

**XIII
JORNADAS
STIC
CCN-CERT**



**vSOC para las EELL
Valencianas**

**COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD**

#XIIIJORNADASCNCERT



Lourdes Herrero Gil

CSIRT-CV / Generalitat Valenciana

lherrero@gva.es



Fondo Europeo de
Desarrollo Regional

Una manera de hacer Europa

UNIÓN EUROPEA

Índice

1. Antecedentes
2. Objetivo del proyecto piloto
3. Modelo de prestación del servicio
4. Casuística a cubrir
5. Fuentes de información a integrar
6. Cumplimiento del ENS en las EELL
7. Proyección futura

Antecedentes

Colaboración CSIRT-CV Generalitat Valenciana y Diputación de Valencia

- La colaboración de ambas instituciones para impulso de soluciones TIC en las AALL se remonta a la década de los 80
- Diversos convenios: Han abarcado un gran abanico de soluciones para ayudar en el cumplimiento de sus obligaciones
- Provincia Valencia: 266 municipios / 28 mancomunidades / 3 entidades locales menores
- Diputación Valencia: EELL tamaño mediano /pequeño ↔ Plataformas de Gestión Municipal:
 - Contabilidad
 - Gestión de Ingresos
 - Padrón de Habitantes
 - Administración electrónica (gestión expedientes)
 - Página web
 -

Antecedentes

Ambito CSIRT-CV: Ciudadanos PyMES y AAPP Comunidad Valenciana



Objetivo del proyecto piloto

Apoyo a las EELL al cumplimiento del ENS

- vSOC para entidades locales nace para ayudar a los ayuntamientos en el cumplimiento del Esquema Nacional de Seguridad, en especial con aquellas medidas que implican la vigilancia de la seguridad de su infraestructura TIC así como la recolección, análisis y almacenamiento de registros y actividad de su red y activos críticos.
- A través del modelo descrito a continuación, la Diputación y los ayuntamientos pueden conectarse a vSOC a través de un canal seguro, y enviar sus logs y registros de actividad, para que estos sean almacenados, correlados y analizados por el equipo de CSIRT-CV.
- Más adelante, el ayuntamiento (o la Diputación) tendrá acceso a las distintas herramientas de vSOC obteniendo visibilidad de la información adquirida, la actividad del vSOC en su ámbito y la gestión de sus incidentes.

Casuística a cubrir

10 municipios representativos de la situación de la provincia

- Diputación provee varias aplicaciones de Gestión Municipal a las EELL
- Las EELL que deciden utilizarlas firman convenio
- De las 266 EELL existentes en la provincia, utilizan recursos de la Diputación:
 - Contabilidad: ~ 220
 - Padrón: ~ 208
 - Gestión de ingresos: ~ 168
 - Administración electrónica: ~ 86
 - Web municipal: ~ 230

Casuística a cubrir

10 municipios representativos de la situación de la provincia

Todos tienen informático e interés

TAMAÑO	HABITANTES	CONTABILIDAD	PADRÓN HABITANTES	GESTIÓN INGRESOS	ADMÓN. ELECTRÓNICA	PÁGINA WEB
MEDIO	5987	DIPU	DIPU	AYTO	Externa	DIPU
MEDIO	7629	DIPU	DIPU	DIPU	DIPU	DIPU
MEDIO	5303	DIPU	DIPU	DIPU	Externa	DIPU
PEQUEÑO	3566	AYTO	DIPU	AYTO	DIPU	DIPU
MEDIO	6426	DIPU	DIPU	AYTO	Externa	Externa
PEQUEÑO	1446	AYTO	AYTO	AYTO	Externa	DIPU
PEQUEÑO	2461	DIPU	DIPU	DIPU	Externa	Externa
MEDIO	7199	DIPU	DIPU	AYTO	AYTO	DIPU
MEDIO	5927	DIPU	DIPU	DIPU	DIPU	Externa
PEQUEÑO	3597	DIPU	DIPU	DIPU	Externa	DIPU

Fase actual

Siguiente fase

A evaluar

Fuentes de información a integrar

Formulario recogida datos medios tecnológicos en cada Ayuntamiento

- Datos identificativos y contacto
- Estaciones de trabajo, servidores... (Nº y SSOO)
- Gestor de identidades: ¿Cuál? ¿Qué almacena?
- Antivirus: ¿Cuál? ¿HIDS?
- Firewall para gestionar el acceso redes internas o el acceso Internet: ¿Cuál?
- Proxies
- Redes inalámbricas: ¿Para quién? ¿Con qué autenticación? ¿Qué dispositivos las gestionan?
- Equipos externos: Se permiten / no. Controles
- Aplicaciones: Gestión Municipal

Qué datos relevantes para la seguridad podemos obtener, e ir incorporándolos

Fuentes de información a integrar

Particularidades de las aplicaciones de gestión municipal

- Mezcla de tecnologías más actuales y más antiguas
- Algunas son cliente servidor, otras son web
- Algunas tienen acceso directo desde Internet, otros a través de pasarelas intermedias

Nos tenemos que adaptar a los datos que proporciona cada una de las aplicaciones.

Fuentes de información a integrar

1º Tipo de aplicación G.M.

- Cliente servidor, accesible a las EELL través de escritorio remoto estilo Citrix
- Usa tecnologías más antiguas y conexión directa de los clientes con la BBDD

Qué datos relevantes para la seguridad podemos obtener:

- Conexiones al escritorio remoto
- Autenticaciones de la aplicación contra la BBDD
- Tipo de acceso realizado (lectura, adición, modificación, borrado)

Fuentes de información a integrar

2º Tipo de aplicación G.M.

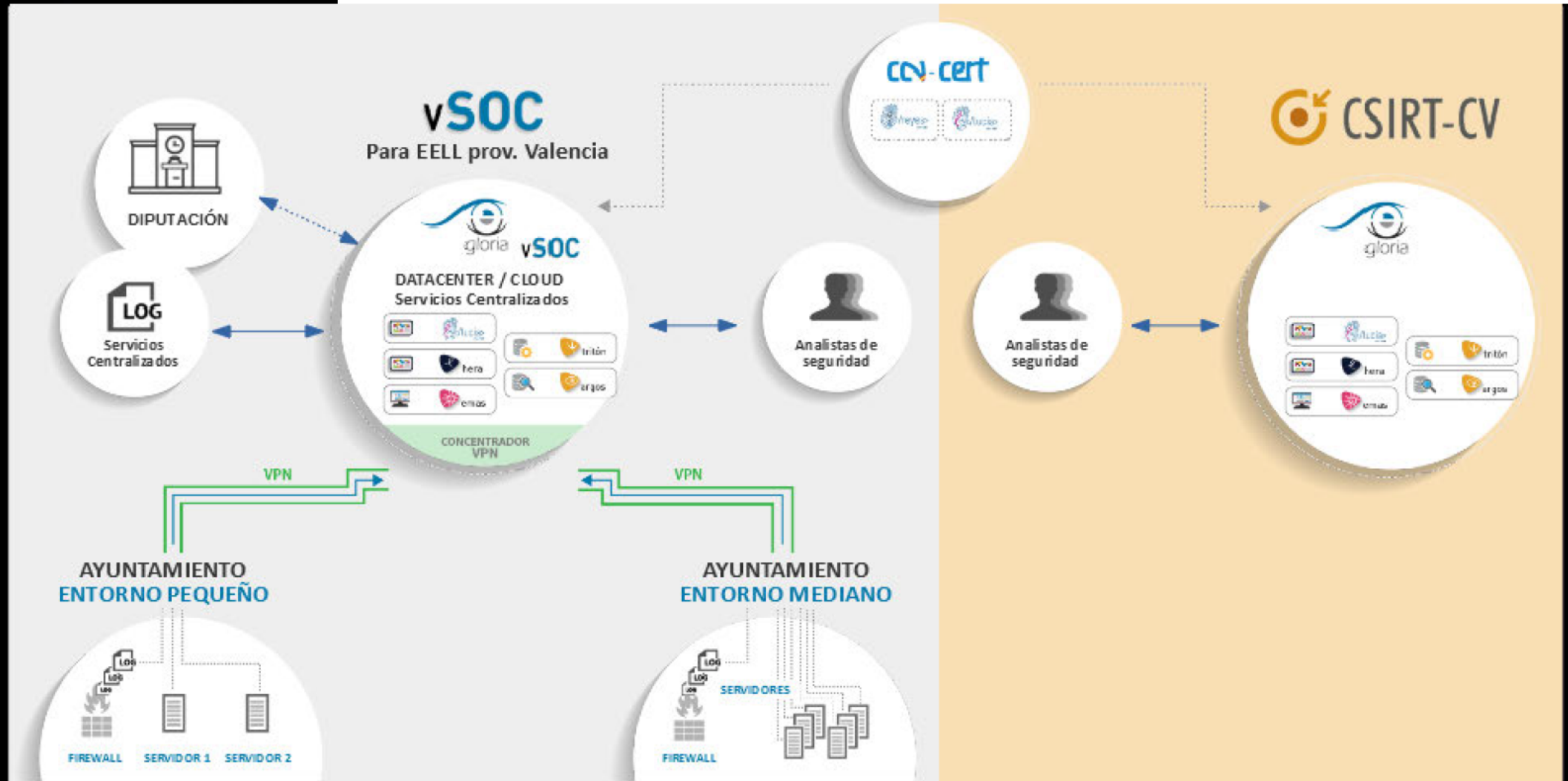
- Cliente servidor, accesible para las EELL directamente por Internet
- Usa tecnologías más actuales y conexión a través de un servidor web

Qué datos relevantes para la seguridad podemos obtener:

- Conexiones al servidor web
- Autenticaciones de la aplicación contra la aplicación web
- Tipo de acceso realizado (lectura, adición, modificación, borrado)

Fuentes de información a integrar

Aquello que sea relevante para la seguridad de la Entidad Local



Cumplimiento del ENS en las EELL

Requisitos cuyo cumplimiento se facilita

✓ **Arquitectura de seguridad [op.pl.2]**

- Con la implantación de un **vSOC** se mejora la arquitectura de seguridad, concretamente las líneas de defensa de la organización

✓ **Protección frente a código dañino [op.exp.6]**

- Complementa la protección mediante los agentes desplegados en cada ayuntamiento

✓ **Gestión de incidentes [op.exp.7]**

- Mediante la detección de eventos de seguridad por el **vSOC** y la inteligencia añadida y el reporte a Lucía

✓ **Notificación de incidentes de seguridad [guía notificación y gestión]**

✓ **Registro de la actividad de los usuarios [op.exp.8]**

- Los agentes desplegados en los sistemas de la organización podrán ayudar a registrar las actividades de los usuarios (especialmente en los servidores) y se revisarán en busca de patrones anómalos

Cumplimiento del ENS en las EELL

Requisitos cuyo cumplimiento se facilita

✓ Registro de la gestión de incidentes [op.exp.9]

- Los incidentes son recogidos en **GLORIA** y gestionados en CSIRT-CV. Esto permitirá que se incluyan las evidencias del incidente y las acciones derivadas del mismo

✓ Detección de intrusión [op.mon.1]

- El **vSOC** detectará patrones anómalos y cualquier comunicación sospechosa bloqueada por el firewall o las sondas

✓ Perímetro seguro [mp.com.1]

- El **vSOC** detectará patrones anómalos y cualquier comunicación sospechosa bloqueada por el firewall o las sondas

✓ Protección de servicios y aplicaciones web [mp.s.2]

- Mediante monitorización de los agentes desplegados en los servicios, firewall...

✓ Protección frente a denegación de servicios [mp.s.8]

- Mediante monitorización de los agentes desplegados en los servicios, firewall...

Proyección futura

Medir, para poder crecer

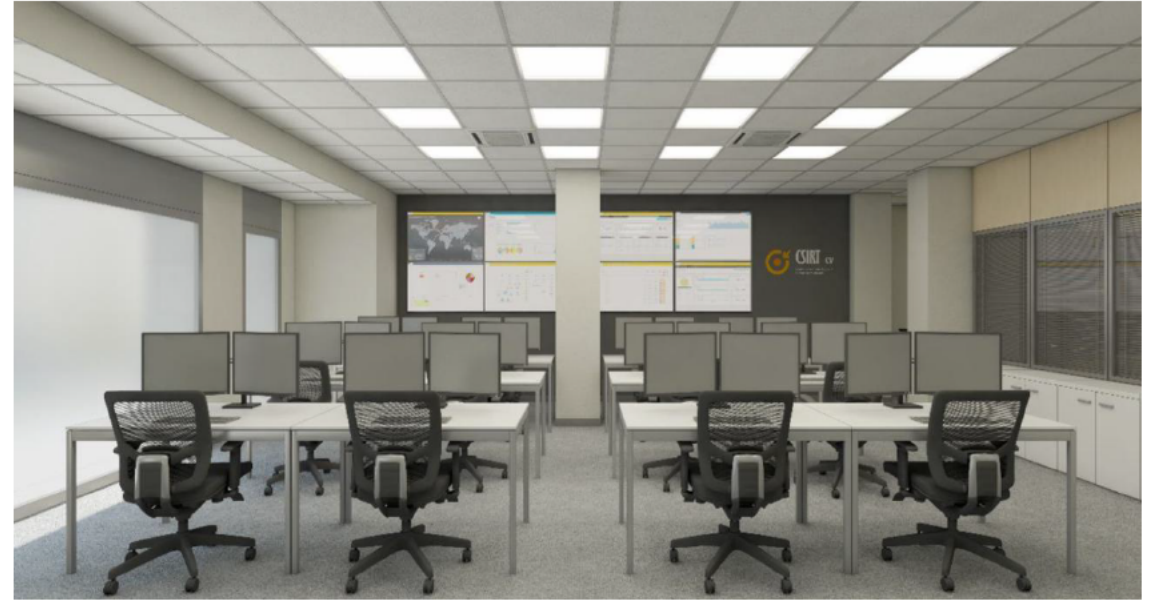
- SIEM operativo. Recibiendo muestras de la Información (ver su significancia)
- Impacto que tiene en el centro
- Reforzar el equipo en CSIRT-CV y Diputación con perfiles especializados para atender a las EELL
- Plantearnos formación para el personal de los ayuntamientos (Plan Valenciano Capacitación)
- Ampliación del SIEM para
 - Incorporar más Ayuntamientos (medianos y pequeños)
 - Incorporar otros aplicativos comunes
 - Incorporar más fuentes
 - Incorporar Alicante y Castellón

Hasta donde el presupuesto nos lleve...

¿Alguna pregunta?

Muchas Gracias

csirtcv@gva.es



UNIÓN EUROPEA

Fondo Europeo de
Desarrollo Regional

Una manera de hacer Europa

COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD

#XIIIJORNADASCNCERT

OC.CCN.CNI.ES

WWW.CCN.CNI.ES

WWW.CCN-CERT.CNI.ES

XIII JORNADAS STIC CCN-CERT

ccn-cert
centro criptológico nacional