Informe Final – Nivel de red, enlace y físico

Redes Computacionales: Hito 3 - Actividad Grupal parte 2

Integrantes Grupo C:

Nicolás Alarcón

Byron Caices

Matías Cortés

Williams Jimenez

Bastián Olea

Reinaldo Pacheco

Stephan Paul

Benjamín Zuñiga

Docente:

Juan Ignacio Iturbe

Índice

1. Introducción

TechMove, empresa líder en logística y distribución de última milla, ha experimentado un proceso acelerado de transformación digital con el objetivo de optimizar sus operaciones y responder a las demandas crecientes del mercado. En una primera etapa, se implementó una red LAN básica en la sede central ubicada en Santiago, la cual permitió habilitar servicios esenciales como Web, Correo, DNS y FTP. No obstante, esta solución inicial, concebida para una rápida puesta en marcha, evidenció una serie de vulnerabilidades críticas: falta de segmentación de red, exposición directa de servicios sensibles a Internet, redes inalámbricas sin cifrado y ausencia de mecanismos de control de acceso.

Actualmente, TechMove se encuentra en plena expansión nacional, con nuevas sucursales en Valparaíso, Concepción y Antofagasta, y planes de abrir otras dos sedes en los próximos tres años. Esta fase requiere una infraestructura de red moderna, segura, escalable y resiliente, capaz de garantizar la continuidad operativa, el acceso seguro a los servicios, y la eficiencia en la administración de recursos.

1.2 Requerimientos de la red

Con base en el análisis de la situación actual y los objetivos estratégicos de la empresa, se establecen los siguientes requerimientos fundamentales para el rediseño de la red:

- Aplicar un esquema de direccionamiento eficiente mediante VLSM, considerando tanto la situación actual como el crecimiento proyectado (200%).
- Implementar VLANs por área funcional (Administración, Ingeniería, Operaciones y Gerencia) en cada sede.
- Garantizar la interconexión segura entre sedes mediante VPN IPsec.
- Establecer políticas de NAT y ACLs para el control de acceso y la protección de los servicios internos.
- Incorporar IPv6 en el datacenter de Santiago para servicios críticos, preparando la red para futuras migraciones tecnológicas.
- Reemplazar la red Wi-Fi abierta por una red inalámbrica segura con WPA2-PSK, segmentada por área.
- Implementar mecanismos de QoS para priorizar el tráfico esencial, especialmente en las áreas de Gerencia e Ingeniería.
- Asegurar la continuidad operativa de los servicios implementados en la primera fase (Web, FTP, Correo, DNS), respetando las nuevas políticas de segmentación y acceso.

Este informe constituye la documentación completa del desarrollo del proyecto de red, abordando desde el diseño conceptual hasta la implementación técnica y las decisiones justificadas que permiten resolver las deficiencias actuales, asegurar la operación continua de la empresa y habilitar su crecimiento futuro.

2. Objetivos

2.1 Objetivos generales

Diseñar una infraestructura de red corporativa que sea segura, escalable y segmentada, incorporando tecnologías avanzadas como VLSM, VLANs, NAT, ACLs, VPN, QoS e IPv6. Esta red debe asegurar una conectividad eficiente y protegida entre el datacenter y las distintas sucursales, permitiendo además una proyección sólida frente al crecimiento previsto de la empresa.

2.2 Objetivos específicos

1. Diseñar la topología de red completa y segmentarla mediante VLANs en todas las sucursales, finalizando antes del avance intermedio.

2. Implementar NAT y ACLs para controlar acceso interno y externo a los servicios críticos, completando configuraciones básicas para el avance intermedio.

3. Aplicar medidas de seguridad como ACLs, VPN IPsec y WPA2-PSK en cada sede, con configuración validada en simulación antes de la entrega final.

4. Configurar QoS en routers para optimizar el rendimiento de la red.

5. Diseñar el direccionamiento y estructura de red considerando un crecimiento proyectado del 200% y mantener operativos los servicios actuales con acceso segmentado para la entrega final.

2.3 Listado de Actividades

Este listado de actividades proviene del desglose de los objetivos específicos mencionados anteriormente, que a su vez están formados por objetivos más simples. Cada uno de estos objetivos simples fue dividido en tres actividades, con el propósito de ofrecer una visión más clara sobre las tareas que serán asignadas a los equipos de trabajo correspondientes.

La distribución de tareas a partir del objetivo de **diseño y segmentación de red** se pueden especificar como:

- ➔ Diseño de Subredes con VLSM
  - ◆ Dividir la red en subredes según la estrategia VLSM
  - ◆ Distribuir y marcar el esquema de las IP por cada subred
  - ◆ Documentar el esquema de subredes
- ➔ Segmentación de la Red con VLANs
  - ◆ Determinar el esquema de VLANs
  - ◆ Configurar la lógica detrás del VLANs y su asignación de puertos
  - ◆ Configurar y comprobar la correcta comunicación entre las diferentes VLANs
  - ◆ Documentar el diseño de VLANs

Ahora las tareas según el objetivo de **implementación de mecanismo de control de tráfico y acceso** puede ser desglosada como:

- ➔ NAT y ACLs
  - ◆ Configurar el tipo e interfaz que poseerán según el tipo de NAT requerido
  - ◆ Realizar un filtrado según IP y Protocolos según las necesidades del sistema
  - ◆ Comprobar la correcta integración de los 2 sin que interfieran en sus tareas
- ➔ Enrutamiento
  - ◆ Planificar y añadir los enrutamientos estáticos del sistema
  - ◆ Configurar un enrutamiento dinámico que se ajuste a las necesidades del sistema diseñado
  - ◆ Documentación de cómo se terminó de distribuir la red

Posteriormente en busca del **fortalecimiento de la seguridad de la red** las tareas son:

- ➔ Seguridad y Encriptación
  - ◆ Configuración de contraseñas de acceso seguro y firewalls del sistema
  - ◆ Implementar medidas de seguridad en los enlaces de conexión tales como VPN
  - ◆ Implementar cifrado del tráfico y encriptación de datos en reposo
- ➔ Seguridad Wi-Fi con WPA2
  - ◆ Configurar contraseñas y puntos de acceso a la red y seleccionar el modo seguro
  - ◆ Desactivar la difusión del SSID
  - ◆ Administrar protocolos de cambio de contraseñas

Pasando al objetivo de **optimizar el rendimiento de la red** la tarea es:

- ➔ Optimización del Tráfico con QoS
  - ◆ Diseño de la Estrategia de QoS para la optimización
  - ◆ Implementación Técnica de la estrategia diseñada
  - ◆ Pruebas y Validación de la configuración

Finalmente, para el último objetivo específico de **garantizar la escalabilidad y continuidad operativa de la red** se precisan:

- ➔ Proyección de Crecimiento y Escalabilidad
  - ◆ Estimación de crecimiento futuro y tiempo de vida de red
  - ◆ Planificar estrategia de direccionamiento y lógica a largo plazo
  - ◆ Documentación de la estrategia para su posterior implementación
- ➔ Continuidad operativa de servicios
  - ◆ Análisis de riesgos asociados a la red o su mal funcionamiento
  - ◆ Diseño de estrategias de continuidad operativas y protocolos propios en caso de ser necesario
  - ◆ Planificación y documentación de planes de respaldo a problemas comunes en redes

3. Contraste de lo definido en el anteproyecto con lo finalmente realizado

3.1 Roles y responsabilidades

A continuación, se presentan los roles de cada integrante del grupo, junto con la descripción y función asociada cada uno, estos roles fueron utilizados para distribuir las actividades en el cronograma y la matriz RACI. Posterior a la presente tabla se encuentra otra tabla con los aportes y brechas de cada integrante para contrastar las responsabilidades planificadas con las tareas que efectivamente fueron realizadas por cada uno.

Rol	Descripción de responsabilidades y funciones asociadas al rol	Integrante
Project Manager	• Centralizar la planificación general del proyecto. • Asegurarse de que cada integrante tenga claras sus tareas, plazos y responsabilidades. • Preparar y supervisar la Carta Gantt • Coordinar las reuniones del equipo y resolver conflictos	• Stephan Paul
Network Designer	• Elaboración de topología y conectividad entre sedes • Segmentación de red inicial en subredes • Configuración de subredes según VLSM • Comunicación entre VLANs	• Byron Caices • Matías Cortés • Benjamin Zuñiga
Documentation Lead	• Elaborar y mantener registros detallados de la configuración de dispositivos, topologías de red y comandos utilizados en cada laboratorio • Redactar informes técnicos que incluyan objetivos, procedimientos, resultados y análisis de las prácticas realizadas • Asegurar que la documentación cumpla con estándares de claridad, precisión y estructura • Incluir diagramas, capturas de pantalla y descripciones que faciliten la interpretación de la configuración en Cisco Packet Tracer	• Williams jimenez
Network Security	• Diseñar e implementar NAT • Configurar ACLs en routers y switches • Establecer y configurar túneles	• Reinaldo Pacheco • Bastián Olea Díaz • Nicolás Alarcón

Rol	Descripción de responsabilidades y funciones asociadas al rol	Integrante
	VPN IPSec entre sucursales y centro de datos	

3.2 Aportes y brechas de cada integrante

Integrante	Rol	Aportes	Brechas
Stephan Paul	Project Manager	Coordinación general del equipo, seguimiento de planificación, revisión de cronograma y consolidación final del proyecto.	Faltó una supervisión más estricta sobre el cumplimiento de horas hombre planificadas. Faltó priorizar la integración de QoS desde etapas tempranas.
Reinaldo Pacheco	Network Security	Diseñó e implementó las configuraciones de NAT en los routers de borde. Participó en la definición de reglas ACL para permitir y restringir el tráfico entre sedes.	La coexistencia de VPN y NAT dificulto la definición de ACL para restringir el tráfico.
Byron Caices	Network Designer	Participó en la elaboración de la topología lógica de red y en la asignación de subredes con VLSM. Encargado de configurar VLANs en switches de cada sede.	Se dificulta la asignación eficiente de subredes por falta de coordinación en los cambios.
Nicolás Alarcón	Network Security	Revisó y ajustó las ACL en routers y switches para QoS. Coordinó pruebas	No se actualizaron reglas ACL para QoS tras los cambios en la red.

		de validación de seguridad interna.	
Matías Cortés	Network Designer	Implementó la conectividad entre sedes en Packet Tracer. Apoyó en la configuración de interfaces VLAN y su ruteo en cada router.	La comunicación inter-sede tuvo que realizarse repetidas veces tras las dificultades en implementar las otras tecnologías.
Williams Jimenez	Documentation Lead	Mantuvo registros detallados de configuraciones y topologías. Redactó informes con comandos, capturas y descripciones técnicas de la red.	Algunos documentos se actualizaron a contratiempo tras cambios de última hora en la red.
Bastián Olea	Network Security	Configuró los túneles VPN IPSec entre las sedes y verificó su operación. Apoyó en la documentación de políticas de seguridad y realizó pruebas de conectividad segura.	No se realizó un monitoreo a tiempo de las VPN, lo que retrasó la detección de errores.
Benjamín Zuñiga	Network Designer	Apoyó en la segmentación de red para cada sede y revisión de subredes. Apoyó de manera lateral en la configuración de VPN, NAT y ACL.	El desarrollo tardío de las ACL faltantes fue causante del retraso en la detección de ineficiencias en VLSM.

3.3 Identificación de problemáticas y cómo se solucionaron

A lo largo del desarrollo del proyecto se presentaron diversas dificultades y obstáculos vinculados principalmente con desajustes, variaciones en la realización de tareas y modificaciones vinculadas a la retroalimentación obtenida en las fases intermedias. Estas dificultades, a pesar de no tener un efecto significativo en el progreso del proyecto,

impactaron en lo previsto en el borrador del proyecto y demandaron una adaptación del equipo. Las siguientes son algunas dificultades que aparecieron durante el desarrollo del proyecto:

3.4 Asignación de Tiempos y Esfuerzos (HH) y horas efectivas

Actividad	Responsable	Horas por responsable (HH)	HH efectivamente utilizadas
Diseño de subredes con VLSM	Project Manager Network Designer	4	5
Segmentación de la red con VLANs	Network Designer	7	15
Configuración de NAT y VPN para acceso	Network Security	10	15
Configurar protocolo de enrutamiento en la red	Network Designer Network Security	7	7
Configurar ACLs en routers y switches para controlar el acceso entre las VLANs	Network Security	8	3
Configurar redes inalámbricas seguras con WPA2-PSK	Network Security	6	2
Configuración QoS en routers	Network Security	8	/
Diseño de direccionamiento y estructura de red	Network Designer Documentation Lead	3	4
Documentación de esquemas, diseños y protocolos	Documentation Lead	8	8

3.5 Cambios Carta Gantt

A continuación, se presentará un extracto de la carta Gantt. El documento completo se encuentra en *Anexo 2*, en la sección de Anexos.

Actividades	Roles Encargados	Fecha Inicio	Fecha Fin	Semana 1	Semana 2	Semana 3	Semana 4	Semana 5	Semana 6	Semana 7
Hito 1: Anteproyecto										
Definir objetivo General y Específicos	Documentation Lead	05/05/2025	11/05/2025							
Listar Actividades por Objetivo Específico	Documentation Lead	05/05/2025	11/05/2025							
Definir roles de cada integrante	Project Manager	05/05/2025	11/05/2025							
Realizar Matriz RACI	Project Manager	12/05/2025	14/05/2025							
Documentar hitos de Entrega	Documentation Lead	05/05/2025	06/05/2025							
Definir esfuerzo Requerido (HH)	Documentation Lead	12/05/2025	14/05/2025							
Construir carta Gantt	Project Manager	12/05/2025	14/05/2025							
Mecanismo interno de solución a problemáticas grupales	Documentation Lead	05/05/2025	06/05/2025							
Realizar presentación del informe realizado	Project Manager	12/05/2025	14/05/2025							
Hito 2: Avance Intermedio										
Diseño de subredes con VLSM	Network Designer	16/05/2025	22/05/2025							
Segmentación de red con VLANs	Network Designer	23/05/2025	29/05/2025							
Configuraciones iniciales de NAT, ACLs o VPN	Network Security	23/05/2025	29/05/2025							
Desarrollar simulaciones parciales en Packet Tracer	Network Designer	30/05/2025	05/06/2025							
Resumir el anteproyecto para la presentación	Documentation Lead	16/05/2025	22/05/2025							
Incluir avances técnicos en la presentación e informe	Network Designer	06/06/2025	08/06/2025							
Incluir evidencia de simulaciones en la presentación e informe	Project Manager	06/06/2025	08/06/2025							
Hito 3: Entrega final y presentación										
Finalizar y probar subredes con VLSM	Network Designer	10/06/2025	20/06/2025							
Finalizar y probar VLANs	Network Designer	10/06/2025	20/06/2025							
Finalizar y probar NAT, ACLs, VPN IPsec	Network Security	10/06/2025	20/06/2025							
Finalizar y probar Red inalámbrica WPA2-PSK segmentada	Network Security	10/06/2025	20/06/2025							
Finalizar y probar Enrutamiento	Network Designer	10/06/2025	20/06/2025							
Finalizar y probar QoS para tráfico crítico	Network Security	10/06/2025	20/06/2025							
Probar que los servicios Web, FTP, Correo y DNS estén activos	Network Security	10/06/2025	20/06/2025							
Validar escalabilidad para crecimiento proyectado	Project Manager	17/06/2025	20/06/2025							
Realizar simulación funcional completa	Network Security	17/06/2025	20/06/2025							
Actualizar presentación con la síntesis del proyecto completo	Project Manager	17/06/2025	22/06/2025							
Realizar informe con la síntesis del proyecto completo	Documentation Lead	17/06/2025	22/06/2025							

Figura 1: Carta Gantt de actividades

3.6 Matriz RACI

Finalmente, se presenta un extracto de lo que es la matriz RACI, la cual no recibió modificaciones durante el proyecto. El documento completo se encuentra en *Anexo 1*, en la sección de Anexos.

Tarea - Anteproyecto related

	Nicolás Alarcón	Byron Caices	Matías Cortés	Williams Jimenez	Bastián Olea	Reinaldo Pacheco	Stephan Paul	Benjamín Zuñiga
Redacción de Introducción	I	I	I	I	R	I	A	I
Definición de Objetivos (General y Específicos)	I	I	I	A	A	I	R	I
Desglose de Actividades y Planificación	I	I	I	R	I	I	A	I
Estimación de Tiempos y Esfuerzos	I	I	C	R	A	I	A	I
Elaboración de Cronograma y Hitos	I	I	I	A	I	I	R	I
Definición de Roles	I	I	I	I	I	R	A	I
Elaboración Matriz RACI	C	R	C	C	C	C	A	C
Redacción de Mecanismo de Solución de Conflictos	I	I	I	I	C	I	A	R
Redacción de Conclusiones	R	I	C	I	R	I	A	I

Tareas - Diseño de direccionamiento IP (VLSM)

	Nicolás Alarcón	Byron Caices	Matías Cortés	Williams Jimenez	Bastián Olea	Reinaldo Pacheco	Stephan Paul	Benjamín Zuñiga
Dividir red en subredes VLSM	C	R	R	I	C	C	A	R
Asignar rangos IP por subred	C	R	R	I	C	C	A	R
Documentar esquema de subredes	C	R	R	I	C	C	A	R

Tareas - Segmentación física y lógica (VLANs)

	Nicolás Alarcón	Byron Caices	Matías Cortés	Williams Jimenez	Bastián Olea	Reinaldo Pacheco	Stephan Paul	Benjamín Zuñiga
Definir esquema de VLANs	C	R	R	I	C	C	A	R
Configurar puertos y asignación de VLANs	C	R	R	I	C	C	A	R
Validar inter-VLAN routing	C	R	R	I	C	C	A	R

Figura 2: Matriz RACI

4. Marco Teórico

4.1 VLSM (Variable Length Subnet Mask)

VLSM es una técnica avanzada de direccionamiento IP que permite dividir una red principal en subredes de diferentes tamaños, adaptándose a las necesidades específicas de cada segmento de la red. Con VLSM, se puede tomar un bloque de direcciones IP y subdividirlo varias veces, asignando máscaras más cortas (subredes grandes) donde se necesitan más hosts y máscaras más largas (subredes pequeñas) donde se requieren menos hosts.

VLSM es ampliamente utilizado en redes empresariales y en el diseño jerárquico de redes, como campus universitarios, grandes oficinas o ISPs, donde diferentes departamentos o regiones requieren diferentes cantidades de hosts.

4.2 Direccionamiento IP (IPv4/IPv6)

El direccionamiento IP es el mecanismo que permite identificar de manera única a cada dispositivo conectado a una red, ya sea una red local o Internet. Hay dos versiones principales de direcciones IP en uso: IPv4 e IPv6.

IPv4 (Internet Protocol versión 4) utiliza direcciones de 32 bits, representadas habitualmente en notación decimal separada por puntos (ejemplo: 192.168.1.1).

IPv6 (Internet Protocol version 6) es la evolución de IPv4 y utiliza direcciones de 128 bits, escritas en notación hexadecimal separada por dos puntos (ejemplo: 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

4.3 VLANs (Virtual LANs)

VLAN es una tecnología que permite segmentar una red física en varias redes lógicas independientes, incluso si los dispositivos están conectados al mismo switch físico. Agrupa un conjunto de dispositivos dentro de la misma red física en una sola red lógica, como si estuvieran en una red física separada. Esto se logra mediante la configuración de los switches, asignando puertos a diferentes VLANs, lo que aísla el tráfico entre ellas.

4.4 NAT (Network Address Translation)

Nat es una técnica implementada en redes para modificar las direcciones IP de los paquetes enviados a través de un router. Su función principal es permitir que múltiples dispositivos dentro de una red local logren utilizar una única dirección IP pública para comunicarse con redes externas, como Internet. De esta manera, NAT proporciona tanto ahorro de direcciones IPv4 como una capa adicional de seguridad al ocultar la estructura interna de la red.

Existen diferentes tipos de NAT:

- **NAT Estática:** Consiste en asignar de forma permanente una dirección IP privada a una dirección IP pública específica. Es una relación uno a uno y se utiliza cuando se

necesita que un dispositivo interno siempre sea accesible desde el exterior con la misma dirección IP pública.

- **NAT Dinámica:** Asigna direcciones IP públicas a dispositivos internos de manera automática y temporal, cada dispositivo recibe una IP pública diferente tomada de un pool de direcciones disponibles.
- **PAT:** Conocido también como "NAT por sobrecarga", no solo traduce direcciones IP, sino que también utiliza los números de puerto para diferenciar múltiples conexiones salientes desde una sola dirección IP pública. Es decir, varios dispositivos de la red pueden compartir la misma IP pública, pero cada conexión se identifica de manera única mediante el puerto de origen.

4.5 ACL (Access Control Lists)

Una Lista de Control de Acceso (ACL) es un conjunto de reglas que se aplican a las interfaces de un router o firewall para controlar el tráfico de red. Su función principal es filtrar los paquetes que entran o salen de la red, permitiendo o denegando su paso según criterios específicos como la dirección IP de origen, la dirección IP de destino, el tipo de protocolo y número de puerto

Existen distintos tipos de ACL:

- **ACL Estándar:** Filtran el tráfico basándose únicamente en la dirección IP de origen del paquete.
- **ACL Extendida:** Pueden filtrar el tráfico basándose en múltiples criterios a la vez:
  - Dirección IP de origen y destino.
  - Protocolo
  - Puertos de origen y destino
- **ACL Nombradas:** Funcionalmente, son iguales que las estándar o extendidas, pero en lugar de identificarse con un número, se les asigna un nombre descriptivo

4.6 Protocolos de Enrutamiento

Según Sepúlveda (2025), un protocolo de enrutamiento es un conjunto de reglas que permiten a los dispositivos de red determinar cómo deben enviar los paquetes de datos hacia su destino. Existen dos enfoques principales: el enrutamiento estático y el enrutamiento dinámico. El enrutamiento estático requiere que un administrador configure manualmente las rutas en cada dispositivo, lo que puede funcionar bien en redes pequeñas, pero se vuelve difícil de mantener y propenso a errores en redes grandes. En contraste, el enrutamiento dinámico utiliza algoritmos y mecanismos de intercambio de información entre dispositivos para calcular automáticamente las rutas más eficientes, lo que lo hace más escalable, flexible y resistente a fallos.

En este último hay 3 protocolos de enrutamiento más destacados, que son:

1. **OSPF (Open Shortest Path First):** Protocolo de enrutamiento de estado de enlace que utiliza el algoritmo de Dijkstra para calcular las rutas más cortas. Es ampliamente utilizado en redes empresariales.

2. **RIP (Routing Information Protocol):** Protocolo de enrutamiento de vector de distancia que basa sus decisiones en el número de saltos entre dispositivos. Aunque es un protocolo antiguo, aún se emplea en redes pequeñas y simples.
3. **EIGRP (Enhanced Interior Gateway Routing Protocol):** Protocolo propietario de Cisco, basado en estado de enlace, que utiliza el algoritmo DUAL (Diffusing Update Algorithm) para determinar las rutas más eficientes en redes empresariales.

(Sepúlveda, 2025)

4.7 VPN IPsec

Una VPN (Red Privada Virtual/ Virtual Private Network) crea un "túnel" por donde puede enviar datos de manera segura con herramientas de cifrado y autenticación. Las empresas suelen usar conexiones VPN porque son una forma más segura de ayudar a los empleados a acceder por vía remota a las redes empresariales privadas, incluso cuando trabajan fuera de la oficina. La VPN permite que los dispositivos remotos, como las computadoras portátiles, operen como si estuvieran en la misma red local. Muchos dispositivos de enrutamiento por VPN pueden admitir decenas de túneles al mismo tiempo, con herramientas de configuración simples, lo que garantiza que todos los trabajadores tengan acceso a los datos empresariales, estén donde estén (Cisco, 2025).

En su forma más básica, las VPN protegen a las empresas, a los usuarios y a sus datos confidenciales. A continuación, se presentan otros motivos por los que una empresa podría beneficiarse con una VPN:

- Comodidad: Las VPN son una manera cómoda de proporcionar a los empleados, incluidos los trabajadores remotos, acceso simple a la red empresarial sin que tengan que estar presentes físicamente, al tiempo que se preserva la seguridad de las redes privadas y los recursos empresariales (Cisco, 2025).
- Mayor seguridad: Las comunicaciones con una conexión VPN proporcionan un mayor nivel de seguridad en comparación con otros métodos de comunicaciones remotas, lo que mantiene las redes privadas cerradas a las personas sin acceso autorizado. Las ubicaciones geográficas reales de los usuarios se protegen y no se exponen a las redes públicas o compartidas como Internet (Cisco, 2025).
- Administración más simple: Las herramientas de software de VPN flexibles permiten agregar nuevos usuarios o grupos de usuarios a las redes de manera simple. Esto resulta conveniente para las empresas que crecen más rápido que sus presupuestos (Cisco, 2025).

Los protocolos de VPN determinan cómo se enrutan los datos entre la computadora y el servidor de VPN. Algunos protocolos aumentan la velocidad, mientras que otros mejoran la privacidad y la seguridad de los datos.

- OpenVPN: Este protocolo es de código abierto, lo que significa que se puede ver el código. OpenVPN también se está convirtiendo rápidamente en un estándar de la industria (Cisco, 2025).
- L2TP/IPSec: El protocolo de túnel de capa 2 es otro protocolo común. Tiene sólidas medidas de seguridad y suele combinarse con el protocolo IPSec, que autentica y cifra los paquetes de datos que se envían por la VPN (Cisco, 2025).
- SSTP: El protocolo de túnel de sockets seguros (SSTP, Secure Socket Tunneling Protocol) está totalmente integrado al sistema operativo de Microsoft (Cisco, 2025).

- PPTP: El protocolo de túnel de punto a punto (PPTP, Point-to-Point Tunneling Protocol) es uno de los protocolos de VPN más antiguos. No obstante, se está empezando a usar menos desde que existen protocolos más rápidos y seguros (Cisco, 2025).

4.8 QoS (Quality of Service)

Es un conjunto de tecnologías y mecanismos diseñados para gestionar el tráfico de red con el objetivo de garantizar un cierto nivel de rendimiento para aplicaciones críticas. Sin QoS todo el tráfico se trata por igual por lo que si se configura, se prioriza el tráfico importante para asegurar baja latencia y fiabilidad en las aplicaciones críticas incluso cuando la red se encuentre congestionada. Una correcta implementación de QoS puede salvaguardar el rendimiento de la red en escenarios de estrés por transferencia.

Para lograr esto, es importante la política de clasificación de tráfico. En el caso de la presente actividad, se tomó toda transferencia de tipo HTTP/HTTPS como tráfico crítico con prioridad ante un escenario de tráfico excesivo.

Un concepto importante para QoS es el “queueing”. Esto significa que cuando el tráfico es alto, los paquetes se pueden colocar en colas según la política definida. Por ejemplo, HTTP/HTTPS como prioridad, mientras que el resto de tráfico (por ejemplo, FTP), caen en el “default” o “common” y se les asigna un lugar menos privilegiado en la cola.

La implementación de QoS se vale también de la ACL creada para tráfico web. De esta forma, se puede identificar y agrupar el tráfico en distintas clases. Luego, entra en juego la política de asignación para el tráfico, que genera las colas y sus características.

El correcto funcionamiento de QoS es fundamental para las instancias de alto estrés en el tráfico dentro de la red, dado que previene el colapso de las mismas.

4.9 Seguridad Inalámbrica (WPA2-PSK)

El protocolo WPA2-PSK es un estándar de seguridad diseñado para proteger redes inalámbricas. Su principal objetivo es asegurar la confidencialidad e integridad de los datos transmitidos a través de una red Wi-Fi.

- Usa Cifrado WAP2 a través del algoritmo de cifrado AES (Advanced Encryption Standard) codificando la información transmitida para que no sea legible por quienes capturen el tráfico.
- Usa autenticación PSK o WPA-Personal el cual da acceso a la red en una única contraseña o frase el cual se configura en el router y se comparte con los dispositivos autorizados para que se puedan conectar.

4.10 Alta Disponibilidad y Continuidad Operativa

La Alta Disponibilidad es la estrategia para maximizar el tiempo de actividad de la red. Se logra con redundancia de los equipos como routers y switches eliminando puntos de fallo con el objetivo de prevenir interrupciones al sistema.

La Continuidad Operativa es un plan que engloba la alta disponibilidad, debido a que su objetivo es asegurar las funciones críticas de una empresa y que sigan durante cualquier tipo de contingencia como cortes de luz, desastre natural u otro inconveniente. La continuidad operativa se logra a través de la alta disponibilidad de los servicios.

4.11 Escalabilidad en Redes Empresariales

Es la capacidad de una infraestructura de red para crecer y adaptarse a un aumento en la demanda. Para este ejemplo, la empresa tiene un aumento de usuarios y dispositivos, por lo que se deben implementar tecnologías para segmentar la red y mantener el rendimiento de los sistemas. Implementando tecnologías que aseguren que el crecimiento no impacte negativamente la velocidad y la seguridad de la red.

5. Documentación Técnica del Diseño e Implementación de la Red

5.1 Diseño de Subredes

El diseño de nuestra simulación busca replicar de la manera más fiel y común posible cómo una empresa con múltiples sucursales en Chile se interconecta de forma segura y costo-efectiva utilizando Internet como medio de transporte.

Aquí desglosamos el porqué de cada elección:

1. ¿Por qué esta Topología? (Hub-and-Spoke con ISP Central)

- **Elección de la Topología:** Hemos simulado una topología Hub-and-Spoke, donde cada sede (STGO, VAL, CON, ANT) es un "spoke" (radio) que se conecta a un punto central.
- **Rol del Router ISP:** El router central **NO es parte de nuestra empresa**. Su función es simular la **infraestructura completa de un Proveedor de Servicios de Internet (ISP)**, como Movistar, Entel o Claro en Chile. Es una "nube" pública y no confiable que simplemente sabe cómo enrutar tráfico entre las direcciones IP públicas de nuestras sedes.
- **Justificación:** Este modelo es el más realista. Las empresas no se conectan directamente entre sí; contratan un servicio de acceso a Internet en cada una de sus ubicaciones, y es el proveedor el encargado de interconectar a través de su red global.

2. ¿Qué Simula la Conexión "Serial DTE" y las "IPs Públicas"?

- **El "Cable Serial":** En nuestra simulación en Packet Tracer, el cable serial es una forma conveniente de crear un enlace punto a punto. En el mundo real, este cable **NO sería un cable serial físico**. Representa el **"Enlace de Acceso a Internet"** o la **"Última Milla"** que el ISP instala en cada una de nuestras oficinas.
    - **Equivalente Real:** Típicamente, sería una conexión de **Fibra Óptica Dedicada**, que es el estándar para empresas que necesitan alta velocidad y fiabilidad.
- **Las "IPs Públicas":** La red en ese enlace (ej. `198.28.4.4/30`) simula el bloque de direcciones IP públicas que el ISP nos asigna. Estas IPs son únicas en todo el mundo y son las que nos permiten tener presencia en Internet.

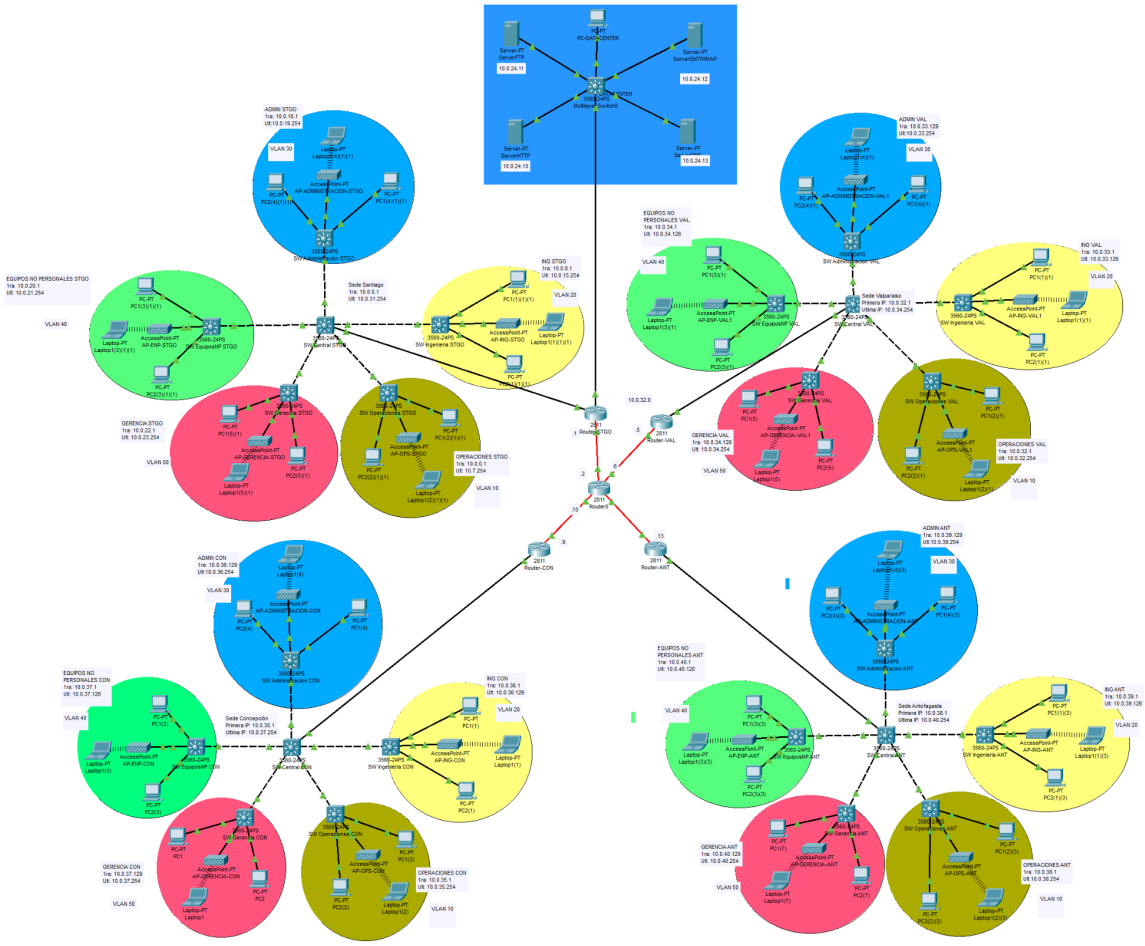


Figura 3: Topología de la red

5.2 Asignación de Direcciones IP

Rangos de IP por sede calculados con VLSM:

- Santiago
  - Red: 10.0.0.0
  - Máscara: /19 (255.255.224.0)
  - Rango utilizable: 10.0.0.1 – 10.0.31.254
  - Broadcast: 10.0.31.255
- Valparaíso
  - Red: 10.0.32.0
  - Máscara: /23 (255.255.254.0)
  - Rango utilizable: 10.0.32.1 – 10.0.33.254
  - Broadcast: 10.0.33.255
- Concepción
  - Red: 10.0.34.0
  - Máscara: /23 (255.255.254.0)
  - Rango utilizable: 10.0.34.1 – 10.0.35.254
  - Broadcast: 10.0.35.255
- Antofagasta
  - Red: 10.0.36.0
  - Máscara: /23 (255.255.254.0)
  - Rango utilizable: 10.0.36.1 – 10.0.37.254
  - Broadcast: 10.0.37.255

5.3 Protocolos de Enrutamiento

El protocolo de enrutamiento implementado fue OSPF (Open Shortest Path First), una opción ideal para redes con una gran cantidad de usuarios y dispositivos. A diferencia del enrutamiento estático, que requiere la configuración manual de cada ruta en los routers, OSPF funciona de manera dinámica, lo que facilita la administración y permite que la red se adapte automáticamente a los cambios en la topología, algo fundamental en redes grandes y complejas.

Comparado con protocolos tradicionales como RIP, que está limitado a un máximo de 15 saltos y presenta una convergencia lenta, OSPF no tiene tales restricciones y ofrece una convergencia mucho más rápida, lo que reduce el tiempo en que la red permanece inestable tras un cambio o fallo. Además, OSPF utiliza métricas basadas en el costo (por ejemplo, ancho de banda) para seleccionar rutas óptimas, a diferencia de RIP, que basa sus decisiones simplemente en la cantidad de saltos.

Respecto a EIGRP, ambos protocolos son capaces de converger rápidamente y soportan VLSM, pero OSPF se diferencia por su arquitectura jerárquica basada en áreas, lo que permite segmentar la red y mejorar la escalabilidad y estabilidad en entornos de gran

tamaño. Además, OSPF utiliza el algoritmo de Dijkstra para calcular rutas libres de bucles, garantizando una topología coherente y eficiente.

En resumen, OSPF es una solución escalable, dinámica y estandarizada que supera las limitaciones del enrutamiento estático y de protocolos más simples, y ofrece ventajas estructurales y de diseño frente a otros protocolos dinámicos, haciendo que sea especialmente adecuado para redes empresariales grandes.

5.4 Segmentación

Sede	Área	Subred	Máscara	Primera IP	Última IP
Santiago	Operaciones	10.0.0.0/21	255.255.248.0	10.0.0.1	10.0.7.254
	Ingeniería	10.0.8.0/21	255.255.248.0	10.0.8.1	10.0.15.254
	Administración	10.0.16.0/22	255.255.252.0	10.0.16.1	10.0.19.254
	Equipos NP	10.0.20.0/23	255.255.254.0	10.0.20.1	10.0.21.254
	Gerencia	10.0.22.0/23	255.255.254.0	10.0.22.1	10.0.23.254
Valparaíso	Operaciones	10.0.32.0/24	255.255.255.0	10.0.32.1	10.0.32.254
	Ingeniería	10.0.33.0/25	255.255.255.128	10.0.33.1	10.0.33.126
	Administración	10.0.33.128/25	255.255.255.128	10.0.33.129	10.0.33.254
	Equipos NP	10.0.34.0/25	255.255.255.128	10.0.34.1	10.0.34.126
	Gerencia	10.0.34.128/25	255.255.255.128	10.0.34.129	10.0.34.254

Sede	Área	Subred	Máscara	Primera IP	Última IP
Concepción	Operaciones	10.0.35.0/24	255.255.255.0	10.0.35.1	10.0.35.254
	Ingeniería	10.0.36.0/25	255.255.255.128	10.0.36.1	10.0.36.126
	Administración	10.0.36.128/25	255.255.255.128	10.0.36.129	10.0.36.254
	Equipos NP	10.0.37.0/25	255.255.255.128	10.0.37.1	10.0.37.126
	Gerencia	10.0.37.128/25	255.255.255.128	10.0.37.129	10.0.37.254
Antofagasta	Operaciones	10.0.38.0/24	255.255.255.0	10.0.38.1	10.0.38.254
	Ingeniería	10.0.39.0/25	255.255.255.128	10.0.39.1	10.0.39.126
	Administración	10.0.39.128/25	255.255.255.128	10.0.39.129	10.0.39.254
	Equipos NP	10.0.40.0/25	255.255.255.128	10.0.40.1	10.0.40.126
	Gerencia	10.0.40.128/25	255.255.255.128	10.0.40.129	10.0.40.254

5.5 Medidas de Seguridad y Alta Disponibilidad

Para garantizar la seguridad y disponibilidad de la red, se han implementado varias medidas prácticas que protegen la infraestructura y aseguran la continuidad del servicio.

En nuestra red, la configuración de NAT se diseñó para que el tráfico interno entre sedes (por ejemplo, entre Valparaíso y Santiago) no sea procesado ni modificado por NAT. Esto se logra mediante una Access-List 100 que bloquea la traducción de direcciones para el tráfico interno, permitiendo que dicho tráfico se dirija directamente a través del túnel VPN seguro. Así, el tráfico interno no se expone ni se traduce a direcciones públicas, garantizando su paso por el canal cifrado de la VPN. Solo el tráfico destinado a redes externas es traducido mediante NAT, asegurando el acceso a Internet con una dirección pública válida.

Las listas de control de acceso (ACL) están configuradas para filtrar y controlar el tráfico de manera granular, permitiendo o denegando el acceso a recursos específicos según criterios como origen, destino o tipo de protocolo. Estas reglas evitan accesos no autorizados y protegen segmentos sensibles de la red ante posibles amenazas.

Para proteger la comunicación entre las diferentes sedes y usuarios remotos, se han implementado túneles VPN que cifran todo el tráfico que atraviesa redes públicas, asegurando la confidencialidad e integridad de los datos en tránsito. Una VPN crea un “túnel” seguro mediante el uso de mecanismos de cifrado y autenticación, permitiendo que los datos viajen de forma segura a través de redes no confiables. En nuestra red, se crean túneles permanentes entre todas las sedes, lo que permite una comunicación directa y protegida entre ellas, además de garantizar el acceso seguro a los servicios del datacenter central. De esta manera, los datos sensibles viajan cifrados, resguardando la información crítica de posibles interceptaciones o ataques durante su transmisión.

Finalmente, para asegurar la alta disponibilidad, la red se apoya en el protocolo de enrutamiento dinámico OSPF, que permite una rápida convergencia y recuperación ante fallos en la topología, minimizando el tiempo de inactividad. Aunque actualmente la red no cuenta con una redundancia física completamente implementada en enlaces y dispositivos clave, la arquitectura está diseñada de manera que facilita futuras mejoras en este aspecto para fortalecer aún más la continuidad del servicio y la confiabilidad de la infraestructura.

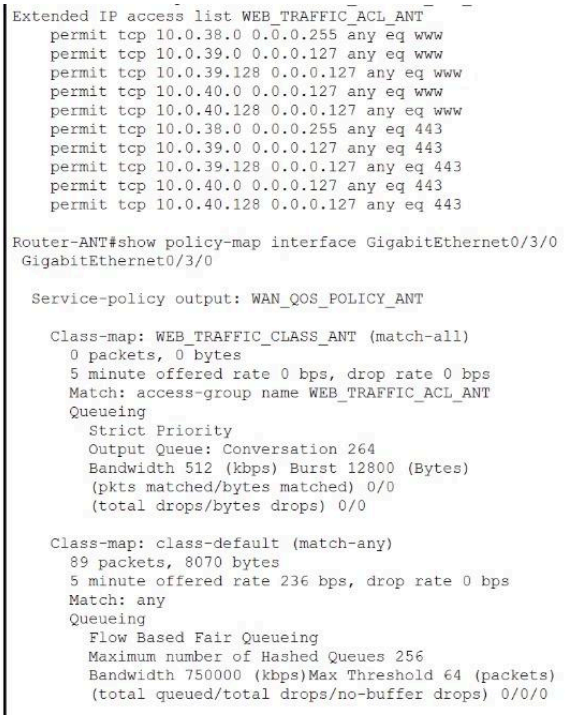
5.6 Optimización del Tráfico

Con el objetivo de garantizar un desempeño óptimo en la transmisión de datos críticos, se implementó una política de Quality of Service (QoS) sobre la interfaz GigabitEthernet0/3/0 del router principal. La política, denominada WAN_QOS_POLICY_ANT, utiliza un enfoque de priorización estricto para el tráfico web proveniente de subredes específicas, identificadas mediante la lisa de acceso extendida WEB_TRAFFIC_ACL_ANT.

Se configuró una política de calidad de servicio para otorgar prioridad al tráfico web, específicamente a las conexiones establecidas mediante los protocolos HTTP y HTTPS. Este tipo de tráfico fue identificado mediante una lista de control de acceso y clasificado en una clase de tráfico con prioridad estricta, a la cual se le asignó un ancho de banda reservado y una capacidad de ráfaga. Esta medida asegura que las comunicaciones web

mantengan un desempeño constante incluso en condiciones de alta demanda evitando retrasos causados por otros tipos de tráfico menos críticos.

Esta configuración permite asegurar que el tráfico web esencial mantenga un buen desempeño incluso en situaciones de congestión, al mismo tiempo que el resto del tráfico se distribuye de forma equitativa mediante un mecanismo de cola justa, optimizando el uso del ancho de banda. Las configuraciones descritas se pueden observar en la figura correspondiente.



```
Extended IP access list WEB_TRAFFIC_ACL_ANT
    permit tcp 10.0.38.0 0.0.0.255 any eq www
    permit tcp 10.0.39.0 0.0.0.127 any eq www
    permit tcp 10.0.39.128 0.0.0.127 any eq www
    permit tcp 10.0.40.0 0.0.0.127 any eq www
    permit tcp 10.0.40.128 0.0.0.127 any eq www
    permit tcp 10.0.38.0 0.0.0.255 any eq 443
    permit tcp 10.0.39.0 0.0.0.127 any eq 443
    permit tcp 10.0.39.128 0.0.0.127 any eq 443
    permit tcp 10.0.40.0 0.0.0.127 any eq 443
    permit tcp 10.0.40.128 0.0.0.127 any eq 443

Router-ANT#show policy-map interface GigabitEthernet0/3/0
 GigabitEthernet0/3/0

  Service-policy output: WAN_QOS_POLICY_ANT

    Class-map: WEB_TRAFFIC_CLASS_ANT (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: access-group name WEB_TRAFFIC_ACL_ANT
      Queueing
        Strict Priority
        Output Queue: Conversation 264
        Bandwidth 512 (kbps) Burst 12800 (Bytes)
        (pkts matched/bytes matched) 0/0
        (total drops/bytes drops) 0/0

    Class-map: class-default (match-any)
      89 packets, 8070 bytes
      5 minute offered rate 236 bps, drop rate 0 bps
      Match: any
      Queueing
        Flow Based Fair Queueing
        Maximum number of Hashed Queues 256
        Bandwidth 750000 (kbps)Max Threshold 64 (packets)
        (total queued/total drops/no-buffer drops) 0/0/0
```

Figura 4: Terminal Router Antofagasta - Configuraciones QOS

5.7 Seguridad Inalámbrica (WPA2-PSK por área)

En la red inalámbrica, se ha habilitado la autenticación y cifrado mediante WPA2-PSK, garantizando que solo dispositivos autorizados puedan conectarse y que la información transmitida se mantenga protegida contra accesos no autorizados. Este protocolo de seguridad está diseñado específicamente para redes Wi-Fi, y su objetivo principal es asegurar la confidencialidad e integridad de los datos transmitidos a través del canal inalámbrico. Gracias a su mecanismo de cifrado robusto y a la clave precompartida, se limita el acceso únicamente a dispositivos confiables y se reduce significativamente el riesgo de ataques externos sobre la red inalámbrica.

5.8 Escalabilidad y Proyección de Crecimiento

Gracias al uso de tecnologías bien configuradas, como el protocolo de enrutamiento OSPF y el direccionamiento mediante VLSM (Variable Length Subnet Masking), se logró implementar una red no sólo confiable, sino también escalable. Esto significa que la red puede adaptarse fácilmente al crecimiento futuro sin necesidad de realizar modificaciones estructurales importantes.

El diseño actual permite incorporar una mayor cantidad de usuarios y dispositivos que los inicialmente previstos, lo cual extiende la vida útil de la infraestructura y reduce los costos asociados a futuras ampliaciones. Además, esta capacidad de crecimiento facilita la expansión de la empresa, ya que no es necesario rediseñar la red cada vez que se integren nuevas sedes o se incremente el personal.

En conjunto, estas decisiones de diseño no solo optimizan la eficiencia de la red, sino que también mejoran la calidad del servicio que esta proporciona, ofreciendo una base sólida y flexible para el desarrollo continuo de la organización.

5.9 Continuidad Operativa de Servicios

De acuerdo con lo expuesto en los apartados anteriores, se puede concluir que la red está diseñada para mantenerse operativa de forma estable y continua, siempre que no se produzcan cambios sustanciales en las políticas internas de la empresa o en la legislación vigente. Sin embargo, excluyendo estos escenarios poco probables, la red garantiza un servicio de conexión confiable entre las distintas sucursales, permitiendo una comunicación eficaz y fluida, de manera que al intentar acceder a la página web desde otra sede que tenga configurado el tunel VPN hacia Santiago se puede acceder a la página techmove, el servicio de correos y el servicio FTP.

Esta conectividad estable contribuye directamente a mejorar el trabajo de la empresa, al facilitar la colaboración entre diferentes sedes y departamentos, y optimiza los tiempos de respuesta dentro de los procesos internos de la organización. En consecuencia, se logra un mejor rendimiento global en la comunicación corporativa, fortaleciendo la productividad y eficiencia de la compañía.

6. Conclusión

Este proyecto ha abordado de forma integral las principales debilidades detectadas en la red original, incorporando segmentación mediante VLANs, direccionamiento eficiente con VLSM, y mecanismos de control de acceso basados en NAT y ACLs. La implementación de túneles VPN IPsec garantiza la comunicación segura entre sedes geográficamente distribuidas, mientras que el uso de WPA2-PSK protege el entorno inalámbrico frente a accesos no autorizados. Asimismo, se han integrado medidas de calidad de servicio (QoS) para priorizar el tráfico crítico en áreas sensibles como Gerencia e Ingeniería.

Desde el punto de vista de la continuidad operativa, se han respetado y fortalecido los servicios existentes (Web, Correo, DNS y FTP), ahora integrados dentro de una red segmentada y protegida. Además, la introducción de IPv6 en el datacenter posiciona a TechMove en una ruta de transición tecnológica que le permitirá adaptarse sin fricciones a los estándares emergentes.

Por otro lado, la planificación de la red ha contemplado un crecimiento proyectado del 200%, lo cual ha sido resuelto mediante un diseño escalable, capaz de adaptarse a nuevas sucursales, usuarios y servicios sin requerir rediseños costosos o interrupciones operativas. Esta visión a largo plazo permite a la empresa crecer de forma ordenada, manteniendo la eficiencia y calidad en sus comunicaciones internas y externas.

Como punto de mejora, se recomienda implementar mecanismos de redundancia en enlaces y dispositivos críticos, con el fin de aumentar la resiliencia y disponibilidad de la red ante posibles fallos o interrupciones.

En resumen, el presente proyecto no solo resuelve las deficiencias del diseño original, sino que sienta las bases para una infraestructura robusta y confiable. Esta red corporativa, alineada con los objetivos estratégicos de TechMove, habilita su operación diaria con mayores garantías de seguridad y rendimiento, y le brinda las condiciones tecnológicas necesarias para seguir liderando el sector logístico en un entorno altamente competitivo y en constante evolución.

7. Bibliografía

References

- Cisco (2025) Cómo configurar una VPN en 6 pasos, Cisco. Available at: https://www.cisco.com/c/es_mx/solutions/small-business/resourcecenter/security/how-to-setup-a-vpn.html (Accessed: 25 May 2025).
- Sepúlveda, M. (2025, 18 marzo). ¿Qué es un protocolo de enrutamiento y cómo funciona? - eClassVirtual - Cursos Cisco en línea. *eClassVirtual - Cursos Cisco en línea*. https://eclassvirtual.com/que-es-un-protocolo-de-enrutamiento-y-como-funciona/
- ¿Qué es la calidad de servicio (QoS) en las redes? (2025) Fortinet. Disponible en: https://www.fortinet.com/lat/resources/cyberglossary/qos-quality-of-service (Consultado: el 23 de junio de 2025).
- What Is QoS (Quality of Service)? Meaning, Working, Importance, and Applications (2022) Spiceworks.com. Disponible en: https://www.spiceworks.com/tech/iot/articles/what-is-qos/ (Consultado: el 23 de junio de 2025).

8. Anexos

10.1 Anexo 1

Matriz RACI: Matriz RACI AG2

10.2 Anexo 2

Carta Gantt: Carta Gantt AG2