**Diseño y Optimización de una Red Corporativa con Segmentación y Seguridad- DataPlus S.A.**

|  |  |
| --- | --- |
| Título del informe: Diseño y Optimización de Red Corporativa con Segmentación y Seguridad – DataPlus S.A. | |
| Portafolio:  Lección 2: Propuesta de rediseño red segmentada – DataPlus S.A. | Entorno:  Caso hipotético de entorno industrial - DataPlus S.A. |
| Clasificación del documento:  Creación de entorno de red hipotético – publica | Modulo:  Fundamentos de redes y protocolos de comunicación. |
| Autor(es): Sebastián Hernández Téllez | Fecha de elaboración: 23 de agosto de 2025 |

**1. Diseño y Seguridad de la Red – Caso DataPlus S.A.**

***Resumen ejecutivo***

El informe presenta el diseño de la red corporativa de **DataPlus S.A.**, empresa con 60 empleados distribuidos en tres pisos. Se propuso una arquitectura jerárquica con **firewall NGFW**, **switches L3 apilados** y **switches PoE** en acceso, además de **Wi-Fi 6** para movilidad. La red fue segmentada en **VLANs** por departamentos y servicios, con rangos IP lógicos documentados. Se aplicaron políticas de enrutamiento inter-VLAN bajo el principio de mínimo privilegio. Se incluyeron medidas de seguridad como cifrado WPA3, autenticación 802.1X, filtrado de contenido e IDS/IPS. Finalmente, se propuso un plan de **escalabilidad** para soportar el crecimiento futuro de la empresa.

**2. Arquitectura de red (roles y dispositivos)**

***Modelo jerárquico (Core/Distribution/Access) con seguridad perimetral y DMZ.***

* **Perímetro** (WAN/LAN/DMZ/GUEST)
  + - **Cortafuegos NGFW** (zona WAN, LAN, DMZ y GUEST): NAT/PAT, VPN, IDS/IPS, filtrado de contenido, TLS inspection selectiva, DoS protection.
    - (Opcional) **Router de borde** si el ISP entrega BGP/PPPoE; en escenarios simples, el NGFW hace de router.
* **Núcleo/Distribución (MDF, piso 1)**
  + - **Par de switches L3 apilados** (core) para routing inter-VLAN a velocidad de cable, gateways virtuales (VRRP/HSRP), enlaces agregados (LACP) hacia cada IDF.
* **Acceso (IDF por piso)**
  + - **Switches PoE** por piso para PCs, impresoras, VoIP e **APs Wi-Fi 6/6E**.
    - **APs**: SSID corporativo con 802.1X y SSID invitados aislado.
* **Servidores**
  + - **Servidor de archivos** en **VLAN SERVERS (interna)**.
    - **Servidor Web** en **VLAN DMZ**, publicado mediante NAT 1:1/Port-forward y (opcional) **WAF/Reverse Proxy** delante.
* **Roles por piso / área**
  + - **Piso 1**: Administración + MDF + Servidores.
    - **Piso 2**: Desarrollo.
    - **Piso 3**: Soporte Técnico.
    - En cada piso: APs y switch de acceso dedicados; el tráfico sube por troncales 802.1Q al core.

**Justificación:** el núcleo L3 reduce latencia y cuellos de botella, la DMZ desacopla el servicio web de la red interna, y el NGFW controla de forma centralizada Internet, invitados y exposición pública.

**3. Topologías seleccionadas**

* **Acceso por piso → Estrella**: cada equipo al switch del piso (simple, fácil de administrar).
* **Backbone (IDF↔Core) → Estrella redundada/híbrida**: cada IDF dual-home al core con **LACP** (2×10GbE); RSTP/MSTP activo.
* **DMZ/Perímetro → Híbrida**: NGFW como punto de control, conmutación en estrella detrás y opciones de alta disponibilidad (par activo/pasivo).

**Justificación:** la estrella simplifica el fallo-aislamiento en acceso; los uplinks redundados + LACP dan resiliencia sin la complejidad de una malla total.

**4. Segmentación (VLANs + direccionamiento)**

**Bloque de direccionamiento:** 10.20.0.0/20 (permite 16 subredes /24 y facilita sumarización). Gateways SVI en el core L3 (VRRP/HSRP).

| **Piso** | **Departamento / Área** | **VLAN** | **Nombre VLAN** | **Subred** | **Gateway** | **Rango DHCP / Asignación IPs** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | Administración | 10 | ADMIN | 10.20.10.0/24 | 10.20.10.1 | 10.20.10.50 – 10.20.10.200 |
| 2 | Desarrollo | 20 | DEV | 10.20.20.0/24 | 10.20.20.1 | 10.20.20.50 – 10.20.20.230 |
| 3 | Soporte Técnico | 30 | SUPPORT | 10.20.30.0/24 | 10.20.30.1 | 10.20.30.50 – 10.20.30.200 |
| N/A | Servidores internos | 40 | SERVERS | 10.20.40.0/24 | 10.20.40.1 | Sin DHCP (IPs estáticas) → Ej: File Server 10.20.40.10, DNS 10.20.40.5 |
| N/A | Telefonía IP | 50 | VOICE | 10.20.50.0/24 | 10.20.50.1 | 10.20.50.20 – 10.20.50.200 |
| N/A | Wi-Fi Invitados | 60 | GUEST-WIFI | 10.20.60.0/24 | 10.20.60.1 | 10.20.60.10 – 10.20.60.250 |
| N/A | Gestión / Control | 70 | MGMT | 10.20.70.0/24 | 10.20.70.1 | Sin DHCP (IPs estáticas) → Switches, APs, controladoras |
| N/A | DMZ (Servidor Web) | 80 | DMZ | 10.20.80.0/24 | 10.20.80.1 | Sin DHCP (IPs estáticas) → Web Server 10.20.80.10 |

***Asignaciones clave (estáticas sugeridas)***

* AD/DNS/NTP: 10.20.40.5 • File Server: 10.20.40.10 • Web DMZ: 10.20.80.10
* Controladora Wi-Fi/NAC/RADIUS (si aplica): 10.20.40.20
* Syslog/SIEM: 10.20.40.30

***Política de enrutamiento inter-VLAN (principio de menor privilegio)***

* **GUEST (60)** → **Internet sólo**, **bloqueado** a LAN/DMZ.
* **DEV (20)/SUPPORT (30)/ADMIN (10)** → Internet permitido; acceso **limitado** a **SERVERS (40)** sólo a servicios necesarios (p.ej., SMB 445 al File Server, DNS/NTP).
* **DMZ (80)**:
  + - Entradas desde Internet: **80/443** únicamente al Web (10.20.80.10) mediante NAT/Port-forward o NAT 1:1 + WAF.
    - **Bloquear** DMZ→LAN por defecto; permitir solo lo imprescindible (ej., syslog hacia 10.20.40.30).
* **MGMT (70)**: sólo desde salt/bastión de administración y redes de TI específicas (ACL).

**5. Medidas básicas de seguridad**

***Cortafuegos (NGFW)***

* **Inbound (WAN→DMZ)**:
  + - Permitir TCP 80/443 → 10.20.80.10 (siempre que el sitio necesite 80; preferir redirección a 443).
    - Bloquear todo lo demás; Geo/IP reputation/DoS protection activos.
* **Outbound (LAN→WAN)**:
  + - Permitir navegación (TCP 80/443), **DNS sólo** hacia resolvers internos (10.20.40.5) o resolvers aprobados, NTP (UDP 123), correo (según política).
    - Bloquear P2P/anonimizadores/categorías de alto riesgo; aplicar **SSL inspection** selectiva para categorías de negocio si es viable legalmente.
* **Inter-VLAN (L3 ACLs)**:
  + **GUEST (60)**: DROP a 10.20.0.0/16; sólo WAN.
  + **DEV (20)**: Allow TCP 445 → 10.20.40.10; Allow UDP/TCP 53 → 10.20.40.5; Deny resto a SERVERS/ADMIN.
  + **SUPPORT (30)**: Accesos mínimos a herramientas internas (ej., ticketing) según puertos.
  + **ADMIN (10)**: Acceso a aplicaciones corporativas aprobadas; no administración de red salvo bastión.
  + **DMZ (80)**: Deny → LAN; Allow → 10.20.40.30 (syslog) y parches desde servidor de actualización mediante ventana controlada (pull desde LAN si se prefiere).

***Filtrado de contenido (SWG/DNS Security)***

* Categorías bloqueadas (malware, phishing, proxies, pornografía, P2P).
* **SafeSearch** forzado y bloqueo de dominios recién creados (DGAs).

***Wi-Fi***

* **SSID CORP**: **WPA3-Enterprise (802.1X EAP-TLS)** con RADIUS (certificados), PMF (802.11w) obligatorio, band-steering 5/6 GHz.
* **SSID GUEST**: WPA2-PSK (o portal cautivo), **aislamiento de clientes**, **solo Internet** (VLAN 60).
* Deshabilitar **WPS**, ocultar administración de APs en **VLAN MGMT (70)**.

***Protección contra intrusiones***

* **IDS/IPS**: reglas para escaneos, explotación web (SQLi/XSS), SMB/LDAP/RDP y botnets; modo prevención para firmas de alta certeza.
* **NAC/802.1X** en cableado (si es viable) para autenticar dispositivos y aplicar VLAN dinámica por rol.
* **End-point**: EDR en estaciones/servidores; hardening del servidor web y del file server (CIS Benchmarks).

***Gestión/Visibilidad***

* **Syslog/SIEM**, **SNMPv3**, **NTP** central, backups de configuraciones, control de cambios y parchado mensual.

**7. Plan de escalado (duplicar a ~120 empleados)**

* **Capacidad de acceso**: añadir switches PoE por piso; los uplinks ya están en **10GbE con LACP**.
* **Direcciones IP**: ampliar subredes de usuarios a **/23** donde se necesite (p. ej., DEV de 10.20.20.0/24 → 10.20.20.0/23), manteniendo el bloque 10.20.0.0/20.
* **Wi-Fi**: más APs por densidad; habilitar 6 GHz si hay clientela; control de RF automático.
* **Perímetro**: par de **firewalls en HA** + **segundo ISP** (failover o balanceo), y (opcional) **WAF** dedicado para el Web.
* **Servidores**: virtualización y almacenamiento central; balanceo para el Web y caché inverso.
* **Gestión de identidades**: reforzar 802.1X/NAC (postura de endpoint) con VLAN dinámica; Zero Trust para accesos remotos (VPN/ZTNA).

**8.** **Razones clave del diseño sugerido**

* **Segmentación por función** limita radios de ataque y simplifica políticas.
* **DMZ** separa exposición pública del core de negocio.
* **Core L3 apilado** = alto rendimiento + puerta de enlace redundante.
* **Políticas “deny-by-default”** inter-VLAN y GUEST solo-Internet reducen riesgo.
* **Topología jerárquica** facilita operación y escalado.

**9. Anexos**

***Diagrama de red segmentada***A diagram of a diagram

AI-generated content may be incorrect.