UNIVERSIDAD DE GRANADA

CSIRC

Programación de Red Orientada a la: Ciberseguridad y Gestión Automatizada"

VNiVERSiDAD D SALAMANCA

ANTONIO RUIZ MOYA

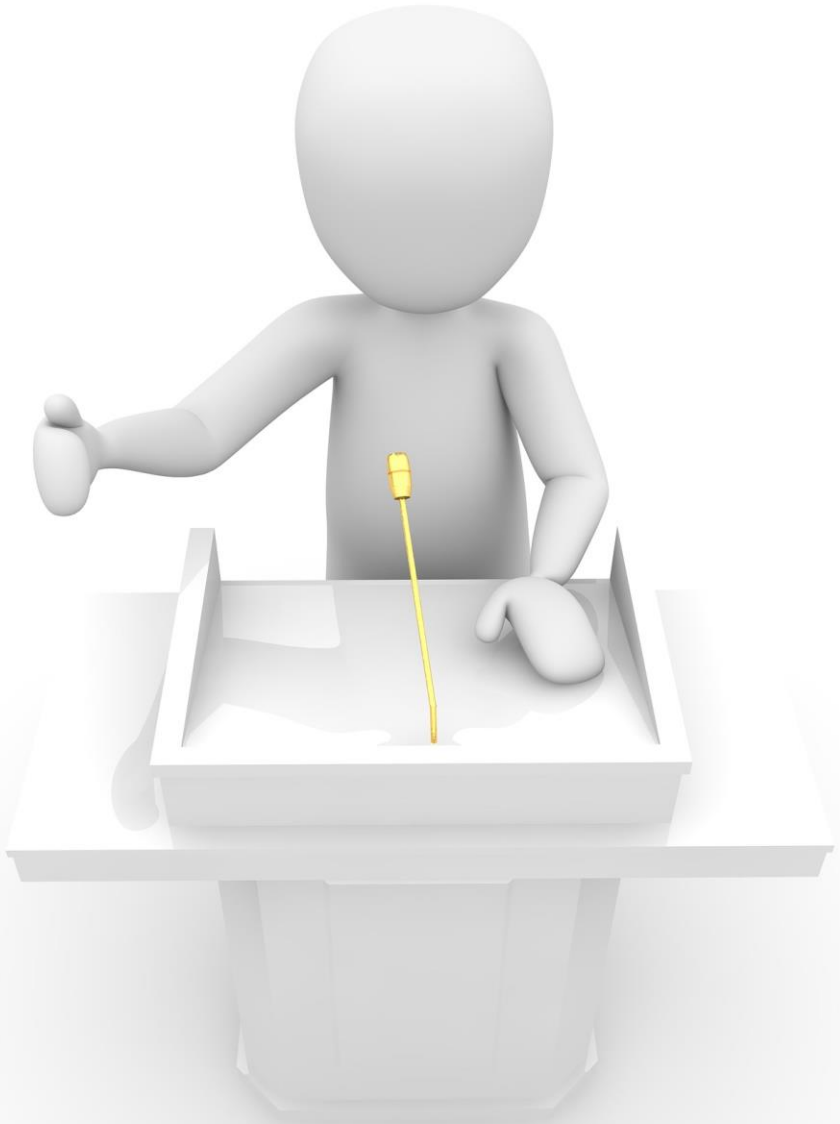
ARUIZ@UGR.ES

SERVICIO DE REDES Y COMUNICACIONES

CENTRO DE SERVICIOS DE INFORMÁTICA Y REDES DE COMUNICACIÓN

UNIVERSIDAD DE GRANADA

Hospedería Arzobispo Fonseca de la Universidad de Salamanca, 9 de mayo de 2018



¿Cuál es la problemática de partida?

¿ PROC PROG ?

¿Cuál es la problemática de partida?

¿Cuál es la problemática de partida?

ISO

ITIL

¿Por qué PROC y PROG?

GESTIÓN DE LOS CAMBIOS

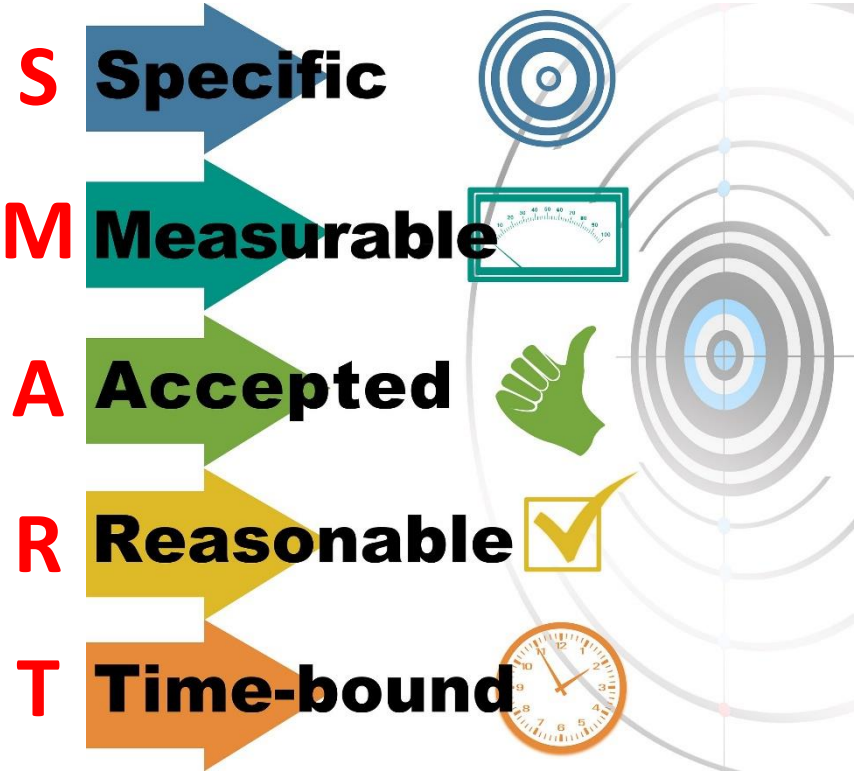
CIBERSEGURIDAD

GESTIÓN DE RED

¿Por qué PROC y PROG?

MODELO DE GESTIÓN DE LOS CAMBIOS EN **RedUGR**

FILOSOFÍA DE DESARROLLO ORIENTADO A LA GESTIÓN DE LA SEGURIDAD Y GESTIÓN DE RED



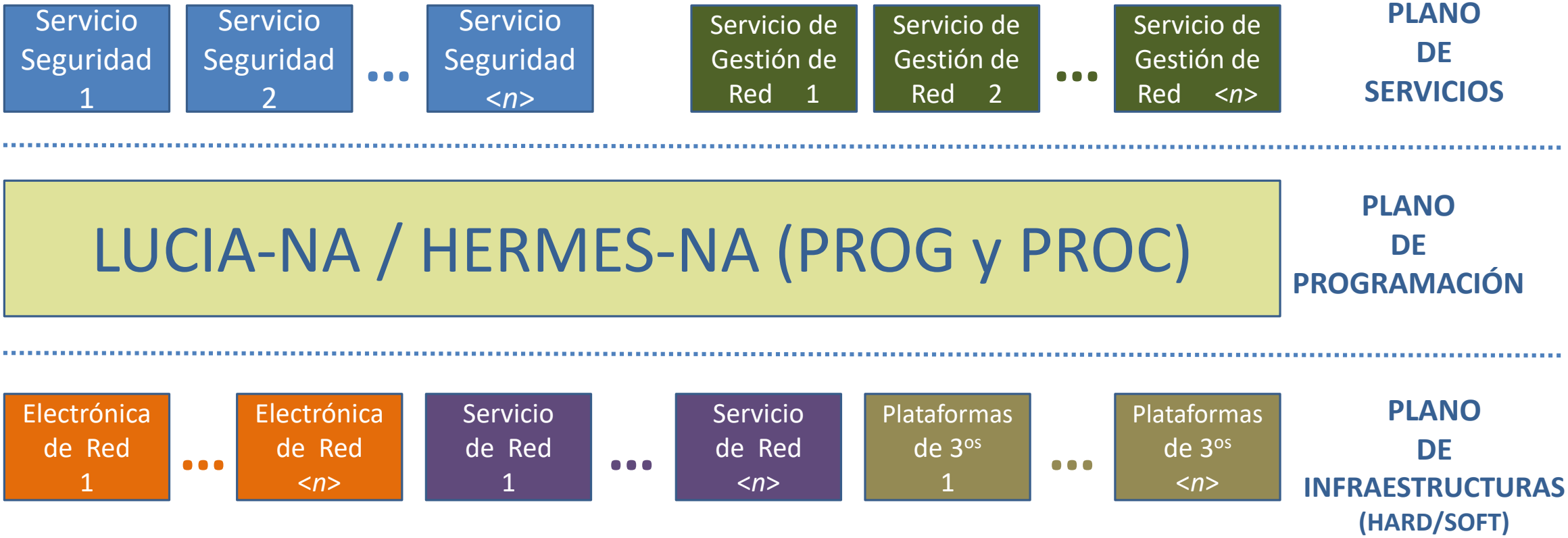
UNIVERSIDAD DE GRANADA

CSIRC

¿Por qué PROC y PROG?

MODELO DE GESTIÓN DE LOS CAMBIOS EN **RedUGR**

FILOSOFÍA DE DESARROLLO ORIENTADO A LA GESTIÓN DE LA SEGURIDAD Y GESTIÓN DE RED



UNIVERSIDAD DE GRANADA

CSIRC

¿Por qué PROC y PROG?

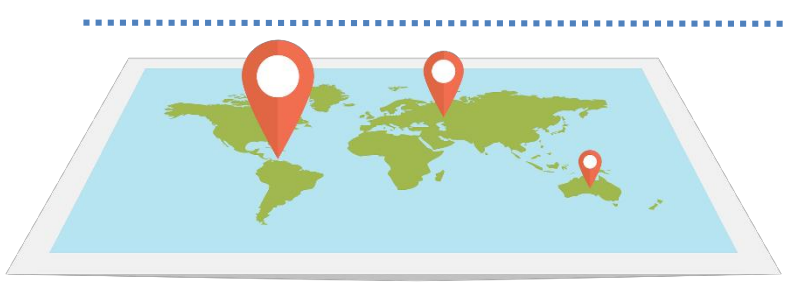
MODELO DE GESTIÓN DE LOS CAMBIOS EN **RedUGR**

MEDIANTE LA PROGRAMACIÓN ORIENTADA A LA GESTIÓN DE LA SEGURIDAD Y GESTIÓN DE RED

Servicio Seguridad 1 | Servicio Seguridad 2 | ... | Servicio Seguridad <*n*>

Servicio de Gestión de Red 1 | Servicio de Gestión de Red 2 | ... | Servicio de Gestión de Red <*n*>

PLANO DE SERVICIOS



PLANO DE PROGRAMACIÓN **LUCIA/HERMES (PROC&PROG)**

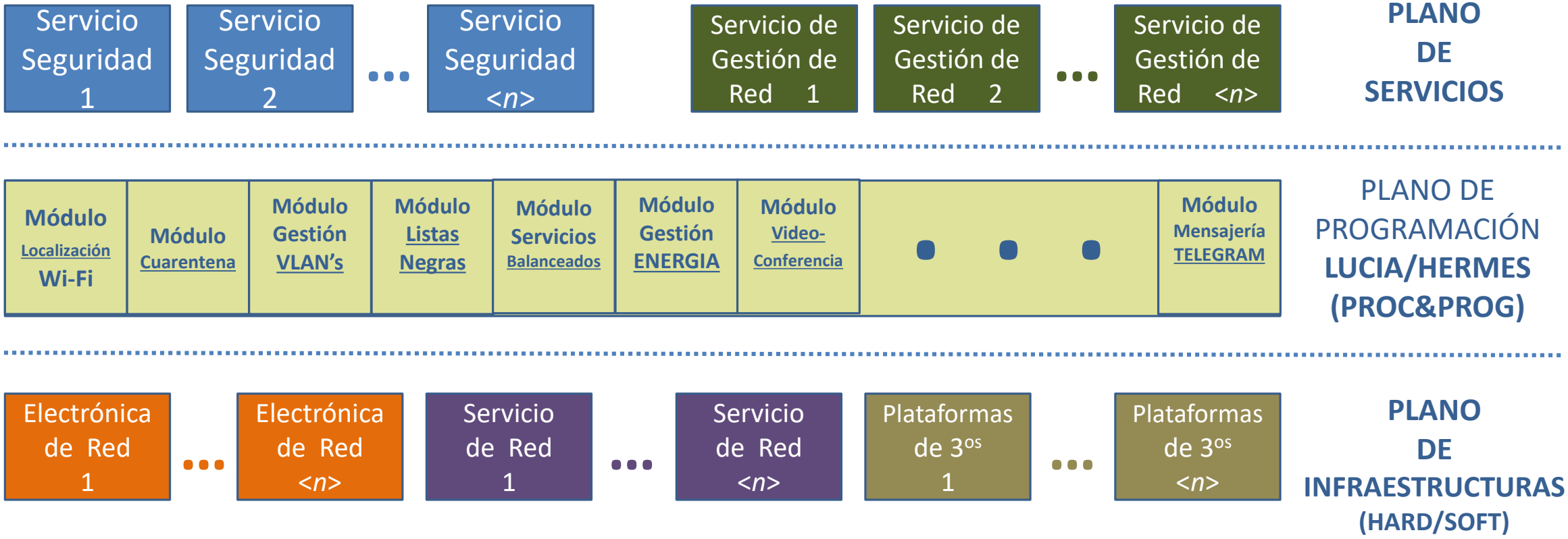
Electrónica de Red 1 | ... | Electrónica de Red <*n*> | Servicio de Red 1 | ... | Servicio de Red <*n*> | Plataformas de 3os 1 | ... | Plataformas de 3os <*n*>

PLANO DE INFRAESTRUCTURAS (HARD/SOFT)

¿Por qué PROC y PROG?

MODELO DE GESTIÓN DE LOS CAMBIOS EN **RedUGR**

MEDIANTE LA PROGRAMACIÓN ORIENTADA A LA GESTIÓN DE LA SEGURIDAD Y GESTIÓN DE RED



Qué veremos

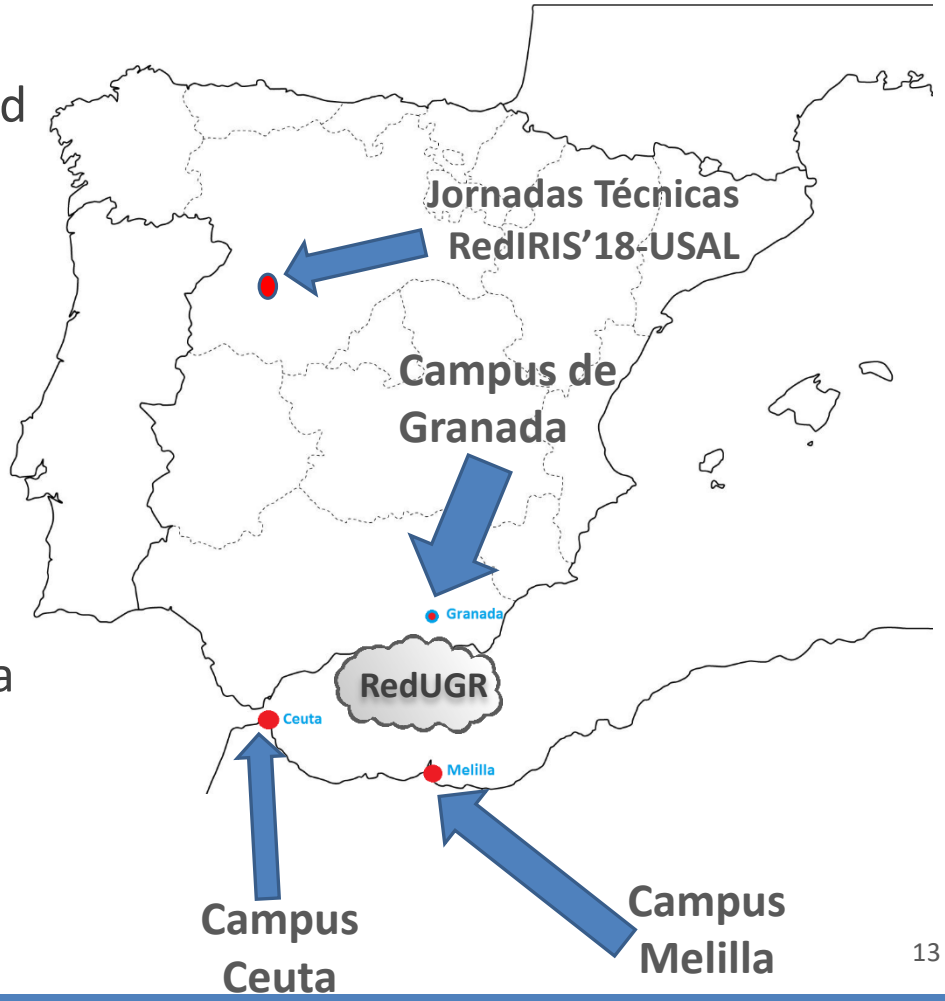
1. Objetivos de Gestión en RedUGR
2. ¿Qué es RedUGR? Infraestructuras y Servicios
3. Sistemas de Gestión LUCIA y HERMES
4. En fase de lanzamiento. Próximamente
5. Referencias
6. Fin

1. Objetivos de Gestión en RedUGR

- **Infraestructuras de Red Universales**
- **Operación de Red Automatizada**
- **Gestión Centralizada de Red**
- **Política de Red Única**
- **Servicios de Red Abiertos**
- **Innovación Tecnológica Continua**

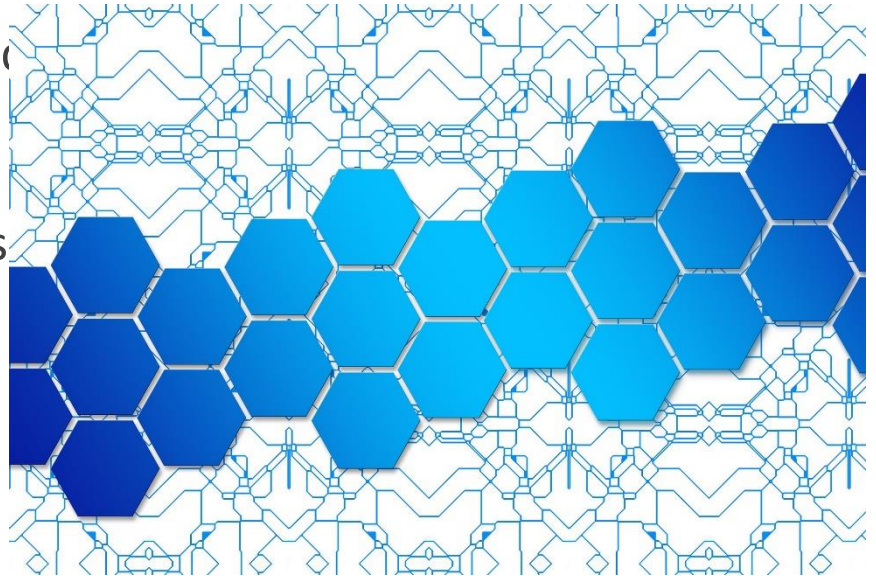
2. ¿Qué es **RedUGR**? Infraestructuras

- Infraestructuras y servicios de Red Globales para toda la Universidad
- 7 Campus Universitarios físicos, 5 en Europa y 2 en África
- 1 Campus Universitario virtual: CVI-UGR (Eduroam)
- 83 Edificios
- 33.000 Nodos de Red físicos
- 85.000 usuarios
- 3.000Km de F/O propia desplegada en Campus de Granada y Melilla
- Núcleo de red HA a 160Gbps, 80Gbps y 20Gbps
- Acceso a Internet HA a 10Gbps



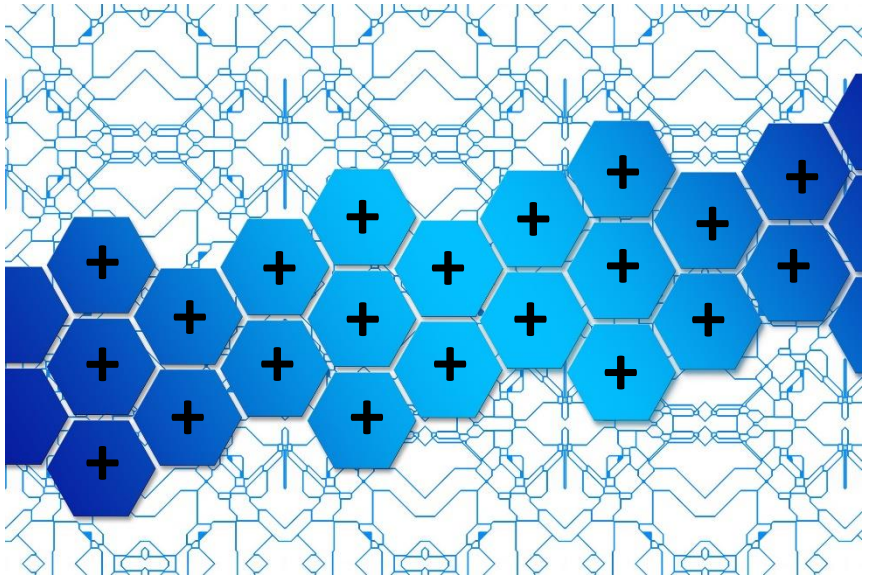
2. ¿Qué es **RedUGR**? Servicios

- Red Inalámbrica Universitaria con 1.500 AP's (orientados a conectividad y próximamente localización), ***EDUROAM-oriented***
- Red de **Videoconferencia** Corporativa con 30 salas físicas y 20 virtuales
- Red de **Control Multimedia** con 230 clases con gestión automatizada
- **Help-Desk** Web on-line y mensajería instántanea
- 144 aulas de **PC's físicas** con 4.200 ordenadores de sobremesa
- Aulas de **PC's virtuales** para trabajo del estudiante desde casa
- Red **VoIP** con 8.000 extensiones telefónicas
- Servicios de **Supercomputación** a través de ALHAMBRA.UGR.es
- Etc.



2. ¿Qué es **RedUGR**? Servicios Plus

- Sistemas de Balanceo de Carga Universitarios. 67 Granjas
- Sistemas de Gestión de Red (Control & Monitorización)
- Gestión de la Seguridad de Red vía:
  - NG-FW
  - NG-NAC
  - Gestión de flujos de red global
  - Captura de tráfico en el núcleo
  - VPN para conectividad exterior
  - Sistema ODBM: PROC + PROG



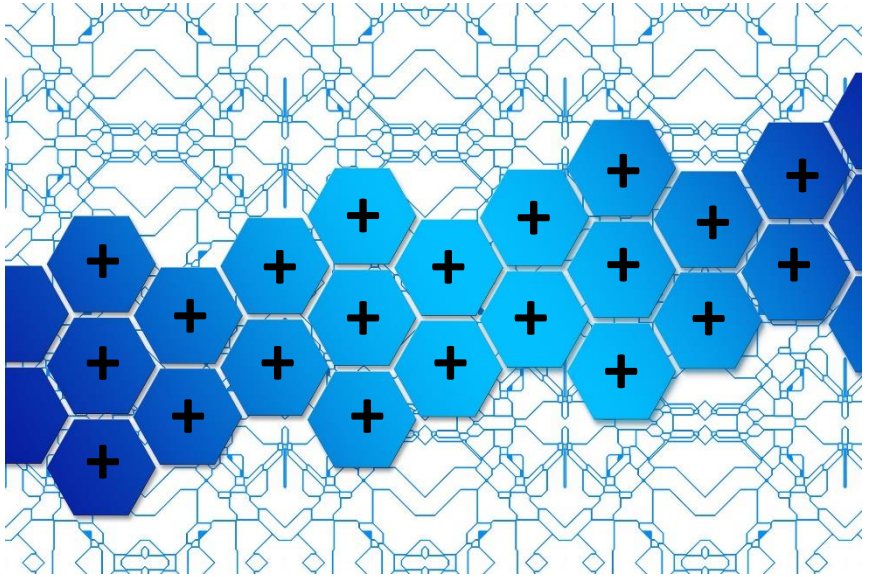
2. ¿Qué es **RedUGR**? Servicios Plus

- Sistemas de Balanceo de Carga Universitarios. 67 Granjas
- Sistema de Gestión de Red (Control & Monitorización)

  Cisco PRIME, Cisco MSE, Cisco CMX, HP-IMC,

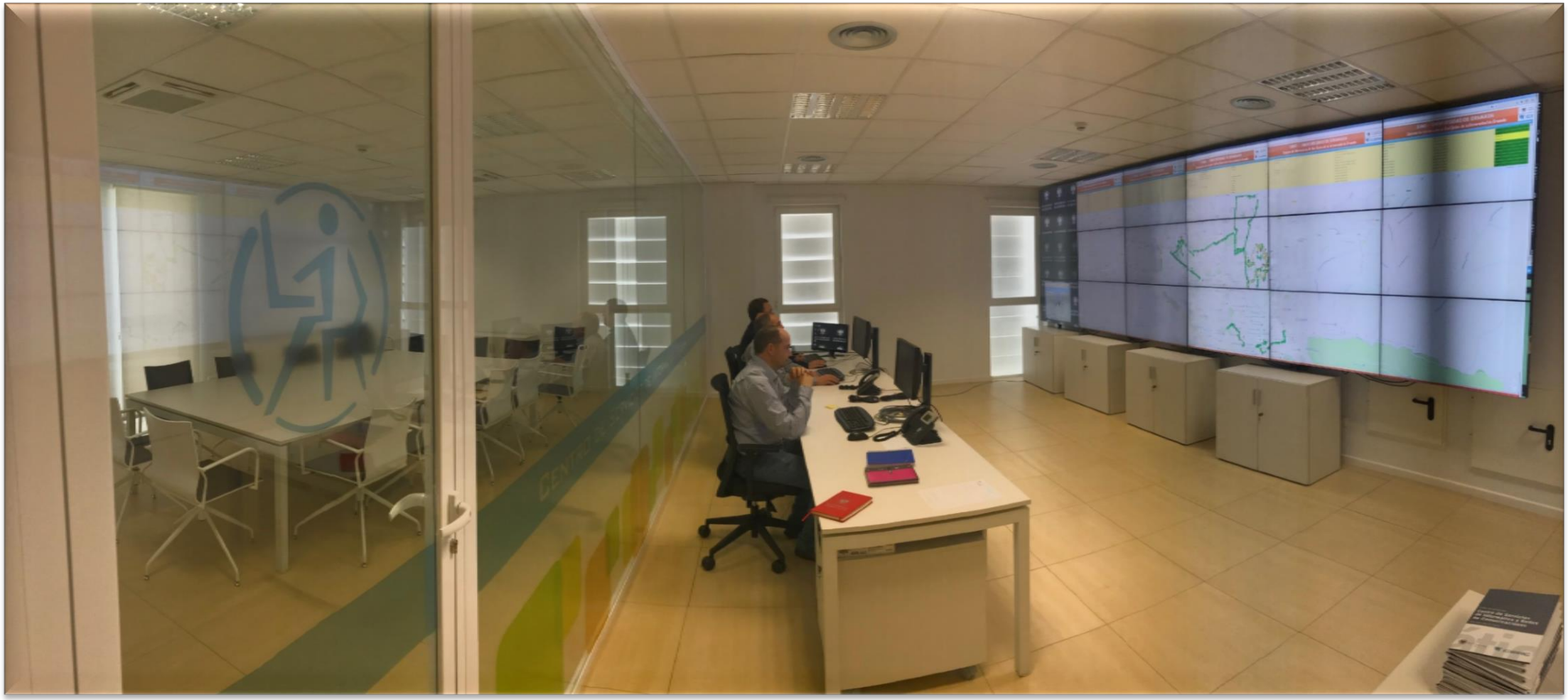
  DESARROLLO PROPIO SRC-UGR (ODBM+SINO)

  Software Libre (Dude, Cacti, MRTG, IRIS,…)

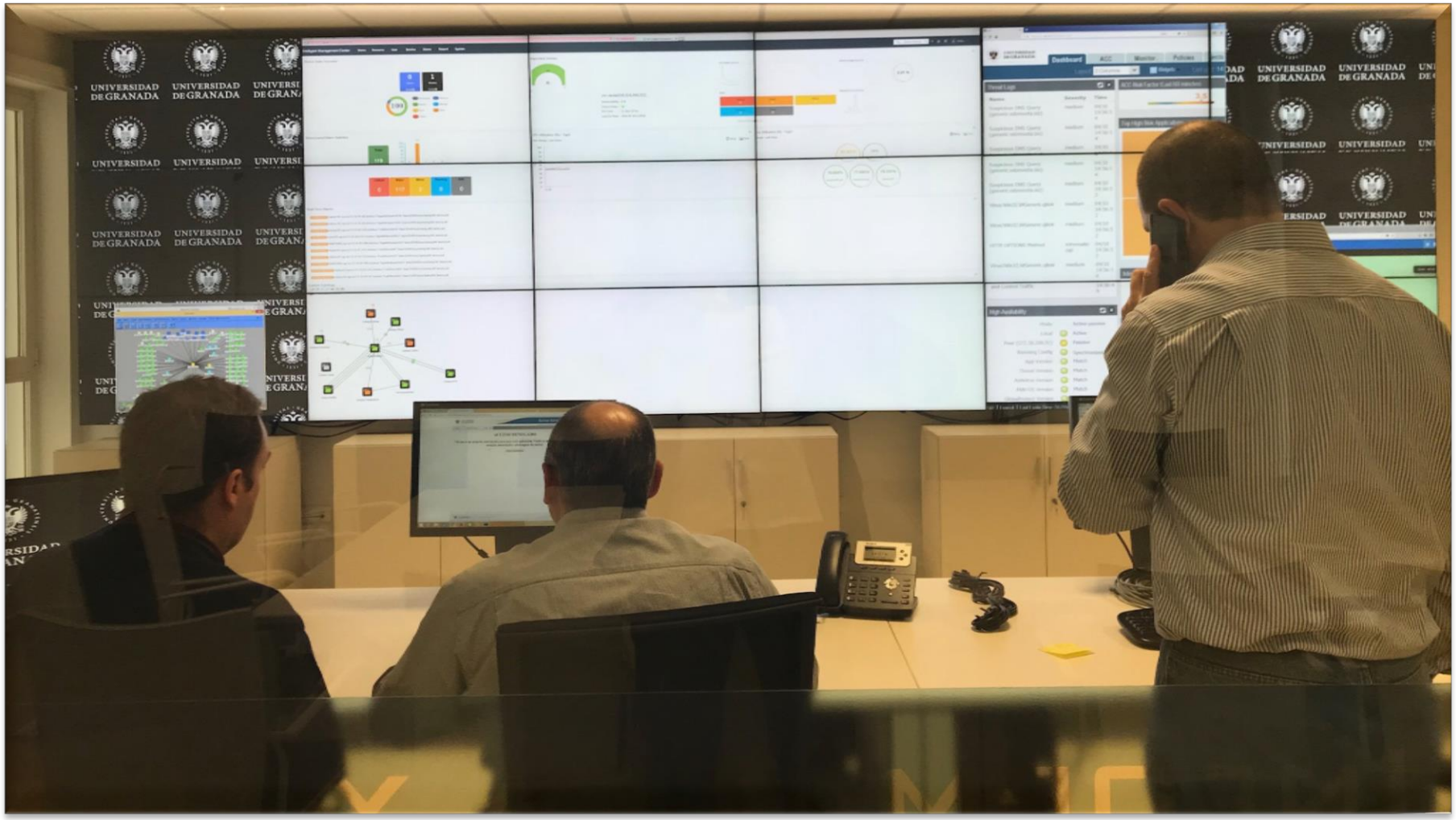


- Gestión de la Seguridad de Red vía:
  - NG-FW …… **PALOALTO NETWORKS**
  - NG-NAC …… **DESARROLLO PROPIO SRC-UGR (ODBM)**
  - Lupa para flujos de red global …… **SCRUTINIZER-Plixer**
  - Captura de tráfico en el núcleo …… **CISCO NAM2**
  - VPN para conectividad exterior …… **CISCO Anyconnect**
  - Sistema ODBM: PROC + PROG …… **DESARROLLO PROPIO SRC-UGR (ODBM)**

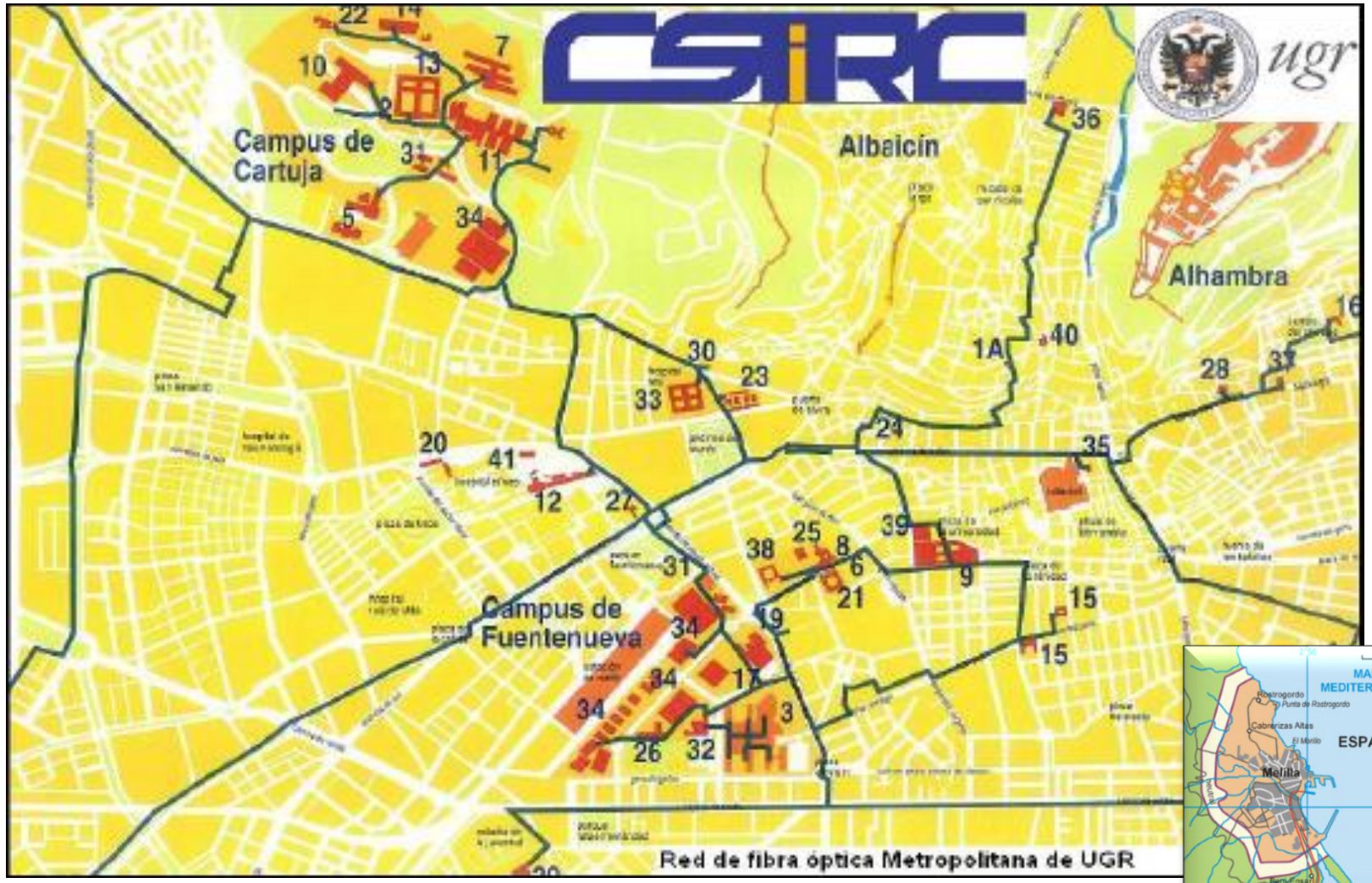
2. ¿Qué es **RedUGR**? Centro de Gestión



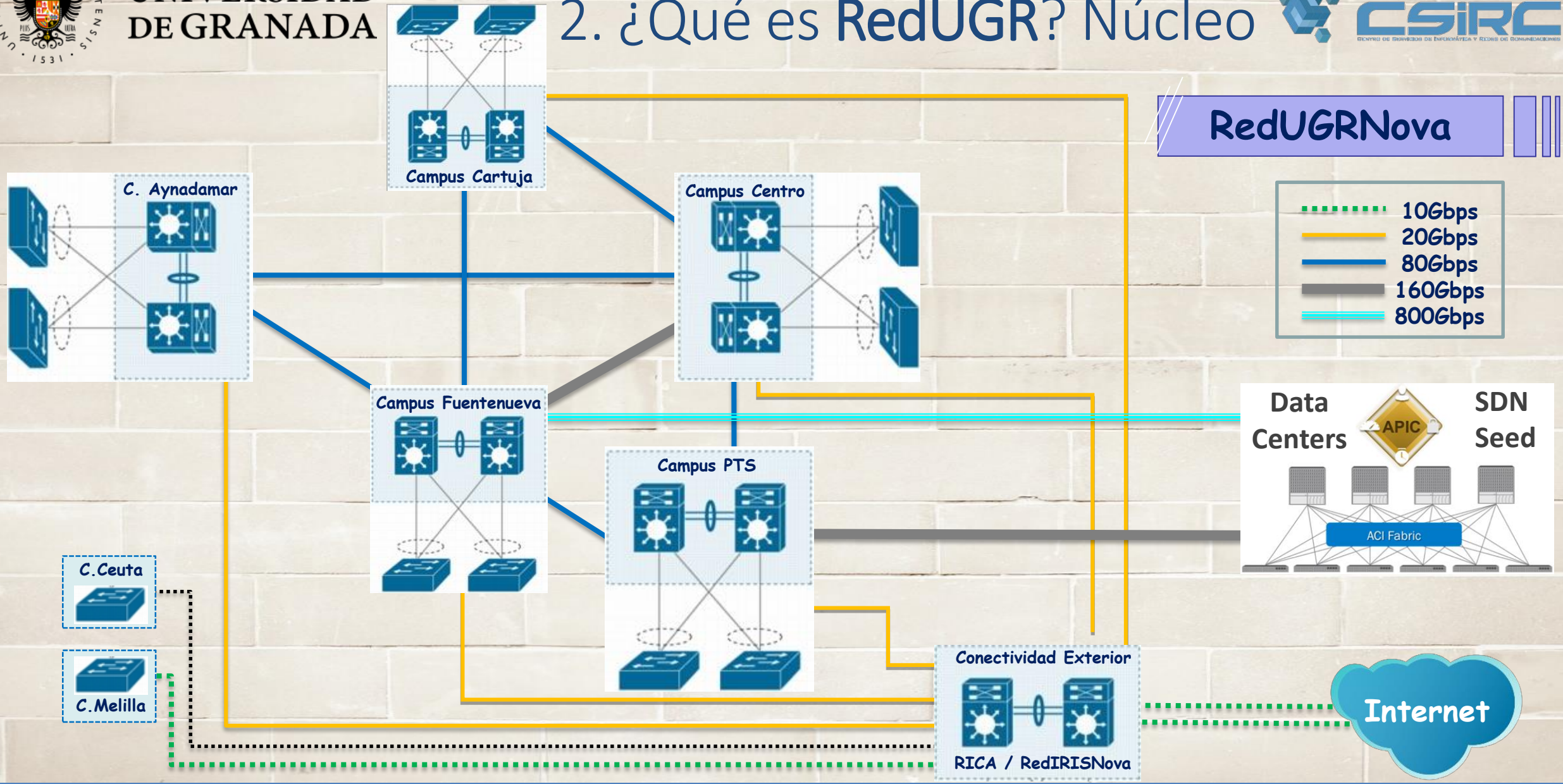
2. ¿Qué es **RedUGR**? Centro de Gestión



2. ¿Qué es **RedUGR**? Red de F/O



2. ¿Qué es **RedUGR**? Núcleo



2. ¿Qué es RedUGR? Núcleo

3. Sistemas de Gestión

LUCIA-NA

GESTIÓN DE RED

HERMES-NA

CIBERSEGURIDAD

UNIVERSIDAD DE GRANADA

CSIRC

Infraestructura de RedUGR-NOVA
(Núcleo, Distribución, Acceso, SDN, NetIoT)

SNMP CLI API

PRIME

MSE

CMX

PA

SCR

IMC

VC VC

Wi-Fi

Conectividad
Localización

API

ODBM
Objects
Data Base
Management
Oracle

LUCIA-NA

HERMES-NA

SQL HTTP

SINO

DNS

Radius

BD Corp. UGR

BD Otros (CLM...)

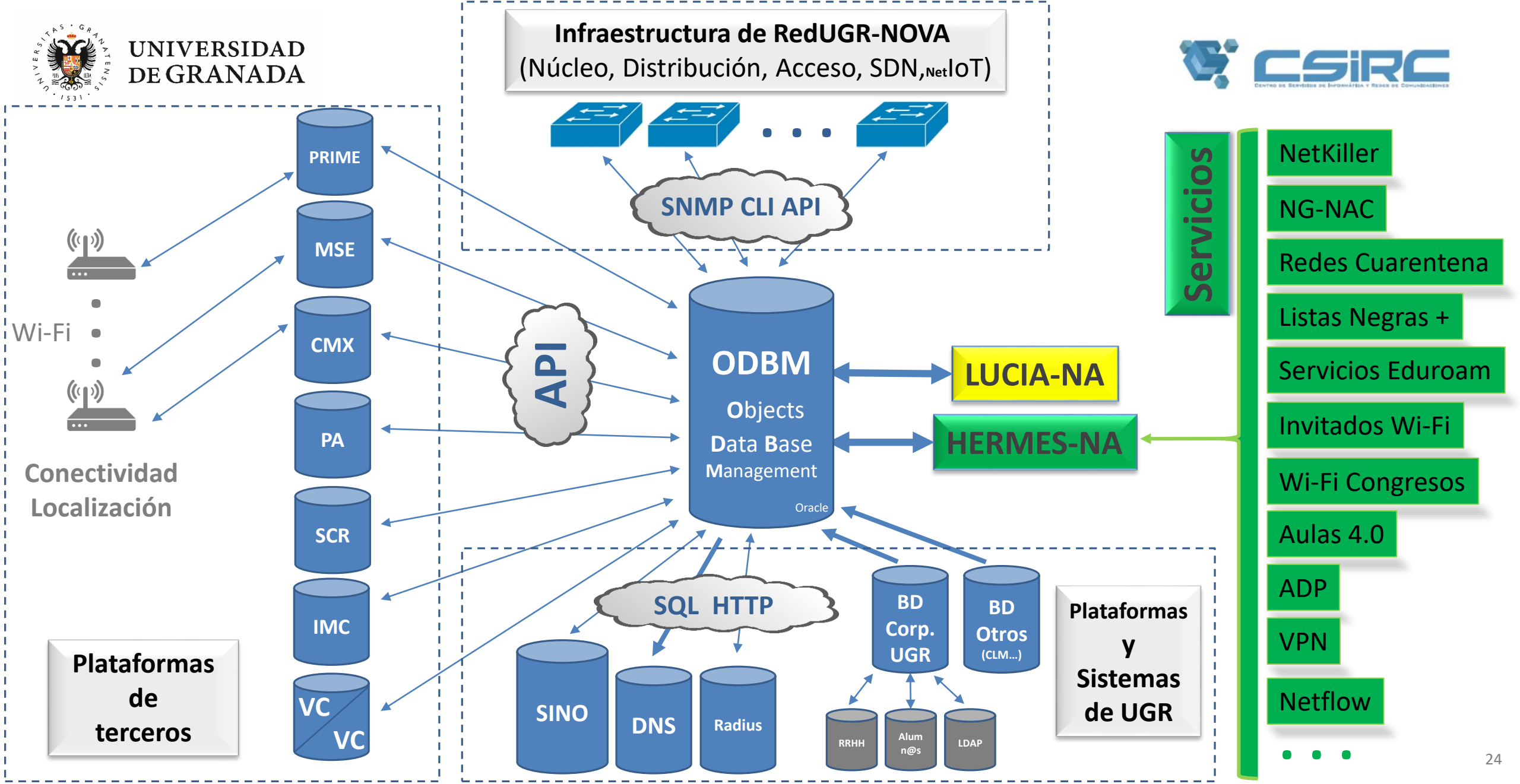
RRHH

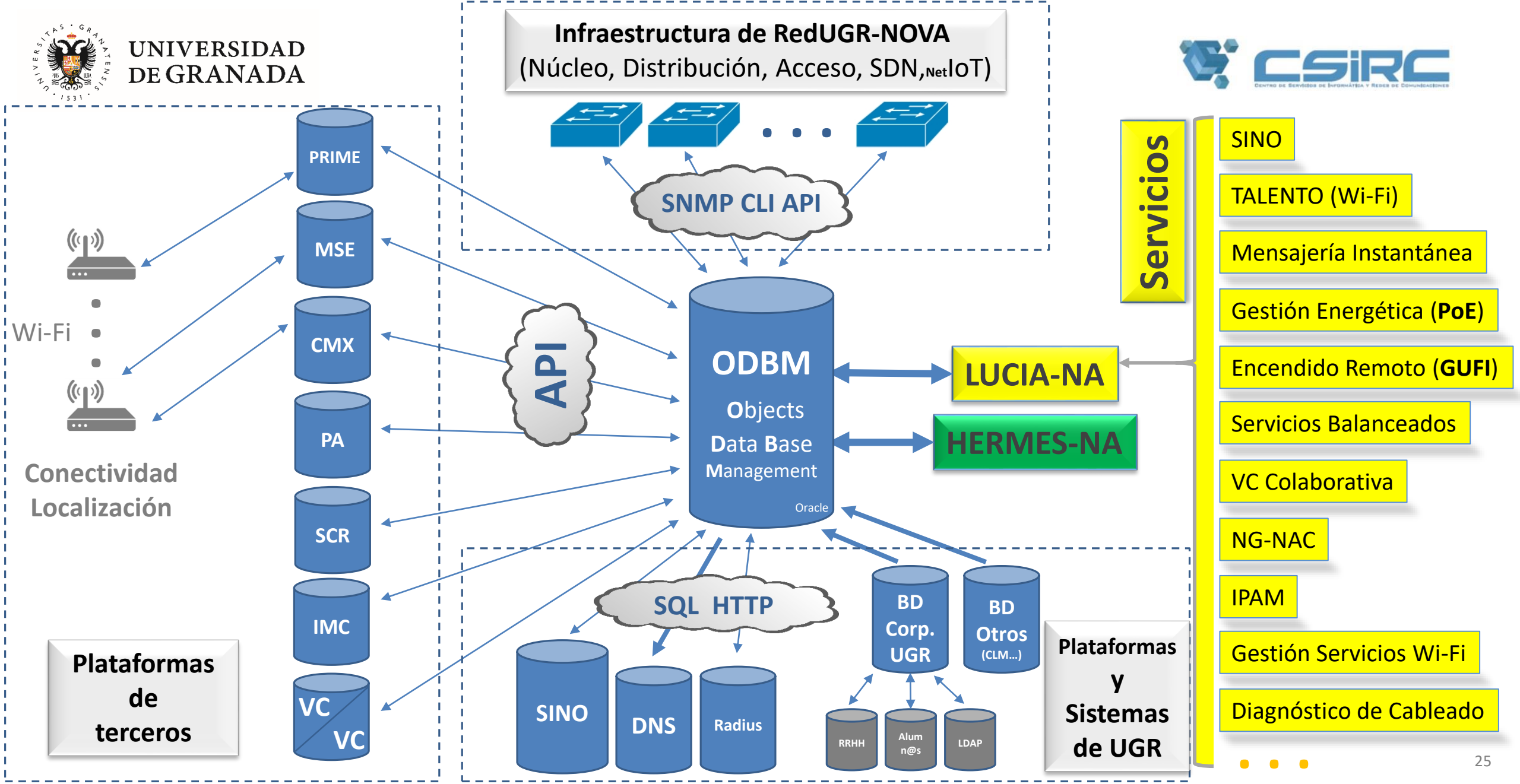
Alum n@s

LDAP

Plataformas y Sistemas de UGR

Plataformas de terceros


Infraestructura de RedUGR-NOVA
(Núcleo, Distribución, Acceso, SDN,NetIoT)
SNMP CLI API
PRIME
MSE
CMX
PA
SCR
IMC
VC
VC
Wi-Fi
Conectividad
Localización
API
ODBM
Objects
Data Base
Management
Oracle
LUCIA-NA
HERMES-NA
Servicios
NetKiller
NG-NAC
Redes Cuarentena
Listas Negras +
Servicios Eduroam
Invitados Wi-Fi
Wi-Fi Congresos
Aulas 4.0
ADP
VPN
Netflow
SQL HTTP
SINO
DNS
Radius
BD Corp. UGR
BD Otros (CLM...)
RRHH
Alum n@s
LDAP
Plataformas y Sistemas de UGR
Plataformas de terceros


Infraestructura de RedUGR-NOVA
(Núcleo, Distribución, Acceso, SDN,NetIoT)
SNMP CLI API
PRIME
MSE
CMX
PA
SCR
IMC
VC
VC
Wi-Fi
Conectividad
Localización
API
ODBM
Objects
Data Base
Management
Oracle
LUCIA-NA
HERMES-NA
Servicios
SINO
TALENTO (Wi-Fi)
Mensajería Instantánea
Gestión Energética (PoE)
Encendido Remoto (GUFI)
Servicios Balanceados
VC Colaborativa
NG-NAC
IPAM
Gestión Servicios Wi-Fi
Diagnóstico de Cableado
SQL HTTP
SINO
DNS
Radius
BD Corp. UGR
BD Otros (CLM...)
RRHH
Alumn@s
LDAP
Plataformas y Sistemas de UGR
Plataformas de terceros

3. LUCIA-NA y HERMES-NA

3. Sistema HERMES-NA

3. Sistema HERMES-NA

HERMES-NA

CONEXION (-)

ETHERNET	00:1B:21:00:90:90	↓ IP	172.18.126.111	↓ NOMBRE	CMA126111	↓ VLANID	626
TOIP(MAC)		↓ TELEFONO		↓			
FECHA	11/08/2004						
HUB/SWITCH	CPTPCEAAU02	↓ MODELO	WS-C2950G-48-EI				
PUERTO	19	↓ Sin Uso Desde	22/03/2018 01:18:31				
TOMA	PS. TOMA AE-D7.23	↓ PARCHEADO		CABLE	-1	↓ HII	
SOLICITUD		↓ CABLE (Descripción)	INEXISTENTE				

CONFIGURACION AVANZADA

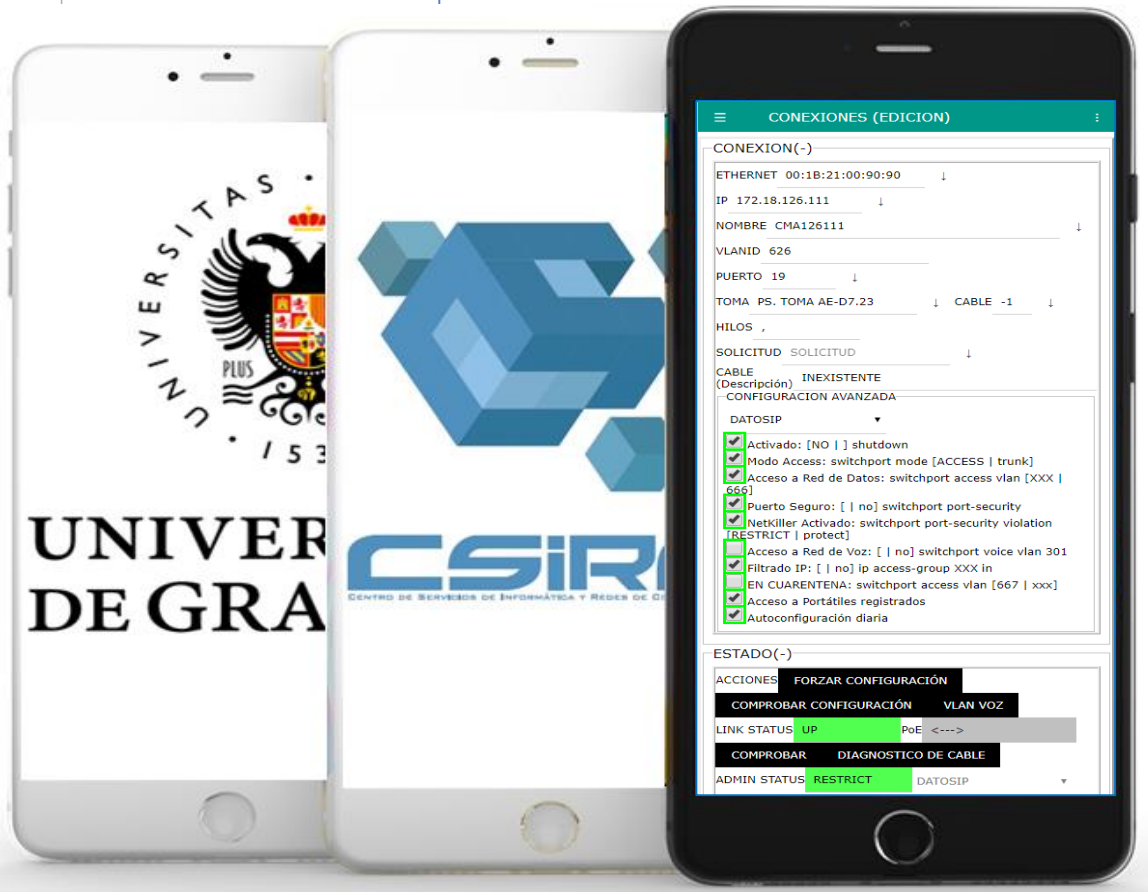
DATOSIP

- [x] Activado: [NO |] shutdown
- [x] Modo Access: switchport mode [ACCESS | trunk]
- [x] Acceso a Red de Datos: switchport access vlan
- [x] Puerto Seguro: [| no] switchport port-security
- [x] NetKiller Activado: switchport port-security violation [RESTRICT | protect]
- [ ] Acceso a Red de Voz: [| no] switchport voice vlan
- [x] Filtrado IP: [| no] ip access-group XXX in
- [ ] EN CUARENTENA: switchport access vlan
- [x] Acceso a Portátiles registrados
- [x] Autoconfiguración diaria

COMENTARIO: PS. toma AE-D7.23

ESTADO (-)

ACCIONES	FORZAR CONFIGURACIÓN	COMPROBAR CONFIGURACIÓN	VLAN VOZ			
LINK STATUS	UP	PoE <--->	COMPROBAR	DIAGNOSTICO DE CABLE		
ADMIN STATUS	RESTRICT	DATOSIP	ACTIVAR	DESACTIVAR	LIBERAR MAC	
REAL: ETHERNET	00:1B:21:00:90:90	↓ NOMBRE CMA126111	IP 172.18.126.111	ToIP NO COMPROBADO	↓	
REAL: IP (Filtrada)	172.18.126.111	VLAN POLITECNICO-AUL - 626	ASIGNAR VLAN			



3. Sistema LUCIA-NA

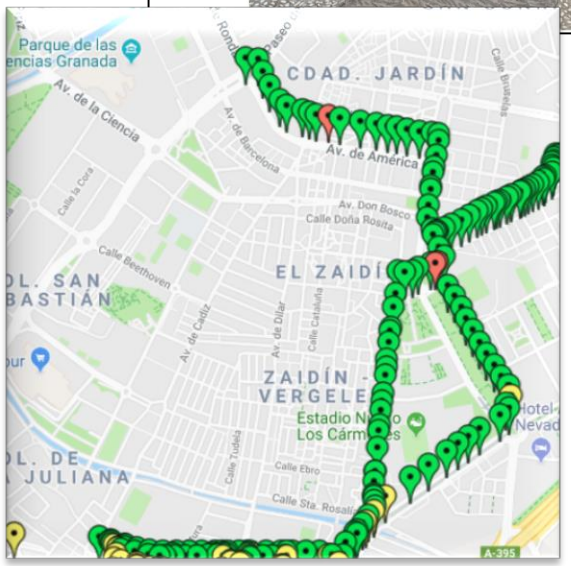
3. Sistema LUCIA-NA. SINO

SINO

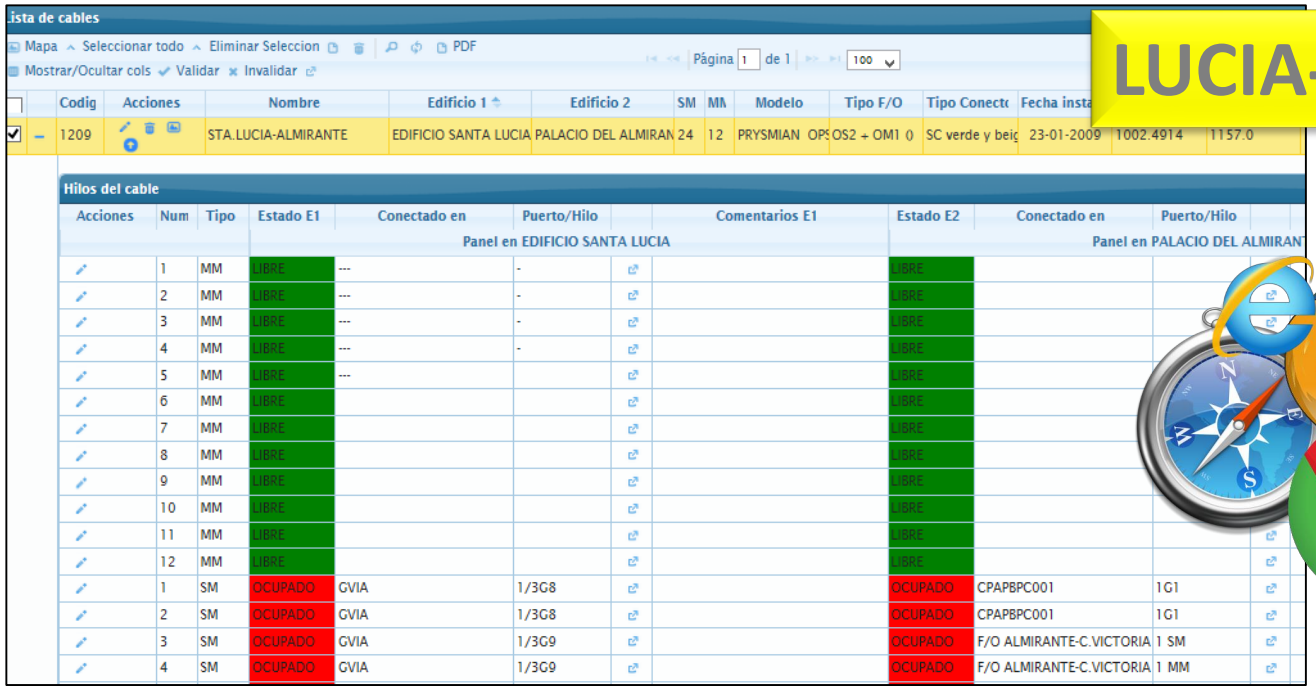
LUCIA-NA

3. Sistema LUCIA-NA. SINO

SINO



LUCIA-NA



3. Sistema LUCIA-NA. SINO Móvil

LUCIA-NA

SINO

Gestión de Operaciones de Campo sobre la Red de F/O Metropolitana en el Móvil

3. Sistema LUCIA-NA. Sistema TALENTO

LUCIA-NA

TALENTO

Orientación a la localización

3. Sistema LUCIA-NA. Sistema TALENTO

LUCIA-NA

TALENTO

Orientación a la localización

3. Sistema LUCIA-NA. Sistema TALENTO

LUCIA-NA

TALENTO

Orientación a la localización

3. Sistema LUCIA-NA. Sistema TALENTO

LUCIA-NA

TALENTO

Orientación a la localización

3. Sistema LUCIA-NA. Sistema TALENTO

LUCIA-NA

TALENTO

Orientación a la localización

International Welcome Centre

TOURIST INFO CENTER

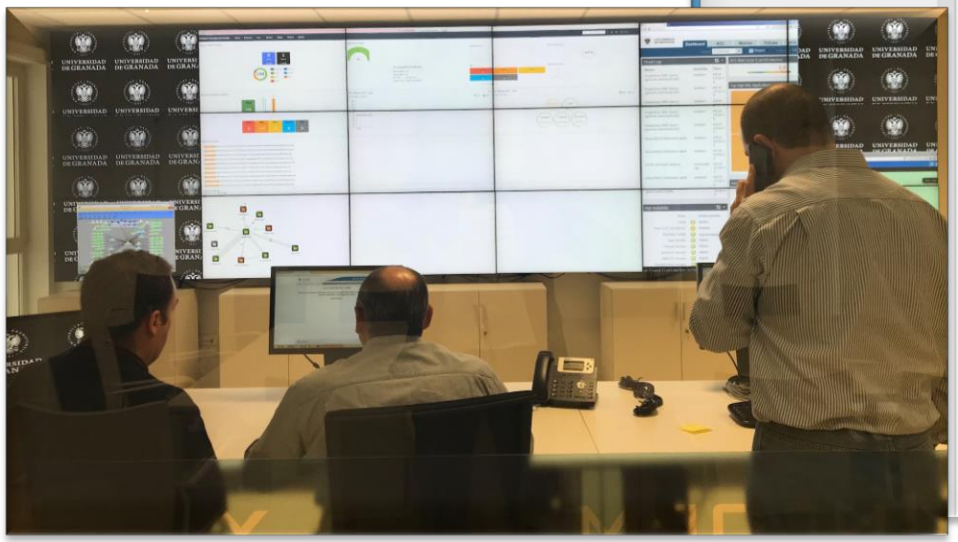
UNIVERSIDAD DE GRANADA

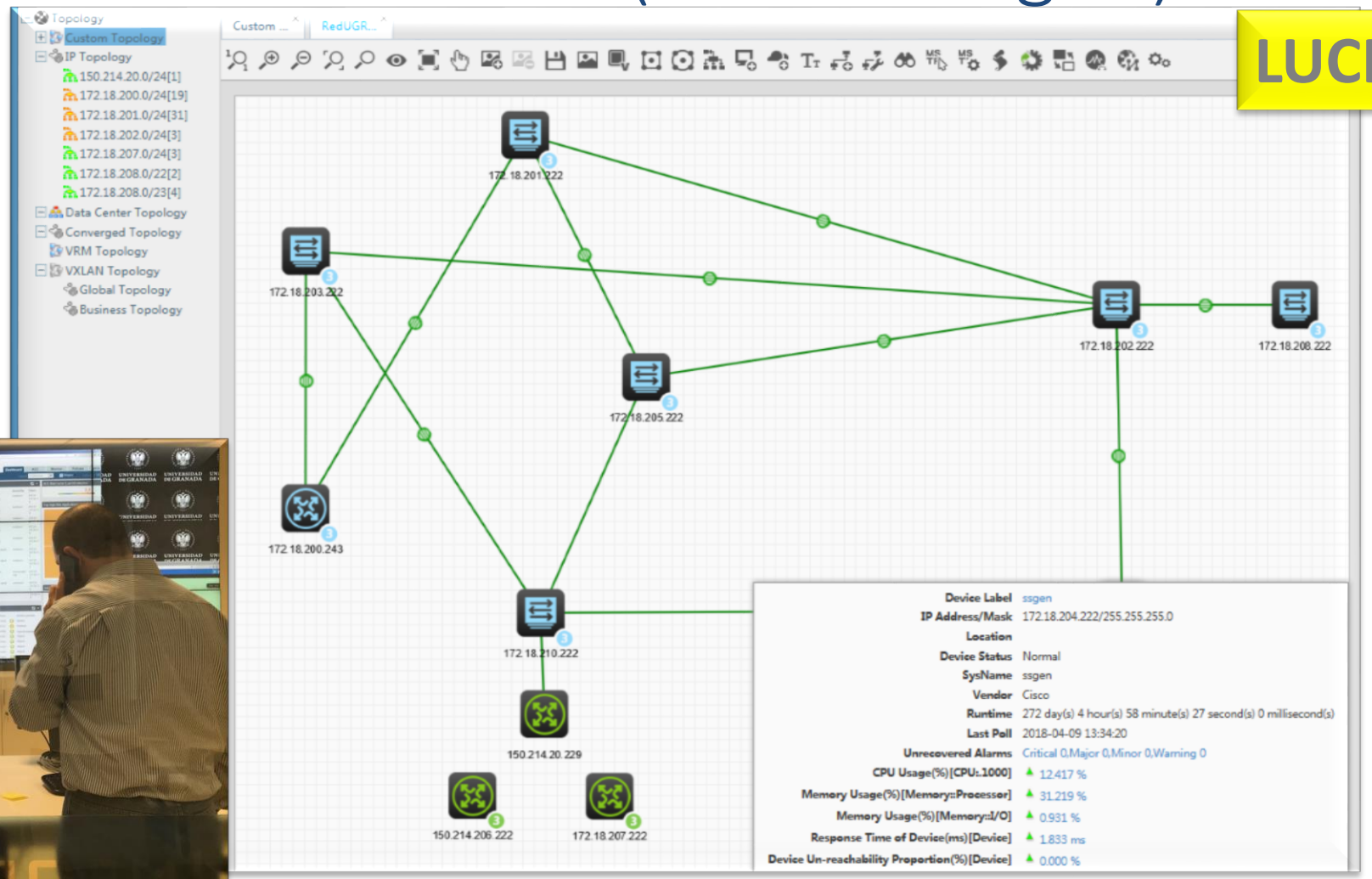
CSIRC

3. Sistema **LUCIA-NA. Otros** (Gestión Lógica)

RedUGRNova

LUCIA-NA





3. Sistema **LUCIA-NA. Otros** (Gestión Lógica)

LUCIA-NA

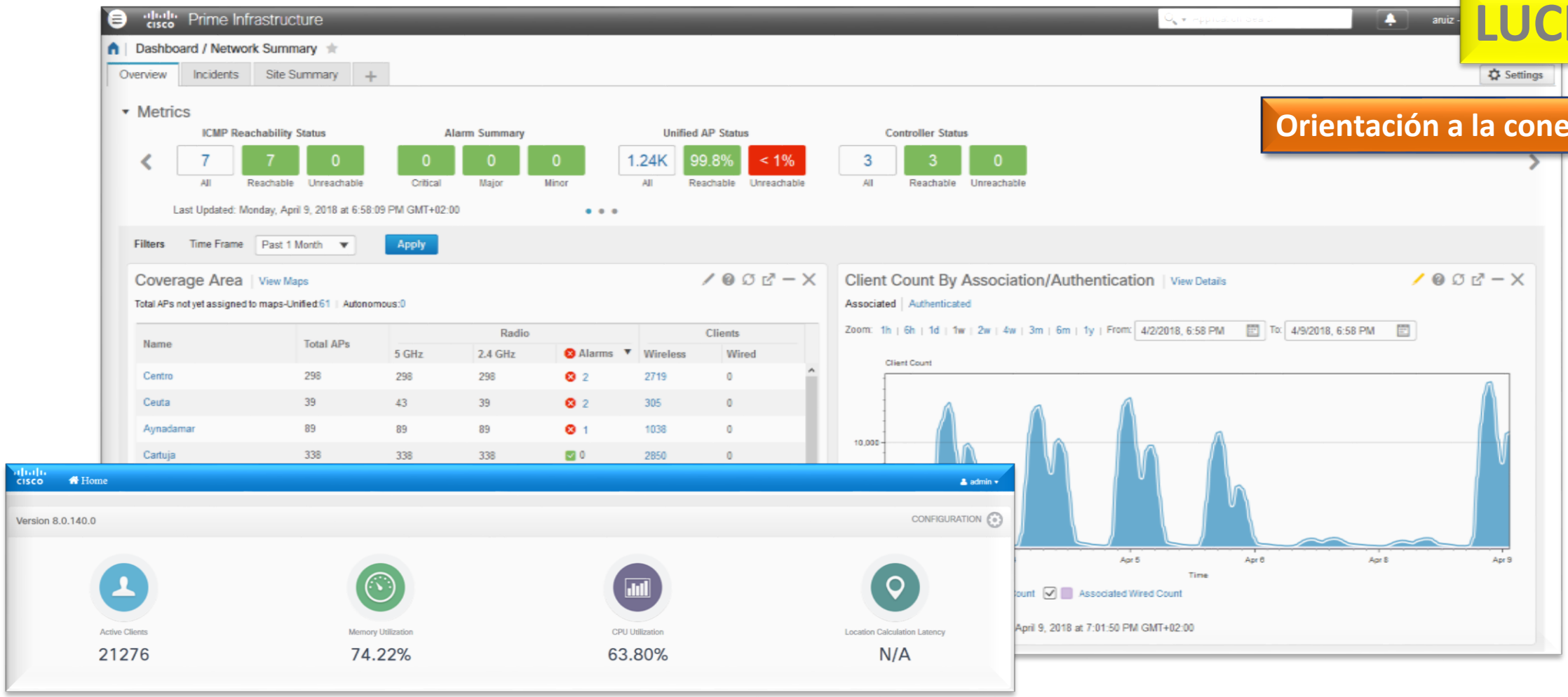
Ej.: Uso de Wi-Fi eduroam:

* 1 día tipo:
  - 40K dispositivos distintos
  - 30K usuarios diferentes
  - 17K usuarios simultáneos
* 1 semana tipo:
  - 500 dominios eduroam IN
  - 400 instituciones UGR OUT

3. Sistema **LUCIA-NA. Otros** (Gestión Wi-Fi)

LUCIA-NA

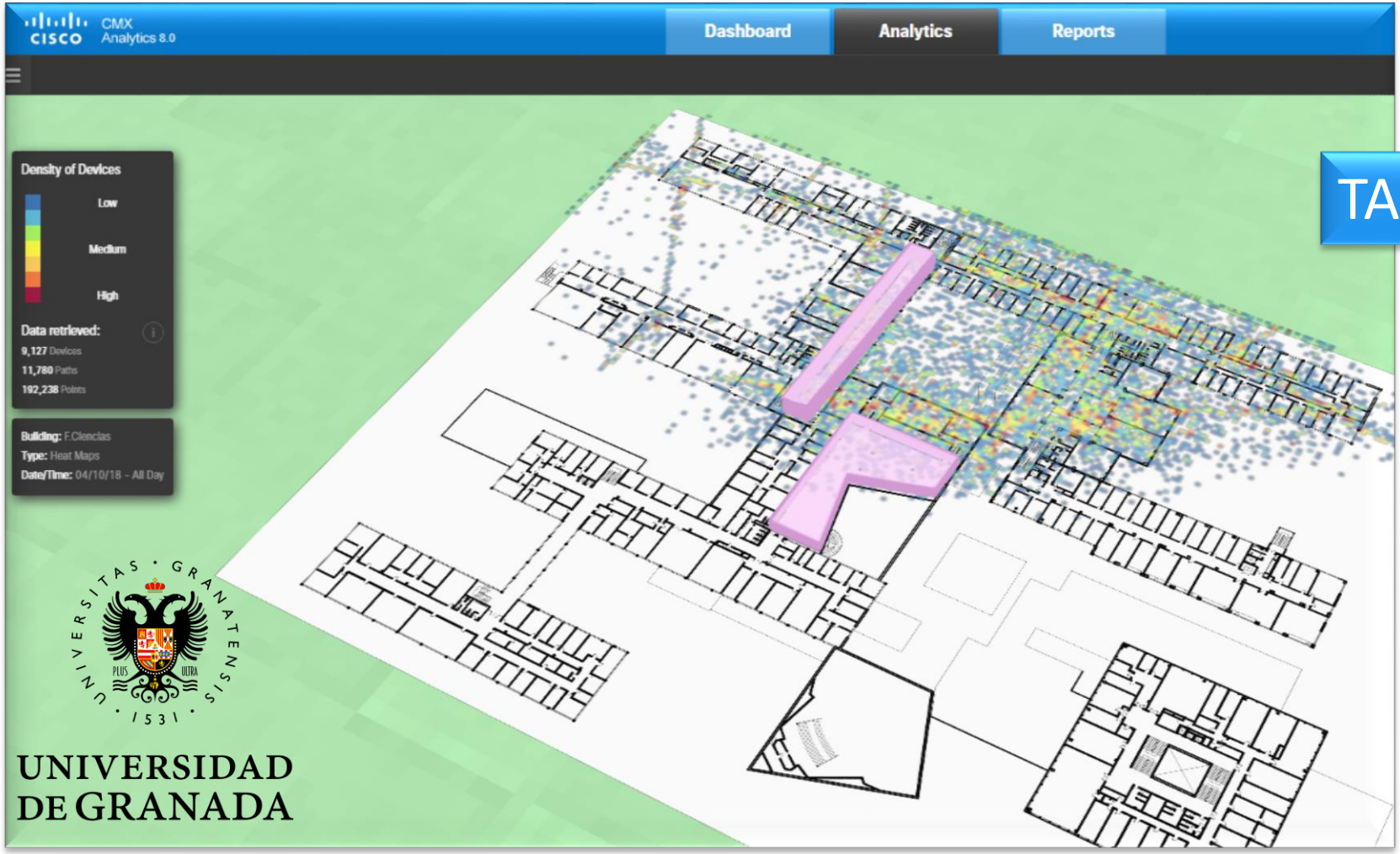
Orientación a la conectividad



3. Sistema **LUCIA-NA. Otros** (Gestión Wi-Fi)

LUCIA-NA

Orientación a la localización



TALENTO

UNIVERSIDAD DE GRANADA

CSIRC

3. Sistema **LUCIA-NA. Otros** (Gestión Sist. Balanceados)

LUCIA-NA

IDP_FARM
idp1[4]:20 (150.214. inService
idp2[4]:10 (150.214. inService
idp3[4]:15 (150.214. inService
idp4[4]:0 (150.214. arpFailed
TOTAL:45

IMAP_FARM
imap1[8]:423 (150.214. inService
imap2[8]:459 (150.214. inService
imap3[8]:532 (150.214. inService
imap4[8]:472 (150.214. inService
imap5[8]:494 (150.214. inService
imap6[8]:491 (150.214. inService
imap7[8]:356 (150.214. inService

LDAPM_FARM
ldapm1[8]:0 (172.18. inService
ldapm2[8]:0 (172.18. inService
ldapm3[8]:0 (172.18. outOfService
TOTAL:0

LDAP_FARM
ldap1[8]:0 (172.18. outOfService
ldap2[8]:0 (172.18. outOfService
ldap3[8]:137 (172.18. inService
ldap4[8]:154 (172.18. inService
ldap5[8]:148 (172.18. inService
TOTAL:439

LISTASTU_FARM
correo7[8]:0 (150.214. inService
correo8[8]:0 (150.214. inService
correo9[8]:0 (150.214. inService
TOTAL:0

LISTAS_FARM
listas1[2]:0 (150.214. outOfService
listas2[2]:0 (150.2 inService
listas3[2]:0 (150.2 inService
listas4[2]:0 (150.2 inService
TOTAL:0

MAIL_FARM
mail1[2]:3 (150. inService
mail2[2]:5 (150. inService
mail3[2]:2 (150. inService
mail4[2]:3 (150. inService
TOTAL:13

AFIRMA_FARM
afirma1[2]:0 (150.214 inService
afirma2[2]:0 (150.214. inService
TOTAL:0

ALFRESCO_FARM
alfresco1[2]:0 (150.214 probeFailed
alfresco2[2]:1 (150.214. inService
TOTAL:1

ARIES_FARM
aries1[2]:0 (150.214. inService
aries2[2]:0 (150.214. inService
TOTAL:0

BLOGS_FARM
blog1[8]:0 (172. inService
blog2[8]:0 (172. inService
blog3[8]:0 (172. inService
TOTAL:0

DI_FARM
dali6[8]:0 (172. inService
dali7[8]:0 (172. inService
TOTAL:0

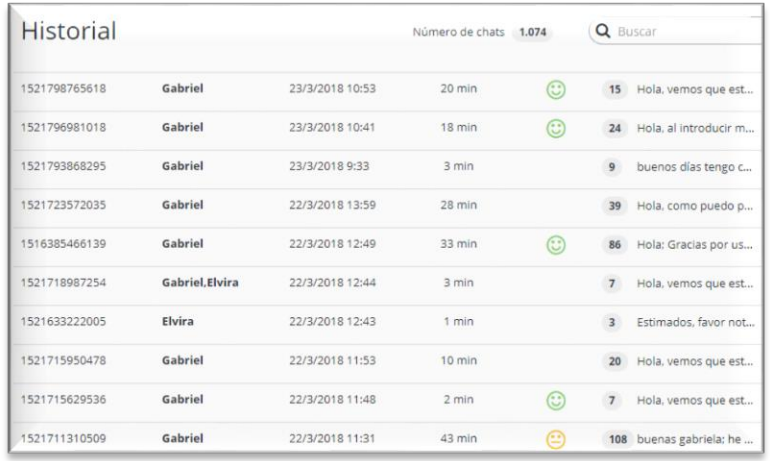
ELECCIONES_FARM
dali1[8]:0 (172. inService
dali2[8]:0 (172. inService
TOTAL:0

ESCRITORIO_FARM
escritorio1[2]:0 (150. inService
escritorio2[2]:0 (150.214. inService
TOTAL:0

FACTURA_FARM
factura1[8]:0 (150.214 inService
factura2[8]:0 (150.214. inService
TOTAL:0

3. Sistema **LUCIA-NA. Otros** (Help-Desk)

LUCIA-NA

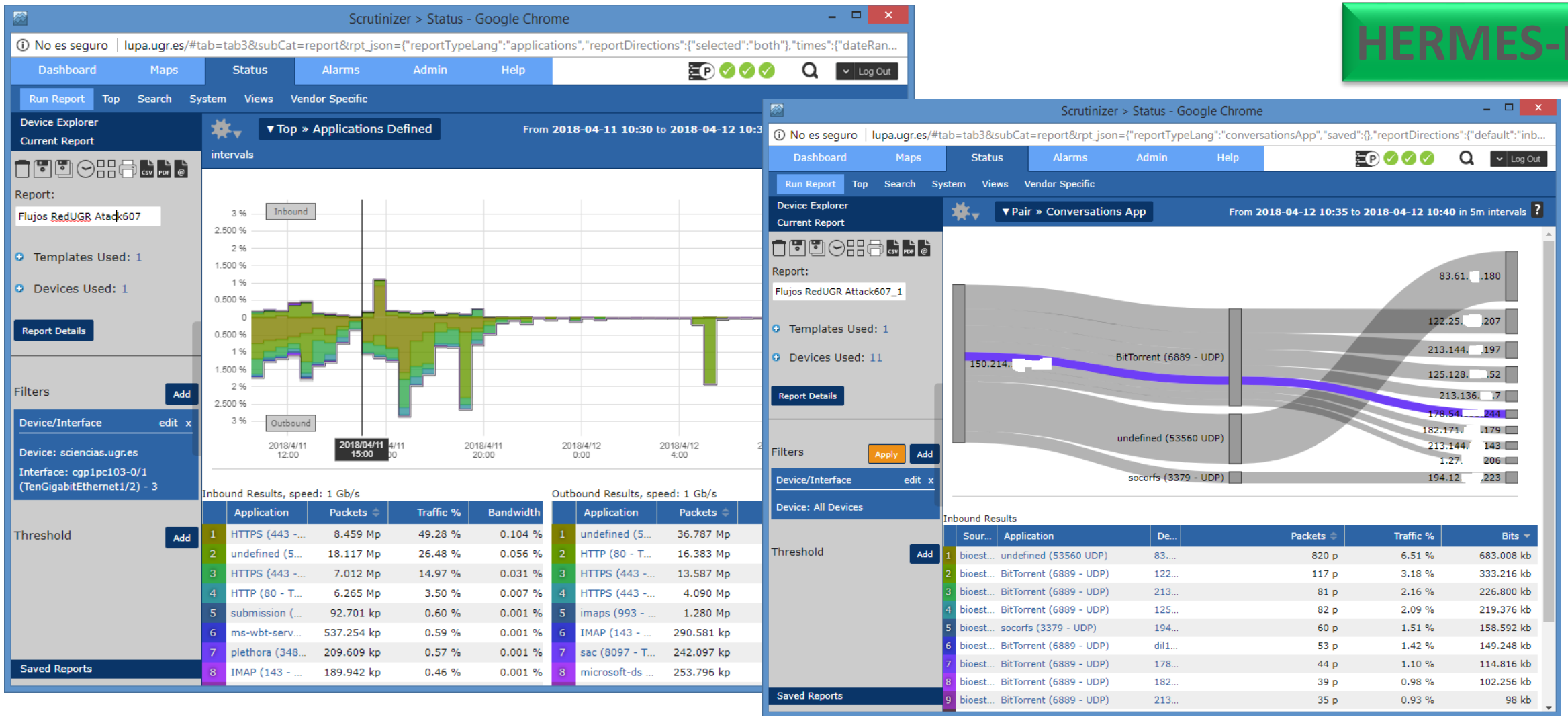


UNIVERSIDAD DE GRANADA

CSIRC

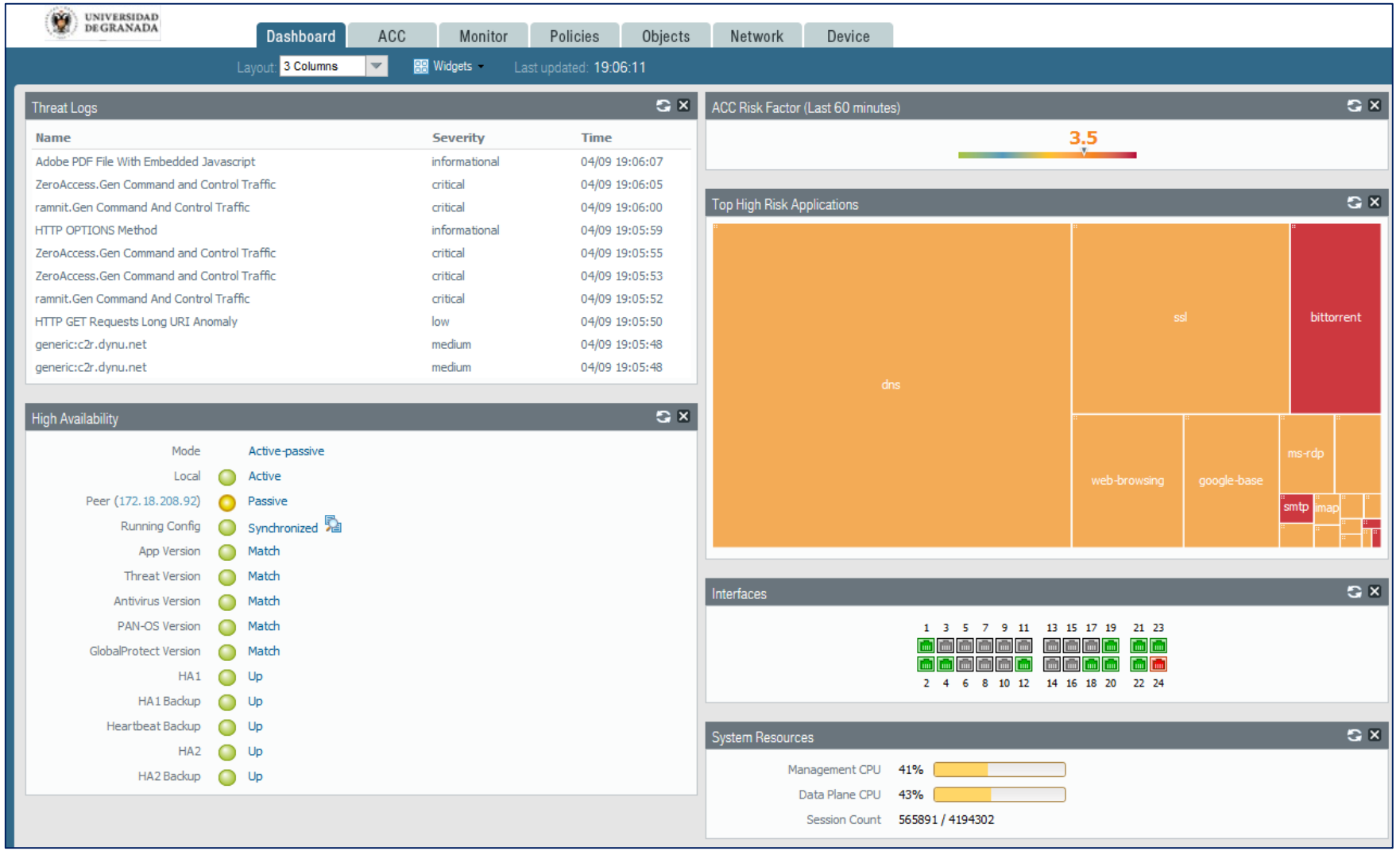
3. Sistema **HERMES-NA. Otros** (Gestión de Flujos)

HERMES-NA

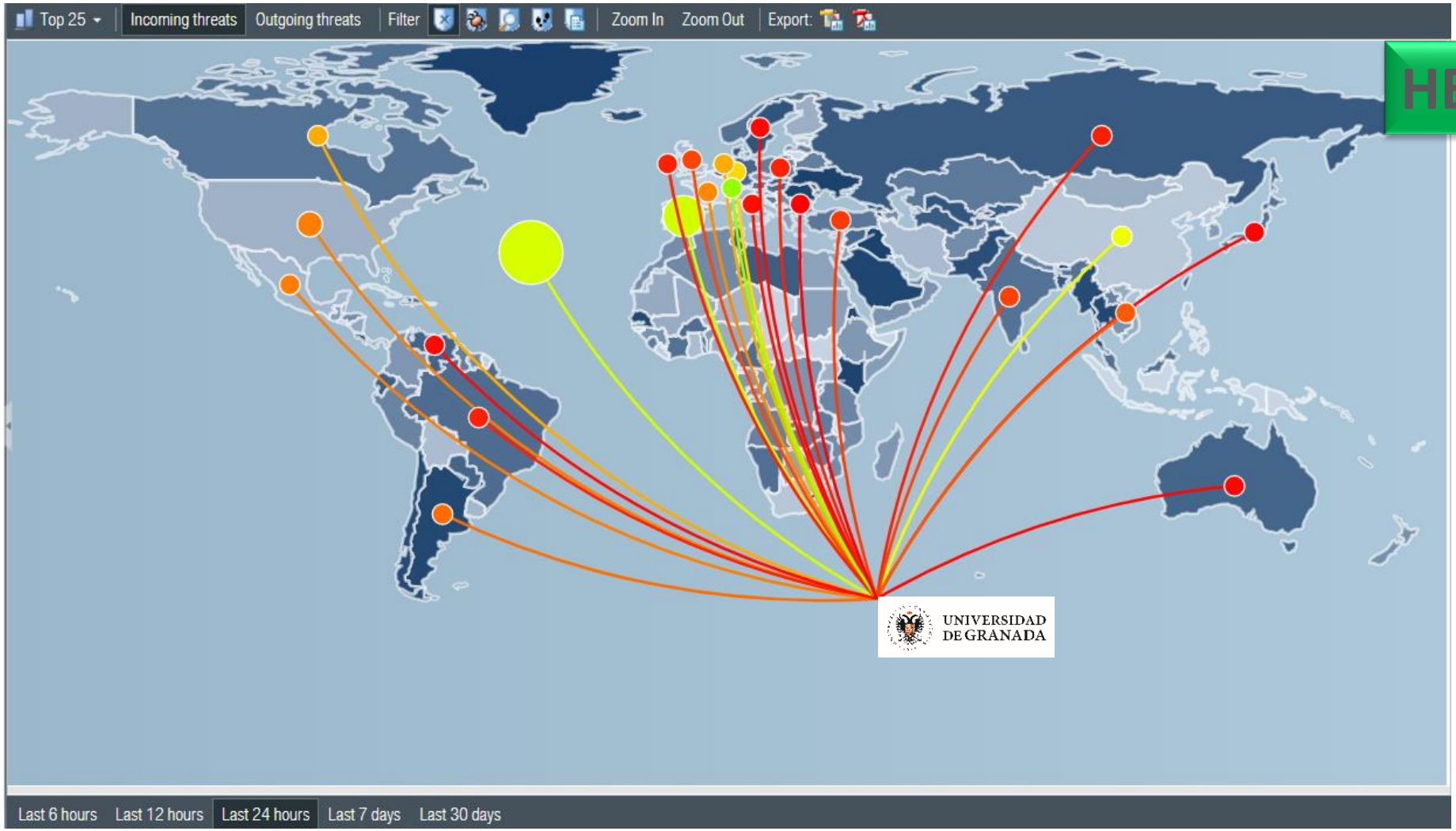


3. Sistema **HERMES-NA. Otros** (Gestión NGFW)

HERMES-NA



3. Sistema **HERMES-NA. Otros** (Gestión NGFW)



4. En fase se lanzamiento. Próximamente,…

LUCIA-NA

HERMES-NA

4. En fase se lanzamiento. Próximamente,…

LUCIA-NA

HERMES-NA

4. En fase se lanzamiento. Piloto en producción,...

HERMES-NA

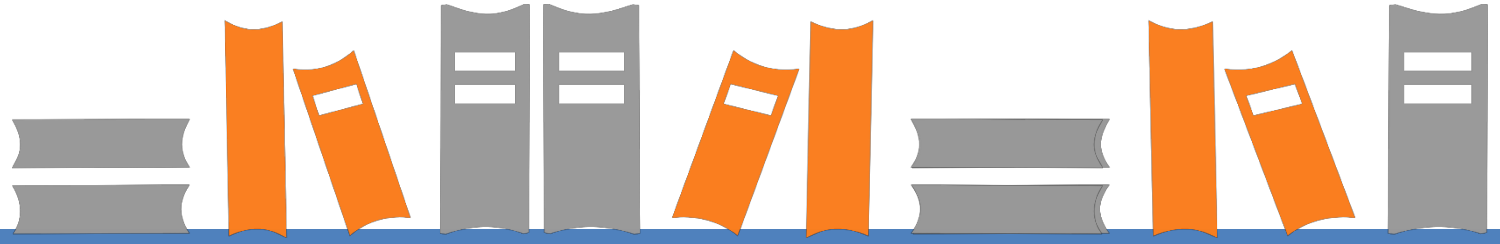
LUCIA-NA

Telegram

Interacción Usuario Registrado Comunicación de incidentes de Seguridad u Operaciones de Gestión de Red

5. Referencias:

- http://www.rediris.es/jt/jt2012/ponencias/jt/jt2012-jt-sesion1a-a3b1.pdf
- http://www.rediris.es/difusion/eventos/ponencias/?id=frc2015-frc-sesion_mon_contr-a8b1c1.pdf
- https://www.cisco.com/c/dam/global/es_es/solutions/publicaciones/caso-practico/2014-01-29-caso-cliente-granada.pdf
- https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/case_study_c36-721612.pdf
- https://wiki.geant.org/download/attachments/97944430/2018-04-19-GEANT-PresentacionRedUGR-Barcelona-Eng-def.pdf?version=1&modificationDate=1524154916992&api=v2
- https://www.top500.org/site/49071
- https://www.rediris.es/cert/doc/reuniones/fs2003/archivo/UGR.pdf



UNIVERSIDAD DE GRANADA

TEAMWORK

CSIRC

UNIVERSIDAD DE GRANADA

CSIRC

Programación de Red Orientada a la: Ciberseguridad y Gestión Automatizada”

ANTONIO RUIZ MOYA

ARUIZ@UGR.ES

SERVICIO DE REDES Y COMUNICACIONES

UNIVERSIDAD DE GRANADA

VNiVERSiDAD D SALAMANCA