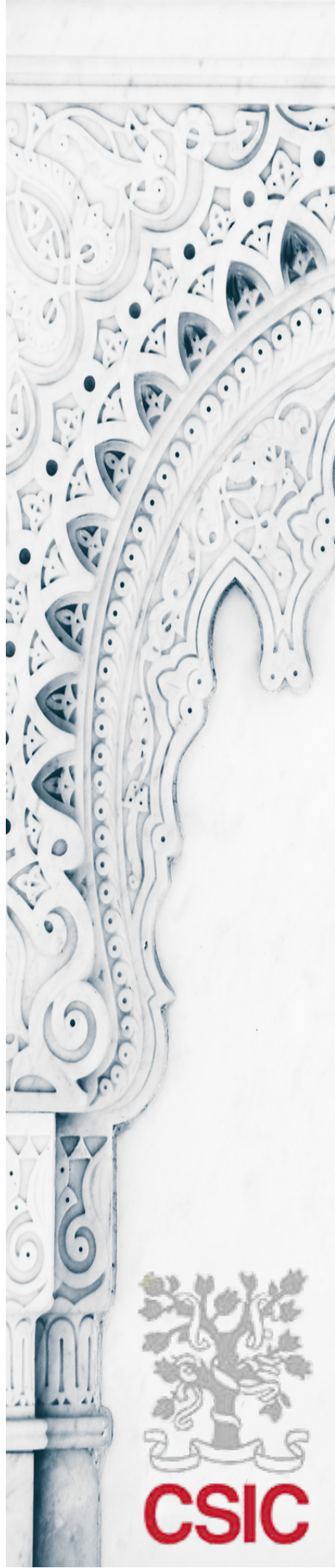
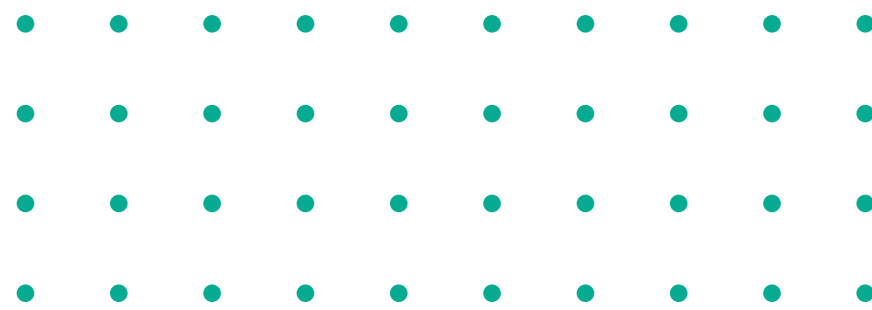


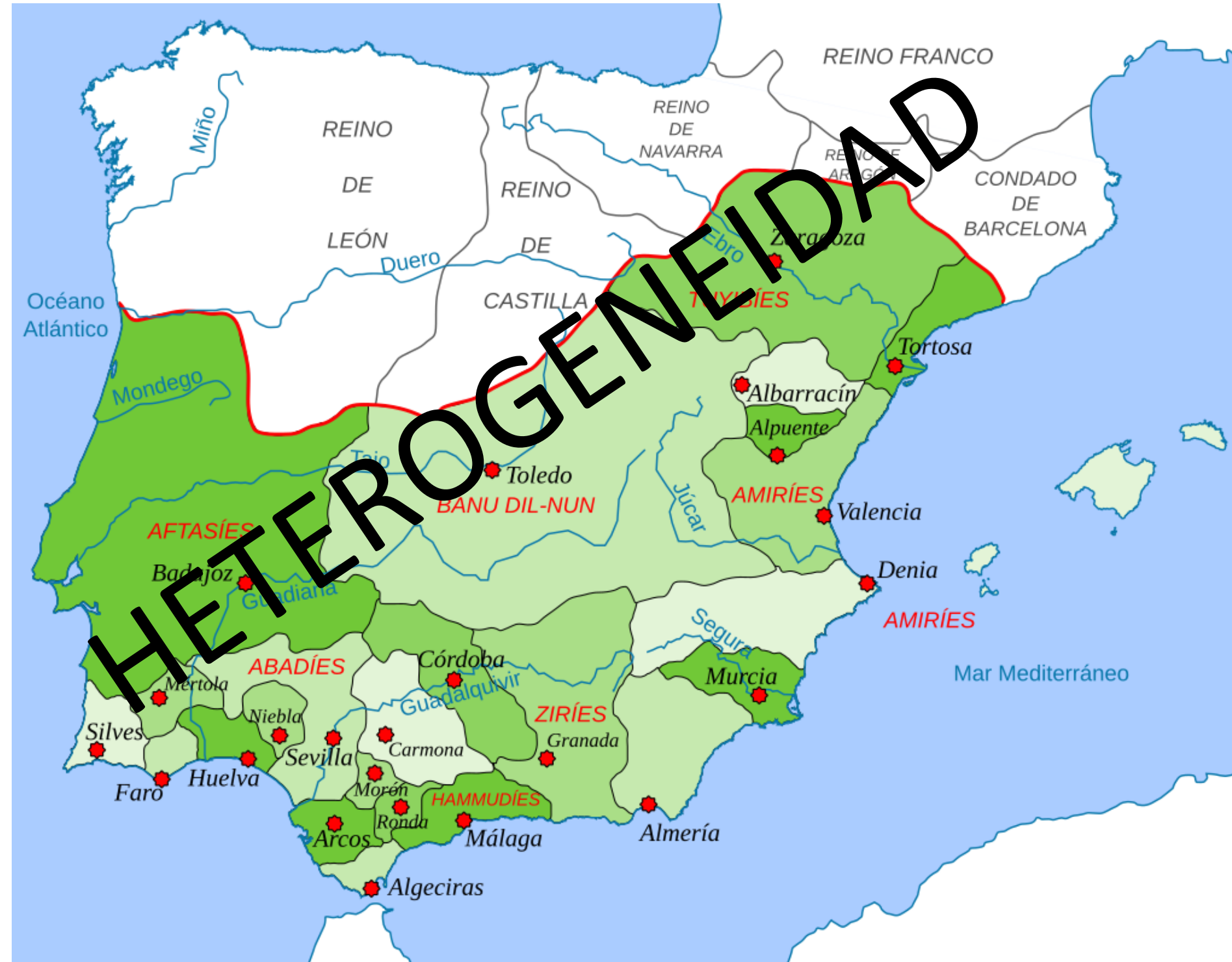
Segmentación, NAC y distribución de servicios básicos de red

JAVIER DE LA FUENTE LOPEZ (CSIC)
JAVIER MERINO AYUSO (CSIC-UAM)



Situación de partida

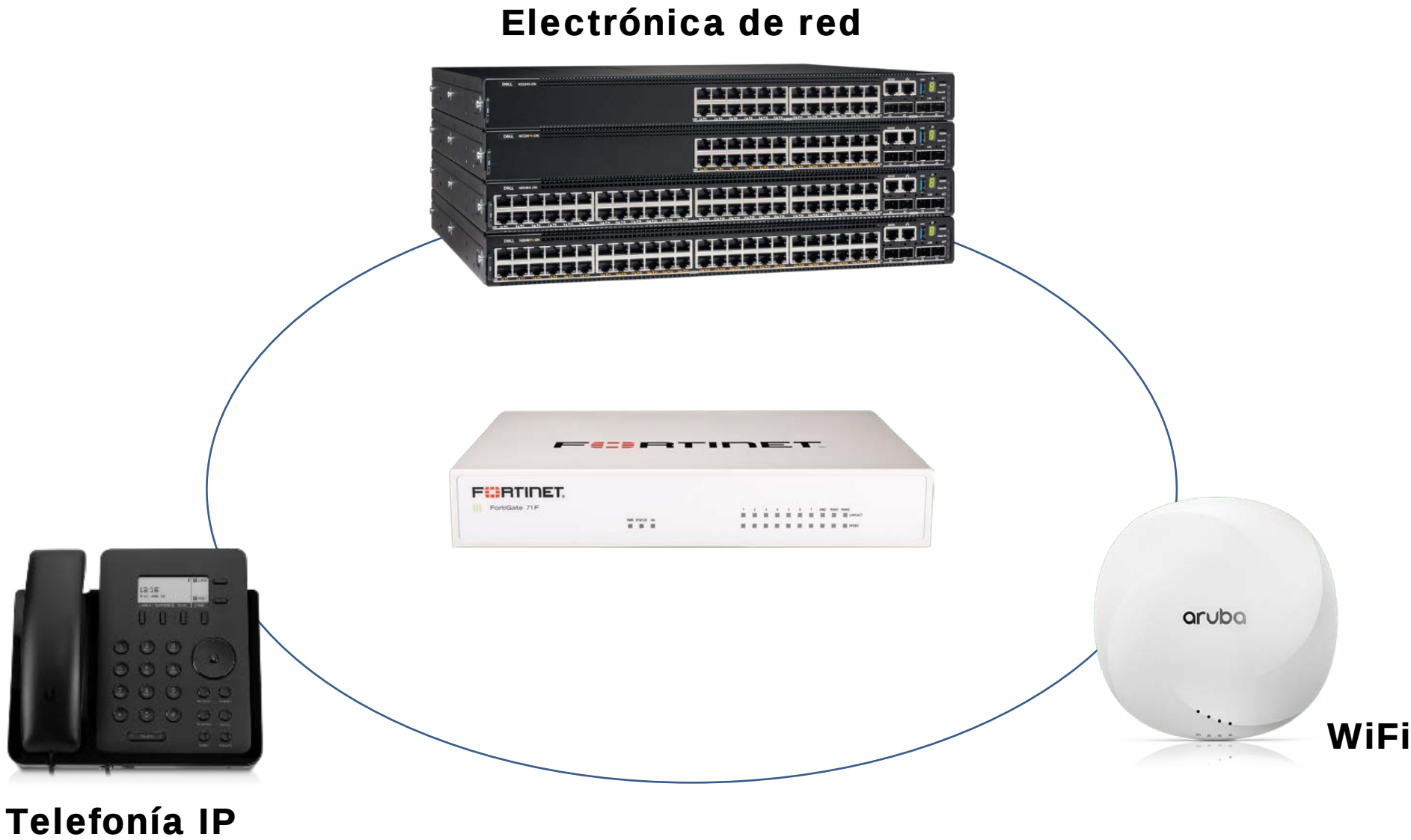
- 121 ICUs (Institutos, Centros y Unidades): 69 propios + 52 titularidad mixta + 3 centros nacionales
- Aprox. 140 TICs
- Desarrollo aislado de la infraestructura de red



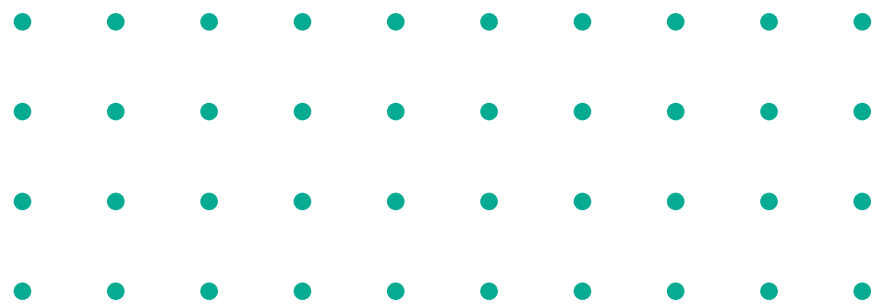
Fuente: wikipedia

Situación de partida

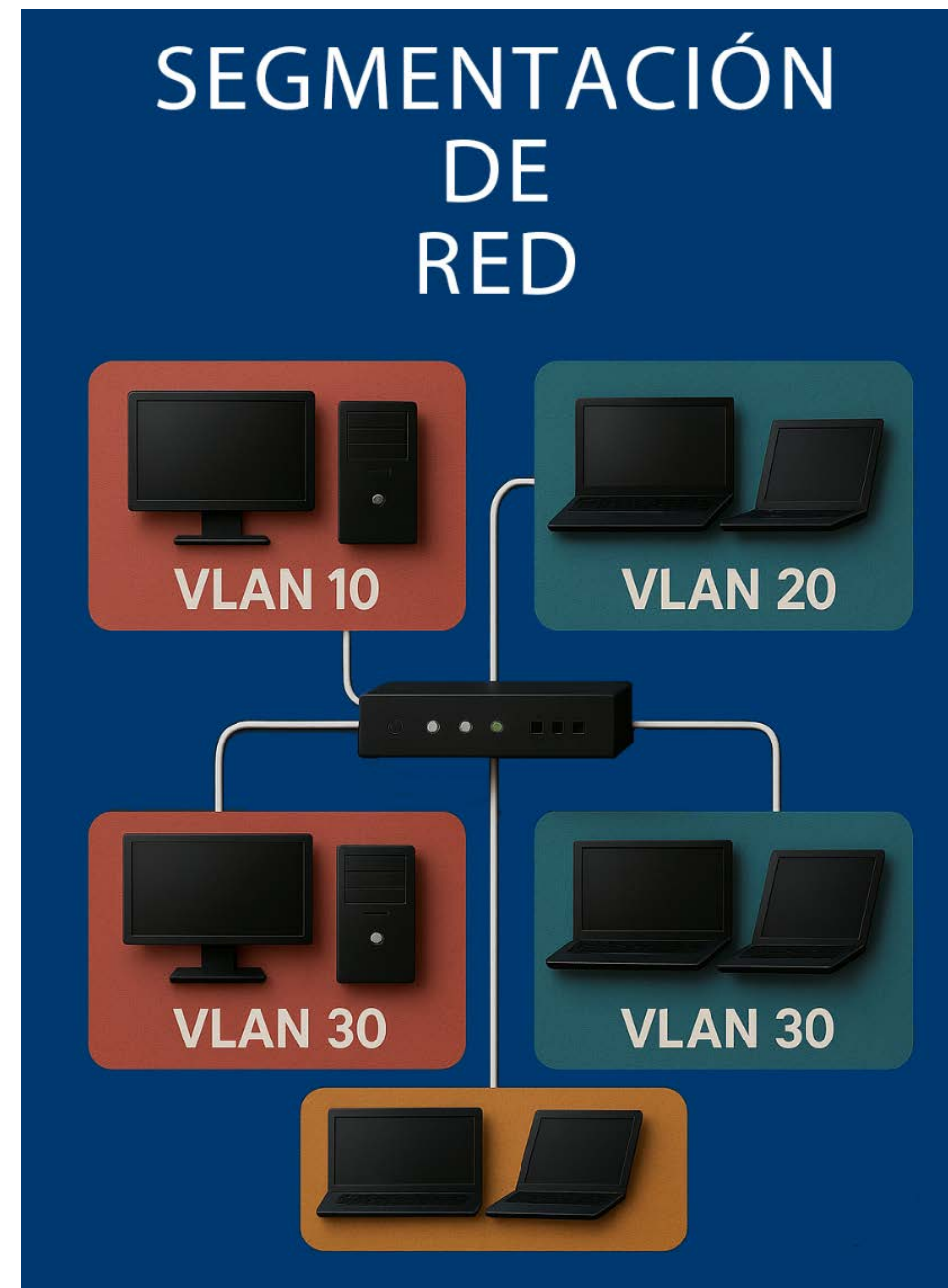
Equipos hardware y Servicios desplegados



Segmentación de red + Direccionamiento IPv4



Segmentación de red + Direccionamiento IPv4



➤ SEGMENTACIÓN

- Redes cableadas escasamente segmentadas
- Segmentación únicamente en WiFi

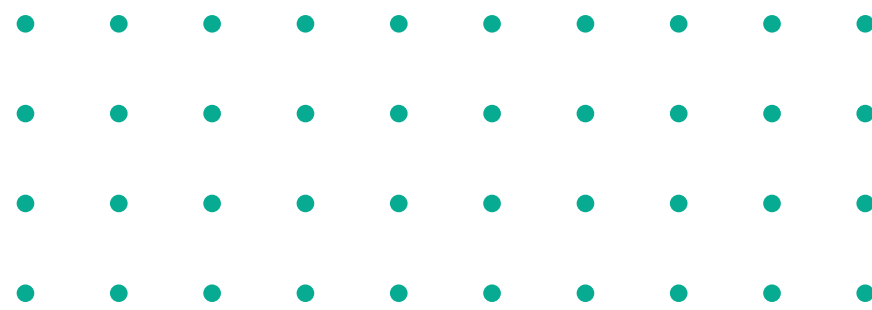
➤ DIRECCIONAMIENTO IPv4

- Direccionamiento IP mixto
 - Público (CSIC, Universidad, CCAA,...)
 - Privado (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16)
 - Asignación por DHCP y en otros casos con IP estática.

➤ MANTENIMIENTO

Poco conocimiento especializado en el ámbito de las redes en los ICUs

- ✓ Servicio ofrecido desde el Área de CyS



Listado de VLANs (L2)

ID	Dir. IP	NOMBRE	DESCRIPCIÓN	Extra
21 / 210		VoIP	Terminales y equipamiento de Telefonía IP	
17/ 26	10.XXX.17.0/24 10.XXX.26.0/24	Switches_Gestion	Switches de infraestructura del ICU.	
96	10.XXX.96.0/21-22	<Reservada a Siglas_ICU>	Reservada para un red del ICU de mayor tamaño.	*
100	10.XXX.100.0/22	<Siglas_ICU>	Red de equipos de servicios generales y equipos de investigación	
108	10.XXX.108.0/24	Gerencia	ZERO TRUST ZONE	
120	10.XXX.120.0/24	Servidores	200	10.XXX.200.0/23 <Siglas_ICU>_NO_EDR Dispositivos corporativos sin capacidad de instalación de EDR+Microclaudia (Obsoletos, equipos de instrumentación, etc.) ZT
128	10.XXX.128.0/24	Servidores_Gest		
136	10.XXX.136.0/24	SAN_NAS	204	10.XXX.204.0/23 Portatiles_Ext Portátiles personales, no corporativos. ZT
140	10.XXX.140.0/24	Impresoras	208	10.XXX.208.0/24 Cuarentena Equipos en cuarentena por incidencia. ZT
148	10.XXX.148.0/24	Cams_Vigilancia	212	10.XXX.212.0/24 Instalaciones Equipos que están siendo instalados. ZT
152	10.XXX.152.0/24	IoT	216	10.XXX.216.0/24 Restringida Equipos con E/S restringida o portal cautivo. ZT
180	10.XXX.180.0/24	Servicio_TIC	218	10.XXX.218.0/24 Cursos Equipos controlados o no. ZT
WIFI				
			400	WIFI_Gestion Gestión de equipos WiFi (Controladores, Aps, etc.)
			401	WIFI_CSIC Red WiFi del CSIC
			402	WIFI_Eduroam Red WiFi Eduroam ZT
			403	WIFI_Invitados WiFi para invitados. ZT
DIRECCIONAMIENTO EXTERNO				
500/ 600	Dir. IP público		DMZ	Servidores en la DMZ
777			MACROLAN	

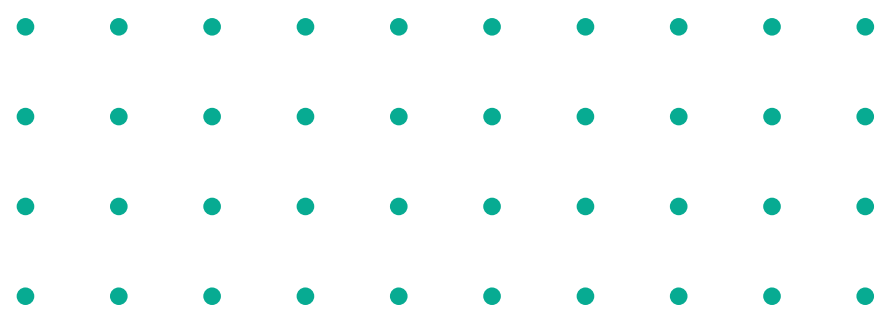


Formato de direccionamiento IPv4 (L3)

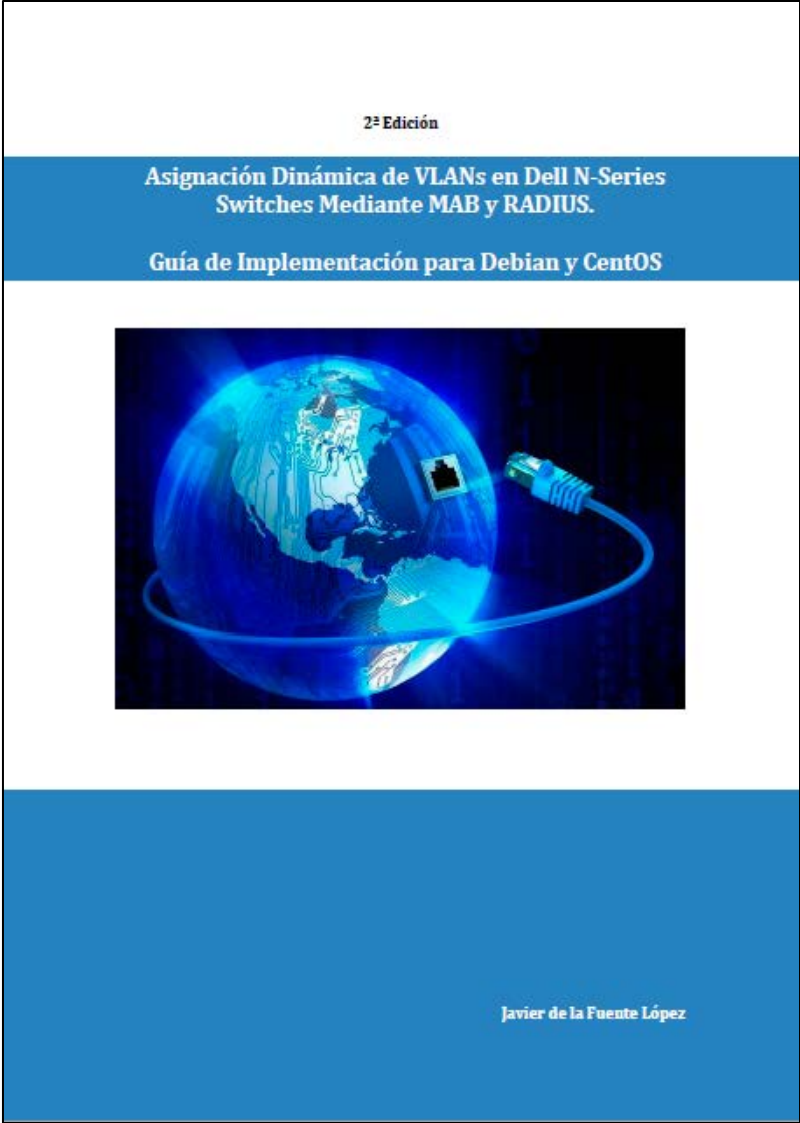
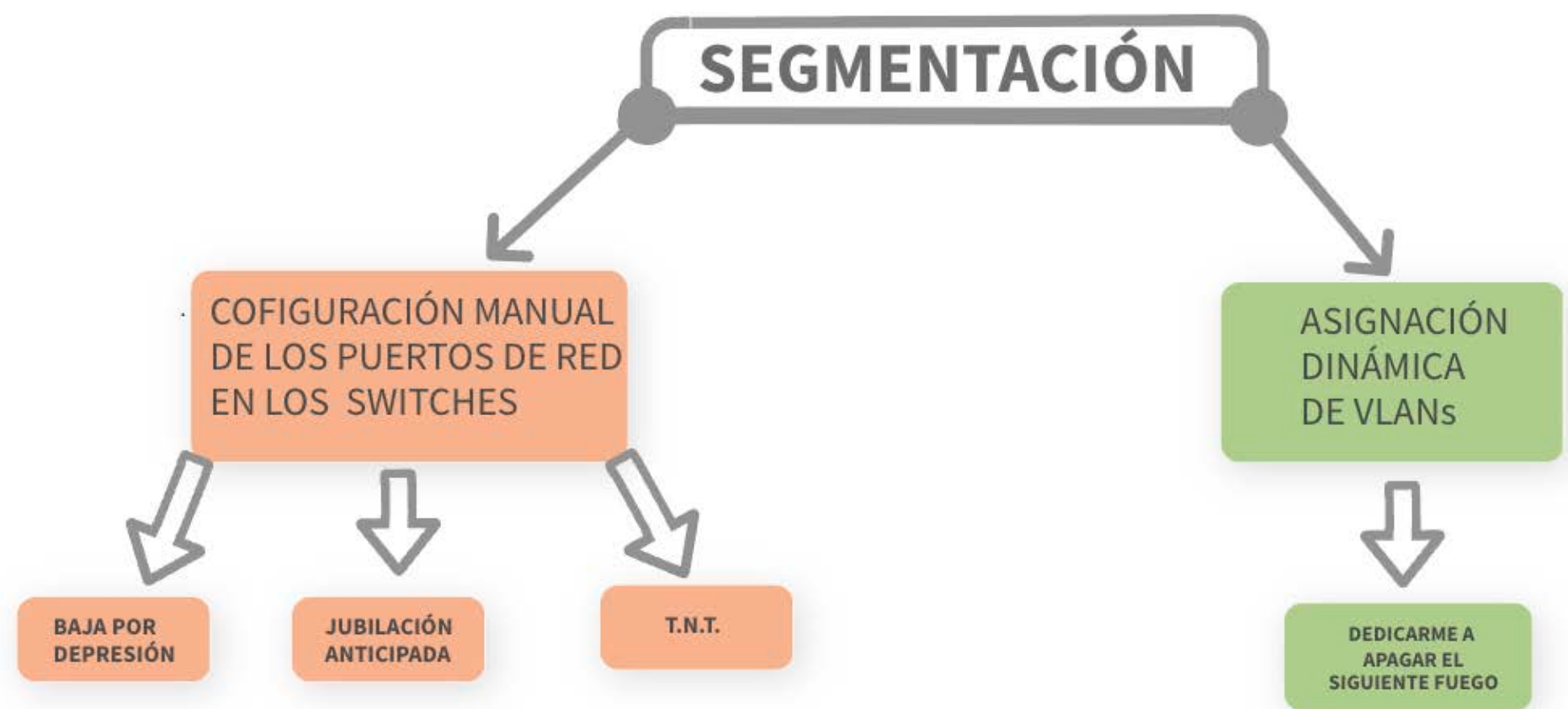
10.73.100.0

10.ICU.TIPO.0

- A cada ICU se le asigna un segmento /16 completo del rango 10.0.0.0/8
 - 2º octeto determina el ICU.
 - 10.73.0.0/16 : EEA
 - 10.251.0.0/16 : IRNASA
 - 3º octeto determina el TIPO de equipos incluidos en la subred (Gerencia, Gr. Investigación, IoT.)
 - 10.73.152.0/24 : IoT EEA
 - 10.251.152.0/24 : IoT IRNASA



Asignación dinámica de VLANs



NAC basado en MAB

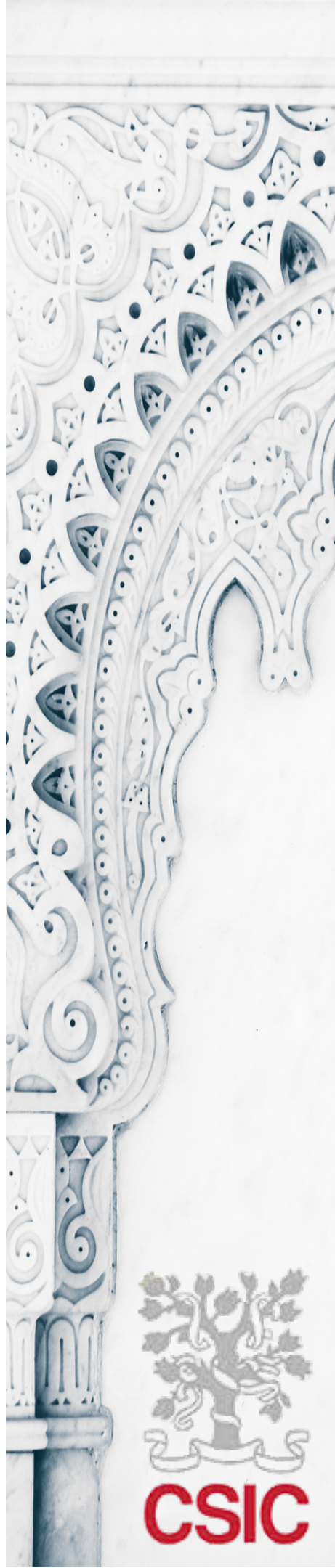
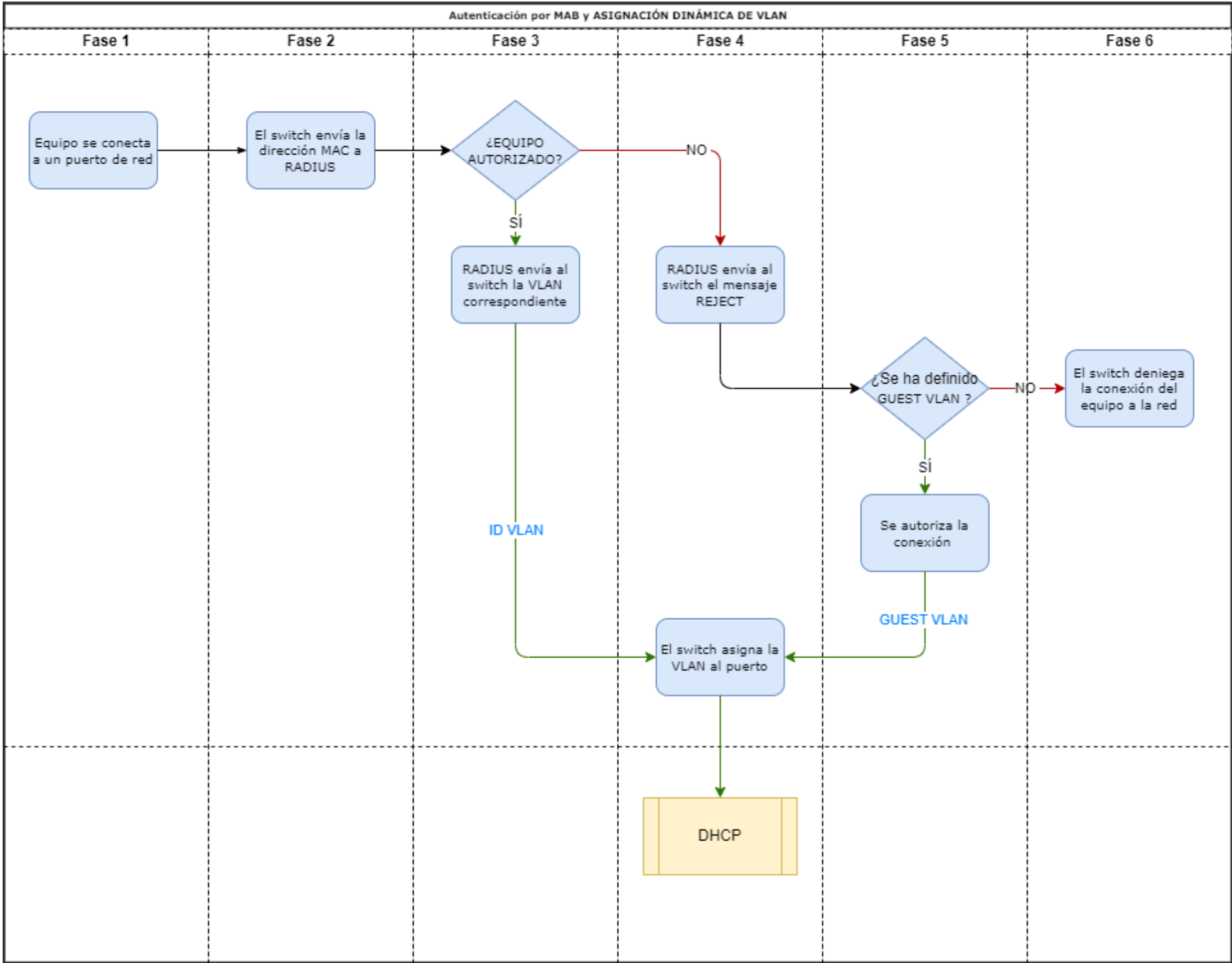
NETWORK ACCESS CONTROL MAC-ADDRESS AUTH BYPASS



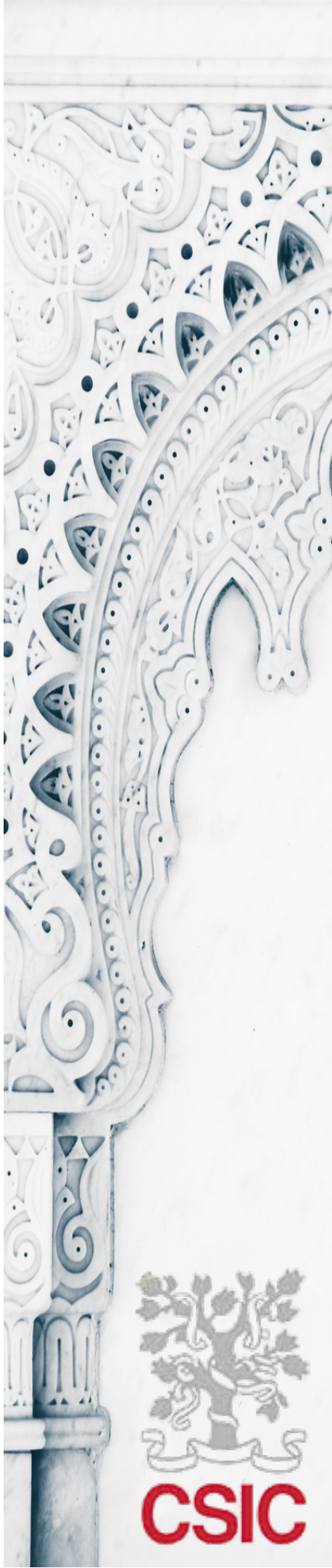
- **Elementos implicados**
 - ❑ Dispositivo del usuario, autenticador (conmutador) , servidor de autenticación (Radius)
- **Control de los dispositivos que se conectan a la red cableada basado en la dirección Ethernet**
 - ❑ Necesidad de inventario
- **Dotar a los ICUs de un equipo en local de gestione los servicios básicos de red. En fase de definición de la plataforma**
 - ❑ Servidor Linux + Docker
- **Beneficios**
 - ❑ Control
 - ❑ Automatización
 - ❑ Movilidad



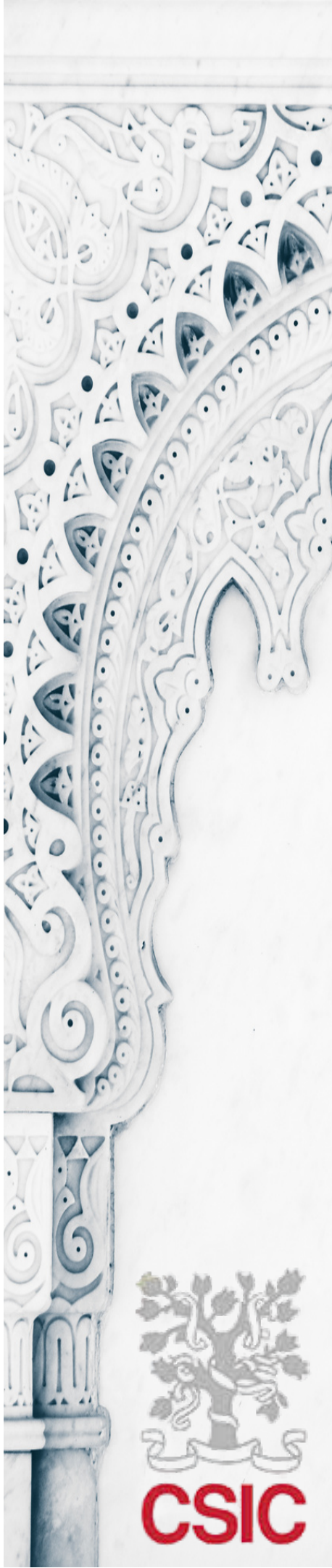
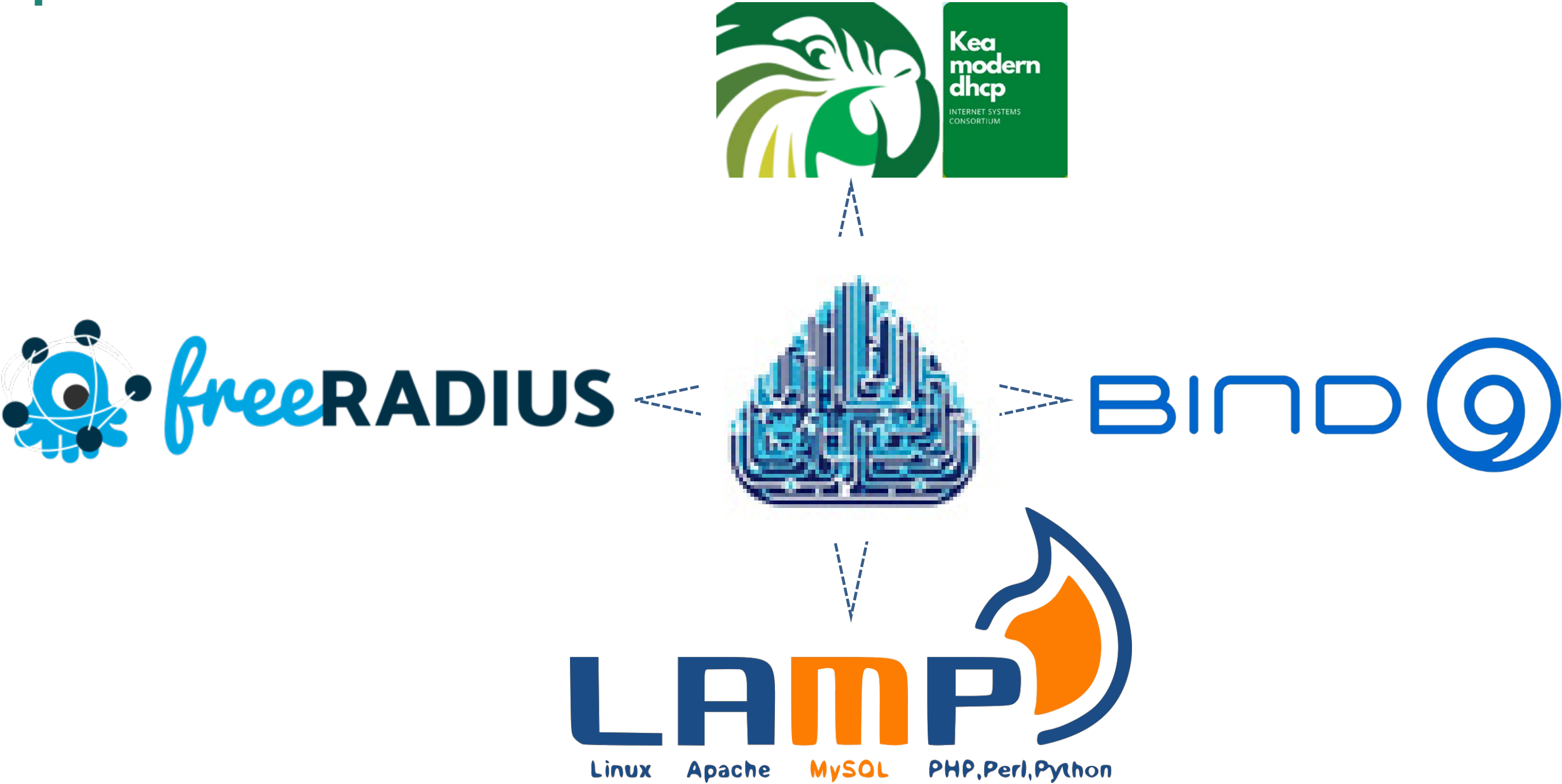
NAC basado en MAB



Componentes del sistema



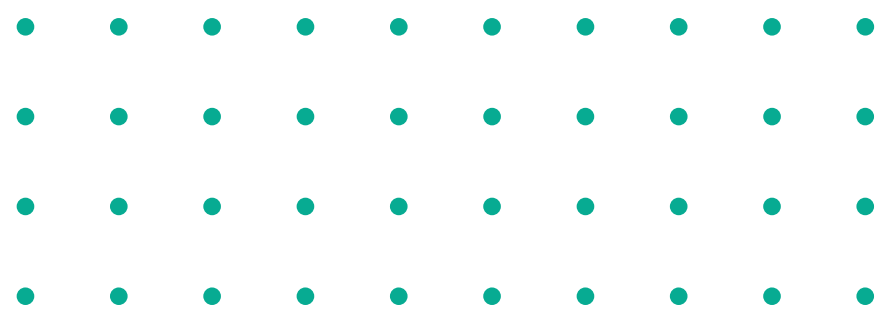
Componentes del sistema





ANSIOSO

All Network Services In One SO





Equipos - ANSIOSO

←

ANSIOSO

Equipos

Extra

Localizaciones

SS.OO.

Usuarios

Subredes

Switches

Zonas DNS

Gestión de Equipos

Subred: EEA

+ Nuevo Equipo

Filtrar: texto a buscar

Borrar	IP ↑	DirecciónMAC	Estado	Conex.	Info	Nombre	Ult. Acceso	Perfil FGT
	10.73.100.1	00:00:00:00:00:00			▶	VLAN-9		Completo
	10.73.100.2	08:5B:0E:53:94:76			▶	fortigate-60d	12 Sep 2023	Completo
+ 10.73.100.3								
	10.73.100.4	00:00:00:00:00:00			▶	tem-4		
	10.73.100.5	00:00:00:00:00:00			▶	pc-5		
+ 10.73.100.6								
	10.73.100.7	00:00:00:00:00:00			▶	inv-7		
+ 10.73.100.8								
	10.73.100.9	00:00:00:00:00:00			▶	WOL-VLAN9		Completo
	10.73.100.10	C8:D3:FF:BC:D7:77			▶	srv-aio	12 Oct 2022	Completo
+ 10.73.100.11								
	10.73.100.12	B4:A9:FC:B7:58:D8			▶	Taller-Port	15 Sep 2023	Completo
	10.73.100.13	40:B0:34:1C:8A:20			▶	secdir-pc	13 Mar 2023	Completo
+ 10.73.100.14								
	10.73.100.15	00:00:00:00:00:00			▶	TEST-15		
+ 10.73.100.16								
+ 10.73.100.17								

Equipos - ANSIOSO

←

ANSIOSO

Equipos

Extra

Localizaciones

SS.OO.

Usuarios

Subredes

Switches

Zonas DNS

Gestión de Equipos

Subred: EEA

+ Nuevo Equipo

Filtrar: texto a buscar

Borrar	IP ↑	DirecciónMAC	Estado	Conex.	Info	Nombre	Ult. Acceso	Perfil FGT
	10.73.100.1	00:00:00:00:00:00			▶	VLAN-9		Completo
	10.73.100.2	08:5B:0E:53:94:76			▶	fortigate-60d	12 Sep 2023	Completo
+ 10.73.100.3								
	10.73.100.4	00:00:00:00:00:00			▶	tem-4		
	10.73.100.5	00:00:00:00:00:00			▶	pc-5		
+ 10.73.100.6								
	10.73.100.7	00:00:00:00:00:00			▶	inv-7		
+ 10.73.100.8								
	10.73.100.9	00:00:00:00:00:00			▶	WOL-VLAN9		Completo
	10.73.100.10	C8:D3:FF:BC:D7:77			▶	srv-aio	12 Oct 2022	Completo
+ 10.73.100.11								
	10.73.100.12	B4:A9:FC:B7:58:D8			▶	Taller-Port	15 Sep 2023	Completo
	10.73.100.13	40:B0:34:1C:8A:20			▶	secdir-pc	13 Mar 2023	Completo
+ 10.73.100.14								
	10.73.100.15	00:00:00:00:00:00			▶	TEST-15		
+ 10.73.100.16								
+ 10.73.100.17								

Datos del Equipo

IP: 10.73.100.10

Dirección Mac: C8:D3:FF:BC:D7:77

Nombre PC: srv-aio

Alias: alias1 alias2

No DNS: ☐

Valido: ☒

Usuario: Javier de la Fuente López

Responsable: Javier de la Fuente López

Localización: C. Mínimos Planta -1

Estancia: Despacho 12

Fecha de alta: 29/10/2021

Fecha expiración: 31/10/2025

S.O.: Windows 10

Teléfono: 449367

Marca: HP

Modelo: EliteDesk 800

Perfil FGT: Completo

Notas: Servidor All-in-One.

Aceptar

Cancelar



ANSIOSO

GESTIÓN DE VLANs



Gestión de Equipos - SUBREDES

[+ Nueva SUBRED](#)

Borrar	Vlan ↓	Info	Nombre	Subred	Mascara	Gateway	Zona DNS	DHCP1	DHCP2	Gen. DHCP	Gen. RADIUS	Gen. DNS	Voice Vlan
	0		VYOS	10.50.9.224	255.255.255.192	10.50.9.230		10.100.201.2	10.100.201.6	☐	☐	☐	☐
	0		WAN1	10.10.110.4	255.255.255.248					☐	☐	☐	☐
	1		Publica	161.111.168.128	255.255.255.128	161.111.168.129	eea.csic.es	10.100.201.2	10.100.201.6	☐	☐	☒	☐
	9		old_EEA	10.50.9.0	255.255.255.128	10.50.9.1	eea.csic	10.100.201.13	10.100.201.14	☒	☒	☒	☐
	10		Portatiles	10.50.9.128	255.255.255.192	10.50.9.130	eea.csic	10.100.201.13	10.100.201.14	☒	☒	☒	☐
	15		VPN_Subnet	10.50.9.192	255.255.255.192	10.50.9.193	eea.csic	10.100.201.13	10.100.201.14	☐	☐	☒	☐
	21		Telefonia	10.231.75.192	255.255.255.192	10.231.75.193				☐	☒	☐	☒
	26		Gest_Switches	10.17.15.0	255.255.255.0	10.17.15.1	eea.csic	10.100.201.2	10.100.201.6	☐	☐	☒	☐
	100		EEA	10.73.100.0	255.255.255.0	10.73.100.1	eea.csic	10.73.100.10		☒	☒	☒	☐
	108		Gerencia	10.73.108.0	255.255.255.0	10.73.108.1	eea.csic			☒	☒	☒	☐
	120		Servidores	10.73.120.0	255.255.254.0	10.73.120.1	eea.csic			☐	☐	☒	☐
	200		EEA_NO_EDR	10.73.200.0	255.255.254.0	10.73.201.1	eea.csic	10.73.100.10		☐	☒	☒	☐
	216		Restringida	10.90.14.0	255.255.255.0	10.90.14.1		10.90.14.1		☐	☐	☐	☐
	218		Cursos	10.73.218.0	255.255.255.0	10.73.218.1	eea.csic			☒	☒	☐	☐
	406		Gest_WIFI	172.25.19.0	255.255.255.192	172.25.19.1		172.25.19.1		☐	☒	☐	☐
	407		WIFI_Ext	172.26.139.0	255.255.255.0	172.26.139.1		172.26.139.1		☐	☐	☐	☐
	408		WIFI_Int	172.26.138.0	255.255.255.0	172.26.138.1		172.26.138.1		☐	☐	☐	☐
	409		WIFI_Invitados	172.26.140.0	255.255.255.0	172.26.140.1		172.26.140.1		☐	☐	☐	☐
	410		WIFI_EEA	172.16.12.0	255.255.255.0	172.16.12.1		172.16.12.1		☐	☐	☐	☐
	1020		Nube200	10.100.200.0	255.255.255.0	10.100.200.1	eea.csic	10.100.201.2	10.100.201.6	☐	☐	☒	☐
	1021		Nube201	10.100.201.0	255.255.255.0	10.100.201.1	eea.csic	10.100.201.2	10.100.201.6	☐	☐	☒	☐
	1024		Nube204	10.100.204.0	255.255.255.0	10.100.204.1	eea.csic	10.100.201.2	10.100.201.6	☐	☐	☒	☐
	1205		Nube205	10.100.205.0	255.255.255.0	10.100.205.1	eea.csic.es	10.100.201.2	10.100.201.6	☐	☐	☒	☐

ea.csic/equipos/subred_extra.php?id_vlan=36

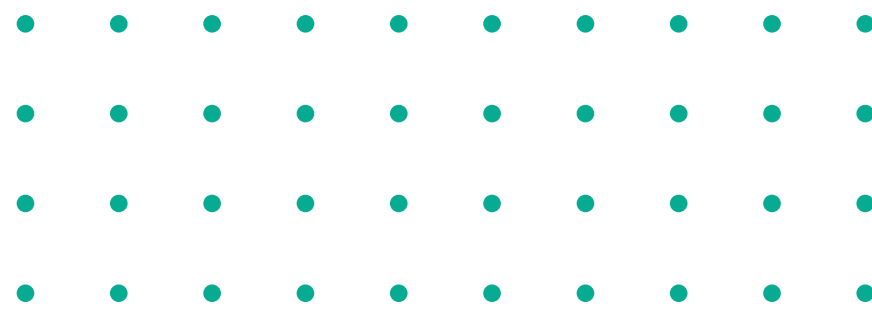
PC GTRED Lecturas Varios

Todos los marcadores

de Equipos - ATRIBUTOS DE SUBRED

ATRIBUTO

Borrar	Subred	Tipo ↑	Valor
	new_EEA	DHCP	10.73.120.10
	new_EEA	DNS	10.73.120.10
	new_EEA	DNS	10.100.201.2
	new_EEA	IP_WOL	10.73.100.9
	new_EEA	POOL-RANGE	10.73.100.11-10.73.100.99



ANSIOSO

All Network Services In One SO

Equipos

Extra

Localizaciones

SS.OO.

Usuarios

Subredes

Switches

Zonas DNS

Gestión de Equipos - ZONAS DNS

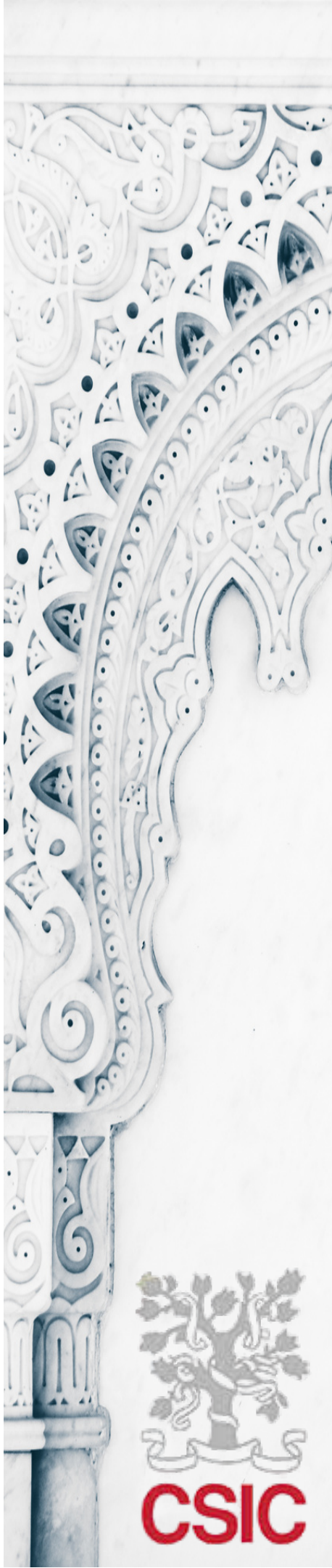
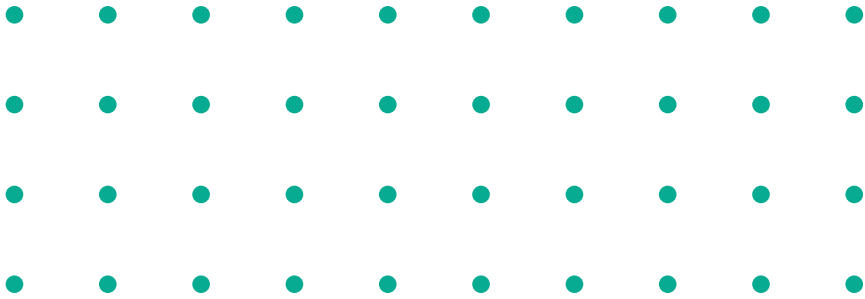
+ Nueva ZONA

Borrar	Info	Zona
		eea.csic
		eea-ugr.csic.es
		funciona.es
		informes.map.es
		app.serviciosinternos.hac
		sede.csic.gob.es
		redsara.es

Atributos de Zona - ANSIOSO

+ Nuevo ATRIBUTO

Borrar	Zona	Tipo ↑	Valor
	eea.csic	NS	ansioso.eea.csic
	eea.csic	NS	wineea2.eea.csic
	eea.csic	QUERY	red-interna
	eea.csic	TXT	v=spf1 mx ip4:161.111.10.57 ip4:161.111.10.60 -all



AN SIO SO

FortiGate 81F FWEEA_1

★ Favorites

Dashboard

Security Fabric

Network

Interfaces

DNS

Packet Capture

SD-WAN Zones

SD-WAN Rules

Performance SLA

Static Routes

Policy Routes

RIP

OSPF

BGP

Multicast

FortiExtender

System

Policy & Objects

Security Profiles

VPN

User & Authentication

Log & Report

Edit Interface

Name Restringida

Alias

Type VLAN

Interface inside (internal1)

VLAN ID 216

VRF ID 0

Role LAN

Address

Addressing mode

IP/Netmask

Create address object matching

Secondary IP address

Administrative Access

IPv4

HTTPS

SSH

RADIUS Acc

DHCP Server

Address range 10.70.216.

Netmask 255.255.2

Default gateway Same as Ini

DNS server Same as Sy

FortiGate 81F FWEEA_1

★ Favorites

Firewall Policy

Interfaces

Addresses

Dashboard

Security Fabric

Network

System

Policy & Objects

Security Profiles

VPN

User & Authentication

Log & Report

Name	Source	Destination	Schedule
Gest_Switches	outside (wan1)		
Gest_Switches	Tunel_Vyos		
Gest_WIFI	outside (wan1)		
inside (internal1)	EEA		
inside (internal1)	Gest_Switches		
inside (internal1)	Gest_WIFI		
inside (internal1)	outside (wan1)		
inside (internal1)	Portatiles		
inside (internal1)	ToiP		
inside (internal1)	Tunel_Vyos		
inside (internal1)	Voip		
outside (wan1)	EEA		
outside (wan1)	Gest_WIFI		
outside (wan1)	inside (internal1)		
outside (wan1)	ToiP		
outside (wan1)	Tunel_Vyos		
Portatiles	EEA		
Portatiles	Gest_Switches		
Portatiles	Gest_WIFI		
Portatiles	inside (internal1)		
Portatiles	outside (wan1)		
Portatiles	Tunel_Vyos		
Restringida	outside (wan1)		

Firewall

javier@JAVIER-PORT-HP: ~

Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.17.15.11' (RSA) to the list of known hosts.
javier@10.17.15.11's password:

EEA_Core#
show running-config | section radius

aaa authentication dot1x default radius
aaa authorization network default radius
switchport voice vlan
radius server auth 10.100.201.17

javier@JAVIER-PORT-HP: ~

EEA_SW_Test#
show running-config interface Gi1/0/11

no green-mode eee
spanning-tree portfast
switchport mode general
switchport general allowed vlan add 21 tagged
authentication host-mode multi-domain
authentication event no-response action authorize vlan 216
authentication periodic
mab
authentication order mab
authentication priority mab
authentication control-direction in
dot1x pml tlv-select port-vlan
switchport voice vlan 21
switchport voice vlan override-authentication

Switches



Grupo de Trabajo - GTRED



Javier Merino Ayuso

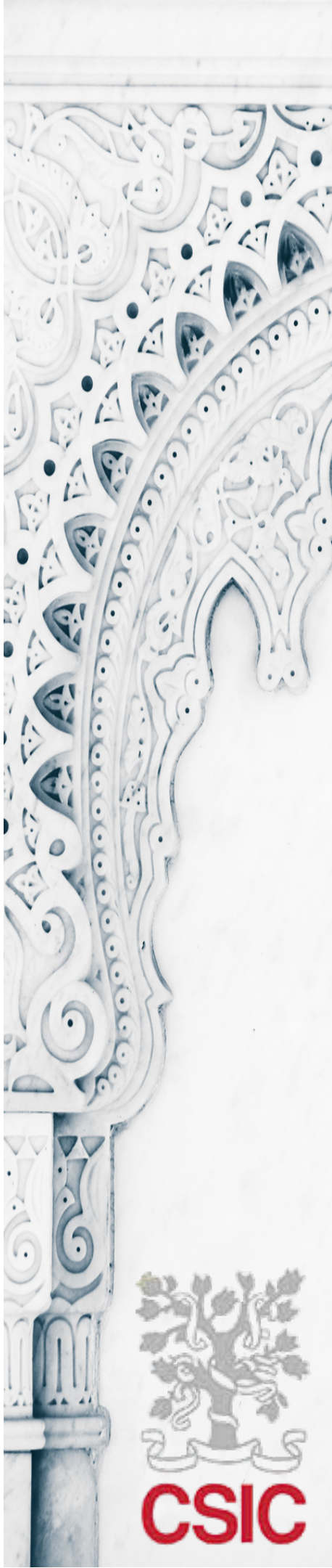
Juan Manuel Bolaño
Ladrón de Guevara

Marta Alarcón Rosero

Javier Moreno

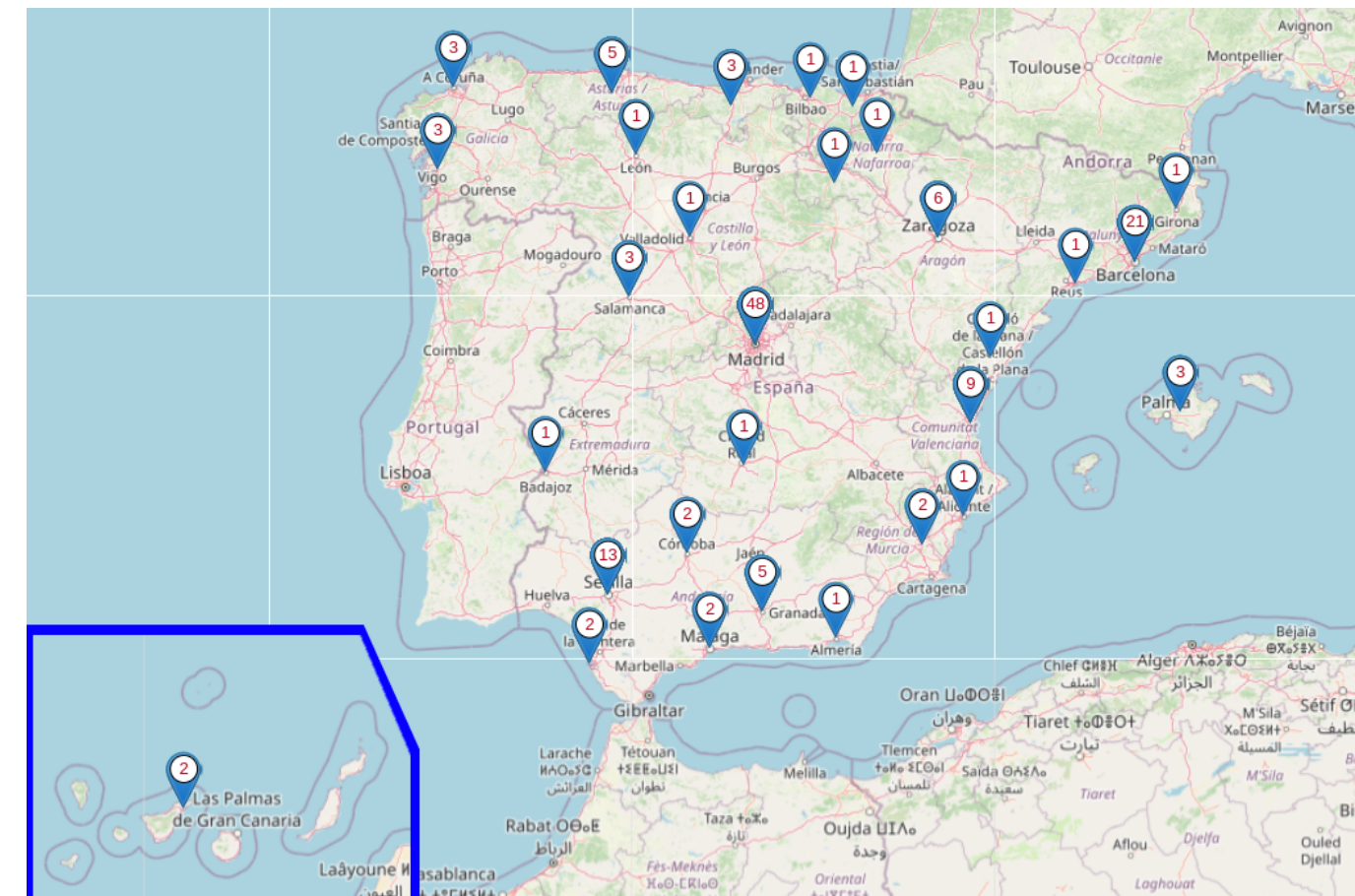
Eva M. de la Calzada
Cuesta

Javier de la Fuente
López

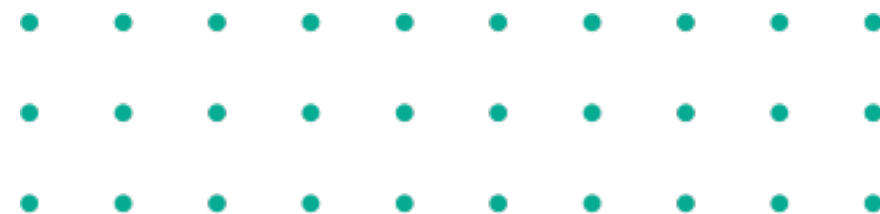


REDES PAREJAS

- En marcha tener **redes homogéneas** con criterios comunes para cada sede.

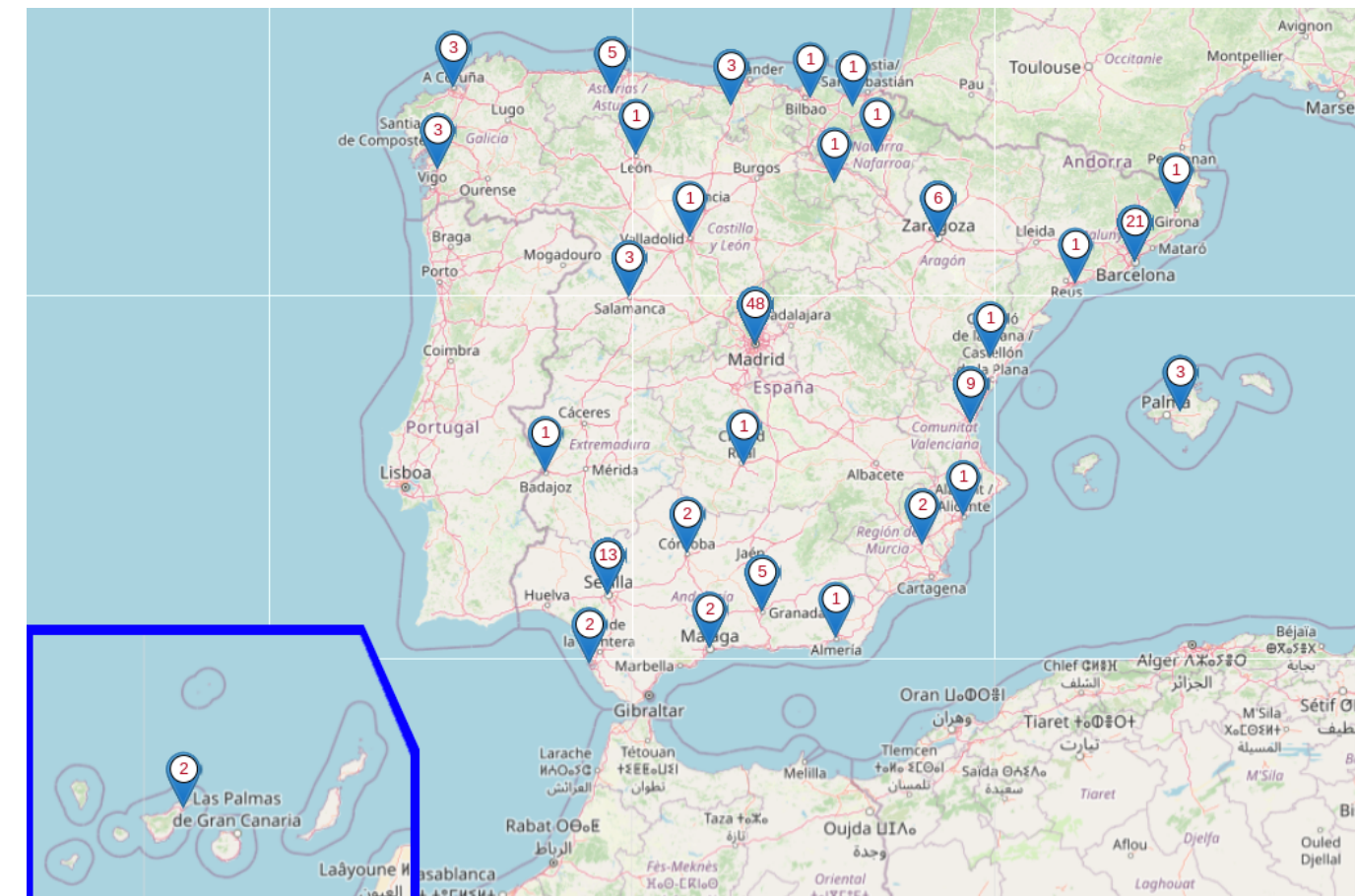


Fuente: <https://www.csic.es/es/el-csic/organizacion/institutos-centros-y-unidades>

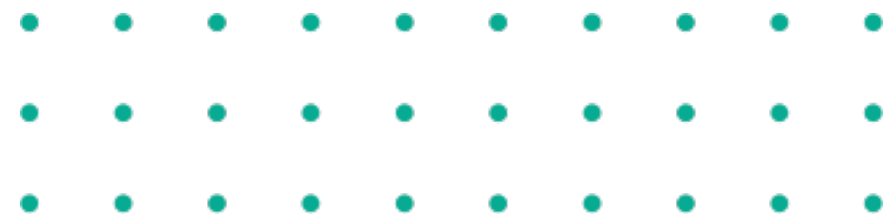


REDES PAREJAS

- En marcha tener **redes homogéneas** con criterios comunes para cada sede.
- Logro al 98%.
Cortafuegos y electrónica de red comunes.

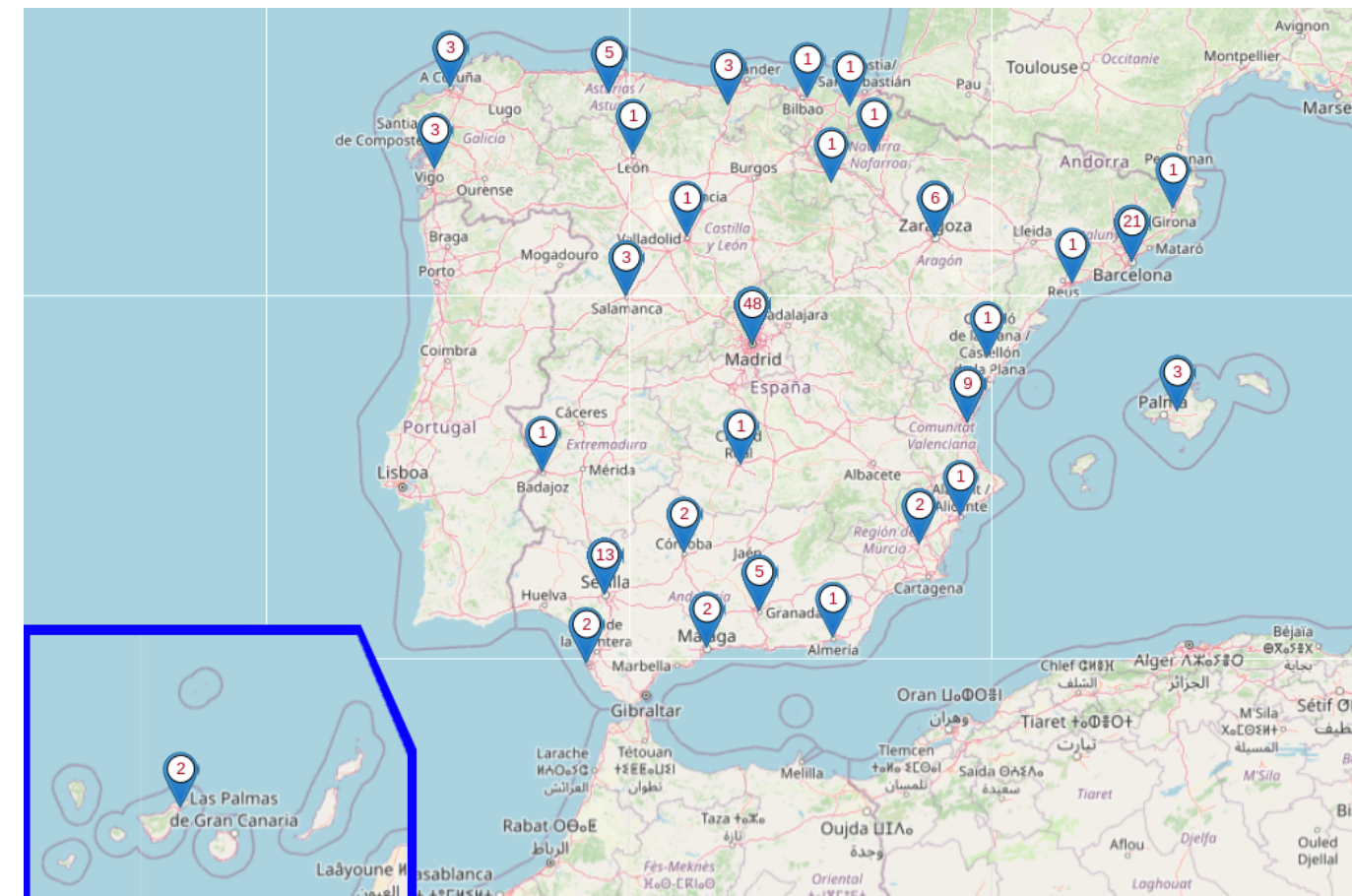


Fuente: <https://www.csic.es/es/el-csic/organizacion/institutos-centros-y-unidades>

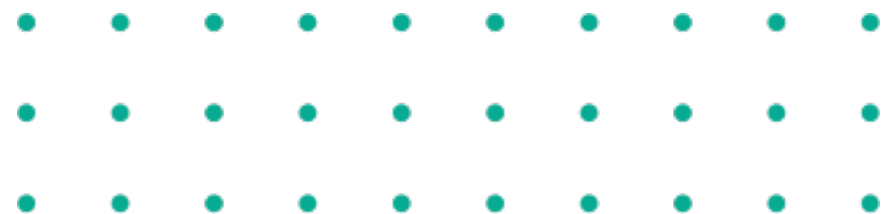


REDES PAREJAS

- En marcha tener **redes homogéneas** con criterios comunes para cada sede.
- Logro al 98%.
Cortafuegos y electrónica de red comunes.
- Siguiente objetivo:
Poder **centralizar la gestión completa de red.**

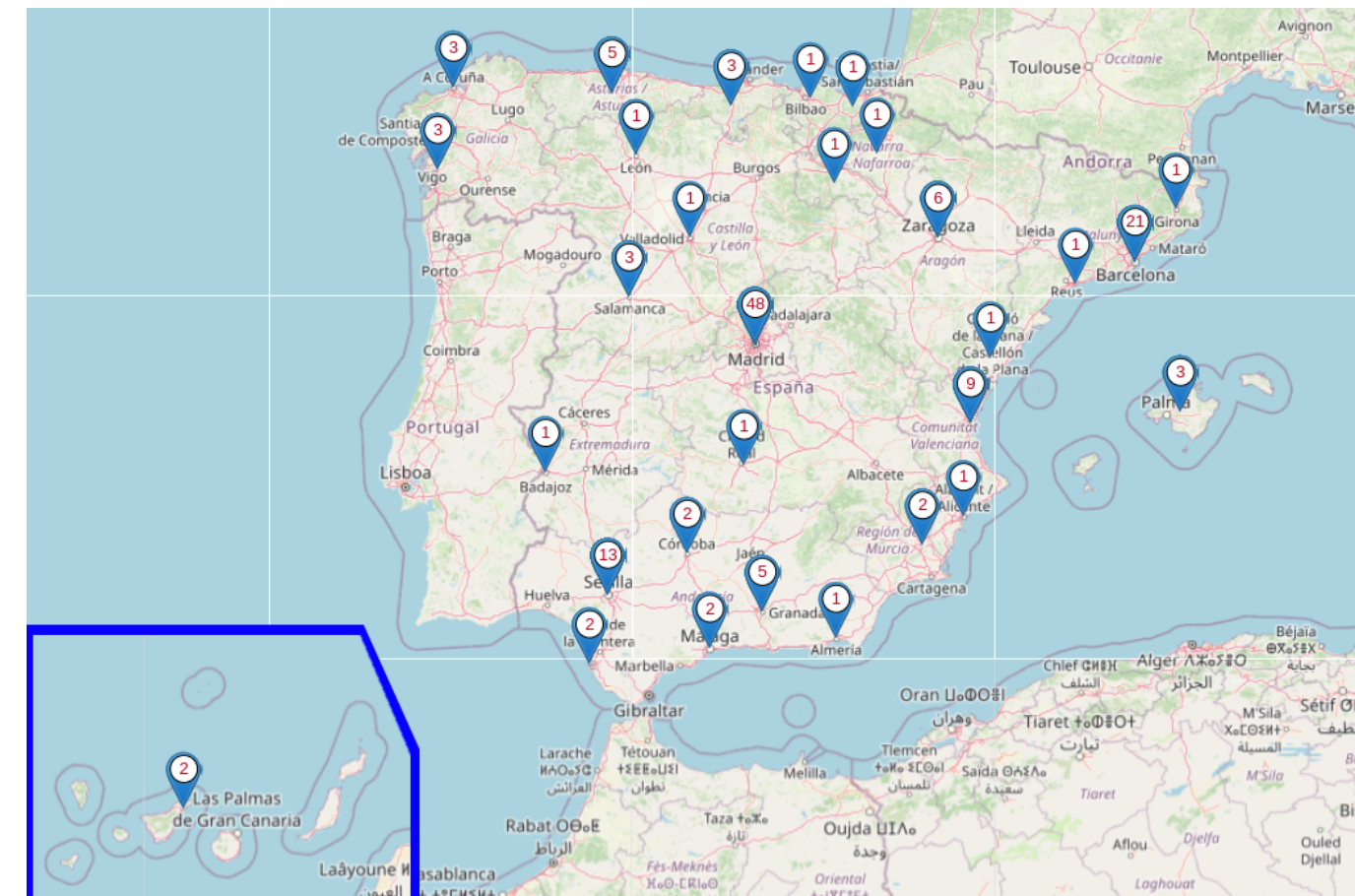


Fuente: <https://www.csic.es/es/el-csic/organizacion/institutos-centros-y-unidades>

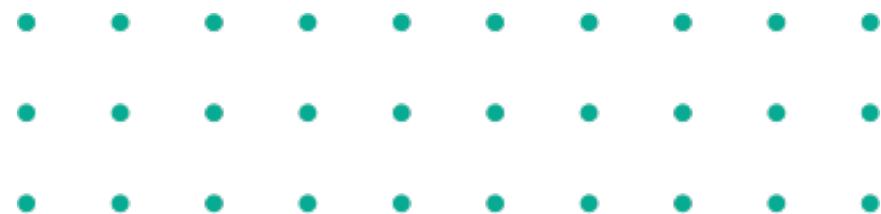


REDES PAREJAS

- En marcha tener **redes homogéneas** con criterios comunes para cada sede.
- Logro al 98%.
Cortafuegos y electrónica de red comunes.
- Siguiente objetivo:
Poder **centralizar la gestión completa de red.**



Fuente: <https://www.csic.es/es/el-csic/organizacion/institutos-centros-y-unidades>

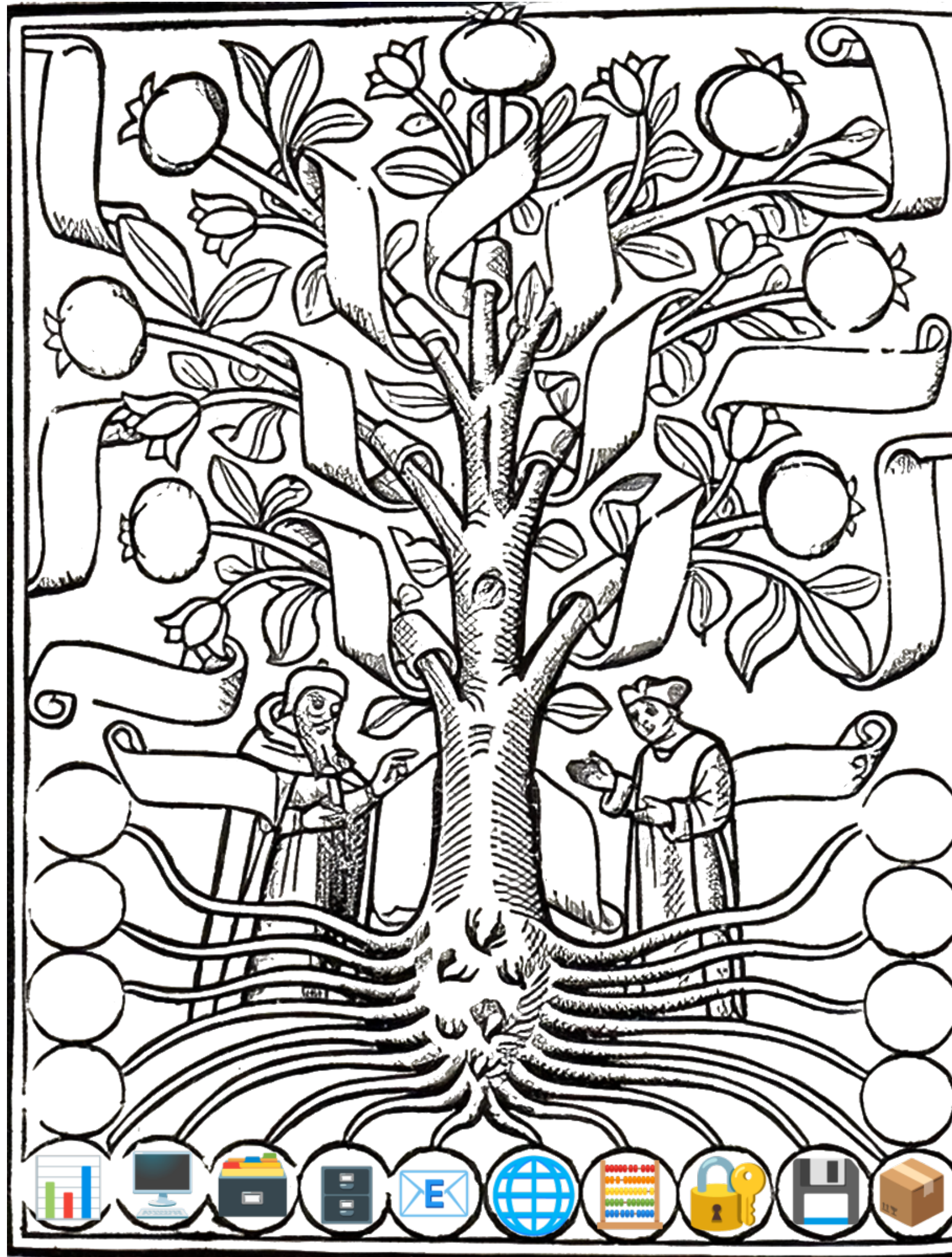
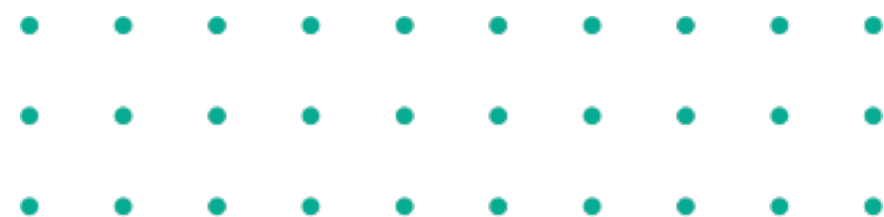


GESTIÓN CENTRALIZADA

Análogo a la gestión centralizada de los ***servicios core institucionales***.

- Correo
- Web Hosting
- Cómputo
- Almacenamiento
- Identidad + AAA
- VDI
-

Completamente centralizados.

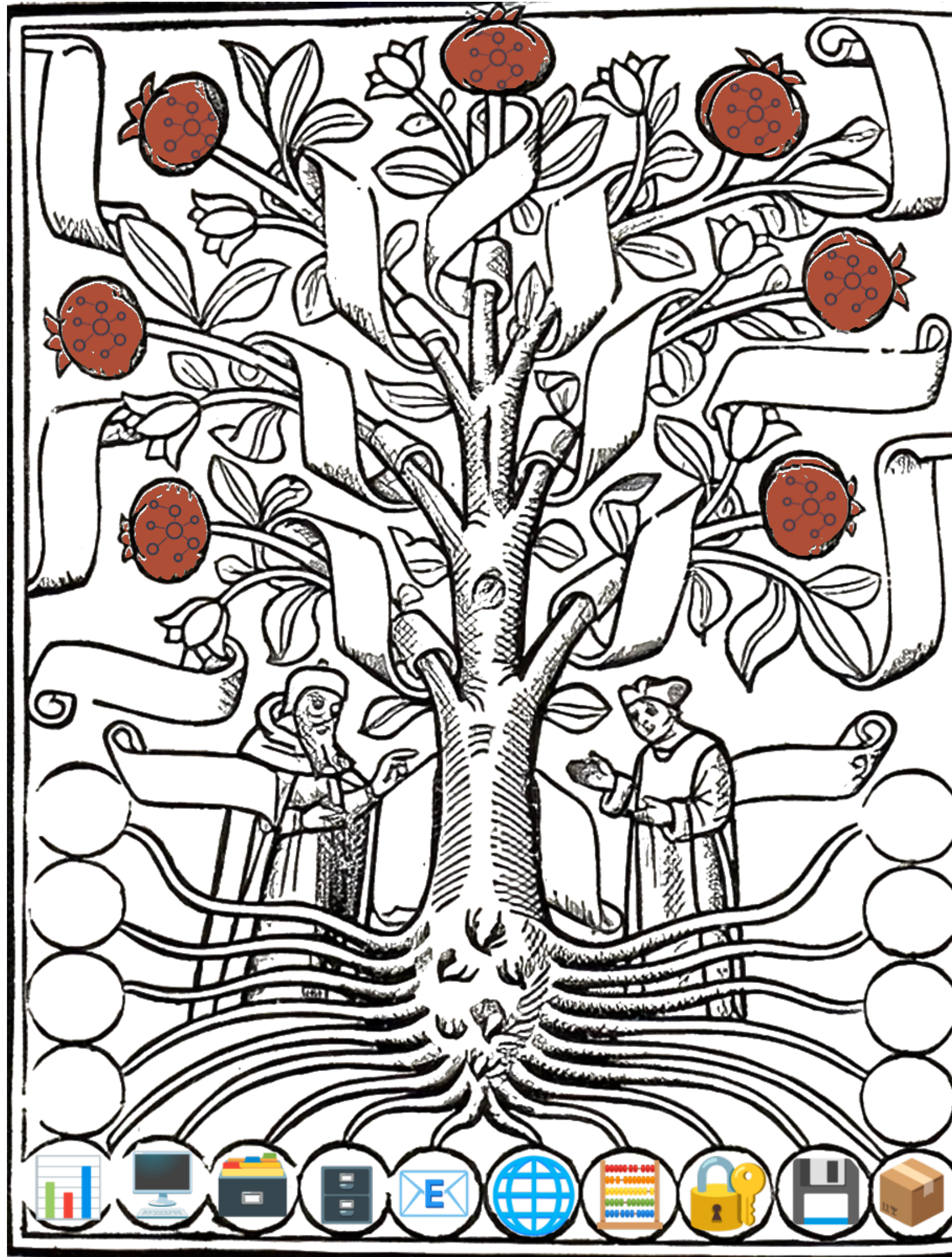
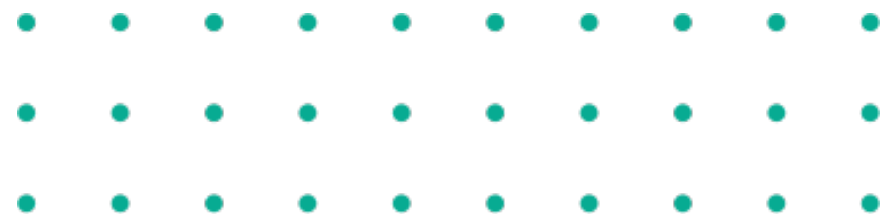


GESTIÓN CENTRALIZADA

Centralizar la gestión de los *servicios resilientes de borde*.

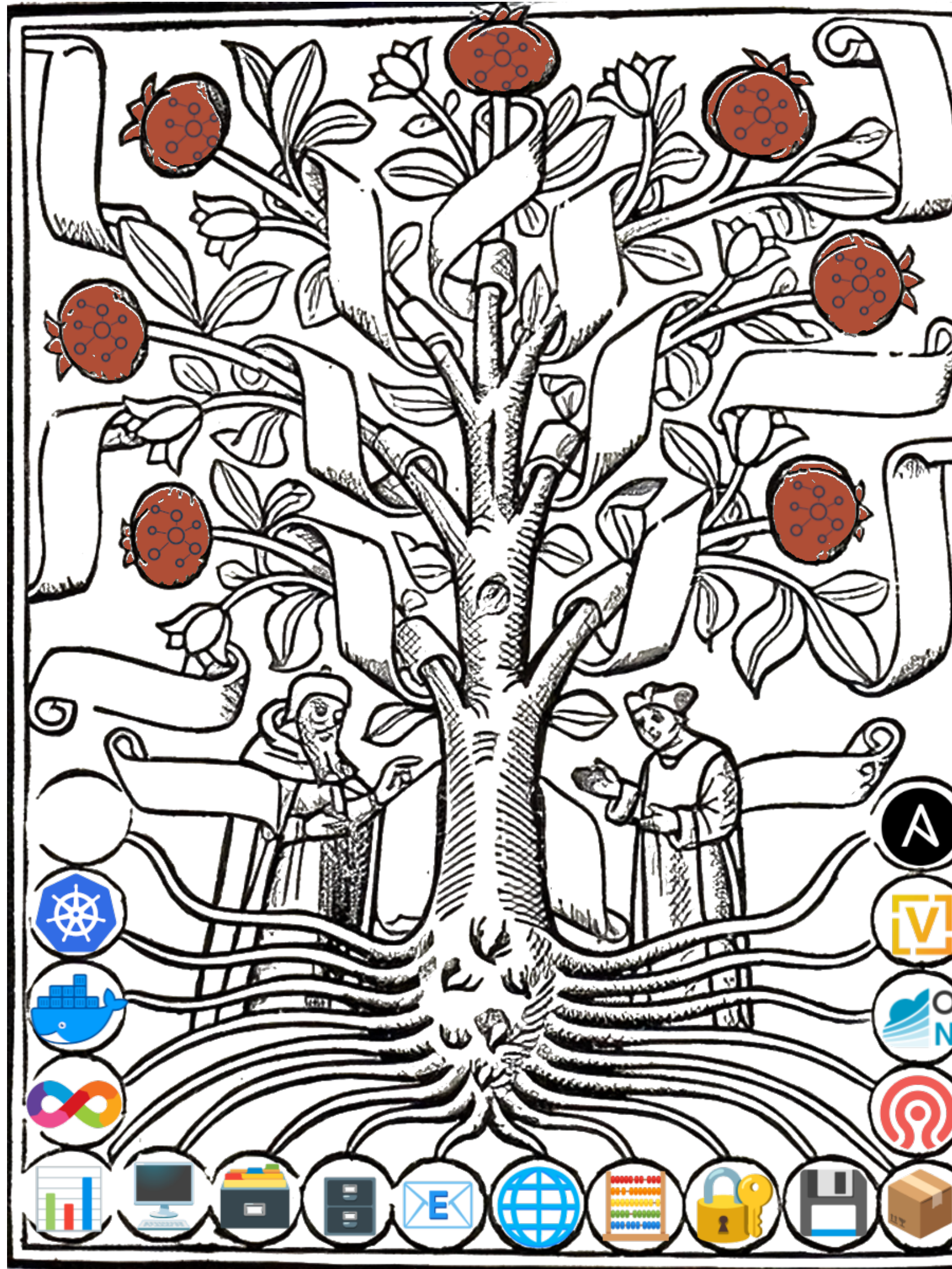
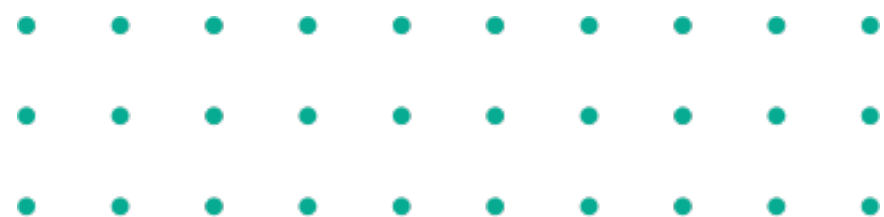
- radius - dhcp - ntp
- dns backup
- aaa backup
- Sistemas físicos (accesos, impresión...)
- logs/trazas - telemetría
- sensores – agentes

Que dan color a nuestros frutos
silentes



GESTIÓN CENTRALIZADA

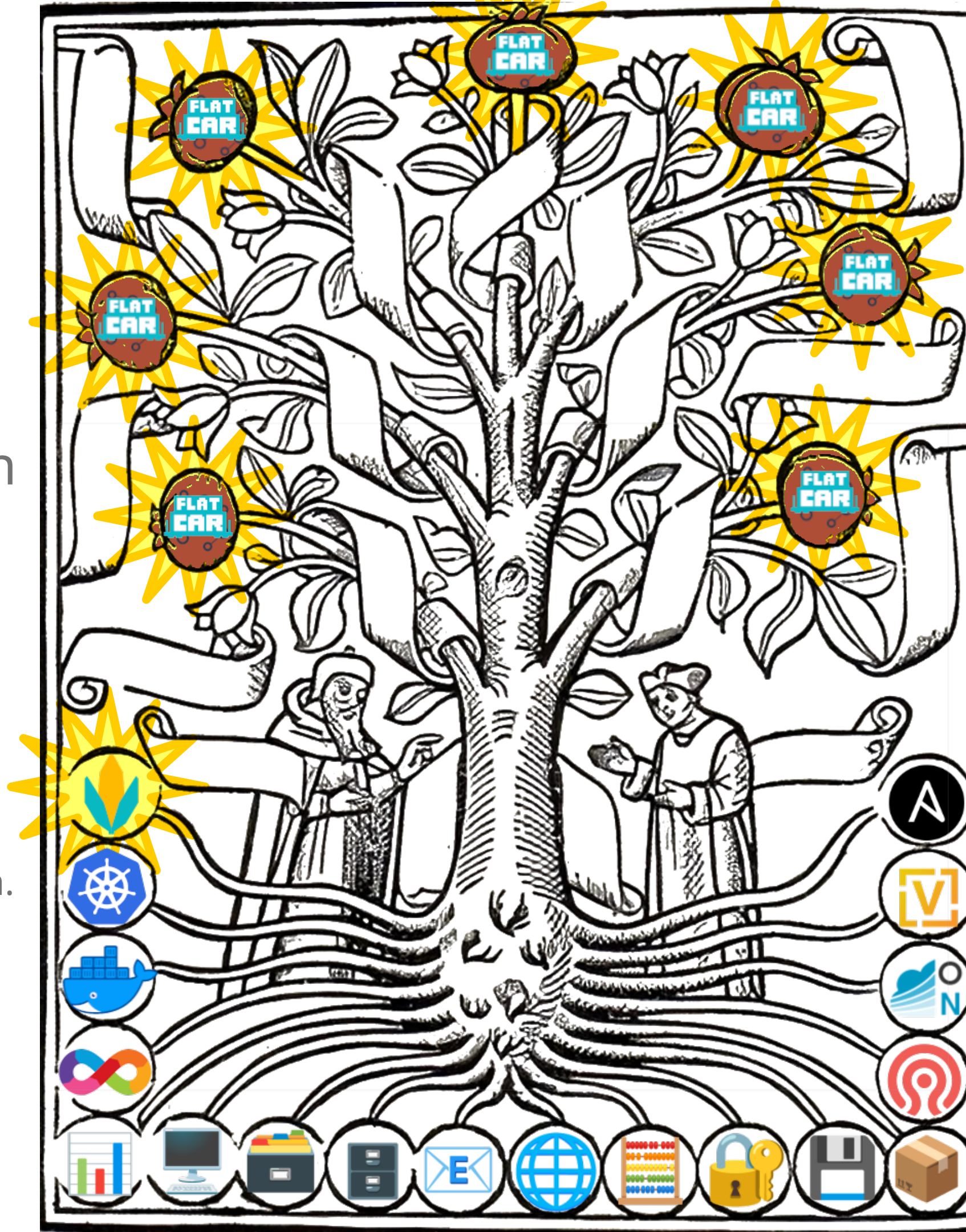
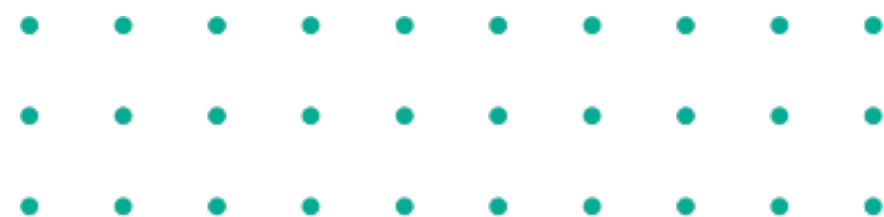
Del mismo modo que nos apoyamos en tecnologías libres para soportar la orquestación de los *servicios core institucionales*.



GESTIÓN CENTRALIZADA

Pretendemos apoyarnos en tecnologías libres para soportar la *orquestración* de los ***servicios resilientes de borde***.

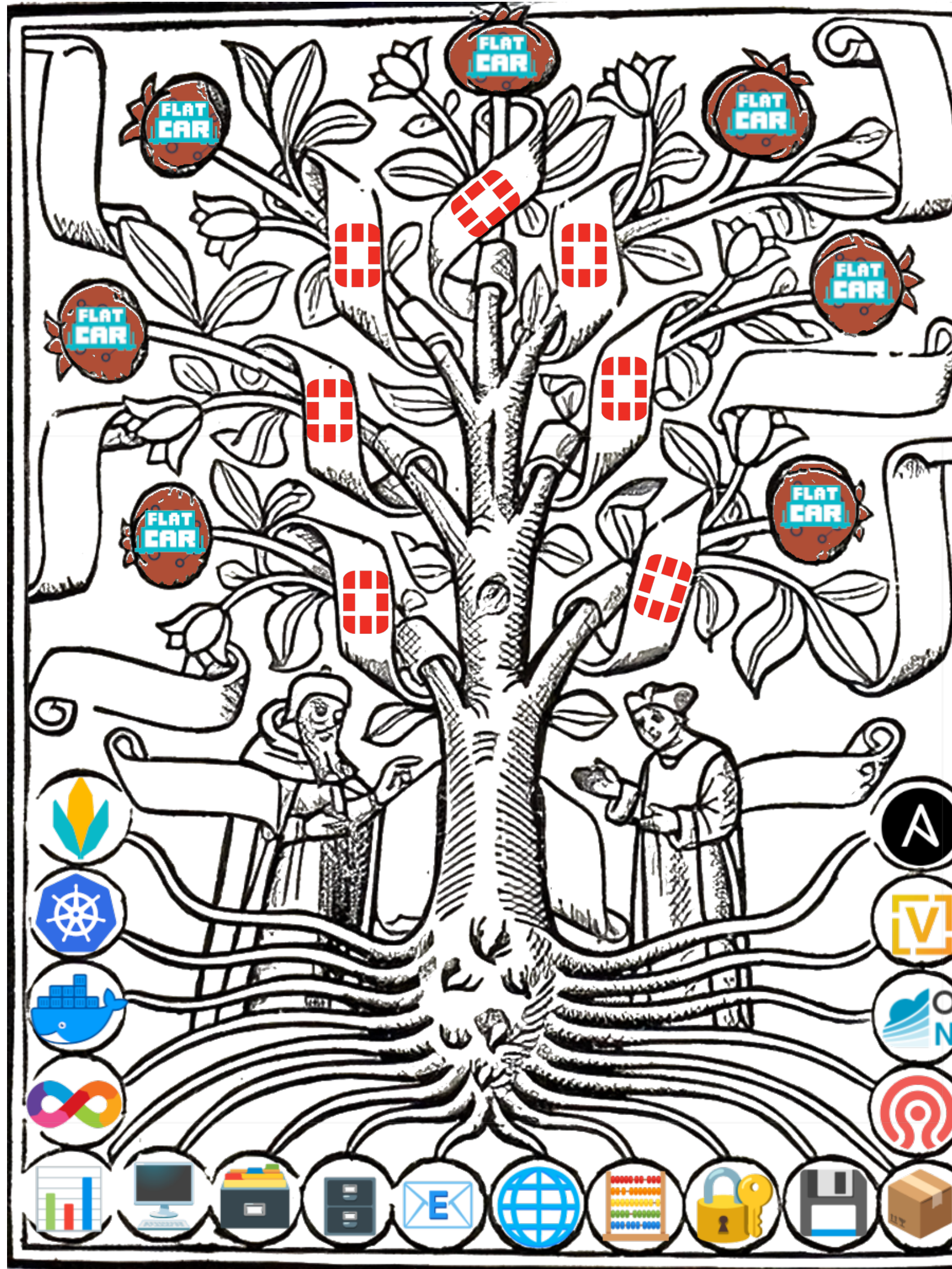
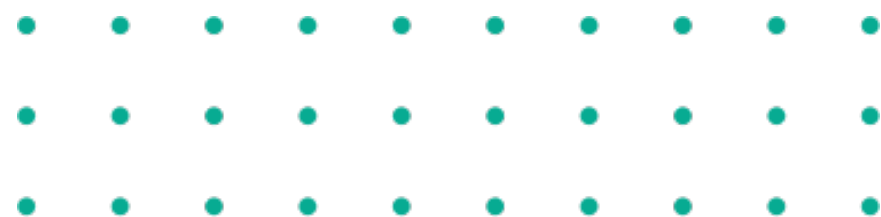
NOTAR:
La palabra orquestración está en cursiva.



GESTIÓN CENTRALIZADA

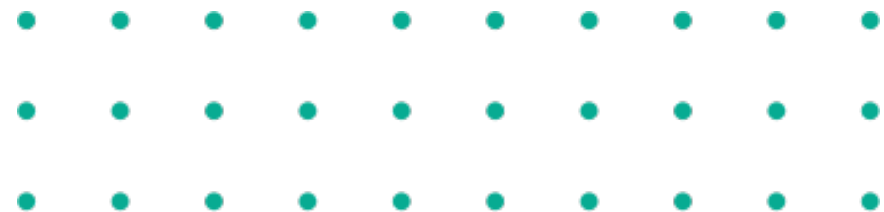
Pretendemos apoyarnos en tecnologías libres para soportar la *orquestración* de los ***servicios resilientes de borde***.

Aprovechando el despliegue existente de cortafuegos que nos permiten acercarnos ese borde.



¿QUÉ PLANTEAMOS?

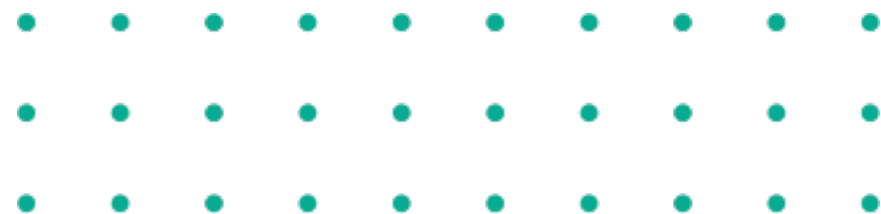
- Hardware



¿QUÉ PLANTEAMOS?

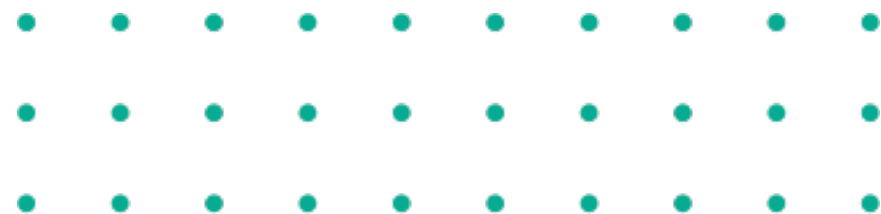
- Hardware
- Características equipo de red
 - ✓ Dimensiones del rack
 - ✓ Doble fuente
 - ✓ Conectividad
 - ✓ Sistema inmutable

Valoramos aprovechar
los cores de red...



¿QUÉ PLANTEAMOS?

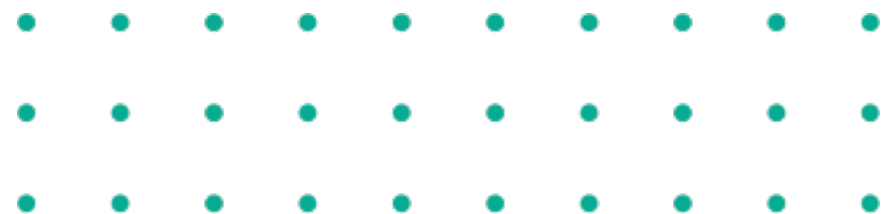
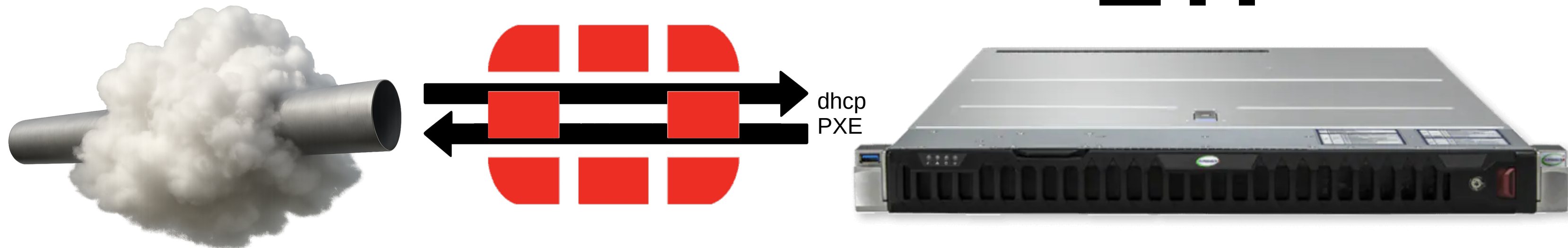
- Hardware
- Características equipo de red
- Idealmente en HA



¿QUÉ PLANTEAMOS?

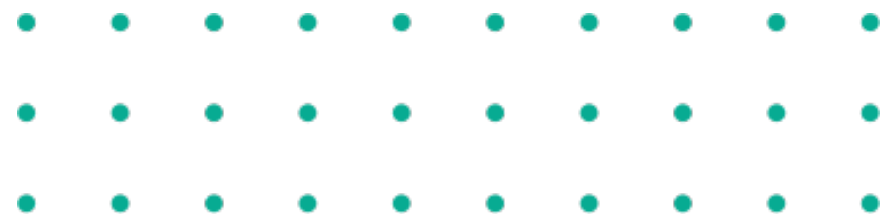
- Hardware
- Características equipo de red
- Idealmente en HA
- Aprovisionamiento desatendido

ZTP



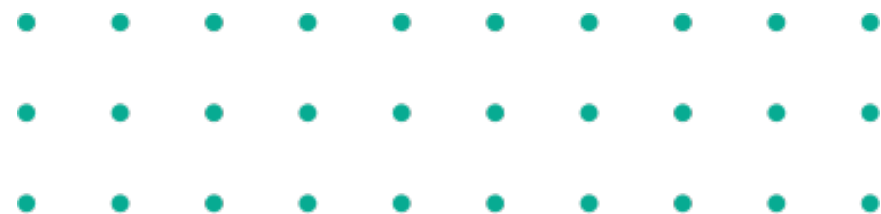
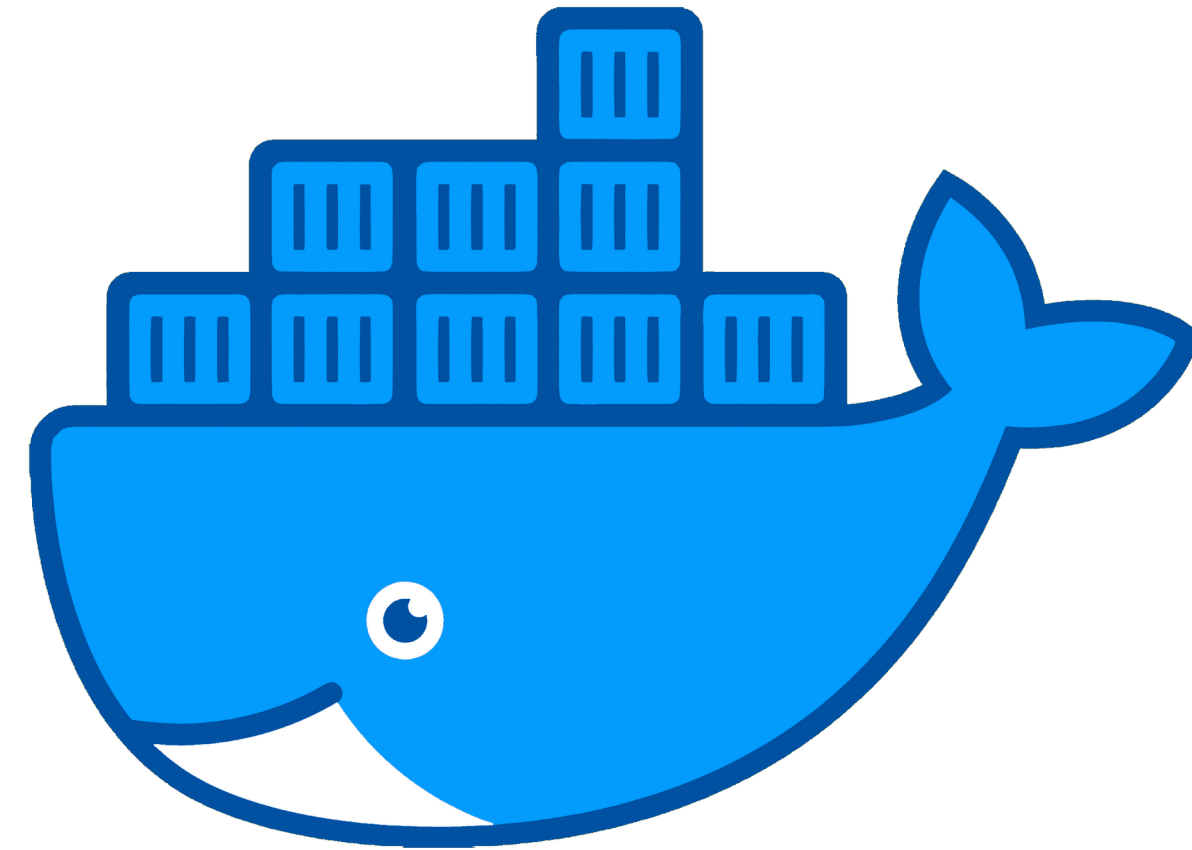
¿QUÉ PLANTEAMOS?

- Hardware
- Características equipo de red
- Idealmente en HA
- Aprovisionamiento desatendido
- Reemplazable



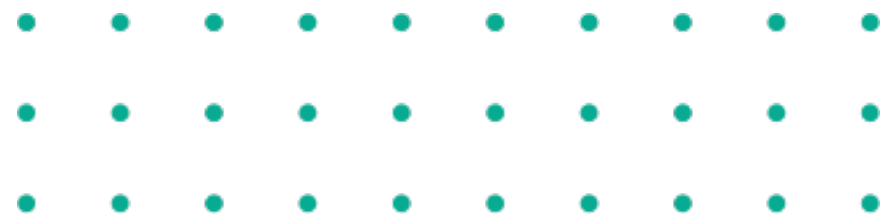
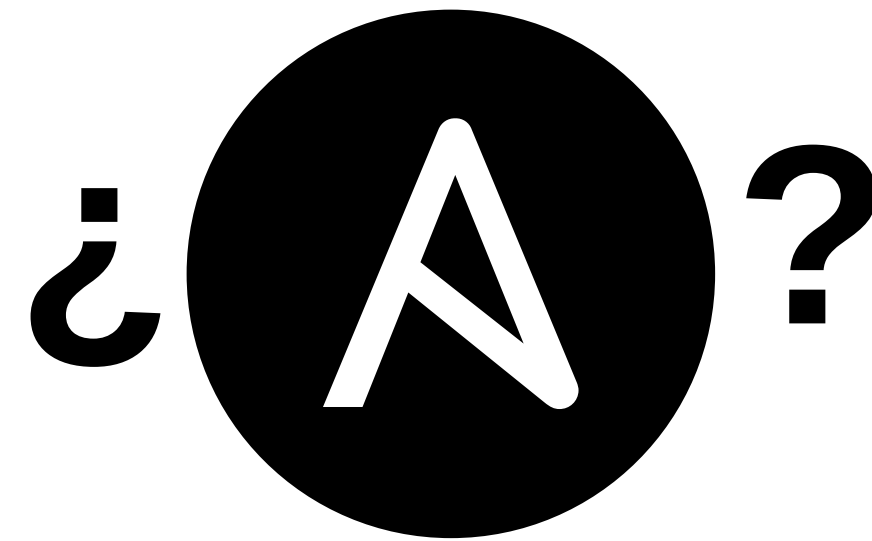
¿QUÉ PLANTEAMOS?

- Hardware
- Características equipo de red
- Idealmente en HA
- Aprovisionamiento desatendido
- Reemplazable
- Corra servicios en contenedores



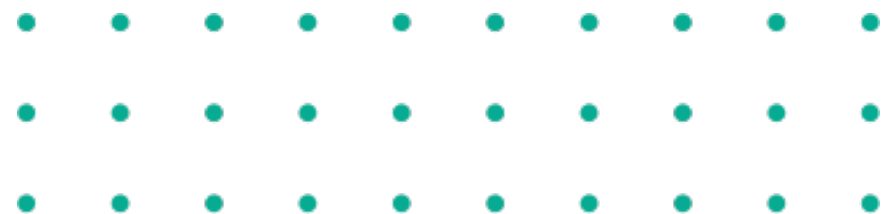
¿QUÉ PLANTEAMOS?

- Hardware
- Características equipo de red
- Idealmente en HA
- Aprovisionamiento desatendido
- Reemplazable
- Corra servicios en contenedores
- Gestión centralizada



¿QUÉ PLANTEAMOS?

- Hardware
- Características equipo de red
- Idealmente en HA
- Aprovisionamiento desatendido
- Reemplazable
- Corra servicios en contenedores
- Gestión centralizada
- Que nos soporten



¿QUÉ PLANTEAMOS?

- Hardware
- Características equipo de red
- Idealmente en HA
- Aprovisionamiento desatendido
- Reemplazable
- Corra servicios en contenedores
- Gestión centralizada
- Soporte
- Versatil
- Potente
- Independiente

• Bueno

• Bonito

• Barato

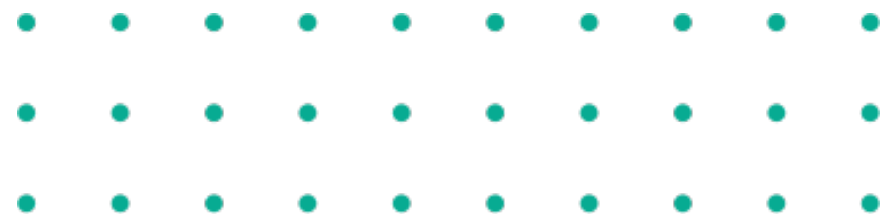


PROPUESTA PoC

- Con empresa.

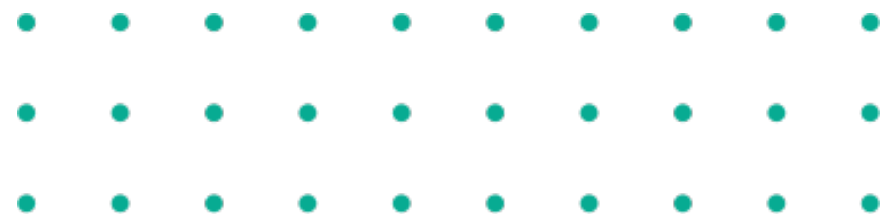
Aprovecho este momento para agradecer el trabajo que en realidad están haciendo otros para nosotros.

No podríamos abordar esta PoC sin ayuda externa.



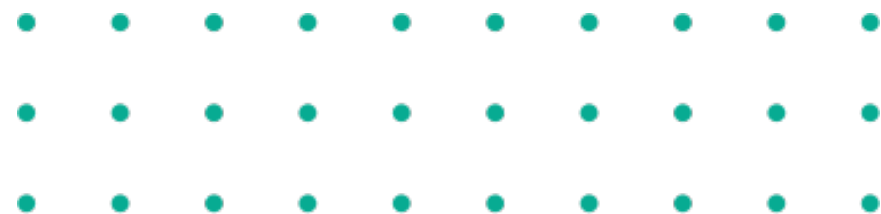
PROPUESTA PoC

- Con empresa
- Utilizando **FlatCar** como SO.
 - Ejecución de contenedores
 - Minimalista, rápido
 - Inmutable, seguro, estable.
 - Despliegue / actualizaciones atómicas y automatizadas.
 - Software Libre



PROPUESTA PoC

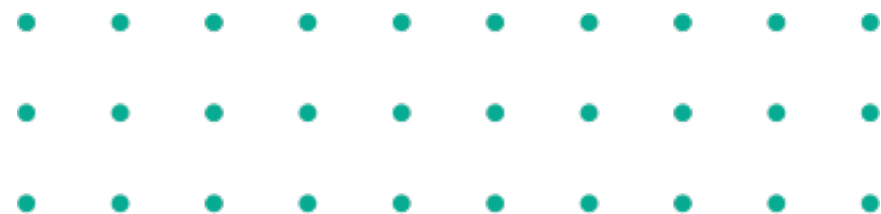
- Con empresa
- Utilizando **FlatCar** como SO.
- **Ignition** para primer arranque.
Con dhcp y PXE por túneles VPN.



PROPUESTA PoC

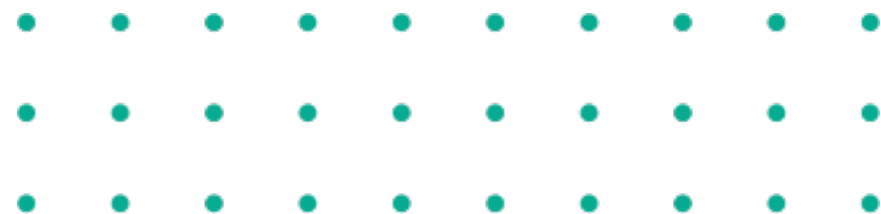


- Con empresa
 - Utilizando **FlatCar** como SO.
 - **Ignition** para primer arranque.
 - Distribuyendo contenedores y actualizaciones con **Nebraska**.
-
- Servidor de actualizaciones automáticas usando protocolo **Omaha**.
 - Control de despliegues.



PROPUESTA PoC

- Con empresa
- Utilizando **FlatCar** como SO.
- **Ignition** para primer arranque.
- Distribuyendo contenedores y actualizaciones con **Nebraska**.
- Utilizando distintos *grupos* y *canales* para la distribución.



Y todo esto ¿para qué?

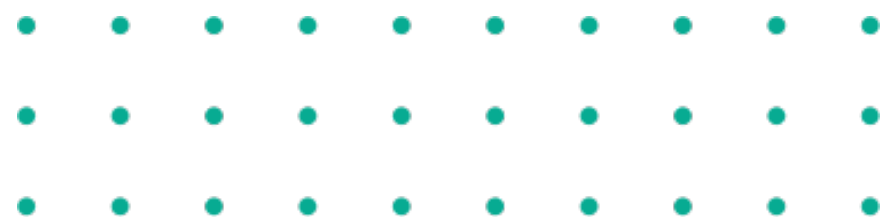
Recordemos el objetivo:

La distribución automática de los servicios que se prestan cerca del borde con gestión centralizada y corriendo sobre un sistema en cada centu.

Llevar la resiliencia de la red al borde.



ANSIOSO
All Network Services In One SO

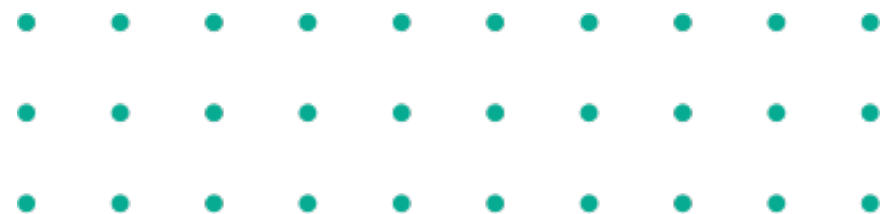
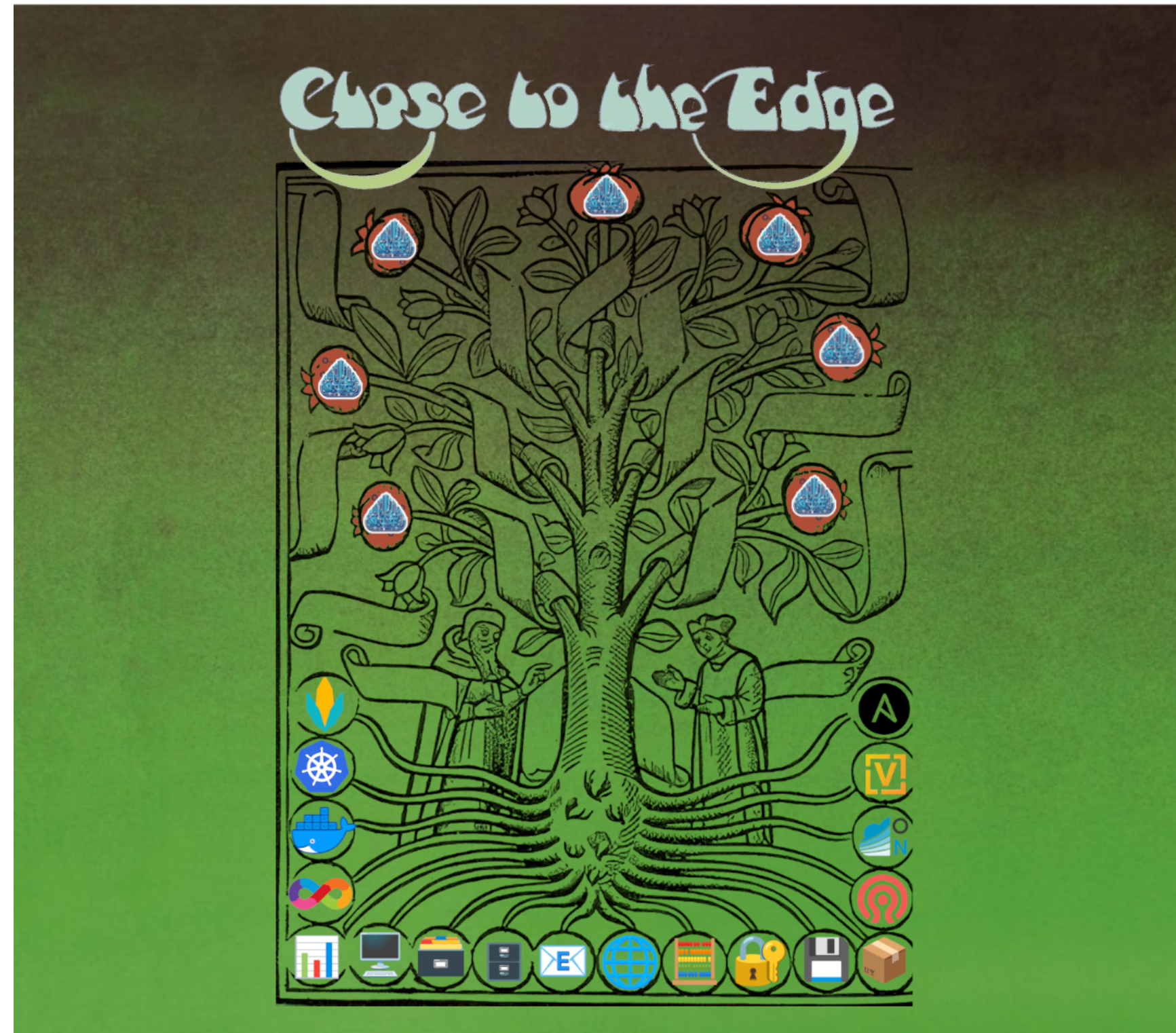


ANSIOSO

Close to the Edge

Si no pongo esta diapo
reviento.

All Network Services In One
"Sistema Operativo"



GRACIAS

Grupo GT-Red CSIC

Referencias:

FlatCar:

- <https://www.flatcar.org>
- docs - <https://www.flatcar.org/docs/latest/>
- code - <https://github.com/flatcar>
- tutorial - <https://www.flatcar.org/docs/latest/tutorial/>

Ignition:

- docs - <https://coreos.github.io/ignition/>
- code - <https://github.com/coreos/ignition>

Nebraska:

- docs - <https://www.flatcar.org/docs/latest/nebraska/>
- code - <https://github.com/flatcar/nebraska>

