



II ENCUENTRO DEL ENS

DIEZ AÑOS DE NUEVOS
RETOS Y SOLUCIONES

Taller Acceso Remoto y Vigilancia

Caso en Universidad de Sevilla y Diputación de León



En colaboración con:



Índice

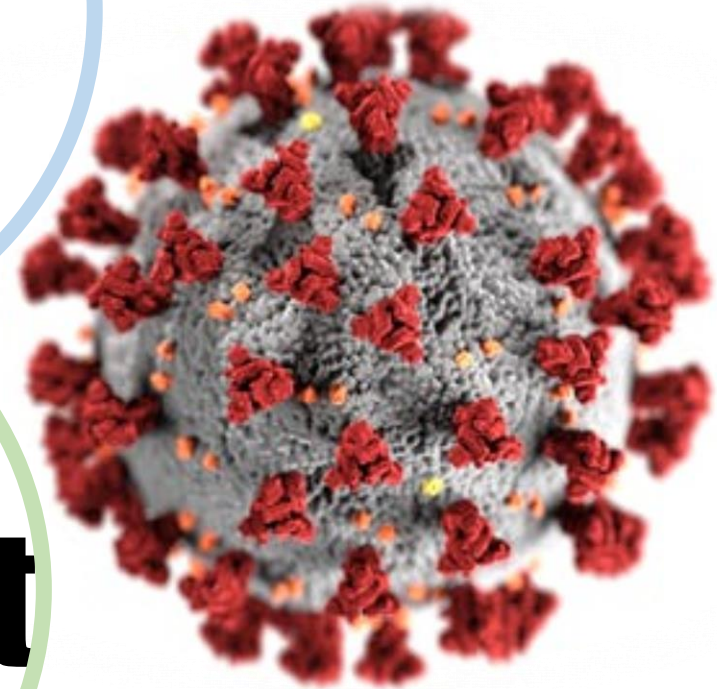
1. Nuevos Retos
2. Acceso Remoto y Vigilancia en el ENS
3. EMMA: Vigilancia sobre la red
4. CSA, partner Certificado
5. Caso de la Universidad de Sevilla
6. Caso de la Diputación de León
7. Preguntas

Nuevos retos



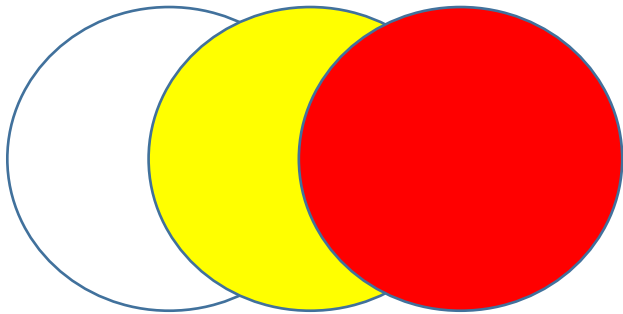
Transformación
Digital

Zero Trust

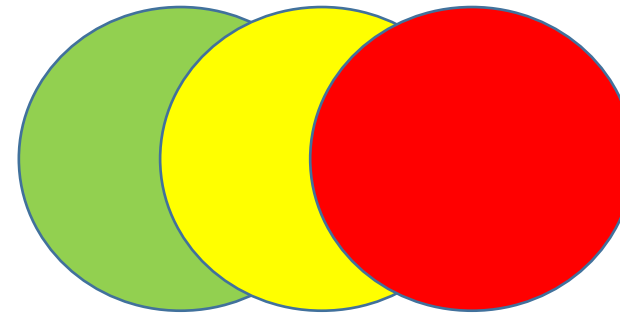


Acceso Remoto y Vigilancia en el ENS

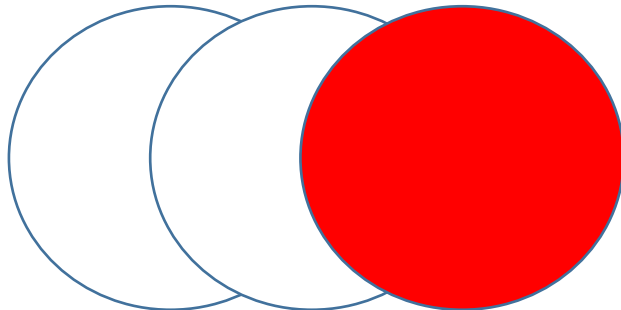
mp.com.2
Protección de la confidencialidad



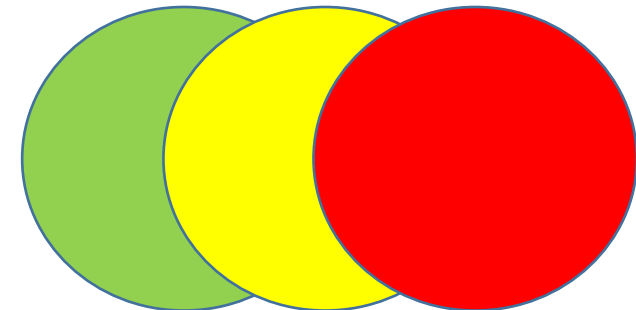
mp.com.3
Protección de la autenticidad e integridad



op.pl.5
Componentes Certificados

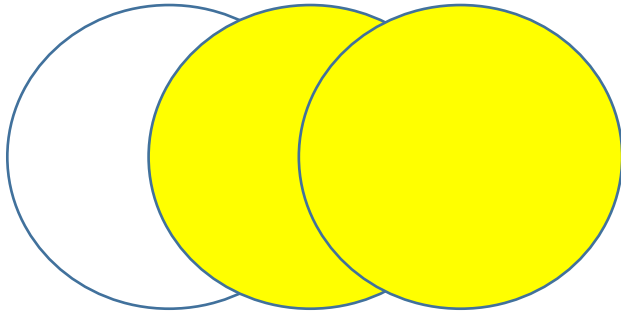


op.acc.5
Mecanismo de autenticación

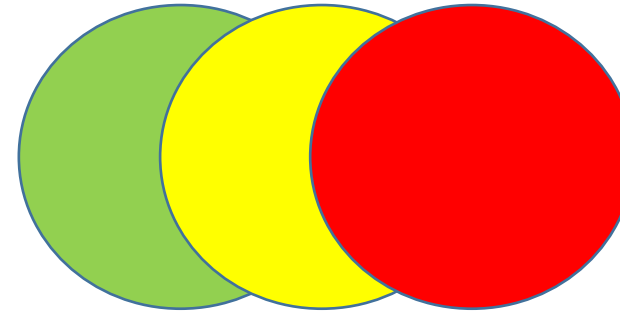


Acceso Remoto y Vigilancia en el ENS

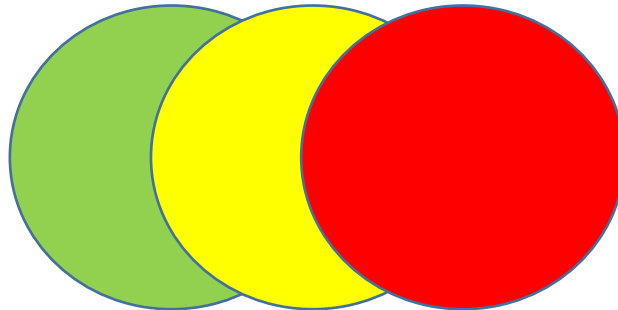
op.mon.1
Detección de intrusión



op.mon.2
Sistema de métricas



op.mon.3
Vigilancia



EMMA Vigilancia sobre la red



Necesidades actuales en el cliente y tendencias

¿Por qué Emma y EMMA-VAR?

- ¿Tengo visibilidad de todo lo que hay conectado en mi red?
- ¿Están los equipos de mis usuarios con un nivel mínimo de seguridad?
- Si alguien externo se tiene que conectar a mi red, ¿puede hacerlo?
- ¿Tengo mi electrónica asegurada?
- Ahora que el trabajo desde casa ha aumentado, ¿como deben conectarse los usuarios a la red corporativa?
-



Módulos de EMMA



Labor del Partner Certificado

- Definir junto con el cliente, y en base a sus requerimientos los módulos de EMMA que mejor se adaptan a sus necesidades
- Colaborar con el CCN cuando recibe la petición de un organismo sobre EMMA, EMMA-VAR
- Prestar los servicios de operación y soporte de la solución. Siempre de la mano del soporte del nivel 3 que da el fabricante.

¿Podemos ayudarte?

Carmen Núñez

dn.emma@csa.es



Características del Proyecto llevado a cabo en la Universidad de Sevilla



Pablo L. Tenorio (pablo@us.es)

Jefe de Sección de Redes.

Área de Comunicaciones.

Servicio de Informática y Comunicaciones.

Universidad de Sevilla

Contexto:

En cuanto al número potencial de usuarios de esta universidad:

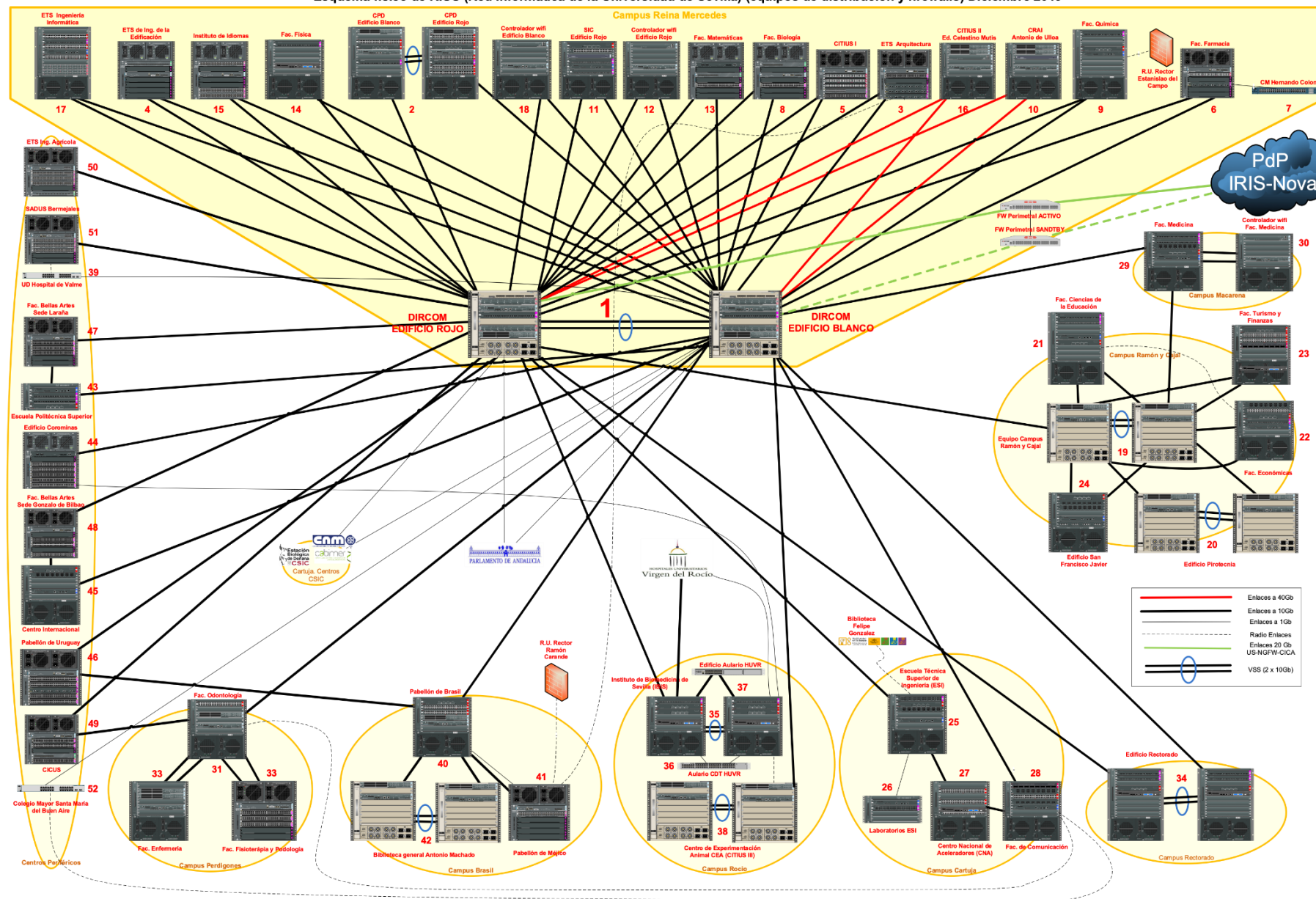
- **70.000** alumnos,
- **32** centros universitarios (entre propios y adscritos),
- **133** departamentos, en los cuales trabajan unos
- **4.200** docentes e investigadores (**PDI**)
- **2.600** compañeros del **P**ersonal de **A**dministración y **S**ervicios (**PAS**)

Respecto a la red universitaria (**RIUS**) también podemos hablar de números:

- **1100** conmutadores, tanto de distribución como de acceso.
- **50.000** puertos cableados de usuario.
- **1.800** puntos de acceso inalámbrico.

El esquema!!

Esquema físico de RIUS (Red Informática de la Universidad de Sevilla) (equipos de distribución y firewalls) Diciembre 2019



Nuestro problema:

Redes Privadas IPv4:

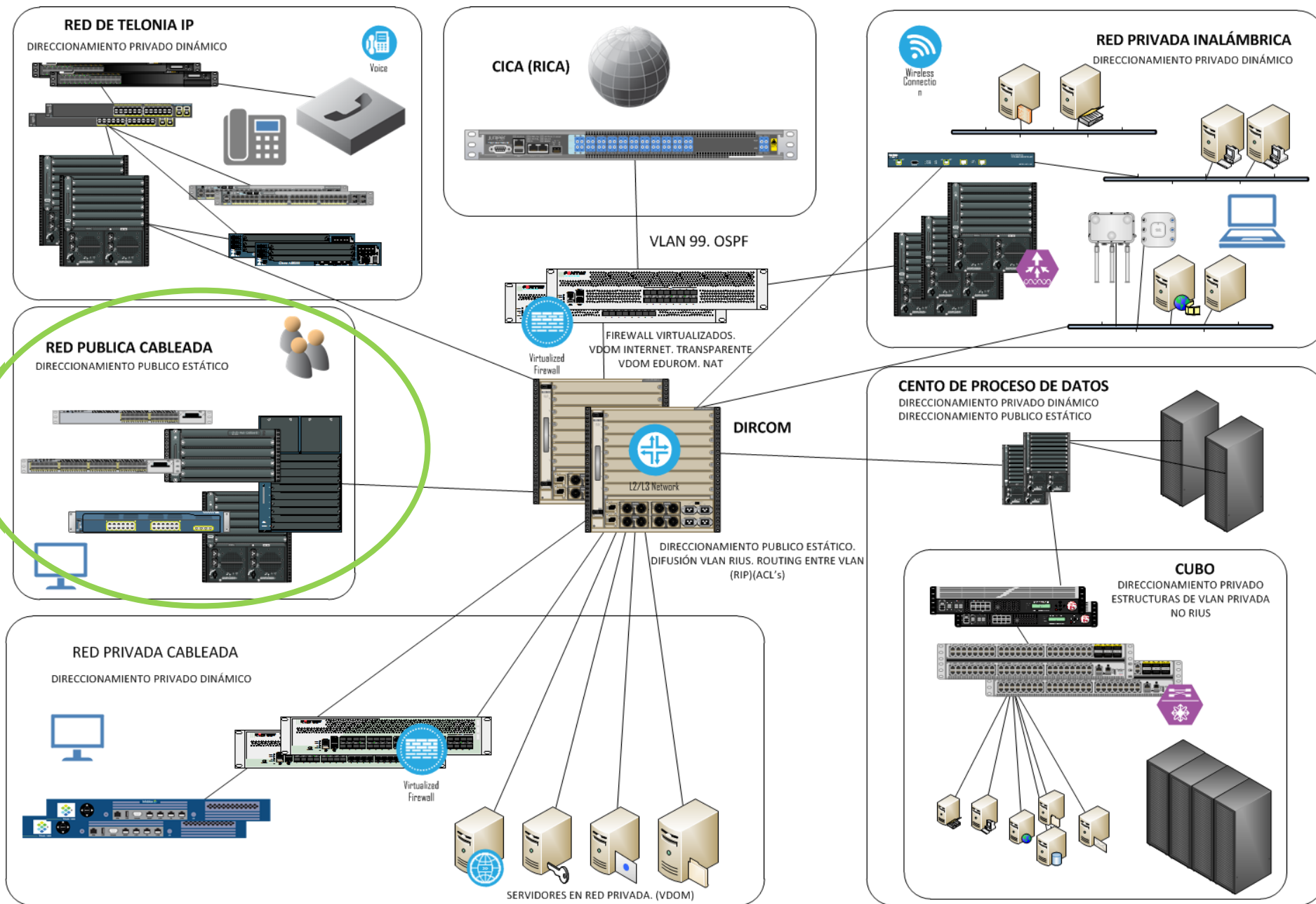
Aulas Informáticas, Red Inalámbrica, Telefonía IP, Data Center, IoT.

- **380.000** posibles direcciones privadas
- Aulas Informáticas, Red Inalámbrica, Telefonía IP, Data Center, IoT.

Redes Públicas IPv4:

- **16.616** posibles direcciones IPv4 públicas. (es menos del 5% del direccionamiento total)
- **15.120** asignadas (90%)
- Redes definidas por servicios (Secretarías de centros, Bibliotecas, Mantenimiento)
- Redes asociadas a centros (Fac. Física, ETSI Informática, etc...)

El otro esquema:



RED INFORMÁTICA DE LA UNIVERSIDAD DE SEVILLA (RIUS)

Nuestra necesidad:

Asegurar el tráfico en nuestras redes y con ellos adaptarnos a Esquema Nacional de Seguridad (ENS)

Valores actuales:

- Cortafuegos perimetral de nueva generación.
- Cortafuegos interno que protege el germen de red privada.

Principales carencias:

- Falta de un conocimiento exhaustivo de los dispositivos que pueblan nuestra red.
- Imposibilidad actual de controlar la naturaleza de los accesos en nuestra red.
 - Dispositivos corporativos (no plafaformados)
 - BYOD

Solución:

EMMA



El famoso ROSCO:

- CSA nos presenta la solución.
- CCN, EMMA, Open Cloud Factory.....
- En el momento de la toma de contacto, el acceso VPN no era una necesidad, ya que está cubierto con una solución OpenVPN propia de la Universidad.
- El PoC de OpenNAC se instala el miércoles 11 de Marzo!.

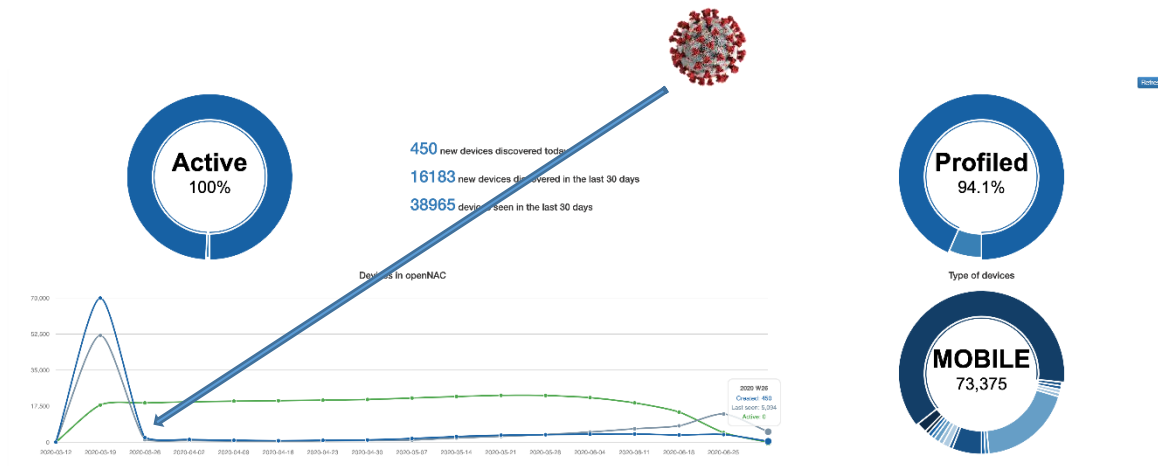
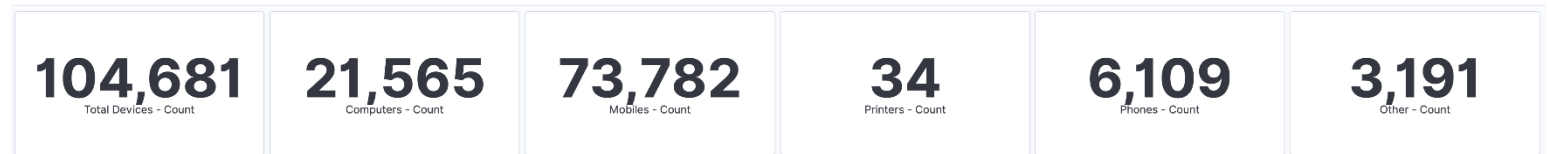


OpenNAC:

Visibilidad :

Más de 100.000 dispositivos (pre Covid-19) :

Perfilado de dispositivos :



- El COVID-19 lo cambia todo.

EMMA-VAR:

Oportunidad:

- Aprovechamos la plataforma del PoC de OpenNAC y crecemos hasta EMMA-VAR de forma natural.

Adaptación:

- Nuestro servicio de VPN dispone al usuario en la red que demanda con el direccionamiento **público** de esa red, por lo que la regulación se realiza en nuestro entorno de red (reglas, políticas, etc..)
- EMMA-VAR usa un direccionamiento **privado** para el cliente, y la regulación de acceso a los recursos de nuestra red universitaria se realizan en el finalizador de túneles.

Vicisitudes:

- Conflictos del agente con un EDR en pruebas (Panda-Cytomic).
- Coexistencia de nuestro cliente Open y del agente de EMMA-VAR.
- Para cliente NO Windows, aún no está desarrollado el agente. La solución cliente Open funciona correctamente, pero deja otras facetas indispensables, a realizar (tenemos un parque elevado de NoW)

Fortalezas:

- **Autenticación robusta:** Perfilado y autenticación mediante nuestro LDAP corporativo, y doble FA (OTP).
- **Perfilado continuo y en tiempo real:** Verificación de **tags** que definen los parámetros mínimos de cumplimiento por parte del usuario (antivirus, firewall, etc..)
- **Motor de políticas:** Permisos de acceso del usuario asociado a su identidad, postura de seguridad del equipo, horario de conexión, tipo de dispositivo, tipo de dispositivo de red, tipo de vlan, etc...

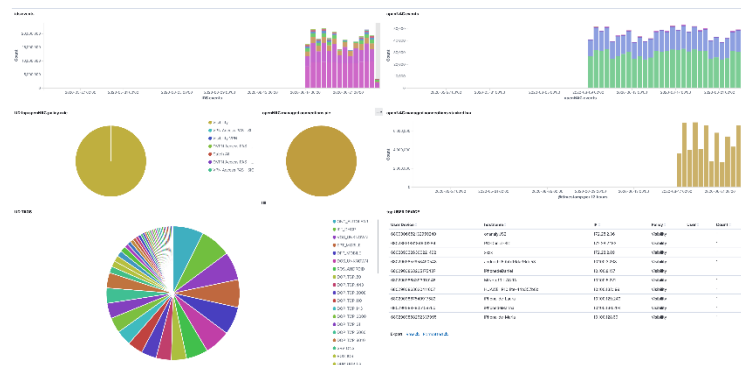


882 898

open nac



| | | | |
|---------------------------|---------------------|----------------------|-----------------|
| General | | | |
| Area | OPN-Servicio de Log | Estado | OK |
| Comentarios | | Estado | NO SE PUEDE VER |
| Modulo | ACTIVAR BLOQUEO | | |
| Propiedades Time | | | |
| Time | NO SE PUEDE VER | | |
| Propiedades User | | | |
| Usuario | | Usuario | |
| Usuario de seguridad (ID) | 11111111 | Usuario de seguridad | |
| Propiedades User Device | | | |
| Device | | Device | |
| Device de seguridad | | Device de seguridad | |
| Propiedades Human Device | | | |
| Propiedades Device | | | |
| Modelo | NO | Modelo | NO |
| Resolución | NO | Resolución | NO |
| Resolución | NO | Resolución | NO |
| Resolución | NO | Resolución | NO |
| Resolución | NO | Resolución | NO |
| Propiedades Device | | | |
| Modelo | NO | Modelo | NO |
| Resolución | NO | Resolución | NO |
| Resolución | NO | Resolución | NO |
| Resolución | NO | Resolución | NO |
| Resolución | NO | Resolución | NO |



- **Vigilancia del sistema:** Monitorización del tráfico y del comportamiento entre el usuario y el sistema

Conclusiones:

- Muy completa herramienta de conocimiento, control de red y acceso seguro.
- **EMMA-VAR** esta auspiciado por el **CCN-CERT**.
- El equipo humano de **Open Cloud Factory** y de **CSA** han demostrado un alto grado de implicación y de especialización técnica.
- Sería de gran importancia avanzar en el agente para dispositivos NO Windows y en compatibilizar el método de autenticación con el uso de SSO.
- Es necesario para nosotros seguir avanzando en el resto de partes del "rosco", segmentación, *BYOD*, compliance, gestión de invitados, pero la percepción del producto ha sido **OPTIMA**.
- Muchas gracias a todos por vuestra atención!.

Características del Proyecto llevado a cabo en la Diputación de León



Javier de la Villa Regueiro
Jefe de Explotación del
Servicio TIC de la Diputación
de León



Situación de partida de la Diputación de León

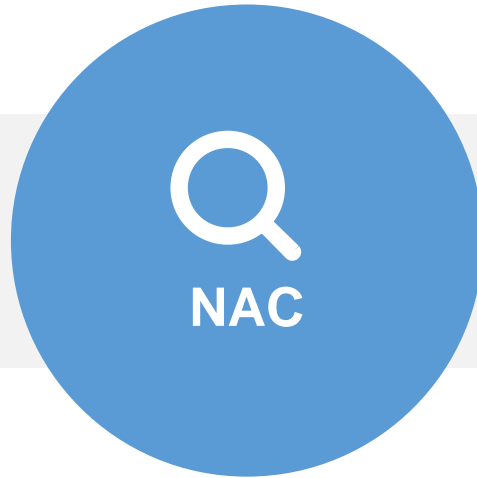
- 27 Sedes de la Diputación en la Provincia interconectadas o en proceso de interconexión.
- 80 unidades de electrónica de red (switches).
- 105 unidades electrónica Wifi (AP, controladora wifi,...).
- 2 Firewall de seguridad perimetral – toda la navegación centralizada.
- \approx 2.000 dispositivos en red local: PCs, equipos de impresión, terminales VoIP, etc.
- \approx 100 equipos portátiles deslocalizados, en redes ajenas a la Diputación.



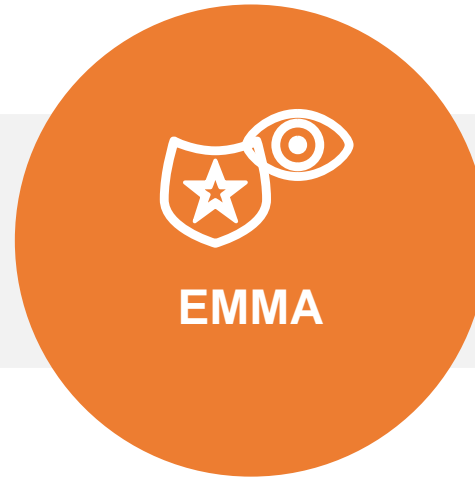
Incertidumbre en la gestión de la red

- Carencias de gestión integral de la electrónica de red, dispositivo a dispositivo.
- Proceso complejo de inclusión, manual, de un equipo nuevo en la red local: alta en DHCP, configuración de switches y puertos para determinar la VLAN en la que se aísla, etc.
- Dependencia total con el proveedor actual del proyecto de comunicaciones integrales para la gestión de la red.
- ¿Cuánta electrónica de red tenemos desplegada realmente? ¿Se ha visto modificada desde la último esquema documentado? ¿Se encuentra bastionada y actualizada? Sin una base de datos automática.
- ¿Quién se está conectado a la red? ¿Alguna persona ha conectado algún equipo ajeno a la Diputación en la red local de una sede remota?

Selección de la solución NAC: EMMA



¿Solución NAC, para el control de acceso a la red?

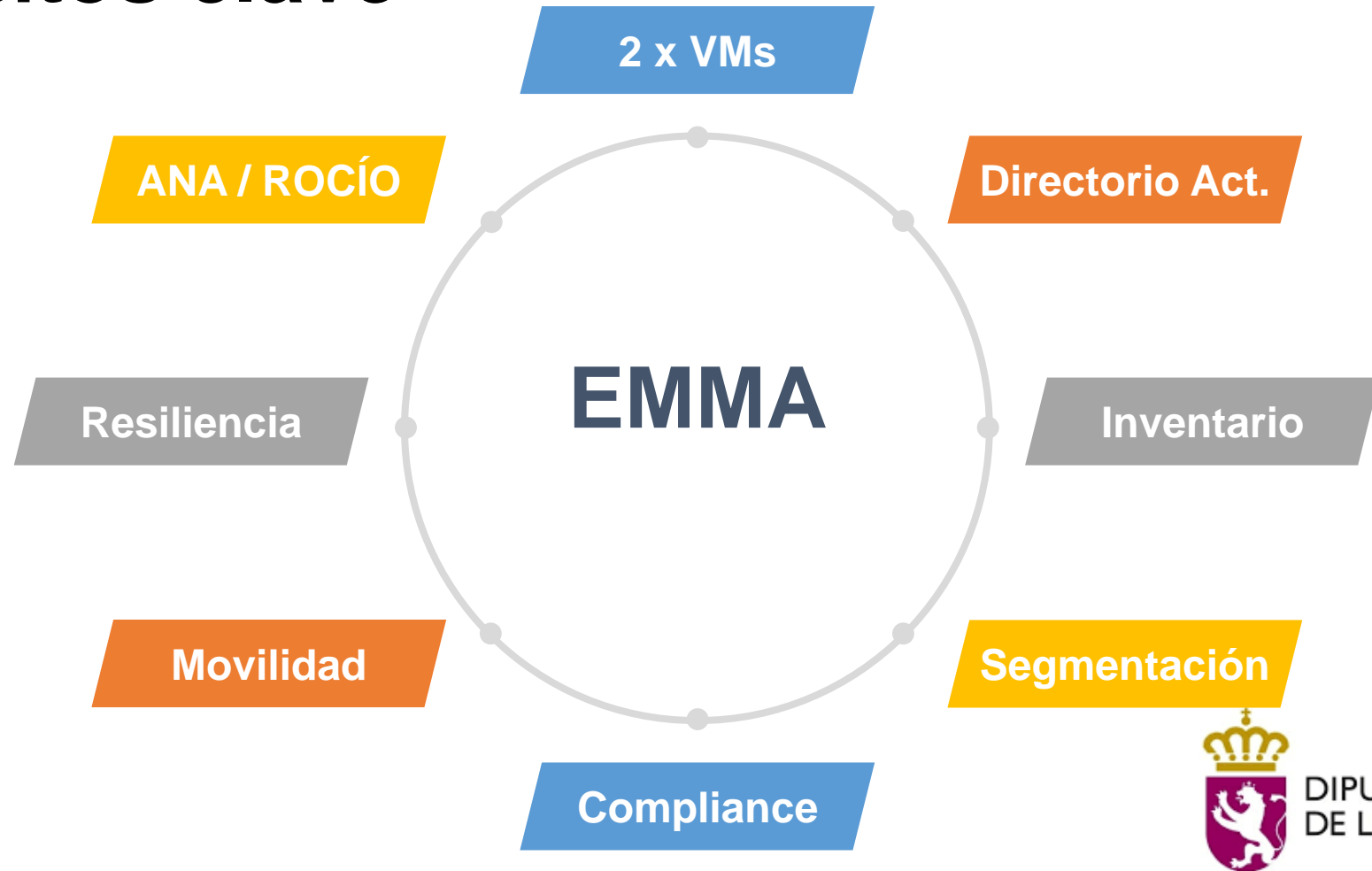


Modular. Adecuación al ENS.



Centro Criptológico Nacional - solución a medio largo plazo.

Arquitectura de la solución y requisitos clave

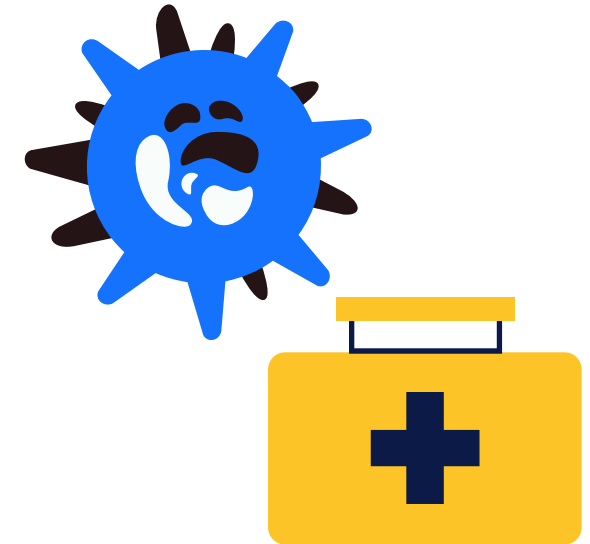


Y llegó el COVID-19

Nuevas necesidades de trabajo a distancia antes no planteadas

- Implantación ágil de conexiones seguras (> 250).
- PC particular del empleado conforme a unos mínimos de seguridad
 - Actualizaciones del SO del PC cliente (ej. Windows update).
 - Antivirus y EDR.
- Heterogeneidad de sistemas operativos y versiones de los mismos.

Posible solución: Modulo EMMA de Vigilancia de Accesos Remotos



Visión de futuro

- Solución de control de acceso al trabajo a distancia de la Diputación de León.
- Solución horizontal, prestada por la Diputación, que puedan adoptar los municipios de la provincia en materia de seguridad de la información y acceso al trabajo a distancia



¿Preguntas?



emma@ccn-cert.cni.es



II ENCUENTRO DEL ENS

DIEZ AÑOS DE NUEVOS
RETOS Y SOLUCIONES



En colaboración con:



Muchas gracias.

Estratégicos



Entelgy Innotec
SECURITY

Forcepoint

mobileiron

Estándar



CYTOMIC



ENJOY SAFER
TECHNOLOGY™

gestiona
espublico.

Ingenia



NUTANIX

oesia
grupo

ONE IDENTITY

paloalto
networks

proofpoint.

Pulse Secure®

redtrust
a KEYFACTOR company

S21
GRUPO
Anticipando un mundo
ciberseguro

S21
SEC

Sidertia

STORMSHIELD

tenable



vmware®