Proyecto de Arquitectura de Red — Volkswagen Guatemala

**Fecha: 09/10/2025**

**1. Alcance y objetivos**

**Este documento define la arquitectura física y lógica de la red corporativa de Volkswagen en Guatemala, incluyendo: diseño de espacios físicos, cableado estructurado (horizontal y vertical), servicios de proveeduría, y un plan de subneteo por departamentos con redes separadas e incomunicadas entre sí.**

**2. Diagrama macro de la red**

**El siguiente diagrama resume la arquitectura de alto nivel (perímetro/DMZ, core/datacenter, acceso por departamentos, sucursales y nube):**

**flowchart TB**

**%% Entradas/Proveedores**

**subgraph Internet\_Proveedores[Internet y Proveedores]**

**ISP1[(ISP Primario)]**

**ISP2[(ISP Secundario)]**

**MPLS[(MPLS / SD-WAN Provider)]**

**Cloud[(Nube Pública: IaaS/SaaS)]**

**end**

**%% Perímetro / DMZ**

**subgraph Perimetro\_DMZ[Perímetro y DMZ]**

**FW\_ACT{{Firewall Perimetral Activo}}**

**FW\_PAS{{Firewall Perimetral Pasivo}}**

**WAF[WAF / Reverse Proxy]**

**LB[Balanceador de Carga]**

**VPN[Concentrador VPN SSL/IPsec]**

**DDI[Servicios DDI (DNS/DHCP/IPAM)]**

**PROXY[Proxy/Seguridad Web]**

**IDS[IDS/IPS]**

**DMZ\_W[Web/App Servers DMZ]**

**DMZ\_M[Mail/Relay/SMTP]**

**end**

**%% Core / Datacenter**

**subgraph DC[Datacenter Core]**

**CORE1[[Core Switch 1]]**

**CORE2[[Core Switch 2]]**

**DIST1[[Distribución 1]]**

**DIST2[[Distribución 2]]**

**VMW[Cluster de Virtualización]**

**STG[Cabina de Almacenamiento]**

**BKP[Backup/DR]**

**NAC[NAC/802.1X RADIUS]**

**MON[Monitoreo (NMS/SIEM)]**

**AD[Directorio/AAA]**

**MAIL[Correo/Collab]**

**ERP[ERP/DB Apps Internas]**

**end**

**%% Acceso / Departamentos (VLANs por área)**

**subgraph Acceso[Capas de Acceso por Departamento]**

**HR[Acceso RRHH]**

**FIN[Acceso Finanzas]**

**VTA[Acceso Ventas]**

**MKT[Acceso Marketing]**

**TI[Acceso TI]**

**OPS[Acceso Operaciones/Logística]**

**PD[Acceso Producción/Servicio]**

**INV[Acceso Inventario]**

**GEST[Acceso Gerencia]**

**INVIT[Red de Invitados]**

**IOT[Red IoT/Impresoras/CCTV]**

**end**

**%% Sucursales**

**subgraph Sucursales[Agencias/Concesionarios / Talleres]**

**SDWAN1[Edge SD-WAN Sucursal 1]**

**SDWAN2[Edge SD-WAN Sucursal 2]**

**SDWANn[Edge SD-WAN n]**

**AP\_B[APs WiFi Sucursales]**

**end**

**%% Conexiones Proveedores → Perímetro**

**ISP1 -- Internet --> FW\_ACT**

**ISP2 -- Internet Backup --> FW\_PAS**

**MPLS -- Transporte/SD-WAN --> FW\_ACT**

**Cloud --- WAF**

**%% Perímetro → DMZ y Core**

**FW\_ACT <--> FW\_PAS**

**FW\_ACT --> WAF --> LB --> DMZ\_W**

**FW\_ACT --> DMZ\_M**

**FW\_ACT --> PROXY**

**FW\_ACT --> IDS**

**FW\_ACT --> VPN**

**FW\_ACT --> DDI**

**FW\_ACT --> CORE1**

**FW\_PAS --> CORE2**

**%% Core redundante**

**CORE1 <--> CORE2**

**CORE1 --> DIST1**

**CORE2 --> DIST2**

**%% DC servicios**

**DIST1 --> VMW**

**DIST1 --> STG**

**DIST1 --> BKP**

**DIST1 --> NAC**

**DIST1 --> MON**

**DIST1 --> AD**

**DIST1 --> ERP**

**DIST1 --> MAIL**

**DIST2 --> VMW**

**DIST2 --> STG**

**DIST2 --> BKP**

**DIST2 --> NAC**

**DIST2 --> MON**

**DIST2 --> AD**

**DIST2 --> ERP**

**DIST2 --> MAIL**

**%% Acceso por departamentos (aislados mediante VLAN/ACL/VRF)**

**DIST1 --> HR**

**DIST1 --> FIN**

**DIST1 --> VTA**

**DIST1 --> MKT**

**DIST1 --> TI**

**DIST1 --> OPS**

**DIST1 --> PD**

**DIST1 --> INV**

**DIST1 --> GEST**

**DIST1 --> INVIT**

**DIST1 --> IOT**

**DIST2 --> HR**

**DIST2 --> FIN**

**DIST2 --> VTA**

**DIST2 --> MKT**

**DIST2 --> TI**

**DIST2 --> OPS**

**DIST2 --> PD**

**DIST2 --> INV**

**DIST2 --> GEST**

**DIST2 --> INVIT**

**DIST2 --> IOT**

**%% Sucursales por SD-WAN**

**FW\_ACT <--> SDWAN1**

**FW\_ACT <--> SDWAN2**

**FW\_ACT <--> SDWANn**

**SDWAN1 --> AP\_B**

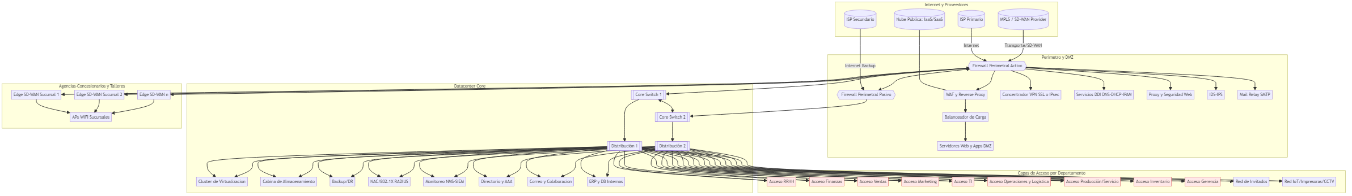
**SDWAN2 --> AP\_B**

**SDWANn --> AP\_B**

**%% Políticas de segmentación**

**classDef aislado fill:#ffe8e8,stroke:#c33,stroke-width:1px**

**class HR,FIN,VTA,MKT,TI,OPS,PD,INV,GEST aislado**

****

**3. Diseño de espacios físicos**

* **Sala MDF (Datacenter/Core):**

**Racks de 42U con rieles, PDU inteligentes, UPS en paralelo (N+1), climatización (in-row o CRAC, 22±2°C), control de acceso y detección/extinción.**

* **Pasillos caliente/frío, pisos técnicos, y canalización separada de datos/energía.**

**IDF por piso/área:**

* **Racks 24–42U, patch panels Cat6A, switches de acceso PoE+, UPS dedicado.**

**Distancia máxima de cobre ≤ 90 m hacia puestos/APs.**

* **Zonas de trabajo:**

**Puntos de red dobles por puesto; tomas eléctricas con UPS donde aplique.**

* **Sitios para AP WiFi según estudio de cobertura.**
* **4. Cableado estructurado**

**Horizontal (oficinas):**

* **Categoría: Cat6A U/UTP o F/UTP según EMI, con patch cords Cat6A.**

**Normas: TIA-568, TIA-606 para etiquetado, TIA-569 para rutas.**

* **Longitudes: 90 m canal permanente + 10 m patch cords.**

**Vertical (backbone):**

* **Fibra OM4 multimodo para inter-IDF en edificio; OS2 monomodo para campus.**

**Redundancia: 2 rutas físicas distintas hacia core; topología dual-homed o anillo.**

* **Conectores LC/UPC; MPO si se requiere alta densidad.**
* **5. Servicios de proveeduría**

**Conectividad:**

* **ISP primario y secundario con SLA empresarial (≥99.9%), BGP o failover.**

**SD‑WAN/MPLS para sucursales con enlace principal + LTE/5G de respaldo.**

* **Nube:**

**Conectividad segura (VPN IPsec/SSL) y opcional enlace dedicado.**

* **Gobernanza: CASB, cifrado en tránsito/repouso, gestión de claves.**

**Seguridad gestionada (opcional):**

* **SOC/SIEM, WAF, pruebas de penetración periódicas.**
* **6. Segmentación y políticas**

**Segmentación por departamentos con VLAN y, si aplica, VRF‑Lite para dominios de routing separados.**

* **Control de acceso a red (NAC 802.1X) con perfiles por rol/dispositivo (corporativo, invitado, IoT).**

**ACL de capa 3/4 y políticas L7 en firewall para bloquear cualquier tráfico inter-departamental, salvo excepciones aprobadas.**

* **Microsegmentación para servidores críticos (por ejemplo, mediante hipervisor o fabric overlay).**
* **7. Plan de subneteo por departamentos**

**Bloque sugerido: 10.0.0.0/16 (ajustable a 10.0.0.0/12 si se proyecta mayor crecimiento).**

* **Cada área con tamaño distinto y no repetido; ejemplos base (ajustables a la cantidad de equipos):**
* **| Departamento | Subred | Hosts útiles |**
* **|----------------------------------|----------------|--------------|**
* **| RRHH | 10.0.4.0/23 | 510 |**
* **| Finanzas | 10.0.8.0/24 | 254 |**
* **| Ventas | 10.0.12.0/22 | 1022 |**
* **| Marketing | 10.0.20.0/24 | 254 |**
* **| TI | 10.0.24.0/23 | 510 |**
* **| Operaciones/Logística | 10.0.28.0/22 | 1022 |**
* **| Producción/Servicio | 10.0.40.0/23 | 510 |**
* **| Inventario | 10.0.44.0/24 | 254 |**
* **| Gerencia | 10.0.48.0/25 | 126 |**
* **| Invitados (cautivo, aislado) | 10.0.49.0/23 | 510 |**
* **| IoT/Impresoras/CCTV | 10.0.52.0/22 | 1022 |**
* **| DMZ Pública | 10.0.60.0/24 | 254 |**
* **| Gestión/OOB | 10.0.61.0/24 | 254 |**
* **| Servidores/Virtualización | 10.0.62.0/23 | 510 |**
* **| Backup/DR | 10.0.64.0/24 | 254 |**

**Gateway por VLAN en los switches de distribución; HSRP/VRRP para HA.**

* **DHCP por VLAN (DDI) con reservas; DNS interno/externo segregado.**

**Políticas: sin enrutamiento entre departamentos (deny any inter-VLAN), excepto servicios comunes (p.ej., DNS, NTP, impresión) a través de puntos de control.**

**8. Incomunicación entre áreas (criterios)**

* **VLANs separadas y, si se desea aislamiento fuerte, VRFs separadas.**

**ACL explícitas en SVI y en firewall: negar cualquier tráfico L3 lateral.**

* **Portal cautivo para invitados y segmentación de IoT con control de acceso por MAC/profiling.**
* **9. Capacidad y crecimiento**

**Reserva del 30–40% de puertos y direcciones por IDF.**

* **Diseñar fibra con hilos de reserva (x2 del cálculo actual en backbone).**

**Roadmap a Wi‑Fi 6/6E; PoE budget dimensionado para APs y IoT.**

**10. Entregables y documentación**

* **Planos MDF/IDF con rutas de cableado, numeración de puertos y etiquetado.**

**Hoja de direccionamiento y plan de VLAN/VRF.**

* **Matriz de ACL/seguridad por departamento.**

**Inventario de proveedores y SLAs.**

**---**

**¿Deseas que convierta este documento a PDF/Word y que ajuste el plan de subneteo con el número real de equipos por cada departamento? Puedo generar una tabla personalizada si me indicas cantidades aproximadas actuales y proyectadas a 3 años.**