



UNIVERSIDAD
DE GRANADA



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

Jornadas
Técnicas
de RedIRIS
2018

Del 7 al 10 de mayo
Universidad de Salamanca
Por la Universidad de Salamanca



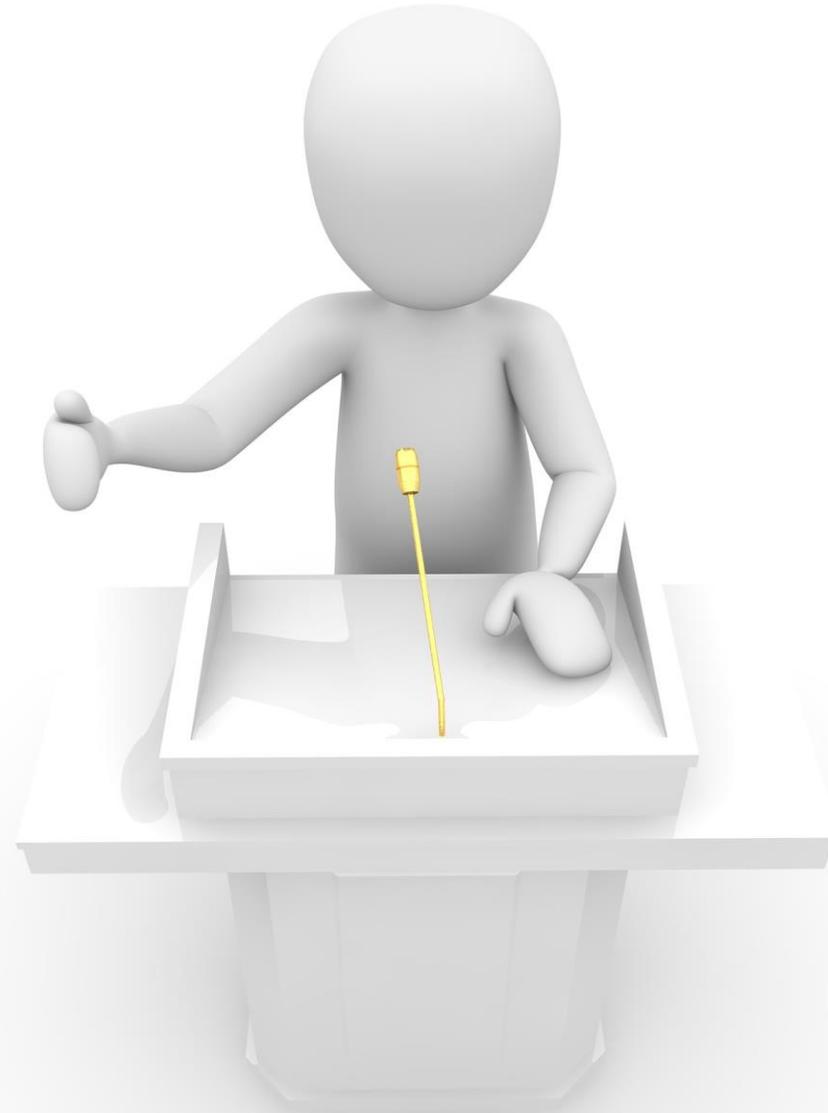
VNiVERSiDAD
D SALAMANCA

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?





¿Cuál es la problemática de partida?



¿Cuál es la problemática de partida?



**GESTIÓN
DE LOS
CAMBIOS**

ISO

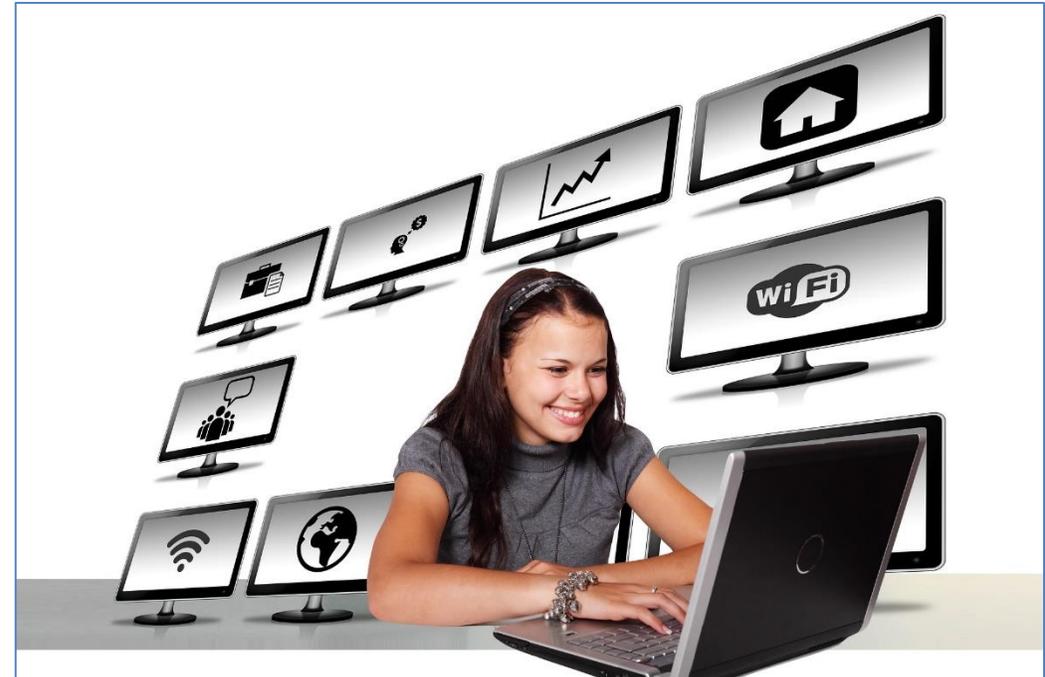
ITIL

¿Por qué PROC y PROG?

GESTIÓN DE LOS CAMBIOS



CIBERSEGURIDAD

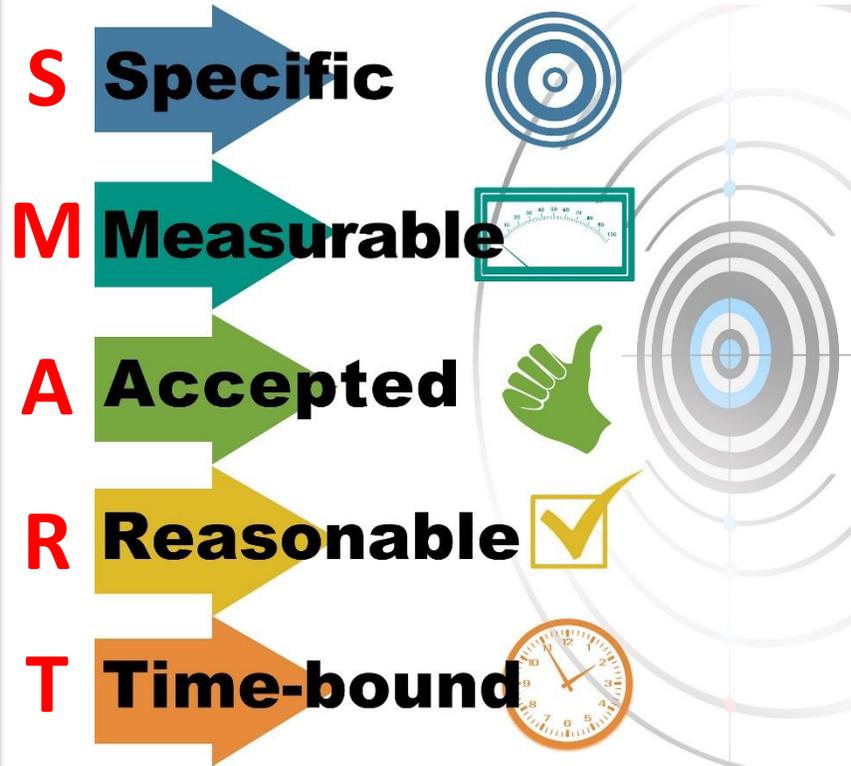


GESTIÓN DE RED

¿Por qué PROC y PROG?

MODELO DE GESTIÓN DE LOS
CAMBIOS EN RedUGR

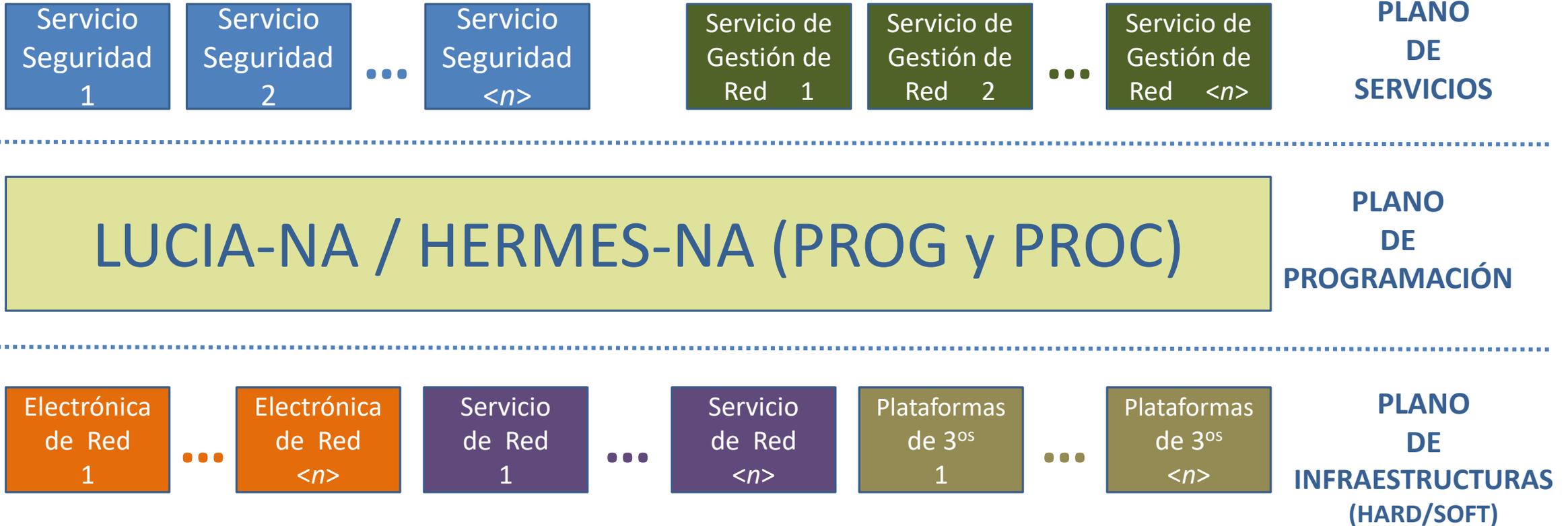
FILOSOFÍA DE DESARROLLO
ORIENTADO A LA GESTIÓN DE LA
SEGURIDAD Y GESTIÓN DE RED





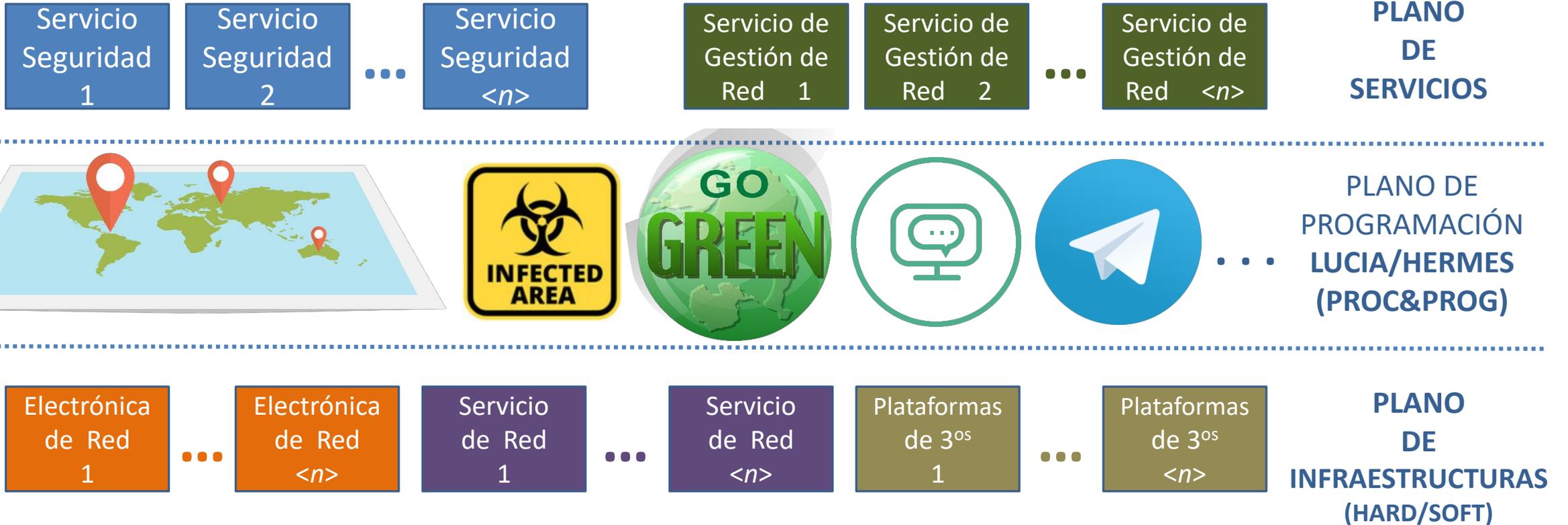
¿Por qué PROC y PROG?

MODELO DE GESTIÓN DE LOS CAMBIOS EN RedUGR
FILOSOFÍA DE DESARROLLO ORIENTADO A LA GESTIÓN DE LA SEGURIDAD Y GESTIÓN DE RED



¿Por qué PROC y PROG?

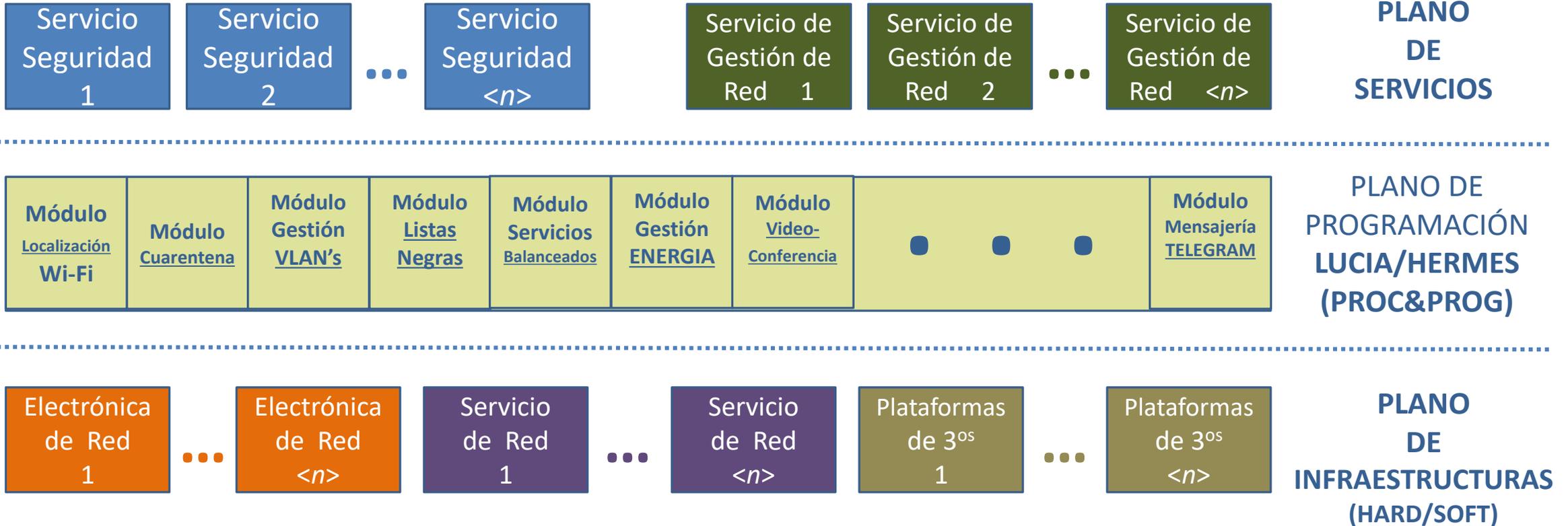
MODELO DE GESTIÓN DE LOS CAMBIOS EN RedUGR
MEDIANTE LA PROGRAMACIÓN ORIENTADA A LA GESTIÓN DE LA SEGURIDAD Y GESTIÓN DE RED





¿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

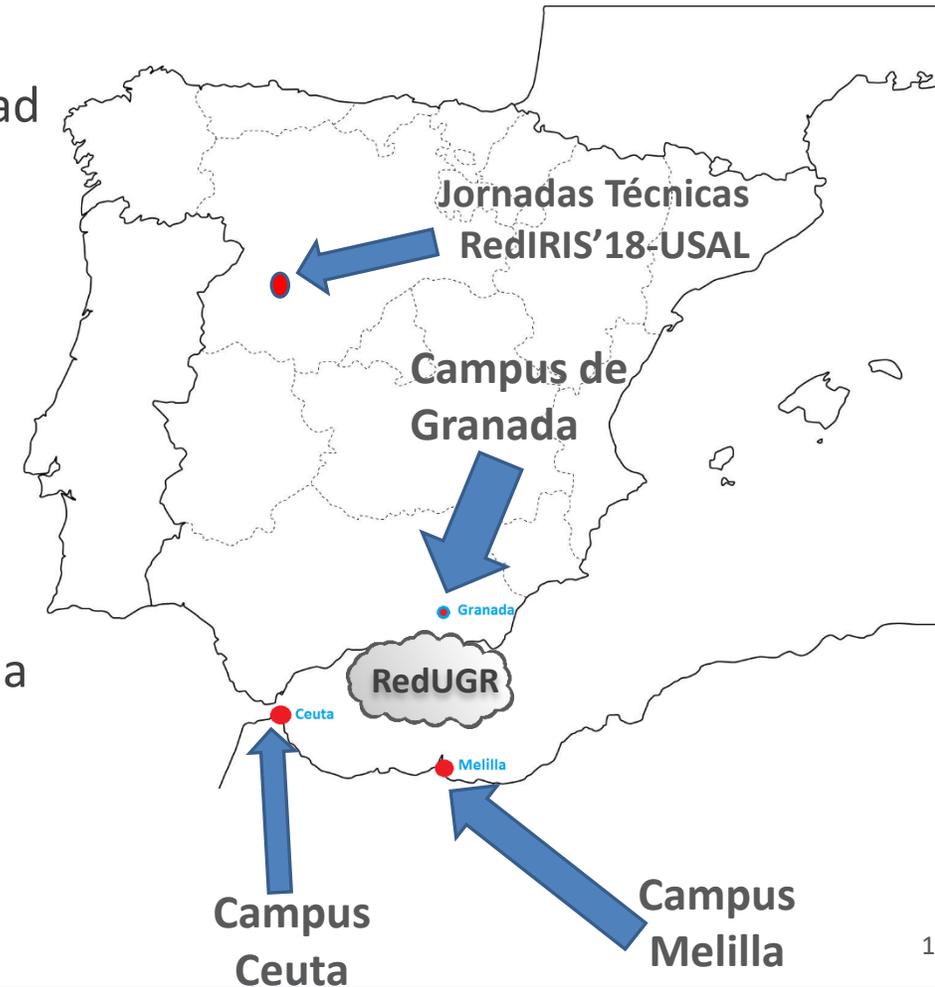
1. Objetivos de Gestión en RedUGR

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



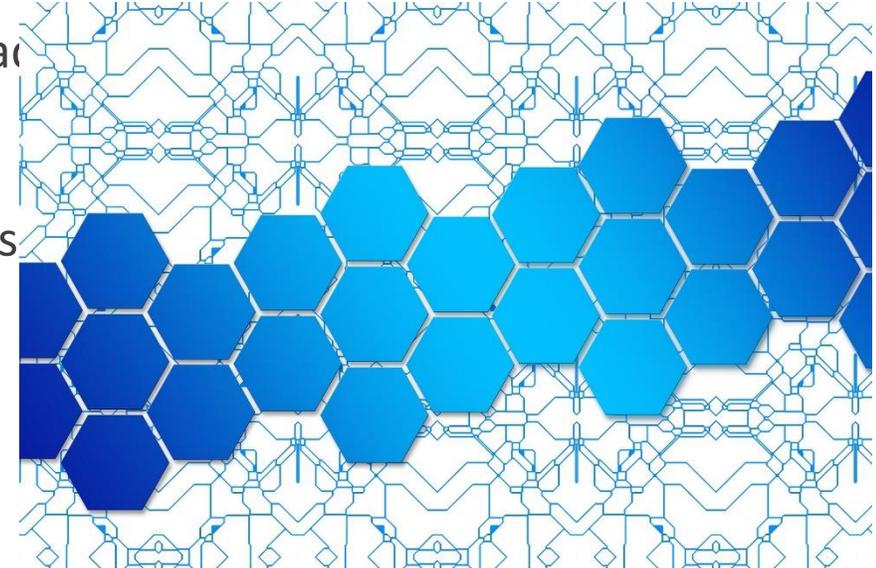
2. ¿Qué es RedUGR? Infraestructuras

- 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



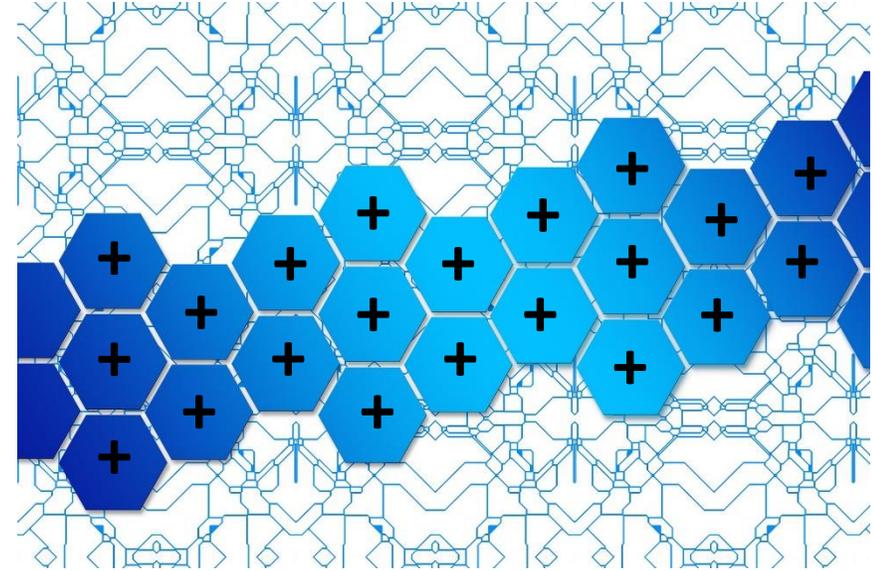
2. ¿Qué es RedUGR? Servicios

- 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 instantánea
- 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

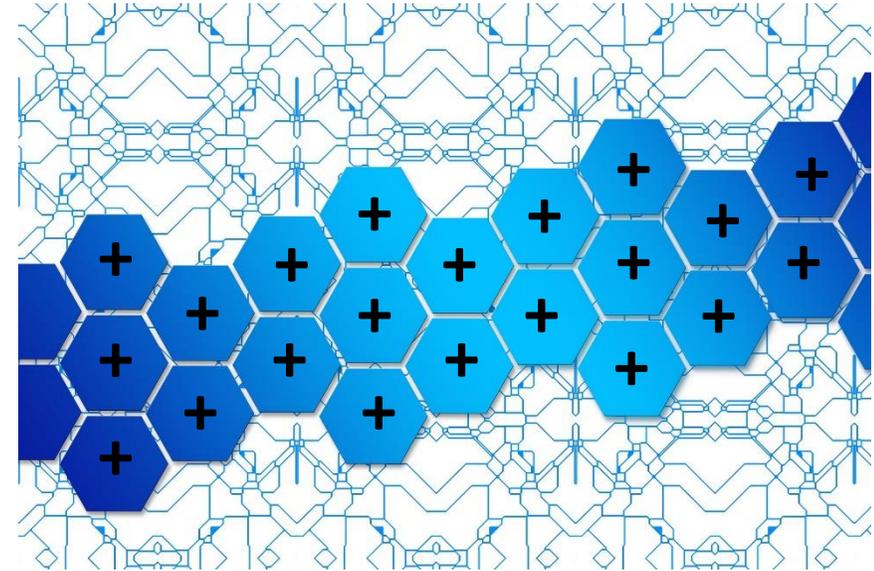
- Sistemas de Balanceo de Carga Universitarios. 67 Granjas
- Sistema de Gestión de Red (Control & Monitorización)

**Cisco PRIME, Cisco MSE, Cisco CMX, HP-IMC,
DESARROLLO PROPIO SRC-UGR (ODBM+SINO)**

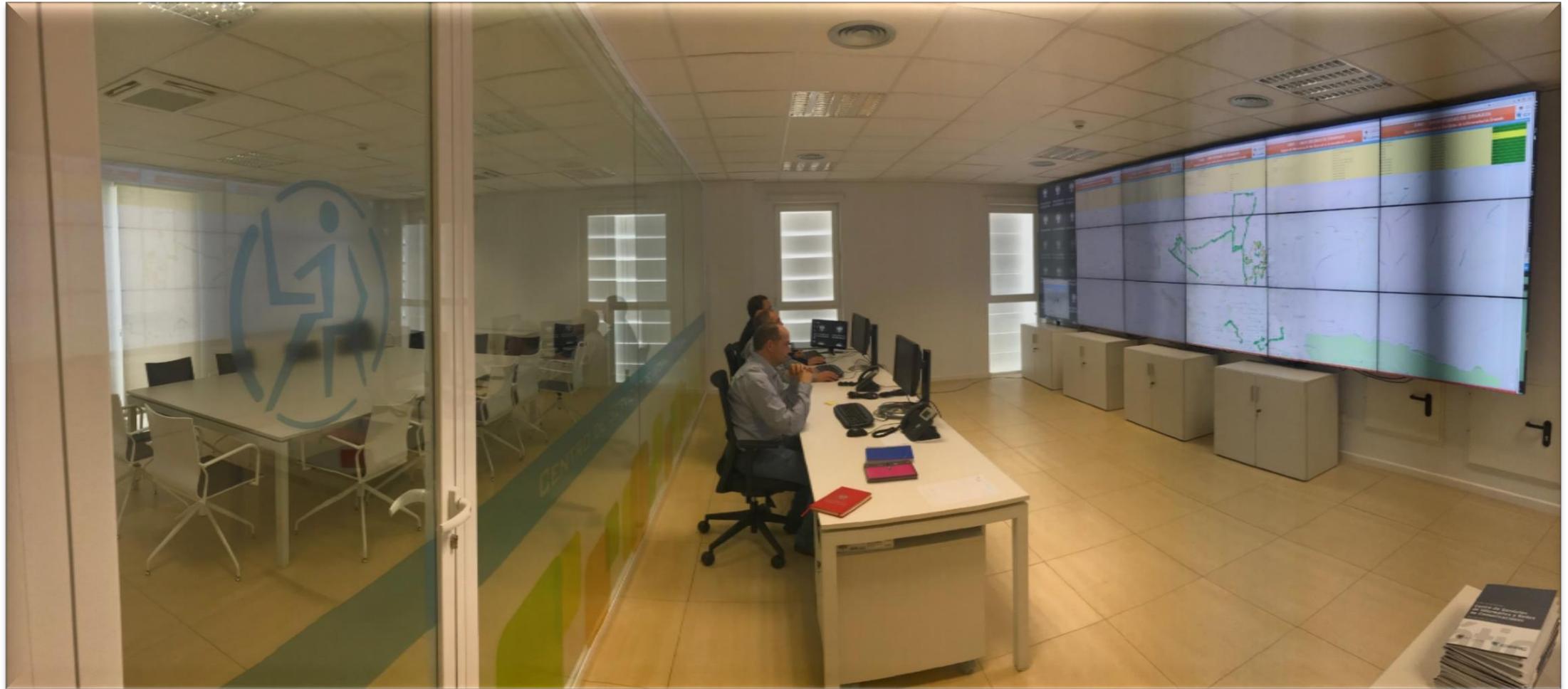
Software Libre (Dude, Cacti, MRTG, IRIS,...)

- Gestión de la Seguridad de Red vía:

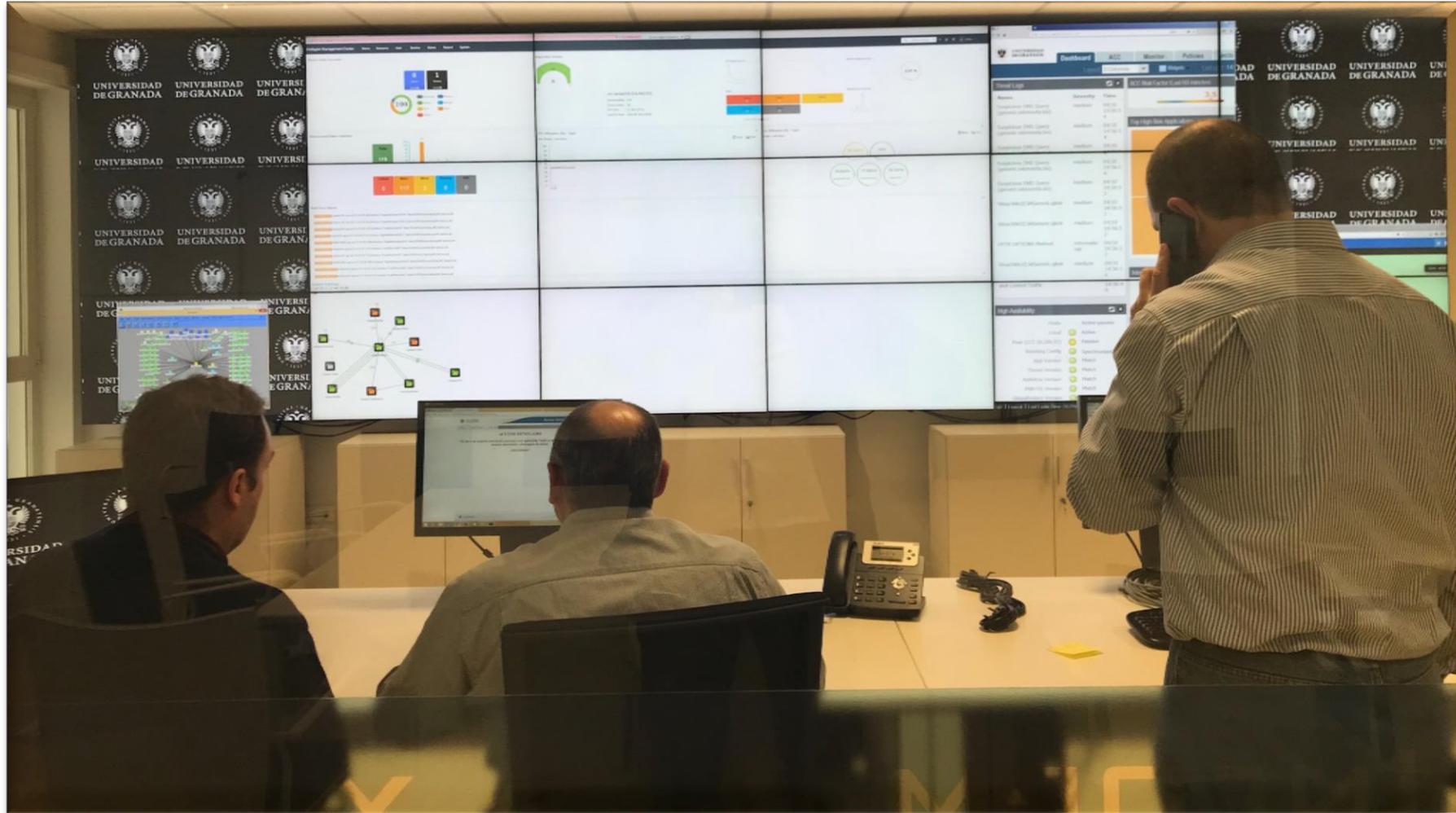
- NG-FW **PALOALTO NETWORKS**
- NG-NAC **DESARROLLO PROPIO SRC-UGR (ODBM)**
- Lupa para flujos de red global **SCRUTINIZER-Plixer**
- Captura de tráfico en el núcleo **CISCO NAM2**
- VPN para conectividad exterior **CISCO Anyconnect**
- Sistema ODBM: PROC + PROG **DESARROLLO PROPIO SRC-UGR (ODBM)**



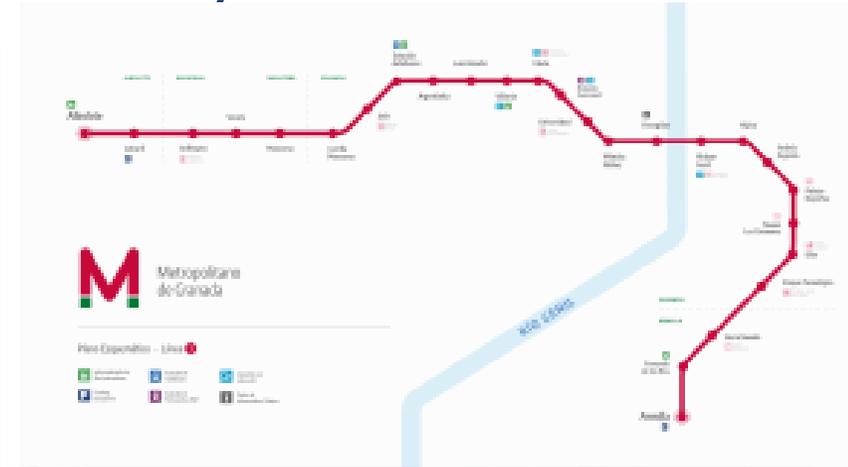
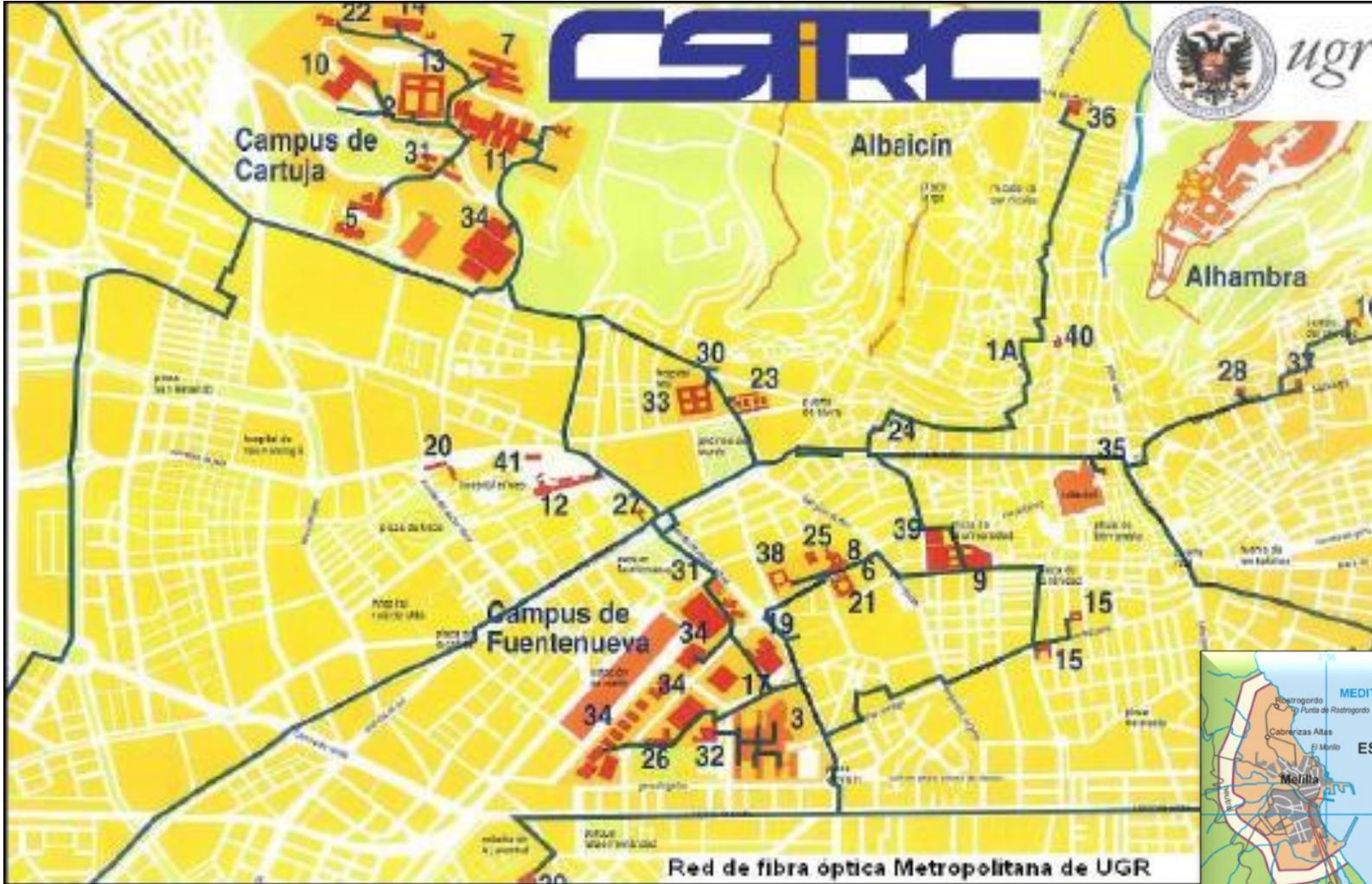
2. ¿Qué es RedUGR? Centro de Gestión



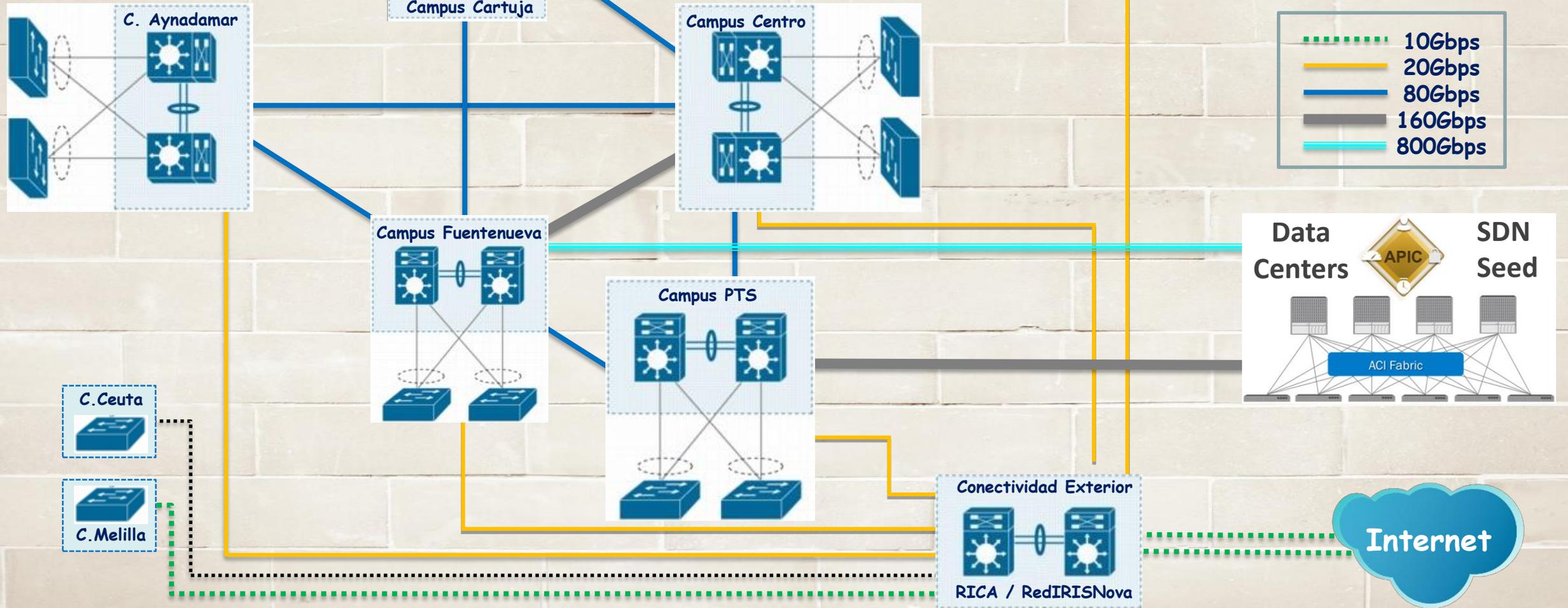
2. ¿Qué es RedUGR? Centro de Gestión



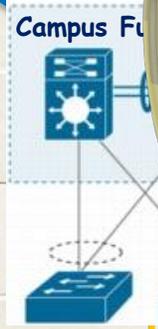
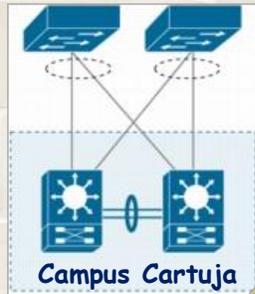
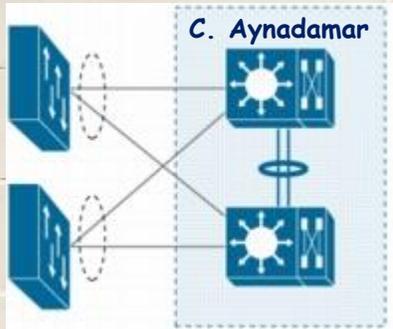
2. ¿Qué es RedUGR? Red de F/O



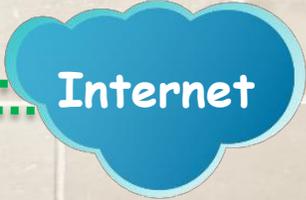
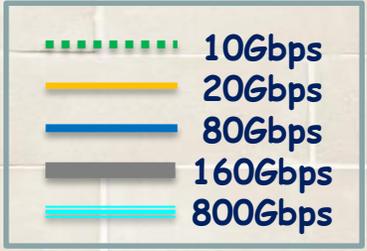
2. ¿Qué es RedUGR? Núcleo



2. ¿Qué es RedUGR? Núcleo



RedUGR Nova



3. Sistemas de Gestión



LUCIA-NA

GESTIÓN DE RED



HERMES-NA

CIBERSEGURIDAD



UNIVERSIDAD DE GRANADA



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



SNMP CLI API

API

ODBM
Objects
Data Base
Management
Oracle

SQL HTTP

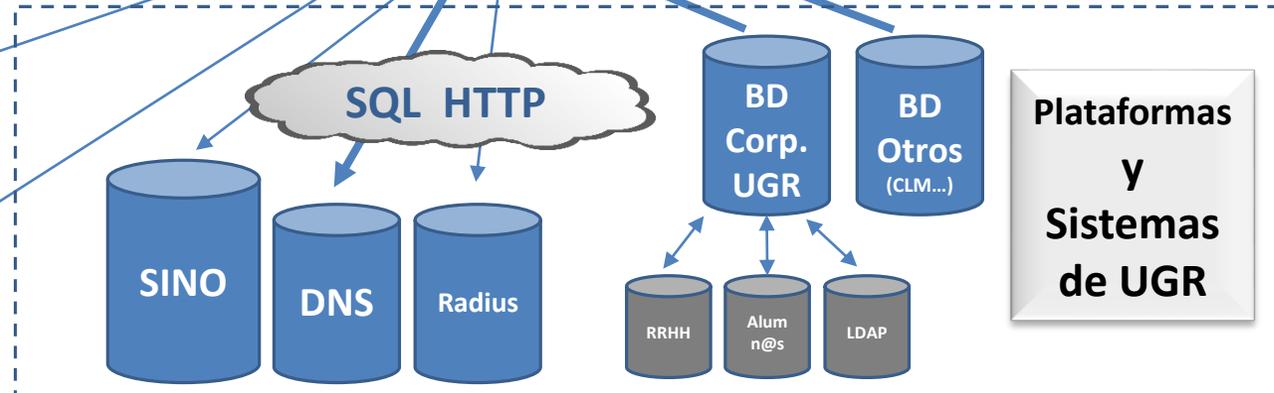
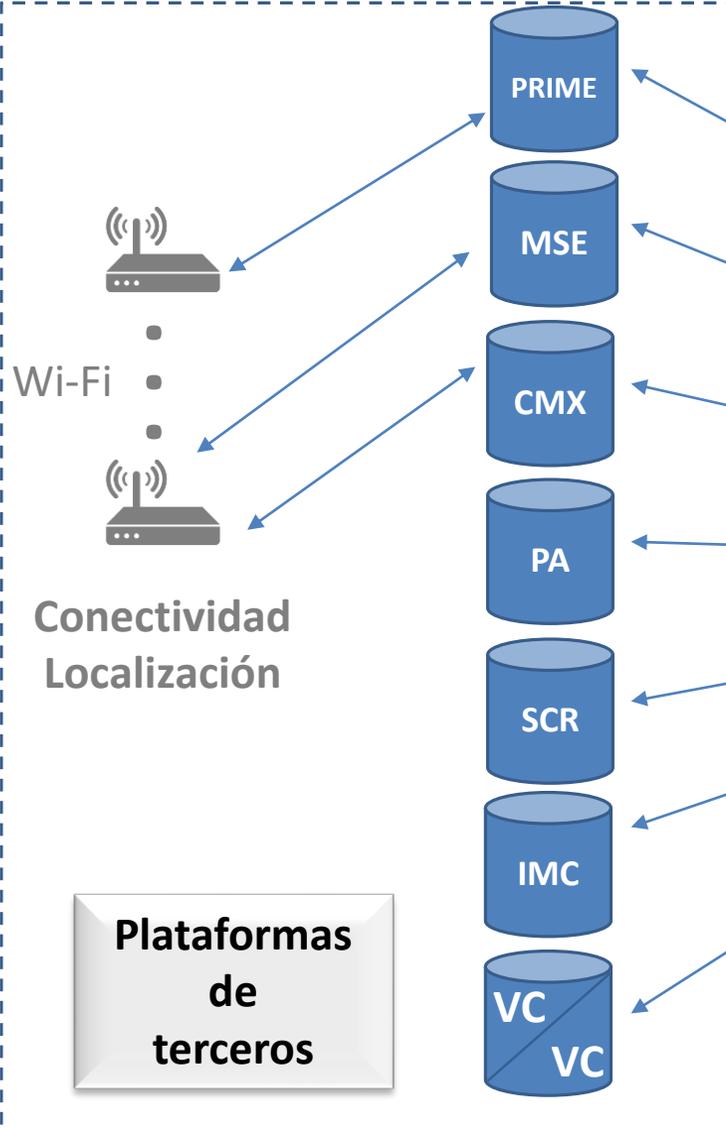
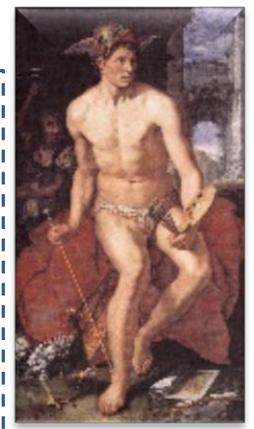
SINO
DNS
Radius

BD Corp. UGR
BD Otros (CLM...)
RRHH
Alum n@s
LDAP



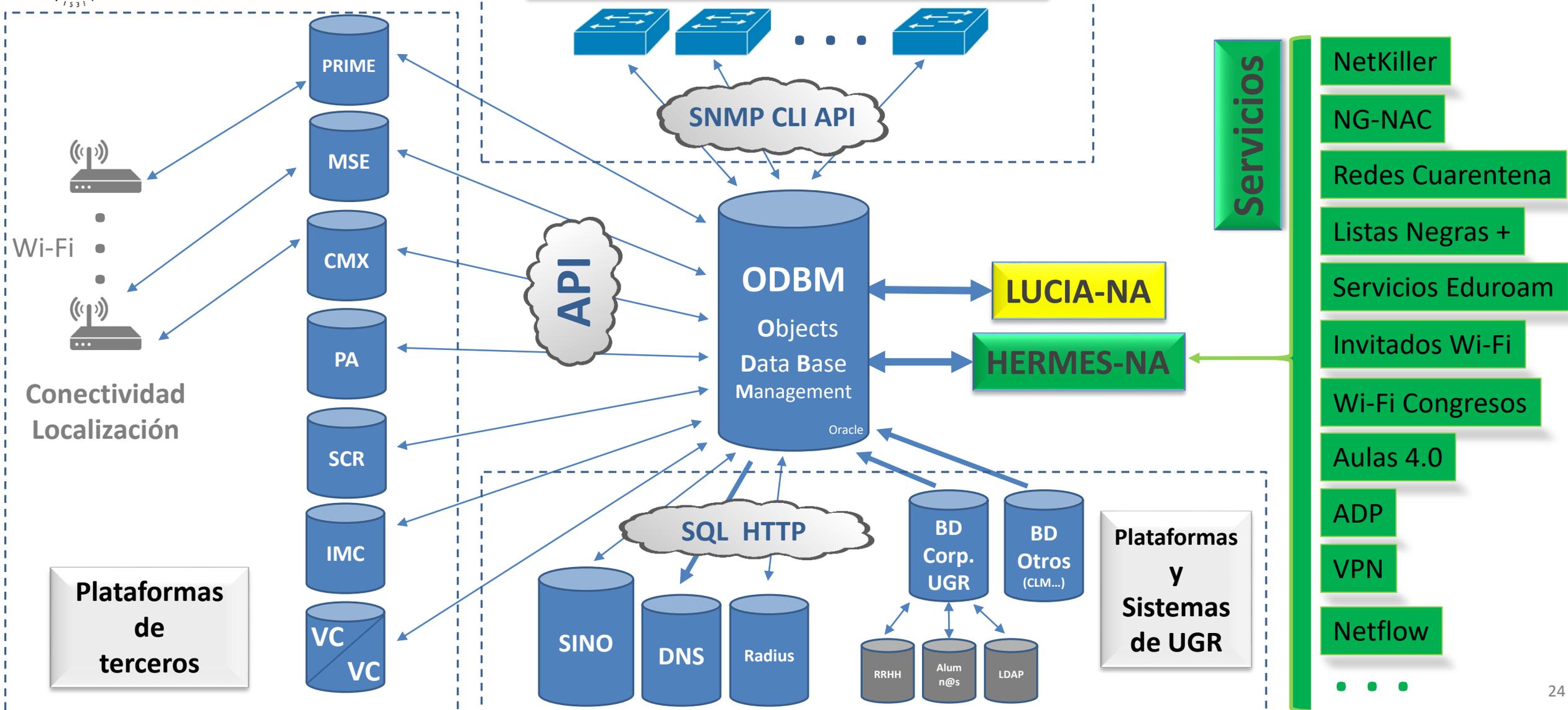
LUCIA-NA

HERMES-NA



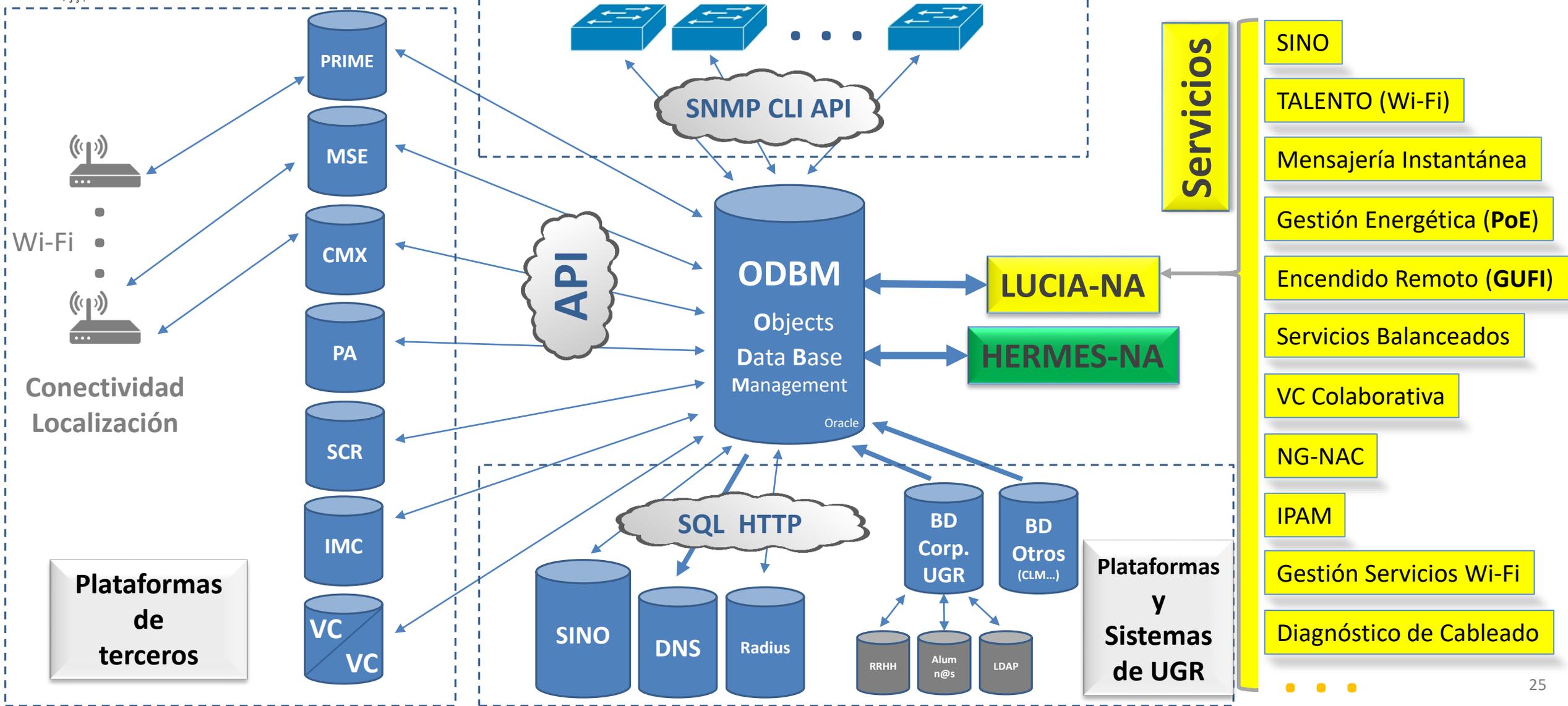


Infraestructura de RedUGR-NOVA (Núcleo, Distribución, Acceso, SDN, NetIoT)





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





3. LUCIA-NA y HERMES-NA



UNIVERSIDAD DE GRANADA **Acceso Identificado**

Usuario: ANTONIO RUIZ MOYA - Perfil: Personal

Inicio Cambiar Clave Salir

Centro de Gestión de RedUGR

UNIVERSIDAD DE GRANADA

HERMES-NA

LUCIA-NA

Núcleo ODBM

© SRC 2018

CSIRC CENTRO DE SERVICIOS DE INFORMÁTICA Y REDES DE COMUNICACIONES

UNIVERSIDAD DE GRANADA

Inicio Cambiar Clave

Aplicaciones

Aplicación

Actas

Centro Gestión RedUGR

UNIVERSIDAD DE GRANADA

UNIVER DE GRA

CSIRC

Centro de Gestión de RedUGR

UNIVERSIDAD DE GRANADA

HERMES-NA

LUCIA-NA

Núcleo ODBM

© SRC 2018



3. Sistema HERMES-NA

UNIVERSIDAD DE GRANADA **Acceso Identificado**

Usuario: ANTONIO RUIZ MOYA - Perf

[Inicio](#) [Cambiar Clave](#) [Salir](#)

Centro de Gestión de RedUGR

HERMES-NA

UNIVERSIDAD DE GRANADA

- Expedientes NetKiller
- Gestión Conexiones Inteligentes (NG-NAC)
- Redes de Cuarentena
- Listas Negras Avanzado
- Servicios Eduroam
- Invitados Wi-Fi



HERMES-NA

UNIVERSIDAD DE GRANADA

CSIRC

Centro de Gestión de RedUGR

HERMES-NA

UNIVERSIDAD DE GRANADA

- Expedientes NetKiller
- Gestión Conexiones Inteligentes (NG-NAC)
- Redes de Cuarentena
- Listas Negras Avanzado
- Servicios Eduroam
- Invitados Wi-Fi
- Wi-Fi Congresos

© SRC 2018

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

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

PS. toma AE-D7.23

COMENTARIO

ESTADO (-)

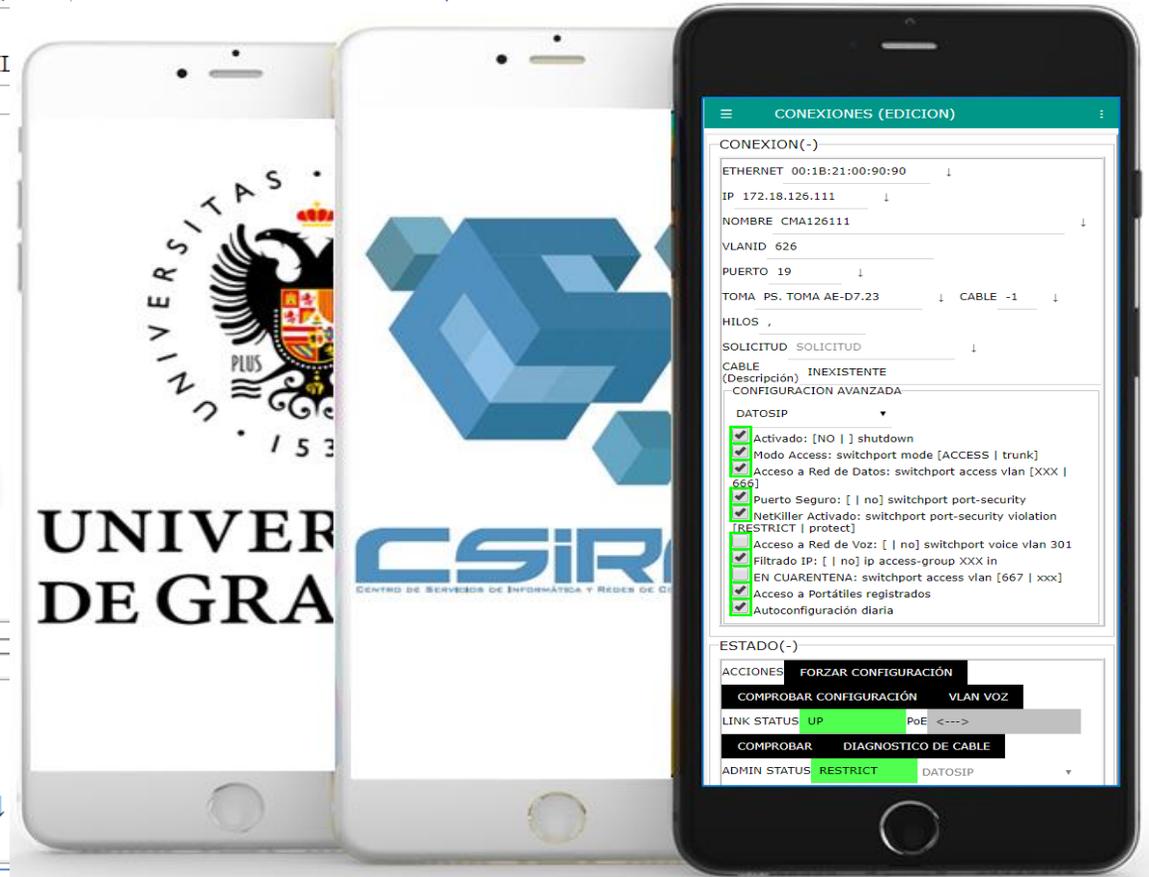
ACCIONES FORZAR CONFIGURACIÓN COMPROBAR CONFIGURACIÓN VLAN VOZ

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



Acceso Identificado

Usuario: ANTONIO I

Inicio Cambiar Clave Salir

Centro de Gestión de RedUGR

LUCIA-NA



UNIVERSIDAD DE GRANADA

Redes Ópticas (SINO)

Sistema TALENTO (Wi-Fi)

Mensajería Instantánea Telegram

Gestión Energética (POE) ▼



© SRC 2018

LUCIA-NA



© SRC 2018 VC Colaborativa



3. Sistema LUCIA-NA. SINO

SINO

LUCIA-NA

SINO - UNIVERSIDAD DE GRANADA
 Sistema de información de Red Óptica de la Universidad de Granada

Inicio | Administración | Operación | Procedimientos | Usted está accediendo a SINO como ADMINISTRADOR

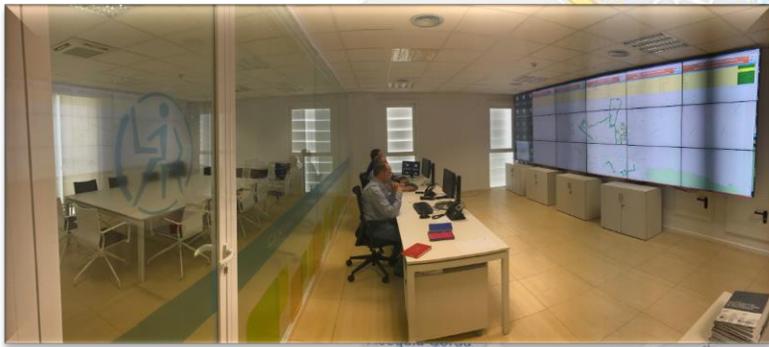
Mapa | Seleccionar todo | Eliminar Selección | PDF | Mostrar/Ocultar cols | Validar | Invaldar

Página 1 de 2 | 100

Administración | Operación | Procedimientos

- MAN
- LAN
- WLAN

- Elementos de registro
- Tramos
- Cables
- Enlaces
- Edificios
- Mapa Zonas



Universidad de Granada. Servicio de Redes y Comunicaciones. Más información: redes@ugr.es. 2017

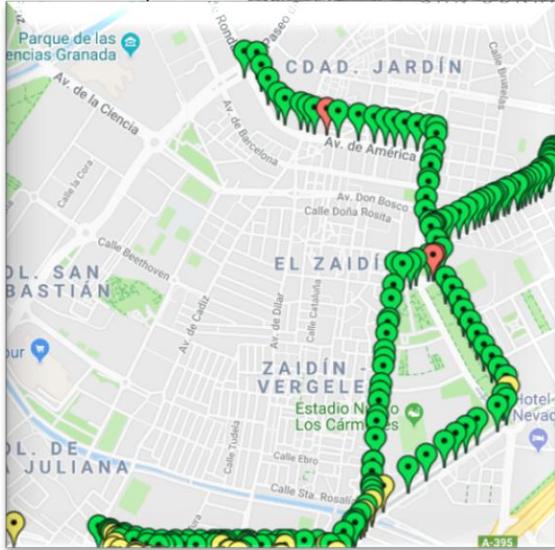
3. Sistema LUCIA-NA. SINO

SINO - UNIVERSIDAD DE GRANADA
Sistema de información de Red Óptica de la Universidad de Granada

Imágenes asociadas a la arqueta ALB026



SINO



Lista de cables

Mapa | Seleccionar todo | Eliminar Selección | PDF

Mostrar/Ocultar cols | Validar | Invaldar | Página 1 de 1 | 100

Codig	Acciones	Nombre	Edificio 1	Edificio 2	SM	MM	Modelo	Tipo F/O	Tipo Conect	Fecha insta	1002.4914	1157.0
1209		STA.LUCIA-ALMIRANTE	EDIFICIO SANTA LUCIA	PALACIO DEL ALMIRAN	24	12	PRYSMIAN OPS	OS2 + OM1 0	SC verde y beig	23-01-2009		

LUCIA-NA

Hilos del cable											
Acciones	Num	Tipo	Estado E1	Conectado en	Puerto/Hilo	Comentarios E1	Estado E2	Conectado en	Puerto/Hilo		
Panel en EDIFICIO SANTA LUCIA											
	1	MM	LIBRE				LIBRE				
	2	MM	LIBRE				LIBRE				
	3	MM	LIBRE				LIBRE				
	4	MM	LIBRE				LIBRE				
	5	MM	LIBRE				LIBRE				
	6	MM	LIBRE				LIBRE				
	7	MM	LIBRE				LIBRE				
	8	MM	LIBRE				LIBRE				
	9	MM	LIBRE				LIBRE				
	10	MM	LIBRE				LIBRE				
	11	MM	LIBRE				LIBRE				
	12	MM	LIBRE				LIBRE				
Panel en PALACIO DEL ALMIRAN											
	1	SM	OCUPADO	GVIA	1/3G8		OCUPADO	CPAPBPC001	1G1		
	2	SM	OCUPADO	GVIA	1/3G8		OCUPADO	CPAPBPC001	1G1		
	3	SM	OCUPADO	GVIA	1/3G9		OCUPADO	F/O ALMIRANTE-C.VICTORIA	1 SM		
	4	SM	OCUPADO	GVIA	1/3G9		OCUPADO	F/O ALMIRANTE-C.VICTORIA	1 MM		





3. Sistema LUCIA-NA. SINO Móvil



LUCIA-NA

SINO

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



F.Filosofía 24MM 0SM	
1 MM CARTUJA 2/3GB	1 MM SBIBLIOTECONOMIA T32
2 MM CARTUJA 2/3GB	2 MM SBIBLIOTECONOMIA T32
3 MM	3 MM
4 MM	4 MM
5 MM CARTUJA 1/3GB	5 MM SBIBLIOTECONOMIA T1
6 MM CARTUJA 1/3GB	6 MM SBIBLIOTECONOMIA T1

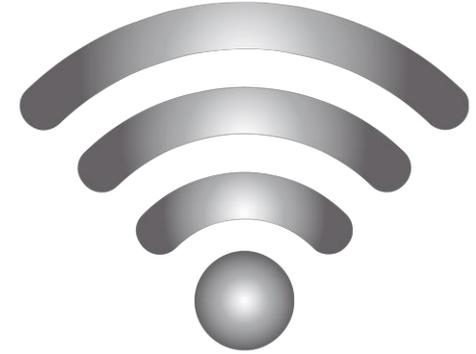


3. Sistema LUCIA-NA. Sistema TALENTO

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

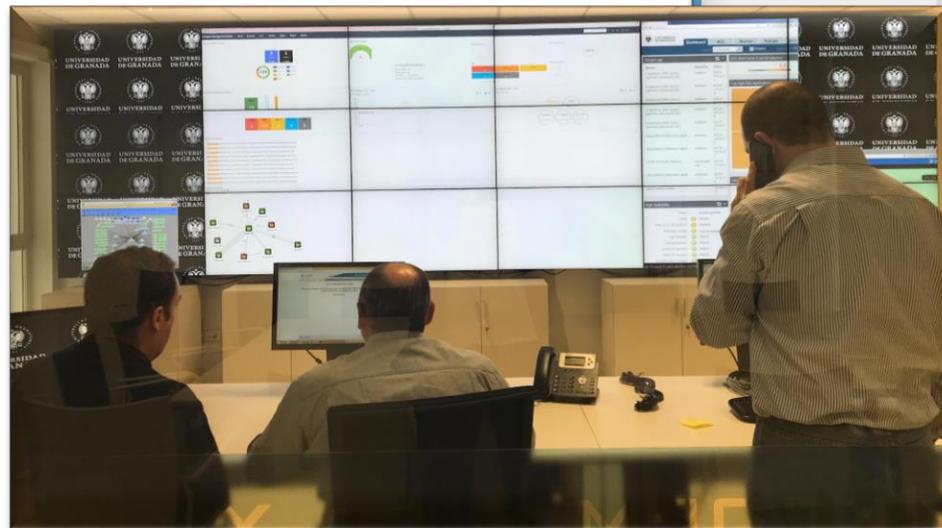
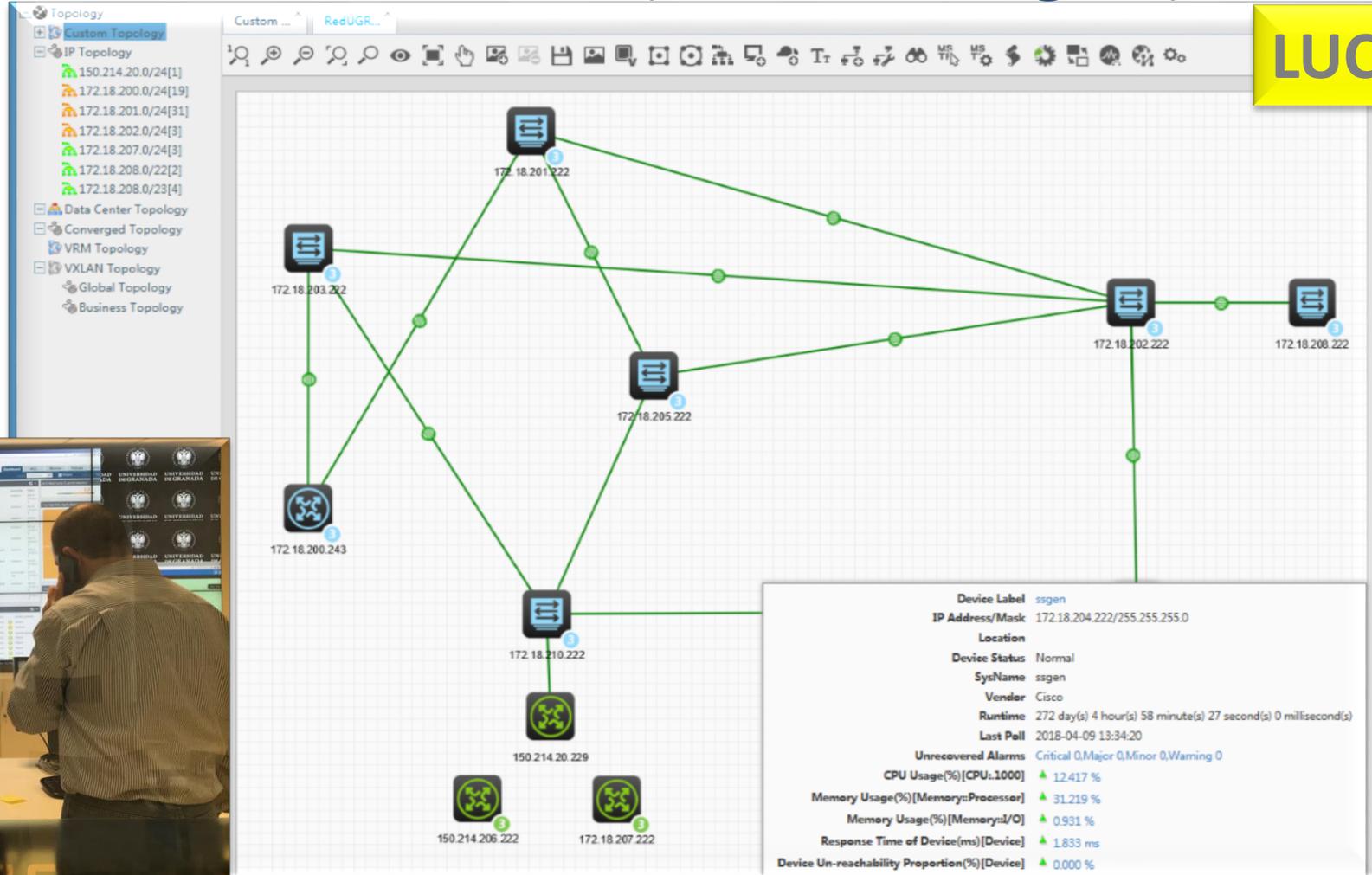


TOURIST INFO CENTER

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

The screenshot displays the Cisco Prime Infrastructure dashboard. At the top, it shows 'Prime Infrastructure' and 'Dashboard / Network Summary'. The 'Metrics' section includes:

- ICMP Reachability Status:** 7 All, 7 Reachable, 0 Unreachable.
- Alarm Summary:** 0 Critical, 0 Major, 0 Minor.
- Unified AP Status:** 1.24K All, 99.8% Reachable, < 1% Unreachable.
- Controller Status:** 3 All, 3 Reachable, 0 Unreachable.

The 'Coverage Area' section features a table with the following data:

Name	Total APs	Radio		Alarms	Clients	
		5 GHz	2.4 GHz		Wireless	Wired
Centro	298	298	298	2	2719	0
Ceuta	39	43	39	2	305	0
Aynadamar	89	89	89	1	1038	0
Cartuja	338	338	338	0	2850	0

The 'Client Count By Association/Authentication' graph shows a line chart of client counts over time from April 5 to April 9, 2018. The y-axis represents the client count, with a marker at 10,000. The x-axis shows dates from Apr 5 to Apr 9. The graph shows several peaks, with the highest peak occurring on April 9.

At the bottom, a 'CONFIGURATION' panel displays system metrics:

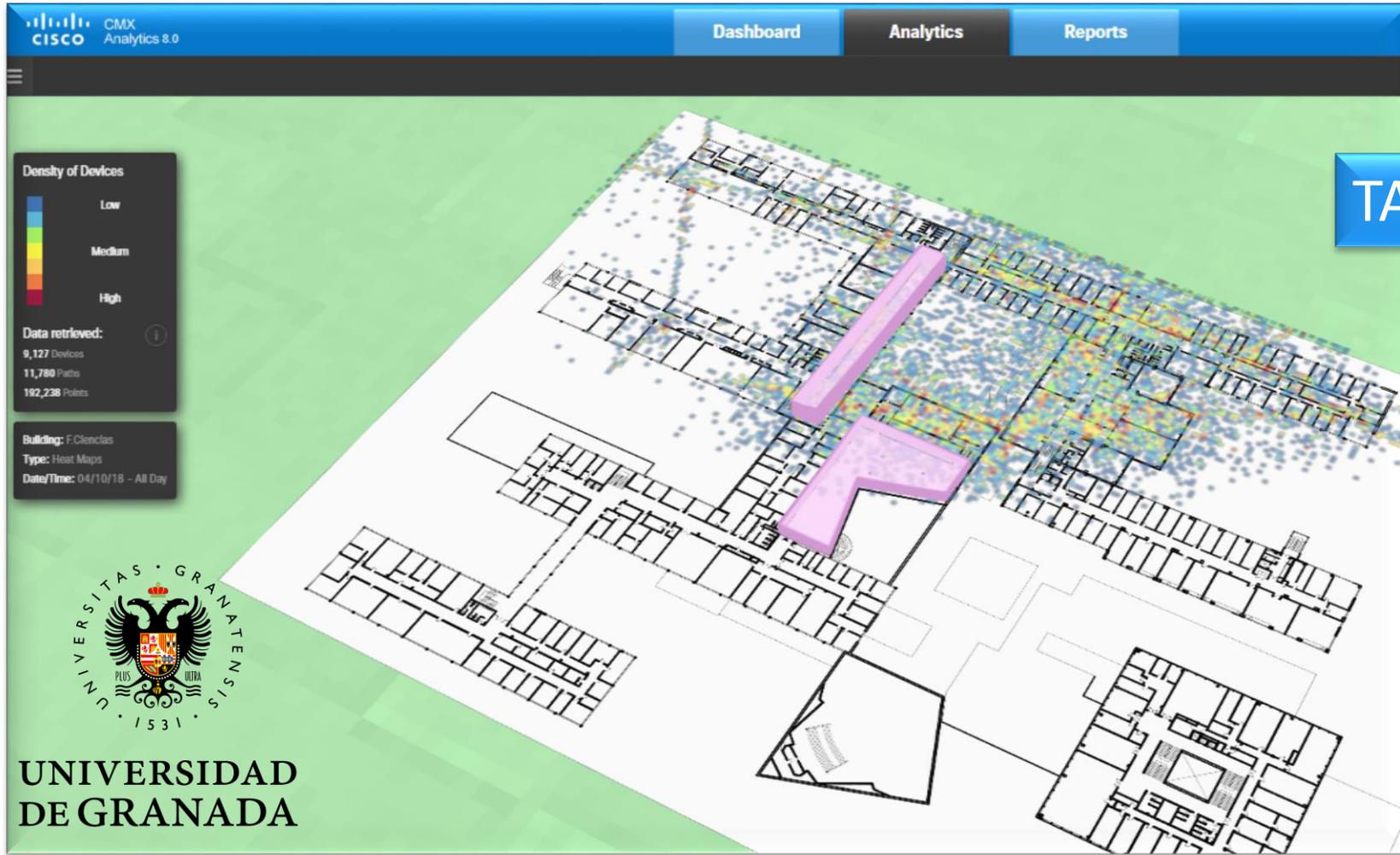
- Active Clients: 21276
- Memory Utilization: 74.22%
- CPU Utilization: 63.80%
- Location Calculation Latency: N/A

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

LUCIA-NA

Orientación a la localización

TALENTO



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)

UNIVERSIDAD DE GRANADA CSIRC

contacto | directorio | mapa web

Inicio > RedUGR

Servicios de Red Ofertados

- RedUGRNova
- Conexiones a RedUGR
- Campus Virtual Analámbrico (CVI-UGR)
- Aulas de Docencia Presencial (ADP)
- Aulas de docencia 4.0
- Red de Control Multimedia
- RedUGR2
- Acceso VPN a RedUGR
- Videoconferencia Profesional
- Normativa Cableado Estructurado
- Toma Multiservicios (TM)
- Sistema GUF1 de Encendido Remoto

UNIVERSIDAD DE GRANADA CSIRC

iris.ugres

Authentication Required

e-mail o nombre de usuario

Contraseña

Inicia sesión

Copyright © CSIRC (Nodo Fuentenueva)

Sistema de Gestión de Tickets - Nodo Fuentenueva
Centro de Servicios de Informática y Redes de Comunicaciones

LUCIA-NA



Help Desk SRC-UGR

Gabriel
Servicio Redes y Comunicaciones

Yo: Buenos días. 10:19

Gabriel se ha unido al chat

Gabriel: Gracias por usar el chat piloto del Servicio de Redes y Comunicaciones del CSIRC. 10:20

Gabriel: ¿En qué puedo ayudarle? 10:20

Les rogaría información sobre...

Get Free live chat by SmartSupp

Enviar

Historial

Número de chats: 1.074

Buscar

1521798765618	Gabriel	23/3/2018 10:53	20 min	😊	15	Hola, vemos que est...
1521796981018	Gabriel	23/3/2018 10:41	18 min	😊	24	Hola, al introducir m...
1521793868295	Gabriel	23/3/2018 9:33	3 min	😊	9	buenos dias tengo c...
1521723572035	Gabriel	22/3/2018 13:59	28 min	😊	39	Hola, como puedo p...
1516385466139	Gabriel	22/3/2018 12:49	33 min	😊	86	Hola: Gracias por us...
1521718987254	Gabriel, Elvira	22/3/2018 12:44	3 min	😊	7	Hola, vemos que est...
1521633222005	Elvira	22/3/2018 12:43	1 min	😊	3	Estimados, favor not...
1521715950478	Gabriel	22/3/2018 11:53	10 min	😊	20	Hola, vemos que est...
1521715629536	Gabriel	22/3/2018 11:48	2 min	😊	7	Hola, vemos que est...
1521711310509	Gabriel	22/3/2018 11:31	43 min	😊	108	buenas gabriela: he ...

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



Scrutinizer > Status - Google Chrome

lupa.ugr.es/#tab=tab3&subCat=report&rpt_json={"reportTypeLang":"applications","reportDirections":{"selected":"both"},"times":{"dateRan...}}

Dashboard Maps Status Alarms Admin Help

Run Report Top Search System Views Vendor Specific

Device Explorer
Current Report

Report: Flujos RedUGR Attack607

Templates Used: 1
Devices Used: 1

Report Details

Filters

Device/Interface edit x

Device: ciencias.ugr.es
Interface: cgp1pc103-0/1 (TenGigabitEthernet1/2) - 3

Threshold Add

Saved Reports

▼ Top » Applications Defined From 2018-04-11 10:30 to 2018-04-12 10:30

intervals

Inbound Results, speed: 1 Gb/s

Application	Packets	Traffic %	Bandwidth
1 HTTPS (443 - ...)	8,459 Mp	49.28 %	0.104 %
2 undefined (5...	18,117 Mp	26.48 %	0.056 %
3 HTTPS (443 - ...)	7,012 Mp	14.97 %	0.031 %
4 HTTP (80 - T...	6,265 Mp	3.50 %	0.007 %
5 submission (...)	92,701 kp	0.60 %	0.001 %
6 ms-wbt-serv...	537,254 kp	0.59 %	0.001 %
7 plethora (348...	209,609 kp	0.57 %	0.001 %
8 IMAP (143 - ...)	189,942 kp	0.46 %	0.001 %

Outbound Results, speed: 1 Gb/s

Application	Packets
1 undefined (5...	36,787 Mp
2 HTTP (80 - T...	16,383 Mp
3 HTTPS (443 - ...)	13,587 Mp
4 HTTPS (443 - ...)	4,090 Mp
5 imaps (993 - ...)	1,280 Mp
6 IMAP (143 - ...)	290,581 kp
7 sac (8097 - T...	242,097 kp
8 microsoft-ds ...	253,796 kp

Scrutinizer > Status - Google Chrome

lupa.ugr.es/#tab=tab3&subCat=report&rpt_json={"reportTypeLang":"conversationsApp","saved":{},"reportDirections":{"default":"inb...}}

Dashboard Maps Status Alarms Admin Help

Run Report Top Search System Views Vendor Specific

Device Explorer
Current Report

Report: Flujos RedUGR Attack607_1

Templates Used: 1
Devices Used: 11

Report Details

Filters

Device/Interface edit x

Device: All Devices

Threshold Add

Saved Reports

▼ Pair » Conversations App From 2018-04-12 10:35 to 2018-04-12 10:40 in 5m intervals

Inbound Results

Sour...	Application	De...	Packets	Traffic %	Bits
1 bioest...	undefined (53560 UDP)	83...	820 p	6.51 %	683,008 kb
2 bioest...	BitTorrent (6889 - UDP)	122...	117 p	3.18 %	333,216 kb
3 bioest...	BitTorrent (6889 - UDP)	213...	81 p	2.16 %	226,800 kb
4 bioest...	BitTorrent (6889 - UDP)	125...	82 p	2.09 %	219,376 kb
5 bioest...	socorfs (3379 - UDP)	194...	60 p	1.51 %	158,592 kb
6 bioest...	BitTorrent (6889 - UDP)	dil1...	53 p	1.42 %	149,248 kb
7 bioest...	BitTorrent (6889 - UDP)	178...	44 p	1.10 %	114,816 kb
8 bioest...	BitTorrent (6889 - UDP)	182...	39 p	0.98 %	102,256 kb
9 bioest...	BitTorrent (6889 - UDP)	213...	35 p	0.93 %	98 kb

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



UNIVERSIDAD DE GRANADA
Dashboard ACC Monitor Policies Objects Network Device

Layout: 3 Columns Widgets Last updated: 19:06:11

Threat Logs

Name	Severity	Time
Adobe PDF File With Embedded Javascript	informational	04/09 19:06:07
ZeroAccess.Gen Command and Control Traffic	critical	04/09 19:06:05
ramnit.Gen Command And Control Traffic	critical	04/09 19:06:00
HTTP OPTIONS Method	informational	04/09 19:05:59
ZeroAccess.Gen Command and Control Traffic	critical	04/09 19:05:55
ZeroAccess.Gen Command and Control Traffic	critical	04/09 19:05:53
ramnit.Gen Command And Control Traffic	critical	04/09 19:05:52
HTTP GET Requests Long URI Anomaly	low	04/09 19:05:50
generic:c2r.dynu.net	medium	04/09 19:05:48
generic:c2r.dynu.net	medium	04/09 19:05:48

ACC Risk Factor (Last 60 minutes)

3.5

Top High Risk Applications

High Availability

Mode	Active-passive
Local	Active
Peer (172.18.208.92)	Passive
Running Config	Synchronized
App Version	Match
Threat Version	Match
Antivirus Version	Match
PAN-OS Version	Match
GlobalProtect Version	Match
HA1	Up
HA1 Backup	Up
Heartbeat Backup	Up
HA2	Up
HA2 Backup	Up

Interfaces

System Resources

Management CPU	41%
Data Plane CPU	43%
Session Count	565891 / 4194302

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



4. En fase de lanzamiento. Próximamente,...

LUCIA-NA

HERMES-NA

The screenshot shows a web form for requesting a professional collaborative video conference. The header includes the University of Granada logo and CSIRC name. A search bar and navigation links are visible. The main content area is titled 'Solicitud de Videoconferencia Profesional Colaborativa Web' and is part of a multi-step process (Paso 2/7). The form fields are as follows:

DATOS DEL SOLICITANTE	
SOLICITANTE:	GENARO GARCÍA
Telefono de contacto(*):	9582 Ext.:
Telefono alternativo / Movil(*):	
Email(*):	XXXXXX@ugr.es
Motivo de la videoconferencia(*):	
Fecha(*):	Calendario ?
Hora inicio(*):	08:00
Hora fin(*):	17:30
Nº de personas asistentes en UGR(*):	
Nº aproximado de personas que se conectarán a la videoconferencia web(*):	1 (Sin contar los asistentes en la sala de la Universidad de Granada) ?



4. En fase se lanzamiento. Próximamente,...

LUCIA-NA

HERMES-NA

Inicio > RedUGR > Videoconferencia > Videoconferencia Profesional Colaborativa Web

▣ Videoconferencia Profesional Colaborativa Web

OFRECEMOS...

- Para Estudiantes
- Para PAS
- Para PDI
- Cuentas Institucionales
- Tarjeta Universitaria
- RedUGR
- Apoyo a la Docencia
- Correo Electrónico
- Supercomputación
- Telecomunicaciones
- Red Administrativa
- Aplicaciones

Pulse para entrar en su reunión

Ingresar en tu cuenta

Iniciar Videoconferencia

UNIVERSIDAD DE GRANADA

© Servicio de Redes y Comunicaciones





4. En fase de 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



- Project Planning*
- Quality Management*
- Development*
- Analysis*
- Controlling*
- Plan*
- System*
- Resources*
- Team*
- Budget*

Success



UNIVERSIDAD
DE GRANADA



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

ANTONIO RUIZ MOYA

ARUIZ@UGR.ES

SERVICIO DE REDES Y COMUNICACIONES

UNIVERSIDAD DE GRANADA



UNIVERSIDAD
DE SALAMANCA

Thank You!



Imágenes bajo licencia CCO

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

Jornadas
Técnicas
de RedIRIS
2018

Del 7 al 10 de mayo
Presentando el programa
de la Universidad de Salamanca

