**Informe sobre Infraestructura de Red, Políticas de Seguridad, Escalabilidad y Documentación Operacional**

**Introducción**

Este documento complementa el diseño lógico de red propuesto para la empresa DataPlus S.A. y amplía los aspectos técnicos relacionados con la elección de dispositivos, políticas de seguridad, escalabilidad proyectada y documentación operativa. Su propósito es consolidar las decisiones de infraestructura desde una perspectiva profesional, anticipando escenarios de crecimiento y cumplimiento de estándares.

**Dispositivos de red y su justificación técnica**

Para una red de tamaño medio distribuida en tres pisos y que requiere alta disponibilidad, control granular y segmentación lógica, se recomienda la siguiente infraestructura:

**Router empresarial con capacidad de enrutamiento dinámico y redundancia WAN**

- **Tipo**: Router empresarial con soporte para BGP/OSPF, NAT y redundancia WAN.
- **Rol**: Enlace entre la red LAN corporativa y el proveedor de servicios de Internet (ISP).
- **Justificación**: Provee resiliencia ante caída de enlaces, permite ruteo eficiente, balanceo de carga y políticas de salida diferenciadas.

**Firewall de Capa 7 (Next Generation Firewall – NGFW)**

- **Tipo**: Firewall con inspección profunda de paquetes (DPI), filtrado de aplicaciones, IPS, VPN y control de acceso por identidad.
- **Rol**: Protección perimetral y control entre zonas de seguridad internas (VLANs).
- **Justificación**: Permite aplicar políticas basadas en usuario/aplicación, proteger contra amenazas, aislar servicios expuestos (DMZ) y habilitar acceso remoto seguro (VPN SSL/IPSec).

**Switch Core L3 (10G, redundante, alta capacidad)**

- **Tipo**: Switch de capa 3, con capacidad de ruteo entre VLANs, enlaces agregados (LACP) y soporte para VRRP/HSRP.
- **Rol**: Núcleo de la red, donde convergen servidores, switches de distribución y enlaces troncales.

- **Justificación**: Soporta alta carga de tráfico, baja latencia, y resiliencia con rutas redundantes y balanceo.

**Switches de distribución (L2+ o L3 stackables)**

- **Tipo**: Gestionables, con múltiples VLANs, STP, PoE+ y puertos uplink SFP+.
- **Rol**: Interconexión entre el core y los switches de acceso de cada piso.
- **Justificación**: Modularidad para futuras expansiones y separación lógica de áreas físicas y funcionales.

**Switches de acceso por piso**

- **Tipo**: Gestionables, PoE, con capacidad de configurar puertos de acceso y troncal, y monitoreo SNMP.
- **Rol**: Punto de conexión para dispositivos finales (PCs, impresoras, APs).
- **Justificación**: Permite aplicar control por puerto (802.1X), segmentar tráfico y alimentar APs sin requerir adaptadores externos.

**Access Points Wi-Fi 6 o superior**

- **Tipo**: APs de doble banda con soporte para WPA3-Enterprise, RADIUS y roaming rápido (802.11r).
- **Rol**: Proporcionar conectividad inalámbrica a dispositivos móviles corporativos y visitantes.
- **Justificación**: Alto rendimiento, menor latencia, mejor cobertura y seguridad avanzada.

**Servidores físicos o virtualizados**

- **Tipo**: Equipos en rack con hipervisores para virtualización (VMware, Hyper-V, Proxmox).
- **Rol**: Alojar servicios internos como almacenamiento, servidor web, autenticación, bases de datos.

- **Justificación**: Ahorro energético y de espacio, rápida provisión de servicios y facilidad de backup.

**UPS para nodos críticos**

- **Tipo**: Sistemas de energía ininterrumpida con monitoreo de batería.
- **Rol**: Garantizar el funcionamiento de switches, firewall y servidores durante cortes eléctricos.
- **Justificación**: Prevención de pérdidas de datos y protección de hardware ante apagones abruptos.

**Políticas de seguridad profesional**

**Políticas de firewall perimetral**

- Permitir solo puertos TCP 80 (HTTP), 443 (HTTPS) y 53 (DNS) hacia Internet desde usuarios internos.
- Bloquear tráfico saliente innecesario (por ejemplo, puertos de P2P, Telnet, NetBIOS).
- Crear zona DMZ para el servidor web público, con inspección específica y sin acceso directo a la LAN.

**Control de tráfico entre VLANs**

- Administración puede acceder a todos los segmentos.
- Desarrollo y Soporte no pueden comunicarse directamente.
- Invitados Wi-Fi aislados sin acceso a VLANs internas.
- Todo el tráfico inter-VLAN debe pasar por el firewall para aplicar inspección y logging.

**Seguridad Wi-Fi corporativa**

- Red interna autenticada por 802.1X contra un servidor RADIUS (posiblemente vinculado a Active Directory).

- Red de invitados aislada con portal cautivo y acceso limitado a Internet mediante políticas de ancho de banda.

- Implementación de WPA3-Enterprise para resistencia ante ataques de diccionario y suplantación.

**Implementación de IDS/IPS**

- Activación del motor IDS/IPS en el firewall perimetral, con firmas actualizadas periódicamente.

- Monitoreo del tráfico entrante y lateral (east-west) para detectar movimientos laterales.

- Reglas personalizadas para alertar sobre patrones de escaneo de puertos, intentos de RDP, SSH y brute-force.

**Monitoreo y filtrado de contenido**

- Filtro web por categorías (malware, redes sociales, apuestas, pornografía).

- Monitoreo del uso de ancho de banda por usuario, IP y protocolo.

- Integración con sistema de alertas vía correo o dashboards (Zabbix, PRTG, Graylog).

**Propuesta de escalabilidad futura**

**Expansión del direccionamiento IP**

- Cambiar máscara de subred de /24 a /23 para duplicar capacidad de hosts sin cambiar esquema de VLAN.

- Agregar subredes adicionales con planificación anticipada (por ejemplo, reservar 192.168.100.0/22 para futuras oficinas o pisos).

**Agregado de switches y stackabilidad**

- Uso de switches stackables que permitan agregar nodos sin modificar el plano de control.

- Incorporación de enlaces redundantes y balanceados con LACP para evitar cuellos de botella.

**Virtualización y migración a la nube**

- Plan para migrar el servidor de archivos a una solución híbrida (ej. Azure Files, Amazon FSx).
- Contemplar Office 365 o G Suite para correo y productividad.
- Considerar infraestructura como código (IaC) para redes virtuales (Terraform, Ansible).

**Aplicación de QoS**

- Clasificación de tráfico mediante DSCP para priorizar VoIP, videollamadas y tráfico de aplicaciones críticas.
- Políticas en switches para evitar congestión en enlaces de distribución.
- Asignación de colas de prioridad en el firewall para evitar pérdida de paquetes en tráfico sensible.

**Documentación avanzada**

**Configuración tipo de switches (VLANs y puertos)**

```
# VLAN tagging
vlan 10
 name Administración
vlan 20
 name Desarrollo
vlan 30
 name Soporte
vlan 40
 name Servidores
```

```
vlan 50
 name Invitados

# Configuración de puerto troncal
interface GigabitEthernet1/0/1
 description Trunk hacia distribución
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30,40,50

# Puerto de acceso (ejemplo para Administración)
interface GigabitEthernet1/0/2
 description PC Administrativo
 switchport mode access
 switchport access vlan 10
```

**Políticas de respaldo**

- Respaldos automáticos diarios de configuraciones de switches y firewall.
- Backup incremental de servidores en NAS local y replicación mensual en la nube.
- Logs de eventos almacenados en servidor syslog central y respaldados por 30 días.

**Inventario de red**

- Etiquetado físico de todos los puertos y cables.
- Registro de número de serie, ubicación física y dirección MAC/IP.
- Hoja de vida de switches, routers, APs y servidores.

**Manual breve para IT interno**

- Procedimiento para agregar una nueva VLAN.
- Instrucciones para recuperar configuración desde copia de seguridad.
- Pasos para diagnosticar caídas de conectividad por capa (física, enlace, red).
- Protocolo ante ataque o incidente (aislar equipo, extraer logs, notificar).

**Conclusión**

Este informe consolida las bases técnicas, de seguridad, crecimiento y operación que requiere una red empresarial de nivel profesional. Cada dispositivo fue seleccionado por su funcionalidad y escalabilidad, cada política de seguridad por su adecuación a estándares reales, y cada recomendación futura por su enfoque modular y sostenible. Esta documentación habilita no solo la implementación inicial del sistema, sino también su evolución responsable y segura.