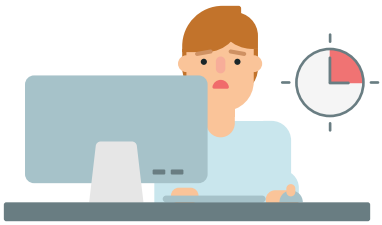
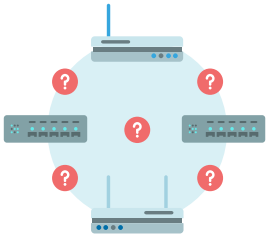
EMMA -
Cumplimiento

El bastionado de la capa de acceso es un **punto clave** en la adecuación del ENS, ya que supone un punto que podría multiplicar el riesgo asociado a cada activo conectado a la red. A pesar de lo **estratégica** que puede ser la capa de acceso en cuanto a la seguridad del organismo y sus sistemas, en ocasiones resulta un punto de vulnerabilidad conocida que requiere aseguramiento y mejora continua.





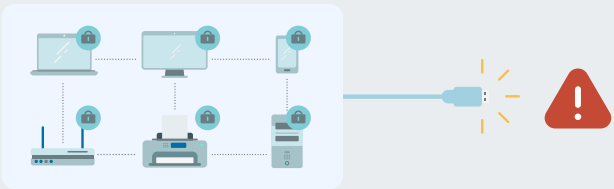
El problema

El correcto bastionado de la capa de acceso es un punto clave en la adecuación al ENS ya que supone un punto que multiplica el riesgo asociado a cada activo conectado a la red.

- La gestión manual y descentralizada de la infraestructura hace que la tarea de actualización, mantenimiento etc. y su correspondiente proceso de auditoria esté sujeto a personas.
- Las empresas gestionan muchos tipos de electrónica (multi-fabricante y multi-versión). Cada uno requiere sus configuraciones concretas en puntos muy dispersos.
- La mayoría de las empresas no tienen una visibilidad centralizada del 100% de todos los dispositivos de red, lo que hace imposible su auditoría.

¿Por qué la capa de acceso es tan **estratégica** para la seguridad del conjunto del organismo?

Rápida difusión de noticias en medios de potenciales situaciones:



La estrategia de **Zero Trust** (donde no se confía en ninguna conexión sin validación) se aplica sobre la capa de acceso con lo cual, si la capa de acceso no está bastionada, la estrategia de Zero Trust se ve comprometida.

Inseguras por defecto

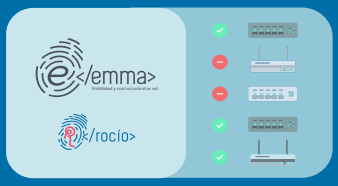
- Para facilitar la instalación, operación y mantenimiento fabricantes crean y distribuyen dispositivos de red con servicios explotables habilitados de forma predeterminada.

Desactualizadas

- A menudo no se modifican las configuraciones predeterminadas de los dispositivos, tampoco se realizan actualizaciones de versiones o de configuraciones de seguridad.

Cisco argumenta que “El 31% de las organizaciones ha experimentado ciberataques a la infraestructura de tecnología operativa”.

La Solución: EMMA - Cumplimiento



- **EMMA -** Cumplimiento es un módulo dentro de la solución **EMMA** que centraliza y automatiza parte del proceso de auditoría de las configuraciones de la electrónica con las configuraciones de las guías STIC **(ROCÍO).**
- Facilita la adecuación a estándares como el ENS y garantiza la implementación segura de la tecnología de control de acceso a la red.

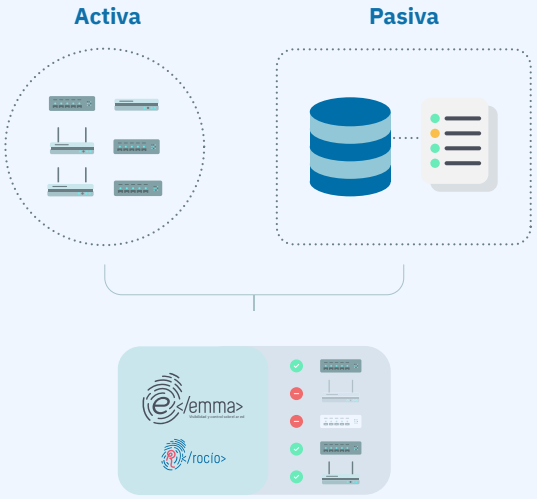
Cumplimiento de Forma **Activa** o **Pasiva**

De forma activa

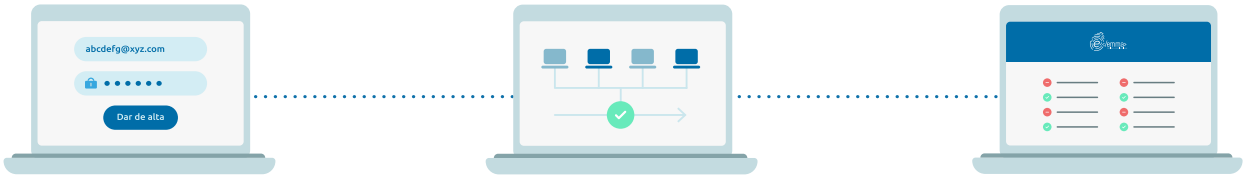
- **EMMA** – Cumplimiento puede lanzar reglas de comprobación de auditorías activas: de manera dinámica (directamente) contra dispositivos de red y de manera estática (primero genera una copia de seguridad de la configuración para posteriormente realizar la comprobación).

De forma pasiva

- También puede realizar comprobaciones de reglas de auditorías de manera pasiva contra un repositorio de configuraciones, sin tener que consultar la electrónica en ningún momento.



Puesta en marcha en **3 pasos**



1. Dar de Alta

1. Un dispositivo de red (por SSH).
2. Un repositorio de configuraciones en el caso de una comprobación pasiva (por SCP).

2. Definir reglas y lanzar

1. Definir las reglas, grupo de reglas correspondientes para el dispositivo y/o grupo de dispositivos.
2. Posibilidad de lanzar las comprobaciones en el momento o programarlas.

3. Revisar resultados

1. Desde los cuadros de mando centralizados se muestran los resultados (comprobaciones con éxito, fallos / hallazgos etc.).

Principales beneficios de **EMMA** - Cumplimiento

Centraliza

- Las comprobaciones de toda la electrónica se realizan desde una solución e única interfaz, simplificando y acelerando el trabajo de auditoría.

Automatiza

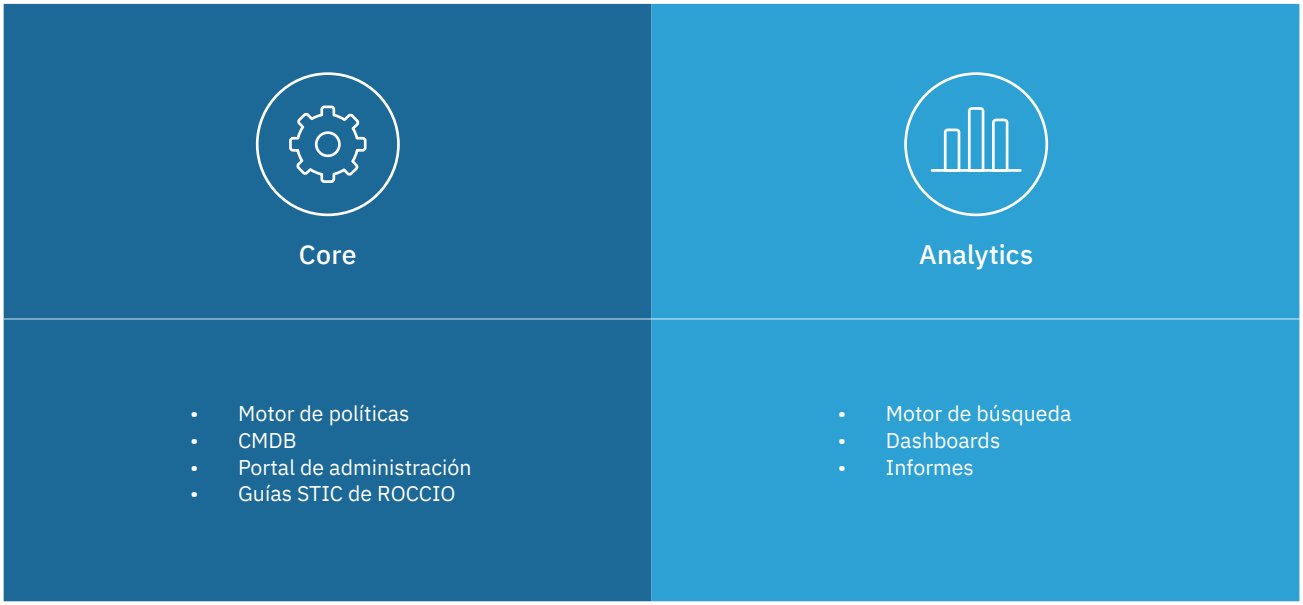
- Las comprobaciones se pueden lanzar bajo demanda o de manera programada para alinearse con las tareas de auditoría.

Facilita: adecuación con el ENS

- Guías STIC / ROCÍO actualizadas e integradas en la lógica de las reglas de EMMA – Cumplimiento.
- Sirve como repositorio de copias de seguridad de configuración de dispositivos de red (medida ENS; MP.INFO.9).
- **Integración con ANA:**
  - Integra los resultados con ANA para que se puedan parametrizar todos los aspectos asociados a los diferentes organismos, también para realizar toda la explotación centralizada de la información: carga de activos, identificación de vulnerabilidades etc.

Arquitectura

La instalación de **EMMA** – Cumplimiento requiere dos máquinas virtuales (Core y Analytics)



emma@ccn-cert.cni.es
www.ccn-cert.cni.es