

**XIII
JORNADAS
STIC
CCN-CERT**



CCN-CERT vSOC

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

#XIIIJORNADASCNCERT



Nombre y apellidos: Ignacio Briones

Organismo / Empresa: CCN-CERT

Email de contacto: socccn@ccn-cert.cni.es

Índice

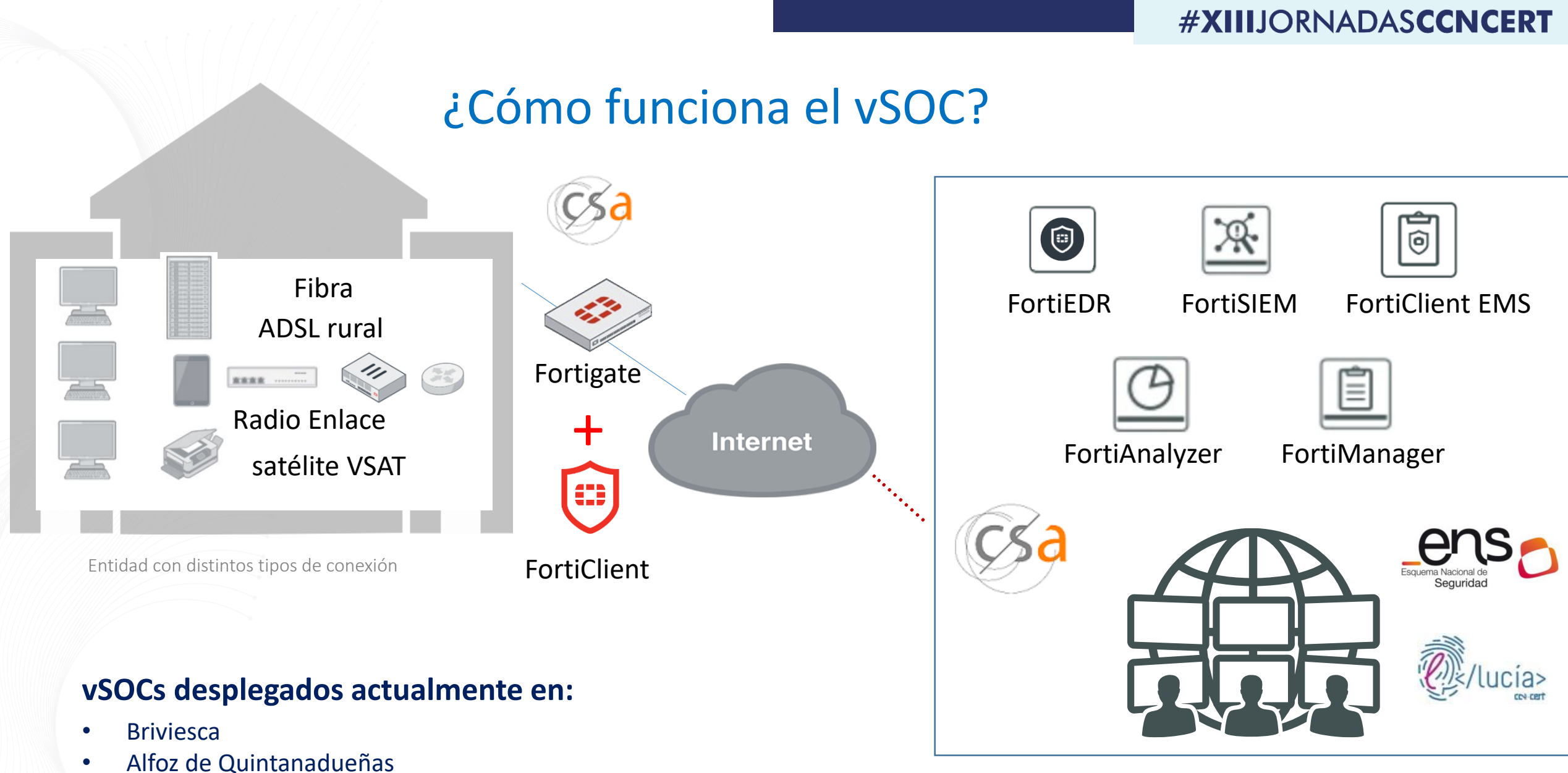
- 1. Introducción al vSOC**
- 2. Servicios vSOC**
- 3. ¿Cómo funciona el vSOC?**
- 4. Presentación de la POC**
- 5. Componentes vSOC**
- 6. Inteligencia CCN-CERT y FortiGuard**



Servicios vSOC

- Despliegue de **firewalls** + Software Suite **Protección del endpoint** 
- Mayor visibilidad sobre **incidentes y vulnerabilidades** 
- **Seguridad** perimetral con **administración centralizada**
- Capacidad de **detección de anomalías** (mucho más que una sonda)
- Capaz de actuar ante ataques tipo **Wannacry y Emotet** 
- **Gestión de cumplimiento** de los puestos de trabajo

¿Cómo funciona el vSOC?



vSOCs desplegados actualmente en:

- Brivesca
- Alfoz de Quintanadueñas

Adaptado a cualquier tipología de entidad local

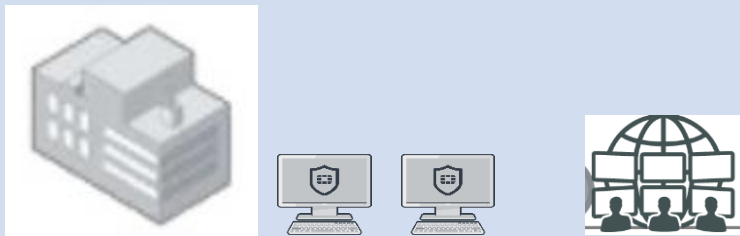
Fibra (10-40 usuarios)
bajada 150 Mb y subida 100 Mb



ADSL rural (1-2 usuarios)
bajada 8-10 Mb y subida 300 kbs



Movistar Radio (1-2 usuarios)
bajada 17Mb y subida 7Mb



satélite VSAT (1-2 usuarios)
bajada 50Mb y subida 8-10Mb



Escenarios encontrados por en Burgos

Entidades locales con:

- Equipos, switch y firewall(s)
- Equipos y switch
- Equipos directos al router



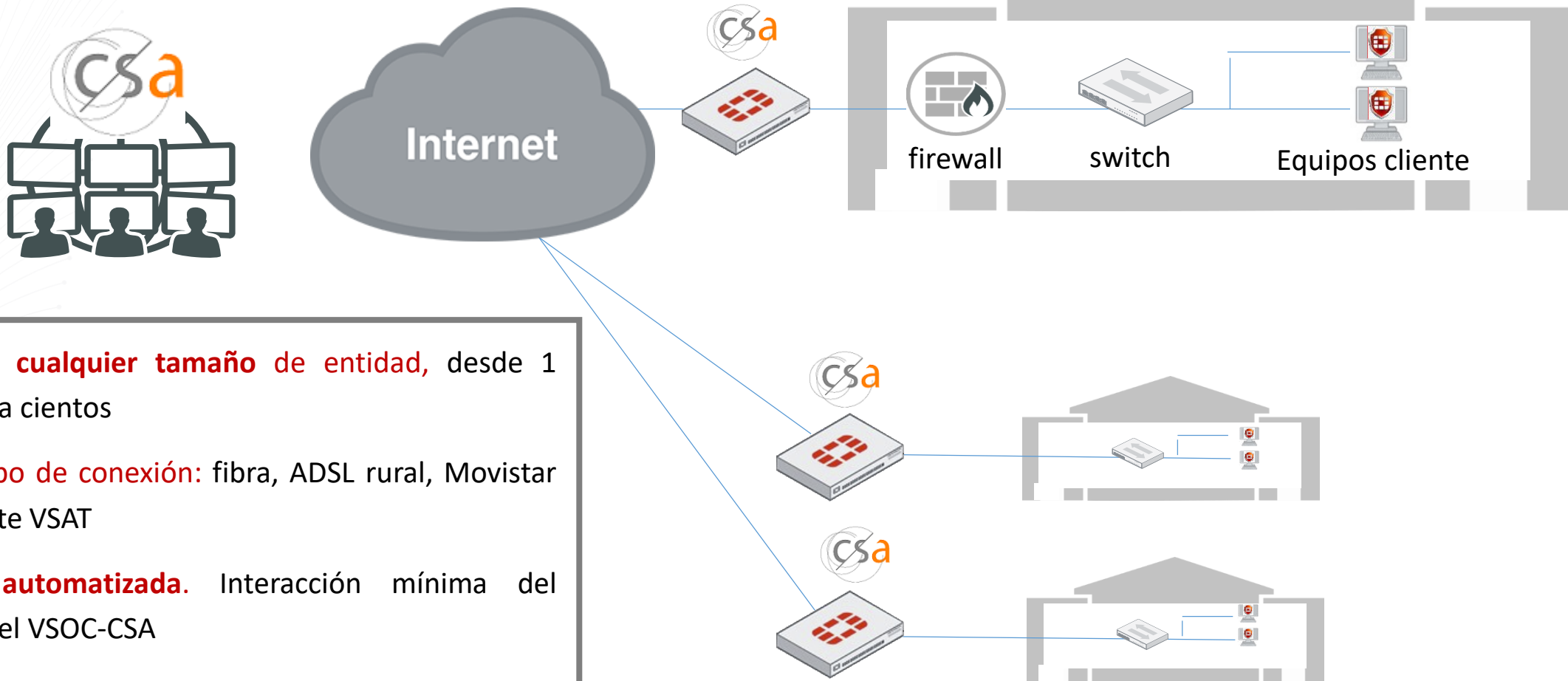
Amenazadas por:

DDoS, malware, ransomware, robo de contraseñas, ataques de MiTM, phishing, botnets...



vSOC

Prevención, Monitorización, Vigilancia y Respuesta



- Adaptado a **cualquier tamaño** de entidad, desde 1 usuario hasta cientos
- **Cualquier tipo de conexión:** fibra, ADSL rural, Movistar Radio, satélite VSAT
- **Respuesta automatizada.** Interacción mínima del usuario con el VSOC-CSA
- Cumplimiento del **ENS** y **Guías CCN-STIC**
- **Servicio** de operaciones remoto **24x7**



Seguridad en los puestos de trabajo



FortiEDR

Gestión de cumplimiento
FortiClient EMS

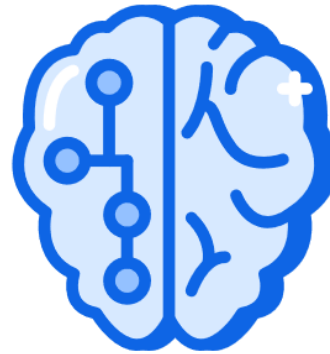


Recepción y almacenamiento de logs para cumplimiento normativo



FortiAnalyzer

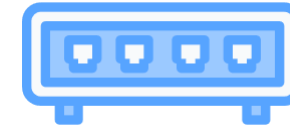
Componentes



Correlación y generación de inteligencia



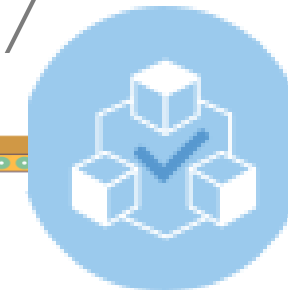
FortiSIEM



Infraestructura de gestión masiva de firewalls



FortiManager

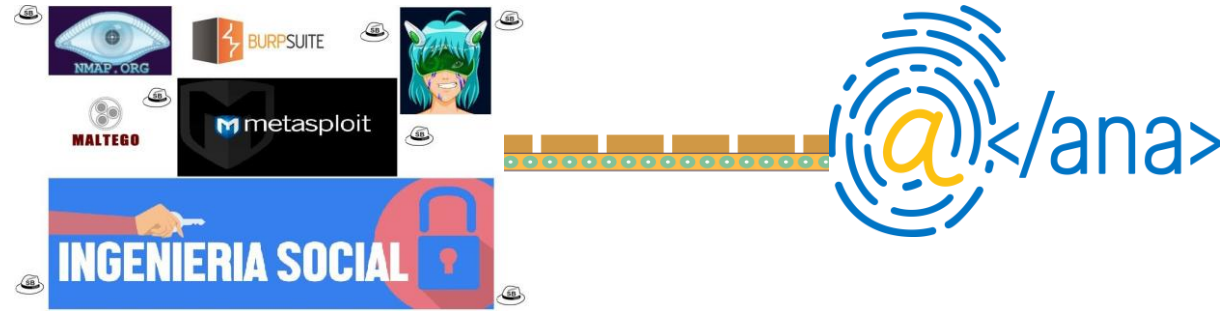


LUCIA

Servicio de operación y vigilancia



Medir la exposición de la seguridad externa e interna



- Revisar la seguridad mediante pentest
- La parte externa tiene mucho peso en imagen y es vía de acceso
- La interna es un campo de batalla
- La medida la reflejamos en ANA
- Ganando ambas se asienta la seguridad

Inteligencia CCN-CERT



ANA



CLARA



REYES



LUCIA

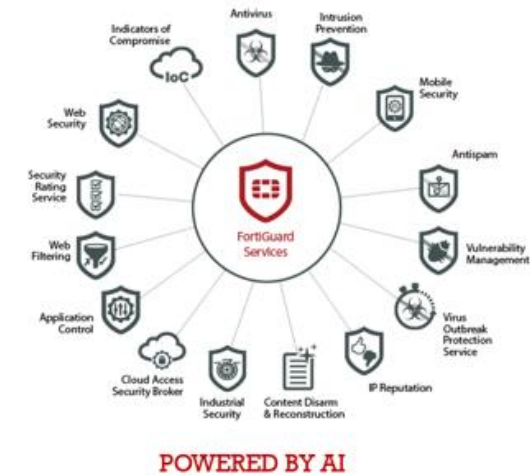


INES



MARIA

Inteligencia FortiGuard



COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD

#XIIIJORNADASCCNCERT

OC.CCN.CNI.ES

WWW.CCN.CNI.ES

WWW.CCN-CERT.CNI.ES

**XIII
JORNADAS
STIC
CCN-CERT**

ccn-cert
centro criptológico nacional