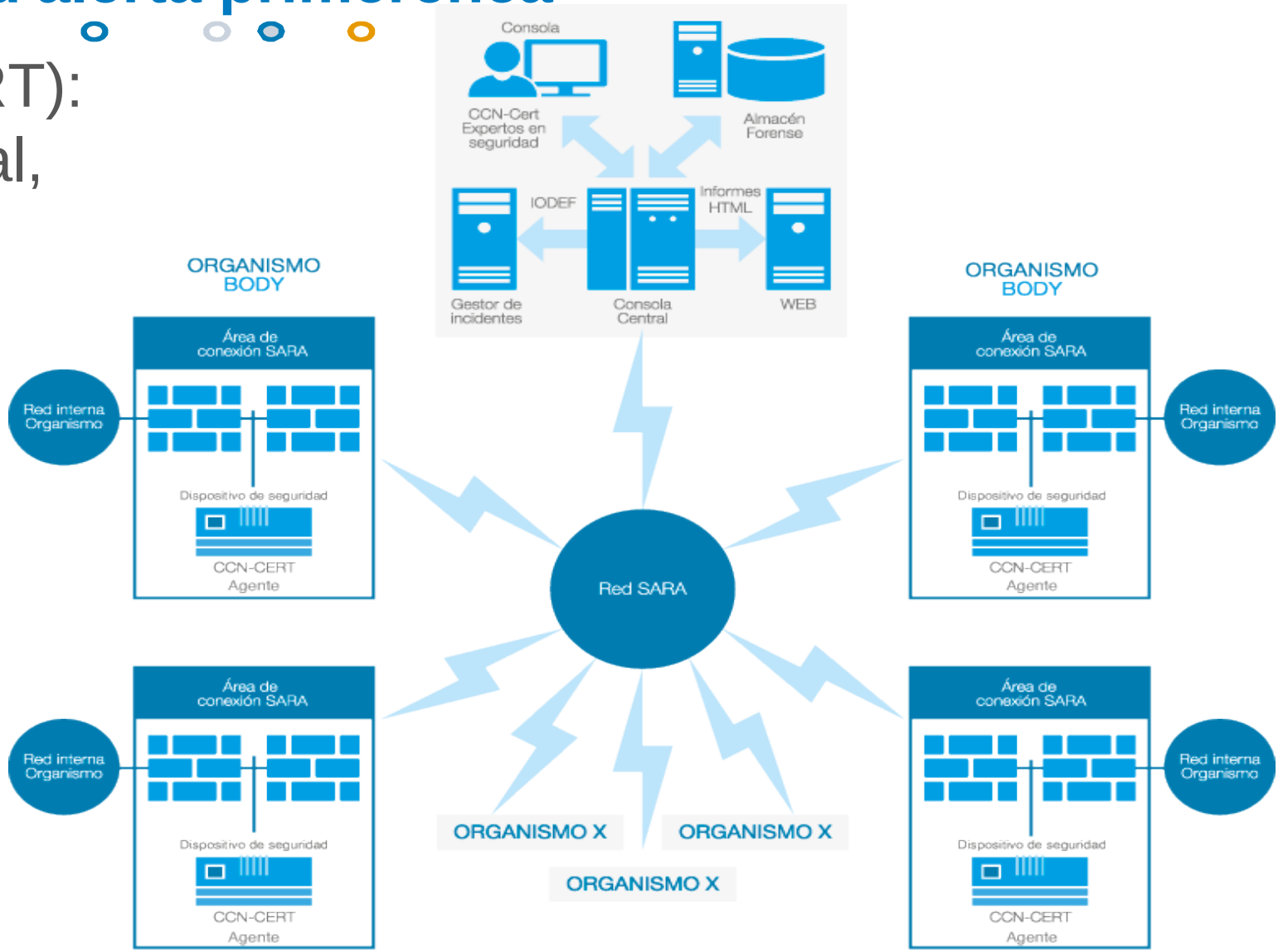
# 4. Responsabilitat Social: Resposta diligent

# Índex del curs: 4. Responsabilitat Social: Resposta diligent

- Resposta a incidents: SOC vs. CSIRT
- Equips mixtos CESIRT + LEA tradicional
  - Suport dels CESIRT a la policia: Peritatge
  - Suport de la policia al CESIRT
  - col·laboració entre equips policials
- Captura i custòdia d'evidències, Live-for
  - Indicis,
  - Evidències
  - Forense
  - No-investigació
- Procés d'investigació: Què? Quan? Qui? Com? On? Perquè?
  - Preparació per captures forenses
- Exemples d'incidents:

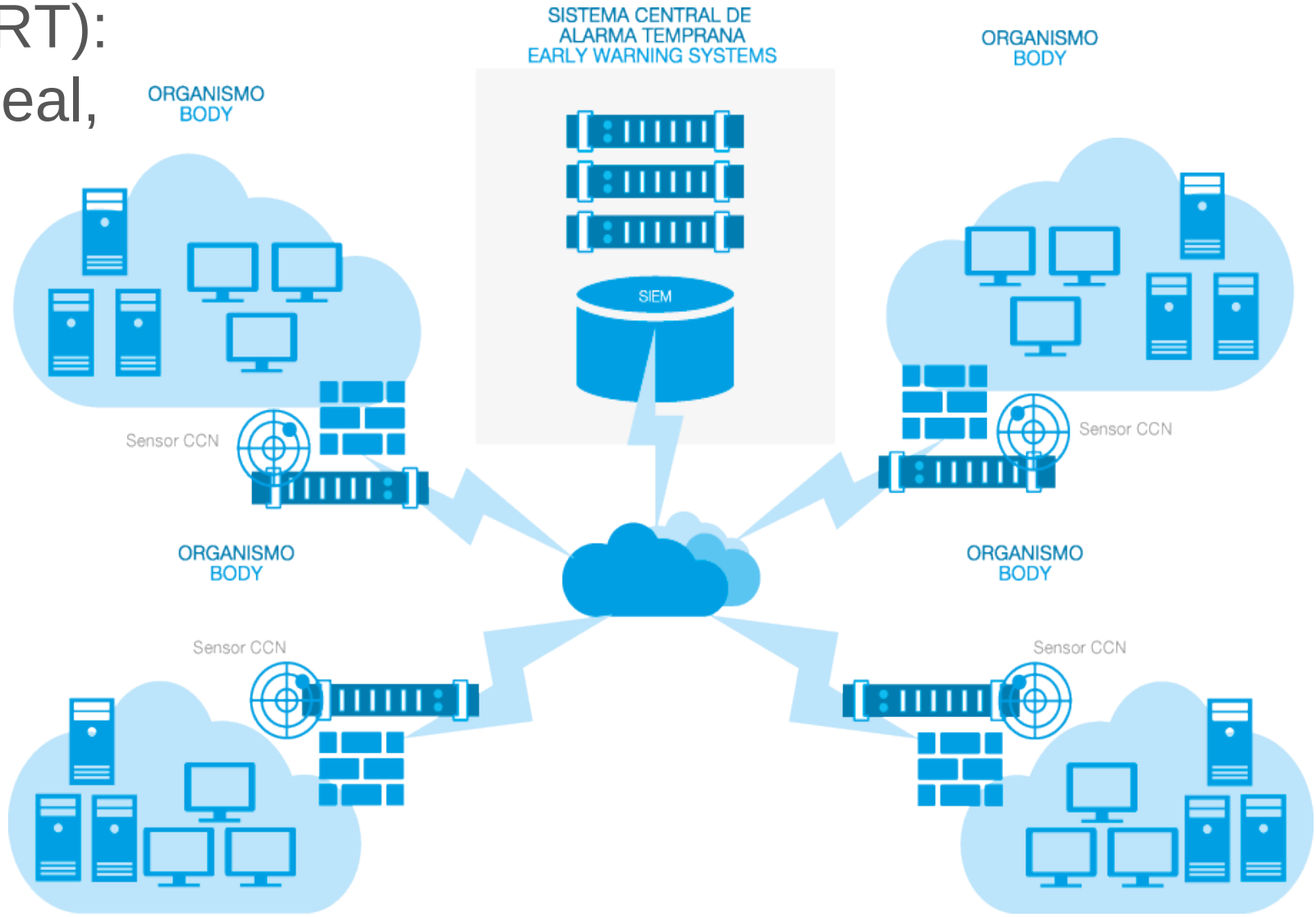
# Serveis d'alerta primerenca

- SAT-SARA (CCN-CERT): Detecció, en temps real, d'atacs i amenaces analitzant el tràfic de xarxa dels Organismes de les Administracions Públiques connectats a la xarxa SARA



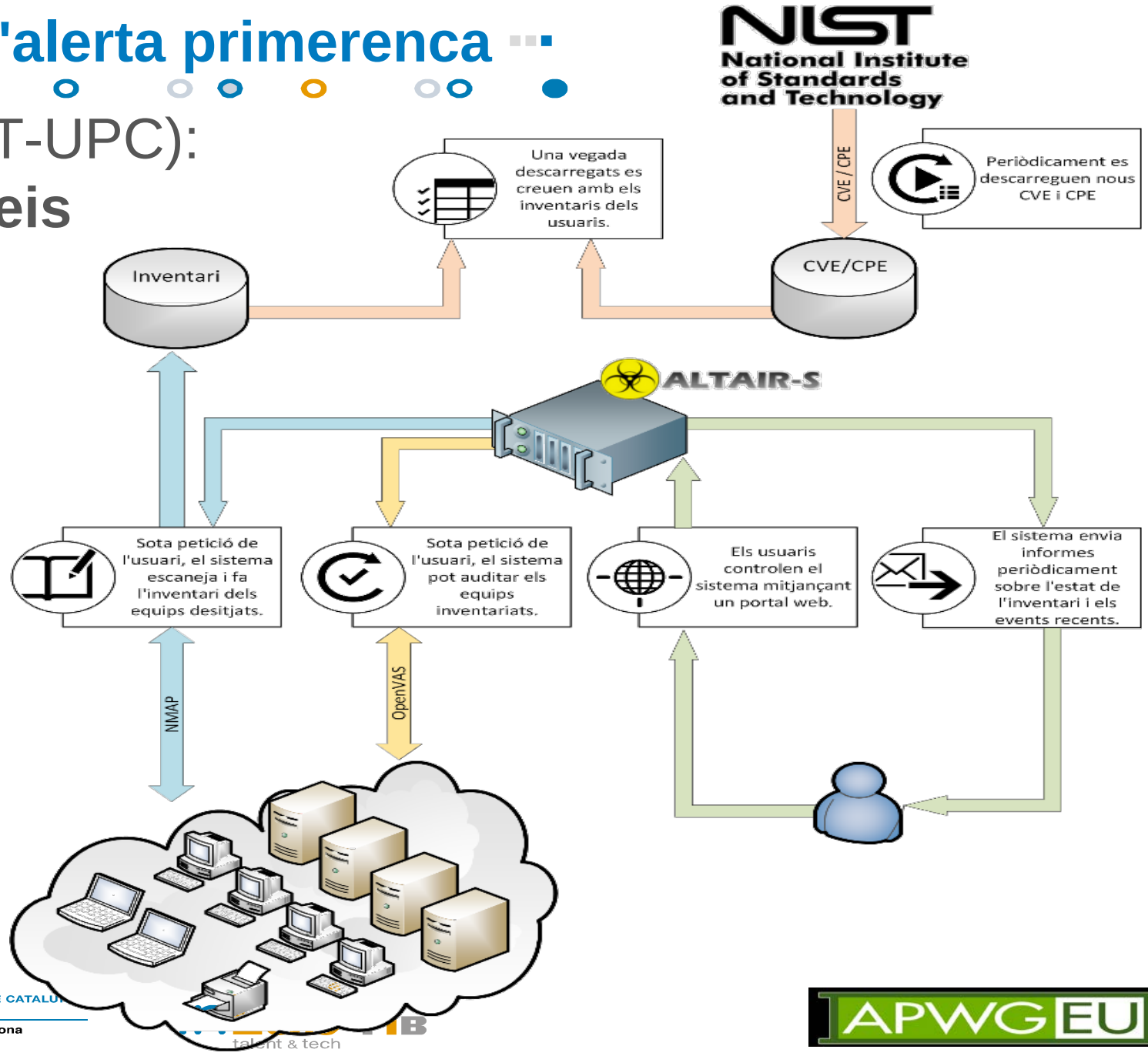
# Serveis d'alerta primerenca

- SAT INET (CCN-CERT): Detecció, en temps real, de les amenaces i incidents existents en el tràfic de xarxa entre l'organisme adscrit i Internet



# Serveis d'alerta primerenca

- ALTAIR-SIGVI (esCERT-UPC): Inventari d'actius i **serveis** d'una Organització amb identificació de les **vulnerabilitats** i posterior classificació segons el nivell de criticitat de les mateixes



# Serveis de comunicació d'incidents

- RTIR (Best Practical):
  - Eina de tractament de tiquets de codi obert basat en RT que permet gestionar incidents de seguretat incorporant cues i fluxos de treball dissenyats per equips de resposta a incidents
- LUCIA (CCN-CERT)
  - Eina de tractament de tiquets desenvolupada pel CCN-CERT per a la gestió d'incidents en les entitats de l'àmbit d'aplicació de l'Esquema Nacional de Seguridad

# RT: Request Tracker

- RT és un sistema gestió de tiquets realitzat en Perl
- La primera versió de RT va ser escrita l'any 1996 per Jesse Vincent qui, posteriorment, va crear "Best Practical Solutions LLC" per a distribuir, desenvolupar i recolzar l'aplicació
- Gratuït i de codi obert (FOSS), es distribueix amb la Llicencia Pública General GNU
- Integració amb correu electrònic (crear i respondre)
- Generació d'una base de dades de coneixement
- Fluxos de treball personalitzats
- Disposa d'interfície des de línia de comandes

# RT-IR

- RT-IR (RT for Incident Response) és un RT modificat amb les eines i fluxos de treball adequats per als equips CERT/CSIRT
- Va ser dissenyat per JANET-CSIRT (Xarxa acadèmica del Regnet Unit) juntament amb TERENA (ara part de la Xarxa europea GÉANT) i desenvolupat per Best Practical Solutions, LLC
- L'any 2006 es va actualitzar i es va ampliar amb el finançament conjunt de 9 Equips de Resposta a Incidents de Seguretat europeus, tant d'àmbit acadèmic com governamental

# RT-IR

- Les característiques principals de RT-IR són les següents:
  - Tauler principal on es mostren els tiquets per cada incident (es pot seleccionar que mostri únicmanet els més importants)
  - Es poden fer cerques per qualsevol atribut dels tiquets
  - Permet genera informes d'activitat en format HTML, text i CSV
  - Disposa d'un API ("RT API") que li permet acceptar dades de sistemes externs tals com Splunk, ArcSight, Nagios, Sguil i Qualys
  - Permet la creació de múltiples cues de notificació d'incidents per segregar els informes rebuts

# Estructures CSIRT: estatals: CCN-CERT: Eines de prevenció

LUCIA (Listado Unificado de Coordinación de Incidentes y Amenazas) es una herramienta desarrollada por el CCN-CERT para la Gestión de Ciberincidentes en las entidades del ámbito de aplicación del Esquema Nacional de Seguridad. Con ella se pretende mejorar la coordinación entre el CERT Gubernamental Nacional y los distintos organismos y organizaciones con las que colabora.

LUCIA ofrece un lenguaje común de peligrosidad y clasificación del incidente y mantiene la trazabilidad y el seguimiento del mismo. El sistema permite, además, automatizar las tareas e integrarse con otros sistemas ya implantados.

Con LUCIA, el organismo podrá gestionar tres tipos de ciberincidentes:

- Los incidentes propios del Organismo
- Los provenientes del Sistema de Alerta Temprana de Red SARA (SAT-SARA).
- Los provenientes del Sistema de Alerta Temprana de Internet (SAT-INET).

# LUCIA

- LUCIA (**L**istado **U**nificado de **C**oordinación de **I**ncidentes y **A**menazas) és l'eina de tractament de tiquets basada en RT-IR i personalitzada per complir amb els requeriments i procediments del CCN-CERT
- Està alineada amb el complimento de l'Esquema Nacional de Seguridad (ENS )
- Permet una interacció entre diferents sistemes de gestió d'incidents i la creació d'una federació d'aquestes sistemes
- Pot integrar la gestió dels serveis d'alerta primerenca SAT-SARA i SAT-INET

# LUCIA

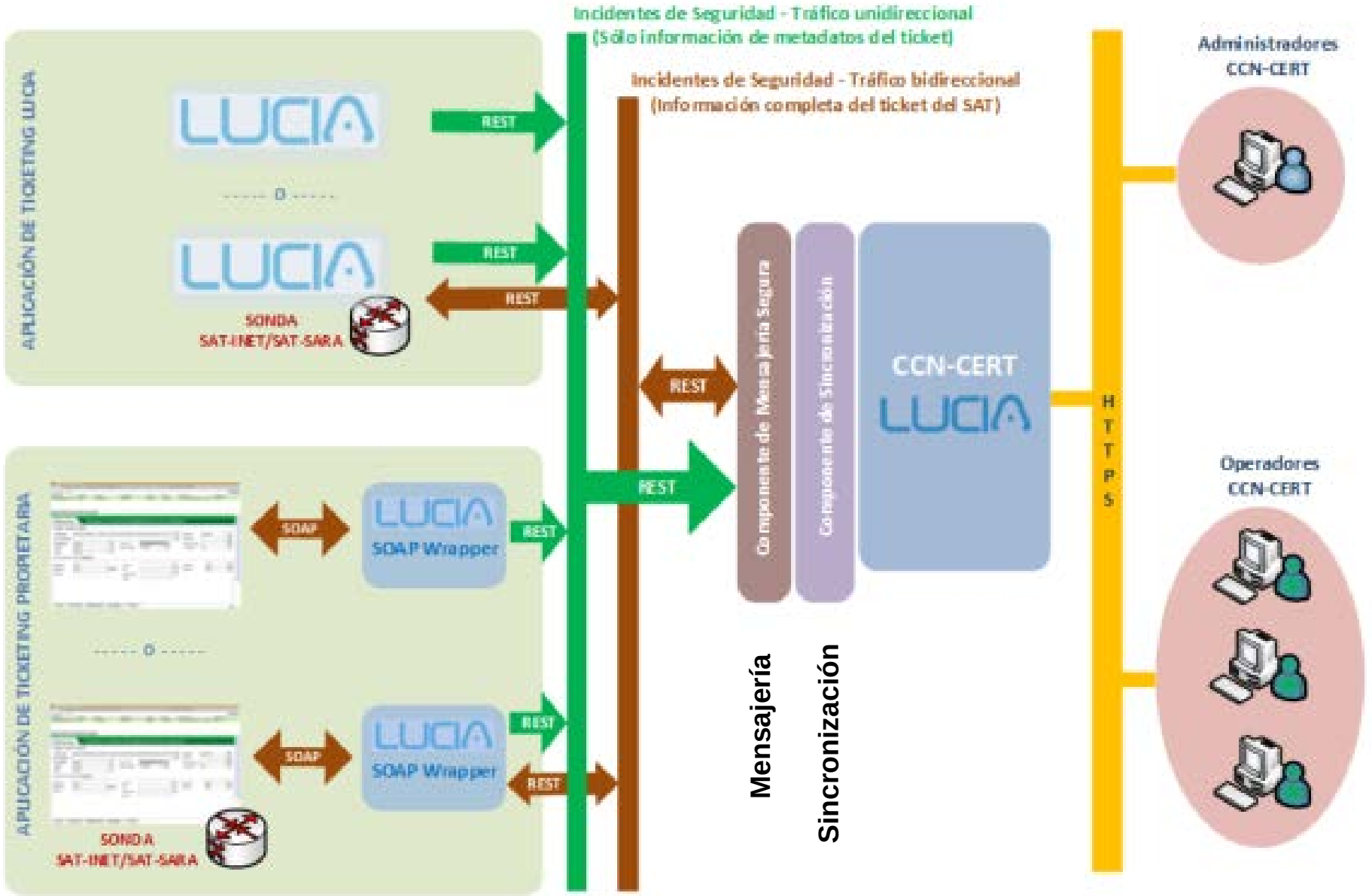
- Els avantatges principals d'utilitzar aquest eina són:
  - Compleix els requisits de l'ENS i la seva guia CCN-STIC-817 per a la Gestió d'Incidents en l'ENS
  - Ofereix un "llenguatge comú" de perillositat i classificació de l'incident basat en dos nivells i avalat per institucions internacionals
  - Millora la coordinació entre el CCN-CERT i tots els organismes als que ofereix els seus serveis mitjançant la integració dels incidents de seguretat amb el CCN-CERT
  - Millora l'intercanvi d'informació d'incidents de seguretat
  - Permet mantenir la traçabilitat i seguiment de l'incident
  - Permet millorar els processos de gestió

# LUCIA

- (...)
  - Permet l'automatització de tasques i la integració amb altres sistemes
  - Permet la categorització del tancament i causes de l'incident
  - Permet la construcció de bases de dades de coneixement
  - Millora la gestió dels projectes SAT-SARA i SAT-INET

# LUCIA

- Esquema de Federació de sistemes LUCIA:



# LUCIA

- Es distribueix com a **màquina virtual** en format OVF
  - Requereix 2 nuclis de processador, 4 gigabytes de RAM i uns 200 gigabytes de disc dur
- Les actualitzacions de seguretat i de versions són realitzades pel CCN-CERT
- La comunicació de LUCIA amb el CCN-CERT és **unidireccional**:
  - Únicament s'envia la meta-informació de l'incident (perillositat, estat, categorització, etc.) sense incloure missatges confidencials ni dades subjectes a la LOPD
- Si l'organisme té mes serveis (p. ex. SAT-SARA), aleshores la comunicació és **bidireccional** (tiquet)

# Estructures CSIRT: estatals: CCN-CERT: Eines de prevenció

- **Sistema de Alerta Temprana (SAT)**

Sistema desarrollado por el CCN-CERT desde el año 2008 que busca actuar antes de que se produzca un incidente o, por lo menos, detectarlo en un primer momento para reducir su impacto y alcance. Este Sistema de Alerta Temprana (SAT) para la detección rápida de incidentes y anomalías dentro de la Administración y de las empresas de interés estratégico, se enmarca dentro de las acciones preventivas, correctivas y de contención realizadas por el CERT Gubernamental Nacional.

- El SAT cuenta con dos vertientes con un denominador común: la detección temprana de intrusiones. En ambos casos existe un portal de informes al que los responsables de seguridad autorizados pueden acceder para la consulta en tiempo real de eventos de seguridad y para la generación de informes a medida.

- SAT SARA
- SAT INET

# Estructures CSIRT: estatals: CCN-CERT: Eines prevenció

El **Sistema de Alerta Temprana (SAT) de la red SARA (SAT-SARA)*** es un servicio desarrollado por el CCN-CERT en colaboración con el Ministerio de Hacienda y Administraciones Públicas (Organismo responsable de la red SARA).

Su objetivo es la detección en tiempo real de ataques y amenazas, llevado a cabo a través del análisis del tráfico de red que circula entre las redes de los Organismos de las Administraciones Públicas conectados a la red SARA.

# Estructures CSIRT: estatals: CCN-CERT: Eines prevenció

Para su puesta en marcha es necesaria la implantación de una **sonda individual** en la red del Organismo, que se encarga de recolectar la información de seguridad relevante que detecta y, después de un primer filtrado, enviar los eventos de seguridad hacia el **sistema central** que realiza una correlación entre los distintos elementos y entre los distintos dominios (organismos). Inmediatamente después, el Organismo adscrito recibe los correspondientes avisos y alertas sobre los incidentes detectados.

# Estructures CSIRT: estatals: CCN-CERT: Eines d'Adequació al ENS

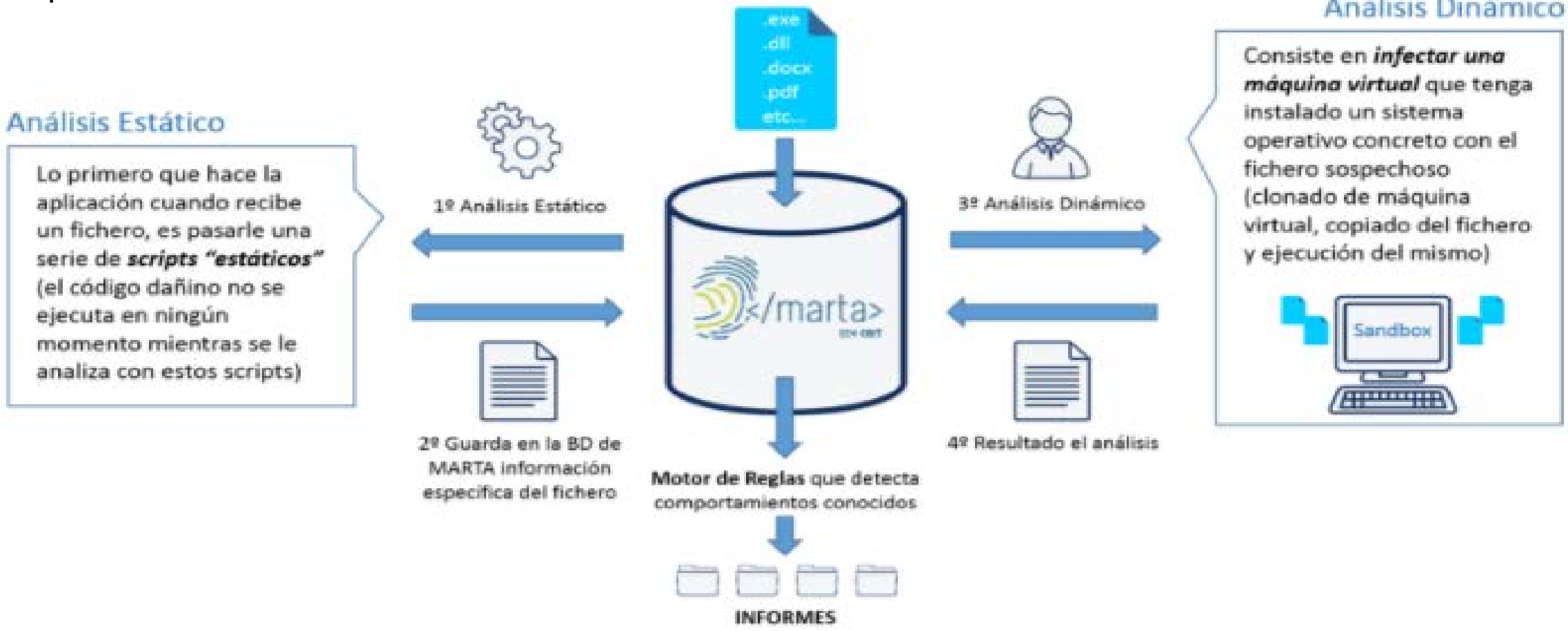
- **MARIA, plataforma multiantivirus en tiempo re**
- Herramienta de detección desarrollada para el an
  dañino a través de múltiples motores antivirus y a
  Windows y Linux.
- La herramienta permite analizar en tiempo real cualquier tipo de fichero, obteniendo la detección de virus, gusanos, troyanos y todo tipo de código dañino.
- Una de las ventajas de MARIA es que analiza cualquiera de los ficheros subidos de forma aislada, lo que garantiza que dicho fichero no es trasladado a ninguna otra organización, ni empresa antivirus. Esta característica hace al nuevo servicio del CERT Gubernamental Nacional una herramienta perfecta para la investigación de incidentes, particularmente APT.

</maría>
Sistema multiantivirus para el análisis estático de código dañino.

# Estructures CSIRT: estatals: CCN-CERT: Eines d'Adequació al ENS

- **La herramienta MARTA, desarrollada por el CCN-CERT,** es una plataforma avanzada de sandboxing que está dedicada al análisis automatizado de múltiples tipos de ficheros que podrían tener algún comportamiento malicioso.
- El análisis de ficheros incluye ejecutables, documentos de office o documentos en pdf, entre otros.

</marta>
Sistema para el análisis dinámico de código dañino.



# Estructures CSIRT: estatals: CCN-CERT: Eines d'Adequació al ENS

CARMEN, Centro de Análisis de Registros y Minería de EveNtos, es un desarrollo del Centro Criptológico Nacional y la empresa S2Grupo para la identificación del compromiso por parte de amenazas persistentes avanzadas (APT), constituyendo la primera capacidad española, basada en conocimiento y tecnología nacionales, en este sentido.

CARMEN es una herramienta de adquisición, procesamiento y análisis de información para la generación de inteligencia principalmente a partir de los tráficos de una red. Se compone de agentes que recopilan los flujos de tráfico (elementos de adquisición), un motor de base de datos en el que se inserta la información y una aplicación web que permite la representación y consulta de la información obtenida, para que un analista trabaje con ella y tome decisiones a partir de los resultados proporcionados por la herramienta.

Los orígenes de datos que actualmente soporta CARMEN son:

- HTTP, tanto a partir de un PROXY, como de forma pasiva.
- DNS, de forma pasiva.
- SMTP, de forma pasiva.
- IPC, de forma pasiva.

Sobre cada una de las fuentes de datos, CARMEN permite la aplicación de reglas predefinidas para la detección de usos indebidos y, especialmente, para la detección de anomalías significativas (estadísticas, cadenas de texto, series temporales y basadas en conocimiento) que puedan ser indicativas de un compromiso en la organización, así como la definición e integración de nuevo conocimiento en la herramienta, desde IOC hasta condiciones de anomalía.

CARMEN está orientada a la identificación de movimientos externos (servidores de C&C y servidores de exfiltración) y movimientos laterales de una amenaza persistente avanzada.

# Estructures CSIRT: estatals: CCN-CERT: Eines d'Adequació al ENS

REYES es una herramienta desarrollada por el CCN-CERT para agilizar la labor de **análisis de ciberincidentes y compartir información** de ciberamenazas.

A través de este portal centralizado de información puede realizarse cualquier investigación de forma rápida y sencilla, accediendo desde una única plataforma a la información más valiosa sobre ciberincidentes. Una información contextualizada y correlada con las principales fuentes de información, tanto públicas como privadas.

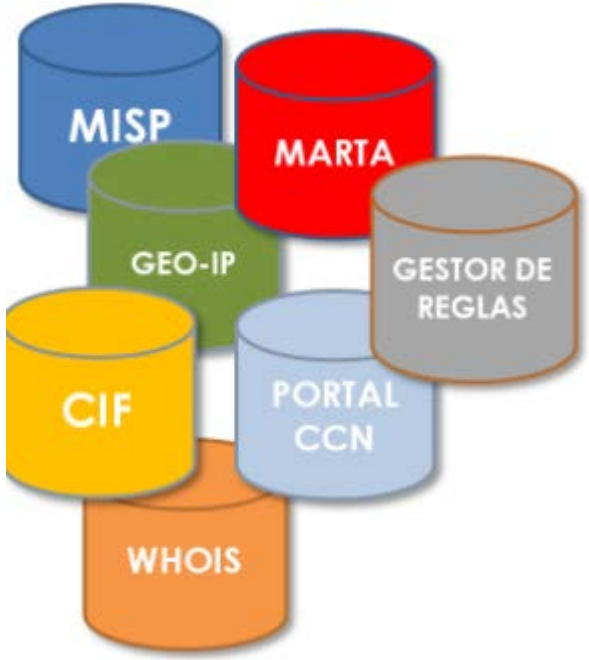
En un primer momento, REYES se basó en la tecnología MISP

Desde REYES se puede acceder a:

- Plataforma MISP, a su vez federada con otras organizaciones como OTAN, FIRST, EGC y otros CERT
- Reglas del SAT
- Listas Negras relacionadas con incidentes (APT, botnet, malware, ransomware, spam o TOR)
- CIF
- WHOIS y geolocalización
- MARTA

</reyes>

Repositorio común y estructurado de amenazas y código dañino.



# Estructures CSIRT: estatals: CCN-CERT: Eines d'Adequació al ENS

Herramienta web diseñada para **analizar las configuraciones** de los dispositivos de red, routers y conmutadores Cisco.

El análisis del cumplimiento está basado en las normas de seguridad proporcionadas a través de las guías CCN-STIC, en concreto la CCN-STIC-641, Seguridad en Routers Cisco, y CCN-STIC-644 Seguridad en equipos de comunicaciones Switches Cisco. Este análisis se basa en la comprobación de una serie de reglas, desarrolladas por el CCN, sobre la configuración y los resultados de ejecutar ciertos comandos en las consolas de los equipos.

Estas **reglas se irán actualizando** conforme los fabricantes actualicen sus sistemas operativos o creen nuevas funcionalidades.

La herramienta se proporciona como una interfaz web en la que se permite almacenar configuraciones, seleccionar distintos paquetes de reglas y generar informes de cumplimiento.

Está previsto ampliar la herramienta a equipos cortafuegos y otros fabricantes

</rocío>
Herramienta de auditoría de cumplimiento con el ENS/STIC en dispositivos de red.

# Gràcies per la vostra atenció!