Servicios CCN-CERT
Sector Salud

USO OFICIAL

Buscar... Abrir sesión

DEFENSA FRENTE A LAS CIBERAMENAZAS

Inicio | Sobre nosotros | Gestión de incidentes | Formación | Guías | Informes | Herramientas | ENS | Empresas | Seguridad al día | Registro

ÚLTIMA HORA 01/06/2015 17:51

Creada una fundación contra el cibercrimen

NIVEL DE ALERTA

MUY ALTO

SAT

CURSOS ONLINE

ENS

INCIDENTES

CARMEN
Herramienta de Detección de APTs

CCNDroid
Herramientas de Seguridad para Android

CLARA
Auditoría de Cumplimiento ENS/STIC en Sistemas Windows

INES
Informe de Estado de Seguridad en el ENS

LUCIA
Sistema de Gestión Federada de Tickets

CURSOS CCN-STIC

X Curso STIC Seguridad en redes inalámbricas
Fase presencial: del 18 al 22 de mayo

SERIES CCN-STIC

Índice de Guías (abril-2015)

Última guía serie 800 (ENS)

INFORMES

Informes de Código Dañino (ID)
CCN-CERT ID-20/14 Informe de Código Dañino e IOC de GeckaSeka

Problemática del Sector Salud

- **Muy atractivo por los datos que maneja**
  - Parte importante de las pérdidas de datos son consecuencia de **errores humanos**.
- **Superficie de exposición grande por los sistemas heredados**, extremadamente vulnerables.
- **Necesidad de implantar buenas prácticas**:
  - Estaciones de trabajo y contraseñas compartidas, segmentar redes, acceso remotos controlados y securizados, etc

Oportunidad de aprovechar el impacto mediático de ciberataques contra el sector sanitario.

El **Ransomware ha evidenciado la debilidad de los sistemas de hospitales en todo el mundo** y ha aumentado la conciencia de posibles amenazas contra este sector.

Fuga de Datos de Salud

Más que el problema número uno,
es el atractivo número uno para los ciberdelincuentes.

- **Historiales clínicos**
- **Datos personales**
- **Información financiera**
- **Propiedad intelectual / Investigación**

El **Big Data y el análisis de datos** abren las puertas a una atención de mayor valor, pero implica **procedimientos adecuados en la gestión** de la protección de esos datos

Sistemas heredados - Legacy

Sistemas anticuados, pero que sigue siendo utilizado por la entidad y no se quiere o no se puede reemplazar o actualizar de forma sencilla.

- A menudo, **profundamente implantados** y puede parecer costoso reemplazarlos
- A medida que las amenazas a la seguridad se intensifiquen, la **sustitución de estos sistemas** por las tecnologías modernas se convertirá en **una prioridad** para los proveedores de atención médica.
- **Software fuera de soporte**.
- **Dificultad de parchear sistemas** y estar actualizados para las vulnerabilidades conocidas.

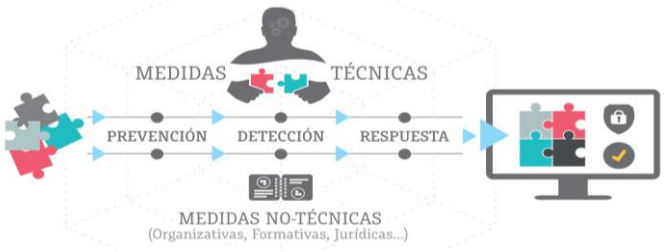
Necesidad de implementar seguridad

- **Los ciudadanos esperan servicios prestados en condiciones de confianza y seguridad**, equivalentes a cuando se acercan a oficinas de la Administración.
- Buena parte de la información y los servicios manejados por las AA.PP. constituyen **activos nacionales estratégicos**.
- Los servicios se prestan en un escenario complejo que **requiere cooperación**.
- La información y los servicios están **sometidos a riesgos** provenientes de acciones malintencionadas o ilícitas, errores o fallos y accidentes o desastres.
- **Los servicios 24x7 -> requieren seguridad 24x7**.

En el paradigma de la resiliencia

Cambio de paradigma:

- → Del **"Doctor NO"** al paradigma de **la resiliencia**
- → De seguridad basada en medidas preventivas a **aceptar un riesgo residual**
- → Aunar las **capacidades de monitorización y vigilancia con a una respuesta eficaz**



objetivos de la seguridad

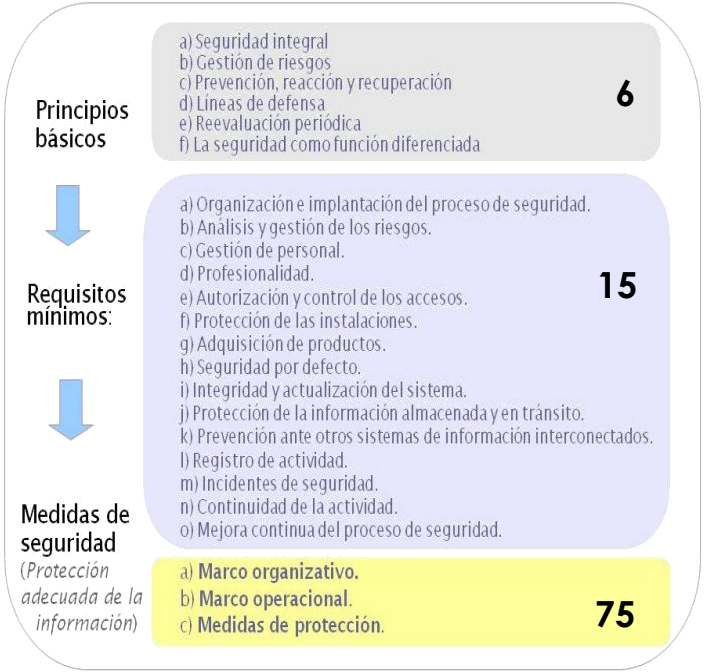
- Mantener la **disponibilidad** de los datos almacenados, así como su disposición a ser compartidos
  - contra la interrupción del servicio
- Mantener la **integridad** de los datos ...
  - contra las manipulaciones
- Mantener la **confidencialidad** de los datos almacenados, procesados y transmitidos
  - contra las filtraciones
- Asegurar la identidad de origen y destino (**autenticidad**)
  - frente a la suplantación o engaño
- Disponer de **trazabilidad**
  - para analizar, entender, perseguir y aprender

Continuidad del Servicio

Para garantizar la continuidad del servicio, hay que ser consciente de que estás sufriendo un ataque, estás siendo comprometido.

- La continuidad del servicio lleva implícito atender a todas **las dimensiones de la seguridad** (confidencialidad, disponibilidad, integridad, trazabilidad y autenticidad) **sin olvidarnos de la privacidad** y las obligaciones que trae consigo la RGPD.
- **Parametrizar la amenaza** para poderla mitigar y garantizar la prestación del servicio en condiciones adecuadas.
- Tener **mecanismos de respuesta oportuna**, la **notificación del incidente sin dilación indebida** es fundamental para asignar recursos y **aplicar planes de contingencia**.

El objetivo principal **es conseguir unos mínimos de seguridad**, y ahí el ENS marca el camino a seguir



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**. (CCN- CERT)
6. El uso de **productos certificados**. Papel del Organismo de Certificación (CCN).
7. La **formación y concienciación**.

Proveer servicios / dar soluciones

AUDITORÍA

- /inés>
- /pilar>
- /clara>
- /rocio>
- /claudia>
- /ana>

DETECCIÓN

- /sat-inet>
- /sat-sara>
- /sat-ics>
- carmen

ANÁLISIS

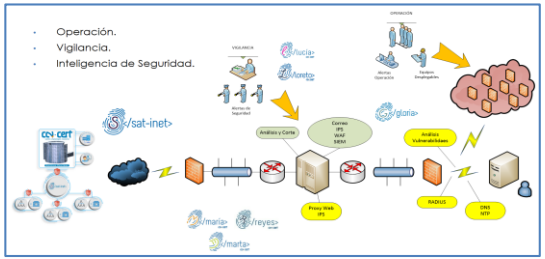
- /gloria>
- /maría>
- /marta>
- /reyes>

INTERCAMBIO

- /lucía>
- /loreto>

FORMACIÓN

- /vanesa>
- ATENEA



ens Esquema Nacional de Seguridad

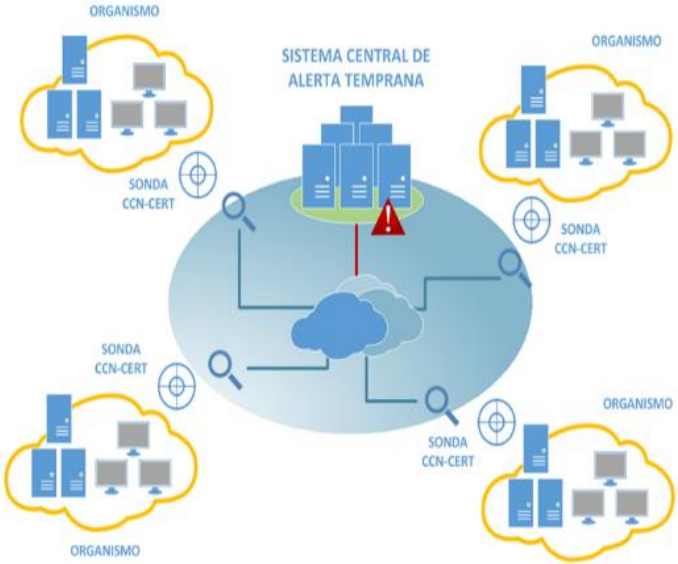
SOC AGE SOC SGNTI

Sistemas de Alerta Temprana (SAT)

La **Detección** abarca todas las actividades de:

- Despliegue de detectores y sistemas de alerta
- Recolección de logs, monitorización de tráfico y vigilancia de la red
- Análisis de malware, ingeniería inversa y análisis forense
- Caracterización técnica de la amenaza y elaboración de inteligencia técnica sobre la misma

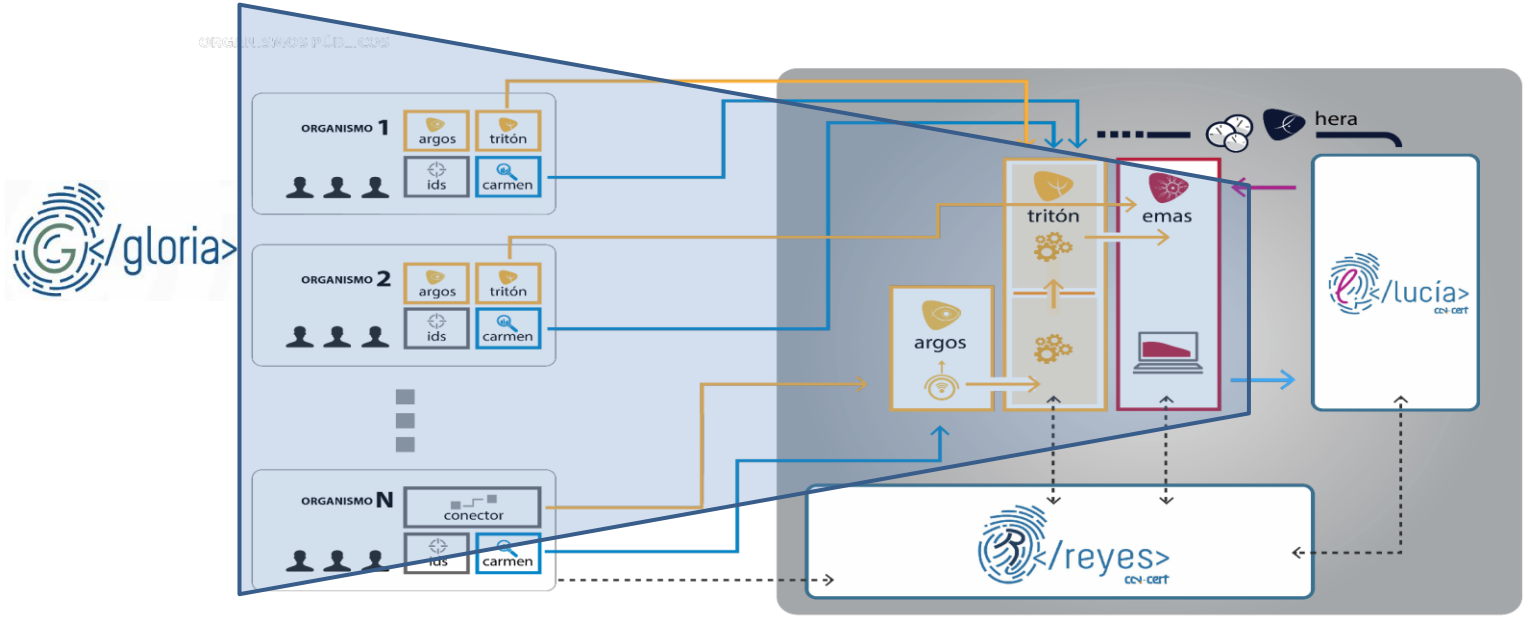
</sat-inet>



- Servicio por suscripción
- Despliegue de sondas.
- **177 Sondas**
- **174 Organismos**
- **+ 100 millones eventos**
- **+ 26.000 incidentes**

Automatización / Integración / Multinivel

La **integración de las capacidades** de "security information and event management" **(SIEM), notificación de incidentes y ciberinteligencia** se hace especialmente necesaria para la mejora de las técnicas de correlación compleja de eventos

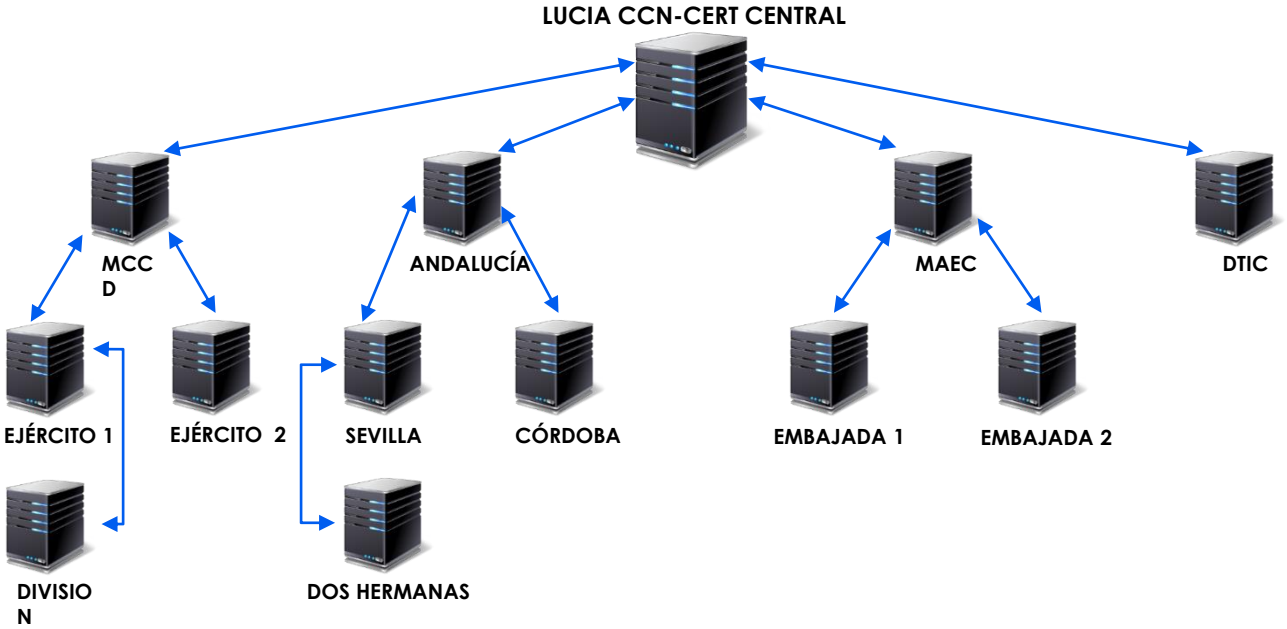


Listado Unificado de Coordinación de Incidentes y Amenazas

- **Cumplir requisitos del ENS** **CCN-STIC 817**
- 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

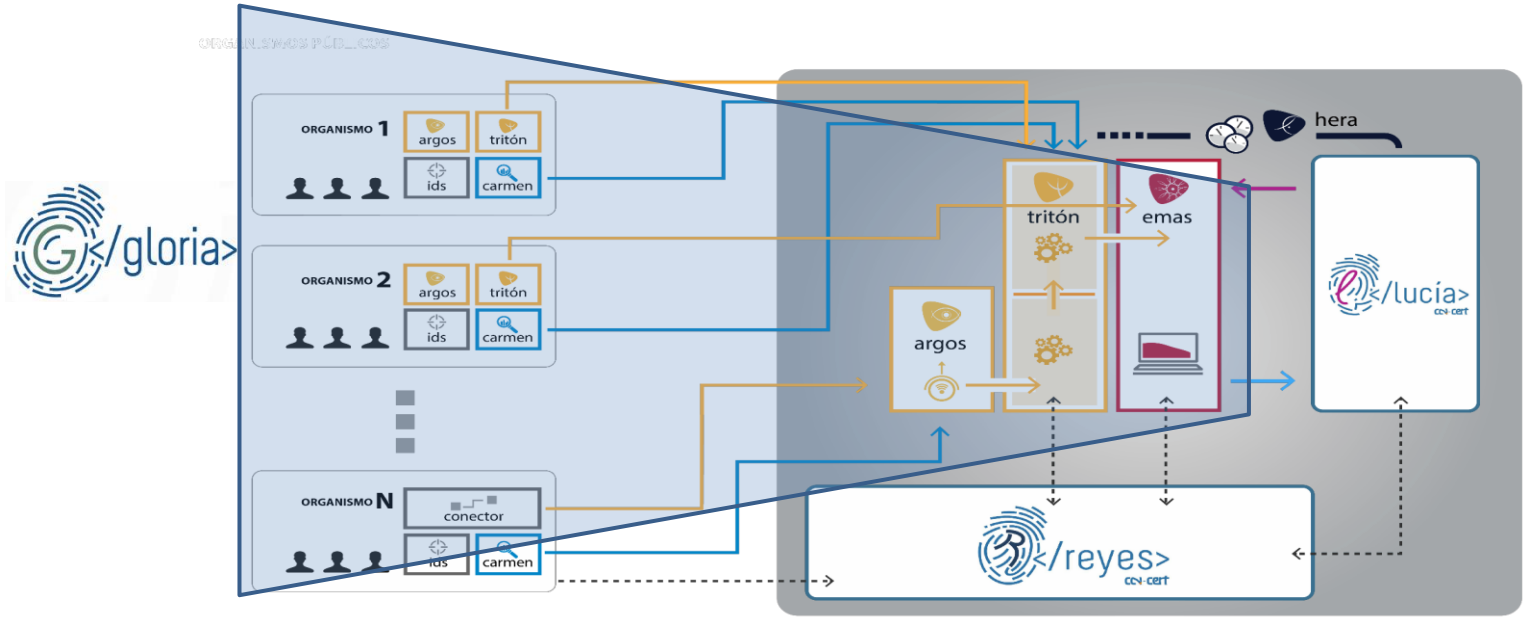
- **Basada en sistema de incidencias Request Tracker (RT)**
- **Incluye extensión para CERT Request Tracker for Incident Response (RT-IR)**

ARQUITECTURA MULTINIVEL

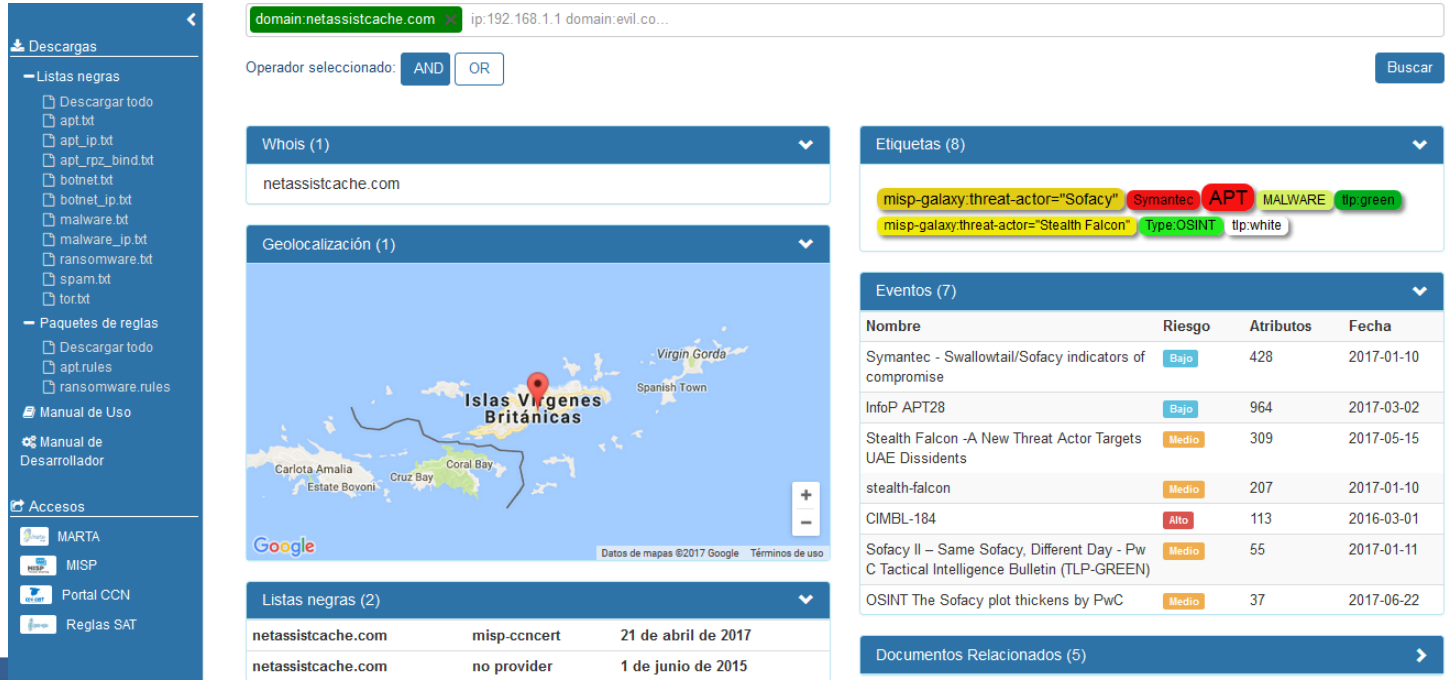


Automatización y reducción tiempos de respuesta

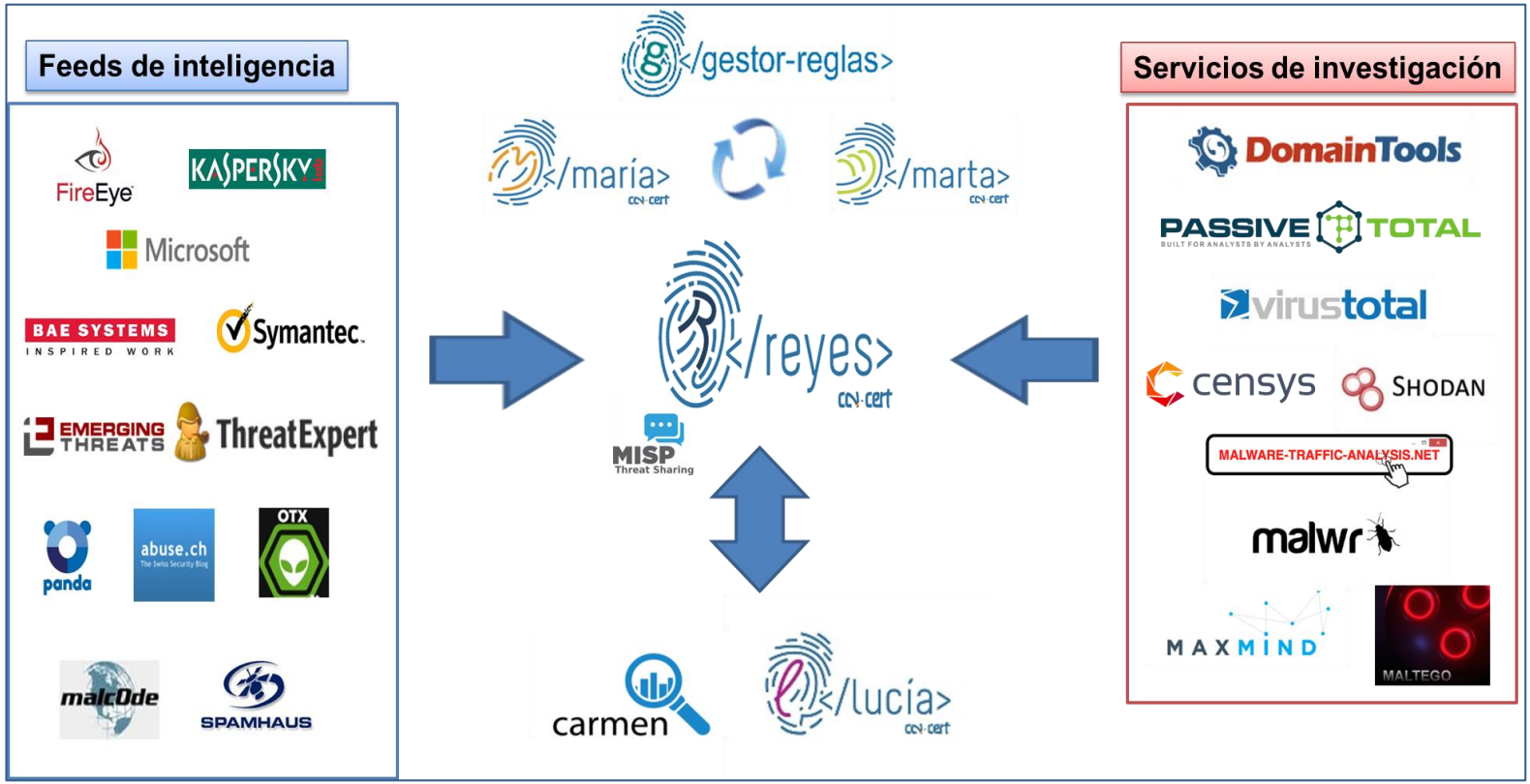
La **integración de las capacidades** de "security information and event management" **(SIEM), notificación de incidentes y ciberinteligencia** se hace especialmente necesaria para la mejora de las técnicas de correlación compleja de eventos



Solución de ciberinteligencia diseñada para almacenar y compartir información relacionada con ciberamenazas e incidentes de seguridad



REYES 2.0


Feeds de inteligencia
FireEye
KASPERSKY
Microsoft
BAE SYSTEMS
INSPIRED WORK
Symantec.
EMERGING THREATS
ThreatExpert
panda
abuse.ch
The Swiss Security Blog
OTX
malcOde
SPAMHAUS
</gestor-reglas>
</maría>
CCN-CERT
</marta>
CCN-CERT
</reyes>
CCN-CERT
MISP
Threat Sharing
carmen
</lucía>
CCN-CERT
Servicios de investigación
DomainTools
PASSIVE TOTAL
BUILT FOR ANALYSTS BY ANALYSTS
virustotal
censys
SHODAN
MALWARE-TRAFFIC-ANALYSIS.NET
malwr
MAXMIND
MALTEGO

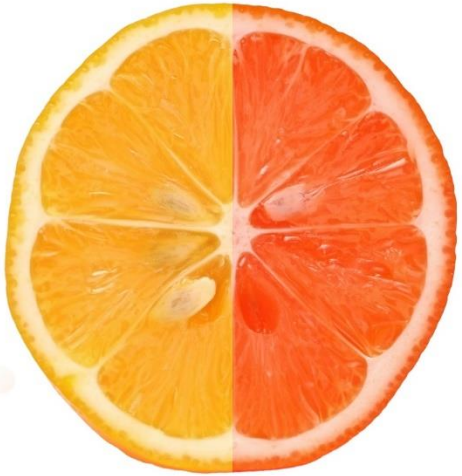
Defensa de la red industrial

OT

Impacto en producción. Daños a personas/medio ambiente

Tolerancia fallos esencial

Difícil por parada
Dependencia de fabricantes

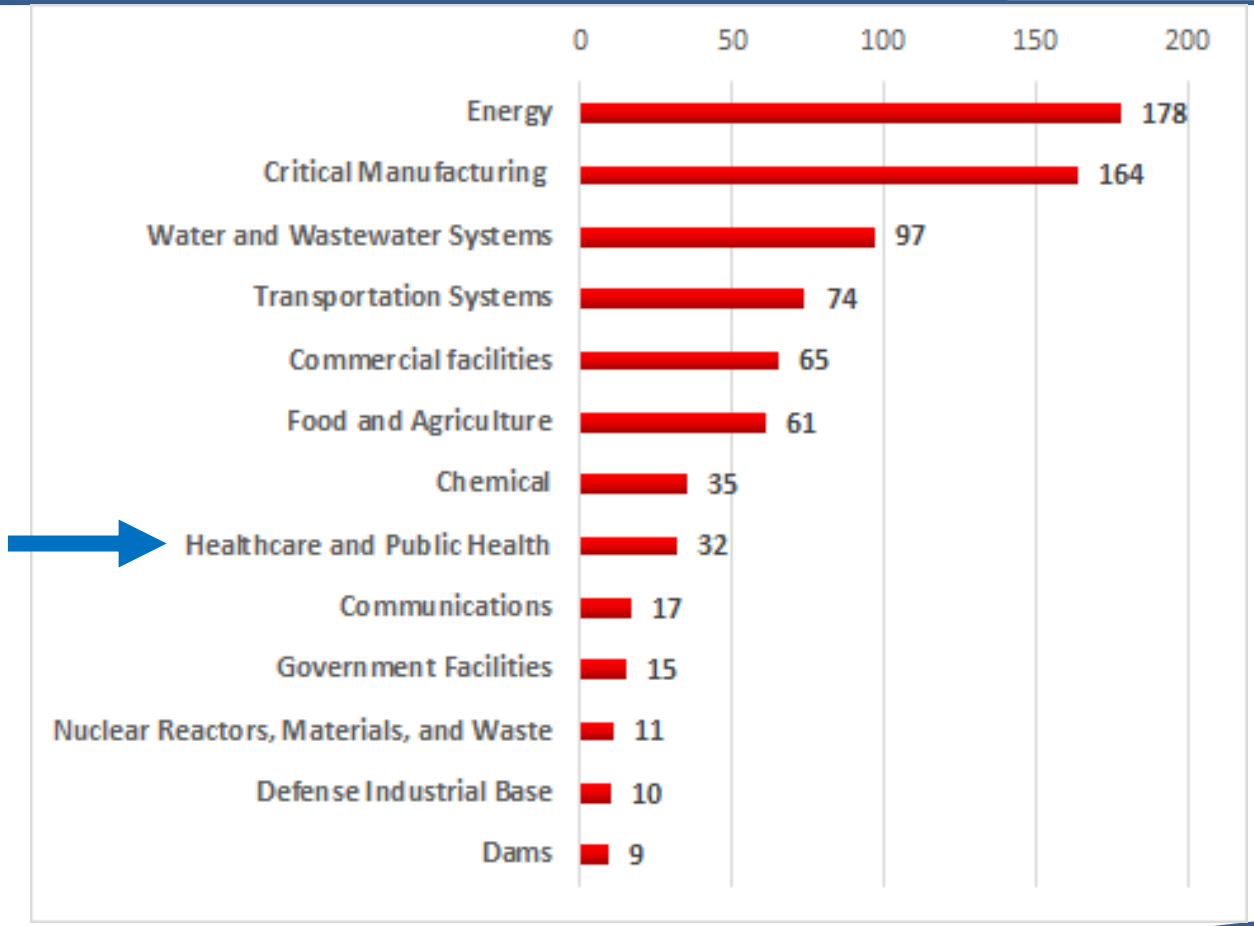


IT

Pérdida datos
Exfiltración

Reinicio/backup

Actualizaciones semi/automáticas



Fuente: Threat Landscape for Industrial Automation Systems in H2 2017. Kaspersky Lab ICS-CERT

Objetivos Atacante ICS

Sistema Climatización (HVAC)

Sistema Gestión de Edificios (BMS)

Extinción de incendios

Control de accesos

Escaleras Mecánicas / Ascensores

Grupo Electrógeno

Datos Médicos

Sistema Alumbrado

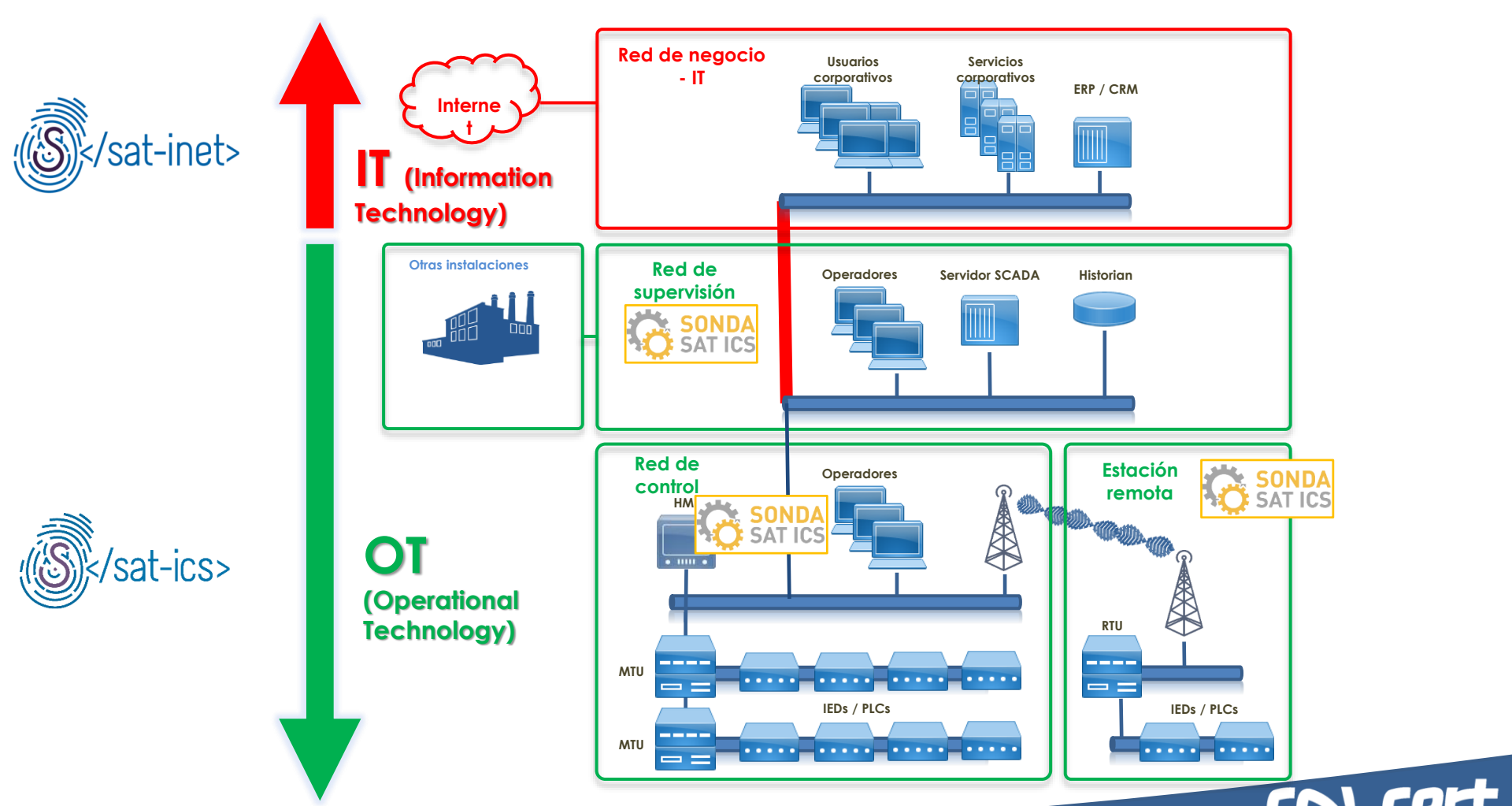
Sistemas ICS

Retos ICS

- Sistemas no homogéneos. Múltiples fabricantes
- Sistemas antiguos > 20 años
- Multitud de protocolos industriales
- Conexiones remotas a equipos médicos
- Mala segmentación de redes IT/OT
- Detección de ataques cadena suministro
- Contraseñas por defecto
- Productos con vulnerabilidades
- Falta de actualizaciones de seguridad

</sat-ics>

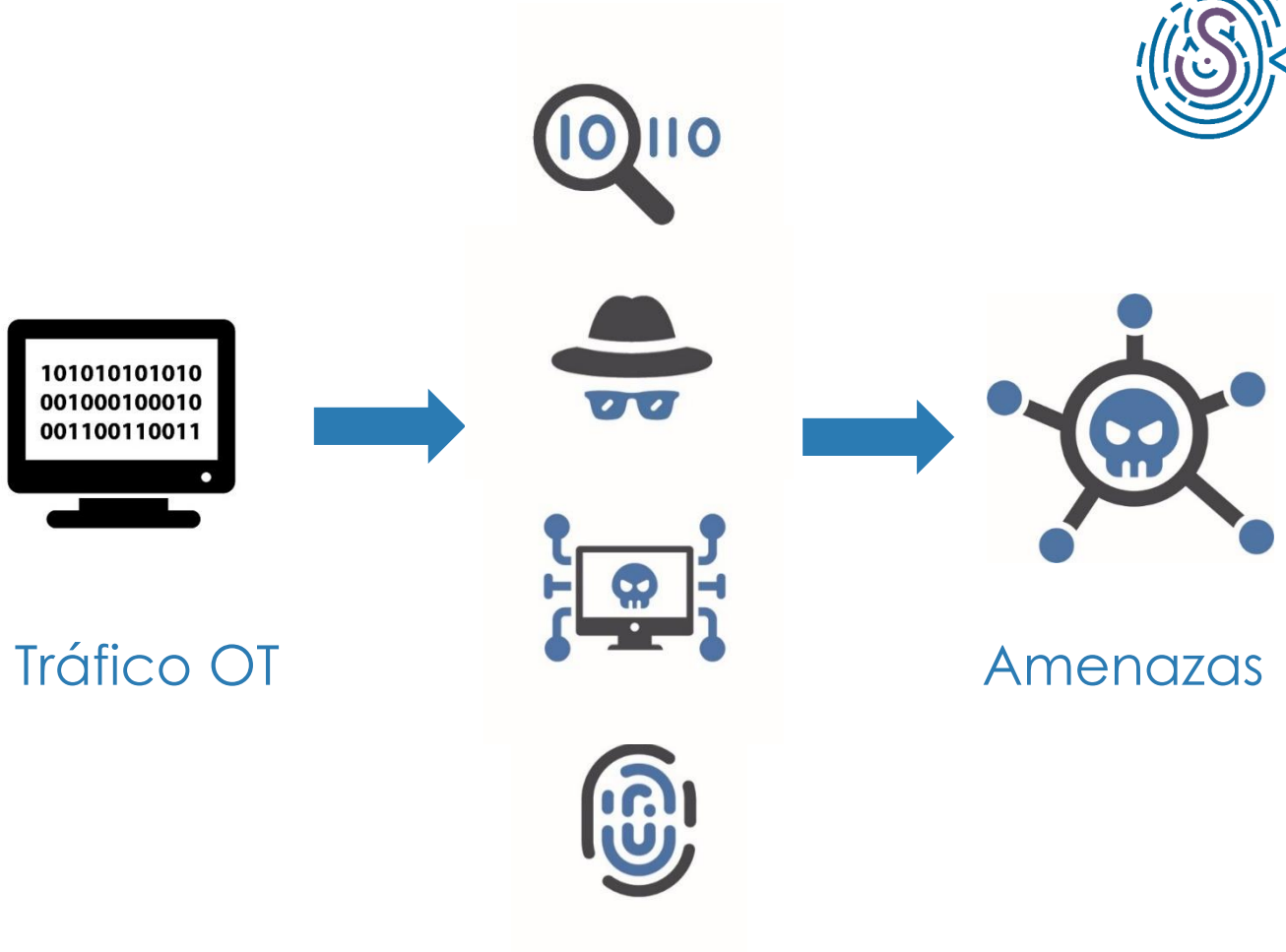
- Configuración adaptada al organismo
  - La sonda SAT ICS permite monitorizar la actividad en los sistemas de control industrial y SCADA de los Organismos
- No interfiere en el proceso industrial
- Detección y notificación de incidentes
  - Detección de acciones anómalas contra los procesos industriales basadas en el análisis del contexto
- Apoyo en la resolución

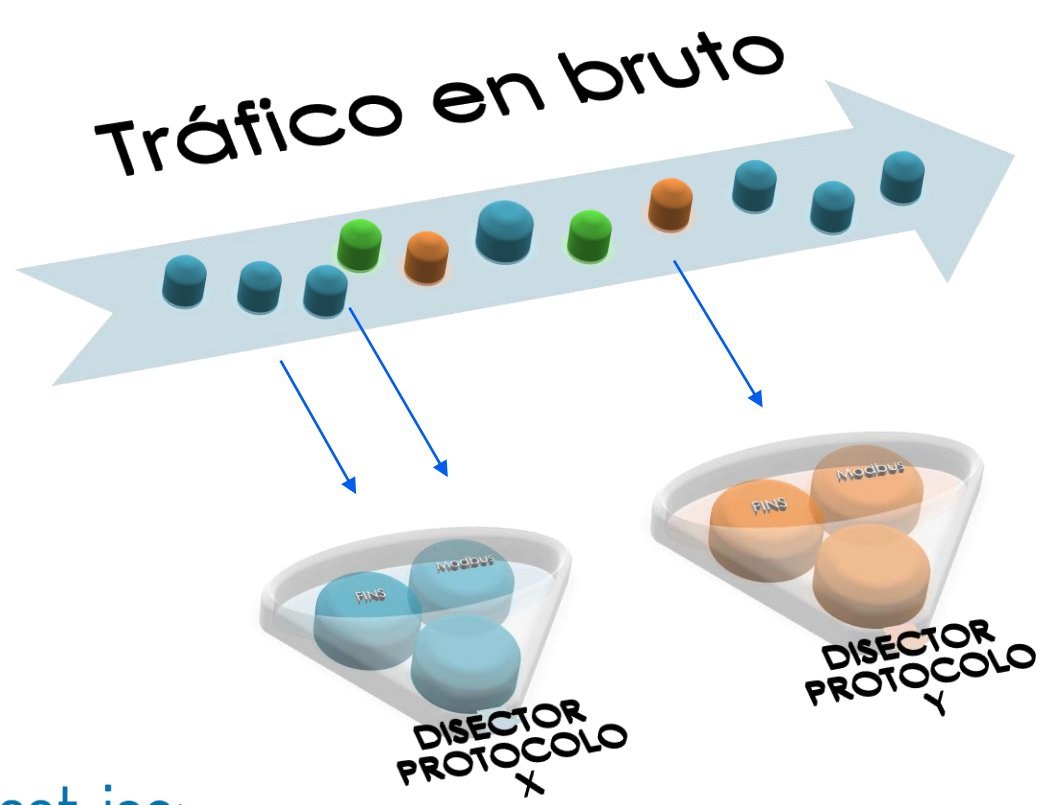

Internet
IT (Information Technology)
Red de negocio - IT
Usuarios corporativos
Servicios corporativos
ERP / CRM
Otras instalaciones
Red de supervisión
SONDA SAT ICS
Operadores
Servidor SCADA
Historian
Red de control
HMI
SONDA SAT ICS
Operadores
MTU
IEDs / PLCs
MTU
OT (Operational Technology)
Estación remota
SONDA SAT ICS
RTU
IEDs / PLCs

Tráfico OT

Sonda

Amenazas


101010101010
001000100010
001100110011
Tráfico OT
Amenazas



EthernetIP

60870-5-104 (IEC104)

Modbus

DNP3

S7 Com

FINS

</sat-ics>

¿Cómo acceder al servicio?

1

Sistema de Alerta Temprana

Sistemas de Control Industrial

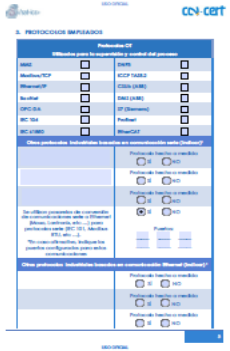
</sat-ics>

Envía un correo a

sat-ics@ccn-cert.cni.es

2

Cuestionario de adhesión



3

Adaptación a tu sistema

4

Instalación de la sonda

</sat-ics>

NECESIDAD DE PERSONAL EXTERNO

59 retos distinta dificultad
6.408 puntos

¿Qué es?

- **ATENEA** es una plataforma de desafíos de **seguridad informática**
- Diversa temática: ciberseguridad básica, criptografía y esteganografía, exploiting, reversing, análisis de tráfico, forense, hacking web…

Objetivos

- **Involucrar** a todo aquél con experiencia en seguridad TIC.
- **Concienciar** al personal TIC sobre los riesgos de la seguridad informática.
- Mostrar a las personas con menos experiencia en la seguridad TIC que **los retos son divertidos** y que la seguridad no es una ciencia secreta que nunca entenderán.

¿Quién puede registrarse?

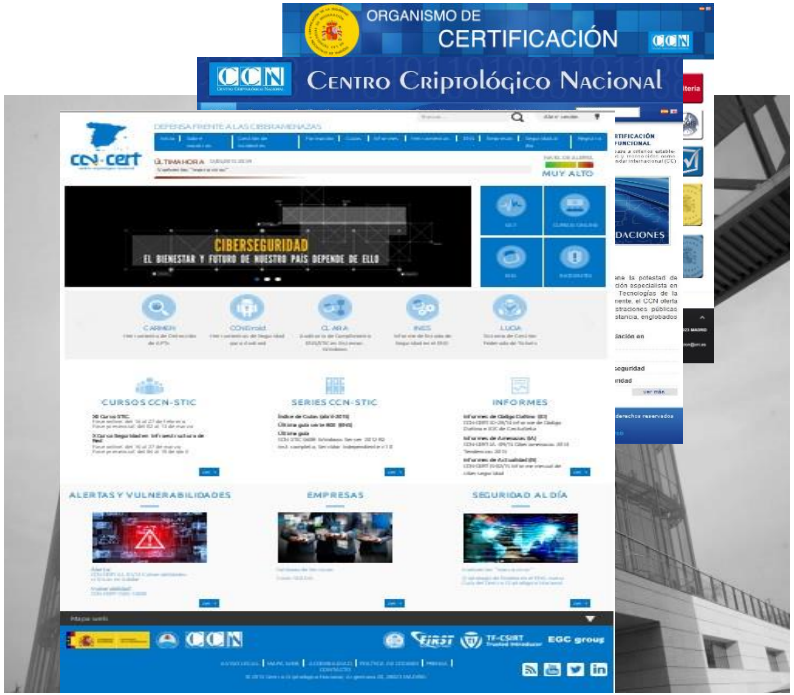
Cualquiera, con una cuenta de correo electrónico.

Soporte limitado.

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

INTERCAMBIAR = CONFIANZA

- **E-Mails**
  - ccn@cni.es
  - info@ccn-cert.cni.es
  - Sat-inet@ccn-cert.cni.es
  - Sat-ics@ccn-cert.cni.es
  - lucia@ccn-cert.cni.es
  - acreditacion.ccn@cni.es
  - organismo.certificacion@cni.es
- **Websites**
  - www.ccn.cni.es
  - www.ccn-cert.cni.es
  - www.oc.ccn.cni.es



Gracias