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

Descripción general del diseño y objetivos

El presente informe documenta el diseño técnico de una red corporativa para DataPlus S.A., una empresa de tamaño medio que opera en un edificio de tres pisos con un total de 60 empleados distribuidos en áreas de administración, desarrollo y soporte técnico. El diseño tiene como objetivo garantizar un alto nivel de disponibilidad, segmentación lógica del tráfico entre departamentos, acceso seguro a servicios internos (servidores de archivos y web) y conectividad confiable a Internet. Se prioriza la aplicación de buenas prácticas en topología, seguridad y escalabilidad, basadas en estándares de redes empresariales.

El diseño contempla una arquitectura jerárquica en tres capas (core, distribución, acceso), el uso de VLANs para aislar departamentos, una política de seguridad integral con firewall perimetral y segmentación interna, y una estructura que permita expandirse si la organización duplica su tamaño en el futuro.

Justificación de los dispositivos de red utilizados

Router de borde
El router conecta la red corporativa con el proveedor de servicios de Internet (ISP) y cumple funciones críticas como traducción de direcciones (NAT), ruteo entre subredes y enrutamiento estático o dinámico hacia redes externas. Puede incluir políticas de calidad de servicio (QoS) y backup de conexión WAN.

Firewall de nueva generación (NGFW)
Colocado en el perímetro, inspecciona el tráfico de entrada y salida a nivel de capa 7. Permite aplicar políticas de control granular, detección de amenazas, filtrado de contenido, protección contra intrusiones (IDS/IPS) y establecimiento de zonas de seguridad (DMZ).

Switches gestionables de nivel acceso
Cada piso cuenta con uno o más switches gestionables que permiten definir VLANs, configurar puertos como troncales o de acceso, implementar STP (Spanning Tree Protocol) para evitar bucles y aplicar políticas de PoE para alimentar puntos de acceso inalámbricos.

Switch de distribución
Conecta los switches de cada piso con el núcleo de red. Permite consolidar tráfico, rutear entre VLANs (si se usan switches capa 3) y aplicar reglas de seguridad entre segmentos.

Switch core (capa de núcleo)
Componente central de alto rendimiento que interconecta distribución, servidores y el firewall perimetral. Soporta velocidades de 10 Gbps o superiores, y se recomienda alta disponibilidad (redundancia).

Access Points Wi-Fi (APs)
Instalados en cada piso, permiten acceso inalámbrico seguro mediante redes WPA3-Enterprise, autenticación vía RADIUS, separación entre red corporativa y red de invitados, y roaming eficiente.

Servidor de archivos y servidor web local
Los servidores internos están conectados en la zona de servidores, idealmente en una VLAN dedicada. El servidor de archivos permite colaboración interna y respaldo, mientras que el servidor web aloja contenido público o herramientas internas.

UPS (Uninterruptible Power Supply)
Se instalan en el rack principal y en la zona de servidores para garantizar continuidad eléctrica, protección contra cortes y sobrecargas.

Asignación de VLANs y rangos IP por piso/departamento

Piso	Departamento	VLAN	Rango IP sugerido
1	Administración	10	192.168.10.0/24
2	Desarrollo	20	192.168.20.0/24
3	Soporte Técnico	30	192.168.30.0/24
-	Servidores internos	40	192.168.40.0/24
-	Red de invitados	50	192.168.50.0/24

Cada VLAN representa un dominio de broadcast aislado, lo que permite controlar el tráfico entre departamentos y reducir la propagación de amenazas. La red de invitados no tiene acceso a recursos internos y utiliza reglas específicas en el firewall para limitar su alcance.

Topología aplicada por segmento

La topología general del diseño es híbrida jerárquica. Se aplican diferentes esquemas según la capa de red:

- Topología en estrella por piso: cada dispositivo terminal se conecta a un switch de acceso.
- Topología jerárquica general: la red se estructura en tres niveles, con switches de acceso, distribución y core.
- Topología malla parcial entre switches de distribución y core: para redundancia y balanceo de carga.
- La zona de servidores está conectada directamente al core, lo que reduce latencia y cuellos de botella.

Esta elección permite una estructura modular, con rutas redundantes en las capas superiores, fácil administración y escalabilidad sin rediseñar el entorno completo.

Política de seguridad general

El diseño contempla una política de seguridad multinivel, basada en los principios de defensa en profundidad y segmentación estricta:

- El firewall perimetral aplica políticas de acceso desde/ hacia Internet, permitiendo únicamente los puertos requeridos (HTTP/HTTPS, DNS, correo) y bloqueando el resto.
- Entre VLANs internas, el tráfico está restringido por reglas ACL o políticas L3. Solo se permite comunicación entre departamentos según funciones definidas.
- El acceso Wi-Fi se segmenta por SSID. La red corporativa requiere autenticación mediante RADIUS y está vinculada a Active Directory. La red de invitados accede únicamente a Internet, mediante un portal cautivo.
- El servidor web local se expone en una zona DMZ, lo que permite filtrar y aislar el tráfico entrante antes de llegar al núcleo de red.
- Se implementa detección y prevención de intrusiones (IDS/IPS) en el firewall, con monitoreo activo del tráfico interno y externo.
- Se incluye un sistema de logs y alertas centralizadas para auditar eventos de red y seguridad.

Estrategia de escalabilidad si la empresa crece

El diseño contempla posibles escenarios de crecimiento y se anticipa a ellos mediante las siguientes prácticas:

- Espacio reservado en el direccionamiento IP para nuevos departamentos y sucursales.
- Uso de switches stackables y con uplinks de 10G para agregar nodos sin rediseñar la red física.
- División modular por piso o área, facilitando la expansión por bloques.
- Posibilidad de migrar servicios internos (servidor de archivos, correo, ERP) a infraestructura en la nube o modelo híbrido.
- Aplicación futura de políticas de calidad de servicio (QoS) para priorizar tráfico de voz sobre IP (VoIP), videoconferencias o aplicaciones críticas.
- Consideración de redes definidas por software (SDN) si el crecimiento requiere mayor automatización y flexibilidad.

Conclusiones técnicas

El diseño propuesto para la red de DataPlus S.A. responde a estándares profesionales de infraestructura corporativa, priorizando rendimiento, seguridad y adaptabilidad. La segmentación por VLAN, el modelo jerárquico de red, el control de tráfico entre capas y la política de seguridad perimetral e interna permiten garantizar la continuidad operativa de la empresa ante fallos, ataques o aumento de demanda. Además, se ha planteado una estrategia de crecimiento que evita cuellos de botella, facilita la integración de nuevas áreas y prepara el entorno para futuras migraciones hacia tecnologías más avanzadas.

Este diseño es sólido, modular y orientado a largo plazo, cumpliendo con los requerimientos técnicos y operativos de una empresa moderna.