# EMMA – **Seguridad para reducir el riesgo de la superficie de exposición de los Ayuntamientos.**

***Una solución viable orientada a los problemas reales de las EELL***

Visibilidad y control sobre la red

opencloud factory

opencloudfactory.com

Superficie de exposición ha crecido de manera exponencial en los últimos 18 meses [¿Dónde empezar?]

Falta de recursos personales – impacto en operaciones

La gestión del presupuesto sigue siendo una gran barrera

## Problema

1 Ampliación exponencial del superficie de posición – foco en conectividad

## Impacto

1 Más dispositivos, más conectividad (desde dentro y fuera) y flujos de datos sin control – más riesgo al EELL no cuantificado

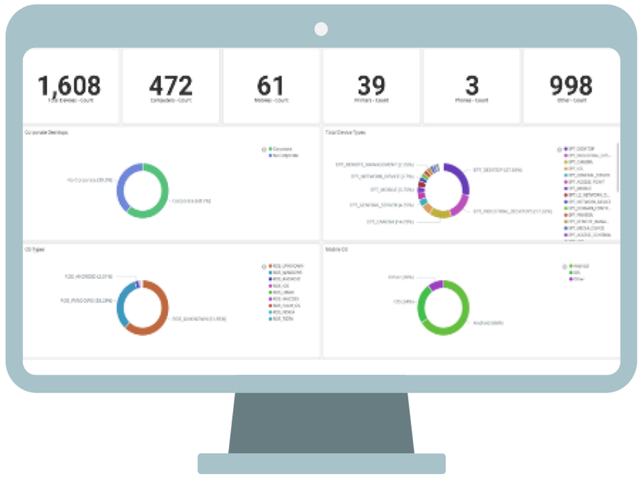
## Solution

### 1. Visibilidad

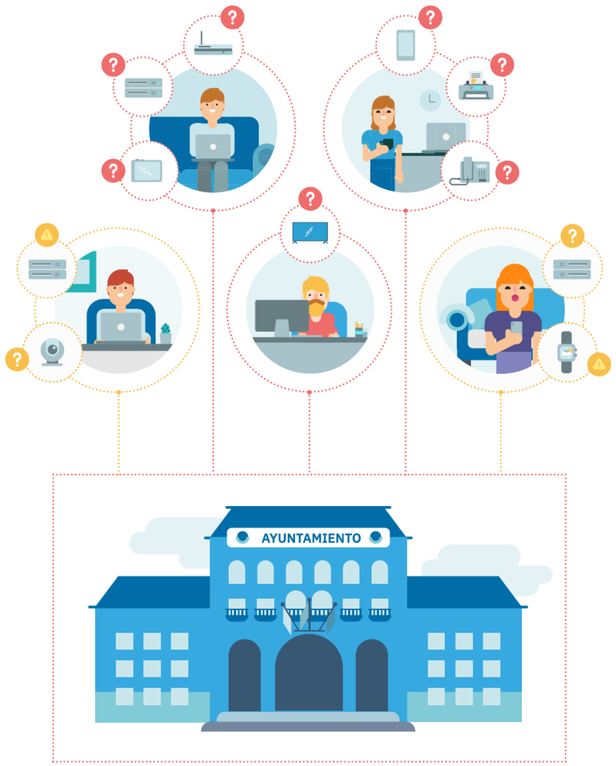
**Establecer una linea base de todo lo conectado**

- Cuantificar y cualificar todos los dispositivos conectados a la red de manera automatizada, centralizada y pasiva.
- Averiguar desviaciones de la línea base
- Zero impacto operacional

# 1. Visibilidad y vigilancia







## Problema

2 Ampliación exponencial del superficie de posición – foco en conectividad en 2020/21

## Impacto

2 Conectividad sin control, nuevo eslabón débil, ataque vía suplantación de identidad, cajas negras

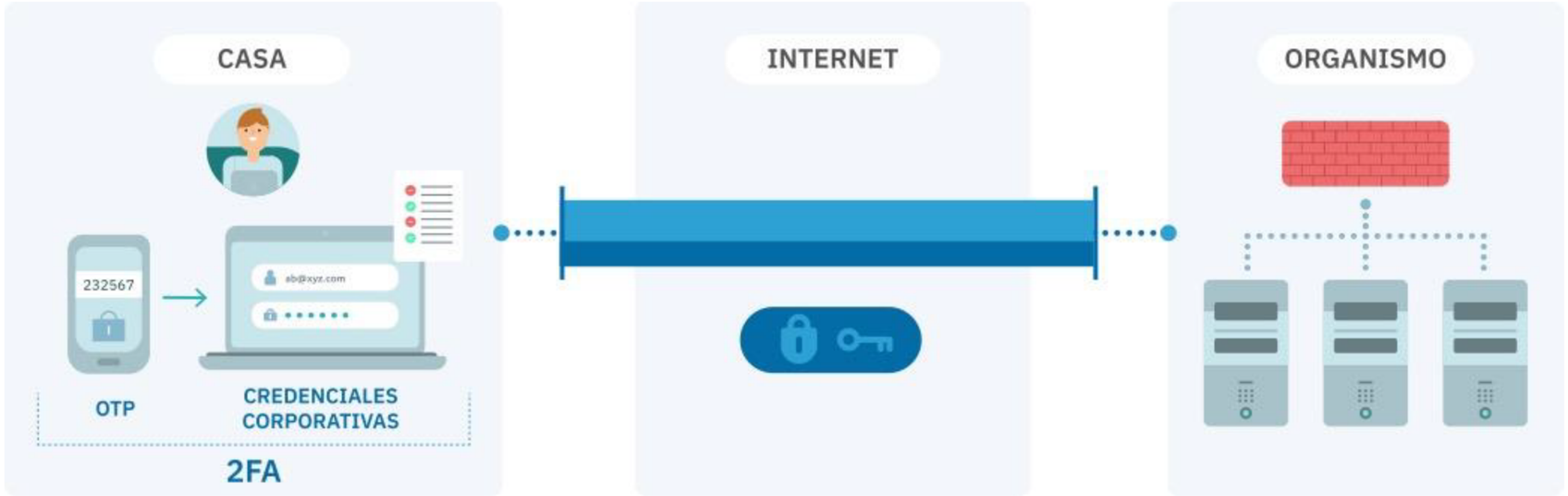
## Solution

**2. EMMA Vigilancia en acceso remoto**

**Asegurar el acceso remoto con vigilancia**

- Mitigar el riesgo critico de las conexiones remotas de los usuarios internos como externos

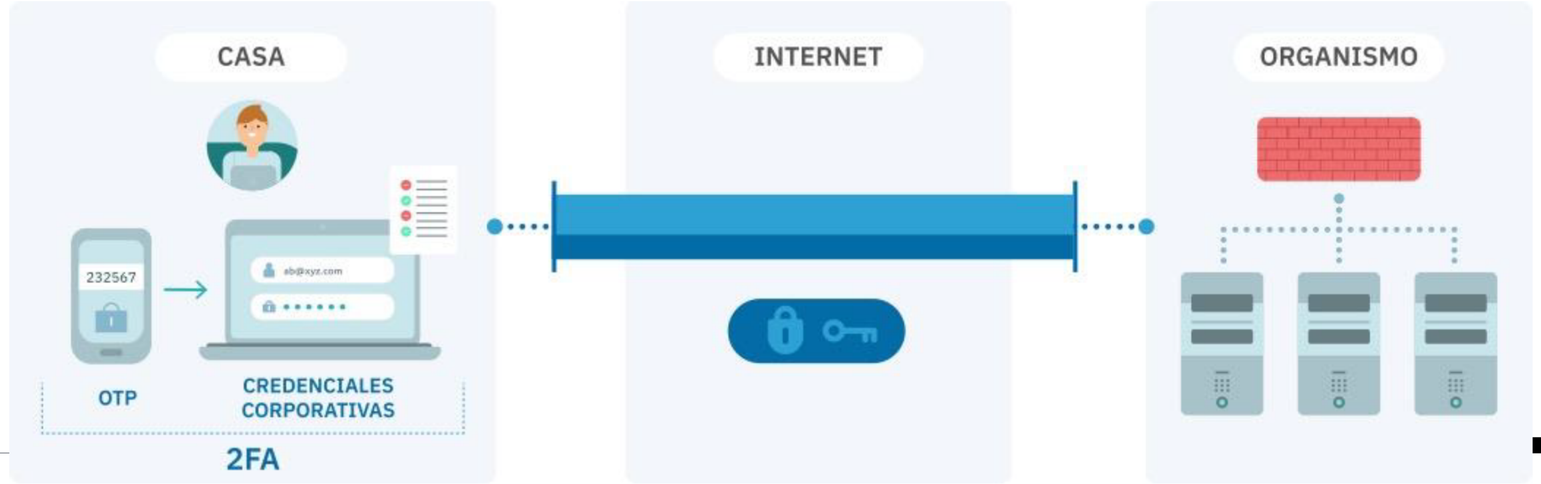
# 2. Acceso remoto seguro



# EMM-VAR

## Vigilancia en acceso remoto

| Riesgos | Solución |
|---|---|
| • Conectividad sin limites de los usuarios (Teamviewer, RDP…) | • Principio de mínimo privilegio (acceso restringido) en función de usuario (autenticación de usuario) , horario etc. |
| • **Suplantación de identidad** | • LDAP / AD + 2FA (segundo factor de autenticación) |
| • Conectividad desde equipos infectados | • Postura de seguridad del equipo (complementa la solución CLARA) |
| • Comunicación insegura (en clara) | • Canal cifrado (VPN) |
| • Comunicación (potencialmente maligna) cifrado – cajas negras | • Vigilancia del trafico (no hay caja negras) |



# Impacto en la adecuación al ENS

Medidas tecnológicas y su mapeo con el ENS (no hay que contemplar ahora pero saber que este)

# Medidas de Seguridad ENS >20k – 75k

## Visibilidad – Cuantificación y Cualificación de Activos

| Medidas de Seguridad | | | | | | | Perfil de cumplimiento | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | Diputaciones | | Ayuntamiento <75K | | Ayuntamiento < 20K | | Ayuntamiento < 5K | | | |
| | | | | | | | Sis. Org Competente | Externalizado | Ayuntamiento | Externalizado | Ayuntamie | Sis. Órgano Compete | | Ap | Mo | N |
| Medidas de Seguridad | 2 | Marco operacional (OP) | Planificación (pl) | 1 | Análisis de riesgos | op.pl.1 | Medio | Medio | Medio | Medio | Medio | Bajo | Bajo | Si | V | Todos |
| | | | | 2 | Arquitectura de | op.pl.2 | Medio | Medio | Medio | Medio | Medio | Medio | Bajo | Si | V | Todos |
| | | | | 4 | Dimensionamiento / Gestión de capacidades | op.pl.4 | Medio | No Aplica | Medio | No Aplica | Medio | No Aplica | No Aplica | Si | V | Medio |
| | | | Explotación (exp) | 1 | Inventariado de Activos | op.exp.1 | Medio | Medio | Medio | Medio | Medio | Medio | Bajo | Si | V | Todos |
| | | | | 8 | Registro de la actividad de los usuarios | op.exp.8 | Medio | Medio | Medio | Medio | Medio | Bajo | Bajo | Si | V | Todos |
| | | | | 9 | Registro de la gestión de incidentes | op.exp.9 | Medio | Medio | Medio | Medio | Medio | Medio | Medio | Si | V | Medio Alto |
| | | | Servicios Externos (ext) | 1 | Contratación y acuerdos de nivel de servicio | op.ext.1 | Medio | Medio | Medio | Medio | Medio | Medio | Medio | Si | V | Medio Alto |
| | 3 | Medidas de Protección (MP) | Continuidad de Servicio | 1 | Análisis de Impacto | op.cont.1 | Medio | Medio | Medio | Medio | No Aplica | No Aplica | No Aplica | Si | V | Medio Alto |
| | | | Monitorización del Sistema (mon) | 1 | Detección de Intrusión | op.mon.1 | Medio | Medio | Medio | Medio | Medio | Medio | No Aplica | Si | V | Medio Alto |
| | | | Protección de los Equipos (eq) | 3 | Protección de equipos portátiles | mp.eq.3 | Medio | Medio | Medio | Medio | Medio | Medio | Bajo | Si | V | Básico |
| | | | Protección de Información (info) | 2 | Calificación de la información | mp.info.2 | Medio | Medio | Medio | Medio | Medio | Medio | Bajo | Si | V | Todos |
| | | | | 7 | Copias de seguridad (backup) | mp.info.9 | Medio | Medio | Medio | Medio | Medio | Medio | No Aplica | Si | V | Todos |

- La visibilidad es un componente básico de cualquier estándar de seguridad. Tener un **inventario de red** actualizado es fundamental

- **La seguridad empieza con la visibilidad**, conocer el sistema permite determinar la manera más apropiada de asegurarlo

- **Hasta 12 medidas de seguridad** dependiendo del perfil de cumplimiento.

# Medidas de Seguridad ENS – VAR

## VAR – Vigilancia en Accesos Remotos

| Medidas de Seguridad | | | | | | | Perfil de cumplimiento | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | Diputaciones | | Ayuntamiento <75K | | Ayuntamiento < 20K | | Ayuntamiento < 5K |
| | | | | | | | Sis. Org Compete | Externalizado | Ayuntamiento | Externalizado | Ayuntamie | Sis. Órgano Competer | |
| Medidas de Seguridad | 2 | Marco operacional (OP) | Planificación (pl) | 2 | Arquitectura de seguridad | op.pl.2 | Medio | Medio | Medio | Medio | Medio | Medio | Bajo |
| | | | Control de Acceso (acc) | 1 | Identificación | op.acc.1 | Medio | Medio | Medio | Medio | Medio | Medio | Bajo |
| | | | | 2 | Requisitos de Acceso | op.acc.2 | Medio | Medio | Medio | Medio | Medio | Medio | Bajo |
| | | | | 4 | Proceso de gestión de derechos de acceso | op.acc.4 | Medio | Medio | Medio | Medio | Medio | Medio | Bajo |
| | | | | 5 | Mecanismo de | op.acc.5 | Medio | Medio | Medio | Medio | Medio | Medio | Bajo |
| | | | | 7 | Acceso Remoto | op.acc.7 | Medio | Medio | Medio | Medio | Medio | Medio | Medio |
| | 3 | Medidas de Protección (MP) | Protección de las Comunicaciones (com) | 1 | Perimetro Seguro | mp.com.1 | Medio | Medio | Medio | Medio | Medio | Medio | Bajo |
| | | | | 2 | Protección de la Confidencialidad | mp.com.2 | Medio | Medio | Medio | Medio | Medio | Medio | Medio |
| | | | | 3 | Protección de la autenticidad y de la integridad | mp.com.3 | Medio | Medio | Medio | Medio | Medio | Medio | Medio |

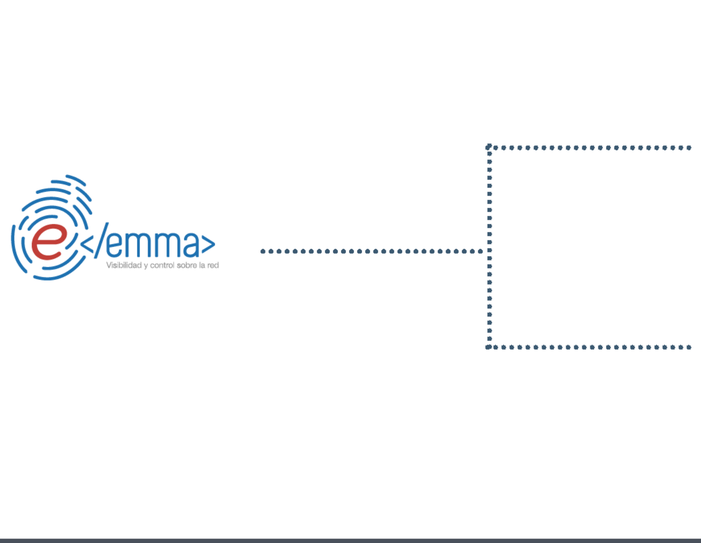
- Cada tipo de organismo tiene su **declaración de aplicabilidad** dependiendo de su tamaño y su sistema
- El módulo de VAR **puede usarse como complemento de una solución actual** para robustecer el sistema y cumplir más medidas
- **Hasta 9 medidas de seguridad** dependiendo del perfil de cumplimiento.

# Solución EMMA

**EMMA** es una solución dentro de un eco sistema

## Soluciones del ecosistema

Además de los módulos mencionados, **EMMA** se integrará con soluciones del ecosistema **CCN-CERT**. Concretamente con las siguientes soluciones: **ROCÍO y ANA.**




Es una herramienta de auditoría de cumplimiento con el ENS/STIC en dispositivos de red.

Es un sistema de auditoría continúa desarrollado por el CCN-CERT que tiene por objetivo incrementar la capacidad de vigilancia y conocer la superficie de exposición.

### Ventajas EMMA

- Producto incluido en el catálogo STIC del CCN-CERT
- Fácil integración con otros productos y tecnologías
- Guías STIC de configuraciones integradas
- Partners (integradores) certificados para garantizar calidad

# ¿Cómo aterrizarla?

# Contrato menor: Despliegue rápido / ágil

**Facilitar a los Ayuntamientos de menos de 500 ordenadores y hasta 100 usuarios remotos: Seguridad viable comenzando por el módulo de visibilidad + vigilancia en accesos remotos.**

Se centra en la funcionalidad sobre la que más valor va a aportar al organismo y que permitirá establecer todas las piezas tecnológicas para implementar otras funcionalidades / medidas tecnológicas posteriormente.

## Sencillez de despliegue y puesta en marcha

- Método pasivo, independientemente de la electrónica
- Pocos requisitos necesarios para desplegar

## Obtención de resultados tangibles en poco tiempo

- Inventario en tiempo real
- Cumplimiento de ENS (hasta 17 medidas)

## ¿Qué incluye?

- **Servicios**
  - Instalación
  - Soporte / mantenimiento
  - Elaboración de dashboards para el Ayuntamiento

~~La superficie de exposición ha crecido de manera exponencial en los últimos 18 meses~~

- Visibilidad del superficie de exposición
- Control de acceso remoto (2FA, postura de seguridad..)

~~Falta de recursos personales – impacto en operaciones~~

Solución de poco impacto implementado por un proveedor de servicios

~~La gestión del presupuesto sigue siendo una gran barrera~~

Todo dentro de un menor

# Gracias

Para más información:
EMMA@opencloudfactory.com