

**Redes y Comunicaciones de Datos**

**Sección: Sección**

**Profesor: Nombres y Apellidos del profesor**

**Integrantes:**

|  |  |
| --- | --- |
| **Apellidos y Nombres del integrante** | **Código de Integrante** |
| **Palma Obispo Adrián Enrique** | **U202210066** |
|  |  |
|  |  |
|  |  |

**Lima-Perú**

**día de mes de 2024**

# Resumen

**TechnoVision S.A. es una empresa líder en desarrollo de software con sede principal en Lima y sucursales en Arequipa y Piura. Ante su rápido crecimiento, necesita actualizar y estandarizar su infraestructura de red para mejorar la comunicación entre sedes, aumentar la seguridad y permitir un crecimiento escalable. Este informe detalla el diseño e implementación de una nueva red empresarial que cumple con estos objetivos.**

Contenido

[Resumen 1](#_Toc142595150)

[Objetivo del Estudiante (Student Outcome): 4](#_Toc142595151)

[Capítulo 1: Presentación, Análisis y Diseño 5](#_Toc142595152)

[1.1 Descripción del caso estudio 5](#_Toc142595153)

[1.1.1 Descripción de la empresa 5](#_Toc142595154)

[1.1.2 Descripción del problema o necesidad 5](#_Toc142595155)

[1.1.3 Objetivos de la solución propuesta 5](#_Toc142595156)

[1.2 Análisis de los requisitos de la red 5](#_Toc142595157)

[1.2.1 Requisitos de la red de la Sede Principal 5](#_Toc142595158)

[1.2.2 Requisitos de la red de la Sede Sucursal 1 5](#_Toc142595159)

[1.2.3 Requisitos de la red de la Sede Sucursal 2 5](#_Toc142595160)

[1.2.4 Requisitos Adicionales de la red 5](#_Toc142595161)

[1.3 Diseño de la nueva red 5](#_Toc142595162)

[1.3.1 Diseño de la topología WAN 5](#_Toc142595163)

[1.3.2 Diseño de la topología LAN 5](#_Toc142595164)

[Capítulo 2: Esquema de Direccionamiento IP 6](#_Toc142595165)

[2.1 Esquema de direccionamiento IP para todas las sedes 6](#_Toc142595166)

[2.2 Esquema de direccionamiento IP para cada sede 6](#_Toc142595167)

[2.2.1 Sede Principal 6](#_Toc142595168)

[2.2.2 Sede Sucursal 1 6](#_Toc142595169)

[2.2.3 Sede Sucursal 2 6](#_Toc142595170)

[2.3 Asignación de Vlan 6](#_Toc142595171)

[Capítulo 3: Solución Cloud (Backup) 7](#_Toc142595172)

[3.1 Descripción de los requisitos Cloud 7](#_Toc142595173)

[3.2 Factores a considerar para implementar una solución en Cloud 7](#_Toc142595174)

[3.2.1 Dimensión o Factor 1 7](#_Toc142595175)

[3.2.2 Dimensión o Factor 2 7](#_Toc142595176)

[3.2.3 Dimensión o Factor 3 7](#_Toc142595177)

[3.2.4 Dimensión o Factor n 7](#_Toc142595178)

[3.3 Proveedores de servicio Cloud 7](#_Toc142595179)

[3.3.1 Proveedor 1 7](#_Toc142595180)

[3.3.2 Proveedor 2 7](#_Toc142595181)

[3.3.3. Proveedor N 7](#_Toc142595182)

[3.4 Proceso de evaluación Cloud 7](#_Toc142595183)

[3.4.1 Dimensión o Factor 1 a evaluar 7](#_Toc142595184)

[3.4.2 Dimensión o Factor 2 a evaluar 7](#_Toc142595185)

[3.4.3 Dimensión o Factor n a evaluar 7](#_Toc142595186)

[3.5 Análisis de almacenamiento y transferencia de datos de los proveedores Cloud 8](#_Toc142595187)

[3.6 Selección y conclusión de la solución Cloud 8](#_Toc142595188)

[Capítulo 4: Componente y cantidades (Dimensionamiento) 9](#_Toc142595189)

[3.1 Dimensionamiento de los equipos de la solución 9](#_Toc142595190)

[3.2 Especificaciones técnicas de los equipos de la solución 9](#_Toc142595191)

[Capítulo 5: Enrutamiento dinámico y estático 10](#_Toc142595192)

[5.1 Implementación de enrutamiento estático 10](#_Toc142595193)

[5.2 Implementación de enrutamiento dinámico 10](#_Toc142595194)

[5.3 Tablas de enrutamiento 10](#_Toc142595195)

[Capítulo 6: Políticas de Seguridad la Red 11](#_Toc142595196)

[6.1 Sede Principal 11](#_Toc142595197)

[6.1.1 Implementación de la Primera política seguridad 11](#_Toc142595198)

[6.1.2 Implementación de la Segunda política seguridad 11](#_Toc142595199)

[6.1.3 Implementación de la N.. política seguridad 11](#_Toc142595200)

[6.2 Sede Sucursal 1 11](#_Toc142595201)

[6.2.1 Implementación de la Primera política seguridad 11](#_Toc142595202)

[6.2.2 Implementación de la Segunda política seguridad 11](#_Toc142595203)

[6.2.3 Implementación de la N.. política seguridad 11](#_Toc142595204)

[6.3 Sede Sucursal 2 11](#_Toc142595205)

[6.3.1 Implementación de la Primera política seguridad 11](#_Toc142595206)

[6.3.2 Implementación de la Segunda política seguridad 11](#_Toc142595207)

[6.3.3 Implementación de la N.. política seguridad 11](#_Toc142595208)

[Capítulo 7: Diagramas de la red 12](#_Toc142595209)

[7.1 Diagrama a nivel WAN 12](#_Toc142595210)

[7.2 Diagrama de la sede Principal 12](#_Toc142595211)

[7.3 Diagrama de la sede Sucursal 1 12](#_Toc142595212)

[7.4 Diagrama de la sede Sucursal 2 12](#_Toc142595213)

[7.5 Diagrama de ISP: 12](#_Toc142595214)

[Capítulo 8: Configuración de los dispositivos de red 13](#_Toc142595215)

[8.1 Configuración de Router 13](#_Toc142595216)

[8.2 Configuración de Switches (Multicapa) 13](#_Toc142595217)

[8.3 Configuración de Switches (Capa 2) 13](#_Toc142595218)

[8.4 Configuración de los Puntos de Acceso y Clientes Wifi 13](#_Toc142595219)

[8.4.1 WiFi Clientes 13](#_Toc142595220)

[8.4.2 WiFi Ejecutivos 13](#_Toc142595221)

[Capítulo 9: Configuración de los servicios de red 14](#_Toc142595222)

[9.1 Configuración del servicio FTP 14](#_Toc142595223)

[9.2 Configuración del servicio Web 14](#_Toc142595224)

[9.3 Configuración del servicio DNS 14](#_Toc142595225)

[9.4 Configuración del servicio de correo 14](#_Toc142595226)

[9.5 Configuración del servicio N 14](#_Toc142595227)

[Conclusiones y recomendaciones: 15](#_Toc142595228)

[Conclusiones: 15](#_Toc142595229)

[Recomendaciones: 15](#_Toc142595230)

[Glosario 16](#_Toc142595231)

[Referencias Bibliográficas: 17](#_Toc142595232)

# Objetivo del Estudiante (Student Outcome):

**Misión**

Diseñar e implementar redes de comunicación robustas y escalables para empresas del sector TI, garantizando conectividad eficiente entre múltiples sedes, alta seguridad y capacidad de crecimiento futuro, aplicando principios de ingeniería de redes y estándares internacionales.

**Visión**

Ser reconocidos como un equipo líder en el diseño de infraestructuras de red innovadoras, seguras y escalables para empresas tecnológicas, contribuyendo al crecimiento de sus operaciones y optimizando su comunicación global.

|  |  |
| --- | --- |
| Integrante | Student Outcome |
| Adrián Enrique Jesús Palma Obispo | **Outcome 1:** Demostrar capacidad de identificar y resolver problemas complejos relacionados con la infraestructura de red, aplicando principios de ingeniería para el análisis y diseño físico y lógico de la red (LAN y WAN), asegurando escalabilidad y seguridad.  **Hito 1:** Diseño físico y lógico de la topología de red (LAN y WAN).  **Hito 2:** Verificación del diseño con pruebas de conectividad y seguridad, y ajuste de la infraestructura para garantizar la viabilidad técnica. |
| Rodrigo | |  | | --- | |  |  |  | | --- | | **Outcome 2:** Demostrar capacidad de diseñar soluciones de redes basadas en un esquema de direccionamiento IP estandarizado, considerando factores como seguridad, escalabilidad y conectividad entre sedes.  **Hito 1:** Planificación del direccionamiento IP y segmentación en VLANs por departamento en todas las sedes.  **Hito 2:** Revisión y ajustes del esquema de direccionamiento durante las pruebas de conectividad y funcionalidad. |   finales y ajustar según sea necesario. |
| Harold | |  | | --- | |  |  |  | | --- | | **Outcome 3:** Demostrar capacidad de evaluar la viabilidad técnica y económica del diseño de red, seleccionando equipos y tecnologías apropiadas, y ajustando la infraestructura conforme a los resultados de las pruebas y necesidades del cliente.  **Hito 1:** Dimensionamiento técnico-económico, especificación de equipos y presupuesto.  **Hito 2:** Evaluación y ajuste del diseño en base a las pruebas finales, y evaluación de proveedores de servicios en la nube. | |
| Aldiaz | **Outcome 4:** Demostrar capacidad para implementar redes LAN y WAN, configurando dispositivos y aplicando políticas de segmentación y seguridad que aseguren una operación eficiente y segura.  **Hito 1:** Configuración de LANs (VLANs, InterVLANs, enrutamiento).  **Hito 2:** Implementación de la conectividad WAN y pruebas de comunicación entre sedes. |
| C | **Outcome 5:** Demostrar capacidad para configurar servicios de red y aplicar medidas de seguridad que aseguren el acceso y funcionamiento adecuado de los recursos dentro de la infraestructura.  **Hito 1:** Configuración de servicios (DNS, Web, FTP, DHCP, correo) y políticas de seguridad (firewalls, segmentación).  **Hito 2:** Evaluación de la seguridad mediante pruebas, e implementación de soluciones en la nube si es viable. |

# Capítulo 1: Presentación, Análisis y Diseño

## Descripción del caso estudio

### 1.1.1 Descripción de la empresa

TechnoVision S.A. es una empresa peruana de desarrollo de software fundada en 2010. Con más de 500 empleados distribuidos en 3 sedes (Lima, Arequipa y Piura), se especializa en soluciones de inteligencia artificial y análisis de datos para diversos sectores.

### 1.1.2 Descripción del problema o necesidad

La infraestructura de red actual de TechnoVision ha crecido de forma no planificada, resultando en problemas de conectividad, seguridad y escalabilidad. Se requiere una actualización completa que permita una comunicación eficiente entre sedes y soporte el crecimiento futuro.

### 1.1.3 Objetivos de la solución propuesta

* Implementar una red WAN segura y eficiente entre las 3 sedes.
* Diseñar una estructura LAN jerárquica en cada sede.
* Establecer un esquema de direccionamiento IP estandarizado.
* Implementar servicios de red centralizados (DNS, Web, FTP, correo).
* Mejorar la seguridad de la red mediante políticas y segmentación.
* Permitir un crecimiento escalable del 25% en los próximos 10 años.
* Implementar seguridad perimetral mediante firewalls en cada sede.

## 1.2 Análisis de los requisitos de la red

### 1.2.1 Requisitos de la red de la Sede Principal (Lima)

* 185 hosts actuales
* Segmentación en VLANs para cada departamento
* Conectividad WAN hacia sucursales
* Servicios centralizados (DNS, Web, FTP, correo)
* Redes WiFi para clientes y ejecutivos

### 1.2.2 Requisitos de la red de la Sede Sucursal (Arequipa)

* 124 hosts actuales
* Segmentación en VLANs similar a sede principal
* Conectividad WAN hacia sede principal
* Servidor FTP y Web local

### 1.2.3 Requisitos de la red de la Sede Sucursal (Piura)

* 110 hosts actuales
* Segmentación en VLANs similar a sede principal
* Conectividad WAN hacia sede principal
* Servidor FTP y Web local

### 1.2.4 Requisitos Adicionales de la red

* Crecimiento proyectado del 25% en 10 años
* Enrutamiento dinámico entre sedes
* Políticas de seguridad para acceso a recursos
* Solución de backup en la nube

## 1.3 Diseño de la nueva red

### 1.3.1 Diseño de la topología WAN

1. Topología Física y Lógica de la red

Se implementará una topología hub-and-spoke con la sede de Lima como hub central conectado a las sucursales de Arequipa y Piura mediante enlaces dedicados. Se utilizará el espacio de direccionamiento 172.4.0.0/16 para la red interna.

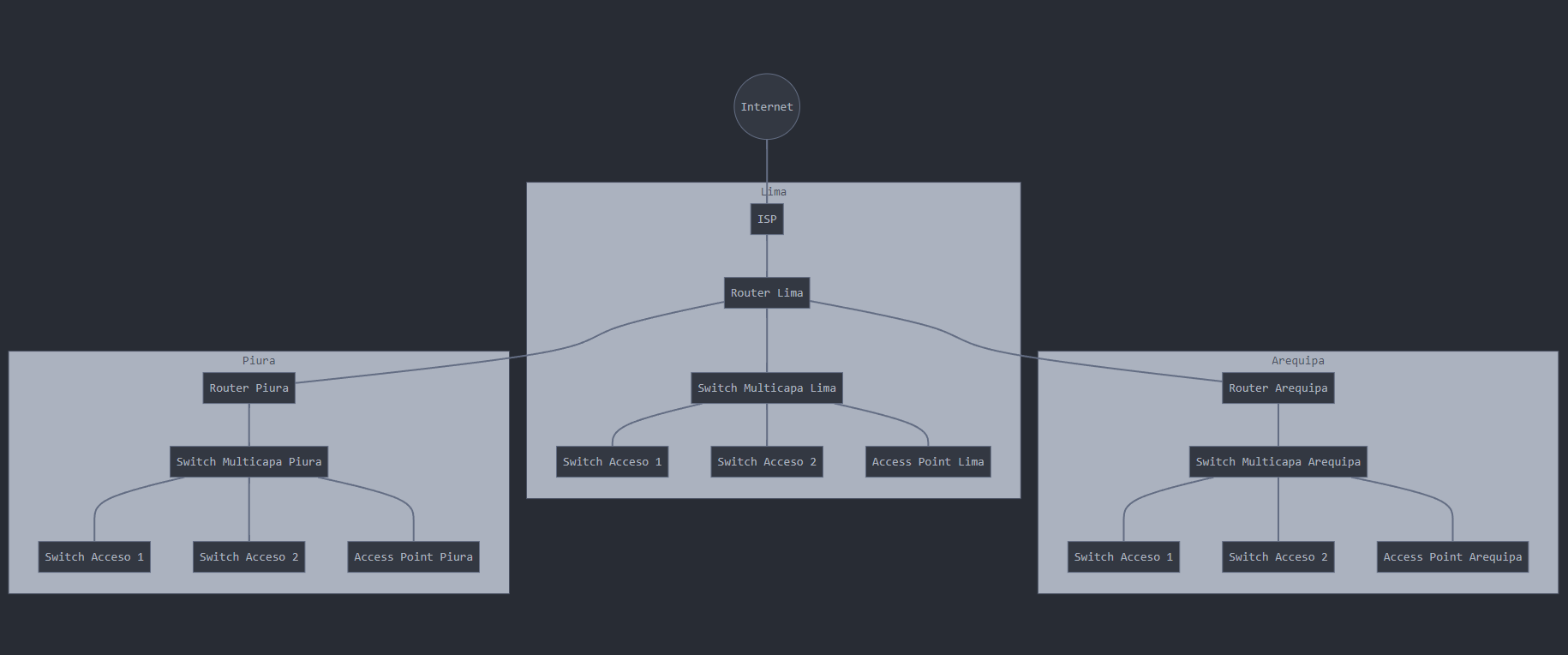
### 1.3.2 Diseño de la topología LAN

1. Topología Física y Lógica de la red

En cada sede se implementará una arquitectura jerárquica de 3 capas:

* Capa de acceso: Switches de acceso para conectar dispositivos finales
* Capa de distribución: Switches multicapa para agregar tráfico y aplicar políticas
* Capa de núcleo: Routers para conectividad WAN e Internet

Se implementarán VLANs para segmentar el tráfico por departamentos y dos redes WiFi (clientes y ejecutivos) en cada sede.

<https://github.com/user-attachments/assets/4261b977-ff3e-4d3c-8fbd-9ff07513722b>

Topología general de la red de TechnoVision S.A

# Capítulo 2: Esquema de Direccionamiento IP

## 2.1 Esquema de direccionamiento IP para todas las sedes

Utilizaremos el espacio de direccionamiento 172.4.0.0/16 asignado a TechnoVision S.A.

## 2.2 Esquema de direccionamiento IP para cada sede

### 2.2.1 Sede Principal (Lima)

* Red: 172.4.0.0/17
* VLANs:
  + Administración: 172.4.0.0/24
  + Logística: 172.4.1.0/24
  + Finanzas: 172.4.2.0/24
  + Marketing: 172.4.3.0/24
  + Ventas: 172.4.4.0/24
  + Servidores: 172.4.5.0/24
  + WiFi Clientes: 172.4.6.0/24
  + WiFi Ejecutivos: 172.4.7.0/24
  + Gestión: 172.4.8.0/24
* Enlaces WAN:
  + Hacia Arequipa: 10.1.1.0/30
  + Hacia Piura: 10.1.1.4/30

### 2.2.2 Sede Sucursal 1 (Arequipa)

* Red: 172.4.128.0/18
* VLANs:
  + Administración: 172.4.128.0/24
  + Logística: 172.4.129.0/24
  + Finanzas: 172.4.130.0/24
  + Marketing: 172.4.131.0/24
  + Ventas: 172.4.132.0/24
  + Servidores: 172.4.133.0/24
  + WiFi Clientes: 172.4.134.0/24
  + WiFi Ejecutivos: 172.4.135.0/24
  + Gestión: 172.4.136.0/24

- Enlace WAN hacia Lima: 10.1.1.0/30

### 2.2.3 Sede Sucursal 2 (Piura)

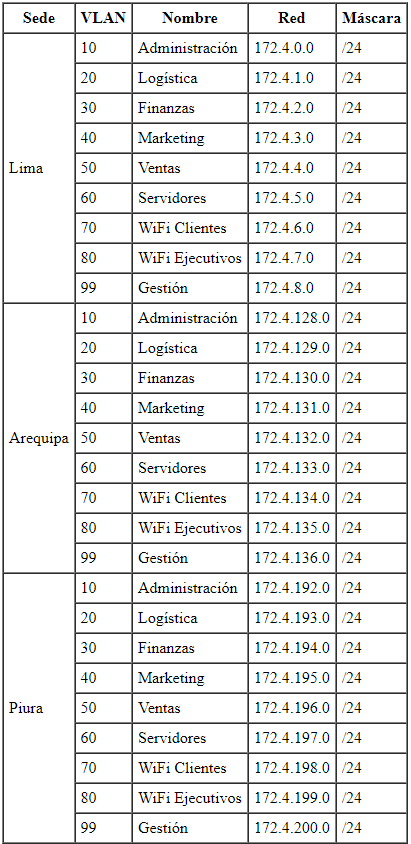
* Red: 172.4.192.0/18
* VLANs:
  + Administración: 172.4.192.0/24
  + Logística: 172.4.193.0/24
  + Finanzas: 172.4.194.0/24
  + Marketing: 172.4.195.0/24
  + Ventas: 172.4.196.0/24
  + Servidores: 172.4.197.0/24
  + WiFi Clientes: 172.4.198.0/24
  + WiFi Ejecutivos: 172.4.199.0/24
  + Gestión: 172.4.200.0/24
* Enlace WAN hacia Lima: 10.1.1.4/30



<https://github.com/user-attachments/assets/b7fe97d9-6f2f-4042-878a-3361eb6cddc2>

## 2.3 Asignación de Vlan

* VLAN 10: Administración
* VLAN 20: Logística
* VLAN 30: Finanzas
* VLAN 40: Marketing
* VLAN 50: Ventas
* VLAN 60: Servidores
* VLAN 70: WiFi Clientes
* VLAN 80: WiFi Ejecutivos
* VLAN 99: Gestión



<https://github.com/user-attachments/assets/7341650e-efd1-4024-94a7-1d8ea42bd671>

# Capítulo 3: Solución Cloud (Backup)

## 3.1 Descripción de los requisitos Cloud

TechnoVision S.A. requiere una solución de almacenamiento en la nube para implementar un sistema corporativo de backup. Los requisitos principales son:

* Capacidad de almacenamiento adecuada para respaldar datos críticos de las 3 sedes
* Alta disponibilidad y durabilidad de los datos
* Seguridad robusta para proteger información sensible
* Escalabilidad para acomodar el crecimiento futuro
* Costos optimizados

3.2 Factores a considerar para implementar una solución en Cloud

3.2.1 Seguridad y cumplimiento normativo

* Encriptación de datos en reposo y en tránsito
* Controles de acceso y autenticación
* Cumplimiento con regulaciones de protección de datos

3.2.2 Rendimiento y latencia

* Velocidad de carga y descarga de datos
* Latencia entre las sedes y la nube

3.2.3 Escalabilidad y flexibilidad

* Capacidad de aumentar almacenamiento según demanda
* Opciones de tipos de almacenamiento (hot, cool, archive)

3.2.4 Costos y modelo de precios

* Costos de almacenamiento por GB
* Costos de transferencia de datos
* Modelos de precios (pago por uso, reservado, etc.)

## 3.3 Proveedores de servicio Cloud

3.3.1 Amazon Web Services (AWS)

3.3.2 Microsoft Azure

3.3.3. Google Cloud Platform (GCP)

## 3.4 Proceso de evaluación Cloud

3.4.1 Seguridad y cumplimiento

1. a. AWS:
   * Ofrece AWS Key Management Service (KMS) para gestión de claves
   * Cumple con múltiples certificaciones (ISO 27001, SOC 2, etc.)
2. b. Azure:
   * Azure Key Vault para gestión de secretos y claves
   * Amplio conjunto de certificaciones de cumplimiento

1. c. GCP:
   * Cloud Key Management Service para encriptación
   * Cumplimiento con estándares internacionales

3.4.2 Rendimiento y latencia

1. a. AWS:

* Múltiples regiones en Sudamérica para menor latencia
* Amazon S3 ofrece alta durabilidad (99.999999999%)

1. b. Azure:

* Presencia de centros de datos en Brasil
* Azure Blob Storage con opciones de redundancia geográfica

1. c. GCP:

* Región en São Paulo, Brasil
* Google Cloud Storage con replicación multi-regional

3.4.3 Costos y modelo de precios

a. AWS:

* Modelo de precios por niveles basado en uso
* Opciones de clases de almacenamiento (S3 Standard, S3 Glacier)

b. Azure:

* Precios competitivos con opciones de compromiso a largo plazo
* Niveles de acceso Hot, Cool y Archive

c. GCP:

* Precios simples y competitivos
* Opciones de clase de almacenamiento (Standard, Nearline, Coldline)

## 3.5 Análisis de almacenamiento y transferencia de datos de los proveedores Cloud

Para este análisis, asumiremos que TechnoVision S.A. necesita almacenar inicialmente 10 TB de datos y transfiere aproximadamente 1 TB al mes.

* AWS:
  + Almacenamiento S3 Standard: $0.0230 por GB/mes
  + Transferencia saliente: $0.09 por GB (primeros 10 TB/mes)
  + Costo mensual estimado: $230 (almacenamiento) + $90 (transferencia) = $320
* Azure:
  + Blob Storage (LRS Hot Tier): $0.0184 por GB/mes
  + Transferencia saliente: $0.087 por GB (primeros 10 TB/mes)
  + Costo mensual estimado: $184 (almacenamiento) + $87 (transferencia) = $271
* GCP:
  + Cloud Storage Standard: $0.020 por GB/mes
  + Transferencia saliente: $0.12 por GB (a América del Sur)
  + Costo mensual estimado: $200 (almacenamiento) + $120 (transferencia) = $320

## 3.6 Selección y conclusión de la solución Cloud

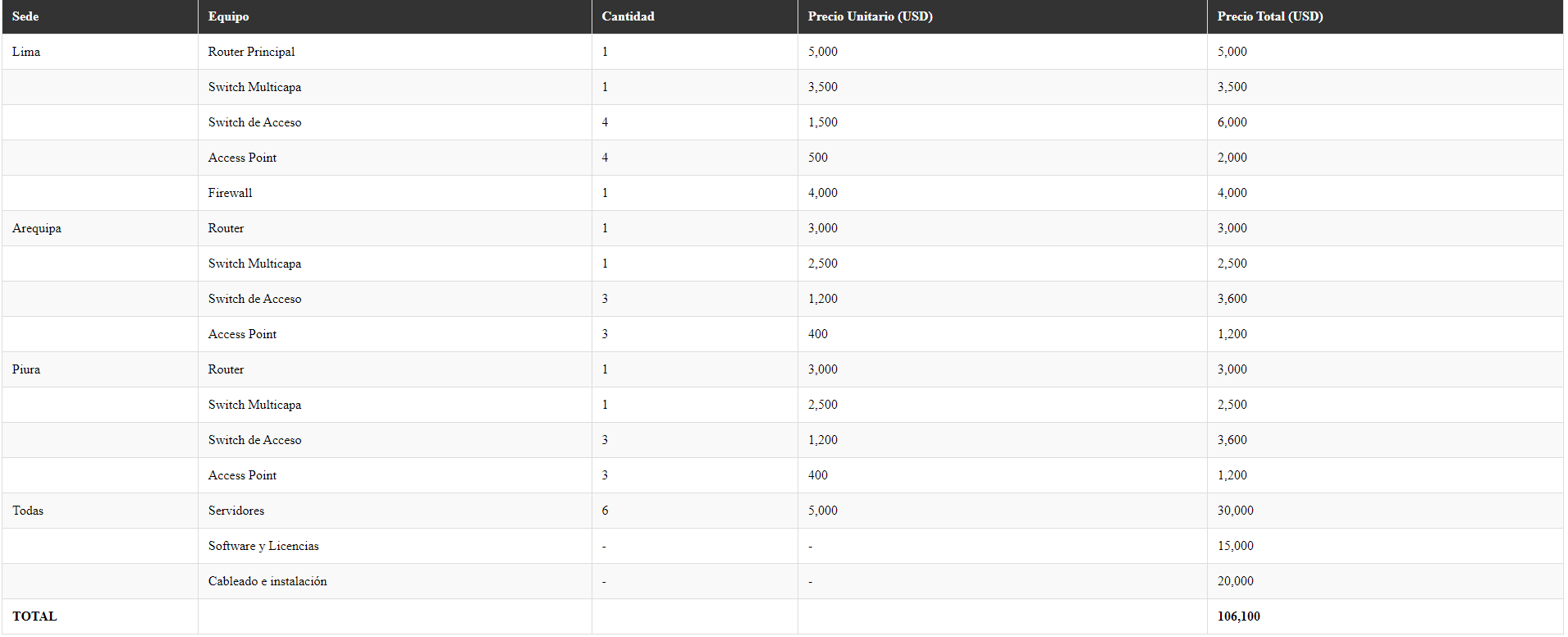
Después de evaluar las opciones, recomendamos Microsoft Azure como la solución de almacenamiento en la nube para TechnoVision S.A. Las razones principales son:

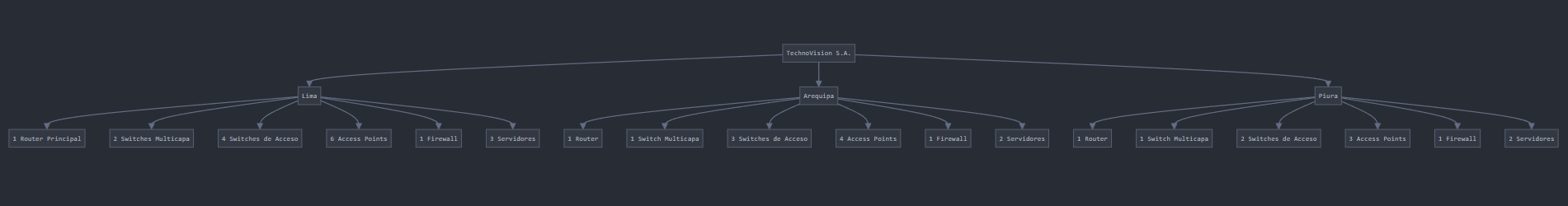
* Mejor relación costo-beneficio en el análisis realizado.
* Fuerte presencia en la región con centros de datos en Brasil, lo que puede mejorar el rendimiento.
* Robusto conjunto de características de seguridad y cumplimiento normativo.
* Flexibilidad en las opciones de almacenamiento y fácil integración con herramientas de backup existentes.

Se recomienda comenzar con Azure Blob Storage en el nivel Hot Access para los backups activos, con la opción de mover datos menos frecuentes a niveles Cool o Archive para optimizar costos a largo plazo.

# Capítulo 4: Componente y cantidades (Dimensionamiento)

## 4.1 Dimensionamiento de los equipos y valorización de la solución

<https://github.com/user-attachments/assets/d1bc26c8-79e1-4b08-acbb-65688c9b1326>

<https://github.com/user-attachments/assets/8eee5e0f-3e67-47b9-bacc-53247703d0c6>

## 4.2 Especificaciones técnicas de los equipos de la solución

## Router Principal (Lima)

## Modelo: Cisco ISR 4451-X

## Interfaces: 4 x 1GE, 2 x 10GE

## Rendimiento: Hasta 2 Gbps

## Soporte para VPN, MPLS, QoS

## Memoria: 16 GB RAM, 32 GB Flash

## Switch Multicapa (Lima)

## Modelo: Cisco Catalyst 9300

## Puertos: 24 x 1GE, 4 x 10GE SFP+

## Capacidad de conmutación: 480 Gbps

## PoE+ en todos los puertos 1GE

## Soporte para SDN y automatización

## Switch de Acceso

## Modelo: Cisco Catalyst 2960-X

## Puertos: 48 x 1GE, 2 x 10GE SFP+

## PoE+ en todos los puertos

## Capacidad de conmutación: 216 Gbps

## Access Point

## Modelo: Cisco Aironet 3800

## Estándares: WiFi 6 (802.11ax)

## Dual-band: 2.4 GHz y 5 GHz

## MIMO 4x4:4

## Soporte para 500+ clientes concurrentes

## Firewall

## Modelo: Fortinet FortiGate 200F

## Rendimiento de Firewall: 20 Gbps

## Rendimiento de VPN IPsec: 10 Gbps

## Sesiones concurrentes: 3 millones

## Nuevas sesiones/segundo: 300,000

## Router (Arequipa y Piura)

## Modelo: Cisco ISR 4331

## Interfaces: 3 x 1GE, 2 x 10GE

## Rendimiento: Hasta 1 Gbps

## Soporte para VPN, QoS

## Memoria: 8 GB RAM, 16 GB Flash

## Servidores

## Modelo: Dell PowerEdge R740

## Procesador: 2 x Intel Xeon Gold 6248R

## Memoria: 384 GB RAM

## Almacenamiento: 8 x 1.92 TB SSD en RAID 10

## Interfaces de red: 4 x 10GE

# Capítulo 5: Enrutamiento dinámico y estático

## 5.1 Implementación de enrutamiento estático

Para la conexión con el ISP y la ruta por defecto, se implementará enrutamiento estático en los routers de borde de cada sede:

* Router Lima:
  + ip route 0.0.0.0 0.0.0.0 200.1.1.1
* Router Arequipa:
  + ip route 0.0.0.0 0.0.0.0 200.2.2.1
* Router Piura:
  + ip route 0.0.0.0 0.0.0.0 200.3.3.1

## 5.2 Implementación de enrutamiento dinámico

Para la comunicación entre sedes, se implementará OSPF (Open Shortest Path First) como protocolo de enrutamiento dinámico:

Router Lima:

router ospf 1

network 172.4.0.0 0.0.127.255 area 0

network 10.1.1.0 0.0.0.3 area 0

network 10.1.1.4 0.0.0.3 area 0

Router Arequipa:

router ospf 1

network 172.4.128.0 0.0.63.255 area 0

network 10.1.1.0 0.0.0.3 area 0

Router Piura:

router ospf 1

network 172.4.192.0 0.0.63.255 area 0

network 10.1.1.4 0.0.0.3 area 0

## 5.3 Tablas de enrutamiento

Router Lima:

Gateway of last resort is 200.1.1.1 to network 0.0.0.0

O 172.4.128.0/18 [110/2] via 10.1.1.2, 00:00:05, GigabitEthernet0/1

O 172.4.192.0/18 [110/2] via 10.1.1.6, 00:00:10, GigabitEthernet0/2

C 172.4.0.0/17 is directly connected, GigabitEthernet0/0

C 10.1.1.0/30 is directly connected, GigabitEthernet0/1

C 10.1.1.4/30 is directly connected, GigabitEthernet0/2

S\* 0.0.0.0/0 [1/0] via 200.1.1.1

Router Arequipa:

Gateway of last resort is 200.2.2.1 to network 0.0.0.0

O 172.4.0.0/17 [110/2] via 10.1.1.1, 00:00:15, GigabitEthernet0/1

O 172.4.192.0/18 [110/3] via 10.1.1.1, 00:00:15, GigabitEthernet0/1

C 172.4.128.0/18 is directly connected, GigabitEthernet0/0

C 10.1.1.0/30 is directly connected, GigabitEthernet0/1

S\* 0.0.0.0/0 [1/0] via 200.2.2.1

Router Piura:

Gateway of last resort is 200.3.3.1 to network 0.0.0.0

O 172.4.0.0/17 [110/2] via 10.1.1.5, 00:00:20, GigabitEthernet0/1

O 172.4.128.0/18 [110/3] via 10.1.1.5, 00:00:20, GigabitEthernet0/1

C 172.4.192.0/18 is directly connected, GigabitEthernet0/0

C 10.1.1.4/30 is directly connected, GigabitEthernet0/1

S\* 0.0.0.0/0 [1/0] via 200.3.3.1

Leyenda:

* O: OSPF
* C: Directamente conectada
* S\*: Ruta estática por defecto

# Capítulo 6: Políticas de Seguridad la Red

## 6.1 Sede Principal (Lima)

### 6.1.1 Implementación de la Primera política seguridad

Política: Restringir el acceso a los servidores desde las redes de usuarios.

Configuración en el Firewall de Lima:

Esta política ayuda a proteger los servidores de accesos no autorizados desde las redes de usuarios, mejorando la seguridad de la infraestructura crítica.



<https://github.com/user-attachments/assets/71766f46-de95-4d45-b269-d9ca6e9d3149>

access-list 101 permit ip 172.4.5.0 0.0.0.255 any

access-list 101 deny ip any 172.4.5.0 0.0.0.255

access-list 101 permit ip any any

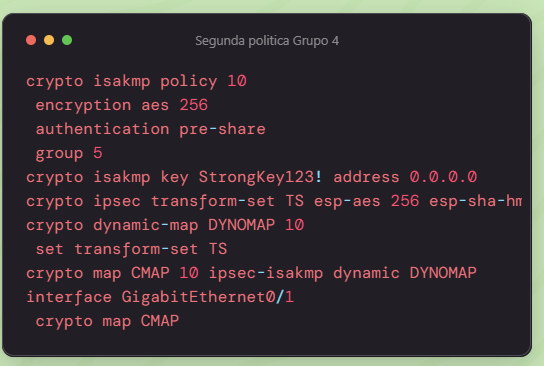
interface GigabitEthernet0/0

ip access-group 101 in

### 6.1.2 Implementación de la Segunda política seguridad

Política: Permitir acceso VPN solo a usuarios autorizados.

Configuración en el Router de Lima:



<https://github.com/user-attachments/assets/040f047f-7409-4337-b4d0-799fe4d2eb3e>

crypto isakmp policy 10

encryption aes 256

authentication pre-share

group 5

crypto isakmp key StrongKey123! address 0.0.0.0

crypto ipsec transform-set TS esp-aes 256 esp-sha-hmac

crypto dynamic-map DYNOMAP 10

set transform-set TS

crypto map CMAP 10 ipsec-isakmp dynamic DYNOMAP

interface GigabitEthernet0/1

crypto map CMAP

### 6.1.3 Implementación de la tercera política de seguridad

Política: Implementar filtrado de contenido web.

Configuración en el Firewall de Lima:



<https://github.com/user-attachments/assets/080468cb-2ed0-4f4f-b8d4-f0def477737f>

url-filtering block-list

entry 1 gambling

entry 2 adult-content

entry 3 malware-sites

web-filter profile DEFAULT\_PROFILE

category gambling action block

category adult-content action block

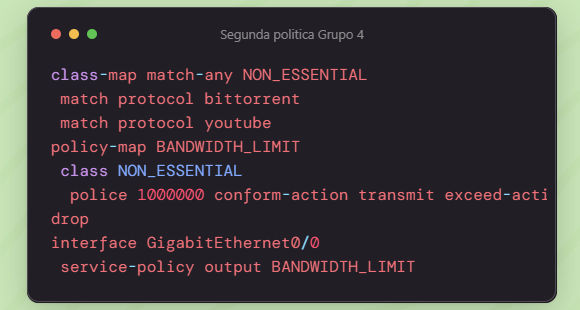
category malware-sites action block

## 6.2 Sede Sucursal 1 (Arequipa)

### 6.2.1 Implementación de la Primera política seguridad

Política: Limitar el ancho de banda para tráfico no esencial.

Configuración en el Router de Arequipa:



<https://github.com/user-attachments/assets/651f43ff-78b5-4450-81d8-932203c58180>

class-map match-any NON\_ESSENTIAL

match protocol bittorrent

match protocol youtube

policy-map BANDWIDTH\_LIMIT

class NON\_ESSENTIAL

police 1000000 conform-action transmit exceed-action drop

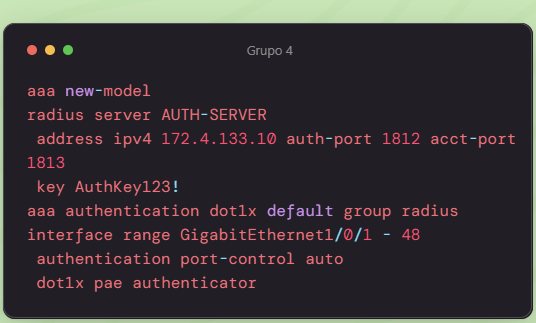
interface GigabitEthernet0/0

service-policy output BANDWIDTH\_LIMIT

### 6.2.2 Implementación de la Segunda política seguridad

Política: Implementar autenticación 802.1X para acceso a la red.

Configuración en el Switch Multicapa de Arequipa:



<https://github.com/user-attachments/assets/9e3833a9-99b3-4ffb-88ed-2c8cdf4d8205>

aaa new-model

radius server AUTH-SERVER

address ipv4 172.4.133.10 auth-port 1812 acct-port 1813

key AuthKey123!

aaa authentication dot1x default group radius

interface range GigabitEthernet1/0/1 - 48

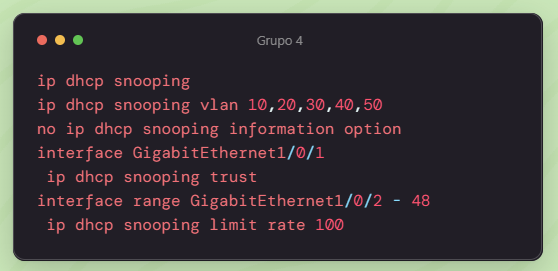
authentication port-control auto

dot1x pae authenticator

### 6.2.3 Implementación de la tercera política de seguridad

Política: Configurar DHCP snooping para prevenir ataques de DHCP rogue.

Configuración en el Switch Multicapa de Arequipa:



<https://github.com/user-attachments/assets/6ace78ec-66d2-4216-bc05-bfc97dd46ebd>

ip dhcp snooping

ip dhcp snooping vlan 10,20,30,40,50

no ip dhcp snooping information option

interface GigabitEthernet1/0/1

ip dhcp snooping trust

interface range GigabitEthernet1/0/2 - 48

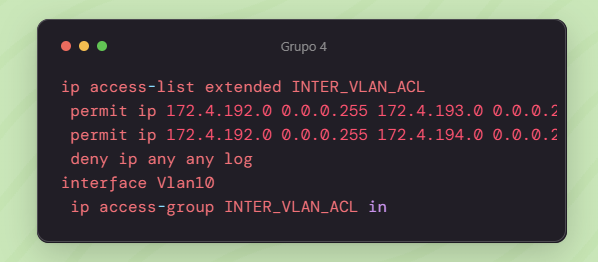
ip dhcp snooping limit rate 100

## 6.3 Sede Sucursal 2 (Piura)

### 6.3.1 Implementación de la Primera política seguridad

Política: Implementar listas de control de acceso (ACL) para restringir el tráfico entre VLANs.

Configuración en el Switch Multicapa de Piura:

<https://github.com/user-attachments/assets/90cd98d3-509a-4d1d-87ca-7935fea0525a>

ip access-list extended INTER\_VLAN\_ACL

permit ip 172.4.192.0 0.0.0.255 172.4.193.0 0.0.0.255

permit ip 172.4.192.0 0.0.0.255 172.4.194.0 0.0.0.255

deny ip any any log

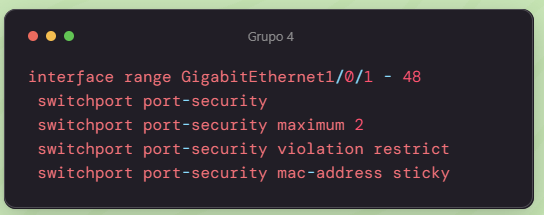
interface Vlan10

ip access-group INTER\_VLAN\_ACL in

### 6.3.2 Implementación de la Segunda política seguridad

Política: Configurar port security para prevenir ataques de MAC flooding.

Configuración en los Switches de Acceso de Piura:



<https://github.com/user-attachments/assets/3f045e2e-6719-4c6b-93e9-4de0e484d092>

interface range GigabitEthernet1/0/1 - 48

switchport port-security

switchport port-security maximum 2

switchport port-security violation restrict

switchport port-security mac-address sticky

### 6.3.3 Implementación de la tercera política de seguridad

Política: Implementar Network Access Control (NAC) para garantizar que solo los dispositivos autorizados y actualizados puedan conectarse a la red.

Configuración en el Router de Piura (asumiendo que se usa Cisco Identity Services Engine):



<https://github.com/user-attachments/assets/67fab042-d173-4699-b720-fa50181795bd>

aaa new-model

aaa authentication dot1x default group radius

aaa authorization network default group radius

radius server ISE

address ipv4 172.4.197.10 auth-port 1812 acct-port 1813

key ISEAuthKey123!

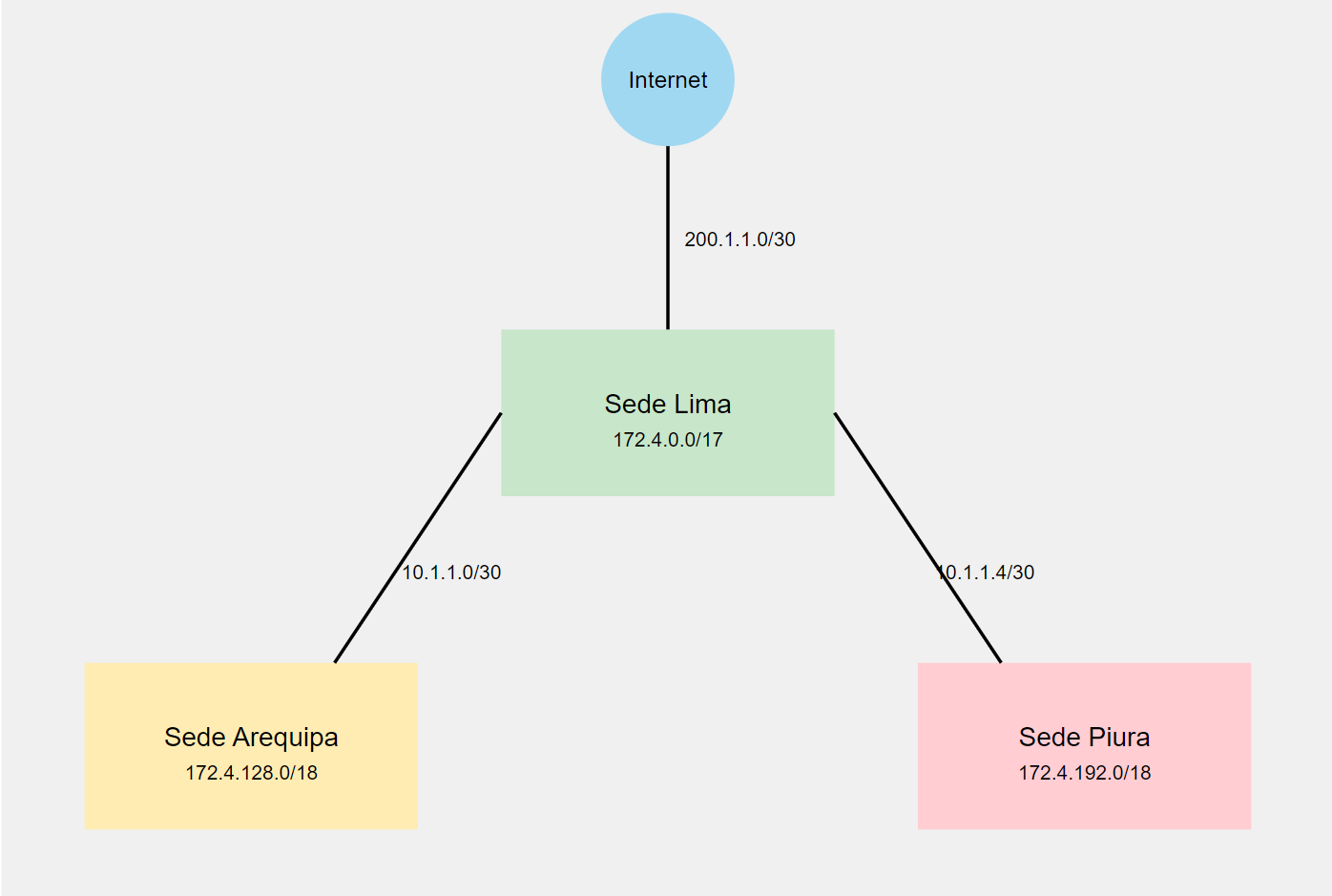
interface GigabitEthernet0/0

dot1x pae authenticator

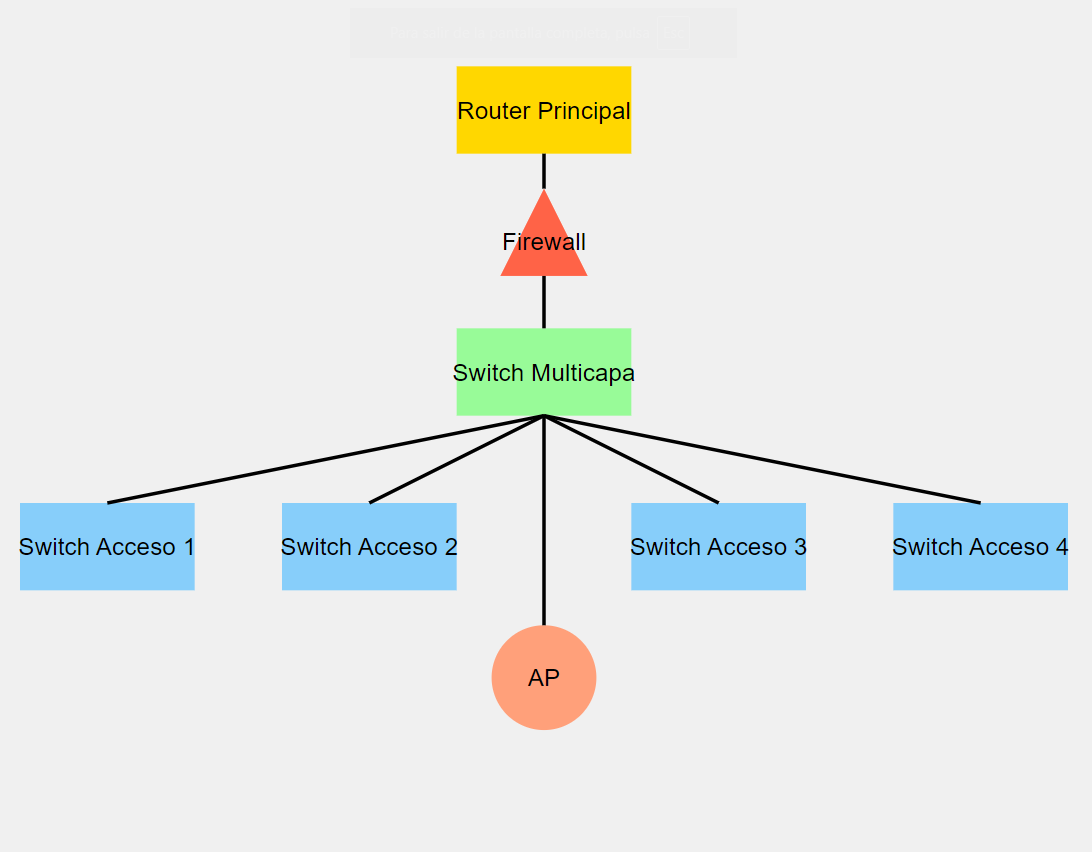
authentication port-control auto

# Capítulo 7: Diagramas de la red

## 7.1 Diagrama a nivel WAN

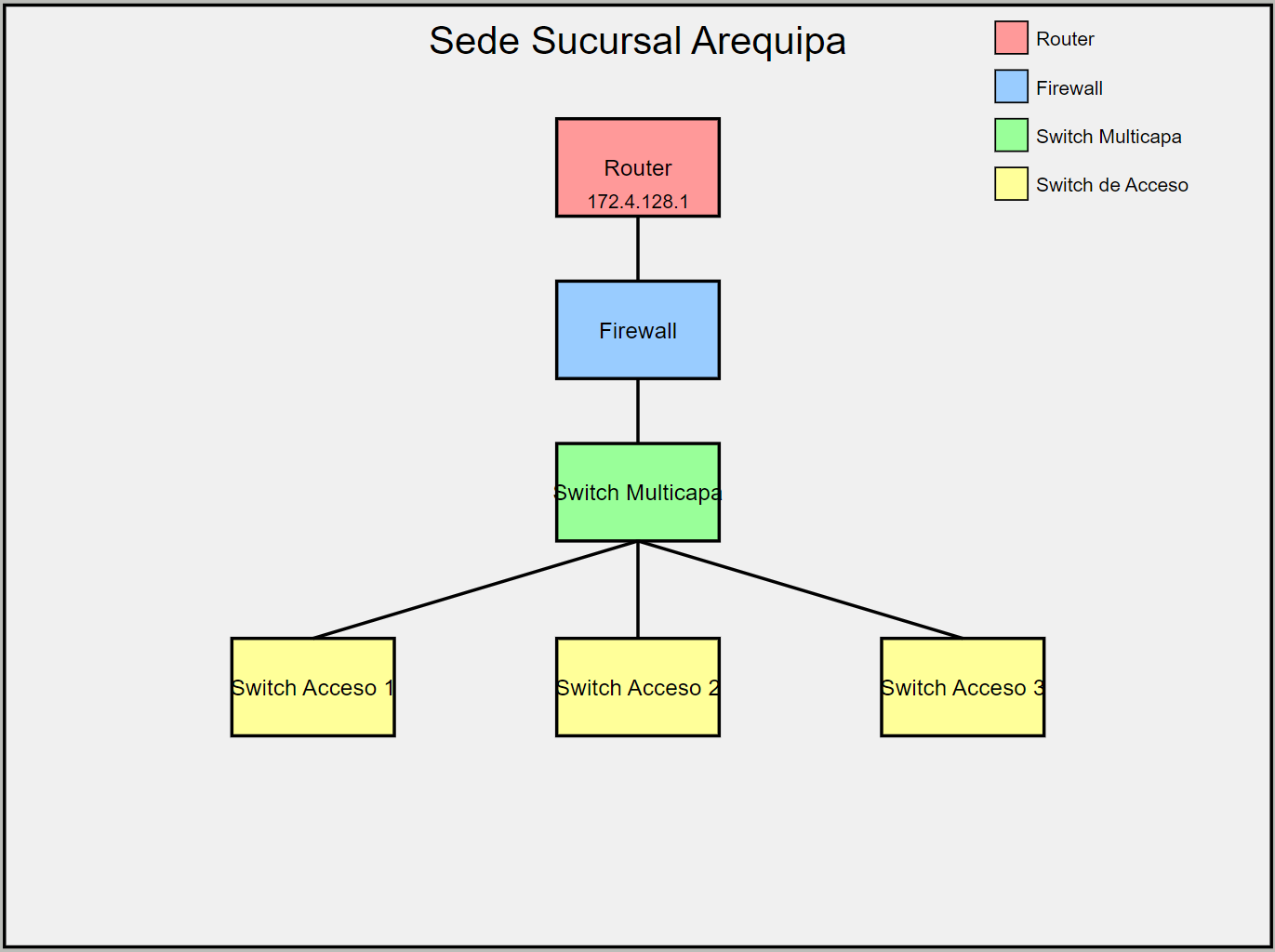
<https://github.com/user-attachments/assets/8b480e62-88ef-488a-acd7-76c51eee181a>

## 7.2 Diagrama de la sede Principal (Lima)



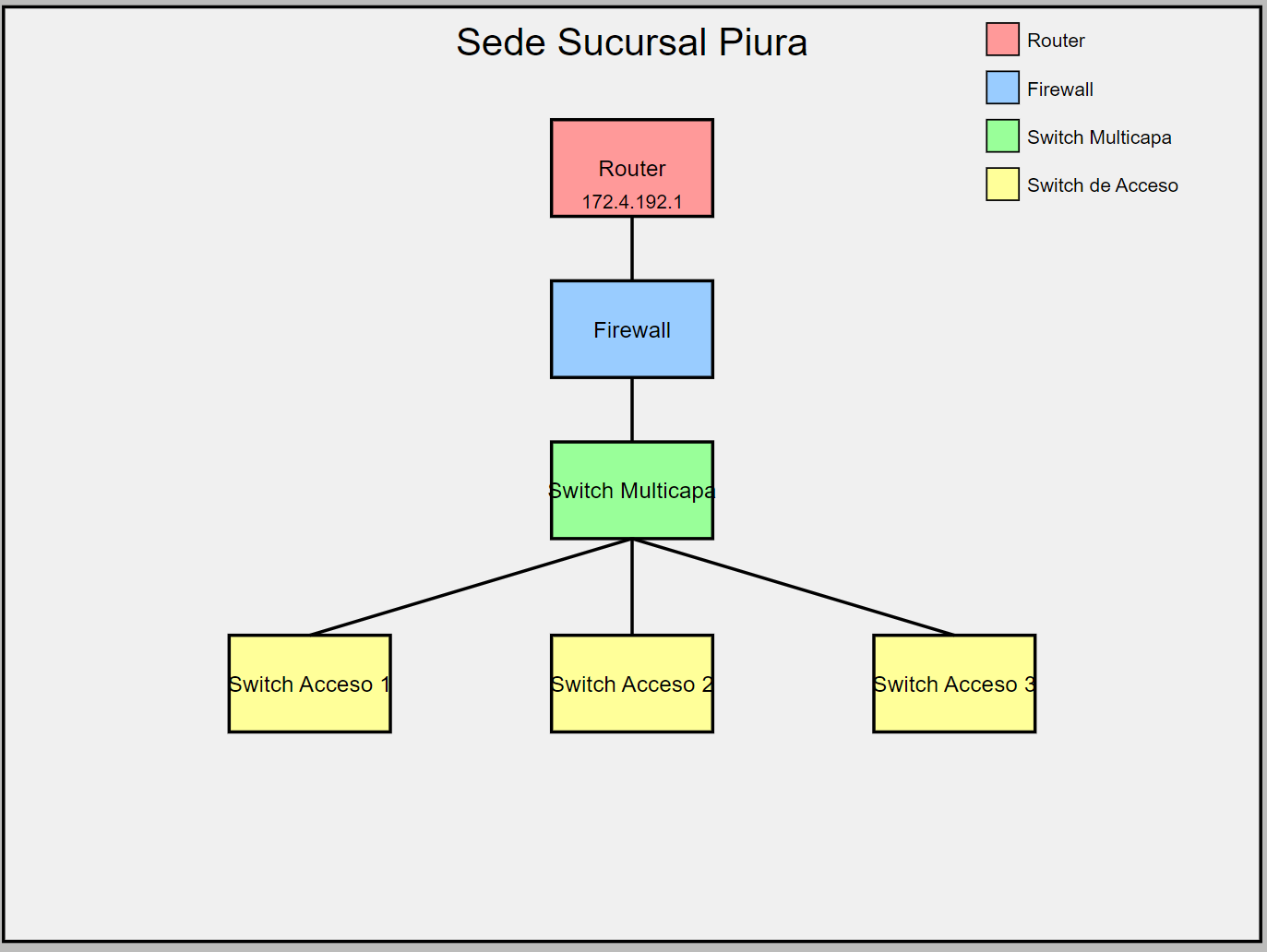
<https://github.com/user-attachments/assets/e66778bf-d7d4-4147-8337-4305b89b08cc>

## 7.3 Diagrama de la sede Sucursal 1 (Arequipa)



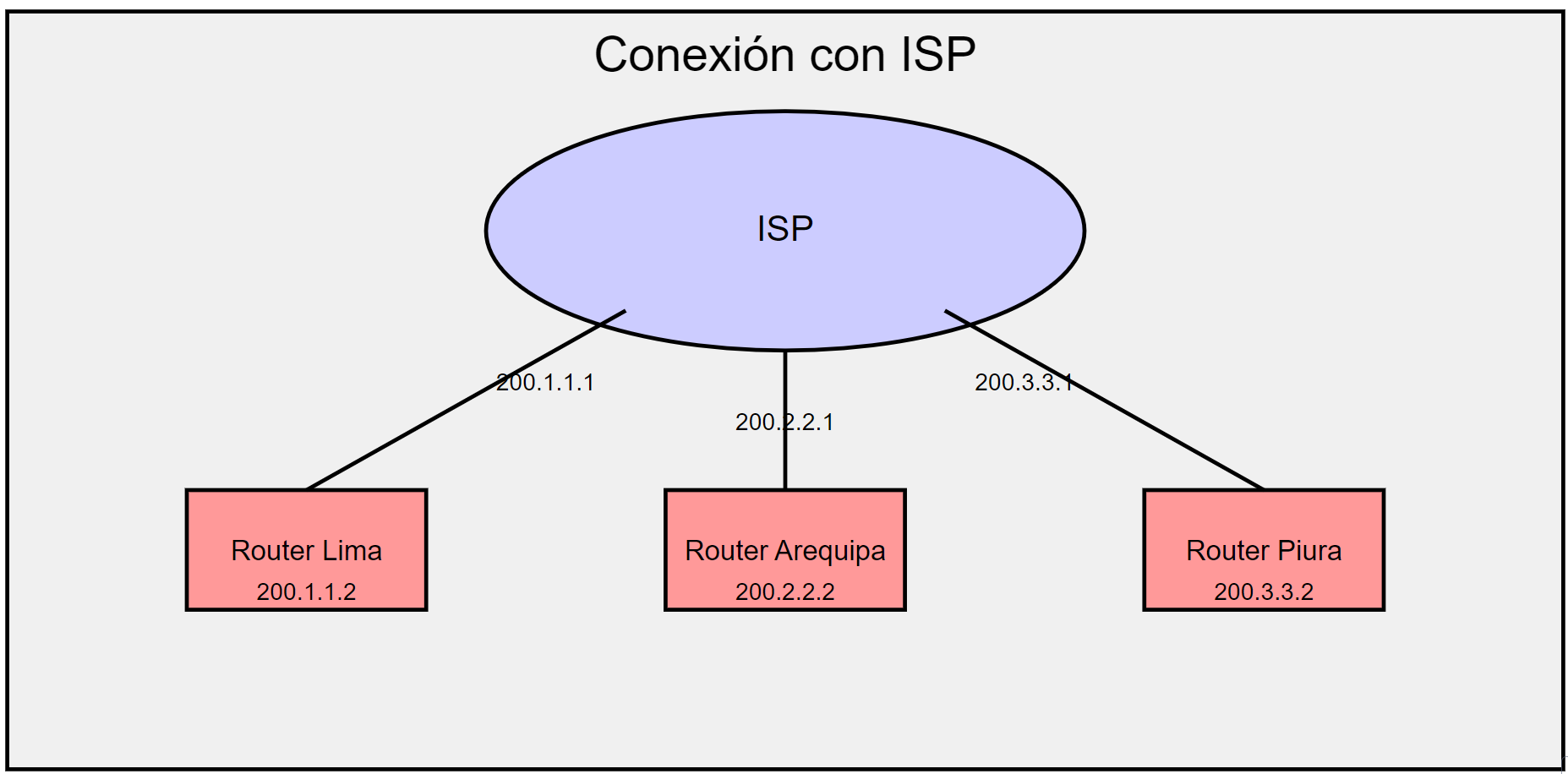
<https://github.com/user-attachments/assets/e1d88ff7-039a-427d-9f56-7c384dba7617>

## 7.4 Diagrama de la sede Sucursal 2 (Piura)



<https://github.com/user-attachments/assets/f7968a1c-b9dd-4242-90f2-d877c07e7ce8>

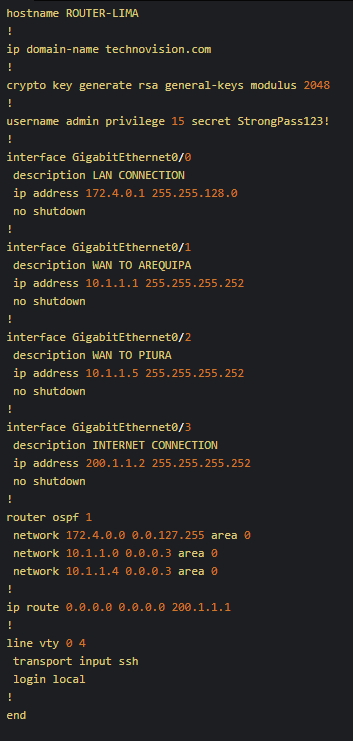
## 7.5 Diagrama de ISP:



<https://github.com/user-attachments/assets/d1b5d8ba-c640-4e0c-9c3a-6b8eadbe6585>

# Capítulo 8: Configuración de los dispositivos de red

## 8.1 Configuración de Router



<https://github.com/user-attachments/assets/38acc714-482f-4435-84bf-35cc5f359e40>

hostname ROUTER-LIMA

!

ip domain-name technovision.com

!

crypto key generate rsa general-keys modulus 2048

!

username admin privilege 15 secret StrongPass123!

!

interface GigabitEthernet0/0

description LAN CONNECTION

ip address 172.4.0.1 255.255.128.0

no shutdown

!

interface GigabitEthernet0/1

description WAN TO AREQUIPA

ip address 10.1.1.1 255.255.255.252

no shutdown

!

interface GigabitEthernet0/2

description WAN TO PIURA

ip address 10.1.1.5 255.255.255.252

no shutdown

!

interface GigabitEthernet0/3

description INTERNET CONNECTION

ip address 200.1.1.2 255.255.255.252

no shutdown

!

router ospf 1

network 172.4.0.0 0.0.127.255 area 0

network 10.1.1.0 0.0.0.3 area 0

network 10.1.1.4 0.0.0.3 area 0

!

ip route 0.0.0.0 0.0.0.0 200.1.1.1

!

line vty 0 4

transport input ssh

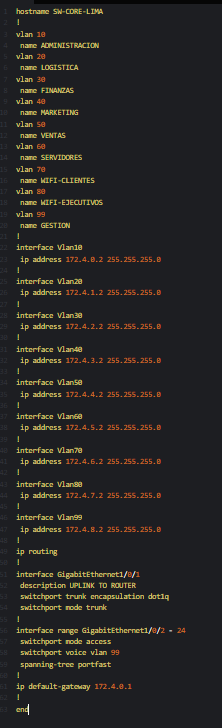
login local

!

end

## 8.2 Configuración de Switches (Multicapa)

Configuración del Switch Multicapa (Lima):



<https://github.com/user-attachments/assets/de04e270-182a-4c26-a07e-5ea5808c91a0>

hostname SW-CORE-LIMA

!

vlan 10

name ADMINISTRACION

vlan 20

name LOGISTICA

vlan 30

name FINANZAS

vlan 40

name MARKETING

vlan 50

name VENTAS

vlan 60

name SERVIDORES

vlan 70

name WIFI-CLIENTES

vlan 80

name WIFI-EJECUTIVOS

vlan 99

name GESTION

!

interface Vlan10

ip address 172.4.0.2 255.255.255.0

!

interface Vlan20

ip address 172.4.1.2 255.255.255.0

!

interface Vlan30

ip address 172.4.2.2 255.255.255.0

!

interface Vlan40

ip address 172.4.3.2 255.255.255.0

!

interface Vlan50

ip address 172.4.4.2 255.255.255.0

!

interface Vlan60

ip address 172.4.5.2 255.255.255.0

!

interface Vlan70

ip address 172.4.6.2 255.255.255.0

!

interface Vlan80

ip address 172.4.7.2 255.255.255.0

!

interface Vlan99

ip address 172.4.8.2 255.255.255.0

!

ip routing

!

interface GigabitEthernet1/0/1

description UPLINK TO ROUTER

switchport trunk encapsulation dot1q

switchport mode trunk

!

interface range GigabitEthernet1/0/2 - 24

switchport mode access

switchport voice vlan 99

spanning-tree portfast

!

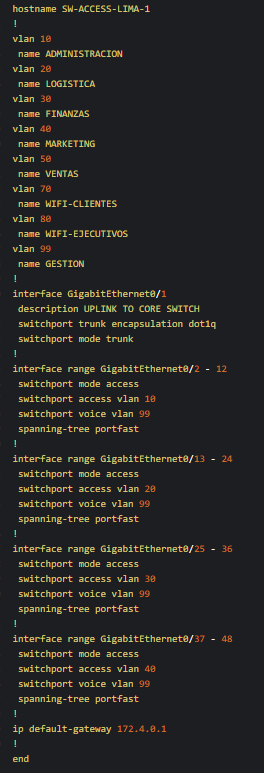
ip default-gateway 172.4.0.1

!

end

## 8.3 Configuración de Switches (Capa 2)

Configuración de un Switch de Acceso (Lima):



<https://github.com/user-attachments/assets/5ffeb404-5812-45a5-909c-ebd6908e4879>

hostname SW-ACCESS-LIMA-1

!

vlan 10

name ADMINISTRACION

vlan 20

name LOGISTICA

vlan 30

name FINANZAS

vlan 40

name MARKETING

vlan 50

name VENTAS

vlan 70

name WIFI-CLIENTES

vlan 80

name WIFI-EJECUTIVOS

vlan 99

name GESTION

!

interface GigabitEthernet0/1

description UPLINK TO CORE SWITCH

switchport trunk encapsulation dot1q

switchport mode trunk

!

interface range GigabitEthernet0/2 - 12

switchport mode access

switchport access vlan 10

switchport voice vlan 99

spanning-tree portfast

!

interface range GigabitEthernet0/13 - 24

switchport mode access

switchport access vlan 20

switchport voice vlan 99

spanning-tree portfast

!

interface range GigabitEthernet0/25 - 36

switchport mode access

switchport access vlan 30

switchport voice vlan 99

spanning-tree portfast

!

interface range GigabitEthernet0/37 - 48

switchport mode access

switchport access vlan 40

switchport voice vlan 99

spanning-tree portfast

!

ip default-gateway 172.4.0.1

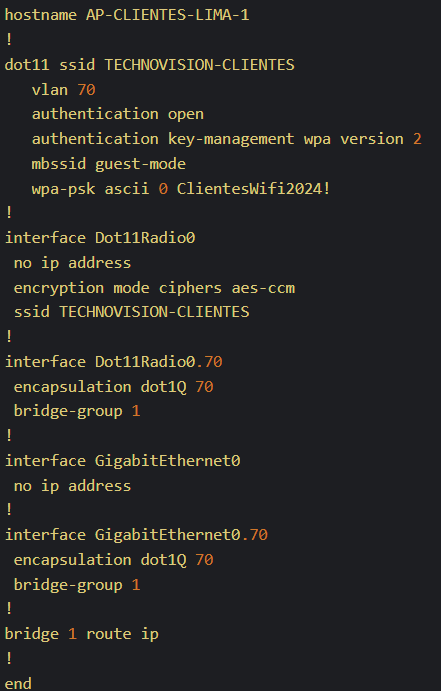
!

end

## 8.4 Configuración de los Puntos de Acceso y Clientes Wifi

### 8.4.1 WiFi Clientes

Configuración del Access Point para clientes:



<https://github.com/user-attachments/assets/139d0829-7117-4a4f-9d8c-ffba34e23765>

hostname AP-CLIENTES-LIMA-1

!

dot11 ssid TECHNOVISION-CLIENTES

vlan 70

authentication open

authentication key-management wpa version 2

mbssid guest-mode

wpa-psk ascii 0 ClientesWifi2024!

!

interface Dot11Radio0

no ip address

encryption mode ciphers aes-ccm

ssid TECHNOVISION-CLIENTES

!

interface Dot11Radio0.70

encapsulation dot1Q 70

bridge-group 1

!

interface GigabitEthernet0

no ip address

!

interface GigabitEthernet0.70

encapsulation dot1Q 70

bridge-group 1

!

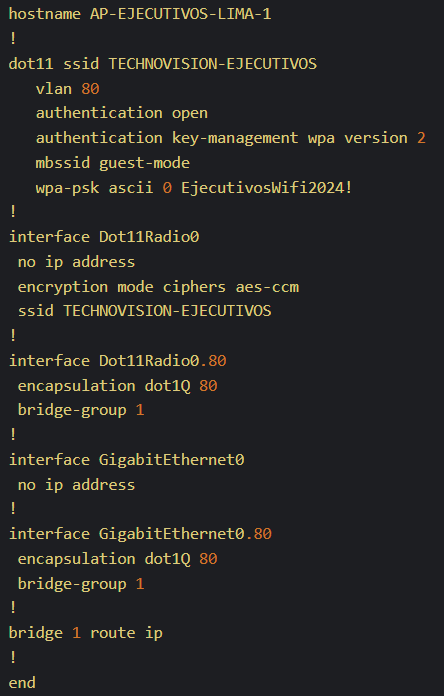
bridge 1 route ip

!

end

### 8.4.2 WiFi Ejecutivos

Configuración del Access Point para ejecutivos:



<https://github.com/user-attachments/assets/55c9a626-0df9-4837-bc47-7e8723be0429>

hostname AP-EJECUTIVOS-LIMA-1

!

dot11 ssid TECHNOVISION-EJECUTIVOS

vlan 80

authentication open

authentication key-management wpa version 2

mbssid guest-mode

wpa-psk ascii 0 EjecutivosWifi2024!

!

interface Dot11Radio0

no ip address

encryption mode ciphers aes-ccm

ssid TECHNOVISION-EJECUTIVOS

!

interface Dot11Radio0.80

encapsulation dot1Q 80

bridge-group 1

!

interface GigabitEthernet0

no ip address

!

interface GigabitEthernet0.80

encapsulation dot1Q 80

bridge-group 1

!

bridge 1 route ip

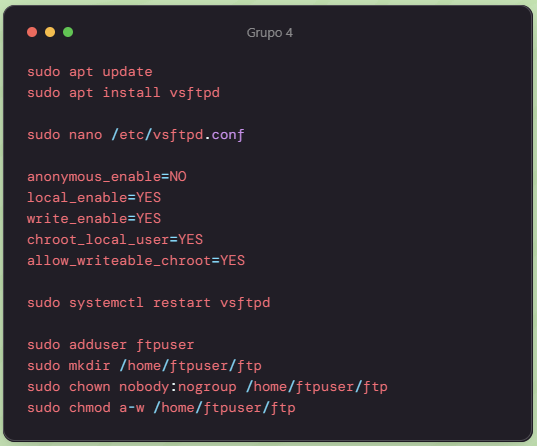
!

end

# Capítulo 9: Configuración de los servicios de red

## 9.1 Configuración del servicio FTP

Configuración del servidor FTP en Linux (Ubuntu Server):



<https://github.com/user-attachments/assets/e3545728-176d-4089-bad2-99e724a9b30a>

sudo apt update

sudo apt install vsftpd

sudo nano /etc/vsftpd.conf

anonymous\_enable=NO

local\_enable=YES

write\_enable=YES

chroot\_local\_user=YES

allow\_writeable\_chroot=YES

sudo systemctl restart vsftpd

sudo adduser ftpuser

sudo mkdir /home/ftpuser/ftp

sudo chown nobody:nogroup /home/ftpuser/ftp

sudo chmod a-w /home/ftpuser/ftp

## 9.2 Configuración del servicio Web

Configuración del servidor web Apache en Linux (Ubuntu Server):



<https://github.com/user-attachments/assets/f014b729-15f2-4971-802b-e8907d99db9e>

sudo apt update

sudo apt install apache2

sudo ufw allow 'Apache'

sudo mkdir /var/www/technovision

sudo chown -R $USER:$USER /var/www/technovision

sudo nano /var/www/technovision/index.html

<html>

<head>

<title>Bienvenido a TechnoVision</title>

</head>

<body>

<h1>Bienvenido al sitio web de TechnoVision S.A.</h1>

</body>

</html>

sudo nano /etc/apache2/sites-available/technovision.conf

<VirtualHost \*:80>

ServerName technovision.com

ServerAlias www.technovision.com

ServerAdmin webmaster@technovision.com

DocumentRoot /var/www/technovision

ErrorLog ${APACHE\_LOG\_DIR}/error.log

CustomLog ${APACHE\_LOG\_DIR}/access.log combined

</VirtualHost>

sudo a2ensite technovision.conf

sudo systemctl restart apache2

## 9.3 Configuración del servicio DNS

Configuración del servidor DNS BIND en Linux (Ubuntu Server):



<https://github.com/user-attachments/assets/19d1855a-e1d1-4dfd-9a6a-7e320bbc57b3>

sudo apt update

sudo apt install bind9 bind9utils bind9-doc

sudo nano /etc/bind/named.conf.local

zone "technovision.com" {

type master;

file "/etc/bind/zones/db.technovision.com";

};

zone "4.172.in-addr.arpa" {

type master;

file "/etc/bind/zones/db.172.4";

};

sudo mkdir /etc/bind/zones

sudo nano /etc/bind/zones/db.technovision.com

$TTL 604800

@ IN SOA ns1.technovision.com. admin.technovision.com. (

3 ; Serial

604800 ; Refresh

86400 ; Retry

2419200 ; Expire

604800 ) ; Negative Cache TTL

;

@ IN NS ns1.technovision.com.

@ IN A 172.4.0.10

ns1 IN A 172.4.0.10

www IN A 172.4.0.20

ftp IN A 172.4.0.30

mail IN A 172.4.0.40

sudo nano /etc/bind/zones/db.172.4

$TTL 604800

@ IN SOA ns1.technovision.com. admin.technovision.com. (

3 ; Serial

604800 ; Refresh

86400 ; Retry

2419200 ; Expire

604800 ) ; Negative Cache TTL

;

@ IN NS ns1.technovision.com.

10 IN PTR ns1.technovision.com.

20 IN PTR www.technovision.com.

30 IN PTR ftp.technovision.com.

40 IN PTR mail.technovision.com.

sudo systemctl restart bind9

## 9.4 Configuración del servicio de correo

Configuración del servidor de correo Postfix en Linux (Ubuntu Server):



<https://github.com/user-attachments/assets/0ba93847-d09e-40bd-b25a-0818e5b15403>

sudo apt update

sudo apt install postfix dovecot-core dovecot-imapd dovecot-pop3d

sudo nano /etc/postfix/main.cf

myhostname = mail.technovision.com

mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain

inet\_interfaces = all

mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128 172.4.0.0/16

sudo nano /etc/dovecot/dovecot.conf

protocols = imap pop3

mail\_location = maildir:/var/mail/%u

sudo systemctl restart postfix

sudo systemctl restart dovecot

## 9.5 Configuración del servicio de Monitoreo

## Configuración de Zabbix para monitoreo de red:



<https://github.com/user-attachments/assets/d449561e-96c2-4688-8436-8300869f7303>

sudo apt update

sudo apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-agent mysql-server php libapache2-mod-php php-mysql

sudo mysql -uroot -p

CREATE DATABASE zabbix CHARACTER SET utf8 COLLATE utf8\_bin;

CREATE USER 'zabbix'@'localhost' IDENTIFIED BY 'password';

GRANT ALL PRIVILEGES ON zabbix.\* TO 'zabbix'@'localhost';

FLUSH PRIVILEGES;

quit;

zcat /usr/share/doc/zabbix-server-mysql\*/create.sql.gz | mysql -uzabbix -p zabbix

sudo nano /etc/zabbix/zabbix\_server.conf

DBPassword=password

sudo systemctl restart zabbix-server zabbix-agent apache2

sudo systemctl enable zabbix-server zabbix-agent apache2

# Conclusiones y recomendaciones:

## Conclusiones:

* La nueva infraestructura de red diseñada para TechnoVision S.A. proporciona una solución robusta y escalable que cumple con los objetivos establecidos de mejorar la comunicación entre sedes, aumentar la seguridad y permitir un crecimiento futuro.
* La implementación de una topología WAN hub-and-spoke con OSPF como protocolo de enrutamiento dinámico asegura una comunicación eficiente y redundante entre las tres sedes de la empresa.
* La segmentación de la red mediante VLANs y la implementación de políticas de seguridad en los firewalls y switches mejora significativamente la seguridad y el control del tráfico de red.
* La solución de almacenamiento en la nube de Microsoft Azure proporciona una opción confiable y rentable para el respaldo de datos críticos de la empresa.
* La configuración de servicios centralizados como DNS, Web, FTP y correo electrónico mejora la gestión y el acceso a los recursos de la empresa desde todas las sedes.

## Recomendaciones:

* Implementar un plan de mantenimiento regular y monitoreo proactivo de la infraestructura de red para asegurar su óptimo funcionamiento y detectar posibles problemas antes de que afecten las operaciones.
* Establecer un programa de capacitación continua para el personal de TI sobre las nuevas tecnologías y configuraciones implementadas

# Glosario

* **VLAN: Red de área local virtual**
* **WAN: Red de área amplia**
* **LAN: Red de área local**
* **OSPF: Open Shortest Path First, protocolo de enrutamiento**
* **NAC: Control de Acceso a la Red**
* **ACL: Lista de Control de Acceso**
* **ISP: Proveedor de Servicios de Internet**
* **VPN: Red Privada Virtual**
* **DHCP: Protocolo de configuración dinámica de host**
* **DNS: Sistema de Nombres de Dominio**
* **FTP (File Transfer Protocol): Protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP.**
* Apache: Servidor web de código abierto multiplataforma.
* DNS (Domain Name System): Sistema de nomenclatura jerárquica para dispositivos conectados a redes IP.
* BIND (Berkeley Internet Name Domain): Implementación de código abierto del protocolo DNS.
* Postfix: Agente de transferencia de correo (MTA) de código abierto.
* Dovecot: Servidor de IMAP y POP3 de código abierto.
* Zabbix: Sistema de monitorización de código abierto para diversos componentes de TI.

# Referencias Bibliográficas:

* Cisco. (2023). Cisco Networking Academy. https://www.netacad.com/
* Kurose, J. F., & Ross, K. W. (2023). Computer Networking: A Top-Down Approach (8th ed.). Pearson.
* Forouzan, B. A. (2022). Data Communications and Networking (6th ed.). McGraw-Hill Education.
* Amazon Web Services. (2024). AWS Documentation. https://docs.aws.amazon.com/
* Microsoft Azure. (2024). Azure Documentation. https://docs.microsoft.com/en-us/azure/
* Google Cloud Platform. (2024). GCP Documentation. <https://cloud.google.com/docs>
* Ubuntu Server Guide. (2024). Recuperado de https://ubuntu.com/server/docs
* Apache HTTP Server Documentation. (2024). Recuperado de <https://httpd.apache.org/docs/>
* BIND 9 Administrator Reference Manual. (2024). Recuperado de <https://www.isc.org/bind/>
* Postfix Documentation. (2024). Recuperado de <http://www.postfix.org/documentation.html>
* Dovecot Documentation. (2024). Recuperado de <https://doc.dovecot.org/>
* Zabbix Documentation. (2024). Recuperado de https://www.zabbix.com/documentation/current/en/manual