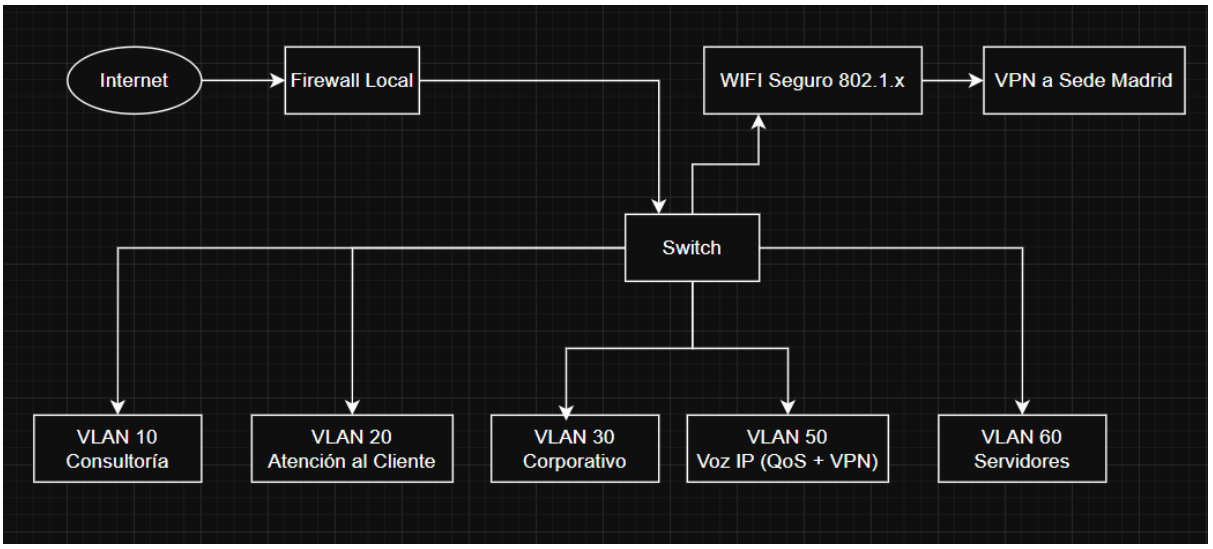
Diagrama de Red y Topologías

TechSys Solutions S.L.

Sede Barcelona

1. Introducción Este documento describe la estructura y configuración segura de la red en la sede regional de TechSys Solutions S.L. en Barcelona. Su propósito es proteger los activos de información, garantizar la continuidad operativa y aplicar medidas de seguridad efectivas sobre el tráfico interno, acceso remoto y perímetro.



2. Topología de Red de la Sede Barcelona

La red de la sede Barcelona está organizada en una topología jerárquica, con segmentación mediante VLANs según funciones organizativas y servicios. Se utilizan SSID diferenciados para el acceso inalámbrico y una VPN site-to-site conecta esta sede con la sede central en Madrid.

3. VLANs y Descripción

VLAN	Uso/Departamento	Comentarios
VLAN10	Consultoría	Acceso a recursos virtualizados en Cisco UCS
VLAN20	Atención al Cliente	Acceso controlado a aplicaciones regionales
VLAN30	Corporativo	Acceso a recursos generales de oficina

VLAN50	Voz IP	Tráfico priorizado por QoS y enrutado por VPN hacia Madrid
VLAN60	Servidores	Segmento para servidores locales y backups

4. Componentes de Red y Servicios

- **Wi-Fi corporativo e invitados**: Con SSID separados, autenticación 802.1X y cifrado WPA3.
- **VPN site-to-site**: Conexión segura con Madrid para sincronización de servicios y voz.
- **Servidores locales**:
    - Servidor de almacenamiento para Consultoría y Soporte.
    - Cisco UCS C240 M6 para virtualización.
    - Backup secundario (Servidor 1).
    - Aplicaciones regionales (Servidor 2).
- **Telefonía IP**: Centralita Avaya IP Office 500V2 en VLAN50, soporte para softphones y apps.

5. Controles de Seguridad Implementados

5.1 Segmentación y filtrado

- VLANs para separar funciones y aplicar RBAC.
- Políticas de firewall entre VLANs según el principio de menor privilegio.

5.2 Perímetro

- NGFW (Firewall de nueva generación).
- Políticas estrictas de salida a Internet.
- Filtrado DNS con detección de malware.

5.3 Supervisión

- Logs enviados al SIEM centralizado en sede Madrid.
- Monitorización de tráfico, conexiones remotas y cambios críticos.

6. Acceso Remoto y Teletrabajo

- VPN corporativa con MFA obligatoria.
- Validación de cumplimiento BYOD (antivirus, cifrado de disco).
- Acceso limitado según roles definidos (RBAC).