Universidad Católica Santa María

Escuela profesional de Ingeniería de Sistemas

Julio Enrique Centeno León, Luis Fabrizio Espinoza Bellido, Jose Alonso Yañez Mejia, Juan Diego Treviño Vilca

julio.centeno@ucsm.edu.pe - luis.espinozab@ucsm.edu.pe - jose.yanez@ucsm.edu.pe - juan.trevino@ucsm.edu.pe

---

Computación en Red II

Diario de Ingeniería Pacifico Seguros

Ingeniera Karina Rosas

Arequipa - 2024

ÍNDICE:

INTRODUCCIÓN:

En el mundo actual, donde la tecnología avanza a pasos agigantados, la infraestructura de redes juega un papel crucial en el funcionamiento de las organizaciones, especialmente en sectores tan sensibles y estratégicos como el de los seguros. Las Redes de Seguros Pacífico representan un componente vital en la operación diaria, asegurando la transmisión eficiente y segura de datos críticos entre diversas entidades, oficinas y sistemas. Este diario de ingeniería se dedica a explorar y analizar conocimientos sobre las complejidades y avances en las redes de seguros, enfocándose en los desafíos y las soluciones aplicables a este sector.

En Seguros Pacífico, la infraestructura de red no es solo un componente técnico; es el pilar fundamental que soporta todas las operaciones de la compañía. Desde la gestión de pólizas y reclamaciones hasta la interacción en tiempo real con clientes y socios, las redes de comunicación deben ser robustas, seguras y altamente eficientes. La capacidad de Seguros Pacífico para ofrecer un servicio ininterrumpido y de alta calidad depende en gran medida de la integridad y el rendimiento de sus redes.

OBJETIVOS:

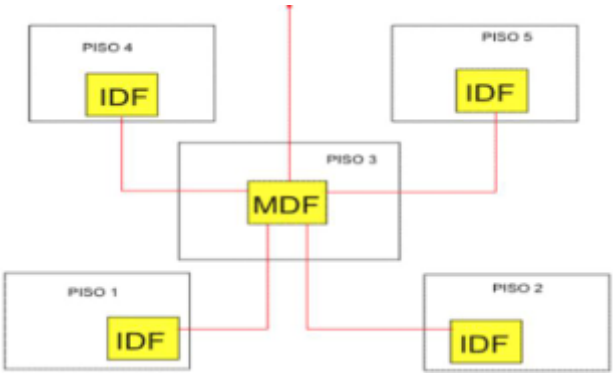
- ***Objetivo Principal:***
  - *Realizar el diario de Ingeniería de Seguros Pacifico, el cual está enfocado en presentar una visión clara de las redes de la empresa teniendo en cuenta la infraestructura de la red tanto física como lógica, teniendo en cuenta todas medidas de seguridad física y lógicas que presenten. Establecer una red robusta y de alta disponibilidad para los datacenters de Pacífico y Tivit. Esto es fundamental para asegurar una comunicación eficiente y segura entre las distintas ubicaciones, permitiendo una operación continua y sin interrupciones.*

- ***Objetivos Específicos:***
  - *Realizar el monitoreo de las redes y hacer los planos de la misma y verificar que la estructura de la red cumpla con los estándares establecidos por la TIA, ANSI y la EIA.*
  - *Realizar mejoras a corto plazo de la infraestructura de red según sea requerido y brindar una propuesta de mejora en el rendimiento de las redes de Pacifico*
  - *Implementar mecanismos de seguridad avanzados para proteger la integridad y confidencialidad de los datos. Además, establecer protocolos de redundancia para asegurar la continuidad del servicio en caso de fallos.*

DESCRIPCIÓN GENERAL DE ARQUITECTURA DE LA RED:

- ***Anchos de Banda:***
  Dentro de la oficina se ofrece una velocidad de 50 Mbps, y la conexión entre sedes es de 10 Gbps

- ***Topología Física y Lógica:***
  - ***Física:***
    La red presenta una topología en estrella, donde múltiples nodos están conectados a un punto central utilizando enlaces MPLS proporcionados por Claro. Esta configuración permite una gestión centralizada y eficiente del tráfico de red, facilitando la monitorización y el control de la red desde un único punto.



Las ubicaciones clave incluyen Tamayo, Chorrillos, Camelias y La Molina. Cada una de estas ubicaciones está conectada mediante enlaces de alta velocidad de 10Gbps y 50 Mbps. Esta distribución asegura que los datos puedan transmitirse rápidamente entre los sitios, minimizando la latencia y maximizando el rendimiento.

En esta red se utilizan "2" switch de capa 3 (Uno Activo y Uno de Backup), los cuales se superponen entre sí en sus respectivos racks para conectar todas las unidades de cada piso. También hay un panel de conexión para datos y un panel de conexión para voz, así como sus respectivos cables de conexión.
Estos switches se consideran puentes multi puertos con dominio de colisión debido a la segmentación. La conmutación generada por los switches aumenta el ancho de banda disponible en una red.

Para cada sede, se implementa un sistema de generación de redundancia en el que cada switch core y sus switches de capa 3 tienen una réplica. La conexión entre estos dispositivos se realiza a través de EtherChannel y Virtual Port Channel (VPC), lo que asegura una alta disponibilidad y resistencia a fallos en la red.

- ***Lógica:***
  La red utiliza una topología de broadcast, lo que significa que los mensajes enviados por cualquier dispositivo se transmiten a todos los demás dispositivos de la red. Sin embargo, con el uso de switches de capa 3, el tráfico de broadcast puede ser segmentado y controlado mediante VLANs. Las cuales se utilizan para segmentar y organizar el tráfico de la red. Esto permite aislar y controlar el tráfico dentro de cada ubicación, mejorando la seguridad y limitando la propagación de mensajes de broadcast.

  Los switches de capa 3 permiten la creación de VLANs, lo que segmenta la red en subredes más pequeñas. Esto mejora la seguridad y el rendimiento al limitar el alcance de los mensajes de broadcast y reducir el dominio de colisión. Cada ubicación clave (Tamayo, Chorrillos, Camelias y La Molina) puede tener su propio conjunto de VLANs, permitiendo un control granular del tráfico y la segmentación de usuarios o servicios. En adición se tiene una vlan con su respectivo segmento de red para la telefonía proporcionada por la marca AVAYA

  El tráfico InterVLAN entre el equipo de red y seguridad se gestiona de manera específica para asegurar el control y la protección adecuada de los datos. La segmentación mediante VLANs y la gestión cuidadosa del tráfico InterVLAN entre el equipo de red y seguridad son prácticas fundamentales en la red de Pacífico. Estas medidas aseguran la eficiencia operativa, la seguridad robusta y la gestión simplificada de los recursos de red.

Las conexiones entre las ubicaciones claves utilizan enlaces MPLS proporcionados por Claro. MPLS permite la creación de rutas de datos eficientes y predefinidas, mejorando la velocidad y la fiabilidad de la transmisión de datos entre las sedes. Se hace uso de HSRP para el control de alta disponibilidad. Esto se da con algunos de los proveedores de la empresa con quienes se tiene doble conexión desde los data center hacia los suyos, como por ejemplo la conexión con "Doctor+" además se emplea STP para asegurar que no haya bucles en la topología de estrella utilizada. Esto permite una redundancia en los enlaces sin crear bucles que podrían causar tormentas de broadcast o problemas de congestión. También cuenta con VTP que facilita la gestión de VLAN en la red, permitiendo cambios en la configuración de VLANs de manera centralizada desde un servidor VTP.

DTP permite que los switches determinen automáticamente si deben establecer un enlace troncal y la forma en que se negocia ese enlace, simplificando la configuración y la administración de troncales VLAN en la red. DHCPv4 se utiliza para asignar direcciones IP dinámicamente a dispositivos dentro de la red de Seguros Pacífico, simplificando la gestión de direcciones IP y asegurando una configuración de red eficiente. No se implementa DHCPv6 en la red solo utiliza IPv4 y no hay una demanda inmediata de migración a IPv6, ya que es más eficiente y económico continuar utilizando DHCPv4 para la gestión de direcciones IP.

- ***Tecnologías Utilizadas:***
  - *MPLS (Multiprotocol Label Switching): Esta tecnología se utiliza para interconectar los diferentes sitios, proporcionando una transmisión de datos eficiente y segura. MPLS permite la creación de caminos específicos para los paquetes de datos a través de la red, lo que mejora la eficiencia y la gestión del tráfico.*
  - *Ethernet 10Gbps: Estas conexiones de alta velocidad se utilizan entre los nodos principales y el Edificio CEA, garantizando un ancho de banda suficiente para soportar grandes volúmenes de tráfico de datos.*
  - *Switches Cisco: Los switches Cisco son fundamentales en la gestión del tráfico de red, proporcionando características avanzadas de conmutación y enrutamiento que aseguran la conectividad entre los distintos componentes de la red.*
  - *Wi-Fi y Redes Inalámbricas de Área Local (WLAN): Wi-Fi es una tecnología que permite a los dispositivos conectarse a internet y entre sí dentro de un área limitada utilizando ondas de radio.*
  - *OSPF: Es un protocolo de enrutamiento dinámico de estado de enlace que se utiliza para encontrar la mejor ruta para los datos a través de una red IP.*
  - *BGP: Protocolo de enrutamiento principal utilizado para intercambiar información de enrutamiento entre sistemas autónomos (AS) en Internet.*
  - *DNS: Protocolo que traduce nombres de dominio legibles por humanos en direcciones IPs utilizables por las computadoras.*
  - *VLAN: Tecnología que divide una red física en múltiples segmentos lógicos para mejorar la seguridad y la eficiencia del tráfico.*
  - *DHCP: Protocolo utilizado para asignar dinámicamente direcciones IPs y otros parámetros de configuración de red a dispositivos conectados a la red.*
  - *IDS/IPS: Sistemas que detectan y previenen intentos de intrusión en la red mediante análisis del tráfico.*

- ***Estándares Cumplidos:***

Estándares	***Descripción***
EIA/TIA 568 B	*Este estándar trata del cableado comercial para los productos y servicios de telecomunicaciones, en este caso para el cableado RJ45*
ANSI/TIA/EIA 607	*Este estándar es para realizar mantenimiento a las puestas a tierra del área o lugar de trabajo.*
IEEE805.11n	*Estándar el cual es una extensión del 802.11, permite una máxima transmisión de 600 Mbps*
IEEE 802.16	*Este estándar hace referencia al banda ancha que posee la conexión inalámbrica del banco.*
EIA/TIA 802.1Q	*Estándar del uso de Vlans IEEE 802.11 Wi-fi 802.1x Autenticación en redes LAN*
IEEE 802.12	*Acceso de Prioridad por demanda 100base VG-Any*
IEEE 802.3	*Ethernet*
IEEE 802.14	*Módems de cable*
LAN IEEE 802.10	*Seguridad de red*

- ***Especificaciones por Capa OSI:***

N°	***Capa***	***Estándares***	***Protocolo***	***Dispositivos***
1	***Física***	*IEEE 802.3*	*Ethernet*	*Cables de red, adaptadores de red, hubs, switches, routers*
2	***Enlace de datos***	*IEEE 802.11 (Wi-Fi), IEEE 802.15 (Bluetooth)*		*Switches, tarjetas de red*
3	***Red***	*IP (Internet Protocol), ICMP (Internet Control Message Protocol), MPLS (Multiprotocol Label Switching)*	*Routers*	*RIP, OSPF, BGP*
4	***Transporte***	*TCP (Transmission Control Protocol), UDP (User Datagram Protocol)*	*Puertos*	*Hosts, servidores*
5	***Sesión***	*TCP (establecimiento de sesiones), RTP (Real-time Transport Protocol)*		*Servidores de aplicaciones*
6	***Presentación***	*ASN.1 (Abstract Syntax Notation 1), XDR (External Data*		

		Representation)		
7	***Aplicación***	*HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol)*	*Navegadores web, clientes de correo electrónico, servidores web, servidores FTP*	*Servicios de red: Correo electrónico, transferencia de archivos, acceso a la web*

- ***Distribución de los Equipos:***

Firewall La Molina

Nro de dispositivos	***VLAN***	***Direc. Red***	***Máscara***	***1ra IP Usable***	***Última IP Usable***	***Broadcast***
254	*560*	*172.30.18.0*	*/24*	*172.30.18.1*	*172.30.18.254*	*172.30.18.255*
254	*570*	*172.30.19.0*	*/24*	*172.30.19.1*	*172.30.19.254*	*172.30.19.255*
254	*580*	*172.30.8.0*	*/24*	*172.30.8.1*	*172.30.8.254*	*172.30.8.255*

Inside

Nro de dispositivos	***VLAN***	***Direc. Red***	***Máscara***	***1ra IP Usable***	***Última IP Usable***	***Broadcast***
510	*500*	*172.30.10.0*	*/23*	*172.30.10.1*	*172.30.11.254*	*172.30.11.255*
1022	*550*	*172.30.4.0*	*/22*	*172.30.4.1*	*172.30.7.254*	*172.30.7.255*
254	*836*	*172.30.252.0*	*/24*	*172.30.252.1*	*172.30.252.254*	*172.30.252.255*
30	*860*	*172.30.22.0*	*/27*	*172.30.22.1*	*172.30.22.30*	*172.30.22.31*
254	*1007*	*172.30.147.0*	*/24*	*172.30.147.1*	*172.30.147.254*	*172.30.147.255*
30	*1037*	*172.30.132.0*	*/27*	*172.30.132.1*	*172.30.132.30*	*172.30.132.31*
14	*1050*	*172.30.188.0*	*/28*	*172.30.188.1*	*172.30.188.14*	*172.30.132*
14	*1051*	*172.30.188.16*	*/28*	*172.30.188.17*	*172.30.188.30*	*172.30.188.15*
14	*1052*	*172.30.188.32*	*/28*	*172.30.188.33*	*172.30.188.46*	*172.30.188.61*
14	*1053*	*172.30.188.48*	*/28*	*172.30.188.49*	*172.30.188.62*	*172.30.188.63*
14	*1054*	*172.30.188.64*	*/28*	*172.30.188.65*	*172.30.188.78*	*172.30.188.79*

Outside

Nro de dispositivos	*Direc. Red*	*Máscara*	*1ra IP Usable*	*Última IP Usable*	*Broadcast*
254	*192.168.219.0*	*/24*	*192.168.219.1*	*192.168.219.254*	*192.168.219.255*
254	*192.168.222.0*	*/24*	*192.168.222.1*	*192.168.222.254*	*192.168.222.255*
254	*192.169.225.0*	*/24*	*192.169.225.1*	*192.169.225.254*	*192.169.225.255*
254	*10.48.132.0*	*/24*	*10.48.132.1*	*10.48.132.54*	*10.48.132.255*
126	*201.234.60.128*	*/24*	*201.234.60.129*	*201.234.60.254*	*201.234.60.255*

FireWall Chorrillos

Nro de dispositivos	*VLAN*	*Direc. Red*	*Máscara*	*1ra IP Usable*	*Última IP Usable*	*Broadcast*
254	*560*	*172.30.18.0*	*/24*	*172.30.18.1*	*172.30.18.254*	*172.30.18.255*
254	*570*	*172.30.19.0*	*/24*	*172.30.19.1*	*172.30.19.254*	*172.30.19.255*
254	*580*	*172.30.8.0*	*/24*	*172.30.8.1*	*172.30.8.254*	*172.30.8.255*

Inside

Nro de dispositivos	*VLAN*	*Direc. Red*	*Máscara*	*1ra IP Usable*	*Última IP Usable*	*Broadcast*
510	*500*	*172.30.10.0*	*/23*	*172.30.10.1*	*172.30.11.254*	*172.30.11.255*
254	*521*	*172.30.12.0*	*/24*	*172.30.12.1*	*172.30.12.254*	*172.30.12.255*
254	*523*	*172.30.13.0*	*/24*	*172.30.13.1*	*172.30.13.254*	*172.30.13.255*
254	*530*	*172.30.15.0*	*/24*	*172.30.15.1*	*172.30.15.254*	*172.30.15.255*
254	*540*	*172.30.254.0*	*/24*	*172.30.254.1*	*172.30.254.254*	*172.30.254.255*
1022	*550*	*172.30.4.0*	*/22*	*172.30.4.1*	*172.30.7.254*	*172.30.7.255*
30	*815*	*172.30.21.0*	*/27*	*172.30.21.1*	*172.30.21.30*	*172.30.21.31*
30	*816*	*172.30.21.32*	*/27*	*172.30.21.33*	*172.30.21.62*	*172.30.21.63*
62	*820*	*172.30.180.0*	*/26*	*172.30.180.1*	*172.30.180.62*	*172.30.180.63*
254	*836*	*172.30.25.0*	*/24*	*172.30.25.1*	*172.30.25.254*	*172.30.25.255*

30	*860*	*172.30.22.0*	*/27*	*172.30.22.1*	*172.30.22.30*	*172.30.22.31*
254	*1007*	*172.30.147.0*	*/24*	*172.30.147.1*	*172.30.147.254*	*172.30.147.255*
30	*1037*	*172.30.132.0*	*/27*	*172.30.132.1*	*172.30.132.30*	*172.30.132.31*
14	*1050*	*172.30.188.0*	*/28*	*172.30.188.1*	*172.30.188.14*	*172.30.188.15*
14	*1051*	*172.30.188.16*	*/28*	*172.30.188.17*	*172.30.188.30*	*172.30.188.31*
14	*1052*	*172.30.188.32*	*/28*	*172.30.188.33*	*172.30.188.46*	*172.30.188.47*
14	*1053*	*172.30.188.48*	*/28*	*172.30.188.49*	*172.30.188.62*	*172.30.188.63*
14	*1054*	*172.30.188.64*	*/28*	*172.30.188.65*	*172.30.188.78*	*172.30.188.79*

Outside

Nro de dispositivos	***Direc. Red***	***Máscara***	***1ra IP Usable***	***Última IP Usable***	***Broadcast***
254	*192.168.219.0*	*/24*	*192.168.219.1*	*192.168.219.254*	*192.168.219.255*
254	*192.168.220.0*	*/24*	*192.168.220.1*	*192.168.220.254*	*192.168.220.255*
2	*200.7.188.36*	*/30*	*200.7.188.37*	*200.7.188.38*	*200.7.188.39*
254	*192.168.225.0*	*/24*	*192.168.225.1*	*192.168.225.254*	*192.168.225.255*
254	*10.48.132.0*	*/24*	*10.48.132.1*	*10.48.132.254*	*10.48.132.255*

BACKBONE LAYER TIVIT/PACÍFICO

Características de la Arquitectura de Red

- ***Confiabilidad:***
  - *La red utiliza equipos Cisco Nexus, conocidos por su alta fiabilidad y rendimiento. Estos equipos proporcionan una plataforma sólida y estable para la gestión del tráfico de red, asegurando que los datos se transmitan de manera eficiente y sin interrupciones.*

- ***Redundancia y Tolerancia a Fallos:***
  La arquitectura de la red incluye múltiples caminos y redundancias, como enlaces duales de 10G, para asegurar la continuidad del servicio en caso de fallos en algún componente. Esto garantiza que si un enlace falla, el tráfico puede ser redirigido automáticamente a través de un camino alternativo, minimizando el impacto en los usuarios. Se utilizan Cirion, Claro, TDP, Winempresas como proveedores de conectividad upstream para garantizar que, si un proveedor falla, el tráfico pueda ser redirigido a otro sin interrupciones.
  Hay protocolos de enrutamiento dinámico que seleccionan automáticamente la mejor ruta para el tráfico, tomando en cuenta la disponibilidad y el rendimiento de los enlaces. Se utilizan routers redundantes en configuraciones de alta disponibilidad, de modo que si un router falla, el otro pueda

asumir el tráfico sin interrupciones. Hay HSRP para garantizar una transición rápida y automática a un router de respaldo en caso de fallo del router principal.

- ***Enfriamiento:***
  - *Configuración N+1 para Enfriadores y CRACs: Se deben tener unidades de refrigeración adicionales para cubrir fallos de cualquier unidad individual.*
  - *Monitoreo Continuo: Sistemas de monitoreo que detecten problemas de temperatura y humedad, activando sistemas de respaldo automáticamente.*
- ***Red de Suministro de Energía:***
  - *Dos Caminos Independientes de Energía: La infraestructura eléctrica debe estar dividida en al menos dos vías independientes y redundantes, de manera que si una falla, la otra mantenga el suministro.*

- ***Infraestructura de Redundancia***
  - ***Conectividad de Red:***
    - *Conexiones Redundantes: Múltiples conexiones a Internet de diferentes proveedores para asegurar redundancia de red.*
    - *Equipos de Red Redundantes: Routers, switches y firewalls configurados en alta disponibilidad (HA) y con caminos de red alternativos.*

- ***Mantenimiento y Pruebas Periódicas***
  - ***Pruebas de Recuperación de Desastres (DR):***
    - *Simulacros Regulares: Ejecución de simulacros de recuperación de desastres para asegurar que todos los sistemas y personal están preparados ante una emergencia real.*
    - *Verificación de procedimientos: Asegurarse de que todos los procedimientos de recuperación y los planes de contingencia estén actualizados y verificados.*
  - ***Mantenimiento Preventivo:***
    - *Calendario de Mantenimiento: Se cuenta con un programa de mantenimiento preventivo regular para todos los sistemas críticos.*
    - *Inspecciones Periódicas: Inspecciones rutinarias para identificar y corregir posibles puntos de fallo antes de que se conviertan en problemas.*

- ***Escalabilidad:***
  - *La red está diseñada para ser escalable, permitiendo la adición de nuevos nodos y enlaces de alta capacidad conforme sea necesario. Esto asegura que la infraestructura pueda crecer y adaptarse a las necesidades cambiantes de la organización.*

- ***Alta Disponibilidad:***
  - *Se utilizan enlaces duales de 10 Gbps entre los centros de datos de Pacífico y Tivit, así como entre los centros de datos y los proveedores de conectividad upstream. Esto garantiza que el tráfico de red pueda seguir fluyendo incluso si uno de los enlaces falla. Se implementan switches, routers, firewalls y servidores redundantes para garantizar que la red pueda seguir funcionando incluso si uno de los dispositivos falla. HSRP se utiliza para garantizar una transición rápida y automática a un router de respaldo en caso de fallo del router principal. BGP se utiliza para seleccionar la mejor ruta para el tráfico de red, tomando en cuenta la disponibilidad y el rendimiento de los enlaces. VRRP se utiliza para garantizar una transición rápida y automática a un servidor virtual de enrutamiento en caso de fallo del servidor principal.*

- ***Seguridad:***
    - *Se tienen implementadas medidas de seguridad en los enlaces y dispositivos para proteger la integridad y confidencialidad de los datos. Esto incluye el uso de firewalls, sistemas de detección de intrusiones (IDS), y la encriptación de datos en tránsito. El firewall que se utiliza es el FirePower el cual combina firewall tradicional con capacidades avanzadas de seguridad, como inspección de paquetes en profundidad, filtrado de contenido web, detección y prevención de intrusiones (IDS/IPS), y protección contra malware avanzado. El firewall principalmente opera en la Capa 7. A diferencia de los firewalls de capa 4 (como los firewalls de estado que operan en TCP/UDP), un firewall de capa 7 puede examinar el contenido completo del paquete de datos, incluyendo encabezados y, en algunos casos, datos de la aplicación. Puede aplicar reglas específicas basadas no solo en direcciones IP, puertos y protocolos, sino también en el contenido real de los datos. Por ejemplo, puede bloquear o permitir el acceso a ciertos sitios web o servicios según palabras clave en el contenido de una página web.*
    - *La empresa utiliza una suite de seguridad integral proporcionada por McAfee que incluye antivirus y protección antimalware. El software antivirus de McAfee monitorea continuamente todos los archivos y actividades en los dispositivos protegidos, detectando y bloqueando amenazas en tiempo real.*
    - *En cuanto a la Prevención de Pérdida de Datos (DLP - Data Loss Prevention), McAfee DLP supervisa el flujo de datos dentro y fuera de la red, identificando y protegiendo información sensible según las políticas de la empresa.*
    - *La Encriptación de Discos (Drive Encryption) ofrecida por McAfee garantiza que todos los datos almacenados en los discos duros estén cifrados, protegiendo la información en caso de pérdida o robo del dispositivo.*
    - *Se hace uso de SIEM (Security Information and Event Management) y plataformas USM (Unified Security Management) los cuales están estrechamente relacionados, ya que los USM incorporan las capacidades de SIEM como parte de su funcionalidad central, ofreciendo una solución más completa y unificada. Los USM Servers actúan como el cerebro del sistema, integrando capacidades de recolección, análisis, correlación, y generación de alertas de seguridad típicas de un SIEM, mientras que los USM Sensors se despliegan en la red para recoger datos de seguridad y enviarlos al servidor. Además de las capacidades de SIEM, los USM proporcionan herramientas adicionales como detección de intrusos (IDS), evaluación de vulnerabilidades, gestión de activos y respuesta a incidentes, permitiendo una gestión integral de la seguridad de la red desde una única plataforma.*
    - *La empresa cuenta con IPS (Intrusion Prevention System), el cual es un sistema de seguridad de red diseñado para detectar y prevenir amenazas en tiempo real, actuando de manera proactiva para bloquear actividades sospechosas mediante el análisis continuo del tráfico de red. Cuando se despliega en "modo SPAN" (Switched Port Analyzer), el tráfico de una o más interfaces del switch se copia a otra interfaz específica para su análisis, lo que permite al IPS (o a otros dispositivos de monitoreo) analizar el tráfico sin interrumpir su flujo normal. Este método es crucial para proporcionar una defensa activa contra amenazas mientras se mantiene la visibilidad y el control detallado del tráfico de red, facilitando la detección y mitigación de actividades maliciosas de manera eficiente.*

- ***Documentación y Procedimientos***
    - *Manuales y Procedimientos: Documentación exhaustiva de todos los procedimientos operativos estándar (SOP), incluyendo pasos a seguir en caso de emergencias.*
    - *Entrenamiento del personal: Capacitación continua del personal en protocolos de emergencia y manejo de equipos críticos.*

Nomenclatura de Rotulación y Direcciones IP'S

- ***Direcciones IP:***
  - *Cada datacenter y nodo de la red tiene asignadas direcciones IP específicas, asegurando una gestión organizada y eficiente del tráfico. Esto facilita la identificación y resolución de problemas, así como la gestión del tráfico de red.*
- ***Rotulación:***
  - *Los equipos y enlaces están claramente rotulados para facilitar la identificación y gestión de la infraestructura de red. Esto es crucial para el mantenimiento y la expansión de la red, permitiendo a los técnicos identificar rápidamente los componentes y sus conexiones.*
  - *Servidor 1 (Etiqueta Física en el Servidor):*
    Etiqueta:
    ID del Servidor: SRV-001
    Nombre del Servidor: WEB-SERVER-01
    Función: Servidor Web
    Dirección IP: 192.168.1.10
    Número de Serie: ABC12345XYZ
    Ubicación: Rack 3, U5
    Responsable: John Doe (IT Manager)

- ***Código de colores de cableado***
  - *Cables de Datos (Ethernet, Fiber, etc.):*
    - *Azul: Conexiones estándar de red (LAN).*
    - *Verde: Conexiones de red administrativa o de gestión.*
    - *Amarillo: Conexiones a VLAN específicas o segmentaciones de red.*
    - *Naranja: Conexiones de red de alta velocidad.*
  - *Cables de Energía:*
    - *Rojo: Conexiones a la Unidad de Distribución de Energía (PDU) principal.*
    - *Negro: Conexiones a la fuente de alimentación de respaldo (UPS).*
    - *Blanco: Conexiones a equipos de bajo consumo o especializados.*
    - *Marrón: Conexiones de energía de alta capacidad.*
    - *Amarillo/Verde: Tierra o conexiones a tierra (grounding).*
  - *Cables de Fibra Óptica:*
    - *Amarillo: Monomodo (Single-mode) de largo alcance.*
    - *Naranja: Multimodo (Multimode) de corto alcance (OM1, OM2).*
    - *Aqua: Multimodo de alto rendimiento (OM3, OM4).*
    - *Rosa: Conexiones de fibra óptica a redes de almacenamiento (SAN).*
  - *Cables de Consola (Management):*
    - *Púrpura: Conexiones a puertos de consola para gestión de equipos.*
    - *Verde Claro: Conexiones seriales o RS-232.*
    - *Cables de Interconexión (Inter-rack):*
    - *Rojo/Blanco: Interconexiones entre racks dentro del mismo data center.*
    - *Azul/Blanco: Interconexiones entre diferentes zonas del data center.*

DIAGRAMA DE SEGMENTACIÓN DE REDES

Descripción General

- ***Objetivo Principal:***
  - *La segmentación de redes tiene como objetivo principal asegurar una gestión eficiente y segura del tráfico de red, separando las diferentes áreas y aplicaciones para minimizar el riesgo de fallos y mejorar la seguridad.*
- ***Segmentación de Redes:***

- *La red se segmenta en diferentes zonas, como producción (Chorrillos), contingencia (La Molina), y varias DMZ (zonas desmilitarizadas) para servicios específicos como conexiones de proveedores, SOC (Security Operations Center), y portales externos.*

Características de la Segmentación

- ***Conectividad y Seguridad:***
  - *Las diferentes zonas realizan uso de mediante firewalls y sistemas de seguridad que controlan y monitorean el tráfico de datos, asegurando que solo el tráfico autorizado pueda pasar entre las zonas.*
- ***Dirección IP y Enrutamiento:***
  - *Las direcciones IP están asignadas de manera estructurada para cada zona y servicio, facilitando la gestión y el enrutamiento del tráfico.*

DISEÑO FÍSICO:

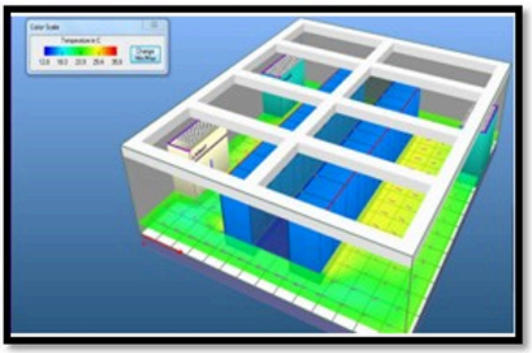


Ilustración 1. Diseño del Plano de Plano de Flujo de Temperaturas.

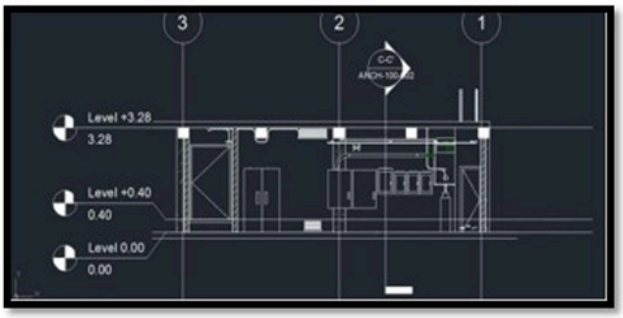


Ilustración 2. Corte en bloques del sistema eléctrico.

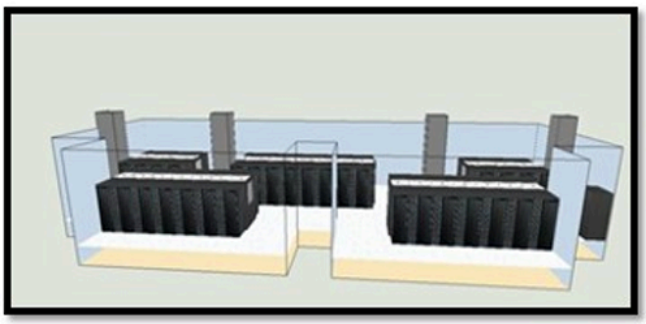


Ilustración 3. Diseño del Plano Lateral

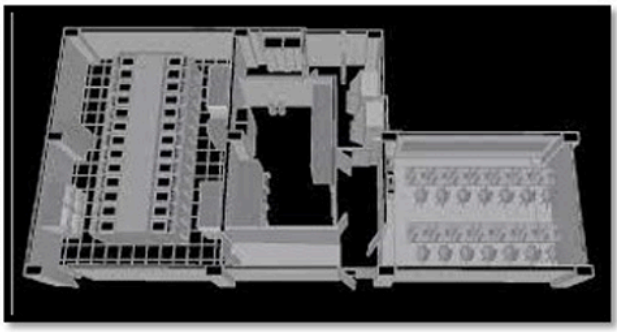


Ilustración 4. Vista de planta del DataCenter

Tipo de Suelo

Suelo Elevado (Raised Floor):

- *Ventilación y Enfriamiento: Permite la circulación de aire frío desde el subsuelo para enfriar los equipos.*
- *Cableado: Facilita la gestión de cables, evitando enredos y mejorando la organización.*
- *Accesibilidad: Permite un acceso rápido y fácil a los cables y sistemas de infraestructura sin necesidad de interrumpir el funcionamiento de los equipos.*
- *Material: Generalmente se utilizan paneles de acero o aluminio con acabado antideslizante y antiestático para evitar descargas electrostáticas que puedan dañar los equipos.*

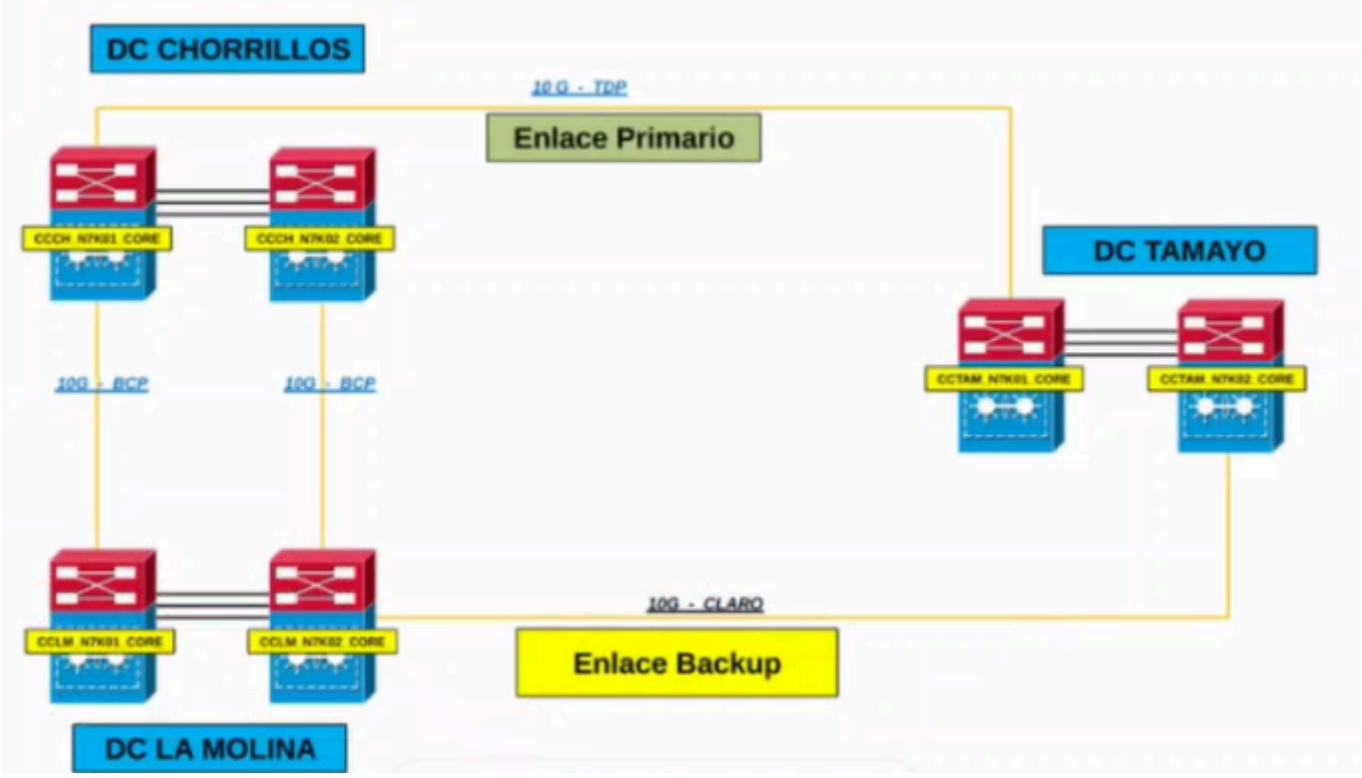
Tipo de Techo

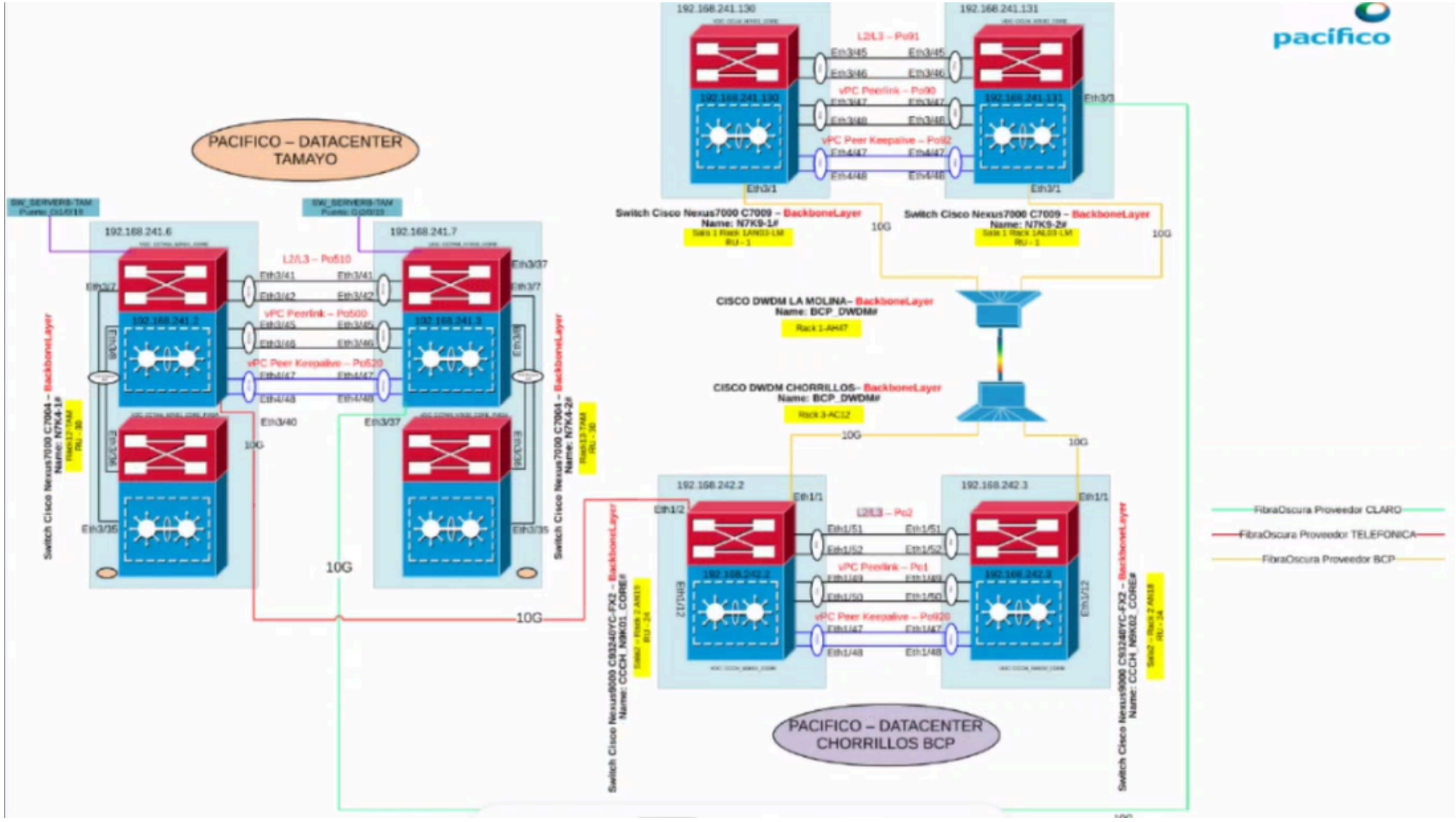
Techo Falso (Drop Ceiling):

- *Gestión de Aire: Utilizado para el retorno de aire caliente y para albergar conductos de aire acondicionado.*
- *Acceso a Sistemas: Facilita el acceso a sistemas eléctricos, de iluminación y a tuberías sin interferir con la operación del data center.*
- *Material: Generalmente se usan paneles de fibra mineral o metal perforado para facilitar la dispersión del aire y mejorar la acústica.*

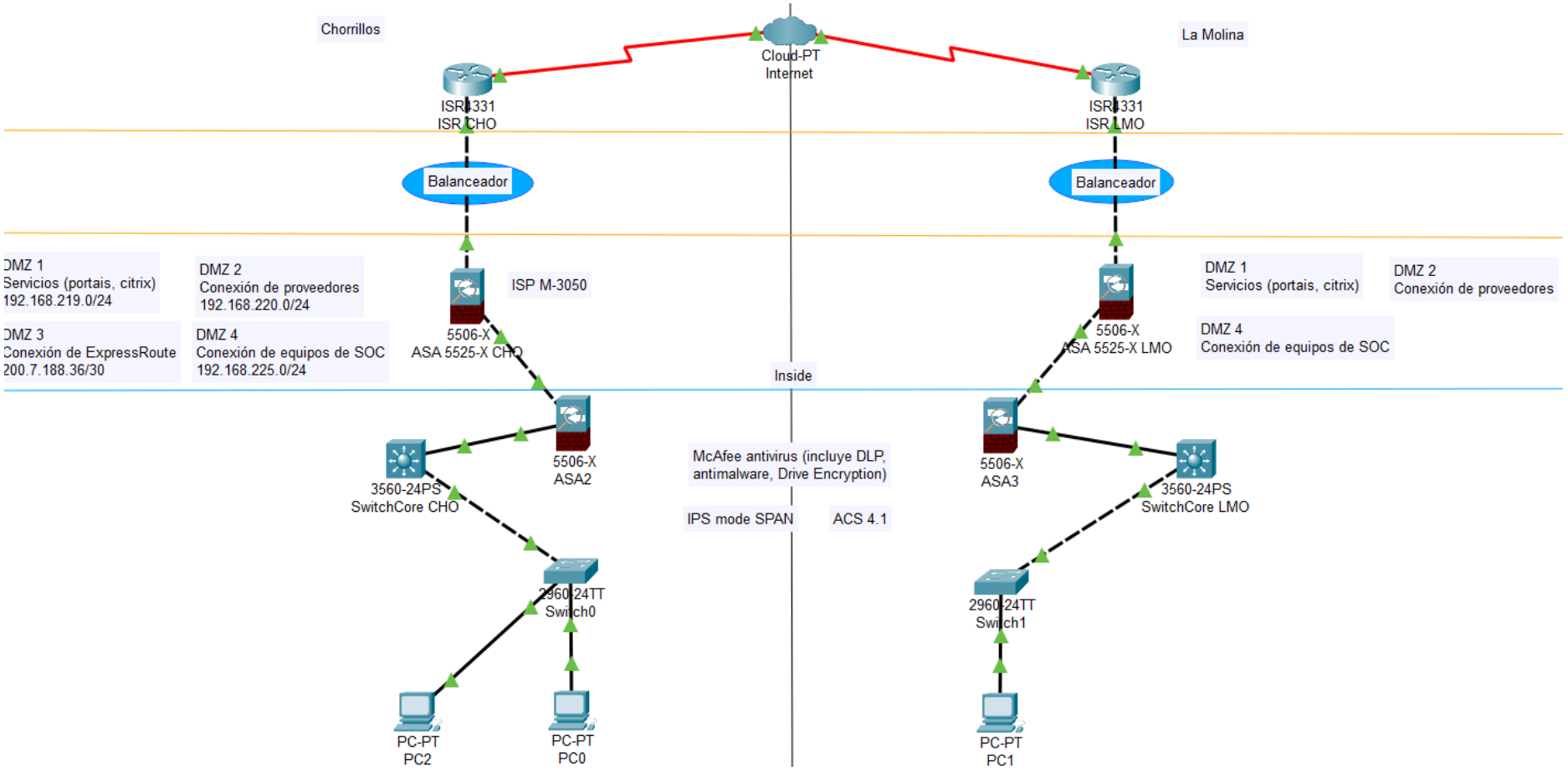
DISEÑO LÓGICO:

- *Diagrama de red del DataCenter:*

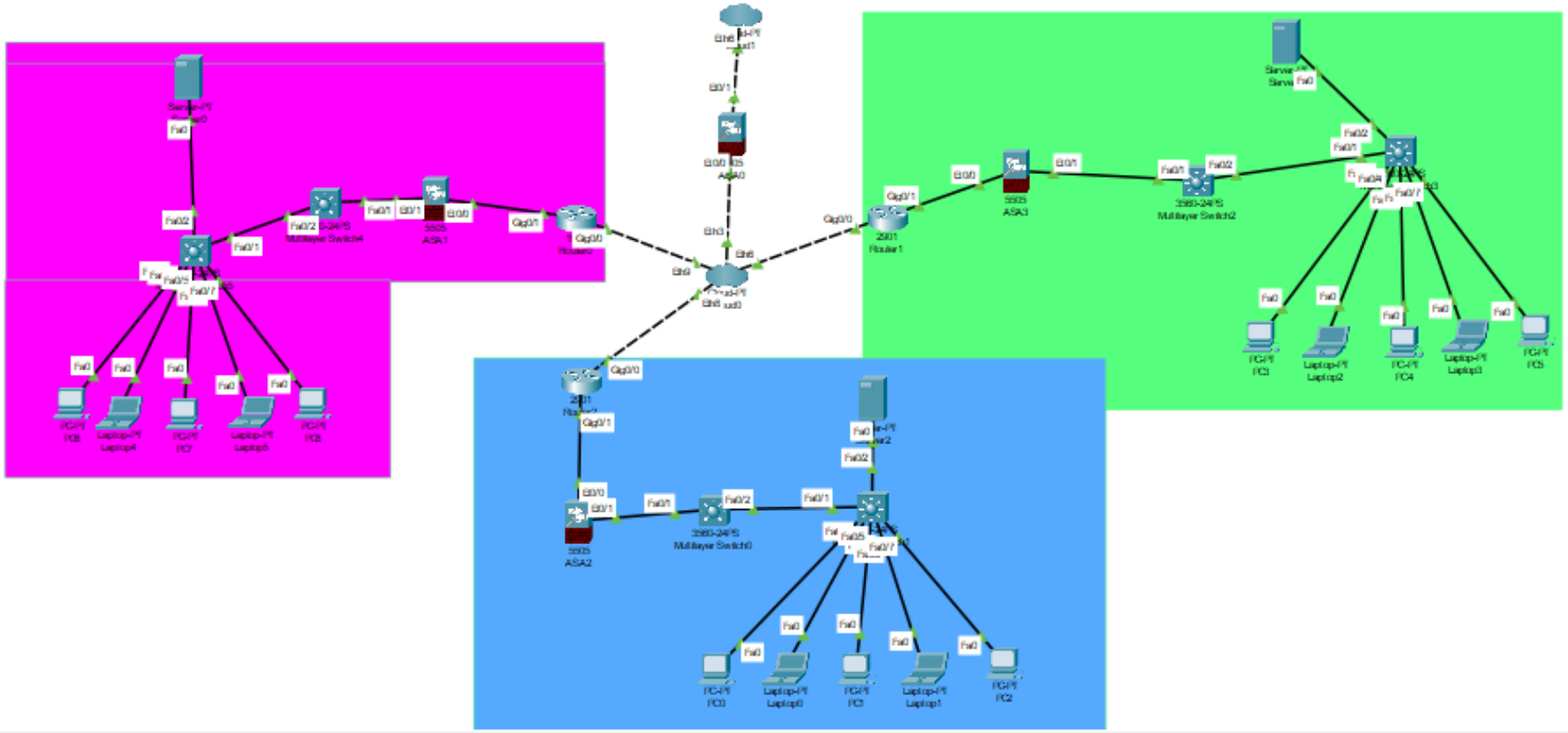



PACIFICO – DATACENTER TAMAYO
PACIFICO – DATACENTER CHORRILLOS BCP
pacífico
192.168.241.130
192.168.241.131
192.168.241.6
192.168.241.7
192.168.242.2
192.168.242.3
Switch Cisco Nexus7000 C7009 – BackboneLayer Name: N7K9-1#
Switch Cisco Nexus7000 C7009 – BackboneLayer Name: N7K9-2#
CISCO DWDM LA MOLINA– BackboneLayer Name: BCP_DWDM#
CISCO DWDM CHORRILLOS– BackboneLayer Name: BCP_DWDM#
L2/L3 – Po91
vPC Peerlink – Po90
vPC Peer Keepalive – Po92
L2/L3 – Po510
vPC Peerlink – Po500
vPC Peer Keepalive – Po520
L2/L3 – Po2
vPC Peerlink – Po1
vPC Peer Keepalive – Po20
10G
FibraOscura Proveedor CLARO
FibraOscura Proveedor TELEFONICA
FibraOscura Proveedor BCP

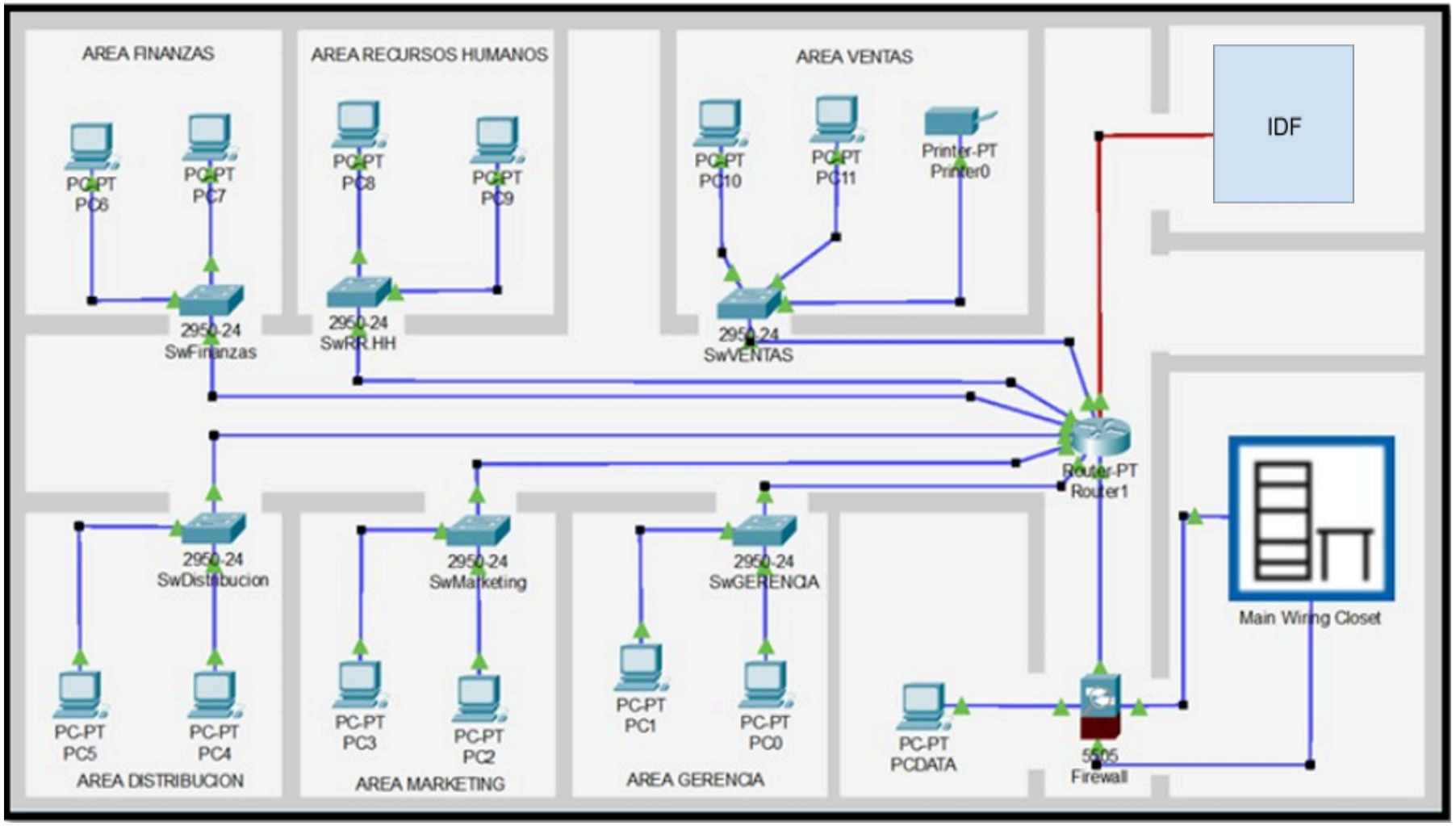
- *Diagrama de conexión inside-outside de la red empresarial*

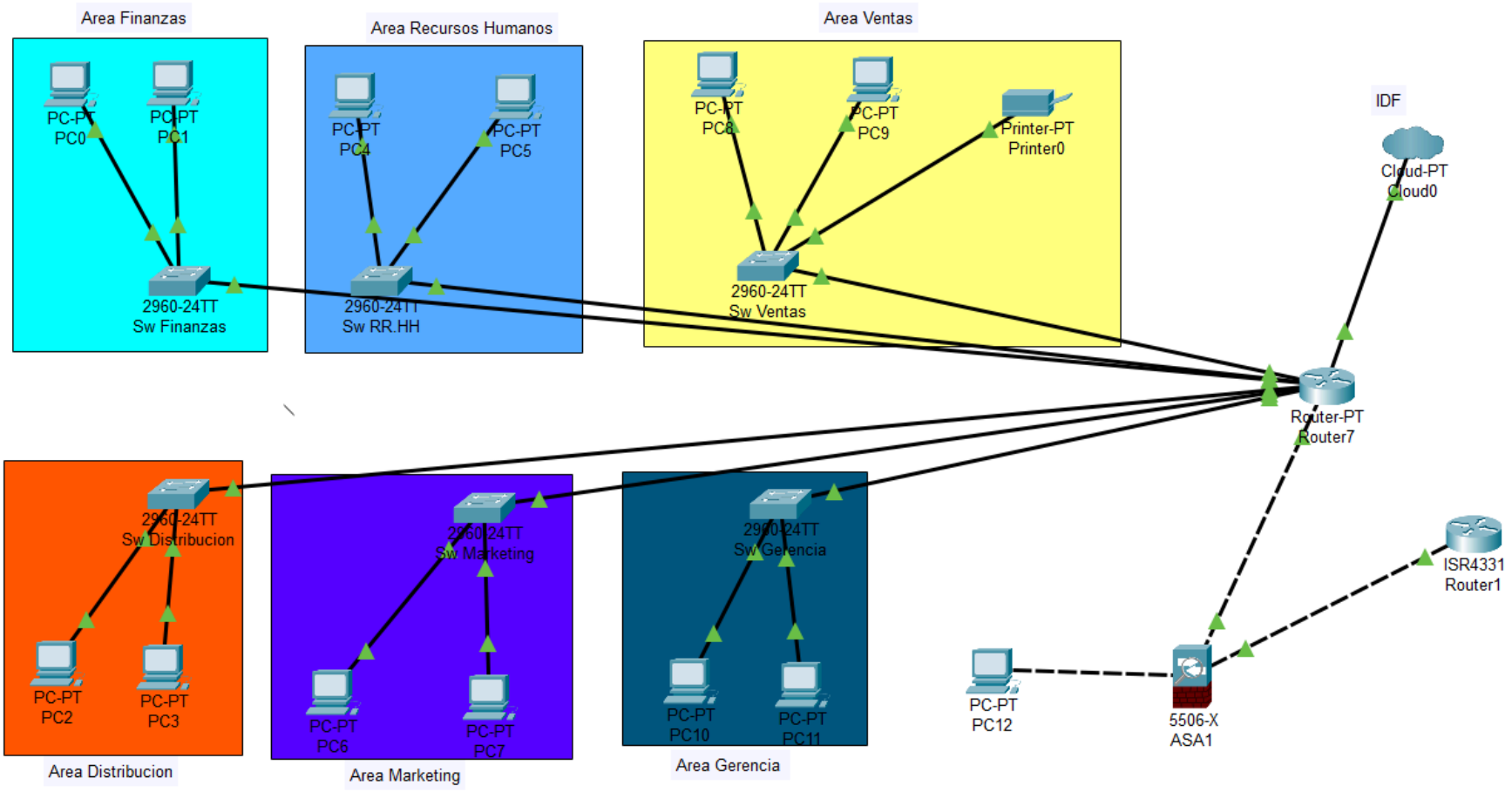


- *Diagrama de Datacenter Sedes:*



- *Distribución de red para una oficina:*




Area Finanzas
PC-PT PC0
PC-PT PC1
2960-24TT Sw Finanzas
Area Recursos Humanos
PC-PT PC4
PC-PT PC5
2960-24TT Sw RR.HH
Area Ventas
PC-PT PC8
PC-PT PC9
Printer-PT Printer0
2960-24TT Sw Ventas
IDF
Cloud-PT Cloud0
Router-PT Router7
2960-24TT Sw Distribucion
PC-PT PC2
PC-PT PC3
Area Distribucion
2960-24TT Sw Marketing
PC-PT PC6
PC-PT PC7
Area Marketing
2960-24TT Sw Gerencia
PC-PT PC10
PC-PT PC11
Area Gerencia
PC-PT PC12
5506-X ASA1
ISR4331 Router1

POZOS A TIERRA:

Cada sede posee un sótano en el cual hay un pozo a tierra para mejorar la seguridad eléctrica al dirigir corrientes no deseadas (como las causadas por fallas de línea o picos de voltaje) hacia la tierra de manera controlada y segura, en lugar de que circulen por partes metálicas accesibles o estructuras cercanas. Esto evita daños en equipos electrónicos y eléctricos al proporcionar un camino de baja resistencia para las corrientes eléctricas, especialmente durante sobretensiones, cortocircuitos o descargas atmosféricas.

TABLAS DE DISPOSITIVOS DE USUARIO FINAL, INTERMEDIARIOS:

NOMBRE	*DESCRIPCIÓN*	*MANTENIMIENTO*
Computadoras	*Dispositivos electrónicos utilizados para procesar y almacenar información.*	*Cada 6 meses*
Impresoras	*Dispositivos que reproducen documentos y gráficos en papel.*	*Cada 13 meses*
Teléfonos IP	*Teléfonos que utilizan el protocolo de Internet para transmitir voz.*	*Cada 6 meses*
Routers	*Dispositivos que encaminan paquetes de datos entre redes diferentes.*	*Cada 6 meses*
Switches	*Dispositivos de red que conectan múltiples dispositivos dentro de la misma red.*	*Cada 12 meses*
Switches de Capa 3	*Switches que pueden realizar enrutamiento entre diferentes subredes.*	*Cada 6 meses*

MEDIDAS DE SEGURIDAD LÓGICAS Y FÍSICAS:

- ***Físicas:***
  - ***Control de acceso físico:***
    Uso de tarjetas de acceso, biometría (huellas dactilares, reconocimiento facial) y códigos PIN para restringir la entrada a áreas críticas como salas de servidores y centros de datos.
  - ***Vigilancia y monitoreo:***
    Instalación de cámaras de seguridad (CCTV) para monitorear continuamente las áreas sensibles. Estas cámaras suelen estar conectadas a un sistema de vigilancia central.
  - ***Guardias de seguridad:***
    Presencia de guardias de seguridad en el perímetro y en las entradas principales para controlar y verificar el acceso de personas no autorizadas.
  - ***Sistemas de alarma:***
    Sistemas de alarma que se activan en caso de intentos de acceso no autorizado, intrusión o emergencias como incendios.
  - ***Bastidores y gabinetes cerrados:***

Uso de racks y gabinetes con cerraduras para asegurar los equipos de red y servidores, previniendo el acceso no autorizado y el robo de hardware.

- ***Control de ambiente:***
  Sistemas de climatización (HVAC) para mantener una temperatura y humedad adecuadas en las salas de servidores, previniendo el sobrecalentamiento y asegurando el buen funcionamiento de los equipos. Sistemas de detección y extinción de incendios (rociadores automáticos, extinguidores) adecuados para entornos de centros de datos.
- ***Redundancia de energía:***
  Uso de sistemas de alimentación ininterrumpida (UPS) y generadores de respaldo para asegurar la continuidad del suministro eléctrico en caso de cortes de energía.
- ***Cableado organizado y protegido:***
  Gestión adecuada del cableado para evitar desorden y minimizar el riesgo de accidentes. Uso de canaletas y etiquetas para facilitar la identificación y mantenimiento del cableado.
- ***Registros de acceso:***
  Mantenimiento de registros detallados de quién entra y sale de las áreas críticas, incluyendo fechas, horas y propósito del acceso.
- ***Sistemas de Detección y Extinción de Incendios:***
  - *Detectores de Humo y Calor: Instalación de detectores de humo y calor en todas las áreas críticas, especialmente en las salas de servidores y centros de datos.*
  - *Sistemas de Supresión de Incendios: Uso de sistemas de extinción automática como rociadores de agua, gases inertes (FM-200, Novec 1230) o sistemas de supresión de incendios con CO_2 que no dañen el equipo electrónico.*
  - *Extintores Portátiles: Colocación de extintores de incendios en puntos estratégicos, accesibles y claramente señalizados.*
- ***Redundancia y Recuperación de Datos:***
  - *Respaldos de Datos (Backups): Implementación de políticas de backup regular de todos los datos críticos. Almacenamiento de copias de seguridad en ubicaciones geográficas diferentes (off-site) para proteger contra desastres locales.*
  - *Sitios de Recuperación (Disaster Recovery Sites): Configuración de sitios de recuperación que pueden asumir las operaciones en caso de que la ubicación principal se vea afectada. Estos sitios deben estar equipados con todo el hardware y software necesario para continuar con las operaciones críticas.*

- ***Lógicas:***
  - ***Enrutamiento Estático:*** *Es un método manual para configurar rutas en una tabla de enrutamiento de un router. Se utiliza en los IDFs de cada torre que se encuentran por piso para tener controlados las redes principales de cada piso de la empresa.*
  - ***Firewalls (FirePower):***
    Se utilizan en 5 zonas (Inside, Outside, Dmz1, Dmz3) configuradas en el firewall y tienen un firewall en cada uno de sus datacenters
  - ***Sistemas de prevención de intrusiones (IPS M-3050 y IPS M-6050):***
    Los IPS se utilizan para detectar y prevenir actividades maliciosas dentro de la red. El IPS M-3050 está ubicado antes del firewall principal para inspeccionar el tráfico que entra a la red, mientras que el IPS M-6050 está en modo SPAN para monitorear el tráfico interno.
  - ***Redes DMZ (Zonas Desmilitarizadas)***
    Las DMZ (DMZ1, DMZ2, DMZ3, DMZ4) se utilizan para aislar los servicios que necesitan ser accesibles desde el exterior (por ejemplo, portales, citrix, conexión de proveedores, conexión de equipos de SOC) del resto de la red interna.
  - ***Antivirus y cifrado***

La red utiliza McAfee Antivirus con capacidades de prevención de pérdida de datos (DLP) y cifrado de disco completo para proteger contra malware y asegurar la confidencialidad de los datos.

- ***Control de acceso (ACS 4.1 y AD 2012)***
  El servidor ACS 4.1 proporciona control de acceso a la red, asegurando que solo los dispositivos y usuarios autorizados puedan acceder a la misma. Además, se utiliza Active Directory (AD 2012) para gestionar las identidades y permisos de los usuarios.
- ***Antispam:***
  Se emplean soluciones antispam (Antispam pvstmg-in y Antispam pvstmg-out) para proteger la red contra correos electrónicos no deseados y potencialmente dañinos.
- ***Segmentación de VLANs***
  La red está segmentada en múltiples VLANs, lo cual ayuda a contener el tráfico y mejorar la seguridad aislando diferentes tipos de tráfico en segmentos separados.
- ***Conexiones de respaldo y contingencia***
  La existencia de sitios de producción y contingencia (Chorrillos y La Molina) conectados a través de un backbone de nivel 3 con capacidad de 256 Mbps, asegura la disponibilidad y continuidad del servicio en caso de fallos.

CONCLUSIONES:

La red de Seguros Pacífico está diseñada para ser robusta y altamente disponible, con configuraciones redundantes y mecanismos de conmutación por error que aseguran la continuidad del servicio en caso de fallos. Se implementan múltiples capas de seguridad, incluyendo firewalls y segmentación mediante VLANs, lo que protege la red de accesos no autorizados y ataques, garantizando la confidencialidad e integridad de los datos. La infraestructura de red cumple con importantes estándares internacionales de telecomunicaciones (TIA, ANSI, EIA, ISO/IEC), lo que garantiza que la red esté construida y gestionada siguiendo las mejores prácticas de la industria.

La red está diseñada para ser fácilmente gestionable y monitoreada, con un esquema de rotulación y direccionamiento de IP's que facilita la identificación y administración de dispositivos, mejorando la eficiencia operativa y la capacidad de respuesta ante problemas. La implementación de mecanismos de tolerancia a fallos asegura que la red pueda soportar interrupciones sin pérdida de servicio, proporcionando una experiencia continua y confiable para los usuarios y sistemas críticos de la empresa. La adopción de tecnologías avanzadas como OSPF, BGP, y EtherChannel demuestra el compromiso de Seguros Pacífico con la innovación, garantizando una infraestructura de red moderna y eficiente.

SUGERENCIAS:

La Infraestructura de Red de Pacífico Seguros ya incluye diversos elementos clave para el funcionamiento eficiente y seguro de su red, como son:

1. ***VLANs (Virtual LANs)**: Permiten segmentar lógicamente la red, lo que mejora la seguridad y facilita el manejo del tráfico al separar distintos tipos de tráfico en diferentes segmentos.*
2. ***Subnetting**: Ayuda a organizar y gestionar la red al dividir un gran bloque de direcciones IP en bloques más pequeños. Esto facilita el control y la asignación de direcciones IP.*
3. ***VTP (VLAN Trunking Protocol)**: Simplifica la gestión de VLANs en toda la red de switches, ya que permite propagar automáticamente la configuración de VLANs entre los switches.*
4. ***DTP (Dynamic Trunking Protocol)**: Automatiza la configuración de enlaces troncales, permitiendo la transmisión de múltiples VLANs a través de un solo enlace.*
5. ***Inter-VLAN Routing**: Permite la comunicación entre diferentes VLANs, lo cual es esencial para que los dispositivos en distintos segmentos puedan interactuar.*

6. ***STP (Spanning Tree Protocol)****: Previene bucles de red, asegurando que haya una única ruta activa entre cualquier par de dispositivos, lo que evita problemas de redundancia y mejora la estabilidad de la red.*
7. ***HSRP (Hot Standby Router Protocol)****: Permite que dos o más routers trabajen juntos en un grupo, donde uno actúa como el router activo principal y los otros están en espera para tomar el control si el router activo falla, asegurando así la alta disponibilidad de la red.*
8. ***DHCP (Dynamic Host Configuration Protocol)****: Simplifica la asignación de direcciones IP, reduciendo el trabajo manual y minimizando errores en la configuración de IPs.*

Además, la infraestructura física del data center cumple con todos los estándares requeridos, asegurando un entorno adecuado para la operación de la red.

Con base en esto, podemos concluir que la infraestructura de Pacífico Seguros ya incluye todos los elementos y estándares que hemos aprendido en el curso de Redes II. Por lo tanto, no es necesario sugerir mejoras adicionales en su infraestructura lógica y/o física.

Automatización de la Gestión de Red (Sugerencia fuera de lo aprendido durante el semestre)*:*

- *Integrar soluciones de automatización para la configuración y monitoreo de la red, utilizando herramientas como Ansible o Puppet, lo que puede reducir el tiempo de inactividad y mejorar la eficiencia operativa.*

Beneficios de la Automatización de la Gestión de Red

1. ***Reducción del Tiempo de Inactividad****:*
   - *La automatización permite una configuración y despliegue más rápidos, reduciendo el tiempo que la red está fuera de servicio.*
   - *Puede detectar y resolver problemas de manera más rápida y eficiente que los métodos manuales.*
2. ***Mejora de la Eficiencia Operativa****:*
   - *Disminuye la carga de trabajo del personal de TI al eliminar tareas repetitivas y propensas a errores.*
   - *Facilita la gestión de configuraciones y actualizaciones en múltiples dispositivos simultáneamente.*
3. ***Consistencia y Estandarización****:*
   - *Asegura que las configuraciones sean consistentes en todos los dispositivos, minimizando errores humanos.*
   - *Implementa políticas de seguridad y configuraciones estandarizadas en toda la red.*
4. ***Escalabilidad****:*
   - *Permite escalar la infraestructura de red fácilmente al automatizar la configuración de nuevos dispositivos y servicios.*

Herramientas de Automatización: Ansible y Puppet

Ansible

1. ***Características Principales****:*
   - ***Sin Agentes****: No requiere instalar agentes en los dispositivos gestionados.*
   - ***Playbooks****: Usa YAML para definir configuraciones y tareas, lo que hace que sea fácil de leer y escribir.*
   - ***Amplia Compatibilidad****: Compatible con una gran cantidad de dispositivos y servicios de red.*
2. ***Uso en la Gestión de Redes****:*

- ***Configuración de Dispositivos****: Permite configurar routers, switches y firewalls de manera automática.*
- ***Orquestación de Tareas****: Coordina múltiples tareas en diferentes dispositivos para asegurar una implementación sin problemas.*
- ***Monitoreo y Reportes****: Integra la monitorización del estado de la red y genera reportes detallados.*

Puppet

1. ***Características Principales****:*
   - ***Basado en Agentes****: Requiere instalar agentes en los dispositivos, lo que puede ofrecer un mayor control y monitoreo.*
   - ***Manifiestos****: Utiliza su propio lenguaje de configuración para definir el estado deseado de los dispositivos.*
   - ***Gestión de Configuraciones****: Excelente para gestionar configuraciones de manera declarativa, asegurando que el estado de los dispositivos sea el deseado.*
2. ***Uso en la Gestión de Redes****:*
   - ***Automatización de Configuraciones****: Permite definir y aplicar configuraciones de red automáticamente.*
   - ***Control de Versiones****: Facilita el seguimiento de cambios en las configuraciones y permite revertir cambios si es necesario.*
   - ***Integración con Otras Herramientas****: Se integra bien con otras herramientas de gestión y monitoreo, proporcionando una vista completa de la red.*

Implementación de la Automatización en el Data Center

1. ***Evaluación Inicial****:*
   - *Realizar un análisis de las tareas de red que pueden ser automatizadas.*
   - *Identificar los dispositivos y servicios que se beneficiarán más de la automatización.*
2. ***Selección de Herramientas****:*
   - *Elegir la herramienta adecuada (Ansible, Puppet, u otras) según las necesidades específicas del data center.*
3. ***Desarrollo de Scripts y Playbooks****:*
   - *Crear scripts y playbooks que definan las configuraciones y tareas a automatizar.*
   - *Realizar pruebas en entornos controlados antes de desplegar en producción.*
4. ***Capacitación del Personal****:*
   - *Capacitar al personal de TI en el uso de las herramientas de automatización.*
   - *Asegurar que todos los miembros del equipo entiendan los procesos automatizados y puedan intervenir en caso de fallos.*
5. ***Monitoreo y Mejora Continua****:*
   - *Monitorear continuamente los procesos automatizados para detectar y corregir problemas.*
   - *Actualizar y mejorar los scripts y playbooks conforme evolucionen las necesidades del data center.*

REFERENCIAS:

- *Cisco Packet Tracer - Networking Simulation Tool. (s.f.). Networking Academy. https://www.netacad.com/es/courses/packet-tracer*
- *Soluciones Digitales. (s.f.). TIVIT. https://tivit.com/es/solucoes/soluciones-digitales/*
- *¿Qué es la prevención de pérdida de datos (DLP)? | Seguridad de Microsoft. (s.f.). Your request has been blocked. This could be due to several reasons. https://www.microsoft.com/es-es/security/business/security-101/what-is-data-loss-prevention-dlp*
- *Configuración de direcciones IP y subredes únicas para nuevos usuarios. (s.f.). Cisco. https://www.cisco.com/c/es_mx/support/docs/ip/routing-information-protocol-rip/13788-3.html*
- *AIX 7.1. (s.f.). IBM - United States. https://www.ibm.com/docs/es/aix/7.1?topic=cards-virtual-local-area-networks*
- *Política de privacidad | Transparencia. (s.f.). Seguros para ti y tu familia, para asegurar tus bienes ¡y más!, en Pacífico. https://www.pacifico.com.pe/transparencia/politica-privacidad#empresas-inversiones*
- *Explicación del protocolo troncal de VLAN (VTP). (s.f.). Cisco. https://www.cisco.com/c/es_mx/support/docs/lan-switching/vtp/10558-21.html*
- *ShieldSquare Captcha. (s.f.). ShieldSquare Captcha. https://networklessons.com/switching/cisco-dtp-dynamic-trunking-protocol-negotiation*
- *Configuración del routing entre VLAN con el uso de un router externo. (s.f.). Cisco. https://www.cisco.com/c/es_mx/support/docs/lan-switching/inter-vlan-routing/14976-50.html*