



Evolución de la arquitectura de red en la UOC: el caso específico en investigación e Innovación

Antoni Roure

[Mayo] [2024] Àrea de Tecnologia

Jornadas de RedIRIS

[INT] ¿Qué pretendemos con esta presentación?

- Explicar el impacto de la migración al cloud sobre la arquitectura de red on-premise.
 - Profundizar en el caso de las redes de laboratorio y investigación.
-

[INT] ¿Quiénes somos? La UOC es una universidad ...



...pionera y experta en
e-learning que forma
personas a lo largo
de la vida,



...nativa digital,
global y con
mandato público...



...que la investigación
en la interacción entre
tecnología y las
ciencias humanas
y sociales.

Una universidad que prepara a las personas y a las comunidades para el mundo en el que vivirán y no para el pasado en el que vivieron generaciones anteriores.

[INT] Casi 30 años de experiencia en aprendizaje en línea de calidad

1995

El año en el que nació la UOC: la primera universidad en línea del mundo



113.500

graduados y graduadas



7.283

profesorado propio, investigador, personal docente de soporte a la docencia (profesorado colaborador y asociado) y tutores y tutoras



87.150

estudiantes



750

programas con docencia



11.814

aulas virtuales



Times Higher Education World University Rankings

Global

Top 150

entre las universidades más jóvenes

Iberoamérica

1.^a

universidad en línea

España

Top 10

universidad estatales

[CONTEXTO]

Antecedentes

[CONTEXTO] Antecedentes

- La UOC ha **migrado** sus sistemas **al cloud**, y en los nuevos proyectos busca que sean con Software as a Service.
- En agosto de 2022, se vació y **cerró el CPD** de Castelldefels, así como el de contingencia en Nexica. Quedan servicios residuales en una pequeña sala de máquinas en Tibidabo.
- Con el proyecto **Nueva Manera de Trabajar** ha cambiado la forma en que los trabajadores de la Universidad interactúan con la red, todos con portátil, con mucho más teletrabajo, sin una mesa asignada, podemos resumirlo con que nos ha aumentado mucho la **movilidad**.
- Con la nueva manera de trabajar crece mucho el uso de **la videoconferencia**, Google Meet, y **pasa a ser un servicio crítico**.

[CONTEXTO] Antecedentes

- La UOC ha ocupado **dos edificios nuevos** en el 22@ configurando un campus urbano **que hay que equipar**.
- La UOC está en medio de un salto importante en investigación; en 2022 se **inauguraron varios laboratorios** en el campus del 22@ que necesitan conexión fiable y segura.
- Una parte importante de la electrónica de red ha llegado al final de su vida útil y se ha quedado obsoleta, por lo que habrá una renovación considerable de la infraestructura, como el wifi.

Gran oportunidad de modernizar la tecnología de red en la UOC.

[RET] Retos

[RET] Retos de la iniciativa

- Pasar de una red para acceder a aplicaciones web localizadas en el CPD a **una red para conectarse a Internet** y acceder al cloud.
 - La **movilidad y la videoconferencia** se vuelven clave.
 - La **seguridad** es una preocupación importante, implementando políticas de **confianza cero**, Zero-Trust.
 - **Integrar** de manera eficaz, fiable y segura **los laboratorios** a la red de la UOC.
-

[RET] Retos de la iniciativa

- La visión es de que **los edificios de la UOC se conecten directamente a Internet** de manera segura y fiable. Esto requiere una nueva infraestructura de comunicaciones y seguridad en las oficinas, que incluye LAN, wifi y firewalls.
 - Proporcionar infraestructura de comunicaciones a los **laboratorios** de la UOC con gran autonomía para los investigadores, implica una **buena segmentación** para lograr la seguridad necesaria.
-

[SOL] Solución tecnológica

[SOL] Solución tecnológica.

1 Conectar cada sede directamente a Internet:

- Las sedes centrales tendrán redundancia de operador y direcciones propias de la UOC.
 - Las sedes territoriales se conectarán mediante fibra doméstica.
 - Cada sede tendrá una conexión dimensionada según su actividad.
-

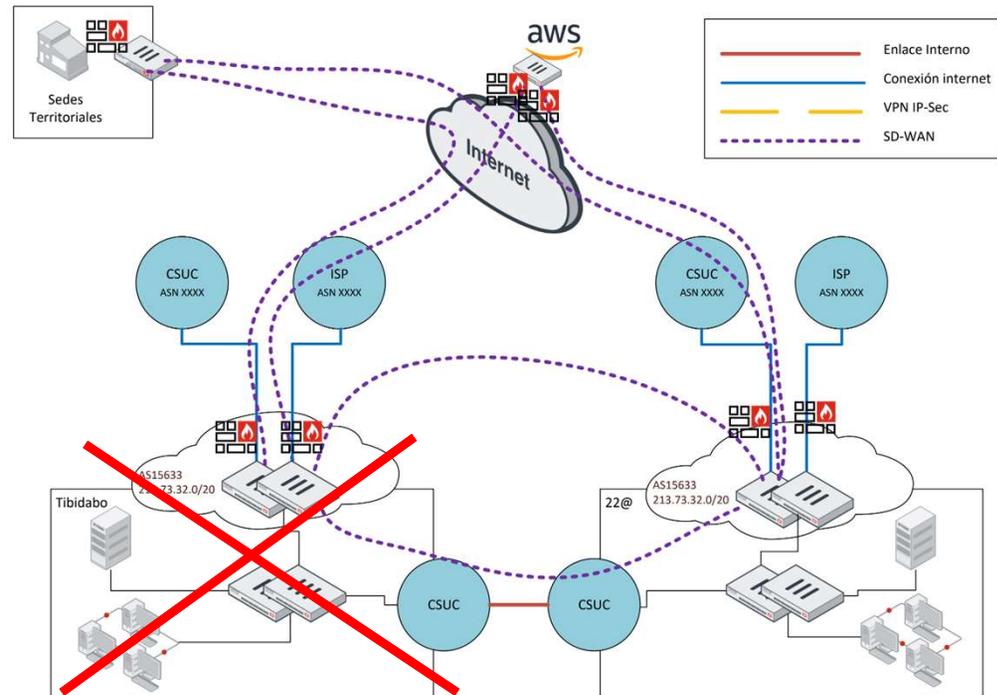
[SOL] Solución tecnológica.

2 Cada sede con su propia seguridad.

- Las sedes son autónomas y garantizan por si mismas su propia seguridad.
 - La política de seguridad se adaptará a las características de la sede, tenemos laboratorios en el 22@, las sedes territoriales son pequeñas, ...
 - Las configuraciones de seguridad en los firewalls se construyen partiendo de cero, no es lo mismo proteger un CPD, como teníamos hasta ahora, que oficinas donde básicamente hay portátiles.
-

[SOL] Solución tecnológica.

- Diagrama de conexión de la sedes con firewalls y servidor de VPN.
- En medio del proyecto, nos anuncian que abandonamos la sede de Tibidabo.



[SOL] Solución tecnológica.

3 SDWAN, red de area extendida definida por software

- El SDWAN independiza el acceso de los servicios y aplicaciones a las comunicaciones de la red física. Por ejemplo nos permite tener aun algunos servicios en la sala de máquinas como el servicio de impresión.
 - Nos permite priorizar y aplicar distintas calidades de Servicio a diversas aplicaciones como la videoconferencia.
-

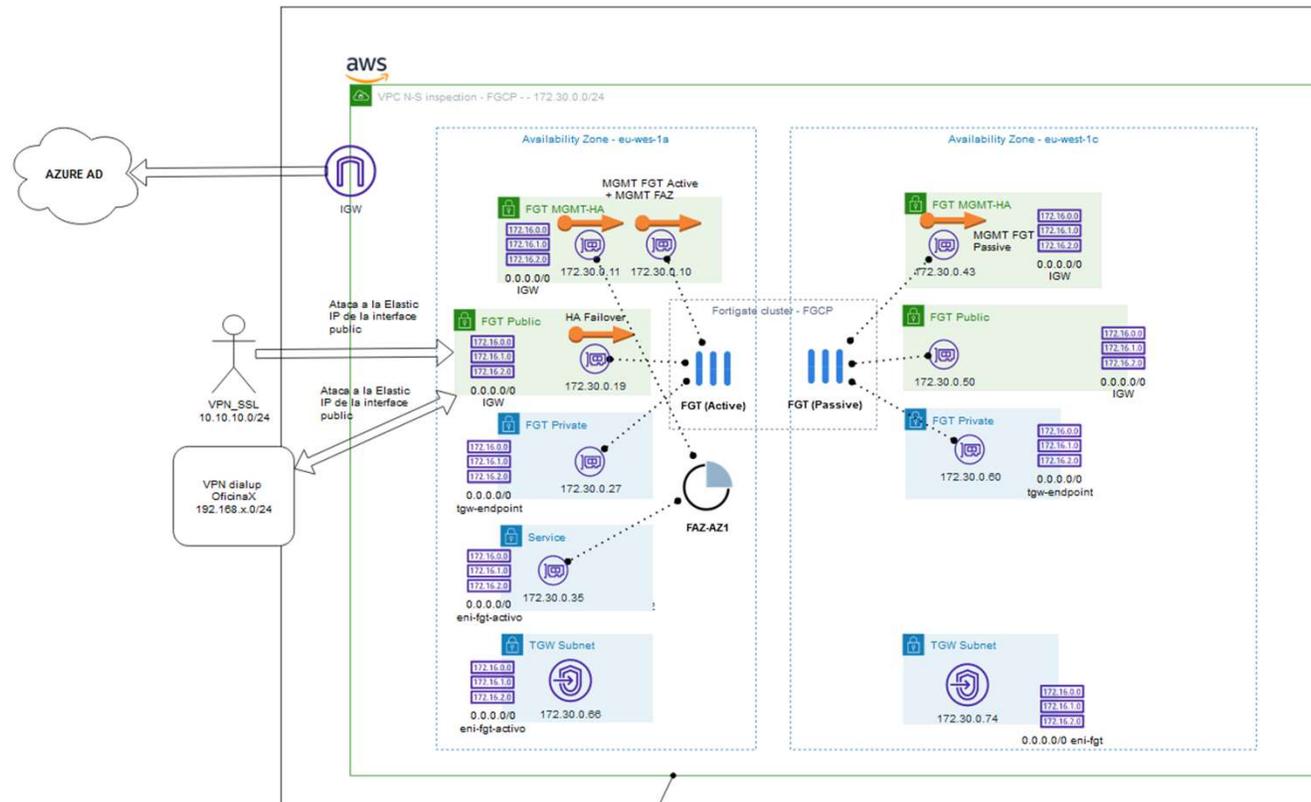
[SOL] Solución tecnológica.

Diagrama HUB

1 región

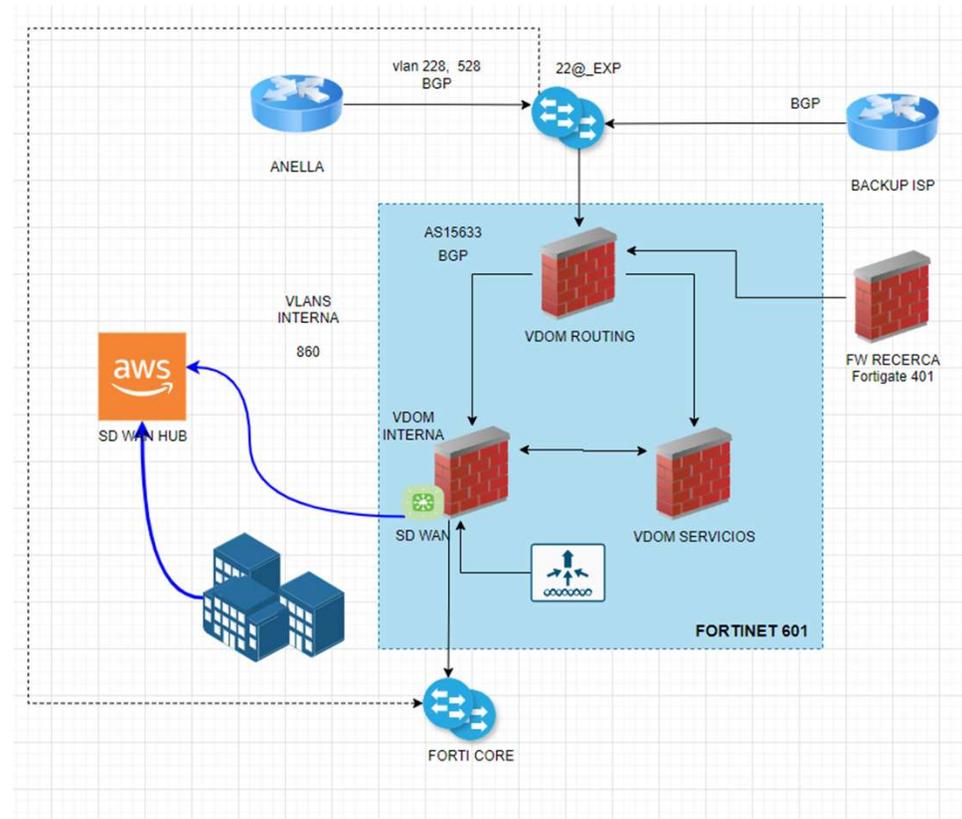
2 zonas de

disponibilidad



[SOL] Solución tecnológica.

- Diagrama campus UOC en el 22@



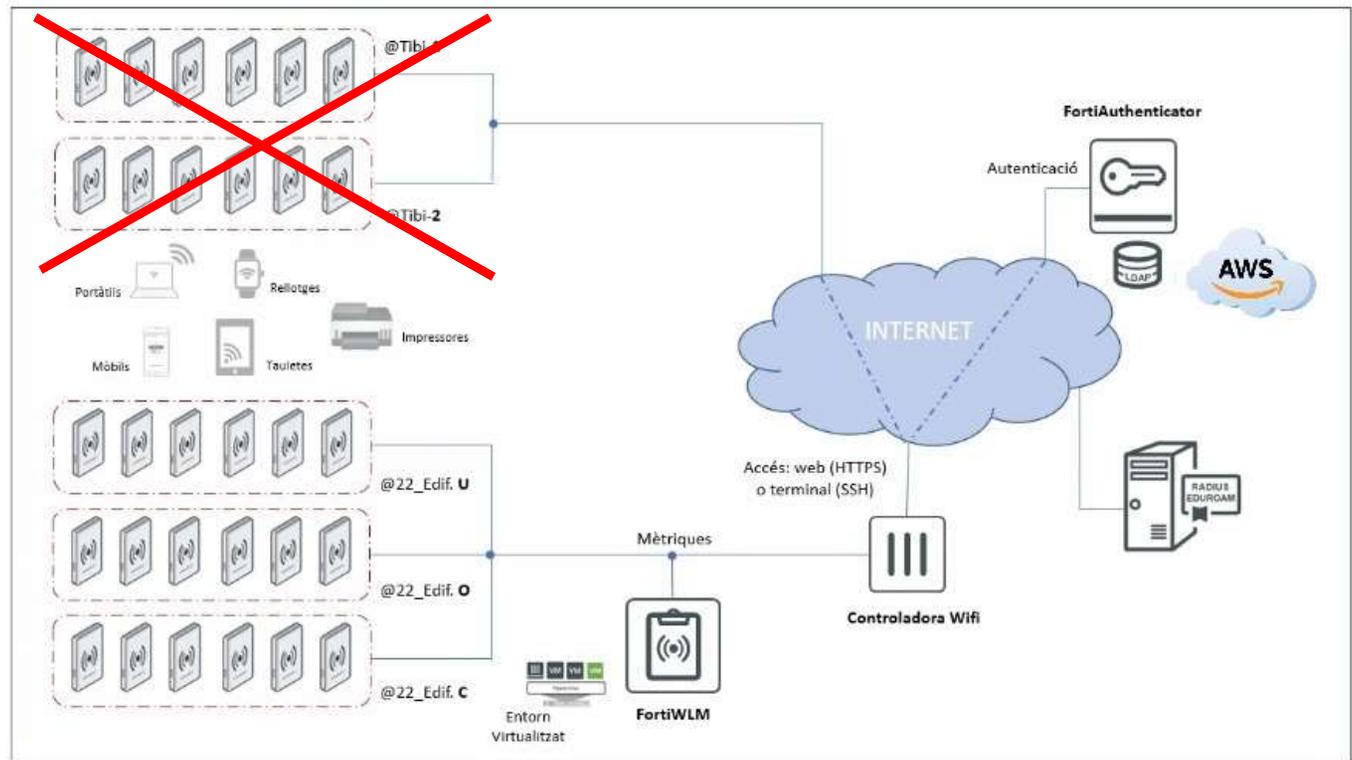
[SOL] Solución tecnológica.

4 La nueva Wifi

- Hemos mejorado las capacidades y prestaciones del servicio wifi anterior, cobertura, densidad de dispositivos y usuarios posibles (x5) y actualizado la tecnología.
- Hemos equipado las nuevas oficinas de la UOC.
- Soportamos dispositivos wifi corporativos y no corporativos.
- Hemos segmentado la red con almenos 6 SSID
 - Red corporativa: CampusUOC
 - Eduroam: eduroam
 - Red de invitados: UOC_Guests
 - Red de Investigación: Damasio
 - IoT (Servicio de Infraestructuras, termostatos, tornos, ...)
 - Red de eventos: CongressosUOC

[SOL] Solución tecnológica.

Diagrama wifi



[SOL] Solución tecnológica.

5 Servidor de VPN en el cloud, AWS

- Las aplicaciones y servicios las tenemos en el cloud, por lo tanto es donde tiene sentido localizar su acceso privilegiado. (Para su administración, configuración, aplicaciones con arquitectura no segura).
 - Necesitaremos también servidores de VPN secundarios en el campus del 22@, para administrar los laboratorios y la pequeña sala de máquinas que nos queda (control de los tornos de acceso, LAN, clima, etc.)
 - Debemos tener un Firewall en el cloud para proteger nuestro entorno del acceso VPN.
-

[SOL] Solución tecnológica.

6 Fabricante único, Fortinet

- Facilita la administración con una consola única. Nos aseguramos la compatibilidad entre distintos elementos y nos facilita su actualización.
 - Usamos el mismo elemento para distintos subservicios, routers, firewalls, concentrador VPN i controladora wifi comparten el mismo hardware. El método de autenticación y autorización será único. Supone un ahorro.
 - Esperamos que aumente la Seguridad al ser un fabricante especializado en Seguridad.
-

[SOL] Solución tecnológica.

7 Autenticación y autorización

- Usamos el doble factor de autenticación de Microsoft/Azure con el Microsoft Authenticator por su fácil integración con nuestro entorno Microsoft y la rapidez de integración.
 - Para distinguir entre dispositivos y aplicar políticas, cuales son corporativos, cuales de investigación, cuales personales usamos el Forticlient.
-

[INV]

Caso de la red de investigación e innovación

[INV] El caso de la red de investigación e innovación.

1 Planteamiento general

- La red de investigación e innovación tiene políticas propias de seguridad, que permiten una mayor flexibilidad que la red corporativa.
 - Para abordar su diseño iniciamos un proceso de benchmark con visitas distintas instituciones, tanto universidades como institutos.
 - El siguiente paso fue entrevistar a miembros de los distintos grupos de investigación para recoger de forma exhaustiva sus necesidades.
-

[INV] El caso de la red de investigación e innovación.

2 Benchmark

- Visitamos instituciones de distinto tipo, ICFO, Departamento TSC de la UPC, diversos laboratorios de la UPF.
 - La principal conclusión es que el catálogo de servicios juega un papel fundamental, tanto los servicios que se prestan a los laboratorios como los que ofrecen.
 - La segmentación de las instituciones visitadas es menos compleja que la que nos planteamos nosotros, una institución por perfil de usuario y tipo de máquina, otra por laboratorio.
 - Los recursos para el soporte y administración de la red y los servicios prestados en estas instituciones son superiores a los que dedicamos en al UOC
-

[INV] El caso de la red de investigación e innovación.

3 Entrevistas a personas de distintos grupos

- Tanto investigadores como gestores, para tener un listado exhaustivo con un enfoque de máximos.
 - Equilibrio entre la autonomía del investigador y la seguridad y facilidad de gestión. Es distinto que en la red corporativa pero sigue existiendo. El entorno debe ser gobernable.
 - Nos aparecen sorpresas, como la petición de poder imprimir de forma fácil desde la wifi de investigación.
 - Equilibrio entre modelo simple y modelo escalable, un cambio de arquitectura tiene un coste alto.
-

[INV] El caso de la red de investigación e innovación.

3 Entrevistas a personas de distintos grupos

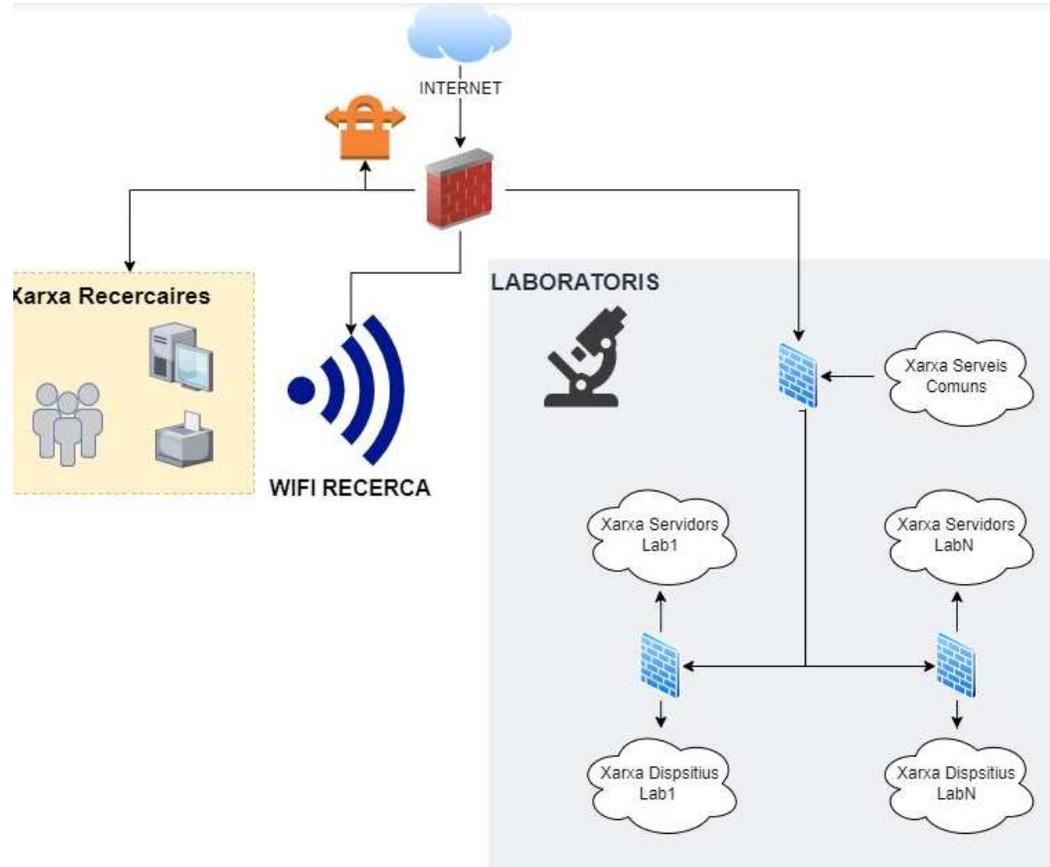
- Tanto investigadores como gestores, para tener un listado exhaustivo con un enfoque de máximos.

Sol·licitant	Categoria	Data	Tipus de requeriment	Requeriment	Comentaris de UOC
WINE	Accesos	28/07/2023	Accesos	Acceso a los equipos desde el exterior de la red	Caso de uso VPN
WINE	Xarxes	28/07/2023	Xarxes	Extender VLANs de Anella hacia el laboratorio (roseta) , tanto externas como entre edificios UOC	Hay que tener en cuenta que esto afecta tanto a la red corpo como a la Red de Recerca
WINE	Xarxes	28/07/2023	Xarxes	Ellos tienen ya una red aislada por un router por tanto solo necesitan que les demos el servicio de Gateway hacia internet. También necesitan que les entreguemos un rango privado de IPs, que gestionaran ellos, y en algunos casos mapear alguna IP privada en una pública para poder publicar servicios (esto lo gestionamos nosotros).	Inicialmente piden una /24 privada y una /29 publica pero ... podemos darles mas privadas pensando en futuro y las publicas .. no creo que tengamos que asignarles un rango para poder gestionarlas mejor
WINE	Xarxes	28/07/2023	Xarxes	Seria deseable poder usar IPv6	
WINE	Administratiu	28/07/2023	Administratiu	Necesidad de instalar FTTH en el laboratorio	Requerimiento administrativo, no afecta al diseño de la red de recerca en si
WINE	Administratiu	28/07/2023	Administratiu	Puenteo de equipos del laboratorio a otros edificios del 22@	Toni comenta que se puede hacer por las fibras tiradas entre edificios. Requerimiento administrativo, no afecta al diseño de la red de recerca en si
WINE	Administratiu	28/07/2023	Administratiu	Desplegar equipos (antenas) en el tejado de los Edificios del 22@	Requerimiento administrativo, no afecta al diseño de la red de recerca en si
WINE	Xarxes	4/9/2023	Xarxes	Tenen algun equip a Tibidabo que voldrien que estiguessin a la Xarxa de Recerca	Cal especificar-ho be

[INV] El caso de la red de investigación e innovación.

Sol·licitant	Àrea / Grup / Institut	Requeriment	Comentaris de UOC
Juanjo Martí	Oficina de Serveis Cientifictècnics	Laboratorios segmentados entre ellos	
Juanjo Martí	Oficina de Serveis Cientifictècnics	Laboratorios segmentados internament (subred de experimentos equipos de medida y red con servidores y equipos de control)	
Juanjo Martí	Oficina de Serveis Cientifictècnics	Servicio de cómputo y disco transversal a todos los laboratorios (backup)	
Juanjo Martí	Oficina de Serveis Cientifictècnics	Algunos laboratorios accesibles y con acceso a internet (segmento de servidores y equipos de control, por ejemplo servidores streaming)	
Juanjo Martí	Oficina de Serveis Cientifictècnics	Conectividad entre redCorp i Recerca para servicios diversos (Servicio de impresión)	
Juanjo Martí	Oficina de Serveis Cientifictècnics	Acceso a internet desde la red de usuarios de Recerca con usuarios autenticados siempre (corporativos, investigadores e invitados)	portal cautivo
Juanjo Martí	Oficina de Serveis Cientifictècnics	red cableada y wifi, con ssid específicos	
Juanjo Martí	Oficina de Serveis Cientifictècnics	Red accesible a usuarios no UOC	
Juanjo Martí	Oficina de Serveis Cientifictècnics	Acceso a los laboratorios VPN/SSH desde Internet y el resto de la red UOC	
Juanjo Martí	Oficina de Serveis Cientifictècnics	Diversos perfiles de acceso: investigadores, estudiante de doctorado y visitas. También startups	
Juanjo Martí	Oficina de Serveis Cientifictècnics	Compatibilidad electromagnética, equipos sensibles a interferencias en el Neurolab sobre todo	
Juanjo Martí	Oficina de Serveis Cientifictècnics	En algunos casos los equipos en la wifi se deben ver entre sí	
Juanjo Martí	Oficina de Serveis Cientifictècnics	Poder configurar IPs fijas en algunos de los equipos de los laboratorios	DHCP Reserves
Juanjo Martí	Oficina de Serveis Cientifictècnics	Mantener los direccionamientos CSUC (los que empiezan por 84.88.xx) para laboratorios especiales.	
Todos	Todos	Guardias Exámenes se hacen en el Edificio C , han de ser puntos de red Corpo	Garantizar que en el edificio C se pueda seguir conectando a Corpo, aunque sea con un nuevo switch
Todos	Todos	Definir como se decide a que red se conecta cada dispositivo (mac, login, ...)	Comentar con Toni
Juanjo Martí David Megías	IN3 Oficina de Serveis Cientifictècnics	Publicación de servicios en internet	
Juanjo Martí David Megías	IN3 Oficina de Serveis Cientifictècnics	Compartición de recursos de cómputo con otros laboratorios (Ya mencionado en línea 4)	
Juanjo Martí David Megías	IN3 Oficina de Serveis Cientifictècnics	Conectividad equipos de sedes UOC (Tibidabo, Almagavars...) con la red de investigación	Prerequisitos una red no debe afectar a la otra, deberían estar separadas
Juanjo Martí	Oficina de Serveis Cientifictècnics	Establecer caso de uso para la conexión de recursos en AWS con los CPD de Tibidabo y 22@ una vez movidos a la red de investigación	
Todos	Todos	Gestion de identidades de los usuarios de la red de investigación	
Todos	Todos	Presencia de puntos de red corpo en edificio C, en recepción y se deben poder añadir puntos nuevos cuando sea necesario.	
David Masip	Escola de Doctorat	Acceso a internet (Duplicado línea 7)	
Todos	Todos	Acceso a servicios de impresión	
Mireia Riera	Recerca i Innovació	Acceso a otros laboratorios para colaboraciones	
Mireia Riera	Recerca i Innovació	Necesidad de dotar de usuario UOC a colaboradores	
Mireia Riera	Recerca i Innovació	Acceso a recursos internos desde internet con usuario UOC, por ejemplo biblioteca	
Mireia Riera	Recerca i Innovació	Red de investigación extendida a Almagavars (duplicado línea 19).	
Todos	Todos	Red de investigación accesible por VPN	
David Megías	IN3	Acceso a los equipos desde el exterior de la red	
David Megías	IN3	Extender VLANs de Anella hacia el laboratorio (roseta) , tanto externas como entre edificios UOC	

[INV] El caso de la red de investigación e innovación.



[CON]

**Conclusión, resultado del
proyecto**

[CON] Resultados y lo que hemos aprendido

- Una migración al cloud tiene un impacto fuerte en la red de la universidad y su arquitectura al cambiar su propósito.
 - En el caso de la UOC la red se simplifica al desaparecer el CPD. A su vez, disminuye su criticidad, ya que los estudiantes siguen recibiendo servicio aunque la red esté caída.
 - Valorar cuantitativamente la simplificación de la administración consecuencia de tener un solo fabricante aún no lo hemos hecho ya que el proyecto no está terminado.
 - Tenemos un piloto de red específica para la investigación con el laboratorio de comunicaciones Wireless. Valorar los compromisos establecidos a priori (autonomía/administración&seguridad, simplicidad/escalabilidad)
-

Universitat Oberta
de Catalunya

UOC

 UOC.universitat
 @UOCuniversitat
 UOCuniversitat
