vSOC

Centro de Operaciones de Ciberseguridad

centro criptológico nacional

vSOC: respuesta a las necesidades prioritarias

Objetivos vSOC

> **“Mejorar las capacidades de despliegue, actuación y protección de las entidades.”**

- Dar seguridad a ayuntamientos y diputaciones
- Más información de ataques
- Mayor visibilidad sobre incidentes
- Mayor capacidad de correlación de ataques
- Mejor capacidad de respuesta

Implementación

Centro de Operaciones de Ciberseguridad

vSOC Inicial

- Notificación de incidentes.
- Avisos y alertas.

vSOC

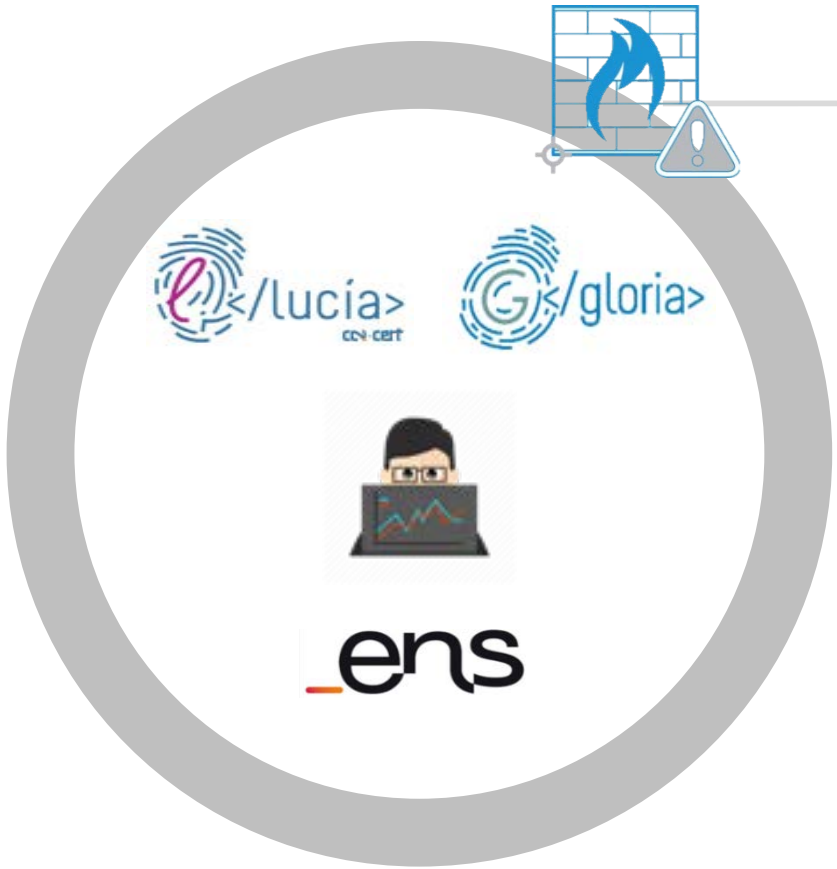
- Actuación sobre el perímetro ante incidentes.
- Capacidad forense e investigación remota.
- Control de equipos infectados.

vSOC Avanzado

- Actuaciones / inspecciones técnicas.
- Evaluación y conocimiento del estado de seguridad.
- Valoración de la exposición.

vSOC Inicial

- Notificación de incidentes.
- Avisos y alertas.



Seguridad perimetral con administración centralizada y capacidad de detección de anomalías (sondas)

Gestión Eventos Seguridad (SIEM)

Compartir Reglas (ciberinteligencia)

Notificación / Federación (LUCIA)

Adecuación al ENS (apoyo normativo)

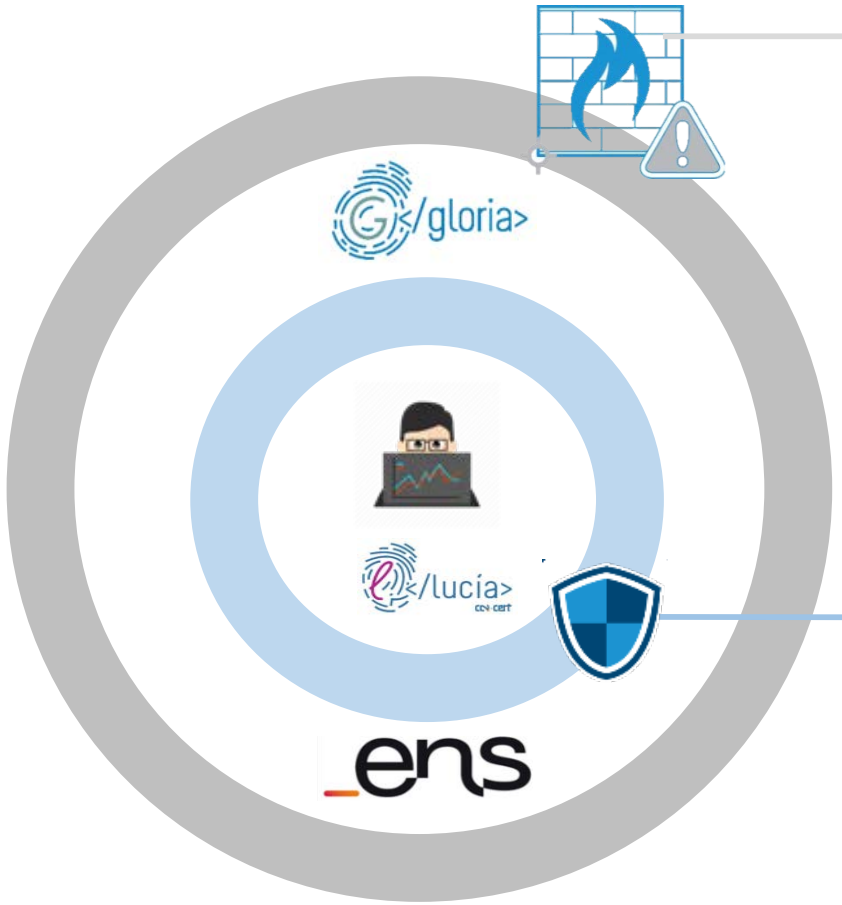
Centro de Operaciones de Ciberseguridad

CCN centro criptológico nacional

vSOC

- Actuación sobre el perímetro ante incidentes.
- Capacidad forense e investigación remota.
- Control de equipos infectados.

Centro de Operaciones de Ciberseguridad



Seguridad perimetral con administración centralizada y capacidad de detección de anomalías (sondas)

Apoyo configuración anti DDoS

Gestión Eventos Seguridad
Compartir Reglas

Notificación / Federación (LUCIA)

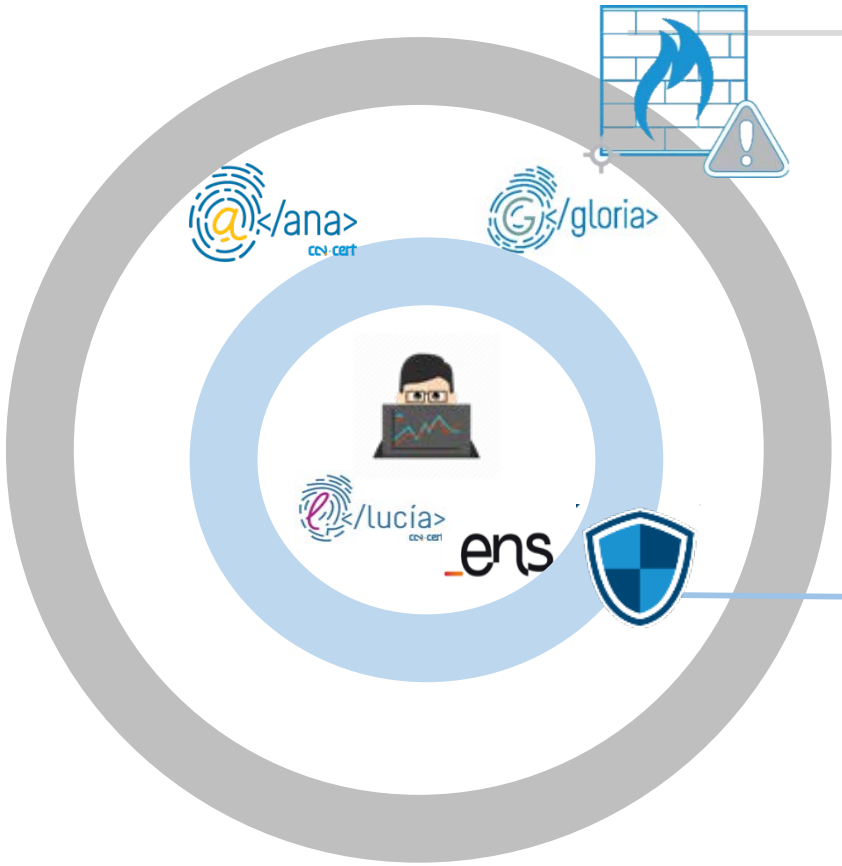
Seguridad Punto Final (Endpoint)

Capacidad forense, remediación remota y reglas de comportamiento

CCN centro criptológico nacional

vSOC Avanzado

- Actuaciones / inspecciones técnicas.
- Evaluación y conocimiento del estado de seguridad.
- Valoración de la exposición.



Seguridad perimetral con administración centralizada y capacidad de detección de anomalías (sondas)

Evaluación Continua (ANA)

Gestión Eventos Seguridad Compartir Reglas

Notificación / Federación (LUCIA)

Seguridad Punto Final (Endpoint)

Capacidad forense, remediación remota y reglas de comportamiento

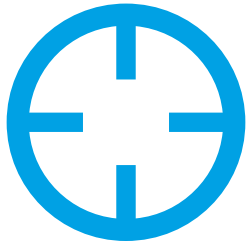
Centro de Operaciones de Ciberseguridad

CCN centro criptológico nacional

Soluciones de Seguridad

CCN
centro criptológico nacional

Seguridad perimetral



Administración centralizada

Posibilidad de actuar ante ataques tipo *Wannacry*

Costes adaptados a los recursos de la entidad

Ampliar navegación por categorías y filtrado web

Mejora de la seguridad en las Entidades Locales

Gestión directa del tráfico

Reglas IDS

Las **detecciones mediante reglas** pueden permitir abrir una ventana en la búsqueda de amenazas tipo APT o código dañino desconocido en los equipos de una entidad, otorgando al vSOC las capacidades de **prevención y detección.**

- ✓ Alerta temprana y adscripción a comunidad CCN-CERT.
- ✓ Adaptaciones de las sondas utilizadas para SAT-INET.
- ✓ Ciberinteligencia (listas blancas).
- ✓ Distribución de reglas (gestor de reglas).
- ✓ Gestión de eventos de seguridad por SIEM vSOC.
- ✓ Transferencia de conocimiento, capacitación y adaptaciones por CCN-CERT.

Valor añadido: Integración con la capacidad de alerta temprana del CCN-CERT.

SIEM

Funcionamiento

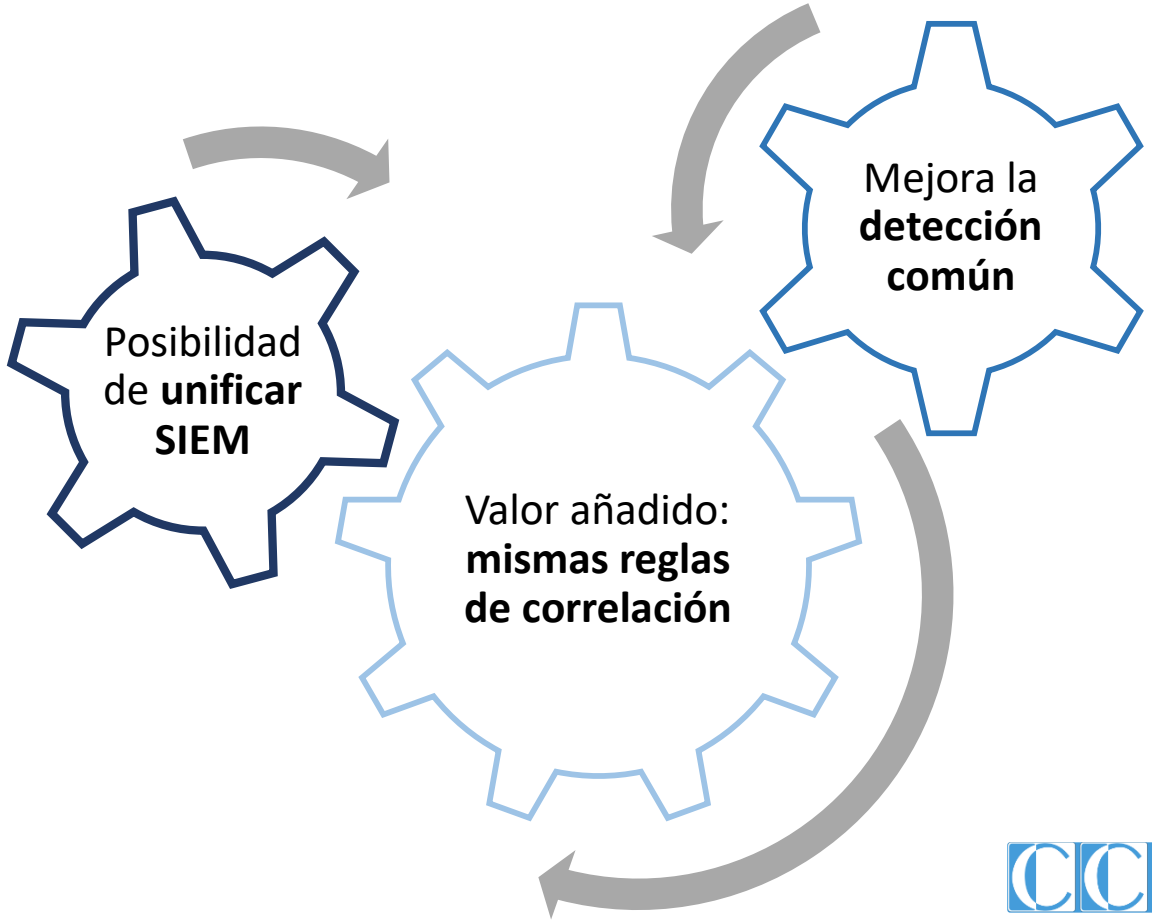
- Intercambio de incidentes a través de **LUCÍA**
- Exportación e importación de eventos seguridad
- Tratamiento de **reglas conforme a estándares**
- **Exportación** de reglas en formato estándar

Flujo de incidentes y métricas de resolución

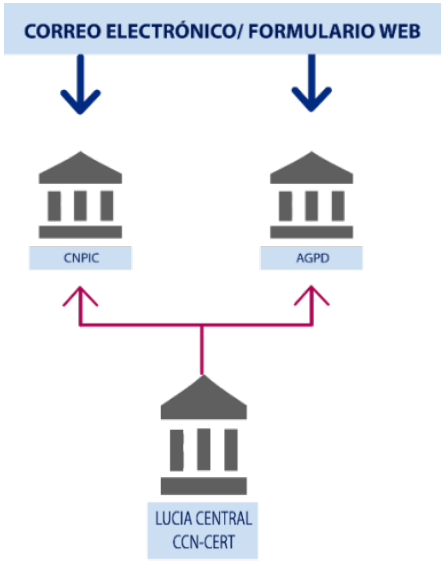
Adaptación de la Guía CCN-STIC 817

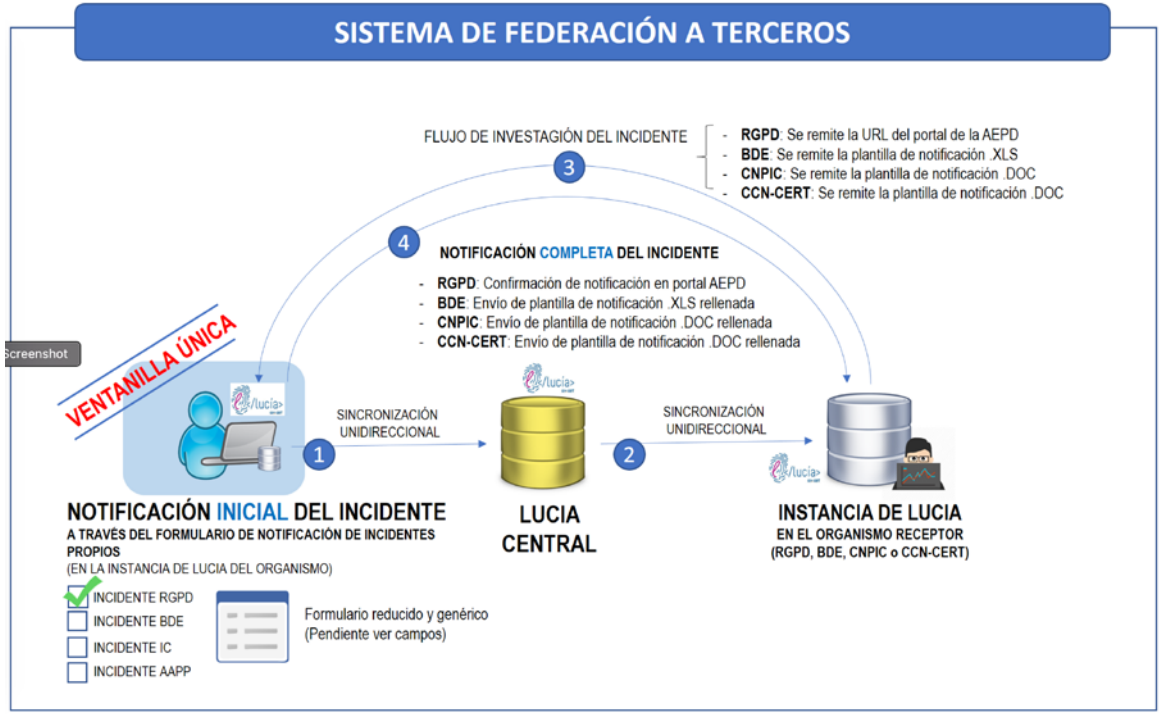
Automatización de notificaciones de nivel 1

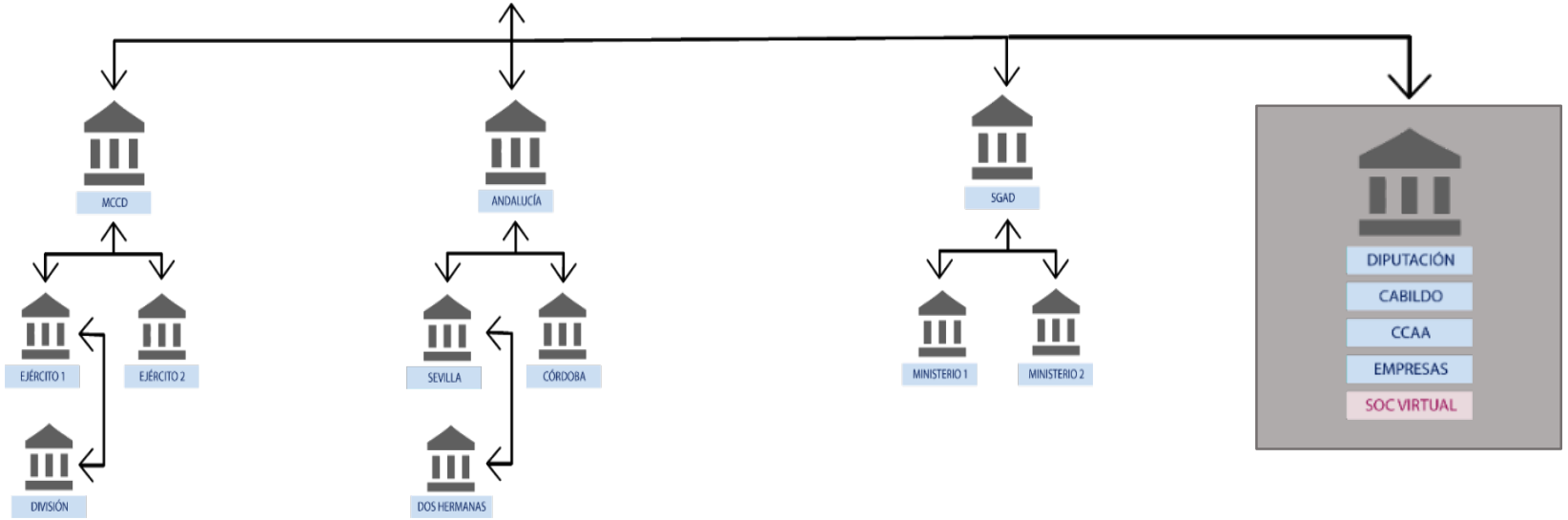
Beneficios



Notificación







Punto final

Detección de anomalías de comportamiento basadas en reglas y en eventos generados por las aplicaciones y acciones en los equipos finales.

Capacidades

- ✓ Creación de reglas por comportamiento.
- ✓ Capacidad forense en el tiempo (un año) y en remoto.
- ✓ Posibilidad de aislar maquinas (*ransomware*).
- ✓ Reglas comunes y administración centralizada.
- ✓ Fuente de información añadida para el SIEM (correlación).
- ✓ Indicadores de compromiso (IOC) proporcionados por *feeds*.
- ✓ Generación de inventario de software y versionado de equipos.
- ✓ Gestión de catálogo de activos.

Resultados

- ↑ **Detección**
- ↑ **Reacción**
- ↑ **Seguridad**

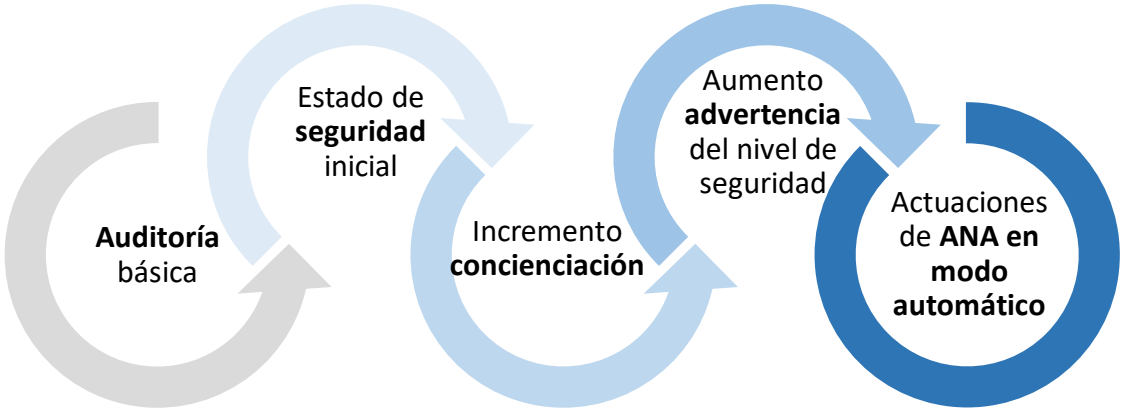
Auditoría continua

Gestión de seguridad

Necesidad de evaluación continua:

*Capacidad de gestionar y medir de manera continua la **evolución de activos** auditados respectos a niveles de seguridad y riesgos definido, posibilitando con **la priorización de recursos disponibles** la capacidad de **reacción y mitigación** ante posibles defectos de configuración y vulnerabilidades detectadas.*

ANA en los vSOC



Apoyo normativo

Los **vSOC** podrán contar con servicio de apoyo a las entidades en su marco normativo y de adaptación al Esquema Nacional de Seguridad (ENS).

En función de las necesidades, este apoyo servirá de refuerzo al servicio existente o bien se prestará a aquellas entidades que no dispongan del mismo.

Soporte técnico

Asesoramiento legal

Apoyo a las entidades:

- ✓ Implementación de medidas de seguridad.
- ✓ Orientación en la declaración de cumplimiento.
- ✓ Superación de auditorías.
- ✓ Consultoría sobre la aplicación del ENS.

ens
Consejo de Certificación
del Esquema Nacional de
Seguridad

CCN
centro criptológico nacional

Comunidad CCN-CERT

Muchas Gracias

E-mails

info@ccn-cert.cni.es

ccn@cni.es

sondas@ccn-cert.cni.es

redsara@ccn-cert.cni.es

organismo.certificacion@cni.es

Páginas web:

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es