vSOC
Nuevo Modelo Gestión de Incidentes

I Encuentro del ENS.
Tendencias y Políticas de Seguridad

Se duplican incidentes ciberseguridad en las grandes empresas estratégicas

EFE 16/11/2017 (15:54)

El 53% de las pymes declara haber sufri

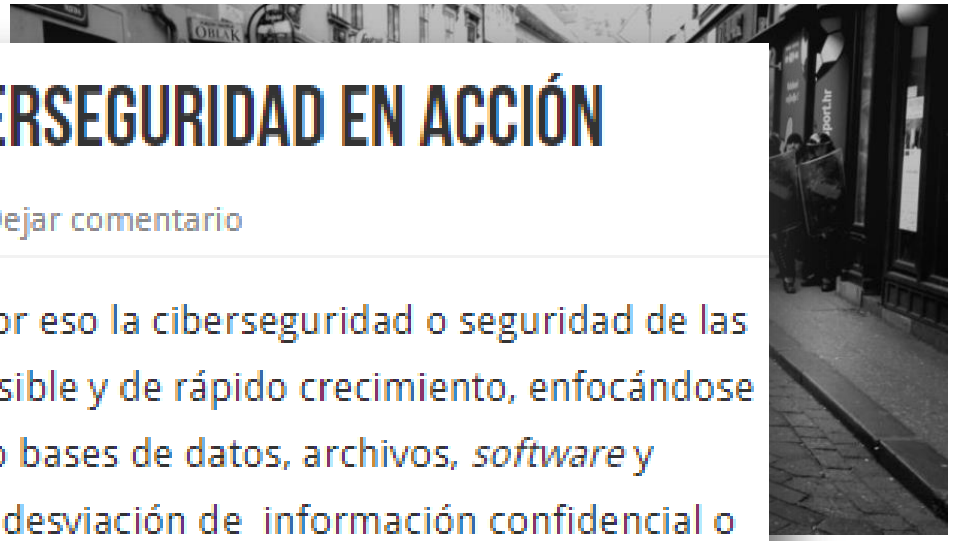
Un 53% d
SMB Cyb
empleado

EFEEMPRES

US au
hacke

31 charg

By Iain Thor



CIBERATAQUES CADA 39 SEGUNDOS: LA CIBERSEGURIDAD EN ACCIÓN

Adriana Bianco 29/09/2018 BLOGS, Tecnologías Dejar comentario

Cada 39 segundos se produce un ciberataque en el mundo, por eso la ciberseguridad o seguridad de las tecnología de la información, se ha convertido en un área sensible y de rápido crecimiento, enfocándose en aspectos de la computación y en las redes, comprendiendo bases de datos, archivos, *software* y *hardware*, y todo sistema que se preste a riesgos de ataque o desviación de información confidencial o privilegiada.

La adaptación a las nuevas amenazas implica **MEJORAR LAS CAPACIDADES DE VIGILANCIA** y diseñar respuestas cada vez más eficaces frente a los ataques

¡¡ Ciberseguridad es generar Confianza !!

Mejora Continua

Determinación de la Superficie de Exposición

Reducción del Tiempo de Respuesta

CCN
centro criptológico nacional

Procedimiento de Mejora Continua

Detrás de esta aproximación está que los organismos **IMPLEMENTEN SEGURIDAD** y que no se limiten a realizar un análisis de riesgos y a documentar sus procedimientos

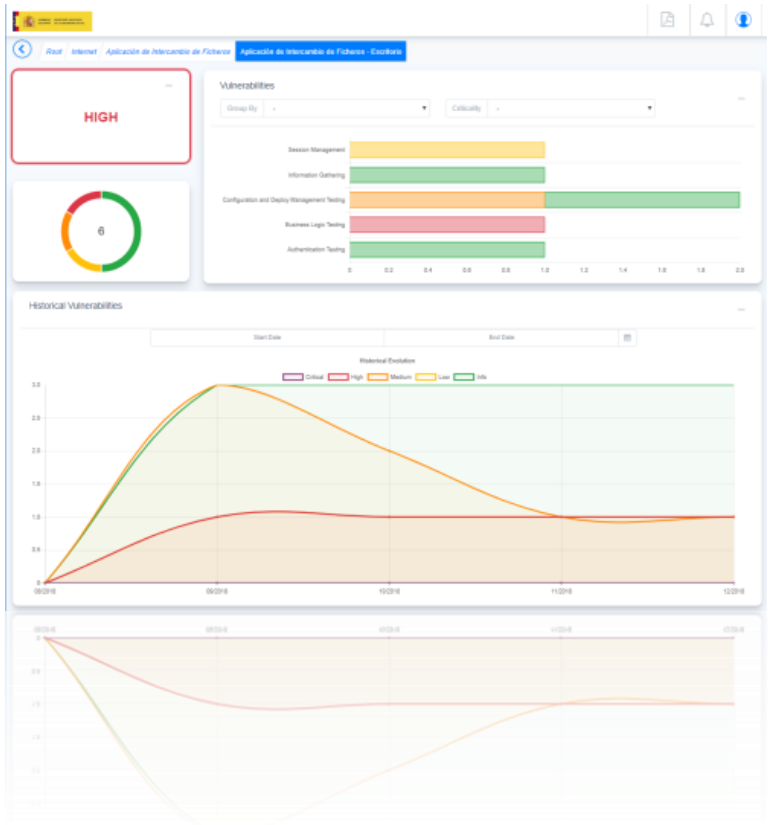
Se buscan los siguientes objetivos…

- Educación y **buenas prácticas**.
- **Planificación auditorías de seguridad** desde el primer momento.
- **Anticiparse** y buscar soluciones (proactividad).
- Analizar **medidas compensatorias**.
- Cumplimiento **a corto, medio y largo plazo**.
- **Gestión de expectativas** asociada a la adopción de compromisos.

Se busca establecer un procedimiento de **MEJORA CONTINUA DE LOS NIVELES DE SEGURIDAD**, a través de una adaptación al medio y establecimiento de prioridades por parte de la entidad.

Determinación de la Superficie de Exposición

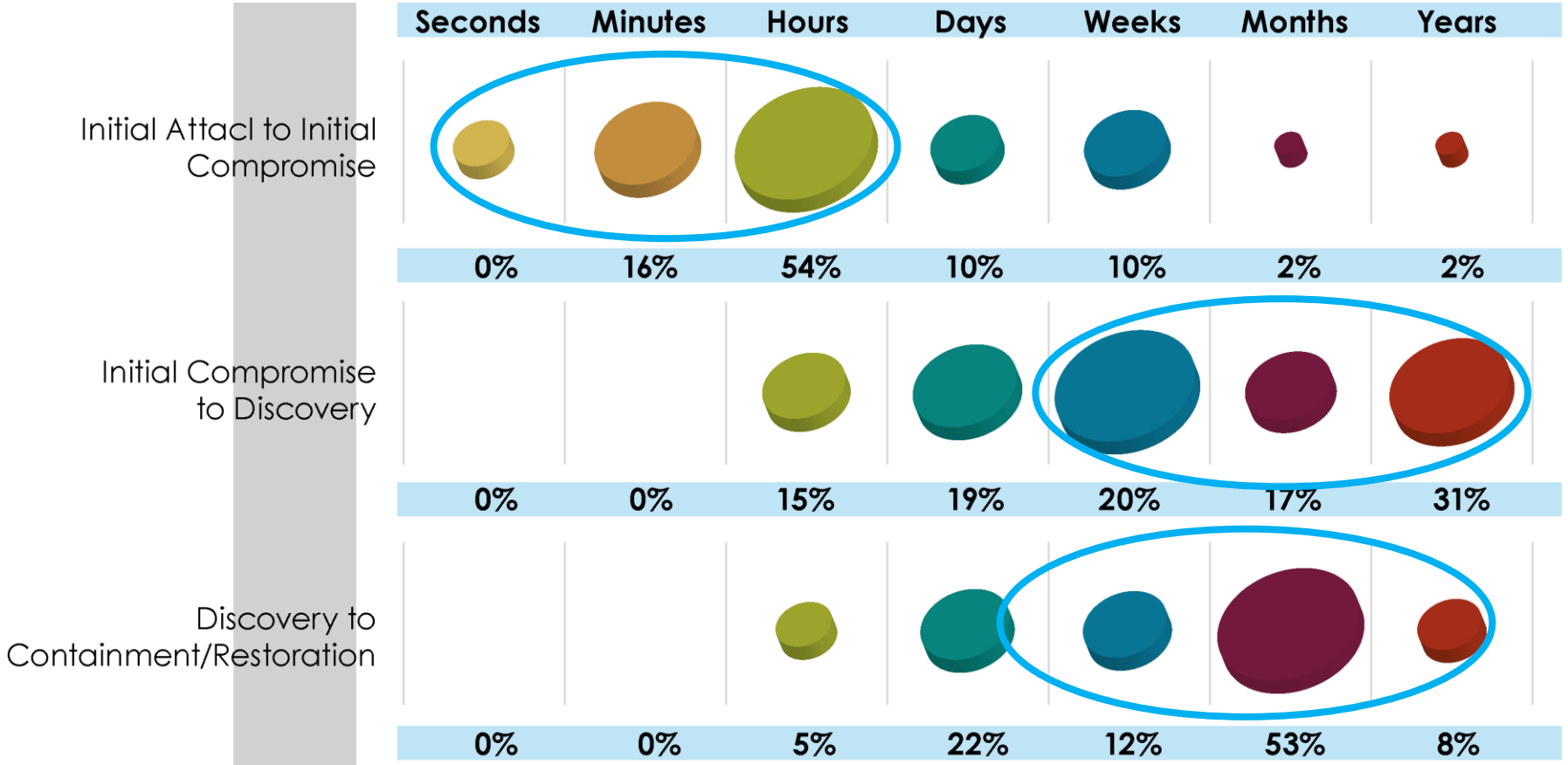
El objetivo es **GESTIONAR Y MEDIR DE MANERA CONTINUA LA EVOLUCIÓN DE ACTIVOS** auditados respecto a niveles de seguridad y riesgo definidos, posibilitando con la **priorización de recursos** disponibles la **capacidad de reacción y mitigación** ante posibles defectos de configuración y vulnerabilidades detectadas.



Capacidad de medir la SEGURIDAD de exposición de la Organización

Ayudar a reducir la exposición de **VULNERABILIDADES** al exterior de la Entidad

Reducción de Tiempos de Respuesta



Las **víctimas** de ciberataques **siguen sufriendo ataques** a lo largo del tiempo

CCN centro criptológico nacional

SOC: respuesta a las necesidades prioritarias

Objetivos vSOC

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

- Dar seguridad a las entidades
- Más información de ataques
- Mayor visibilidad sobre incidentes
- Mayor capacidad de correlación de ataques
- Mejor capacidad de respuesta

Gobernanza de la Ciberseguridad

Centro de Operaciones de Ciberseguridad

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.

1 Asesoramiento normativo

2 Soporte técnico

CCN centro criptológico nacional

Oficina de Ciberseguridad

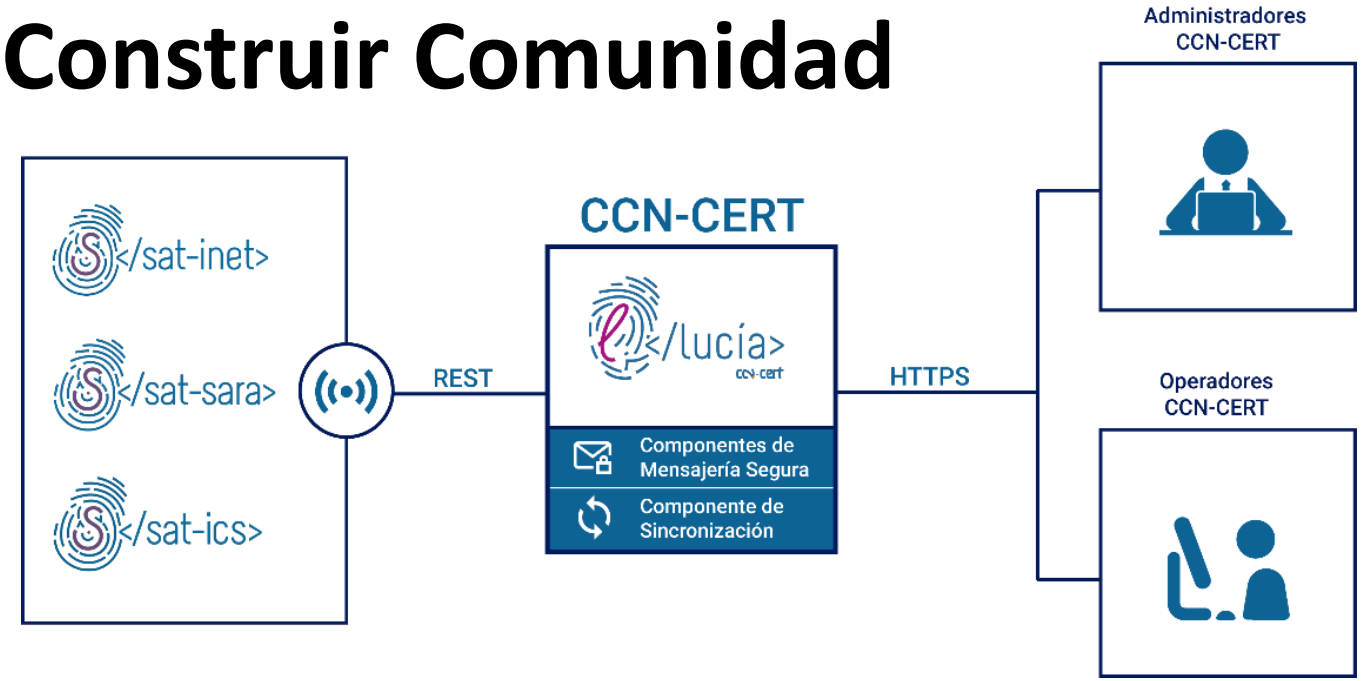
Centro de Operaciones de Ciberseguridad

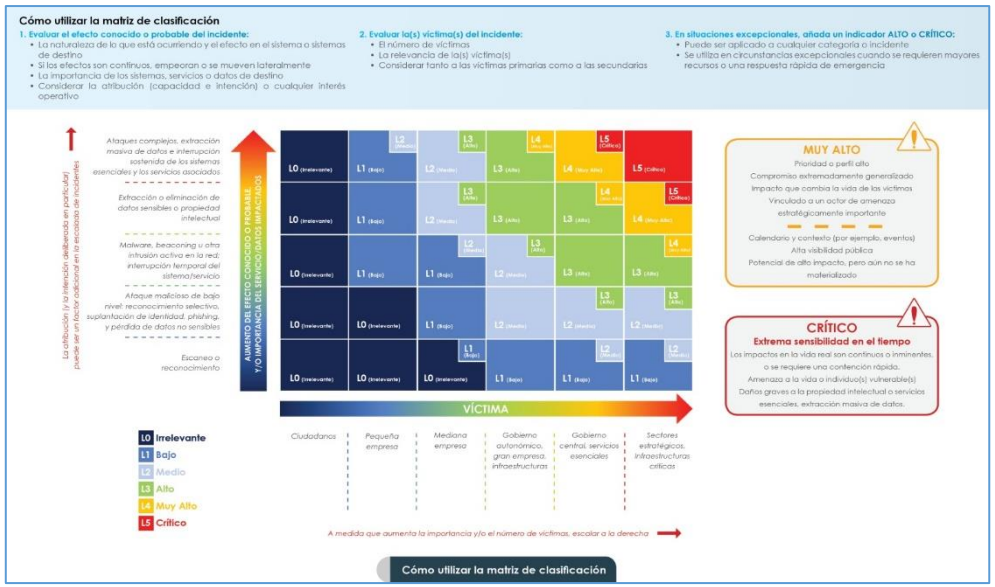
Apoyo en la adopción de **PROCEDIMIENTOS Y MEDIDAS TÉCNICAS DE SEGURIDAD**: **recomendaciones**, **implementación**, **configuración** y **mantenimiento**

Recomendaciones | Implementación | Configuración | Mantenimiento

CCN centro criptológico nacional

Construir Comunidad





Ventajas

- Incremento notificación de incidentes
- Cuantificar la notificación de VSOC

Más información de ataques

Mayor visibilidad sobre incidentes

centro criptológico nacional

Soluciones de Seguridad

CCN
centro criptológico nacional

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.

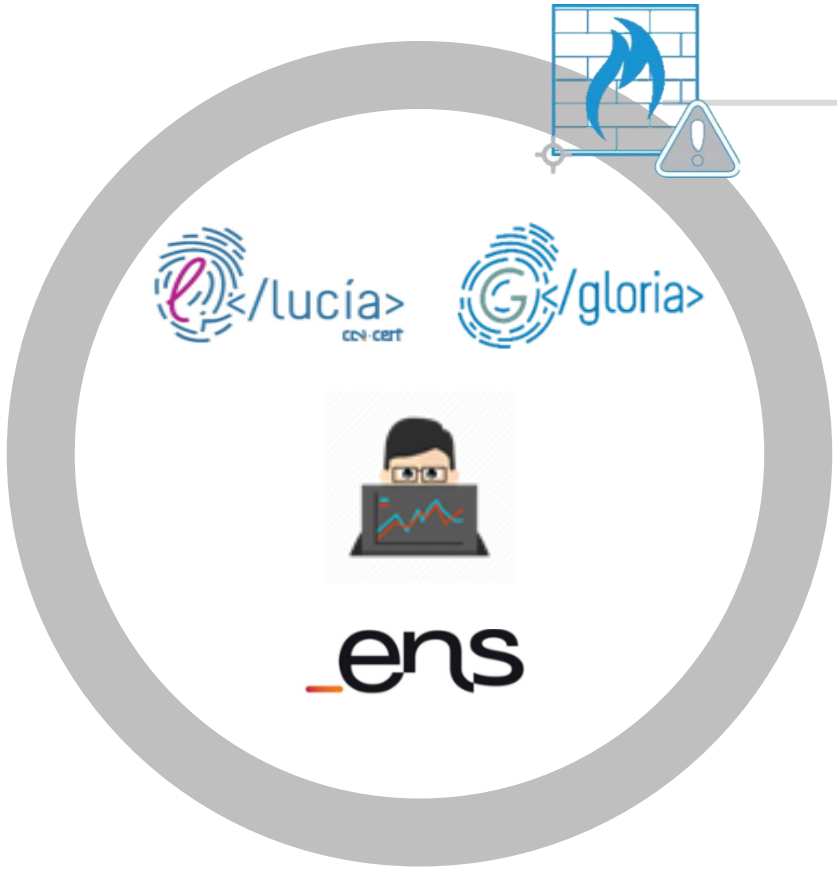
vSOC Avanzado

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

CCN centro criptológico nacional

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)

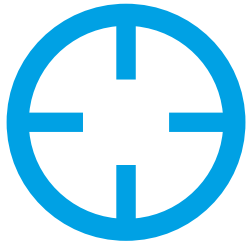
Notificación / Federación (LUCIA)

Adecuación al ENS (apoyo normativo)

Centro de Operaciones de Ciberseguridad

CCN centro criptológico nacional

Seguridad Perimetral



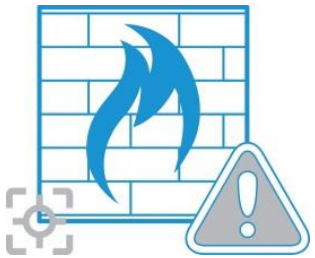
Administración centralizada

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

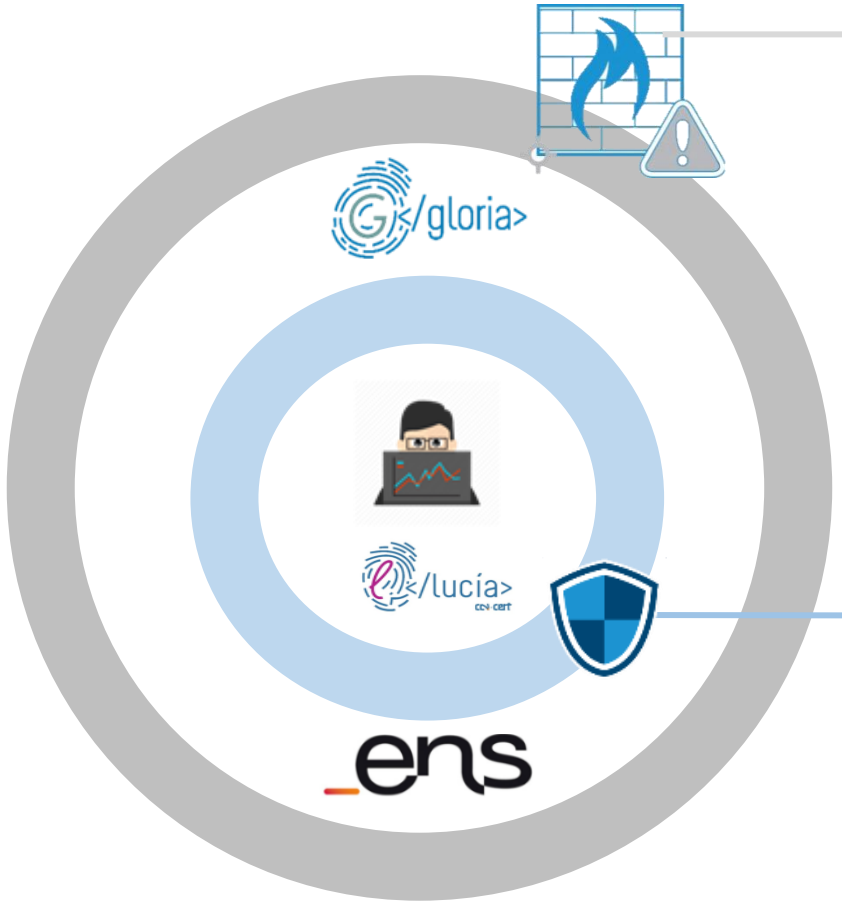
Adaptación de la Guía CCN-STIC 817

Automatización de notificaciones de nivel 1

Beneficios

vSOC

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



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

Centro de Operaciones de Ciberseguridad

CCN centro criptológico nacional

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.

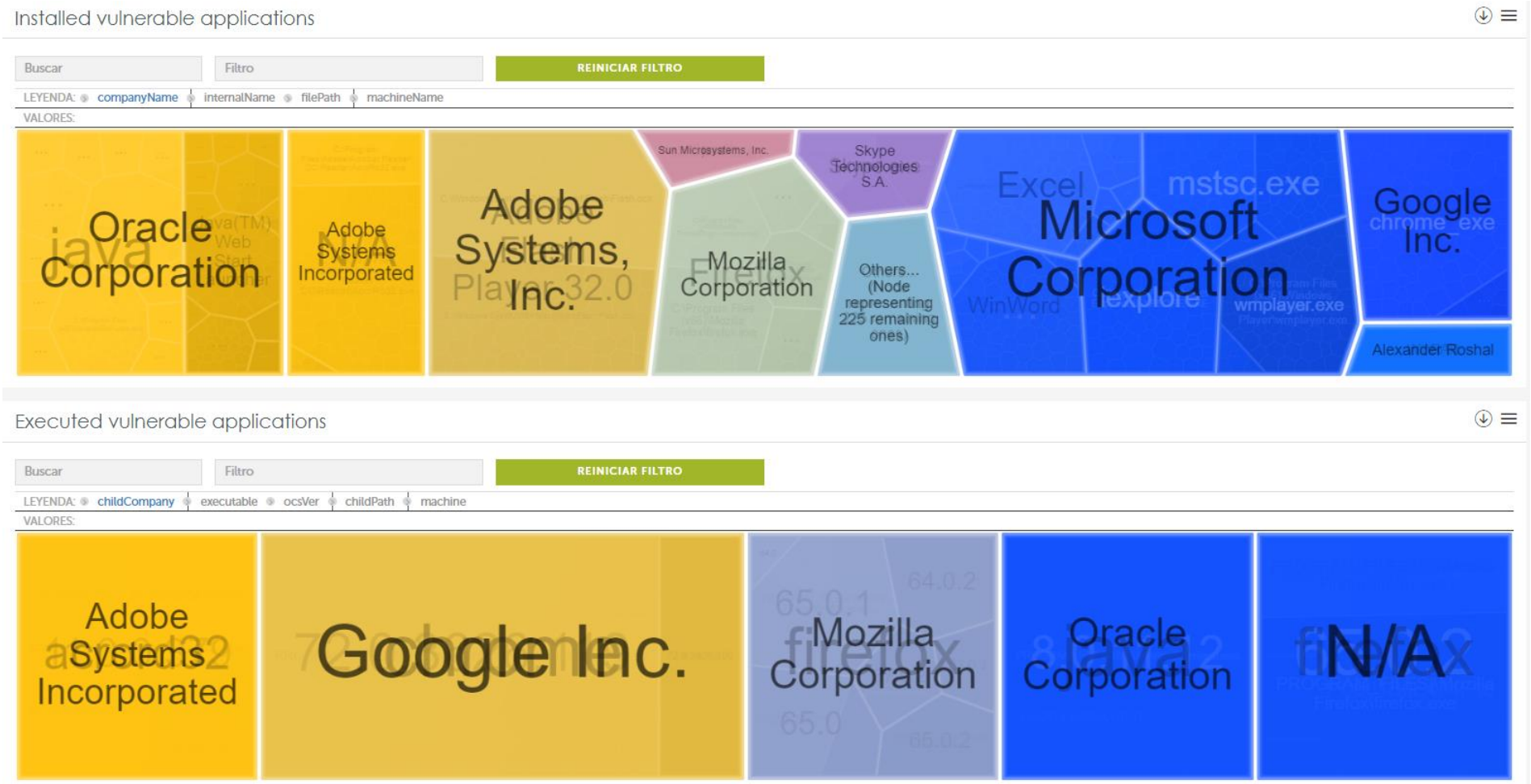
Resultados

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

Punto final: Estado de seguridad centralizado

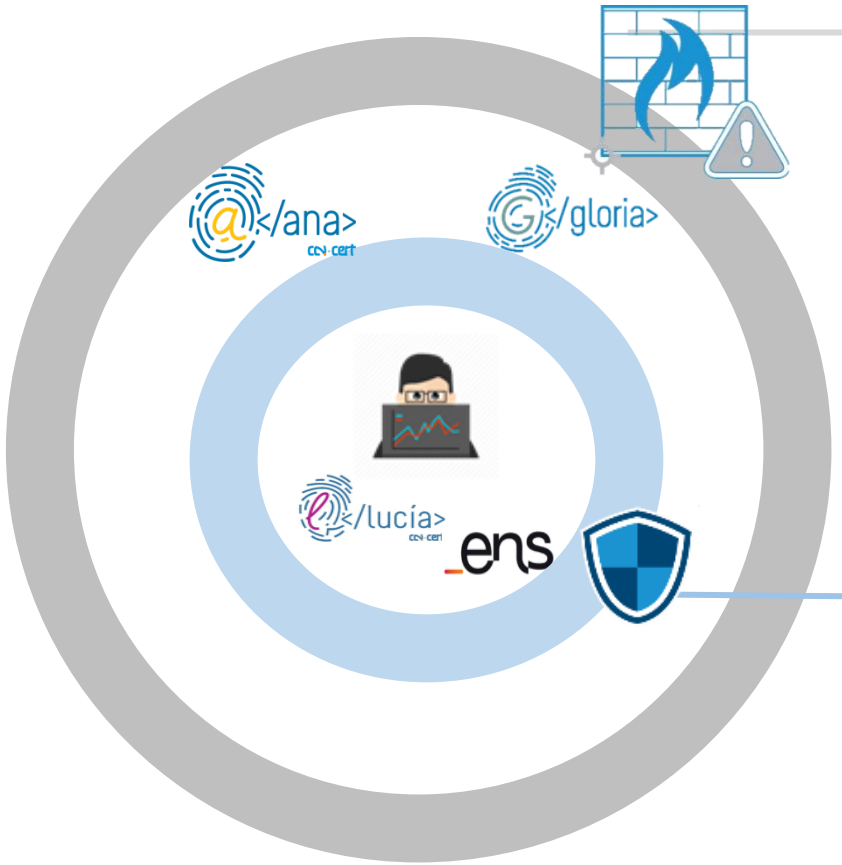
Concepto	Datos
Tiempo POC (hasta hoy)	60 días aprox.
Máquinas Instaladas actualmente	≈ 115
Ficheros clasificados	≈ 14.000
Ficheros Malware ejecutados	**52**
Ficheros PUPs ejecutados	**89**

Punto final: Inventario de aplicaciones



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)

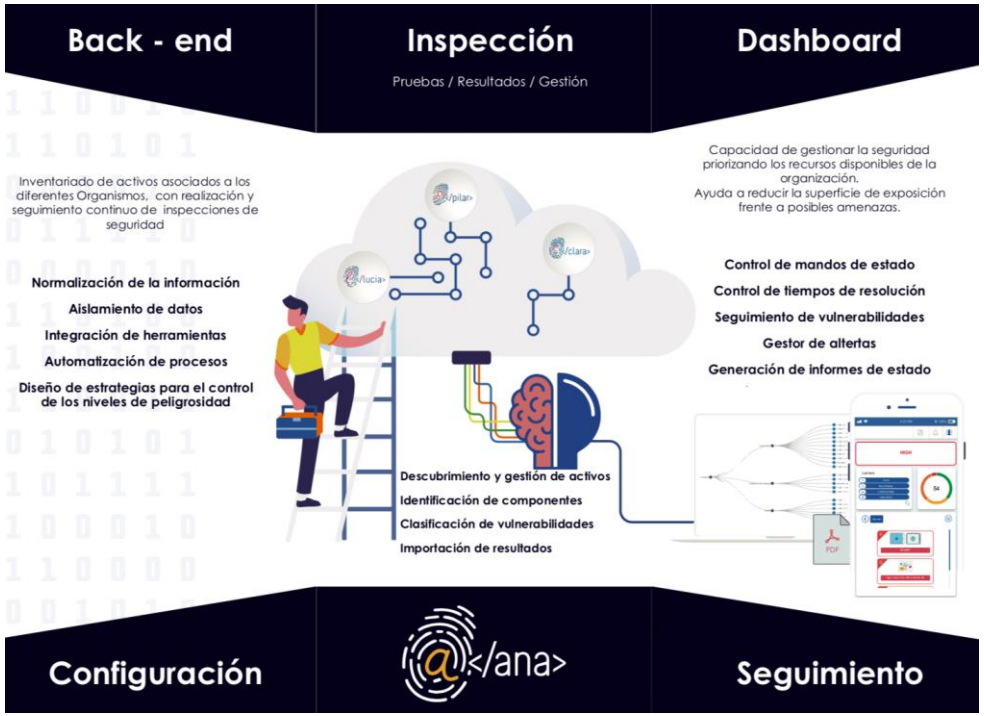
Capacidad forense, remediación remota y reglas de comportamiento

Centro de Operaciones de Ciberseguridad

CCN centro criptológico nacional

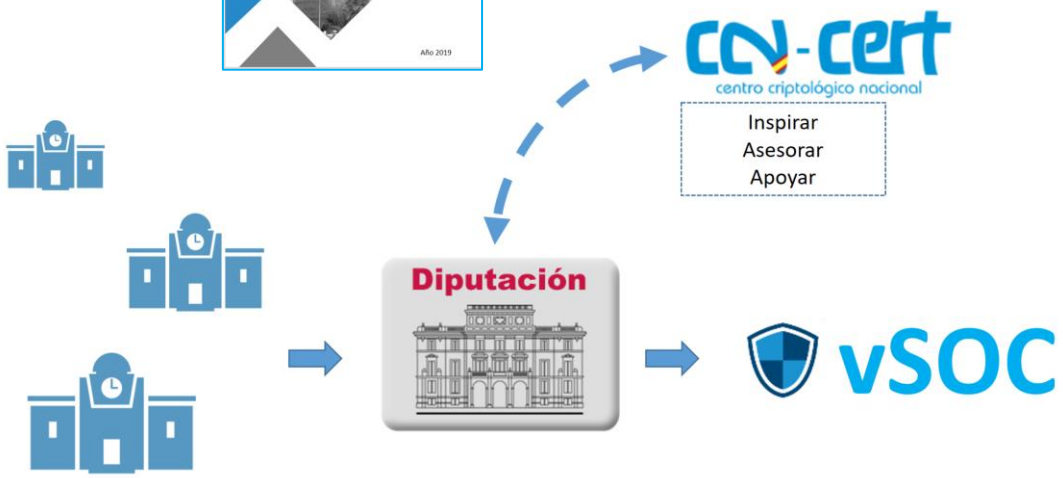
Automatización y Normalización Auditorías (ANA)

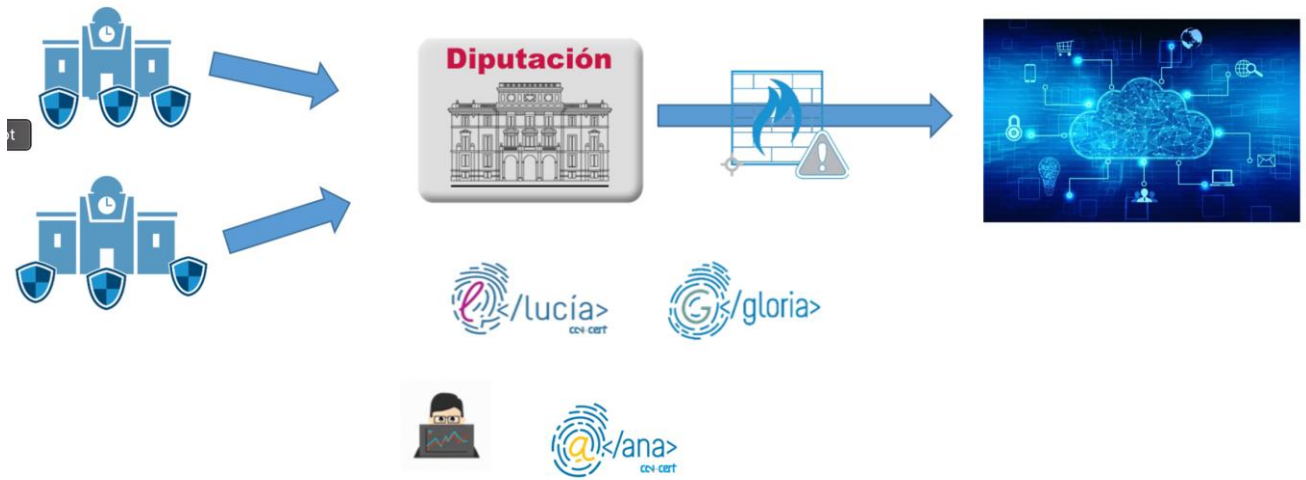
1. Control centralizado del estado de los activos del organismo.
2. Seguimiento continuo de los activos y vulnerabilidades para mejorar los tiempos de resolución.
3. Normalización de todas las auditorías realizadas.
4. Sistema de alertas.
5. Evaluación de vulnerabilidades en tiempo real.
6. Histórico de evolución de medidas correctivas.
7. Generación de informes ejecutivos y técnicos, según evolución en el tiempo.
8. Diferentes vistas técnicas y ejecutivas del estado de los sistemas y misiones del organismo.
9. Reducción de tiempos en la gestión de la seguridad.

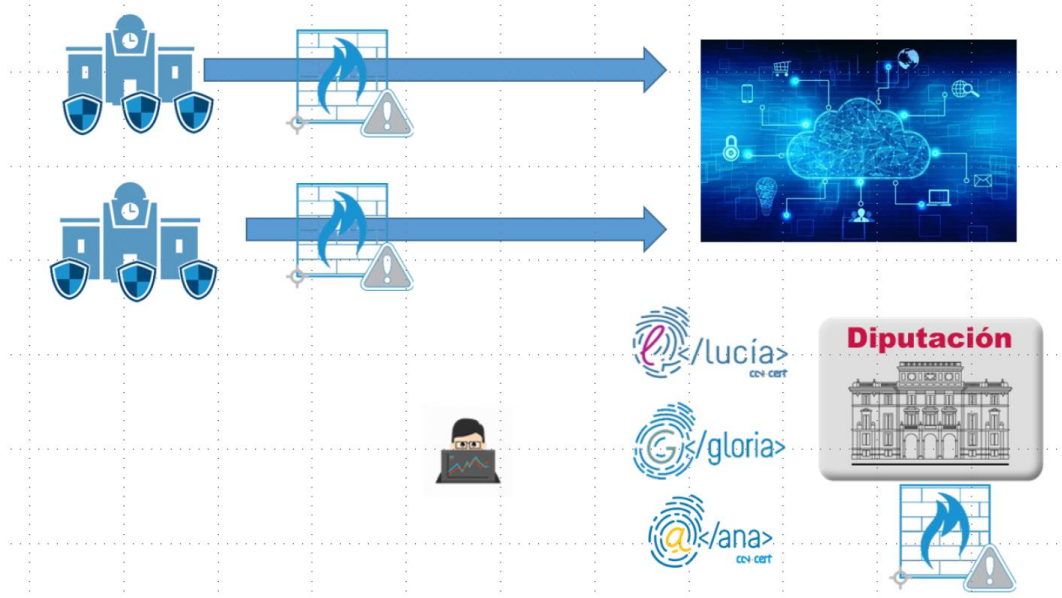


centro criptológico nacional

Arquitectura







CCN
centro criptológico nacional

Casos de Estudio

Tras mantener varias reuniones con organismos interesados en la iniciativa del vSOC hemos detectado varios elementos en común, a modo de ideas, que pueden servir para iniciar el proyecto siguiendo un esquema de piloto.

Líneas de acción…

- Punto inicial es la instalación de LUCIA.
- Una vez instalada LUCIA, el siguiente paso es la unificación de la administración de los firewalls.
- El siguiente paso que puede dar buenos resultados es la instalación de Endpoints y antivirus centralizado.
- El siguiente paso es la adquisición, instalación, configuración y manejo de un SIEM.
- Realización de auditorías de servicio transversal o direcciones IP públicas siempre que la duración de la mismas se evalúe en un alcance máximo de cuatro (4) días.
- Sujeto a lo anterior es la instalación de la solución ANA con el fin de tener una revisión periódica de los sistemas evaluados en la instalación.
- La revisión/inspecciones técnicas es una actividad recomendable pero se es consciente del coste de la misma aun así se considera que aporta buenos resultados.
- Para la gestión del proyecto, se considera suficiente disponer en un principio de 1 a 2 personas.

CONCLUSIONES

- **Incremento** constante del **número, alcance y complejidad** de los ciberataques.
- Necesidad de determinar la **superficie de exposición**.
- Es preciso **reforzar** la capacidad de **prevención**, **monitorización**, **vigilancia** y **respuesta** en todas las instancias del Estado (ciudadanos, empresas y sector público).
- Evolución del modelo de **gestión de incidentes**.
- El **vSOC tiene por objeto** proporcionar protección de manera centralizada mediante la dotación de **una infraestructura global y servicios horizontales de ciberseguridad asociados**.

Comunidad CCN-CERT

Muchas gracias