Introducción

En el contexto actual de rápida evolución tecnológica, la infraestructura de red de una organización juega un papel crucial en su capacidad para adaptarse, crecer y mantenerse competitivamente en el mercado. Sin embargo, con frecuencia nos enfrentamos al desafío de arquitecturas de red obsoletas o inadecuadas que no pueden satisfacer las demandas cada vez mayores de conectividad, rendimiento y seguridad.

En este proyecto, nos enfocamos en abordar el problema de la arquitectura de red inadecuada en Cosaalt. Esta cooperativa se enfrenta a una serie de desafíos derivados de su infraestructura de red actual, que incluyen problemas de rendimiento, vulnerabilidades de seguridad y limitaciones de escalabilidad. Estas deficiencias no solo afectan la productividad y la eficiencia operativa de Cosaalt, sino que también representan un riesgo significativo para la integridad y confidencialidad de los datos críticos de la empresa.

El objetivo de este proyecto es diseñar e implementar una nueva arquitectura de red que satisfaga las necesidades tecnológicas de Cosaalt, mejorando su rendimiento, seguridad y escalabilidad. A través de un enfoque integral que abarca desde el análisis de la infraestructura de red existente hasta la documentación y explicación del personal, buscando proporcionar una solución sólida y sostenible que impulse el éxito futuro de la infraestructura.

En las siguientes secciones, se presentará una descripción detallada del problema a tratar, los objetivos del proyecto, la metodología propuesta, así como los resultados esperados y su relevancia para Cosaalt. Al abordar estos aspectos de manera integral, esperamos proporcionar una base sólida para la mejora de la arquitectura de red y, en última instancia, contribuir al éxito continuo de la organización en un entorno tecnológico en constante cambio.

CAPÍTULO I: DEFINICIÓN DEL PROYECTO

I.1. Descripción del proyecto

I.1.1. Antecedentes

La Cooperativa de Servicios de Agua y Alcantarillado de Tarija – COSAALT R.L. es la entidad prestadora de servicios de agua potable y alcantarillado sanitario a la población de la ciudad de Tarija. COSAALT, fue fundada el 22 de septiembre de 1986 en reemplazo de la Administración Regional de Obras Sanitarias AROS – TARIJA. En fecha 16 de febrero de 2001, COSAALT suscribió el contrato de concesión con la Superintendencia de Saneamiento Básico, para la prestación de los servicios por un periodo de 40 años. Tomando en cuenta la ampliación de la infraestructura de los Sistemas de Agua Potable y Alcantarillado Sanitario, se requiere una organización administrativa de la Cooperativa compatible con los futuros desafíos que significara para la operación y mantenimiento de los indicados servicios.

Para ese acometido, COSAALT RL conformo una comisión responsable de elaborar una propuesta de Actualización del Manual de Organización, Funciones y Perfiles de Cargos, cuyo resultado fue objeto de aprobación por el Consejo de Administración mediante la Resolución Nro. 53/2021 de fecha 24 de septiembre de 2021 y la Resolución Nro. 67/2021, de fecha 25 de noviembre de 2021.

I.1.2. Justificación del proyecto

Desde el funcionamiento de la cooperativa esta ha estado en constante crecimiento lo que ocasionó el requerimiento de más equipos conectados a la red y constantes actualizaciones del diseño para el correcto funcionamiento de la cooperativa, aunque estas actualizaciones no se hicieron correctamente es por lo que con este proyecto se quiere dar solución a muchos de los problemas que presenta actualmente.

Justificación tecnológica

Al desarrollar este proyecto se mejorará el proceso de envío y recepción, así también se analizará la escalabilidad y la seguridad para un mayor rendimiento a futuro

Una red inadecuada puede no aprovechar las últimas tecnologías y estándares, lo que resulta en un rendimiento subóptimo y una incapacidad para aprovechar al máximo las innovaciones tecnológicas.

Las necesidades de Cosaalt cambiaron con el tiempo, lo que limito su capacidad de escalar y adaptarse a sus necesidades en constante evolución.

La seguridad de la red es una preocupación muy importante, cuando no se cuenta con una buena estructura de red puede ser vulnerable a ataques cibernéticos y brechas de seguridad, lo que puede poner en riesgo la integridad y confidencialidad de los datos de Cosaalt.

Justificación social

Productividad y colaboración: un mal diseño de red puede obstaculizar la colaboración y la productividad de los trabajadores al dificultar el acceso a los recursos compartidos, la comunicación efectiva y el intercambio de información.

Acceso equitativo: el buen acceso a recursos a la tecnología y la información es crucial y un mal funcionamiento de la red puede crear disparidades en el acceso a recursos tecnológicos, lo que puede ampliar la brecha digital y afectar desproporcionalmente a ciertos grupos dentro de Cosaalt.

Justificación económica

Con este proyecto se pretende ayudar a mejorar la organización de la cooperativa, con especial énfasis a los encargados del TI, haciendo más fácil su trabajo para posteriores cambios y

mantenimientos, para reducir costos y tiempo cuando se produzca algún daño, permitiendo ubicar el daño sin necesidad de revisar toda la red.

Eficiencia operativa: un mal diseño de red puede resultar en costos operativos más altos debido a problemas de rendimiento, mantenimiento constante y tiempos de inactividad no planificados. Mejorar el funcionamiento de la red puede conducir a una mayor eficiencia operativa y ahorraos en costos a largo plazo.

Retorno de la inversión: si bien mejorar el funcionamiento de la red puede requerir una inversión inicial significativa, esto puede traducirse en un retorno de inversión a largo plazo en términos de mayor productividad, eficiencia operativa, seguridad mejorada y capacidad de adaptación a las demandas cambiantes del marcado.

I.1.3. Planteamiento del problema

Cosaalt enfrenta serios desafíos en su infraestructura de red, la cual no está preparada para satisfacer las crecientes demandas tecnológicas y operativas. La red actual presenta problemas de conectividad, falta de escalabilidad y medidas insuficientes de seguridad, lo que impacta negativamente en la eficiencia operativa y en la capacidad de la organización para adoptar sistemas avanzados como SCADA y medidores inteligentes. Esta situación afecta la productividad, la seguridad de los datos y la calidad de los servicios, por lo que es fundamental diseñar una solución integral que permita modernizar la red, optimizando su desempeño y garantizando su sostenibilidad a futuro.

I.1.4. Análisis del cuadro de involucrados

Nombre	Ingeniero Iván Rios
Rol	Encargado del área de TI

Categoría profesional	Licenciado de sistemas
Responsabilidades	Mantenimiento de software, hardware y de la red de datos
Información de contacto	71878585
Aprobación	

Tabla 1: cuadro de involucrado de sistemas
Fuente: elaboración propia

Nombre	Ingeniero Marco Cadena
Rol	Encargado del área de TI
Categoría profesional	Licenciado de sistemas
Responsabilidades	Mantenimiento de software, hardware y de la red de datos
Información de contacto	72966862
Aprobación	

Tabla 2: cuadro de involucrados de sistema 2
Fuente: elaboración propia

Nombre	Ingeniero Jose Luis Patiño
Rol	Gerente General
Categoría profesional	licenciado

Responsabilidades	Dirigir y controlar las actividades y los planes de la cooperativa
Información de contacto	73495936
Aprobación	

***Tabla 3**:* cuadro de involucrados de gerente
Fuente: elaboración propia

I.1.5. Árbol de problemas

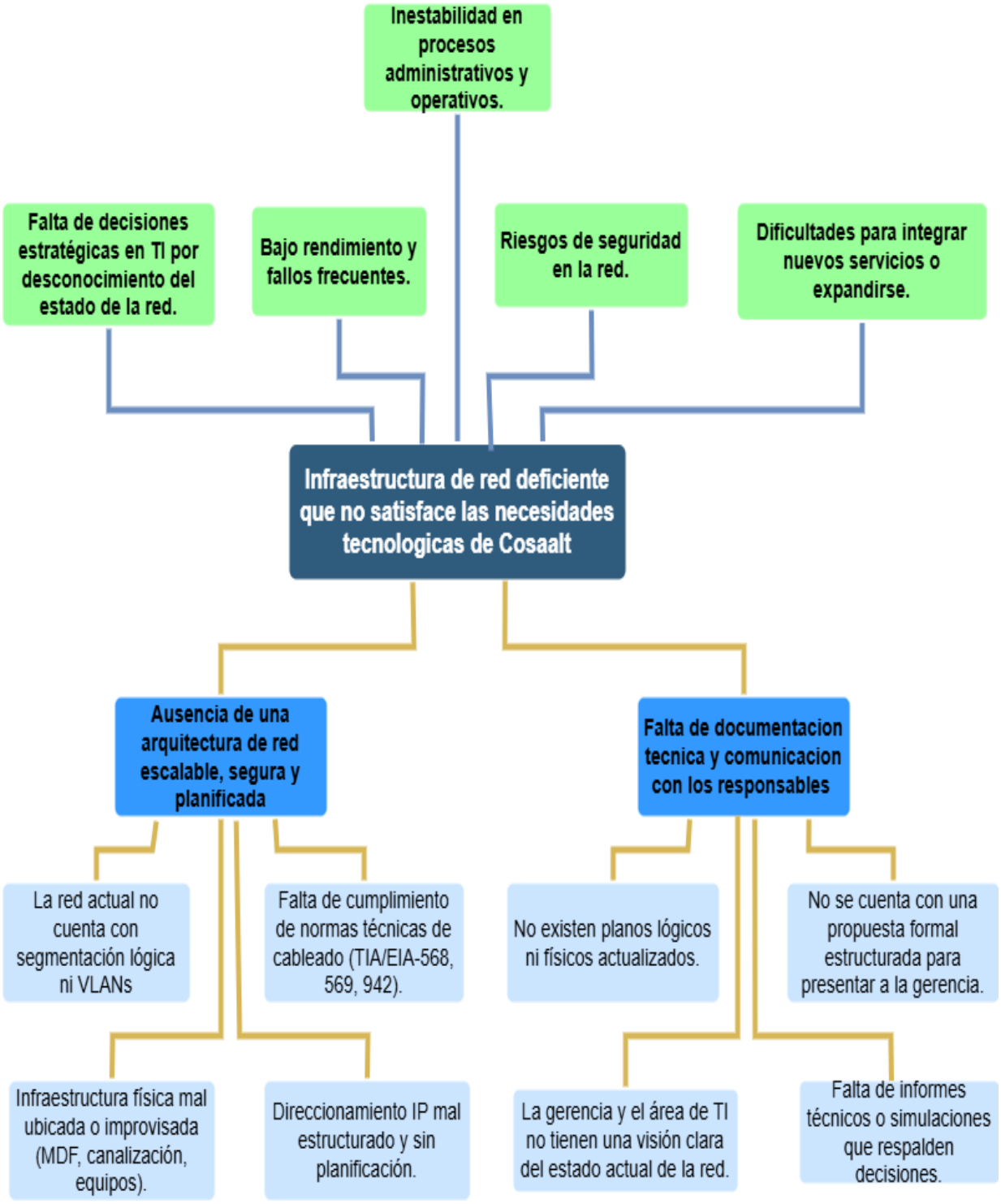


Figura I.1.1 Árbol de problemas
Fuente: elaboración propia

I.1.6. Árbol de objetivos

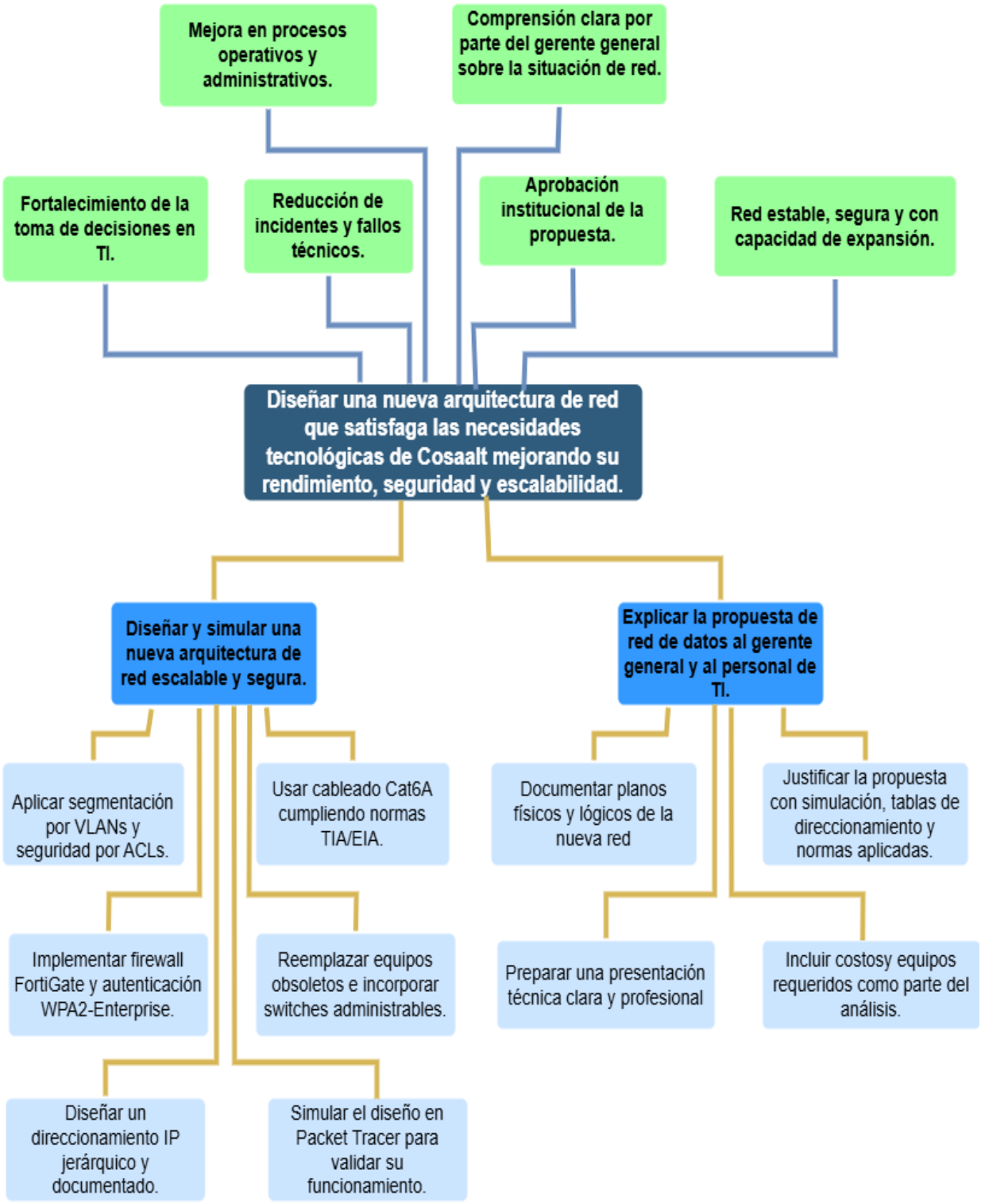


Figura I.1.2: Árbol de objetivos
Fuente: elaboración propia

I.1.7. Objetivos

I.1.7.1. Objetivo general

Diseñar una nueva arquitectura de red que satisfaga las necesidades tecnológicas de Cosaalt mejorando su rendimiento, seguridad y escalabilidad.

I.1.7.2. Objetivos específicos

Diseño mejorado de una nueva arquitectura de red para Cosaalt

Propuesta técnica de red documentada, validada y presentada ante las autoridades de COSAALT.

I.1.8. Resultados esperados

Mejora del rendimiento: se espera que la simulación de la nueva arquitectura de red pueda cumplir con el mejoramiento de la infraestructura de comunicaciones, reduciendo los tiempos de respuesta, la latencia y los cuellos de botella en la red.

Incremento de la seguridad: Los resultados esperados incluyen una mejora en la seguridad de la red, con una reducción en el número de brechas de seguridad, intrusiones no autorizadas y vulnerabilidades identificadas.

Escalabilidad mejorada: los resultados esperados incluyen una arquitectura de red más escalable que pueda adaptarse fácilmente al crecimiento de Cosaalt y a las demandas cambiantes de tráfico de red.

Adopción de nuevas tecnologías: se espera una exitosa transición a nuevas tecnologías y servicios de red, como la computación en la nube y la virtualización de redes, según sea necesario.

I.2. Cronograma de actividades

Actividad	Inicio	Días	Final
analizar requerimientos	1/11/2023	53	23/12/2023
desarrollar diseño lógico	20/2/2024	61	20/4/2024
Desarrollar diseño físico	21/4/2024	48	7/6/2024
Probar, optimizar y documentar el diseño	8/6/2024	73	19/8/2024
Realizar modificaciones	20/8/2024	109	6/12/2024

Tabla 4: cronograma de actividades
Fuente: elaboración propia

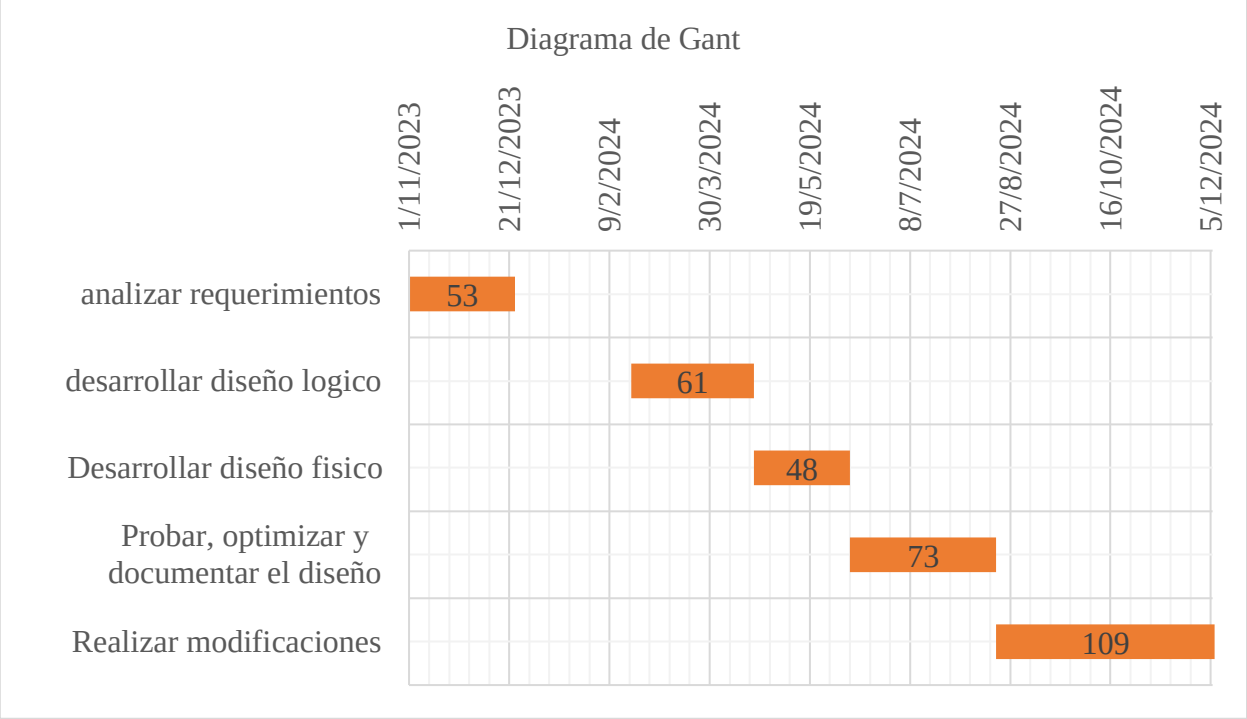


Figura I.2.1: Diagrama de Gant
Fuente: Elaboración propia

I.3. Gastos generales

Para obtener el costo total de la red se tomará en cuenta: canaletas, tuberías, cables, conectores, patch cords y demás accesorios. En lo referente a los materiales y accesorios, se detalla una estimación aproximada de las cantidades que se necesitara para el nuevo rediseño.

I.3.1. Dispositivos

Descripción	Descripción	Cantidad	Precio unitario	Total
Switch de 48 puertos	TP-Link T3700G-52TQ	3 U	17,594 Bs	52,785 Bs
Switch de 24 puertos	D-Link DGS-3130-30TS	1 U	6,606 Bs	6,606 Bs
Servidor de 24 núcleos	HP Servidor DL380 G9	1 U	3,900 BS	3,900 BS
TOTAL				63,291 Bs

Tabla 5: Gasto de dispositivos
Fuente: Elaboración propia

I.3.2. Cableado UTP

Descripción	Cantidad	Precio unitario	Total
Rollo (305 m) cable UTP cat. 6	3 U	1000 Bs	3000 Bs
RJ-45 cat. 6	140 U	2.50 Bs	350 Bs

Patch cord cat. 6 de 2m	12 U	41,35 Bs	496 Bs
Patch Cord cat. 6 de 0,5m	88 U	21 Bs	1848 Bs
Patch Cord cat. 6 de 1m	10 U	35 BS	350 Bs
Total			6044 Bs

Tabla 6: Gastos de cable UTP
Fuente: Elaboración propia

I.3.3. Fibra óptica

Descripción	Cantidad	Precio unitario	Total
Cable de Fibra óptica multimodo 6 hilos 10GIG 50/125	10 m	32 Bs	320
Total			320 Bs

Tabla 7: Gastos de fibra óptica
Fuente: Elaboración propia

I.3.4. Costos finales de una simulación de implementación

Presupuesto general para los componentes de la red y los costos del proyecto. Sujeto a cambios.

Descripción	Total
Dispositivos	63,291 Bs

Cable UTP y Patch Cord	6044 Bs
Fibra óptica	320 Bs
Total	138,134 Bs

Tabla 8: Costos finales de implementación
Fuente: Elaboración propia

I.3.5. Costos del diseño y simulación de la tesis

Descripción	Total
Software de diseño y simulación	0 Bs
Investigación y análisis	0 Bs
Capacitación y formación	0 Bs
Reuniones con el personal de TI	40 Bs
Documentación	0 Bs
Total	40 Bs

Tabla 9: Costos finales de diseño y simulación
Fuente: Elaboración propia

I.4. Matriz de marco lógico

La matriz de marco lógico fue utilizada como herramienta metodológica para estructurar la propuesta técnica de red de forma sistemática, asegurando coherencia entre los objetivos, productos, indicadores y actividades. Esta herramienta permite facilitar la evaluación del cumplimiento de metas técnicas, en línea con el enfoque de la metodología top-dow

Resumen narrativo del proyecto	Indicadores	Medios de verificación	Supuestos
Fin FinContribuir a la mejora de la infraestructura tecnológica de COSAALT mediante el fortalecimiento de la red de datos para garantizar continuidad operativa, escalabilidad y eficiencia.	A dos años de finalizado el proyecto, la disponibilidad de red supera el 98% y la percepción del servicio es valorada como “excelente” por al menos el 90% del personal operativo.	Encuestas institucionales, reportes de monitoreo de red, bitácoras de incidentes.	La infraestructura general de COSAALT se mantiene sin cambios estructurales graves. El personal hace uso activo de los sistemas de red.
Objetivo General (Propósito) Diseño de la arquitectura de red de COSAALT mejorada (aplicando estándares de diseño y simulación	Las simulaciones reflejan un 40% de mejora en la capacidad operativa de la red, y reducción del 50% en tiempos de respuesta entre VLANs..	Informe de simulación en Cisco Packet Tracer y GNS3, carta de validación técnica de la gerencia de TI de COSAALT.	Acceso a información precisa sobre la red actual. Colaboración del personal técnico.

de redes de forma escalable, redundante y segura).				
Objetivos Específicos (Componentes) 1. Diseño mejorado de una nueva arquitectura de red para Cosaalt 2. Propuesta técnica de red documentada, validada y presentada ante las autoridades de COSAALT.	Documento técnico del diseño lógico y físico validado por simulación en Packet Tracer. Acta firmada por la gerencia general indicando conformidad con la propuesta.		Capturas de pantalla de simulación, documentación técnica. Carta de conformidad firmada y registrada por el Gerente General.	Disponibilidad de software y equipos para simulación. Tiempo disponible para la socialización de la propuesta.
Actividades **Componente 1:** **Fase 1: Análisis de requerimientos.**	Dispositivos	63,291 Bs	Documento de requerimientos funcionales y técnicos.	Obtención de la información requerida para el análisis de la red existente.
	Cable UTP y Patch Cord	6,044		

<table>
<tr>
<td>

- Analizar las metas del negocio.
- Analizar las metas técnicas.
- Analizar la red existente.
- Analizar el tráfico existente.

Fase 2: Desarrollo de diseño lógico

Definición de VLANs, IP, protocolos, enrutamiento y redundancia.

Selección de protocolos de switching (RSTP, EtherChannel) y routing (HSRP, OSPF).

Fase 3: Desarrollo de diseño físico

- Diseñar el cable de red, normas y estándares.

Fase 4: Documentar el diseño

Componente 2:

</td>
<td>
<table>
<tr><td>Fibra óptica</td><td>320 Bs.</td></tr>
<tr><td>Diseño y simulación</td><td>40 Bs.</td></tr>
<tr><td>Total</td><td>138,174 Bs</td></tr>
</table>
</td>
<td>

Diagramas en Draw.io y Packet Tracer.

Inventario de equipos y hoja de costos.

Hoja de cálculo, cotizaciones y catálogo técnico.

Manual de configuración, políticas de red.

</td>
<td>

Equipos en GNS3 con licencias gratuitas.

Presupuesto estimado mantenido.

Aceptación de la configuración necesario en los equipos requeridos en Packet Tracer y GNS3.

Disposición de tiempo por parte del gerente y de los encargados de TI

</td>
</tr>
</table>

2.1Definición de medios y estrategias de socialización. 2.2Presentacion técnica al personal.			

Tabla 10: Matriz de marco lógico
Fuente: Elaboración propia

CAPÍTULO II: MARCO TEÓRICO

II.1. Elementos físicos de la red

II.1.1. Medios de transmisión

El medio de transmisión es el camino físico entre el transmisor y el receptor. Cualquier medio físico que pueda transportar información en forma de señales electromagnéticas se puede utilizar en las redes de datos como un medio de transmisión.

El medio físico puede condicionar la distancia, velocidad de transferencia, topología y el método de acceso.

Los principales medios de transmisión pueden ser:

- Guiados, cuando las ondas se transmiten confinándolas a lo largo de un camino (medio) físico, como por ejemplo un cable.
- No guiados (inalámbricos), la propagación de la señal se hace a través del aire, el mar o el espacio.

Los principales medios guiados emplean cobre y fibra óptica, ejemplos son:

- El par trenzado
- El cable coaxial
- El cable de fibra óptica

Los principales medios no guiados son los enlaces radios y micro ondas para redes inalámbricas. (Barcell)

II.1.1.1. Cable de cobre

El medio más utilizado en la actualidad para la comunicación de redes locales (LAN) es el cable de cobre, este cable está formado por ocho conductores de cobre sólido, son ocho conductores independientes con una función específica la cual va a depender de la aplicación para la cual sea utilizado, sin embargo, para este caso en particular hablando de redes de datos, el cable va a tener distintas propiedades de conducción eléctrica lo que le va a permitir transportar por las diferentes frecuencias que son las portadoras de las señales que van a ser nuestra información. (INNOVANET, 2018).

Cable FTP (foiled twisted pair)

El cable FTP es una variante del cable de par trenzado que cuenta con una lámina metálica (foil) que cubre los pares de cables y que actúa como una pantalla de protección contra las interferencias electromagnéticas externas. Esta lámina metálica evita que las señales eléctricas se escapen del cable y protege la transmisión de datos contra interferencias electromagnéticas externas, como las generadas por cables eléctricos cercanos o equipos electrónicos. (GROUP, s.f.)

Figura II.1.1: cable FTP
Fuente: Cablecel

Cable UTP

Es uno de los tipos más comunes de cables usados en redes de área local y está compuesto por pares de cobre trenzados sin ninguna capa de blindaje externo (cada par se compone de dos cables de

cobre aislados que están entrelazados entre sí). Se trata de un tipo de cable más económico y que facilita el trabajo de instalación debido a su gran flexibilidad. (GROUP, s.f.)

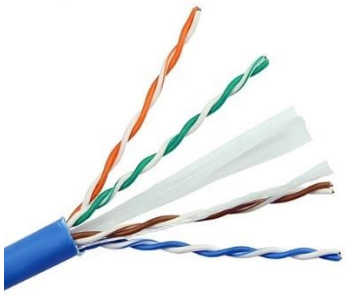


Figura II.1.2: cable UTP
Fuente: Bolivian Electric

Cable STP

El cable STP aporta una capa de protección al tipo UTP, con un blindaje externo que envuelve los pares de cables individuales, lo que proporciona un entorno de protección ideal (contra corrientes electromagnéticas generadas principalmente por cables eléctricos o equipos electrónicos cercanos). (GROUP., s.f.)

Figura II.1.3: cable STP
Fuente: Kroton

II.1.1.2. Fibra óptica

El de fibra óptica es un tipo de cable utilizado para la transmisión de datos a través de pulsos de luz, en lugar de utilizar señales eléctricas como los cables de cobre. Los datos se transportan empleando hilos extremadamente delgados de vidrio o plástico (fibras ópticas). Esto permite una mayor capacidad de ancho de banda y una mayor distancia. (GROUP., s.f.)

Por lo general, los cables de fibra óptica son más ligeros y menos susceptibles a las interferencias electromagnéticas. Sin embargo, la fibra óptica tiende a ser más frágil que los cables con conductor de metal. (CABLES, 2023)

II.1.1.3. Transmisión inalámbrica

Redes inalámbricas de área local (WLAN)

Están diseñadas para proporcionar acceso inalámbrico en zonas con un rango típico de hasta 100 metros y se utilizan sobre todo en el hogar, la escuela, una sala de ordenadores, o entornos de oficina. Esto proporciona a los usuarios la capacidad de moverse dentro de un área de cobertura local y permanecer conectado a la red. Las WLAN se basan en el estándar 802.11 del IEEE y son comercializadas bajo la marca Wi-Fi. (SALAZAR).

Figura II.1.4: WLAN
Fuente: Salazar

Esquema de una WLAN en el hogar

Esta tecnología inalámbrica proporciona una solución eficiente y flexible para las necesidades de conectividad de Cosaalt, dado que el área de Lecturación cuenta con equipos móviles para la realización de su trabajo.

II.1.2. Dispositivos de interconexión

La infraestructura de red de Cosaalt se compone de varios dispositivos de interconexión que desempeñan roles fundamentales en la transmisión eficiente de datos y la conectividad entre diferentes sistemas y usuarios.

II.1.2.1. Switches

Un switch de red es un dispositivo que permite la conexión de múltiples dispositivos en una red. Los switches de red actúan como «puentes» entre dispositivos en una red, permitiendo que la información se transfiera entre ellos a través de paquetes de datos. Los paquetes de datos son pequeños bloques de información que se transmiten a través de la red. Cuando un dispositivo envía un paquete de datos a otro dispositivo, el switch de red lo recibe y lo envía al dispositivo correcto según la dirección MAC del dispositivo. (Rodríguez, 2023)

II.1.2.2. Routers

El router es un dispositivo utilizado en redes de mayor porte. Es más" inteligente" que el switch, pues, además de cumplir la misma función, también tiene la capacidad de escoger la mejor ruta que un determinado paquete de datos debe seguir para llegar a su destino. Es como si la red fuera una ciudad grande y el router elige el camino más corto y menos congestionado. De ahí el nombre de router. (Plata)

II.1.2.3. Access point

Un punto de acceso inalámbrico (WAP o AP, por sus siglas en inglés: Wireless Access Point) en redes de computadoras es un dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica. Normalmente, un WAP también puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red cable y los dispositivos inalámbricos. (Plata)

II.1.2.4. Firewalls

Los firewalls vienen en formas de hardware y software, y funcionan inspeccionando paquetes de datos y determinando si los permiten o bloquean en función de un conjunto de reglas. Las organizaciones pueden configurar estas reglas para permitir o denegar el tráfico en función de varios criterios, como direcciones IP de origen y destino, números de puerto y tipo de protocolo.

Los firewalls son la base de la seguridad de la red, protegiendo la red del acceso no autorizado. Evitan que los actores maliciosos, piratas informáticos, bots y otras amenazas, sobrecarguen o se infiltren en una red privada para robar datos sensibles.

Los firewalls protegen contra el tráfico malicioso. Están estratégicamente posicionados en el borde de la red o en un centro de datos, lo que les permite monitorear de cerca cualquier cosa que intente cruzar este límite. (FORTINET).

Los firewalls han constituido una primera línea de defensa en seguridad de la red durante más de 25 años. Establecen una barrera entre las redes internas protegidas y controladas en las que se puede confiar y redes externas que no son de confianza, como Internet. (CISCO).

II.1.2.4.1. Fortigate

En el ámbito de la ciberseguridad, Fortigate, desarrollado por Fortinet, se posiciona como una solución integral diseñada para proteger las infraestructuras corporativas. Fortigate es un firewall avanzado que no solo bloquea accesos no autorizados, sino que también inspecciona el tráfico interno y externo para detectar amenazas potenciales. Al ser parte de la categoría Next-Generation Firewall (NGFW), supera las capacidades de los firewalls tradicionales al incorporar tecnologías de inspección profunda de paquetes, prevención de intrusiones (IPS) y control de aplicaciones.

Este firewall está diseñado específicamente para entornos corporativos con un gran volumen de conexiones y tráfico, permitiendo a las organizaciones controlar y proteger sus redes con mayor precisión y automatización. (Corporativo, 2022).

II.1.3. Normativas y Estándares técnicos aplicados al diseño de redes

II.1.3.1. TIA/EIA-568 (Estándar de cableado estructurado).

Definen la forma de diseñar, construir y administrar un sistema de cableado que es estructurad o, lo que significa que el sistema está diseñado en bloques que tienen

características de rendimiento muy específicos.

NORMA TIA/EIA - 568 – C

Es una revisión del ANSI/TIA/EIA 568-B, publicado entre 2001 y 2005. El nuevo estándar consolida los documentos centrales de las recomendaciones originales y todos los “adendum”, pero cambia la organización, generando una recomendación “genérica” o “común” a todo tipo de edificios. Está armado en varias partes:

TIA/EIA 568-C.0 tiene como objetivo permitir la planificación y la instalación de un sistema de cableado estructurado para todo tipo de instalaciones. Esta norma específica un sistema que

soportes cableados de telecomunicaciones genéricos en un entorno multi-producto y multiproveedor. Varios de los conceptos originalmente indicados en la recomendación ANSI/TIA/EIA 568-B.1 (que era específica para edificios comerciales) fueron generalizados e incluidos en la 568-C.0.

TIA/EIA 568-C.1 provee información acerca del planeamiento, instalación y verificación de cableados estructurados para edificios comerciales. Los aspectos de la anterior recomendación ANSI/TIA/EIA 568-B.1 que aplican únicamente a este tipo de edificios fueron detallados y actualizados en esta nueva recomendación.

TIA/EIA 568-C.2 detalla los requerimientos específicos de los cables de pares trenzados balanceados, a nivel de sus componentes y de sus parámetros de transmisión

TIA/EIA 568-C.3 especifica los componentes de cable de fibra óptica, incluyendo aspectos mecánicos, ópticos y requisitos de compatibilidad. (Blogger.com, Blogger.com, 2015).

Tipos de cable

Cables planos. Se utilizan para conectar dispositivos de tipo diferente Los cables o latiguillos de cable UTP se montan engastando los conectores RJ-45 en cada uno de los extremos de cable según uno de los estándares (568A o 568B). Los dos extremos deben ser montados siguiendo el mismo estándar. Este tipo de cables se utilizan para la conexión de un ordenador a su roseta en la pared. (wordpress, 2016).

Parámetros técnicos establecidos

En el presente diseño, se toman en cuenta los siguientes lineamientos aplicables:

- Uso de cableado categoría 6A, adecuado para velocidades de hasta 10 Gbps.
- Radio mínimo de curvatura de 33 mm para evitar daño físico al cable.
- Longitud máxima de canal horizontal: 90 metros, más 10 metros en patch cords.

- Estructura en estrella, conexión desde puntos de red hacia el MDF.
- Utilizar colores distintos de cables por tipo de conexión o VLAN (ej. azul para datos, amarillo para IP phones, rojo para backbone).
- Garantizar que los cables UTP no estén tensos ni doblados en exceso
- Todos los cables deben tener conectores RJ45 de alta calidad, y las terminaciones deben realizarse con herramientas certificadas (crimpado profesional).
- Uso de patch panels para facilitar la conexión modular.
- Verificación y certificación de puntos de red con herramientas de testeo.

II.1.3.2. TIA/EIA-569 (Estándar de Espacios y Rutas de Telecomunicaciones)

Estándar ANSI/TIA/EIA-569 de Rutas y Espacios de Telecomunicaciones para Edificios Comerciales. Este estándar reconoce tres conceptos fundamentales relacionados con telecomunicaciones y edificios: Los edificios son dinámicos. Durante la existencia de un edificio, las remodelaciones son más la regla que la excepción. Este estándar reconoce, de manera positiva, que el cambio ocurre. Los sistemas de telecomunicaciones y de medios son dinámicos. Durante la existencia de un edificio, los equipos de telecomunicaciones cambian dramáticamente. Este estándar reconoce este hecho siendo tan independiente como sea posible de proveedores de equipo. Telecomunicaciones es más que datos y voz. Telecomunicaciones también incorpora otros sistemas tales como control ambiental, seguridad, audio, televisión, alarmas y sonido. De hecho, telecomunicaciones incorpora todos los sistemas de bajo voltaje que transportan información en los edificios. Este estándar reconoce un precepto de fundamental importancia: De manera que un edificio quede exitosamente diseñado, construido y equipado para telecomunicaciones, es imperativo que el diseño de las telecomunicaciones se incorpore durante la fase preliminar de diseño arquitectónico.

Este estándar será el central al momento de diseñar el sistema de cableado estructurado, ya que su enfoque central son las rutas y espacios donde se instalan los cables. Permitirá generar un diseño en el que las rutas sean las óptimas para cada subsistema, por medio de la especificación de materiales, ductos y prácticas de instalación. (RDU-UNAM, 2004)

Parámetros técnicos establecidos

En el presente diseño, se toman en cuenta los siguientes lineamientos aplicables:

- Separación mínima de 30 cm entre cables eléctricos y cables de datos, para evitar interferencias electromagnéticas.
- Uso de bandejas porta cables cerradas para mantener rutas limpias y ordenadas.
- Canalización con 25% de capacidad libre, asegurando posibilidad de expansión.
- Mantener un mínimo de 15 cm entre cables de red y fuentes de calor (ej. luminarias, transformadores).
- Los caminos de canalización deben permitir acceso al personal sin obstáculos, tanto en bandejas superiores como piso técnico.
- Evitar esquinas agudas o curvas cerradas al instalar bandejas o canaletas.
- Respetar una separación vertical mínima de 2 m entre bandejas de energía y de datos si están en paralelo en paredes o racks.

II.1.3.3. TIA/EIA-606 (Administración de Infraestructura de Telecomunicaciones)

Estándar ANSI/TIA/EIA-606 de Administración para la Infraestructura de Telecomunicaciones de Edificios Comerciales. El propósito de este estándar es proporcionar un esquema de administración uniforme que sea independiente de las aplicaciones que se le den al sistema de cableado, las cuales pueden cambiar varias veces durante la existencia de un edificio. Este estándar

establece guías para dueños, usuarios finales, consultores, contratistas, diseñadores, instaladores y administradores de la infraestructura de telecomunicaciones y sistemas relacionados.

Si un diseño de cableado se documenta desde su fase inicial, y si esta documentación se hace siguiendo las indicaciones a este estándar, la administración de los servicios y del mismo cableado en un futuro serán muy sencillos. Esto facilitará la modificación en los diseños, ya que teniendo en cuenta detalles como la ocupación de las rutas, la utilización de los pares de fibra, se podrá decidir si se agregan cables, se reutilizan los instalados o si se tiene capacidad para crecer. La administración de los servicios que se ofrecen a través del cableado será más fácil de realizar si se tiene una documentación, ya que sabiendo que cable en el panel de terminación lleva a cada área de trabajo será muy fácil conectar el cable del servicio que se requiere en cada una de ellas. (RDU-UNAM, revista.unam.mx, 2004).

Parámetros técnicos establecidos

En el presente diseño, se toman en cuenta los siguientes lineamientos aplicables:

- Se establece etiquetado alfanumérico por VLAN, etiquetas resistentes al calor y humedad para identificar puntos de red en ambientes críticos, piso y rack.
- Se planifica el registro físico y digital de conexiones, puntos de red y paneles de parcheo.
- Documentar cambios en las conexiones o puertos mediante un registro de mantenimiento o bitácora técnica.
- Establecer un sistema de codificación estándar, por ejemplo: [PISO]-[RACK]-[PUERTO]-[VLAN], como: 2F-R1-P06-V10.

II.1.3.4. Estándar ANSI/TIA-942

El objetivo principal de este estándar es establecer un conjunto de requisitos mínimos para la infraestructura de telecomunicaciones de los centros de datos, con el fin de garantizar su eficiencia, seguridad y fiabilidad.

Este estándar proporciona directrices detalladas para el diseño, la instalación y la operación de los centros de datos, abarcando aspectos críticos como la topología del cableado, la infraestructura eléctrica y los sistemas de enfriamiento. Su propósito es asegurar que los data centers sean capaces de operar de manera óptima, adaptarse a nuevas tecnologías y minimizar el tiempo de inactividad.

De acuerdo a esta norma, la infraestructura de un data center está compuesta por cuatro subsistemas: sistemas eléctricos, sistemas mecánicos, telecomunicaciones y arquitectura.

El estándar ANSI/TIA-942, además, utiliza un sistema de clasificación TIER del estándar Uptime Institute que evalúa y categoriza los centros de datos según su nivel de redundancia y disponibilidad. Aunque proporciona un marco detallado para entender estos niveles, no incluye una certificación formal de TIER como la del Uptime Institute. (Powernet, 2020).

Parámetros técnicos establecidos

En el presente diseño, se toman en cuenta los siguientes lineamientos aplicables:

- Reubicación o remodelación del MDF para evitar exposición a polvo, ventanas o humedad.
- Instalación de UPS, ventilación y racks cerrados.
- Acceso restringido al personal técnico autorizado.
- Considerar suelo falso o ductos elevados para cableado estructurado según espacio disponible.
- Asegurar que los equipos estén montados en racks con ventilación frontal y trasera.

- Uso de piso vinílico antiestático si hay riesgo de descargas electrostáticas (ESD).

II.1.3.5. Modelo OSI: Para diseño lógico

El modelo OSI es una arquitectura conceptual en 7 capas. En esta propuesta se trabajó especialmente en:

Capa 2: Capa de enlace de datos

Uso de VLANs para segmentar la red y aislar tráfico por área.

La capa 2 del modelo OSI se divide en dos subcapas: control de acceso al medio (MAC) y control de enlace lógico (LLC). La capa MAC encapsula las tramas de datos transmitidas a través de los medios de conexión de red, como cables. El protocolo de resolución de direcciones (ARP) traduce las direcciones IP a direcciones MAC y actualiza los encabezados de las tramas creadas para establecer la comunicación. En caso de fallo de la transmisión de datos, el LLC ayuda a gestionar la retransmisión de paquetes. (Powell, 2024)

Capa 3: Capa de red

Implementación de enrutamiento entre VLANs y direccionamiento ip organizado.

La función principal de la capa de red es decidir la ruta física que seguirán los datos. Esto se conoce como enrutamiento de paquetes: elegir la mejor ruta posible que conecte dos redes diferentes para garantizar una transferencia de datos eficiente y aplicar direcciones IP para el enrutamiento. Recibe segmentos de datos y los divide en paquetes más pequeños en el lado del emisor para permitir su tránsito eficiente hacia y a través de otras redes. En el lado del receptor, la Capa 3 reensambla los datos. (Powell, 2024).

II.1.3.6. ISO/IEC 27001: seguridad de la información

La norma ISO/IEC 27001 proporciona a las empresas de cualquier tamaño y de todos los sectores de actividad orientación para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información. La conformidad con la norma ISO/IEC 27001 significa que una organización o empresa ha implementado un sistema para gestionar los riesgos relacionados con la seguridad de los datos que posee o maneja la empresa, y que este sistema respeta todas las mejores prácticas y principios consagrados en esta Norma Internacional. (ISO, 2022).

Aunque no se implementa directamente, esta norma internacional establece buenas prácticas para gestionar la seguridad de la información, incluyendo: control de acceso, segmentación de red, seguridad perimetral.

Estas prácticas para la seguridad se establecen en la propuesta mediante: la segmentación con VLANs, uso de ACLs, autenticación en red WiFi (WPA2-Enterprise), integración de firewall FortiGate para proteger la red perimetral.

Parámetros técnicos establecidos

En el presente diseño, se toman en cuenta los siguientes lineamientos aplicables:

- Control de tráfico mediante ACLs.
- Seguridad perimetral con firewall FortiGate.
- WiFi seguro con autenticación RADIUS (WPA2-Enterprise).
- Definición de zonas seguras o VLANs restringidas (por ejemplo, una VLAN para servidores que no tenga acceso directo a Internet).
- Uso de backups automáticos de configuraciones de red y registros de logs.
- Monitoreo constante del tráfico con herramientas IDS/IPS (como Snort o funciones del FortiGate).

- Aplicación de políticas de mínimo privilegio: usuarios solo pueden acceder a los servicios necesarios para su rol.

II.2. Protocolos y estándares de la capa de enlace de datos

II.2.1. Protocolos de acceso al medio

II.2.1.1. Ethernet

Ethernet es un popular protocolo de red para conectar dispositivos y crear redes de área local (LAN, por sus siglas en inglés). Permite que los dispositivos intercambien paquetes de datos entre sí a través de una red para comunicarse. Fue inventado en la década de 1970 y, desde entonces, se ha ido desarrollando para admitir distancias más largas y velocidades más rápidas.

Ethernet se basa en los protocolos CSMA/CD (Carrier Sense Multiple Access with Collision Detection), que ayudan a evitar colisiones de datos cuando varios dispositivos intentan enviar datos de forma simultánea. Este protocolo se utiliza para controlar el tráfico de la red y garantizar una transmisión de datos fiable. Además, los datos también se envían a través de una conexión de cobre o fibra óptica mediante una técnica de capa física. (HPE, s.f.)

Los tres tipos principales de protocolos son Ethernet estándar, Ethernet rápida y Ethernet Gigabit. Todos ellos funcionan con cableado de cobre y tienen una velocidad que oscila entre 10 Mbps y 1 Gbps. La Ethernet estándar es una conexión de 10 Mbps, la más común y utilizada. Fast Ethernet es una conexión de 100 Mbps, y es el tipo más avanzado de conexión que todavía puede funcionar con cableado de cobre. Por último, Gigabit Ethernet es una conexión de 1000 Mbps, la más rápida y avanzada, y requiere cableado de fibra óptica. Vamos a conocer un poco más en detalle en qué consiste cada una de ellas. (trainingIT, 2023)

II.2.1.2. Wifi (IEEE 802.11)

El estándar 802.11 es una familia de normas inalámbricas creada por el Institute of Electrical and Electronics Engineers (IEEE). 802.11n es la forma más apropiada de llamar a la tecnología Wi-Fi, lanzada en 2009. Mejoró con respecto a versiones anteriores de Wi-Fi con múltiples radios, técnicas avanzadas de transmisión y recepción, y la opción de usar el espectro de 5 GHz. Todo implica una velocidad de datos de hasta 600 Mbps.

La familia 802.11 consta de una serie de técnicas de modulación semidúplex (half duplex) por medio del aire que utilizan el mismo protocolo básico. Al estándar 802.11-1997 le siguió el 802.11b, que fue el primero aceptado ampliamente. Posteriormente, surgirían versiones mejoradas: 802.11a, 802.11g, 802.11n y 802.11ac. Otras normas de la familia (c-f, h, j) son las modificaciones de servicio que se utilizan para extender el alcance actual de la norma existente, que también puede incluir correcciones de una especificación anterior. (Wikipedia, 2024).

II.2.1.3. STP (Spanning Tree Protocol)

El Protocolo de Árbol de Expansión, o Spanning Tree Protocol (STP), es un protocolo de red que se utiliza para evitar los bucles de red que pueden ser creados por “enlaces redundantes” en una red de computadoras.

Los bucles son perjudiciales para la red y pueden llevar a la propagación sin fin de los paquetes de datos, congestionando y degradando severamente el rendimiento de la red.

STP fue desarrollado por el Dr. Radia Perlman y publicado por primera vez como el estándar IEEE 802.1D en 1990.

El STP trabaja creando una topología de árbol, un “árbol de expansión“, que abarca todos los switches en una red. Este árbol es usado para determinar un camino sin bucles en la red.

La idea es asegurarse de que solo haya un camino activo entre dos nodos de la red. Para hacer esto, STP asigna roles (raíz, designado y bloqueado) a todos los puertos en la red. (Escalante, 2023)

II.3. Enrutamiento de paquetes

II.3.1. Tablas de enrutamiento

Tanto los switches como los routers utilizan tablas de enrutamiento para determinar cómo reenviar los datos a través de la red. Mientras que los switches se centran en las direcciones MAC para el reenvío de tramas en una red local, los routers utilizan tablas de enrutamiento basadas en direcciones IP para el enrutamiento de paquetes entre redes. Estas tablas se actualizan dinámicamente a medida que cambian las condiciones de la red para garantizar una conectividad eficiente y confiable.

II.3.2. Tipos de enrutamiento

Hay varios tipos de enrutamiento que se utilizan en redes de computadoras. Aquí hay más detalles sobre los tipos más comunes:

Enrutamiento estático: En el enrutamiento estático, la tabla de enrutamiento se configura manualmente por un administrador de red. Esto significa que cualquier cambio en la red requiere una modificación manual en la tabla de enrutamiento. (eclassvirtual).

Enrutamiento dinámico: En el enrutamiento dinámico, la tabla de enrutamiento se actualiza automáticamente a medida que los cambios en la red se producen. Los protocolos de enrutamiento dinámico, como OSPF y EIGRP, utilizan información sobre la topología de la red para calcular la mejor ruta a utilizar. (eclassvirtual).

Enrutamiento por defecto: En el enrutamiento por defecto, se establece una ruta predeterminada para los paquetes de datos que no se pueden enrutar de otra manera. La ruta por

defecto se especifica en la tabla de enrutamiento y generalmente conduce a un gateway de salida. (eclassvirtual).

Enrutamiento de red virtual (VRF): El enrutamiento de red virtual es un tipo de enrutamiento que permite a los administradores de red crear múltiples tablas de enrutamiento en un solo router. Esto es útil cuando se deben separar diferentes redes lógicas en una misma física. (eclassvirtual).

II.3.3. Protocolos de enrutamiento

El enrutamiento es el proceso de transferir información desde un origen a un destino a través de la interconexión de redes. Normalmente, se encuentra al menos un nodo intermediario a lo largo de la ruta. El enrutamiento se realiza en la capa 3 (la capa de red) del modelo OSI. Normalmente, las redes emplean una combinación de enrutamiento estático y dinámico. El enrutamiento estático es preferible para redes pequeñas, mientras que el enrutamiento dinámico es ideal para redes grandes. (zenarmor, 2022).

Según sus propiedades, los protocolos de enrutamiento pueden clasificarse en distintas clases. En particular, pueden clasificarse según su comportamiento, propósito y funcionamiento.

- Comportamiento: Protocolo con clase (heredado) o sin clase.
- Propósito: Protocolo de puerta de enlace interior (IGP) o Protocolo de puerta de enlace exterior (EGP).
- Operación: Protocolo de vector de ruta, protocolo de vector de distancia y protocolo de estado de enlace.

Los protocolos de enrutamiento IPv4 se clasifican de la siguiente manera:

- RIPv1 (heredado): IGP, vector de distancia, protocolo con clases
- RIPv2: IGP, vector de distancia, protocolo sin clases
- OSPF: IGP, estado de enlace, protocolo sin clase
- IGRP: IGRP (heredado) es el protocolo IGP, de vector de distancia y de clase de Cisco (obsoleto a partir de la versión 12.2 IOS y posteriores)
- EIGRP: IGP, vector de distancia, protocolo sin clases
- EGP
- BGP: EGP, protocolo de vector de ruta sin clases
- IS-IS: Protocolo de Internet, estado de enlace, sin clases

Los protocolos de enrutamiento son mecanismos para intercambiar información de enrutamiento entre enrutadores y tomar decisiones de enrutamiento. Facilitan una comunicación eficaz y eficiente entre redes informáticas. Independientemente del tamaño de la red, estos protocolos facilitan la entrega segura de datos a su destino. Comprender las distintas categorías y tipos ayuda a determinar qué método de enrutamiento se adapta mejor a sus objetivos. (zenarmor, 2022).

II.4. Tecnologías de red LAN

II.4.1. VLAN

Una VLAN (Red de Área Local Virtual) es una red lógica que se crea dentro de una red física mayor. Las VLAN permiten segmentar una red en subredes virtuales más pequeñas, que pueden utilizarse para aislar el tráfico y mejorar el rendimiento de la red.

Las VLAN suelen utilizarse en redes empresariales para separar distintos departamentos o grupos, o para segmentar distintos tipos de tráfico (como voz, datos y vídeo). También pueden

utilizarse en redes domésticas para aislar distintos dispositivos o usuarios, o para separar las redes de invitados de la red principal. (ASUS, 2024)

II.4.2. VPN

VPN significa "Virtual Private Network" (Red privada virtual) y describe la oportunidad de establecer una conexión protegida al utilizar redes públicas. Las VPN cifran su tráfico en internet y disfrazan su identidad en línea. Esto les dificulta a terceros el seguimiento de sus actividades en línea y el robo de datos. El cifrado se hace en tiempo real.

Una VPN oculta su verdadera dirección IP al permitirle a la red redireccionarla por un servidor remoto especial, alojado por el proveedor de una VPN. Esto significa que, si navega en línea con una VPN, el servidor de la VPN se convierte en la fuente de sus datos. Esto significa que su Proveedor de servicios de internet (ISP) y otros terceros no pueden ver los sitios web que visita o qué datos envía y recibe en línea. Una VPN funciona como un filtro que convierte a todos sus datos en texto incomprensible. Si alguien lograra interceptar su información, de nada le sirve. (Lab, 2024).

II.5. Protocolos comunes para el transporte de datos

II.5.1. Transmission Control Protocol (TCP)

El protocolo TCP es, al igual que los protocolos UDP y SCTP, un protocolo de Internet que está ubicado en la capa de transporte del modelo OSI. El objetivo de TCP es crear conexiones dentro de una red de datos compuesta por redes de computadoras para intercambiar datos. Además, en cuanto a su funcionamiento, garantiza que los datos llegarán a destino sin errores y en el mismo orden en el que fueron transmitidos. También proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto. (WIKIPEDIA, 2024)

II.5.2. User Datagram Protocol (UDP)

UDP es un protocolo de transporte sin conexión, lo que significa que no establece una conexión antes de enviar datos, a diferencia de TCP, que establece una conexión antes de la transmisión. Esto hace que UDP sea más ligero y eficiente en términos de velocidad de transferencia de datos, pero también menos confiable, ya que no garantiza la entrega de paquetes en orden o la detección de errores. En lugar de una conexión, UDP utiliza datagramas, que son paquetes de datos independientes que se envían de un extremo a otro de la red. (nosololinux, 2023)

El funcionamiento de UDP es simple pero efectivo. Cuando una aplicación desea enviar datos a través de UDP, simplemente crea un datagrama que incluye la dirección del destinatario y el puerto de destino. Luego, este datagrama se envía a través de la red, donde puede atravesar múltiples dispositivos y routers antes de llegar a su destino. UDP no establece una conexión de tres vías como lo hace TCP, lo que significa que no hay un apretón de manos inicial. Esto permite una transmisión de datos más rápida, ya que no se requiere tiempo para establecer la conexión. (nosololinux, 2023).

II.6. Protocolos y servicios usados directamente en las aplicaciones

II.6.1. HTTP

El HTTP (del inglés HyperText Transfer Protocol o Protocolo de Transferencia de Hiper Textos) es el protocolo de transmisión de información de la World Wide Web, es decir, el código que se establece para que el computador solicitante y el que contiene la información solicitada puedan "hablar" un mismo idioma a la hora de transmitir información por la red. (Etecé, 2023)

Con el http se establecen criterios de sintaxis y semántica informática (forma y significado) para el establecimiento de la comunicación entre los diferentes elementos que constituyen la

arquitectura web: servidores, clientes, proxies. Se trata de un protocolo “sin estado”, vale decir, que no lleva registro de visitas anteriores, sino que siempre empieza de nuevo. La información relativa a visitas previas se almacena en estos sistemas en las llamadas “cookies”, almacenadas en el sistema cliente. (Etecé, 2023).

II.6.2. SMTP

Es un estándar técnico para la transmisión de correo electrónico a través de una red. Al igual que otros protocolos de red, SMTP permite a los ordenadores (computadoras) y servidores intercambiar datos independientemente de su hardware o software subyacente. Al igual que el uso de una forma estandarizada de escribir una dirección en un sobre permite el funcionamiento del servicio postal, el protocolo SMTP estandariza la forma en que el correo electrónico viaja del remitente al destinatario, permitiendo la entrega generalizada de correo electrónico (Cloudflare, s.f.)

El funcionamiento del SMTP se basa en una comunicación entre dos servidores de correo electrónico: el servidor de origen y el servidor de destino. El proceso de envío de un correo electrónico utilizando SMTP generalmente implica los siguientes pasos, conexión inicial, autentificación, preparación de mensajes, transferencia del mensaje, entrega al servidor destino, notificación de entrega y entrega al cliente de correo electrónico. (CM, s.f.)

II.6.3. FTP

Las siglas de FTP significan File Transfer Protocol, que se traduce como Protocolo de Transferencia de Archivos. Como su nombre indica, se trata de un protocolo que permite transferir archivos directamente de un dispositivo a otro.

FTP proporciona tareas tales como listar directorios remotos, cambiar el directorio remoto actual, crear y eliminar directorios remotos y transferir varios archivos en una sola petición. FTP

mantiene el transporte seguro pasando contraseñas de usuario y cuenta al sistema principal externo. Aunque FTP está principalmente diseñado para que lo utilicen las aplicaciones, también permite sesiones interactivas orientadas al usuario. (IBM, 2021).

II.6.4. DNS

El protocolo DNS (Domain Name System) de forma sencilla, traduce un dominio a una IP, como si de una agenda de contactos se tratase. Permite que con base en que dominio estés resolviendo y accediendo a la IP, esta te muestre una respuesta distinta, esto es lo que se conoce como Virtual Hosting (alojamiento compartido). Permite que en un mismo servidor se puedan almacenar varias webs. (Mena, 2023)

Esta es la idea base que sustenta el protocolo DNS, ahora bien, para que se lleve a cabo en la práctica es un poco más complejo. Antes de hablar de los tipos de servidores DNS, lo más importante es conocer la sintaxis y estructura de un dominio cuando de resolución DNS se trata: (Mena, 2023)

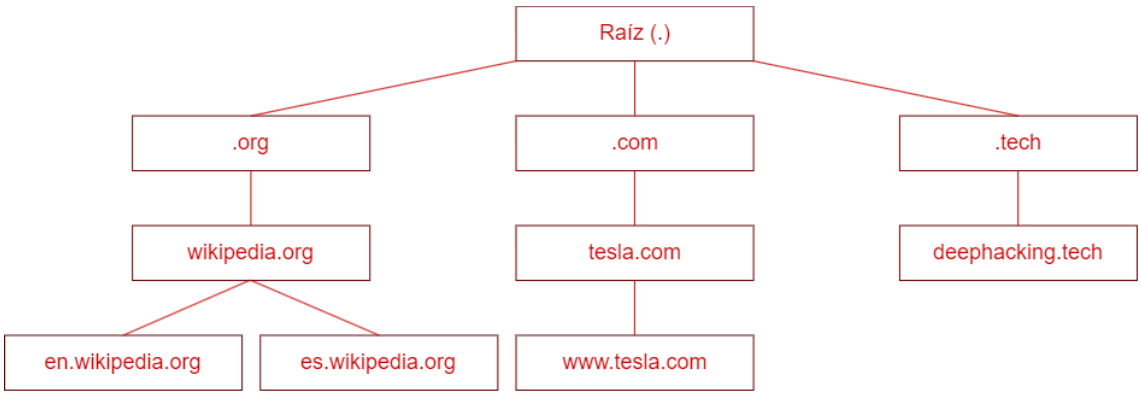


Figura II.6.1: ejemplo DNS
Fuente: Mena

II.7. Herramientas de software y simulación

II.7.1. Software utilizado

II.7.1.1. Cisco Packet Tracer

Cisco Packet Tracer es un programa de simulación de redes desarrollado por Cisco Systems. Este software se utiliza principalmente para crear y simular redes informáticas, permitiendo a los usuarios diseñar, configurar y poner en funcionamiento redes virtuales. (CCNA, s.f.)

También es una herramienta de aprendizaje ampliamente utilizada en la capacitación de redes y la preparación para exámenes de certificación de Cisco, como CCNA y CCNP. Con Cisco Packet Tracer, los usuarios pueden experimentar con diferentes configuraciones de red y escenarios sin la necesidad de hardware físico, lo que lo convierte en una herramienta valiosa para estudiantes y profesionales de redes. (CCNA, s.f.)

Cisco Packet Tracer tiende a ser más sencillo y menos exigente en términos de recursos de hardware en comparación con otras alternativas como GNS3. Esto significa que Packet Tracer es más fácil de usar para principiantes y puede funcionar en computadoras menos potentes. (CCNA, s.f.)

II.7.1.2. Wireshark

Es un analizador de protocolos de red, llamado analizador de paquetes, diseñado para proporcionar visibilidad del tráfico que se produce en una red o entre máquinas. Permite mirar desde el interior de la red y examinar los detalles del tráfico inalámbrico y por cable a varios niveles: desde la información a nivel de conexión hasta los bits que hacen un determinado paquete y los datos que contiene. Wireshark también permite visualizar la información en varios niveles de la pila, de modo que el operador puede aislar, identificar y depurar las conexiones de red desde los niveles más bajos hasta la capa de aplicación. (Abba, 2023)

II.7.1.3. GNS3

GNS3 (Graphic Network Simulation o Simulación Gráfica de Redes) es un simulador gráfico de red que permite diseñar topologías de red complejas y poner en marcha simulaciones sobre ellos. Con GNS3 los usuarios tendrán la posibilidad de poder escoger cada uno de los elementos que llegarán a formar parte de una red informática. GNS3 está estrechamente vinculada con: (Madrid, s.f.)

- Dynamips, un emulador de IOS que permite a los usuarios ejecutar binarias imágenes IOS de Cisco Systems.

- Dynagen, un front-end basado en texto para Dynamips

- Qemu, un emulador de PIX.GNS3 es una excelente herramienta complementaria a los verdaderos laboratorios para los administradores de redes de Cisco o las personas que quieren pasar sus CCNA, CCNP, CCIE DAC o certificaciones.

CAPÍTULO III:

COMPONENTE

III.1. Componentes I: Diseño mejorado de una nueva arquitectura de red para Cosaalt

Resumen de las metodologías utilizadas

La metodología usada para el rediseño de la red es la metodología TOP-DOWN que permite de forma estructurada abordar el diseño de redes poniendo un énfasis inicial en los objetivos y requisitos generales. Esta metodología puede conducir a soluciones más alineadas con las necesidades del negocio y facilitar una comunicación efectiva a lo largo del proceso.

La metodología se define por 6 fases de las cuales solo se desarrollarán 4 por qué se realizará una simulación de implementación de una red en lugar de realizarla físicamente.

Estas 4 fases son:

Fase 1: analizar requerimientos: esta fase se centrará en comprender y definir los requisitos de la red. Se recopilará los requisitos de rendimiento, escalabilidad, seguridad y otros aspectos relevantes para el diseño de la red.

Fase 2: Desarrollar diseño lógico: en esta fase, se elaborará el diseño lógico de la red, definiendo la arquitectura y los protocolos que se utilizarán. Se realizarán decisiones sobre la topología de red y otros aspectos lógicos.

Fase 3: Desarrollar diseño físico: Al no realizarse una implementación física, esta fase se adaptará para definir la configuración y disposición de los componentes en el entorno de simulación. Se determinará la infraestructura necesaria, incluyendo los dispositivos de red y las conexiones entre ellos.

Fase 4: Probar, optimizar y documentar diseño: esta fase será crucial para el proceso de simulación. Se realizarán pruebas de diseño de la red en el entorno virtual, utilizando Cisco Packet

Tracer y GNS3. Se identificarán y corregirán problemas y se documentarán los resultados obtenidos durante las pruebas.

III.1.1. Fase 1: Análisis de requerimiento

III.1.1.1. Analizar las metas del negocio

La cooperativa de servicios públicos de agua potable y alcantarillado sanitario de Tarija presta diferentes tipos de servicios dentro del área de la ciudad de Tarija, llegando a muchos barrios de la ciudad, brindando una mejor calidad de vida a sus consumidores.

Misión

Garantizar el suministro de agua potable, así como la recolección y disposición de las aguas servidas dentro de los parámetros de calidad, eficiencia y economía necesarios para atender satisfactoriamente a la población actual y futura de la ciudad de Tarija.

Visión

Ser una EPSA líder en el Sur de Bolivia, comprometida con la mejora continua en la prestación de los servicios de agua potable y alcantarillados sanitario, con calidad a la ciudad de Tarija.

III.1.1.2. Analizar las metas técnicas

Se busca un nuevo diseño de red con la finalidad de mejorar la red de datos de Cosaalt. Para el diseño de red propuesto se tomarán en cuenta la seguridad, escalabilidad y flexibilidad.

A partir de este rediseño de datos se busca mejorar los servicios de información en nivel interno para cumplir con las distintas actividades laborales de los usuarios de distintas áreas.

Seguridad: es necesario que la res de datos y los servicios de Cosaalt se mantengan a través de un sistema de seguridad, evitando que usuarios no autorizados provenientes del exterior puedan

acceder a la información de Cosaalt. Considerando que es necesario un firewall perimetral interpuesto después del router del proveedor de servicio y de esta manera será controlado el tráfico de la red actual. También contará con una segmentación de Vlans.

Flexibilidad: se busca que no exista problemas de interoperabilidad y despliegue de aplicaciones o servicios.

Escalabilidad: es posible que la empresa alcance a incorporar dispositivos a su red satisfaciendo la demanda futura.

III.1.1.3. Analizar red existente

Para realizar el análisis de la red actual de Cosaalt, se llevó a cabo una visita a la empresa con el objetivo de colaborar en la mejora de la arquitectura de su red. Durante la visita, se entrevistó al encargado de TI para obtener información detallada sobre el funcionamiento actual de la red. A través de esta entrevista, se pudo recopilar datos fundamentales sobre la infraestructura de datos existente en Cosaalt, la cual cuenta de un diseño lógico no documentado y tampoco de una documentación estructurada de las direcciones IP utilizadas.

Cosaalt cuenta con 66 puntos de red, cuentan con 4 racks de diferentes tamaños, la banda ancha de la empresa es de 60 Mbps.

En Cosaalt, la red está organizada mediante el uso de VLANs (Virtual Local Área Networks) para asegurar una gestión eficiente y segura de sus recursos de red. Originalmente, el edificio principal utilizaba la dirección de red 192.25.3.0/24 para todas sus operaciones internas, asignando direcciones IP estáticamente por piso. Sin embargo, debido a un crecimiento no estructurado de la empresa, la asignación de direcciones IP se ha vuelto desorganizada y no existe documentación adecuada. Los

nuevos equipos ahora reciben direcciones IP sin seguir el esquema original de asignación por piso, lo cual dificulta significativamente la gestión y localización de direcciones IP en la red.

La red con la que cuenta Cosaalt está diseñada de la siguiente manera:

Dirección de red para equipos de cómputo 192.25.3.0

Dirección de red para equipos móviles 192.25.2.0

Dirección de red para equipos de impresoras 192.25.1.0

Como se puede ver en la siguiente tabla, Cosaalt destina 6 direcciones IP para cada punto de pago exterior a través de la subred 192.25.6.0

Edificio	**Dirección de Red**	**Mascará**
Banco Sol	192.25.6.2	255.255.255.128
Churqui	192.25.6.3	255.255.255.128
Catedral	192.25.6.4	255.255.255.128
Cooperativa Madre y Maestra	192.25.6.6	255.255.255.128
Fassil	192.25.6.12	255.255.255.128
Prodem	192.25.6.18	255.255.255.128
Total, de Hosts asignados		126

Tabla 11: Ips designadas a bancos
Fuente: Elaboración propia

III.1.1.3.1. Estructura de la red

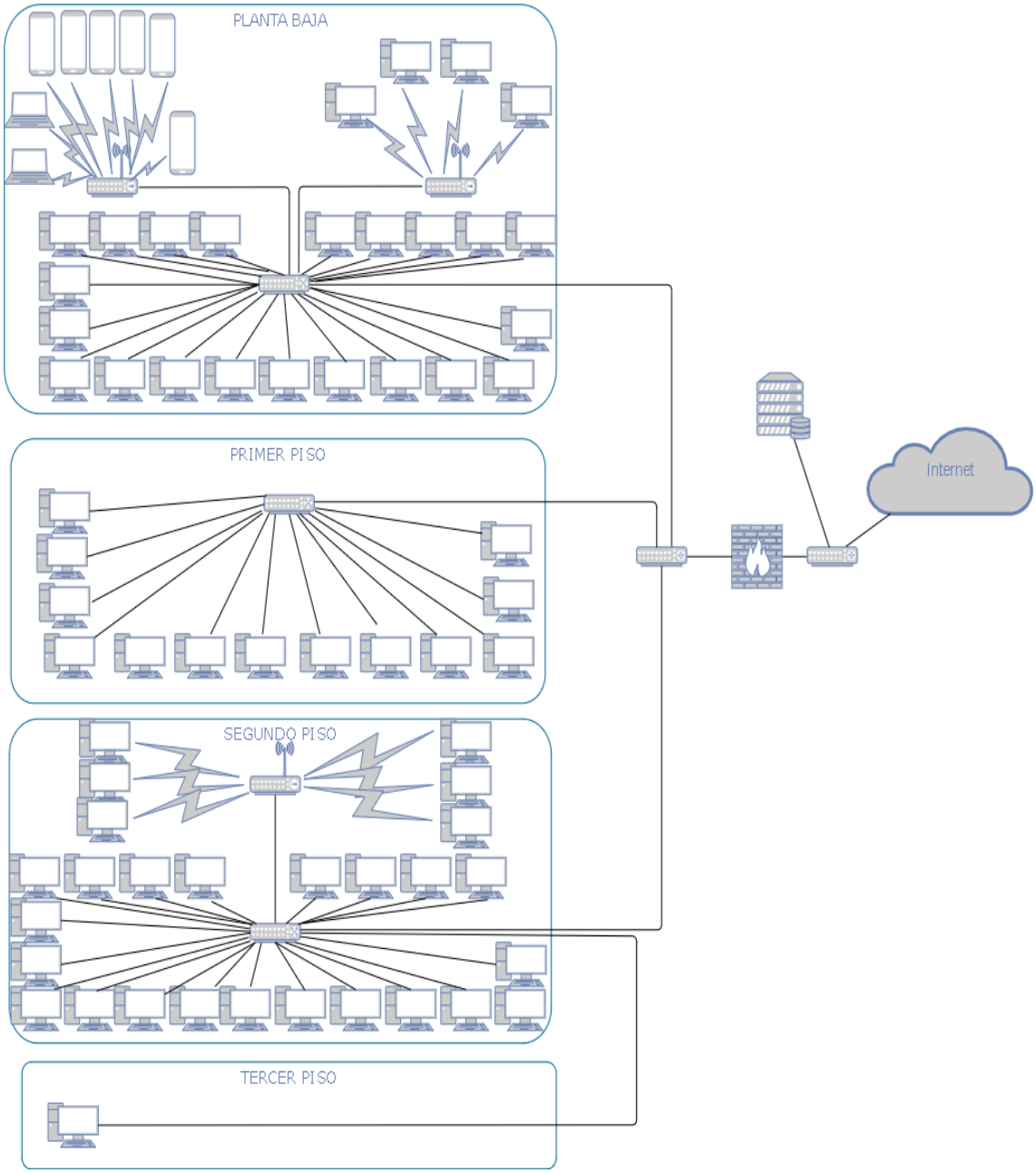


Figura III.1.1: arquitectura de la red de Cosaalt
Fuente: Elaboración propia

La figura proporciona una visión clara de cómo se estructuran los componentes de la red de Cosaalt, en donde se muestra la cantidad exacta de los equipos y la forma en la que se encuentran conectados entre sí.

Cosaalt para el vínculo entre pisos usa cable estructurado de categoría 6, la red actual se inicia desde el router del proveedor TIGO el cual brinda un servicio de internet de 50 Mbps, que es distribuida por todos los pisos del edificio principal de Cosaalt. Este router se conecta hacia los servidores con seguridad mediante firewall.

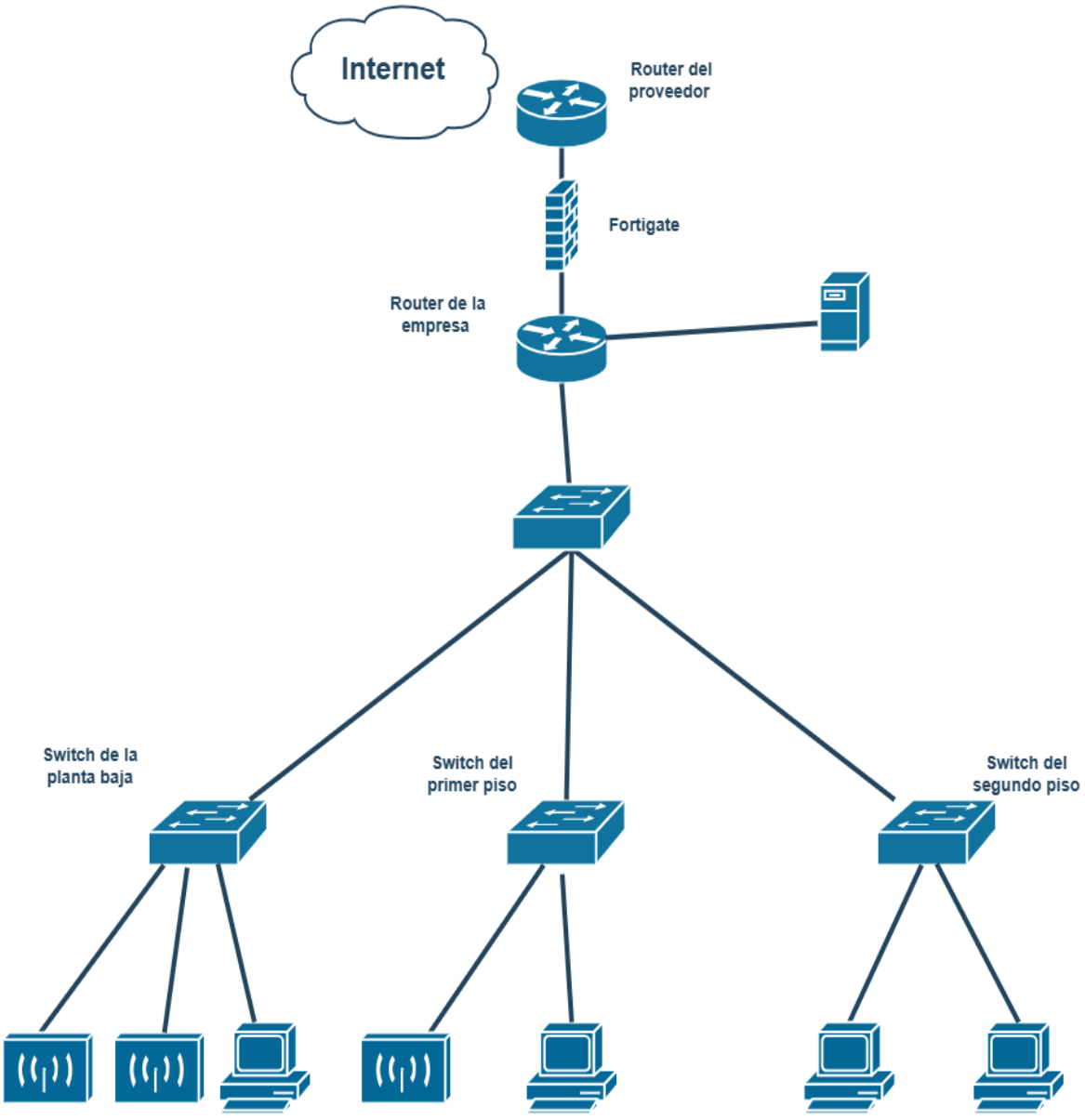


Figura III.1.2: Topología de red de Cosaalt
Fuente: Elaboración propia

La red actual de Cosaalt se basa en una topología mixta, principalmente estrella con elementos lineales, donde varios puntos de acceso están conectados a un núcleo central. La infraestructura incluye una variedad de dispositivos clave como router, switches administrables y no administrables, así como puntos de acceso distribuidos estratégicamente para dar cobertura a la red.

La topología está centralizada en un núcleo principal ubicado en el centro de datos del edificio, específicamente en el primer piso. Este núcleo central alberga los principales equipos de red y servidores críticos para el funcionamiento de la red. Los equipos como routers gestionan el tráfico de datos entrante y saliente, mientras que los switches administran la conectividad dentro de cada piso y entre ellos.

En cuanto a la distribución de dispositivos, se cuenta con un total de 2 routers (uno activo y el otro inactivo) instalados en el centro de datos principal (MDF). Además,se utilizan 4 switches para la interconexión de dispositivos en cada piso, con switches principales ubicados en el primer piso (MDF) y nodos distribuidos en la planta baja y otros pisos del edificio. La conectividad entre estos equipos se realiza mediante cable UTP.

Para seguridad, la red utiliza segmentación mediante VLANs con subredes, separando la red que utilizan las entidades financieras y la red del edificio principal. Además, para controlar y filtrar el acceso desde y hacia internet, se utiliza firewall perimetral. El firewall perimetral gestiona el acceso desde y hacia internet, el firewall de Mikrotic, aunque no está configurado de manera óptima con funciones avanzadas como el filtrado de paquetes, desempeña un papel crucial en la seguridad y gestión de la red, el firewall realiza NAT para traducir direcciones IP internas a direcciones públicas, manteniendo la privacidad de la topología de red interna y mejorando la seguridad global.

Especificación de los equipos de la red actual

N°	Equipo	Marca	Cantidad
1	Computadoras cableadas		54
2	Computadoras inalámbricas		15
3	Router/firewall	Mikrotic	1
4	Switch	Tplink	3
5	Firewall	UNIPER	1
6	Servidor	Dell	1
7	servidor	IBM	3
8	Switch	DLINK	1
9	Router	DLINK	1
	Impresoras		56

Tabla 12: especificación de los equipos de red actual
Fuente: Elaboración propia

Con el crecimiento de la cooperativa y la expansión de algunas oficinas o dependencias, se ha visto en la necesidad de implementar punto de acceso inalámbrico para algunos puestos de trabajo que lo requieran, como es el caso del área de facturación y lecturación. Estas áreas experimentan problemas de conexión en sus dispositivos, lo que puede resultar en fluctuaciones en la calidad de la señal y la velocidad de transmisión. Las redes inalámbricas, aunque ofrecen flexibilidad, son más vulnerables a instrucciones y ataques de seguridad. Además, la calidad de la señal inalámbrica puede verse afectada por interferencias externas, obstáculos físicos y la distancias desde los puntos de acceso

Cosaalt utiliza tres puntos de acceso inalámbrico ubicados en el primer piso y el otro en el segundo piso como se puede apreciar en la figura 3.1.1 y 3.1.2.

III.1.1.3.2. Direcciones de red actual separadas por pisos

Con la información recolectada y la información dada por el encargado de TI, se pudo obtener el direccionamiento de los equipos conectados a la red.

Planta baja

SALA	DIRECCIÓN IP	Mascará
Odeco	192.25.3.45	255.255.255. 128
Odeco	192.25.3.47	255.255.255. 128
Odeco	192.25.3.46	255.255.255. 128
Caja 1	192.25.3.20	255.255.255. 128
Caja 2	192.25.3.21	255.255.255. 128
Caja 3	192.25.3.22	255.255.255. 128
Caja 4	192.25.3.23	255.255.255. 128
Atención al cliente	192.25.3.346	255.255.255. 128
Atención al cliente	192.25.3.41	255.255.255. 128
Atención al cliente	192.25.3.43	255.255.255. 128

Atención al cliente	192.25.3.130	255.255.255. 128
Atención al cliente	192.25.3.34	255.255.255. 128
Atención al cliente	192.25.3.40	255.255.255. 128
Atención al cliente		255.255.255. 128
Morosidad	192.25.3.30	255.255.255. 128
Secretaria de gerencia comercial	192.25.3.25	255.255.255. 128
Gerencia comercial	192.25.3.33	255.255.255. 128
Archivos	192.25.3.171	255.255.255. 128
Archivos	192.25.3.246	255.255.255. 128
Archivos	192.25.3.61	255.255.255. 128
Archivos	192.25.3.241	255.255.255. 128
Recursos humanos	192.25.3.62	255.255.255. 128
Recursos humanos	192.25.3.37	255.255.255. 128
Facturación	192.25.3.29	255.255.255. 128

Facturación	192.25.3.159	255.255.255. 128
Facturación	192.25.3.42	255.255.255. 128
Facturación	192.25.3.158	255.255.255. 128
Facturación	192.25.3.171	
Facturación	192.25.3.172	

Tabla 13: Direcciones de la planta baja
Fuente: Elaboración propia

Primer piso

SALA	DIRECCIÓN IP	MASCARA
Secretaria	192.25.3.99	255.255.255. 128
Secretaria	192.25.3.129	255.255.255. 128
Gerencia general	192.25.3.92	255.255.255. 128
Secretaria de consejo de administración	192.25.3.104	255.255.255. 128
Consejo de administración	192.25.3.85	255.255.255. 128

Consejo de administración	192.25.3.84	255.255.255. 128
Sistemas de computación	192.25.3.81	255.255.255. 128
Sistemas de computación	192.25.3.32	255.255.255. 128
Auditoria y asesoría	192.25.3.91	255.255.255. 128
Auditoria y asesoría	192.25.3.179	255.255.255. 128
Auditoria y asesoría	192.25.3.101	255.255.255. 128
Auditoria y asesoría	192.25.3.102	255.255.255. 128
Auditoria y asesoría	192.25.3.	255.255.255. 128
Auditoria y asesoría	192.25.3.103	255.255.255. 128

Tabla 14: Direcciones del primer piso
Fuente: Elaboración propia

Segundo piso

SALA	DIRECCIÓN IP	MASCARA

Operación de mantenimientos de obras	192.25.3.15	255.255.255. 128
Operación de mantenimientos de obras	192.25.3.87	255.255.255. 128
Operación de mantenimientos de obras	192.25.3.14	255.255.255. 128
Operación de mantenimientos de obras	192.25.3.19	255.255.255. 128
Operación de mantenimientos de obras	192.25.3.59	255.255.255. 128
Operación de mantenimientos de obras	192.25.3.94	255.255.255. 128
Operación de mantenimientos de obras	192.25.3.245	255.255.255. 128

Operación de mantenimientos de obras	192.25.3.239	255.255.255. 128
Secretaria gerencia técnica	192.25.3.90	255.255.255. 128
Gerencia técnica		255.255.255. 128
Gerencia administrativa y financiera	192.25.3.152	255.255.255. 128
Gerencia administrativa y financiera	192.25.3.112	255.255.255. 128
Gerencia administrativa y financiera	192.25.3.111	255.255.255. 128
Contabilidad	192.25.3.162	255.255.255. 128
Contabilidad	192.25.3.121	255.255.255. 128
Contabilidad	192.25.3.97	255.255.255. 128
Contabilidad	192.25.3.117	255.255.255. 128

Contabilidad	192.25.3.166	255.255.255. 128
Contabilidad	192.25.3.118	255.255.255. 128
Contabilidad	192.25.3.156	255.255.255. 128
Contabilidad	192.25.3.116	255.255.255. 128
Contabilidad	192.25.3.251	255.255.255. 128
Topografía catastro	192.25.3.127	255.255.255. 128
Topografía catastro	192.25.3.157	255.255.255. 128
Topografía catastro	192.25.3.126	255.255.255.128

Tabla 15: Direcciones del segundo piso
Fuente: Elaboración propia

Tercer piso

SALA	DIRECCIÓN IP	MASCARA
Consejo de vigilancia	192.25.3.119	255.255.255.128
Consejo de vigilancia	192.25.3.170	255.255.255.128

Tabla 16: Direcciones del tercer piso
Fuente: Elaboración propia

Rango de direcciones de redes inalámbricas

Piso	Rango de direcciones	Mascará
Planta baja (lecturadores y pasantes)	192.25.2.140 - 192.25.2.159	255.255.255.0
Plana baja	192.25.3.161 – 192.25.3.170	255.255.255.0
Segundo piso	192.25.3.86 – 192.25.3.100	255.255.255.0

Tabla 17: Direcciones inalámbricas
Fuente: Elaboración propia

III.1.1.3.3. Distribución de MDF e IDFs

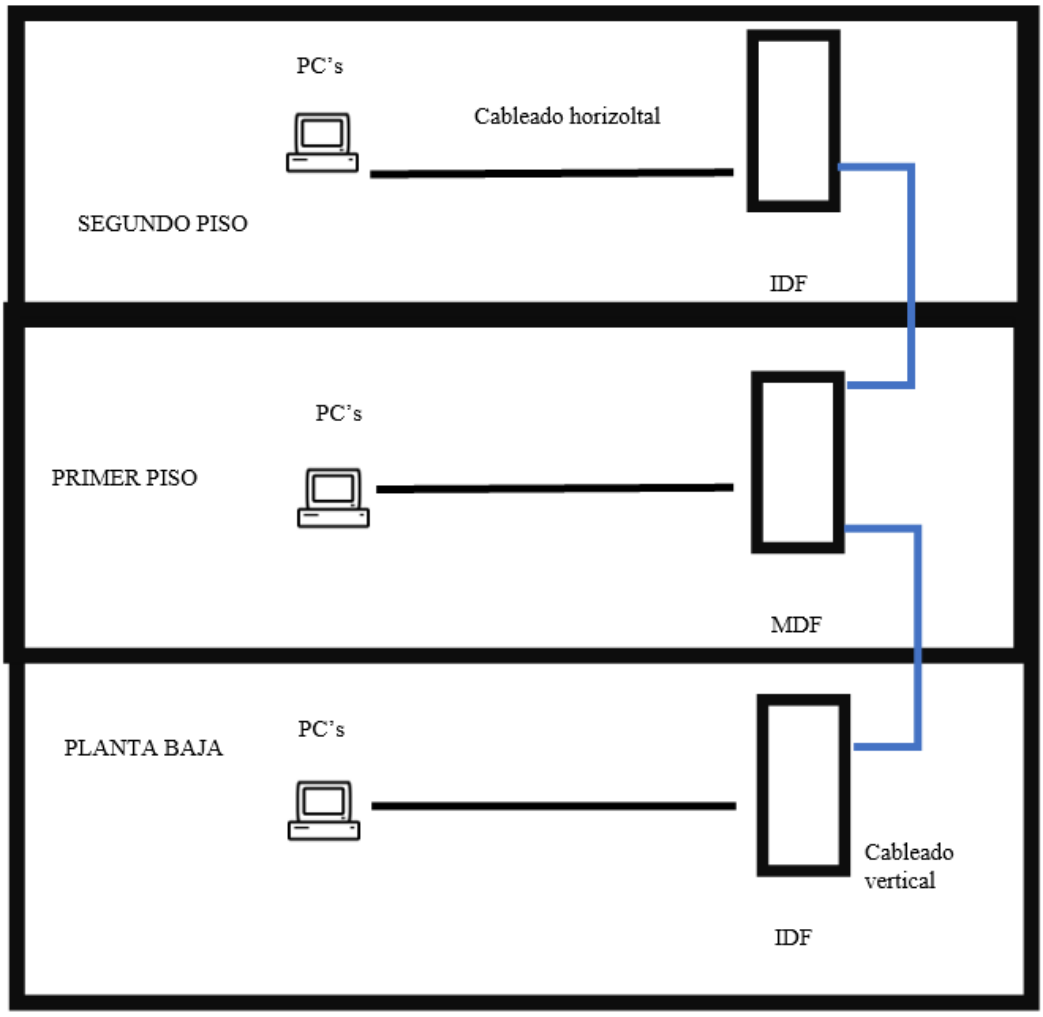


Figura III.1.3: Ejemplo de distribución de centrales de Cosaalt
Fuente: Elaboración propia

Esta figura muestra cómo la disposición de los racks de Cosaalt, donde el cable negro representa el cable UTP y el azul indica la conexión de switch a switch. Actualmente, los cables no se encuentran etiquetados debidamente, esto ocasiona problemas al momento de resolver algún inconveniente suscitado.

La habitación que alberga el Cuarto de Telecomunicaciones Principal (MDF, por sus siglas en inglés) funciona como oficina para los encargados de TI y está equipada con dos sistemas de aire acondicionado independientes para los armarios de equipo. Actualmente, en esta sala operan cuatro

servidores, de los cuales tres están activos. Estos servidores son dedicados a funciones críticas como Base de Datos, Calidad de Servicio y servicios web, ejecutándose en hardware físico dedicado.

Lamentablemente, el diseño del MDF no cumple con los estándares óptimos de seguridad y protección. El cuarto fue ubicado de manera provisional dentro del área de sistemas, separado por una única puerta y paredes de vidrio que incluyen dos ventanas. Esta configuración no cumple con las políticas de seguridad recomendadas para un MDF, exponiendo el equipo a posibles riesgos de acceso no autorizado y comprometiendo la integridad de los datos y la continuidad operativa.

Además, la sala presenta un exceso de cables desorganizados, lo cual no solo afecta la estética y el orden, sino que también incrementa el riesgo de fallos operativos y dificulta la gestión eficiente de la red. Este desorden no solo obstaculiza las tareas de mantenimiento y solución de problemas, sino que también afecta negativamente la eficiencia del entorno de TI en general. Esto no solo compromete su función como centro de control, sino que también se utiliza como un espacio de almacenamiento adicional, como se puede observar en las imágenes adjuntas.

Figura III.1.4: Imagen real del MDF
Fuente: Elaboración propia

Figura III.1.5: Servidores del MDF
Fuente: Elaboración propia

En la infraestructura de red de la empresa, se observa una leve falta de organización en el manejo de cables, lo cual representa un problema significativo tanto estético como funcional. En varias áreas, como el centro de datos y otras oficinas. Se pueden ver cables colgando de los racks de servidores, serpentinas de cables en el suelo y cables apilados en las esquinas, creando un entorno propenso a interrupciones y dificultades en el mantenimiento.

Este desorden no solo afecta la apariencia profesional del entorno de trabajo, sino que también plantea serios riesgos de seguridad y operativos. Según las normativas estándar de seguridad y buenas prácticas en gestión de redes, tales como las establecidas por la ANSI/TIA-942 y otras regulaciones locales, la organización adecuada del cableado es fundamental. Los cables visibles y mal gestionados

aumentan el riesgo de accidentes físicos, como tropiezos y caídas, además de posibles daños accidentales al equipo de red.

Además de los riesgos físicos, la falta de organización afecta la capacidad de diagnóstico y resolución de problemas en la red. Identificar y aislar un cable específico para mantenimiento o reparación se vuelve una tarea ardua y prolongada, lo cual impacta negativamente en la disponibilidad y rendimiento de los servicios de TI.

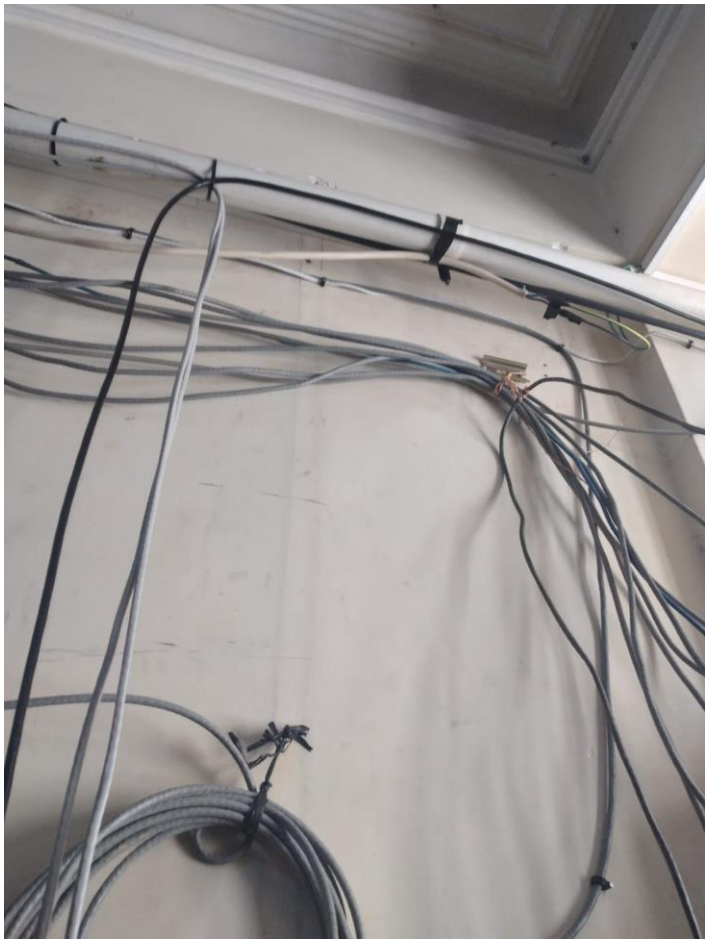


Figura III.1.6: Cableado actual de Cosaalt
Fuente: Elaboración propia

III.1.1.4. Problemas encontrados en el análisis de la red existente

Crecimiento no planificado y falta de documentación:

La red de Cosaalt ha experimentado un crecimiento no planificado, resultando en una asignación caótica de direcciones IP y una falta significativa de documentación. Esta falta de estructura dificulta la gestión eficiente de la red y la localización precisa de recursos.

Incumplimiento de la norma ANSI/TIA 942 para cableado físico:

El diseño físico de la red en Cosaalt no cumple con los estándares de la norma ANSI/TIA 942 ni de la norma ANSI/TIA-606-B, lo cual compromete la confiabilidad y la capacidad de expansión de la infraestructura de cableado. Esto puede afectar la estabilidad y el rendimiento general de la red.

Desorganización y condiciones del cuarto del MDF:

La organización del cuarto del Main Distribution Frame (MDF) no está adecuadamente mantenida, lo que aumenta el riesgo de fallos de infraestructura y dificulta las operaciones de mantenimiento y actualización.

Problemas de conectividad y velocidad de internet:

Existen problemas significativos con la velocidad de internet y la estabilidad de la red en varias áreas de trabajo. Esto afecta la productividad y la eficiencia operativa de los empleados que dependen de conexiones rápidas y estables.

Ausencia de segmentación eficiente de la red para las áreas de trabajo dentro del edificio principal:

La falta de segmentación en una misma Subred genera muchos cuellos de botella sobre todo a finales de mes donde el movimiento laboral es mayor.

Uso inalámbrico ineficiente para equipos de trabajo fijo:

Algunos equipos de trabajo están conectados de manera inalámbrica a la red, a pesar de ser estacionarios. Esto puede resultar en una conexión menos confiable y un rendimiento inferior en comparación con una conexión cableada.

Falta de filtrado de paquetes en el firewall:

El firewall de la red no está configurado con un filtrado adecuado de paquetes, lo que representa un riesgo significativo de seguridad al permitir el tráfico no autorizado o malicioso dentro de la red.

Diseño de red no adaptado a necesidades y falta de escalabilidad:

El diseño actual de la red en Cosaalt no ha sido ajustado para satisfacer las necesidades operativas actuales ni para ser escalable frente a futuros crecimientos. Esto limita la capacidad de la empresa para adaptarse rápidamente a cambios en la demanda y en la tecnología.

III.1.1.5. Analizar tráfico existente

Cosaalt, una empresa de servicios de agua y alcantarillado en Tarija, opera con una infraestructura de red basada en una única dirección IP (192.25.3.0/24), sin segmentación mediante VLANs. Esto implica que todo el tráfico, tanto interno como externo, circula por el mismo espacio de red, lo cual genera una carga significativa y riesgos de congestión. La capacidad de ancho de banda disponible es de 50 Mbps, administrada por el servidor de Quality of Service (QoS), encargado de distribuir los recursos de manera eficiente según las necesidades de cada área.

Condiciones Operativas del Tráfico de Red

1. Tráfico General y Servicios Corporativos

El tráfico generado por correo electrónico y navegación web es constante en todas las áreas. La administración, atención al cliente y gerencia son las que más utilizan estos servicios para comunicarse internamente y con clientes externos. Aunque el uso de este tipo de tráfico es menor en comparación con otras aplicaciones, su constante demanda ocupa aproximadamente un 15% del ancho de banda total.

2. Transferencia de Archivos y Consultas a Sistemas Internos

La transferencia de archivos es una actividad recurrente, particularmente en contabilidad, recursos humanos y facturación. Documentos financieros, contratos y reportes se comparten regularmente, lo que representa un 20% del ancho de banda. Además, las consultas a los sistemas de planificación de recursos y gestión de quejas y reclamos generan un tráfico importante, especialmente desde áreas operativas como caja, facturación y atención al cliente. Este tráfico puede alcanzar un 30% del ancho de banda, reflejando la necesidad de acceso en tiempo real a datos administrativos y comerciales.

3. Bases de Datos y Servicios Web

El acceso a las bases de datos de clientes y medidores es fundamental para las áreas de caja y atención al cliente, generando un tráfico significativo debido a las constantes actualizaciones y consultas relacionadas con el consumo y los reclamos. Este componente utiliza alrededor del 25% del ancho de banda, lo que pone en evidencia la necesidad de priorizar este tráfico para garantizar la fluidez de las operaciones. A esto se suma el tráfico de servicios web internos y portales externos, que aunque menor, representa un 10% del ancho de banda debido a la consulta de información y gestión en línea por parte de empleados y usuarios.

Proyección Futura: Implementación de IoT y SCADA

Cosaalt prevé la futura integración de dispositivos IoT y sistemas SCADA para monitorear en tiempo real la red de suministro y control de estaciones de bombeo. Esto implicará una conexión directa entre medidores inteligentes ubicados en los hogares y la red central de la empresa. Aunque actualmente estos dispositivos no generan tráfico, su implementación futura requerirá un análisis detallado para segmentar el tráfico mediante una VLAN específica, evitando que sobrecarguen la red principal.

Los porcentajes indicados no son sumatorios, sino orientativos para gestionar el tráfico en diferentes situaciones. No significan que el ancho de banda esté reservado permanentemente, sino que indican qué fracción del ancho de banda disponible podrá usarse según la prioridad del tráfico actual.

Sistemas de operaciones diarias especificadas por áreas.

El Sistema de Atención y Servicios al Cliente en Línea involucraría varias áreas de Cosaalt para garantizar su funcionamiento eficiente y alineación con los objetivos organizacionales.

1. Atención al Cliente y ODECO (Oficina de Defensa del Consumidor):

    - Sistema de Gestión de Quejas y Reclamos: Para documentar, gestionar y resolver problemas de clientes de manera eficiente.

2. Facturación y Morosidad:

    - Sistema de Facturación: para la emisión de facturas.

3. Caja:

    - Sistema de Punto de pagos: Para la recepción de pagos y emisión de recibos, integrando las transacciones con el sistema de facturación.

4. Gerencia Comercial:

    - Sistema de planificación de recursos: Para la gestión integrada de ventas, finanzas y relación con los clientes.

5. Recursos Humanos:

- Sistema de Gestión de Personal (HRMS): Para el control de nóminas, asistencia, evaluaciones de desempeño y capacitaciones.

6. Auditoría y Asesoría Legal:

- Sistema de Gestión Documental: Para gestionar y almacenar documentos legales, auditorías y registros de cumplimiento normativo.

7. Contabilidad y Gerencia Administrativa y Financiera:

- Sistema Contable: Para llevar registros financieros, generación de reportes y cumplimiento tributario.
- Gestión de Presupuestos: Para el control de gastos y planificación financiera.

8. Gerencia Técnica, Topografía y Mantenimiento:

- Sistemas GIS (Geographic Information System): Para la gestión y análisis de datos geoespaciales relacionados con la red de agua y alcantarillado.

9. Consejo de Administración y Vigilancia:

- Sistemas de Gestión de Reuniones y Documentación: Para mantener registros de decisiones, actas y reuniones.

10. Sistemas de Computación:

- Sistema de Seguridad de la Información: Incluye firewalls, antivirus, y sistemas de detección y prevención de intrusiones.

El estado actual de la red de Cosaalt revela una sobrecarga potencial debido a la falta de segmentación. La administración eficiente del ancho de banda por el servidor QoS permite mantener la operatividad, pero es crucial implementar una estrategia de segmentación por VLANs para optimizar el uso del ancho de banda, garantizar la seguridad y preparar la infraestructura para futuros proyectos tecnológicos, como el IoT y SCADA. Esta planificación será esencial para la escalabilidad y sostenibilidad de la red.

Debido a consideraciones de privacidad relacionadas con las cajas de pago y las cuentas de la empresa, no fue posible realizar una evaluación exhaustiva del tráfico actual. En su lugar, se llevó a cabo un cálculo estimado del tráfico en la red. Este cálculo se basó en parámetros generales de uso y demanda, permitiendo una comprensión aproximada de las necesidades de ancho de banda y capacidad de la red.

III.1.2. Fase 2: Desarrollar diseño lógico

Diagrama lógico

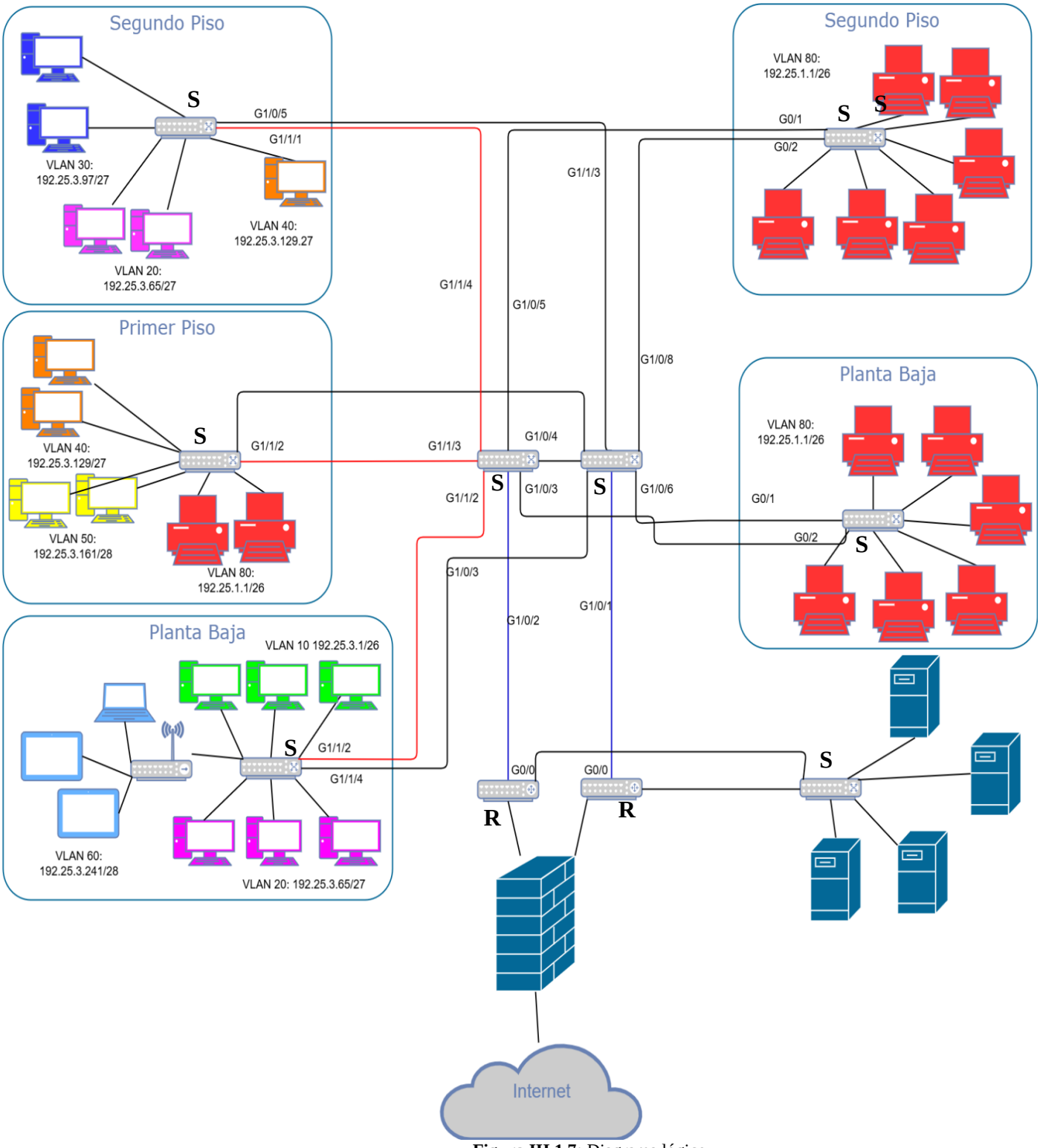


Figura III.1.7: Diagrama lógico
Fuente: Elaboración propia

III.1.2.1. Diseño de la topología de red

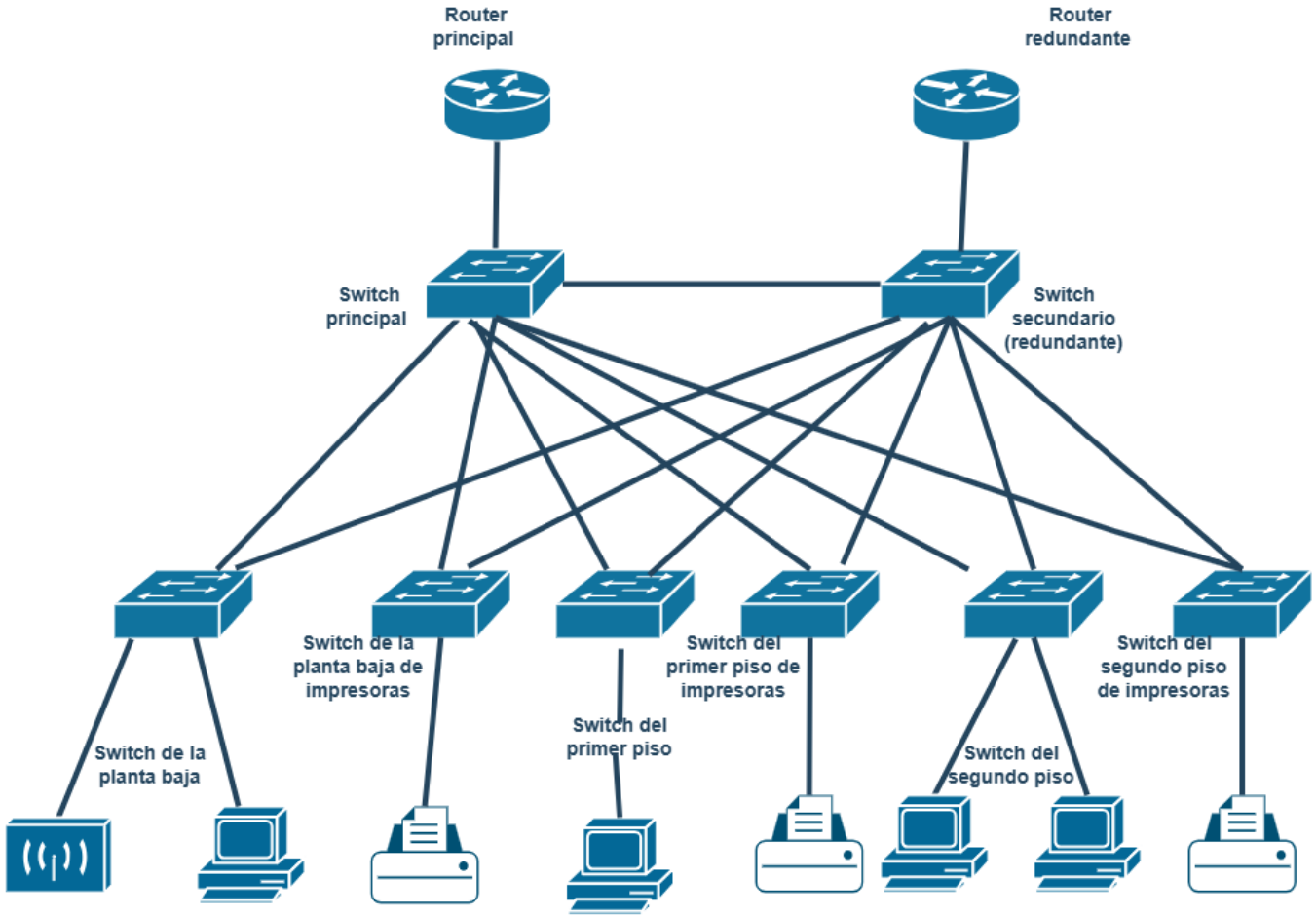


Figura III.1.8: Nueva topología de red
Fuente: Elaboración propia

El diseño mezcla características de dos tipos de topologías principales:

Topología de estrella:

Los dispositivos finales están organizados de forma jerárquica y conectados a un switch de acceso por piso, formando estrellas locales.

Topología en malla parcial:

Los enlaces redundantes entre MDF1, MDF2 y los IDFs son típicos de una malla parcial, diseñada para proporcionar resiliencia y alta disponibilidad.

Desde los switches principales, la red se extiende hacia 5 switches de acceso mediante conexiones redundantes. Esta configuración redundante garantiza que haya múltiples rutas disponibles para la transmisión de datos entre los switches principales y los dispositivos finales. Esta redundancia mejora la tolerancia a fallos y optimiza la disponibilidad de red al proporcionar rutas alternativas para el tráfico en caso de problemas en una ruta específica.

El diseño de red de Cosaalt se fundamenta en una topología jerárquica que incorpora redundancia y escalabilidad para asegurar un funcionamiento robusto y flexible. En el corazón de este diseño se encuentran dos switches de núcleo, Core-SW1 como primario y Core-SW2 como secundario, conectados entre sí mediante un enlace troncal. Este enfoque proporciona redundancia y balanceo de carga, permitiendo que la red mantenga su integridad operativa incluso ante la falla de uno de los switches principales.

Core-SW1 despliega un rol central, gestionando la conexión principal de la red y actuando como el punto focal para todos los switches de piso, el router, el firewall y los servidores. Core-SW2, por su parte, actúa como backup de Core-SW1, asegurando continuidad operativa al estar conectado de manera redundante a los mismos dispositivos críticos.

La conectividad a nivel de piso se establece mediante switches distribuidos en diferentes áreas (Piso 1, Piso 2, Piso 3), los cuales están conectados tanto a Core-SW1 como a Core-SW2 mediante enlaces troncales. Estos enlaces troncales permiten que el tráfico fluya a través de rutas alternativas, garantizando que la red mantenga su conectividad incluso en caso de fallos locales o parciales.

El firewall se posiciona estratégicamente para controlar y filtrar el tráfico entre la red interna y externa, asegurando así la seguridad perimetral y facilitando la segmentación de la red para mejorar la protección y el control de acceso.

Además, la inclusión de servidores dedicados para funciones críticas como DHCP para cada VLAN y gestión de red (SNMP, Syslog, etc.) y 2 servidores de Base de Datos, optimiza la eficiencia operativa y la capacidad de respuesta de la red ante las demandas cambiantes del entorno empresarial.

Este diseño no solo garantiza una escalabilidad sin complicaciones, adaptándose a las necesidades de crecimiento de la empresa, sino que también ofrece una alta disponibilidad y resiliencia operativa mediante la redundancia cuidadosamente implementada a nivel de núcleo y de acceso. La estructura jerárquica y la configuración de enlaces troncales permiten una gestión eficaz del tráfico y una rápida recuperación ante eventos adversos, asegurando así un rendimiento óptimo y seguro de la red de Cosaalt.

III.1.2.2. Conectividad Lógica:

- Los routers gestionan el tráfico entre la red interna y externa, garantizando la seguridad y el acceso adecuado a recursos de Internet.
- El Main Switch maneja la distribución del tráfico entre los diferentes switches de acceso y los dispositivos finales dentro de la red interna.
- Cada switch de acceso proporciona conexiones locales optimizadas para dispositivos finales en cada piso del edificio.
- **Firewall**: Controla el tráfico entrante y saliente, implementa políticas de seguridad como filtrado de paquetes, VPN, y protección contra intrusiones.

Cabe mencionar que en cada terminal se encuentra una tarjeta de interfaz de red (NIC) que permite el intercambio de datos y servicios. Estas tarjetas NIC están equipadas con un conector RJ45 (Registered Jack), que se conecta a un panel de parcheo mediante un cable UTP (Unshielded Twisted Pair) de categoría 6A.

N°	Especificaciones	Cat 5	Cat 5e	Cat 6	Cat 6a
1	Frecuencia	100 MHz	100 MHz	250 MHz	500 MHz
2	Atenuación (min. A 100 Mhz)	22 db	22 db	19.8 db	--
3	Perdida de retorno (min. A 100 Mhz)	16 db	20.1 db	20.1 db	8 db
4	Redes soportadas	100 BASE-T	100 BASE-T	100 BASE-TX	10 GBASE

Tabla 18: Elección de cable de red
Fuente: Elaboración propia

Para el diseño físico de la red, utilizaremos cable UTP categoría 6A, que tiene un diámetro exterior de 8.3 mm y un radio de curvatura mínimo de 33 mm. Este cable está diseñado para operar en un rango de temperatura de -10 °C a 60 °C y soporta velocidades Ethernet de hasta 10 Gbps, lo que garantiza que será adecuado para futuras expansiones de ancho de banda.

Todo el cableado estructurado estará conforme a la norma TIA/EIA-568-B, que define las pautas para el diseño e implementación de sistemas de cableado estructurado en edificios comerciales, así como entre edificios y entornos de campus. Esta normativa asegura la interoperabilidad y rendimiento del sistema de cableado.

El cableado se instalará dentro de canalizaciones y tomas de red (rosetas) adecuadas. En cada punto de red, se utilizará un cable de parcheo (patch cord) para conectar el equipo final al punto de red.

Al llegar al patch panel, se dejará una longitud adicional de cable de 8 metros. Esta práctica permitirá futuras modificaciones o ampliaciones del punto de red y facilitará la reconexión en caso de fallas.

III.1.2.3. Diseñar modelos de direccionamiento y hostname

En Cosaalt es aconsejable utilizar un direccionamiento clase C se utiliza para las redes de tamaño pequeño que ofrecen suficientes direcciones para 254 dispositivos. Las direcciones del IP con un primer octeto a partir del 192 al 223 son parte de esta clase.

En la siguiente tabla están distribuidos los usuarios.

N.º de habitación	Unidades de Administración	Usuarios
1	Atención al cliente	5
2	Caja y Odeco	6
3	Secretaria de Gerencia Comercial	1
4	Gerencia Comercial	1
5	Morosidad	1
6	Archivos	3
7	Recursos humanos	2
8	Lecturación y Facturación	4
8	Lecturadores y pasantes	12
9	Gerencia General	2
10	Secretaria	2

11	Auditoria y Asesoría legal	6
12	Secretaria de consejo de administración	2
13	Sistemas de computación	3
14	Gerencia técnica	1
15	Secretaria de Gerencia técnica	1
16	Operación y Mantenimiento de obras	8
17	Gerencia Administrativa y financiera	3
18	Contabilidad	9
19	Topografía y Catastro	3
20	Consejo de vigilancia	1
TOTAL		76

Tabla 19: Especificación de usuarios
Fuente: Elaboración propia

Para realizar un diseño del modelo de direccionamiento se necesita conocer la cantidad total de host que se va a utilizar, para lo cual se considera todos los equipos que requieran un direccionamiento IP.

Los dispositivos que requieren una dirección IP son:

- 59 computadoras de escritorio

- 10 portátiles
- 55 impresoras
- 2 Router
- 1 Access Points

Una vez establecido la cantidad de dispositivos que se conectarán a la red, se considera la segmentación de red asignando un rango de direcciones IP. Para lo cual se debe determinar que todos los hosts formarán parte de subredes.

Por la cantidad de dispositivos que tendrán conectividad se considera trabajar con IP privadas Clase C versión 4, la red tendrá dirección IP 192.25.3.0 /24 que se dividirá en 6 segmentos de la misma subred que serán distribuidas de la siguiente manera:

Tabla de direccionamiento de red

ID	ÁREA/GRUPO	SUBRED	RANGO DE IP	MASCARA	HOST DISPONIBLES
-	Servidores	10.0.0.0/29	10.0.0.1-0.0.0.6	255.255.255.248	6
10	Comercial y atención al cliente	192.25.3.32/26	192.25.3.1-192.25.3.62	255.255.255.192	62
20	Administrativa y financiera	192.25.3.64/27	192.25.3.65-192.25.3.94	255.255.255.224	30
30	Técnica y operativa	192.25.3.96/27	192.25.3.97-192.25.3.126	255.255.255.224	30

40	Directiva y supervisación	192.25.3.128/27	192.25.3.129-192.25.3.158	255.255.255.224	30
50	Sistemas y soporte	192.25.3.160/28	192.25.3.161-192.25.3.174	255.255.255.240	14
60	Access Point	192.25.3.240/28	192.25.3.241-192.25.3.254	255.255.255.240	14
80	Impresoras	192.25.1.0/26	192.25.1.1-192.25.1.62	255.255.255.192	62

Tabla 20: Direcciones propuestas
Fuente: Elaboración propia

Detalle de la tabla

- VLAN ID: identificador de la VLAN que segmenta el tráfico de la red.
- Área/Grupo: el nombre del área o grupo que utiliza la subred asignada.
- Subred: red identificada por su dirección base y la longitud de la máscara de subred.
- Rango de IP: rango de direcciones IP que abarca la subred, excluyendo la dirección de red y la dirección de broadcast.
- Mascara: mascara de subred en notación decimal con puntos, que indica cómo se divide la red.
- Hosts disponibles: cantidad de direcciones IP utilizables en la subred.

En la tabla 21 se presentan las áreas de Cosaalt, organizadas según direcciones específicas:

Agrupaciones por Áreas:

1. Comercial y atención al cliente:

Agrupa todas las áreas que se relacionan directamente con la interacción a clientes y la gestión de transacciones, por lo que comparten necesidades de acceso a sistemas de clientes y bases de datos.

Áreas:

- Atención al Cliente
- Caja
- Morosidad
- ODECO
- Gerencia Comercial

2. Administrativa y financiera:

Estas áreas están centradas en la gestión interna de la empresa, incluyendo el manejo de personal, finanzas y la gestión de documentos y registros internos.

Áreas:

- Recursos humanos
- Facturación
- Contabilidad
- Gerencia administrativa y financiera
- Archivos

3. Técnica y operativa:

Estas áreas se encargan del mantenimiento y operación técnica de la infraestructura, así como de la gestión de datos geográficos y catastrales.

Áreas:

- Operación y mantenimiento de obras
- Gerencia técnica
- Topografía/Catastro

4. Directiva y supervisión:

Estas áreas están involucradas en la toma de decisiones estratégicas y la supervisión general, por lo que requieren acceso seguro y priorizado a la información crítica de la empresa.

Áreas:

- Gerencia General
- Consejo de Administración
- Consejo de Vigilancia
- Auditoria y Asesoría

5. Sistemas y soporte:

Esta área está encargada de la gestión y soporte de la infraestructura de TI, por lo que necesita acceso directo a todos los componentes de la red y los sistemas de gestión.

Áreas:

- Sistemas de Computación

III.1.2.4. Asignación de ancho de banda

Distribuye el ancho de banda de 70 Gbps de acuerdo con las prioridades:

Sin la VLAN 90 para sistemas implementados en un futuro

VLAN	Descripción	Porcentaje del ancho de banda	Ancho de banda (Mbps)	Justificación
10	Comercial y Atención al Cliente	25%	17.5	Maneja sistemas críticos de atención al cliente, caja y gestión de pagos, que requieren alta disponibilidad y rapidez en transacciones.
20	Administrativa y Financiera	20%	14	Gestión de contabilidad, recursos humanos y archivos, con uso intensivo de ERP y bases de datos.

30	Técnica y Operativa	15%	10.5	Tráfico moderado enfocado en sistemas de mantenimiento y topografía con transferencias de archivos técnicos.
40	Directiva y Supervisión	10%	7	Uso esporádico pero crítico para reuniones, gestión y supervisión de alto nivel, incluyendo tráfico a sistemas estratégicos y ERP.
50	Sistemas y Soporte	15%	10.5	Soporte de red y gestión de sistemas informáticos que requieren acceso a todos los recursos de la red, con tráfico regular pero controlado.
60	Access Points (Lecturadores de medidores)	5%	3.5	Bajo volumen de tráfico constante para sincronización y transmisión de datos de medidores inteligentes, sin generar picos altos de ancho de banda.
70	Servidores	5%	3.5	Tráfico interno para la sincronización y acceso a bases de datos, QoS y aplicaciones web.
80	Impresoras	5%	3.5	Tráfico bajo, usado principalmente para documentos corporativos y facturación.
Total		**100%**	**70**	

Tabla 21: Asignación del ancho de banda
Fuente: Elaboración propia

Con la VLAN 90 para sistemas implementados en un futuro

VLAN	Descripción	Porcentaje del ancho de banda	Ancho de banda (Mbps)	Justificación
10	Comercial y Atención al Cliente	20%	14	Tráfico alto debido a sistemas de facturación y atención al cliente, pero ajustado para compartir con otras VLANs críticas.
20	Administrativa y Financiera	15%	10.5	Administración, contabilidad y archivos con acceso regular a sistemas internos.
30	Técnica y Operativa	10%	7	Tráfico moderado, uso técnico de topografía y mantenimiento de redes.
40	Directiva y Supervisión	10%	7	Tráfico esporádico, pero con prioridad alta en momentos clave como decisiones estratégicas y reuniones.
50	Sistemas y Soporte	10%	7	Gestión de soporte técnico con acceso prioritario a la infraestructura y recursos esenciales.
60	Access Points (Lecturadores de medidores)	5%	3.5	Uso constante pero moderado para la recolección de datos de medidores inteligentes.

70	Servidores	5%	3.5	Acceso constante a bases de datos y aplicaciones web internas, balanceado por QoS.
80	Impresoras	5%	3.5	Mínimo uso de ancho de banda, dedicado a documentos internos y facturación.
90	IoT y SCADA	20%	14	Tráfico crítico para la gestión y monitoreo en tiempo real de la infraestructura de agua y alcantarillado.
Total		**100%**	**70**	

Tabla 22: Asignación del ancho de banda con la Vlan 90 para loT y SCADA
Fuente: Elaboración propia

Cálculo del ancho de banda

En un escenario donde Cosaalt no utiliza VLANs, el tráfico fluye sin segmentación, lo que genera una mayor competencia por el ancho de banda disponible entre todos los dispositivos y sistemas. El cálculo estimado es:

Usuarios Corporativos (75 usuarios):

Promedio de 1 Mbps por usuario.

75 x 1 Mbps = 75 Mbps.

Servicios Críticos:

- ERP y CRM: 15 Mbps.
- Videoconferencias: 1 sesiones simultáneas, promedio de 3 Mbps cada una.

- 1 x 3 Mbps = 3 Mbps.
- Transferencia de Archivos: 7 Mbps.
  Ancho de Banda Total Estimado sin VLANs: 100 Mbps.

La implementación de VLANs segmenta el tráfico por áreas funcionales, optimizando el uso del ancho de banda. Esto reduce la competencia directa entre sistemas, permitiendo una gestión más eficiente del tráfico.

Efecto de la Segmentación:

- Reducción de colisiones y retransmisiones innecesarias.
- Priorización de tráfico según la criticidad del área mediante QoS.
- Estimación de reducción: entre un 15% y un 25% del tráfico general debido a la eficiencia en la segmentación.
  Nuevo Cálculo: 100 Mbps - 20% eficiencia = 80 Mbps.

Con QoS y VLANs, el ancho de banda requerido podría optimizarse a aproximadamente 70 Mbps, considerando la priorización y la reducción del tráfico interno redundante.

III.1.2.5. Asignación de los puertos de los dispositivos

R1 MIKROTIK ccr1009-7g-1c-1s+

PUERTOS	ASIGNACIÓN	RED
Gigabit 0	VLAN 10	192.25.3.25
	VLAN 20	192.25.3.57
	VLAN 30	192.25.3.121
	VLAN 40	192.25.3.153
	VLAN 50	192.25.3.185
	VLAN 60	192.25.3.201

	VLAN 80	192.25.1.0
Gigabit 1	Conectado a la ISP	200.1.2.2
Gigabit 2	Conectado al switch de los servidores	192.25.4.1

Tabla 23: Asignación de puertos para el router R1
Fuente: Elaboración propia

R2 TP-LINK TL-R600VPN

PUERTOS	ASIGNACIÓN	RED
Gigabit 0	VLAN 10 VLAN 20 VLAN 30 VLAN 40 VLAN 50 VLAN 60 VLAN 80	192.25.3.25 192.25.3.57 192.25.3.121 192.25.3.153 192.25.3.185 192.25.3.201 192.25.1.0
Gigabit 1	Conectado a la ISP	200.1.2.3
Gigabit 2	Conectado al switch de los servidores	192.25.4.2

Tabla 24: Asignación de puertos para el router R2
Fuente: Elaboración propia

MainSwitch1 D-Link DGS-3130-30TS

PUERTOS	ASIGNACIÓN	RED

Ethernet Gig 1/0/23- Ethernet Gig 1/0/24	Conectado al MainSwitch2	No aplica
Gigabit 1	Reservado	No aplica
Gigabit 2	VLAN 10 comercial y atención al cliente VLAN 20 administrativa y financieraVLAN 60 Access point	192.25.3.25 192.25.3.57 192.25.3.201
Gigabit 3	VLAN 40 Directiva y supervisión VLAN 50 Sistemas y soportes	192.25.3.153 192.25.3.185
Gigabit 4	VLAN 20 Administrativa y financiera VLAN 30 Técnica y operativa VLAN 40 Directiva y supervisión	192.25.3.57 192.25.3.121 192.25.3.153
Ethernet Gig. 1	VLAN 1 DEFAULT	No aplica
Ethernet Gig 2	Conectado al router R1-principal	No aplica
Ethernet Gig. 3	VLAN 80 Impresoras	192.25.1.0
Ethernet Gig. 5	VLAN 80 Impresoras	192.25.1.0
Ethernet Gig. 7-22	Reservados para expansión	No aplica
Ethernet Gig. 10-11	servidores	

Tabla 25: Asignación de puertos para el switch Main-switch1
Fuente: Elaboración propia

MainSwitch2 TP-Link T2600G-28TS

PUERTOS	ASIGNACIÓN	RED
Ethernet 1	Conectado al Router R2-redundante	No aplica
Ethernet 2	VLAN 1 DEFAULT	No aplica
Gigabit 1	Conectado al puerto SFP del MainSwitch2	No aplica
Gigabit 2	VLAN 10 comercial y atención al cliente VLAN 20 administrativa y financiera VLAN 60 Access point	192.25.3.25 192.25.3.57 192.25.3.201
Gigabit 3	VLAN 40 Directiva y supervisión VLAN 50 Sistemas y soportes	192.25.3.153 192.25.3.185
Gigabit 4	VLAN 20 Administrativa y financiera VLAN 30 Técnica y operativa VLAN 40 Directiva y supervisión	192.25.3.57 192.25.3.121 192.25.3.153
Ethernet Gig. 6	VLAN 70 Impresoras	192.25.1.0
Ethernet Gig. 8		
Ethernet Gig.10 - Ethernet Gig.22	Reservados para expansión	No aplica
Ethernet Gig.23 - Ethernet Gig.24	Conectado al MainSwitch2	No aplica

Tabla 26: Asignación de puertos para el switch Main-switch2
Fuente: Elaboración propia

Switch de acceso 1

PUERTOS	ASIGNACIÓN	RED

Ethernet 1-2	VLAN 1 DEFAULT	No aplica
G3-G19	VLAN 10 comercial y atención al cliente	192.25.3.25
G19-G44	VLAN 20 administrativa y financiera	192.25.3.57
G 45	VLAN 60 Access point	192.25.3.201

Tabla 27: Asignación de puertos para el switch de acceso 1
Fuente: Elaboración propia

Switch de acceso 2

PUERTOS	ASIGNACIÓN	RED
Ethernet 1-2	VLAN 1 DEFAULT	No aplica
G3-G20	VLAN 40 Directiva y supervisión	192.25.3.153
G21-G24	VLAN 50 Sistemas y soportes	192.25.3.185

Tabla 28: Asignación de puertos para el switch de acceso 2
Fuente: Elaboración propia

Switch de acceso 3

PUERTOS	ASIGNACIÓN	RED
Ethernet 1-2	VLAN 1 DEFAULT	No aplica
G3-G24	VLAN 20 administrativa y financiera	192.25.3.57
G24-45	VLAN 30 Técnica y operativa	192.25.3.121
G45-48	VLAN 40 Directiva y supervisión	192.25.3.153

Tabla 29: Asignación de puertos para el switch de acceso 3
Fuente: Elaboración propia

Switch de la planta baja para impresoras

PUERTOS	ASIGNACIÓN	RED

Ethernet 1-2	VLAN 1 DEFAULT	No aplica
G3-G24	VLAN 80 Impresoras	192.25.1.1

Tabla 30: Asignación de puertos para el switch de la planta baja de impresoras
Fuente: Elaboración propia

Switch del primer piso para impresoras

PUERTOS	ASIGNACIÓN	RED
Ethernet 1-2	VLAN 1 DEFAULT	No aplica
G3-G24	VLAN 80 Impresoras	192.25.1.1

Tabla 31: Asignación de puertos para el switch del segundo piso de impresoras
Fuente: Elaboración propia

Hostname:

- Router Principal: R1
- Router Secundario: R2
- **Firewall Perimetral:** firewall
- **Switches de Distribución:** Main-switch1, Main-switch2
- **Switches de Acceso:** access-switch1, access-switch2, etc.

III.1.2.6. Seleccionar protocolos switching y routing

En el diseño de red propuesto, se han seleccionado protocolos de switching y routing basados en su capacidad para garantizar la escalabilidad, redundancia, velocidad y seguridad de la red. Estos protocolos han sido implementados estratégicamente para cumplir con los objetivos de la simulación, asegurando un desempeño óptimo y una administración eficiente de los recursos de red.

Protocolos de Switching:

Para la implementación de la red, se seleccionaron diversos protocolos de switching que garantizaron una segmentación eficiente, redundancia y prevención de bucles.

Se planea implementar VLANs (Redes de Área Local Virtual) utilizando el protocolo 802.1Q, el cual permitirá segmentar el tráfico entre los diferentes departamentos y servicios de la empresa. Esta segmentación busca mejorar la seguridad, el rendimiento y la administración de la red al mantener el tráfico aislado entre áreas como Comercial, Administrativa, Técnica y otras.

Dado que la redundancia es una prioridad en el diseño, se propone utilizar el protocolo Rapid Spanning Tree Protocol (RSTP) para prevenir bucles en la red y garantizar la continuidad del servicio en caso de fallas. Este protocolo, una evolución del STP, permitirá tiempos de convergencia más rápidos en situaciones de cambios topológicos.

Para maximizar el rendimiento y garantizar redundancia a nivel de enlace, se planea configurar LACP (Link Aggregation Control Protocol) en los enlaces críticos, especialmente entre los switches del MDF y los switches de piso. Este protocolo permitirá combinar múltiples enlaces físicos en un único enlace lógico, incrementando el ancho de banda disponible y asegurando que no haya interrupciones en caso de fallas en uno de los enlaces.

Se utilizarán enlaces trunk configurados con 802.1Q entre los switches del MDF y los switches de piso. Esto permitirá transportar el tráfico de múltiples VLANs sobre una sola conexión física, facilitando la propagación de las VLANs por toda la red.

Protocolos de routing:

se plantean los siguientes protocolos y estrategias de enrutamiento para asegurar una comunicación eficiente y resiliente entre las diferentes subredes y VLANs:

Se implementará el modelo Router-on-a-Stick en el router principal, el cual se encargará de gestionar el tráfico entre las VLANs. Este método utiliza subinterfaces en el router principal, permitiendo que cada VLAN tenga un gateway en la subred correspondiente. Esta configuración es esencial para permitir la comunicación entre los diferentes departamentos y servicios, manteniendo la segmentación lógica.

Se implementarán rutas estáticas tanto en el router principal como en el redundante D-Link DSR-1000AC garantizando un control preciso del tráfico entre subredes y dispositivos. Adicionalmente, se evaluará la posibilidad de implementar técnicas de equilibrio de carga para distribuir el tráfico de manera uniforme entre los routers principales y redundantes, optimizando así el uso del ancho de banda y los recursos disponibles.

Para garantizar alta disponibilidad y continuidad operativa, se utilizará el protocolo VRRP (Virtual Router Redundancy Protocol). Este protocolo estándar permitirá configurar un router secundario como respaldo activo del router principal. En caso de falla del principal, el secundario asumirá automáticamente las funciones de gateway, minimizando el tiempo de inactividad y asegurando la conectividad para los usuarios.

III.1.2.7. Desarrollar estrategias de seguridad

Seguridad Perimetral:

La seguridad perimetral será garantizada mediante la implementación de un firewall dedicado (Juniper SSG-20) configurado con reglas restrictivas de entrada y salida, solo se permitirá el tráfico necesario y se bloqueará todo el tráfico no autorizado. Además de implementar listas de control de acceso (ACL) para especificar que tráfico es permitido o denegado basado en direcciones IP, puertos y protocolos.

Uso de inspección profunda de paquetes (DPI) para analizar el contenido de los paquetes en profundidad y detectar amenazas potenciales como malware, intrusiones y otros tipos de tráfico malicioso.

Segmentación de Red:

Implementación de VLANs para segmentar la red en diferentes departamentos y servicios, como Comercial, Administrativa, Legal, Técnica, Servidores, e Impresoras. También se realizará la configuración de ACLs en switches y routers para controlar el tráfico entre VLANs y restringir el acceso a recursos sensibles.

Se realizó la segmentación de la Vlans para cada dirección de la empresa, ya que tendrá su propia (virtual LAN). Esto permitirá que las estaciones de trabajo ubicadas físicamente en lugares diferentes puedan trabajar en la misma red lógica.

Control de Acceso y Autenticación: Utilizar VLANs y configuraciones de switch para limitar el acceso a recursos sensibles. En los switches administrables se configurarán ACLs (Access Control Lists) para filtrar el tráfico basado en direcciones IP, puertos y protocolos. Esto permitirá:

- Restringir el acceso a ciertos recursos únicamente a dispositivos autorizados.
- Bloquear tráfico sospechoso o no deseado dentro de la red.

Además, se habilitará 802.1X (Network Access Control) para garantizar que solo los dispositivos autenticados puedan conectarse a la red.

Redundancia y Alta Disponibilidad: Configurar enlaces redundantes y protocolos de conmutación para minimizar el tiempo de inactividad en caso de fallo.

Uso de VRRP (para redundancia de gateway), STP (Spanning Tree Protocol) y RSTP (Rapid Spanning Tree Protocol) para prevenir bucles en la red y asegurar una convergencia rápida en caso de

cambios en la topología. Esto asegura la continuidad operativa en caso de fallas, reduciendo los tiempos de inactividad y los puntos únicos de falla que podrían comprometer la seguridad.

Seguridad inalámbrica (Wireless Security): se realizará WPA2-Personal, Filtrado de Mac y Cambio de SSID esto lo realizamos para evitar un ataque, necesita productos específicamente diseñados para proteger la red inalámbrica.

1. Cuentas **de Usuarios ID o SSID:** El Router tendrá de nombre SBVM para que se puedan conectar las personas solo de la institución.

2. Autenticación**:** Se utilizará el Cifrado WPA2-Personal, el área comercial estará conectada de este modo con este tipo de seguridad, ¡la oficina de facturación tendrá de cifrado la contraseña Z8hT!**s4V@3kNpL$7**, dado que es segura, compleja y difícil de adivinar.

III.1.2.8. Desarrollar estrategias de administración de red

Políticas de Actualización y Mantenimiento Preventivo

Se establecerá un calendario de mantenimiento para garantizar que todos los dispositivos estén actualizados y funcionando correctamente:

- **Actualización de firmware: Mantener actualizados los sistemas operativos de los switches, routers y firewalls para cerrar vulnerabilidades y añadir nuevas funcionalidades.**
- **Inspección física de hardware: Revisar regularmente los equipos para identificar signos de desgaste o fallos.**
- **Limpieza y orden del cableado: Asegurar que el cableado esté etiquetado y organizado, facilitando el diagnóstico y la reparación.**

Segmentación de Red:

Para mejorar la seguridad y la eficiencia de la red, se segmentarán los diferentes departamentos y servicios en VLANs específicas. Esto incluye áreas como Comercial, Administrativa, Legal, Técnica, Servidores y Routers, y las Impresoras. La segmentación permitirá aislar el tráfico de cada área, reduciendo el riesgo de que un compromiso en una parte de la red afecte a otras. Se utilizarán Listas de Control de Acceso (ACL) en los switches y routers para restringir el tráfico entre VLANs y asegurar que solo los usuarios autorizados puedan acceder a recursos específicos.

Estrategias de Escalabilidad y Planificación Futura

La red estará diseñada para facilitar su expansión futura:

- **Capacidad de puertos: Garantizar que los switches del MDF y de piso cuenten con puertos libres para conectar nuevos dispositivos o enlaces ascendentes.**
- **Segmentación dinámica: Configurar VLANs dinámicas que permitan incorporar nuevos departamentos o servicios sin modificar la estructura física de la red.**
- **Planificación del crecimiento del ancho de banda: Monitorear las necesidades de cada VLAN y ajustar las asignaciones de ancho de banda según sea necesario, priorizando servicios críticos.**

Seguridad en la Administración de la Red

Para proteger la administración de la red de accesos no autorizados:

- Restricción de acceso administrativo: Configurar ACLs para permitir el acceso a interfaces de administración únicamente desde direcciones IP específicas.
- Cifrado de datos: Utilizar protocolos seguros como SSH y HTTPS para todas las conexiones de administración.

Redundancia y Alta Disponibilidad:

Para minimizar el tiempo de inactividad y asegurar la continuidad del servicio, se configurarán enlaces redundantes utilizando el Protocolo de Control de Agregación de Enlaces (LACP). Esto permitirá que varios enlaces físicos se combinen en un solo enlace lógico, proporcionando mayor ancho de banda y redundancia. Además, se implementarán protocolos de redundancia de gateway como HSRP (Hot Standby Router Protocol) para garantizar que, en caso de falla de un dispositivo, otro pueda tomar el control sin interrupción del servicio. El uso de STP (Spanning Tree Protocol) y RSTP (Rapid Spanning Tree Protocol) ayudará a prevenir bucles en la red y asegurar una rápida convergencia en caso de cambios en la topología.

Documentación

La documentación de la red es un pilar esencial para una administración eficiente y para la resolución rápida de problemas. Se propone implementar un sistema de documentación centralizado y actualizado periódicamente, el cual incluirá:

Inventario de dispositivos: listado de todos los equipos de red, incluyendo routers, switches, puntos de acceso y firewalls, junto con su ubicación física. Incluyendo especificaciones de cables y conexiones físicas.

Configuración de dispositivos: Detalles de los parámetros configurados, como VLANs, ACLs, rutas estáticas y dinámicas, y políticas de calidad de servicio (QoS).

Diagramas de topología: diagramas físicos y lógicos actualizados que reflejen la estructura de la red, las conexiones entre dispositivos y las asignaciones de VLANs.

III.1.3. Fase 3: Desarrollar diseño físico

Para esta propuesta se usará un cable de cobre UTP categoría 6ª, ya que este cableado tiene una durabilidad de 10 años y una velocidad de hasta 10 Gbps hasta los 100 metros. Esta categoría tiene características que nos permiten transmitir por un mismo cable de voz, datos, video. También es compatible con cables de categorías inferiores.

Diagrama físico

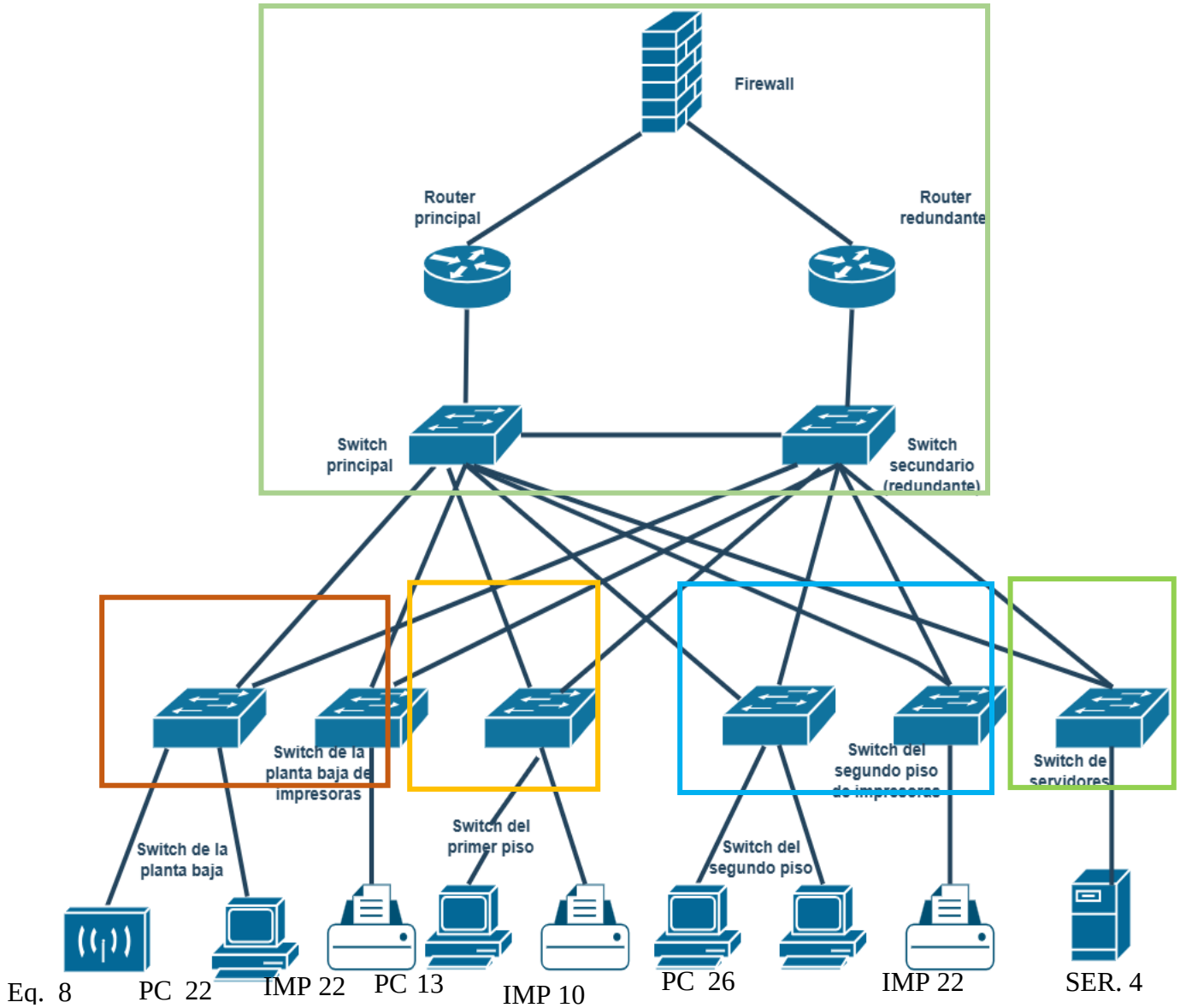
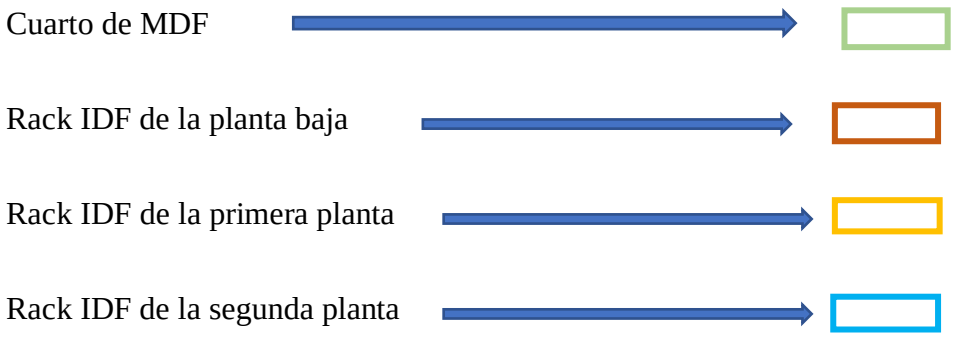


Figura III.1.9: Diagrama físico
Fuente: Elaboración propia



Para la conexión de piso a piso de la cooperativa se escogió el cable de fibra óptica por su alta velocidad, ancho de banda, mayor distancia de transmisión, inmunidad a interferencias electromagnéticas y seguridad de transmisión de datos.

Debido a que la fibra óptica transmite datos en forma de luz, es extremadamente difícil de interceptar. Esto brinda mayor seguridad y privacidad en la transmisión de datos. Lo que no se puede obtener con un cable de cobre no son del todo seguros, es por esta razón que para la conexión de piso a piso se usara fibra óptica y no así cable UTP.

Tabla de equipos actuales y requeridos para Cosaalt

Equipo	Características Técnicas Esenciales	Ubicación en la Red	Estado Actual / Requerido
Firewall Uniper SSG-20	- Operación en la capa del modelo OSI 4-7. -Inspección profunda de paquetes (DPI). -Soporte para VPN IPsec. - Control de acceso basado en políticas (ACLs).	Perímetro (conexión a Internet)	Actual

	- Filtrado de contenido web y prevención de intrusiones (IPS).		
Router Mikrotik CCR1009-7G-1C-1S+	- Operación en la capa del modelo OSI 3 -Procesamiento multinúcleo para alto rendimiento. - RouterOS con soporte para OSPF, BGP, VRRP y QoS. - Filtro de tráfico avanzado y balanceo de carga. - Capacidad para rutas dinámicas.	Router principal en el centro de la red	Actual
Router TP-Link TL-R600VPN	- Operación en la capa del modelo OSI 3 - Firewall SPI (Stateful Packet Inspection). - Gestión básica de VPN (IPsec, L2TP, PPTP). - Balanceo de carga WAN dual.	Router secundario en el centro de la red	Actual
Switch TP-Link T3700G-52TQ	- Operación en la capa del modelo OSI 2/3 - 52 puertos Gigabit Ethernet. - Soporte para agregación de enlaces (LACP). - Gestión basada en web, CLI, SNMP. - VLANs privadas para aislamiento.	Switch de acceso ubicado en la periferia de la red	Requerido
Switch D-Link DGS-3130-30TS	- Operación en la capa del modelo OSI 2/3 - Funciones avanzadas de seguridad como 802.1X y listas de control de acceso (ACLs). - Soporte para enrutamiento estático. - Gestión centralizada y CLI.	Switch principal ubicado en la parte intermedia de la red	Requerido

	- Capacidades PoE opcionales para puntos de acceso.		
Servidor Dell PowerEdge R740	- Operación en la capa del modelo OSI 7 - Procesadores escalables Intel Xeon. - Gestión de almacenamiento flexible (RAID). - Soporte de virtualización (VMware, Hyper-V).	Servidor ubicado en la periferia de la red	Actual
Servidor IBM System x3650 M5	- Operación en la capa del modelo OSI 7 - Redundancia en fuentes de alimentación y discos. - Amplia capacidad de almacenamiento con soporte para discos SSD y HDD. - Alta fiabilidad para entornos empresariales.	Servidor ubicado en la periferia de la red	Actual
Switch TP-Link T2600G-28TS	- Operación en la capa del modelo OSI 2/3 - Puertos Gigabit gestionados. - Seguridad avanzada con ACLs. - Compatible con VLANs privadas y agregación de enlaces.	Switch secundario ubicado en la parte intermedia de la red	Actual
Switch D-Link DGS-3630-28SC	- Operación en la capa del modelo OSI 2/3 - Switching de alta densidad con soporte avanzado de QoS. - Enrutamiento estático y dinámico. - Capacidades avanzadas de gestión de red con	Switch principal ubicado en la periferia de la red	Actual

	CLI y SNMP. - Ideal para capas de distribución o core.		
Servidor HP ProLiant DL380 Gen9	- Operación en la capa del modelo OSI 7 -Compatibilidad RAID (0, 1, 5, 10). - Hasta 2 CPUs Xeon y 384 GB de RAM. - Soporte para despliegue en entornos virtualizados.	Servidor de respaldo para base de datos ubicado en la periferia de la red	Requerido

Tabla 32: Lista de equipos requeridos y actuales
Fuente: Elaboración propia

III.1.3.1. Diseño del cable de red

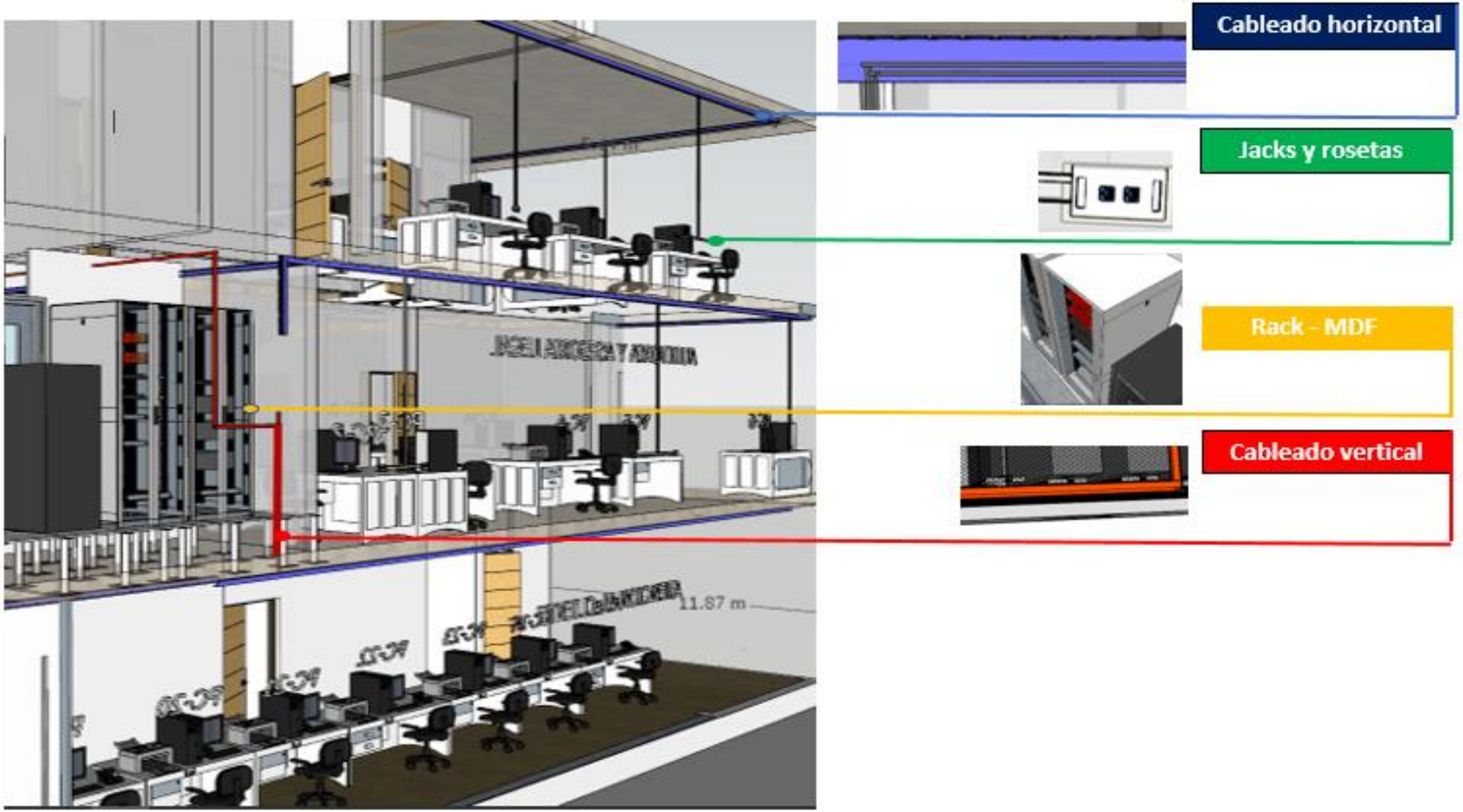


Figura III.1.10: Diagrama de cableado horizontal y vertical
Fuente: Elaboración propia

III.1.3.2. Planta baja

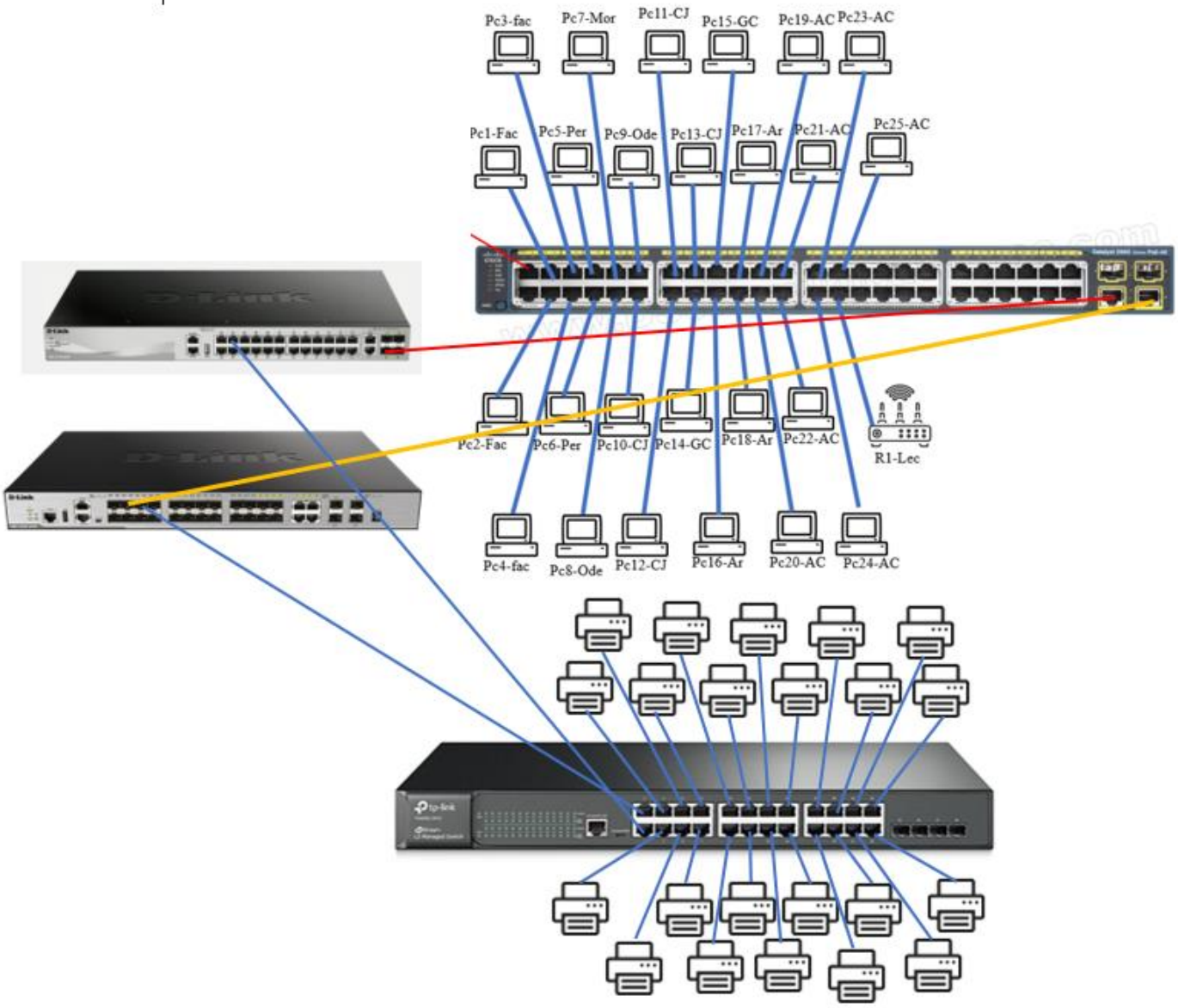


Figura III.1.11: cableado de la planta baja
Fuente: Elaboración propia

Fibra óptica

cable UTP

Cable UTP conectado al Main-Switch2

Tabla de abreviaciones

N°	Abreviatura	Nombre del área al que hace referencia
1	fac	Facturación
2	Mor	Morosidad
3	CJ	caja
4	GC	Gerencia comercial
5	AC	Atención al cliente
6	Per	Recursos humanos
7	Ode	Odeco
8	Ar	Archivos

Tabla 33: abreviaciones de la planta baja
Fuente: Elaboración propia

Ubicación del cableado de la planta baja

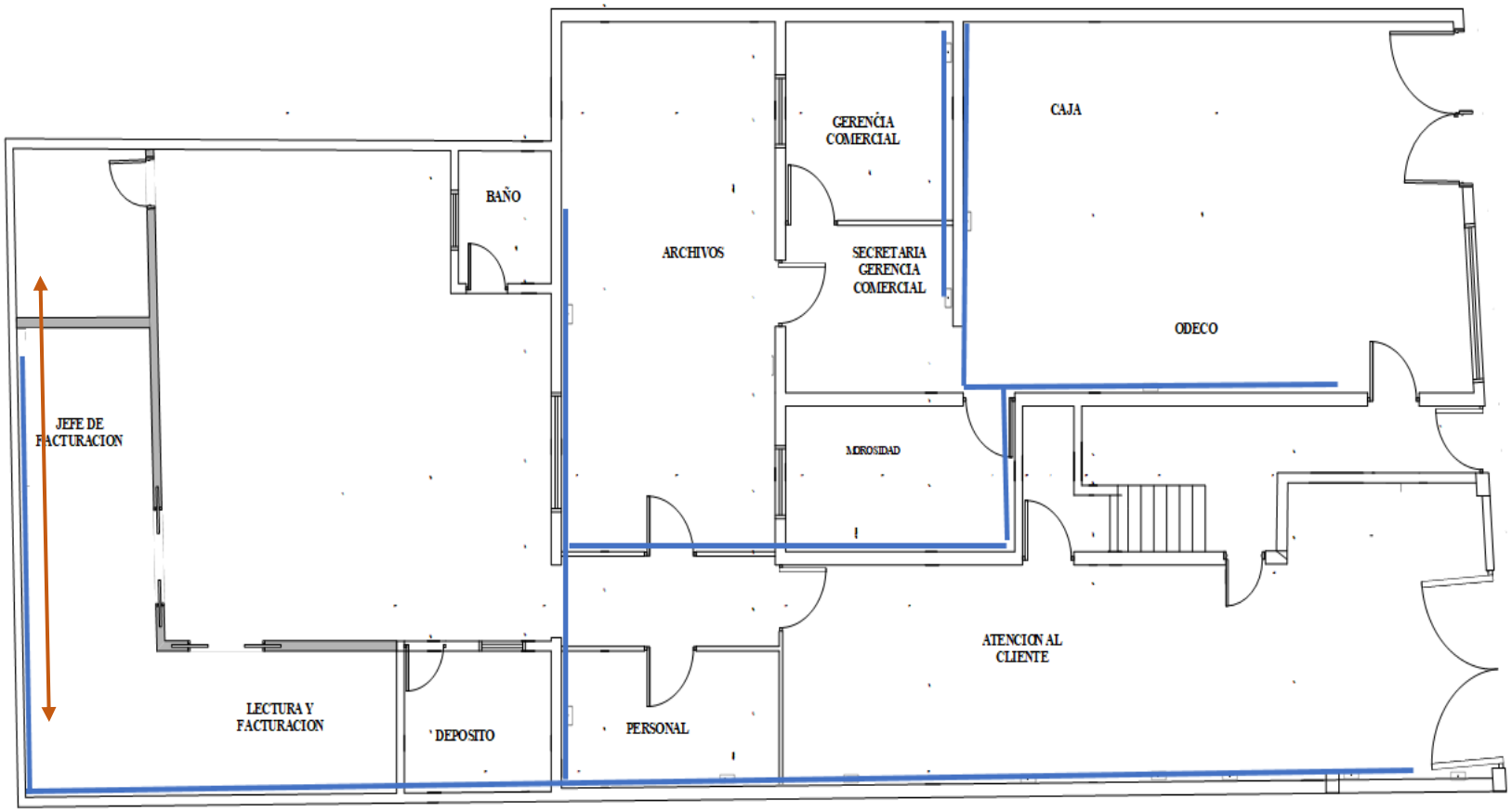


Figura III.1.12: Organización del cableado mediante plano de la planta baja
Fuente: Elaboración propia

Ubicación de los puntos de datos o nodos

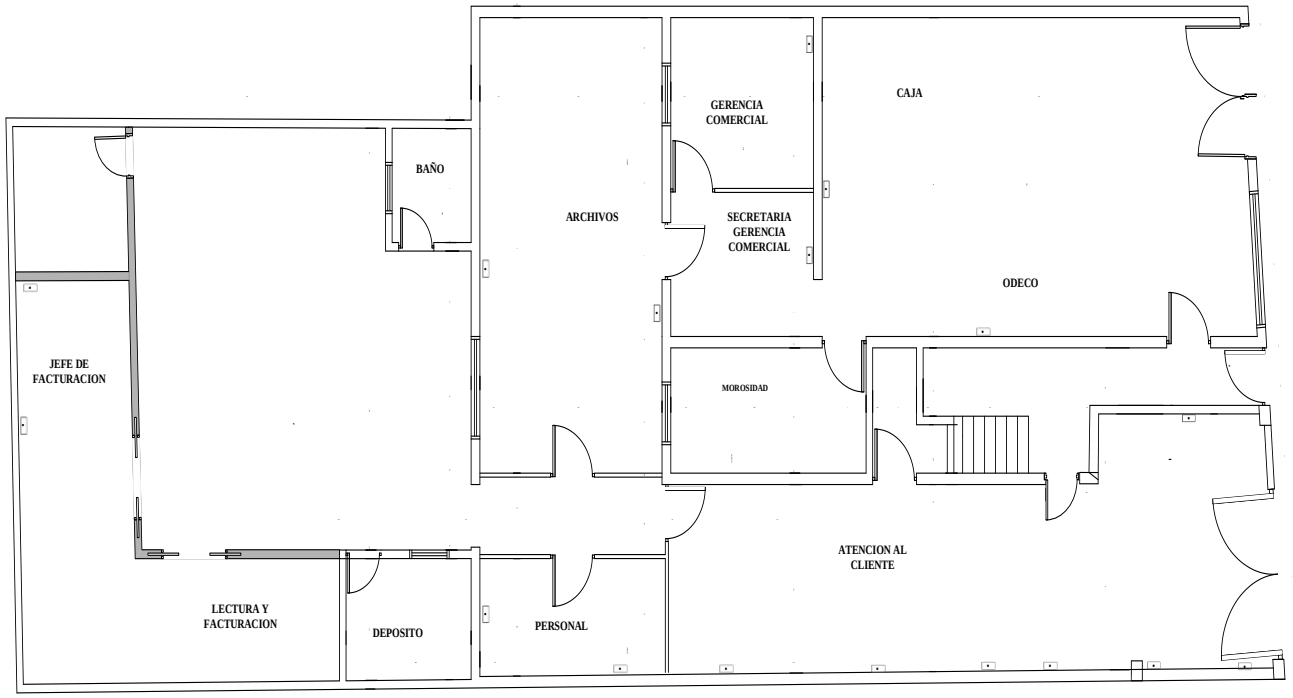


Figura III.1.13: Organización de nodos mediante plano de la planta baja

Fuente: Elaboración propia

Identificación y ubicación de los puntos de datos y nodos

Figura III.1.14: Organización completa de la planta baja

Fuente: Elaboración propia

III.1.3.3. Primer piso

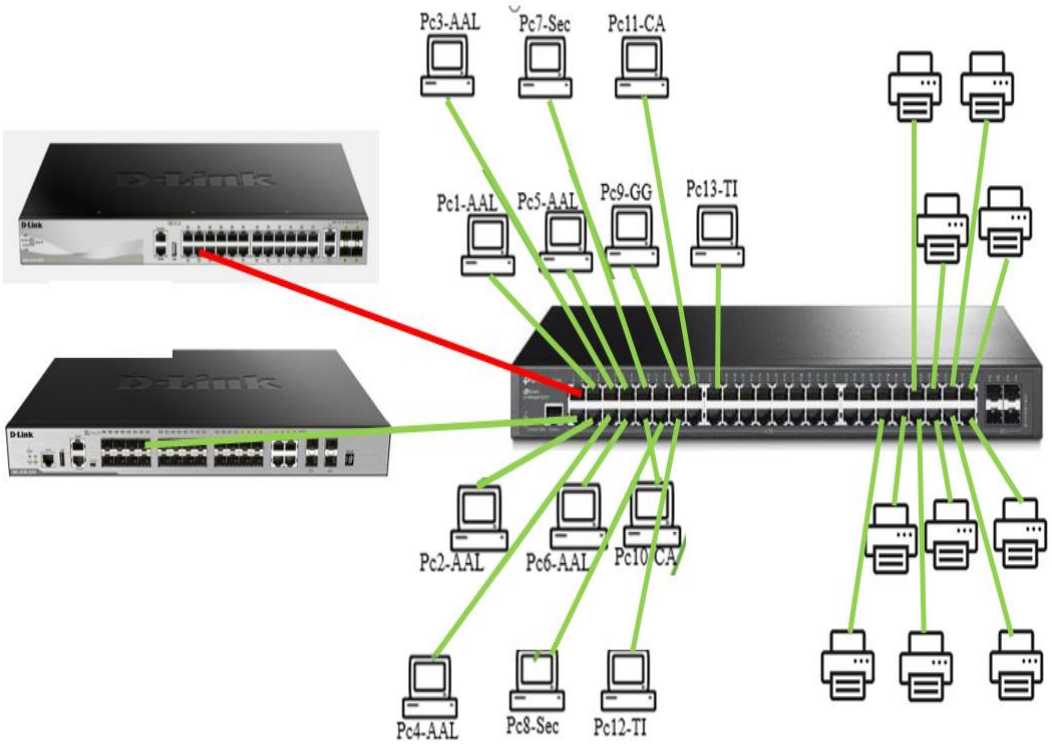


Figura III.1.15: Diseño del cableado del primer piso
Fuente: Elaboración propia

Fibra óptica

Cable Utp

Tabla de abreviaturas

N°	Abreviatura	Nombre del área al que hace referencia
1	AAL	Auditoria y asesoría legal
2	CA	Consejo de administración
3	Sec	secretaria
4	GG	Gerencia general
5	TI	Sistemas de computación

Tabla 34: abreviaciones del primer piso
Fuente: Elaboración propia

Ubicación del cableado del primer piso

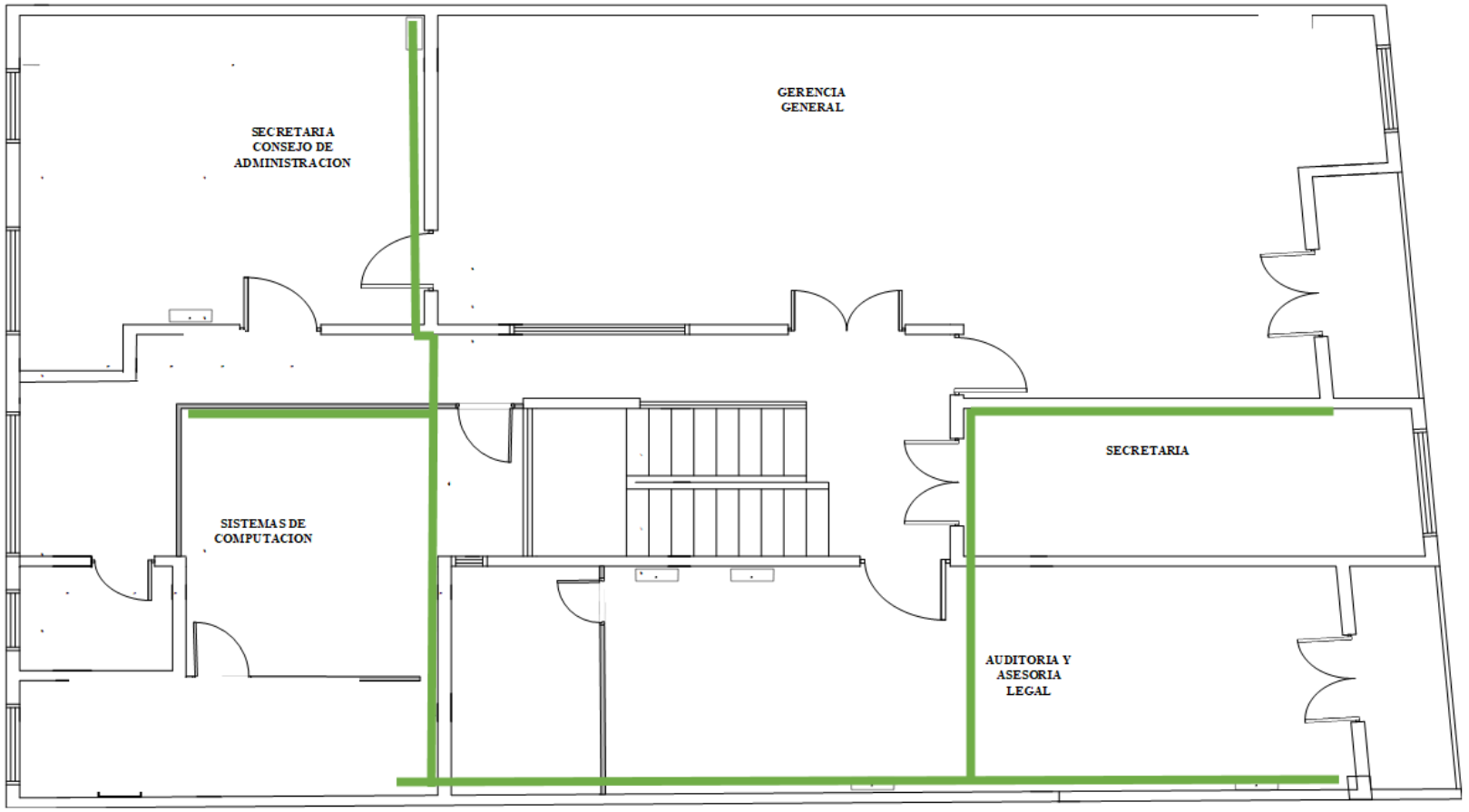


Figura III.1.16: ubicación del cable de red-primer piso
Fuente: Elaboración propia

Ubicación de los puntos de datos o nodos

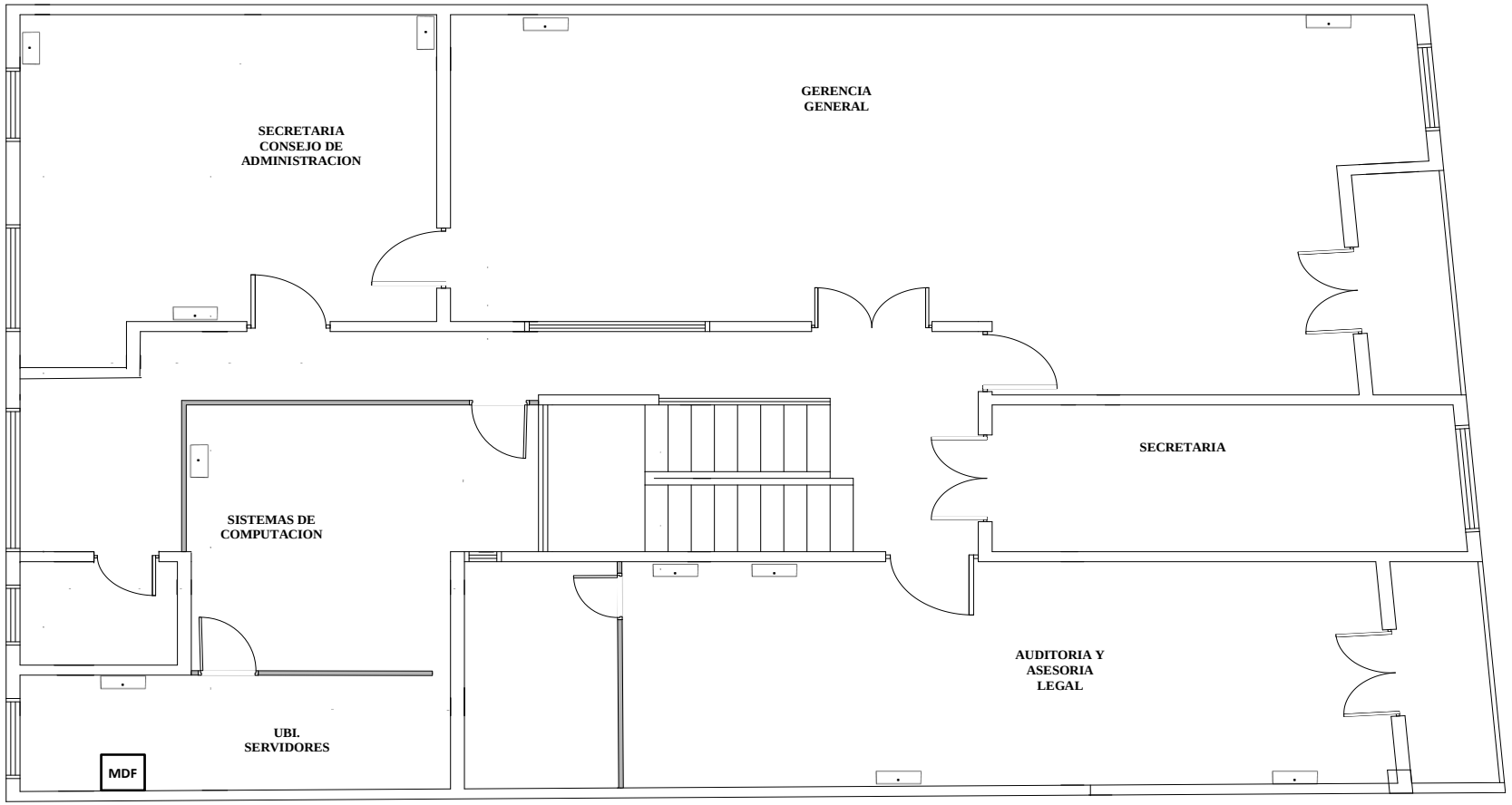


Figura III.1.17: Ubicación de los nodos del primer piso
Fuente: Elaboración propia

Identificación y ubicación de los puntos de datos y nodos

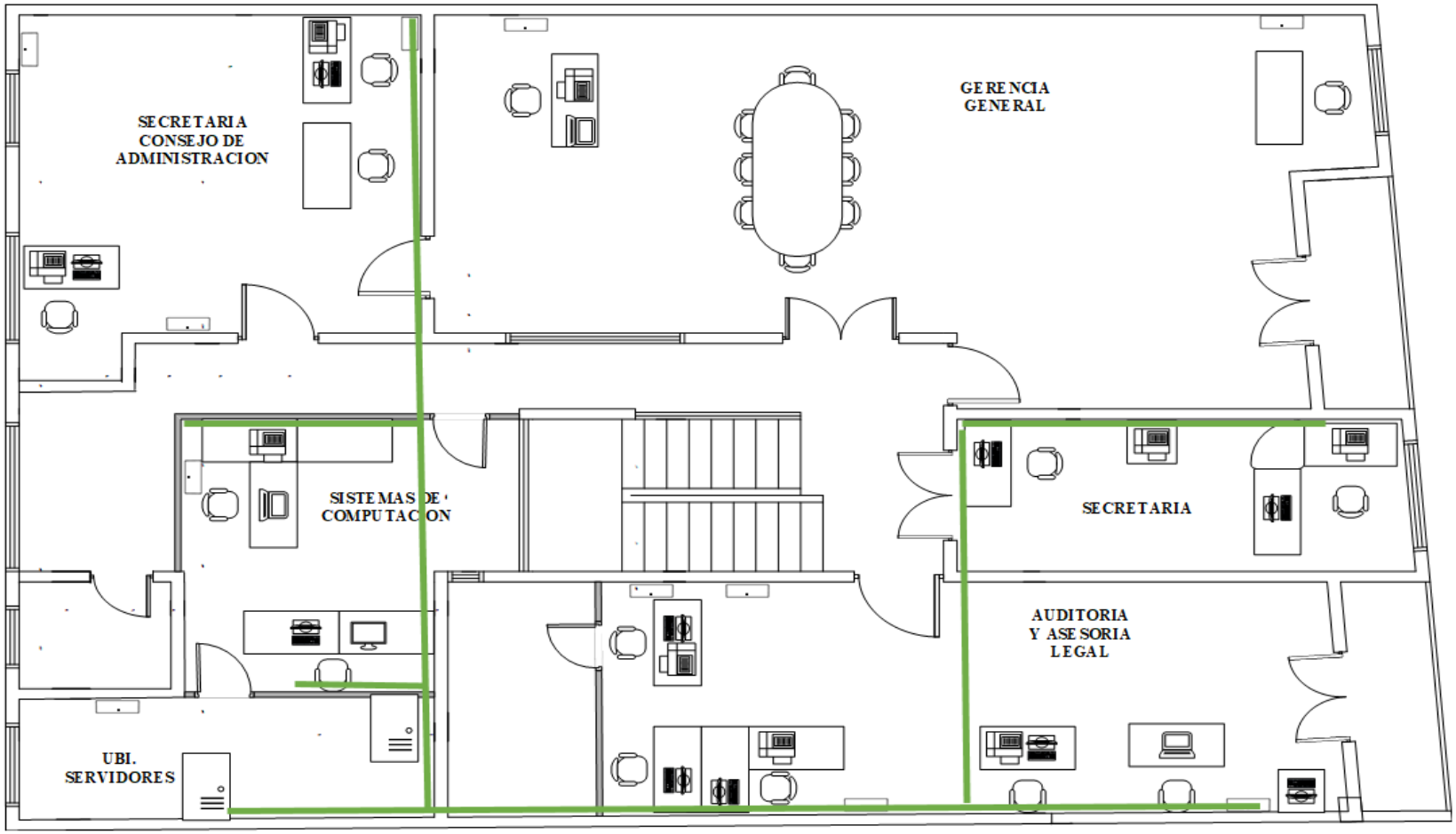


Figura III.1.18: Organización completa del primer piso
Fuente: Elaboración propia

III.1.3.4. Segundo piso

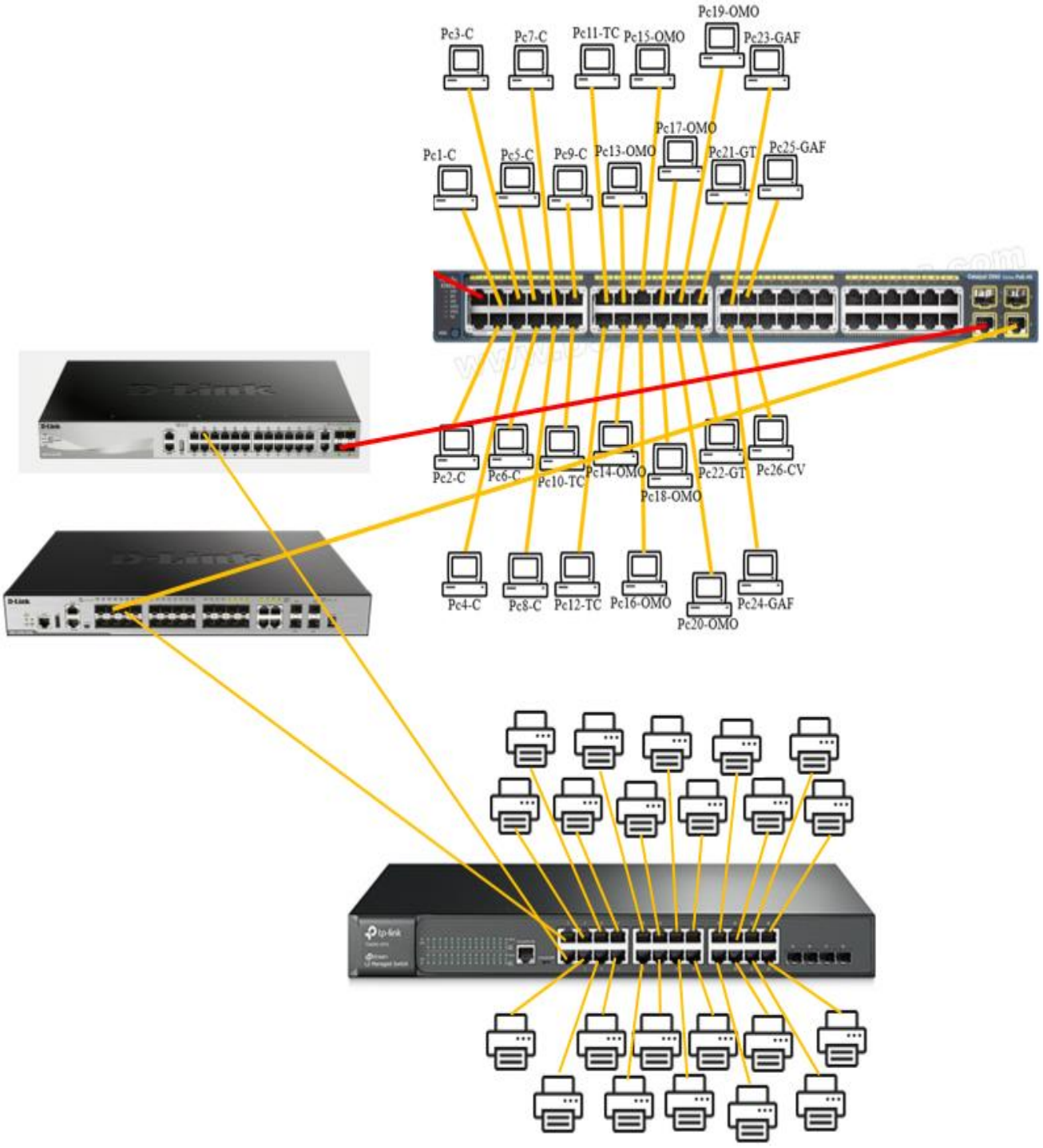


Figura III.1.19: Diseño del cableado del segundo piso
Fuente: Elaboración propia

Fibra óptica

Vlan 3 – Segundo piso

Tabla de abreviaciones

N°	Abreviatura	Nombre del área al que hace referencia
1	C	Contabilidad
2	TC	Topografía/Catastro
3	OMO	Operaciones y mantenimiento de obras
4	GAF	Gerencia administrativa y financiera
5	GT	Gerencia técnica

Tabla 35: Abreviaciones del segundo piso
Fuente: Elaboración propia

Ubicación del cableado del segundo piso

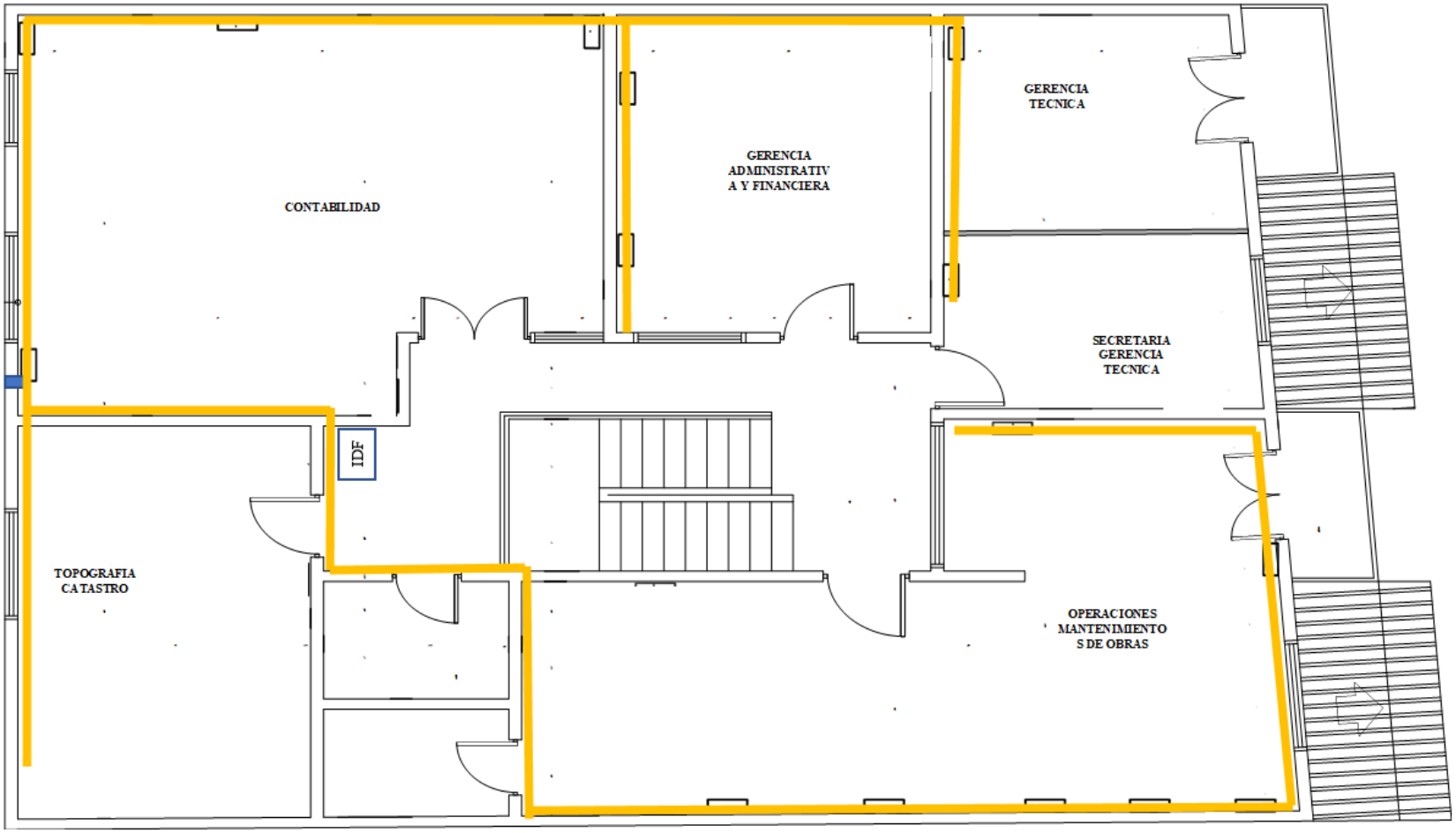


Figura III.1.20: Ubicación del cableado del segundo piso
Fuente: Elaboración propia

Ubicación de los puntos de datos y nodos

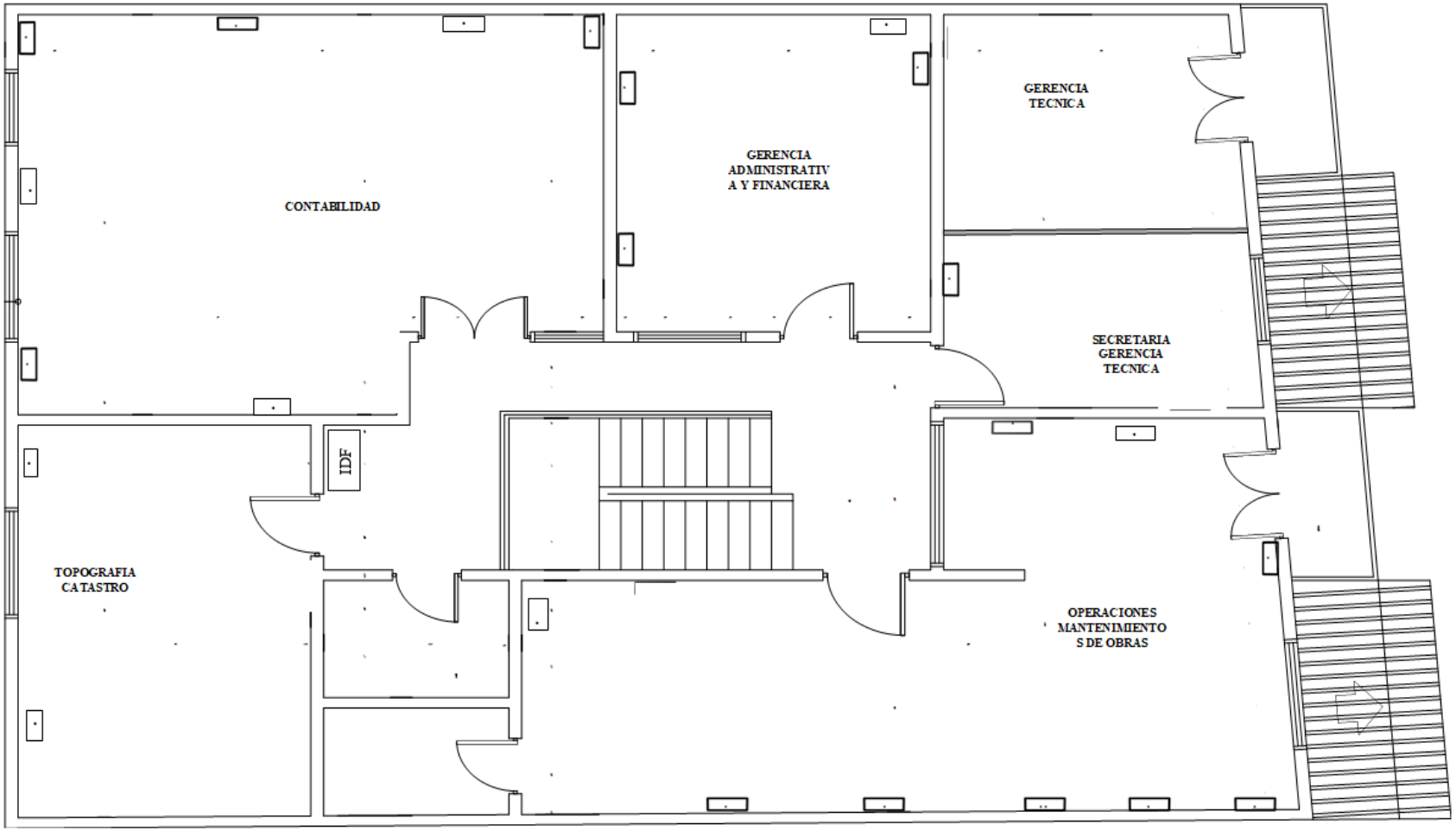


Figura III.1.21: Ubicación de los nodos-segundo piso
Fuente: Elaboración prop

Identificación y ubicación de los puntos de datos y nodos del segundo y tercer piso

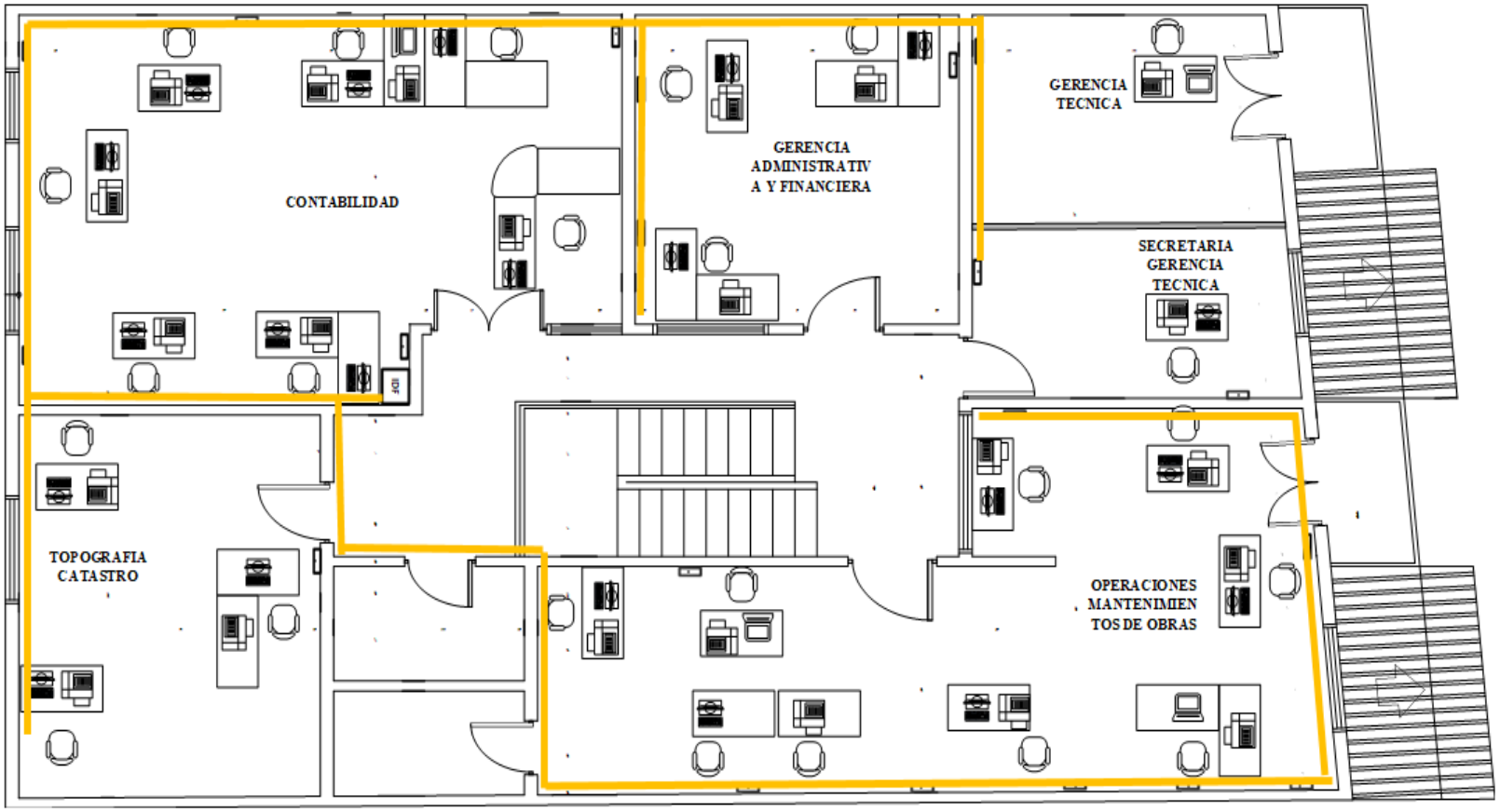


Figura III.1.22: Organización completa del segundo piso
Fuente: Elaboración propia

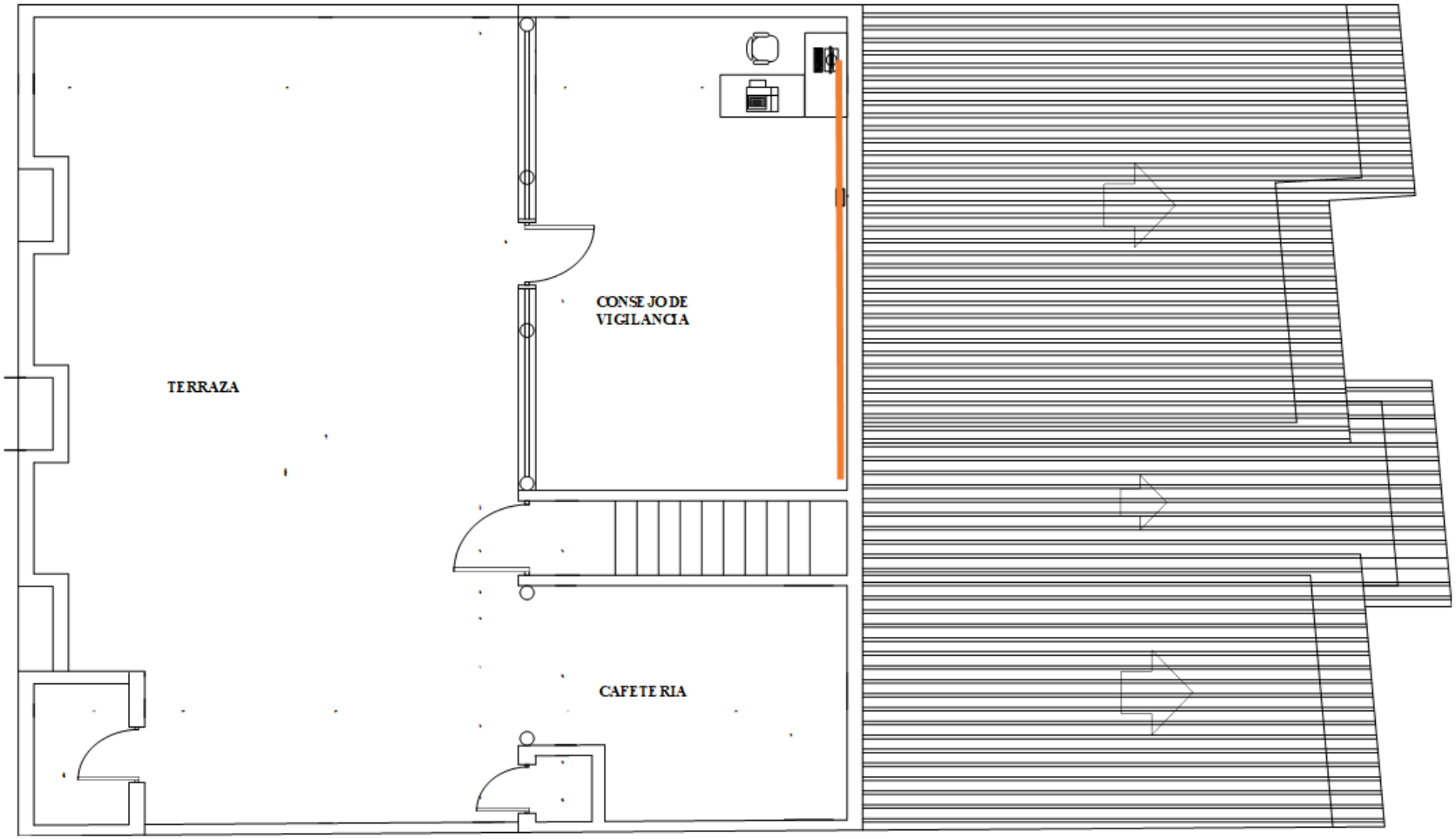


Figura III.1.23: Organización completa del tercer piso
Fuente: Elaboración propia

III.1.3.5. MDF (Main Distribution Frame)

El MDF actual de la empresa fue evaluado y se determinó que no cumple con los requisitos establecidos en la norma ANSI/TIA-942, debido a que:

- Se encuentra expuesto a condiciones ambientales inapropiadas (ventanas, polvo, humedad).
- No posee ventilación adecuada ni control de temperatura.
- Está ubicado en un espacio sin seguridad física y con acceso libre al personal.

Por ello, se propone la remodelación en el mismo piso garantizando el cumplimiento de la normativa, o la reubicación del MDF a la planta baja del edificio, en un espacio cerrado, acondicionado y exclusivo para el área de telecomunicaciones. Esta decisión se basa en la necesidad de garantizar:

- Protección del equipamiento crítico ante desastres naturales o cortes eléctricos.
- Mejores condiciones ambientales: instalación de ventilación forzada para mantener temperaturas entre 18°C y 27°C y humedad controlada.
- Acceso restringido solo a personal autorizado de sistemas.
- Eliminación de ventanas y sellado de ranuras para evitar entrada de polvo o humedad.

El MDF estará equipado con:

- Racks metálicos de 19 pulgadas.
- Bandejas porta cables horizontales y verticales.
- Una UPS dedicada para protección de los equipos ante cortes de energía.
- Espacio para alojamiento de switches principales, servidores, firewall y router.

III.1.3.6. Material de canalización

III.1.3.6.1. Cableado

Cable de Categoría 6A

El sistema de cableado estructurado propuesto para la red de Cosaalt está basado en la norma ANSI/TIA-568-C, asegurando el cumplimiento de parámetros técnicos como rendimiento, orden, mantenibilidad y soporte a futuro crecimiento. Para ello, se implementará cable UTP categoría 6A, con capacidad de transmisión de hasta 10 Gbps a 100 metros.

El diámetro del cable seleccionado es de 8.3 mm, por lo cual se respetará un radio de curvatura mínimo de 33 mm durante la instalación, evitando interferencias o pérdida de señal. La longitud máxima de canal horizontal se mantendrá por debajo de los 90 metros.

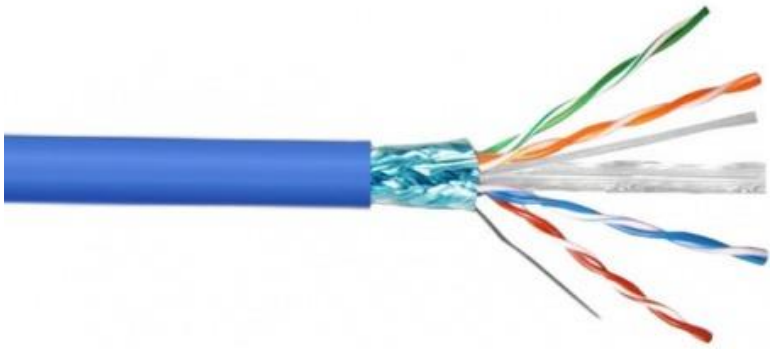


Figura III.1.24: cable Cat. 6A
Fuente: Panduit

El cableado se desplegará en forma radial desde el MDF hacia los switches de acceso en cada piso. Se dejará una reserva mínima de cable de 1 metro en cada punto final, y en el MDF se considerará un excedente adicional para permitir futuras reconfiguraciones.

Cable de Fibra Óptica

Para las conexiones entre switches principales y de acceso, se empleará cable de fibra óptica multimodo OM3 con conectores LC. Este tipo de cable es esencial para garantizar una conexión de alta velocidad y baja latencia entre los dispositivos de red más críticos. El modelo sugerido es el Corning MIC® OM3, que ofrece una excelente performance y durabilidad. La fibra óptica es

especialmente adecuada para largas distancias y entornos con altas demandas de ancho de banda, asegurando que el tráfico de red fluya sin interrupciones.

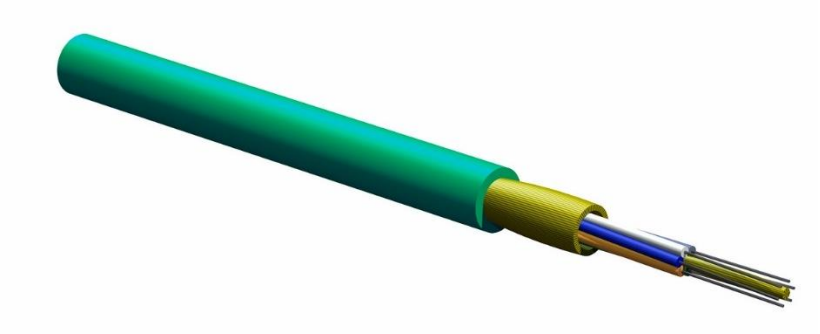


Figura III.1.25: fibra óptica
Fuente: Corning

III.1.3.6.2. Componentes de Conexión

Rosetas (Outlets)

Las rosetas son componentes esenciales para proporcionar puntos de conexión ordenados y seguros para los cables de red. Se utilizarán placas de pared con puertos RJ45 diseñadas específicamente para cables de categoría 6A. Estas rosetas se instalarán en ubicaciones estratégicas como paredes, suelos y mesas, permitiendo una fácil accesibilidad y organización de las conexiones de red.

Figura III.1.26: rosetas de conexión
Fuente: mercado libre

Conectores RJ45

Para garantizar conexiones seguras y fiables, se emplearán conectores modulares RJ45 para los cables de categoría 6A. El modelo recomendado es el Panduit CJ6X88TGBU, que proporciona una conexión robusta y minimiza la pérdida de señal. Estos conectores se utilizarán para terminar los cables de red, asegurando que todas las conexiones sean firmes y de alta calidad.

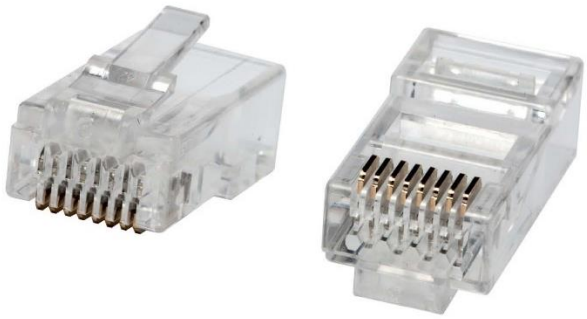


Figura III.1.27: RJ45
Fuente: Emelec Viascom

III.1.3.6.3. Canalización

Canaletas y conductores

La canalización de la red estará diseñada según las especificaciones de la norma ANSI/TIA-569-C, que establece requisitos para la instalación física de rutas y espacios destinados al cableado de telecomunicaciones.

Para garantizar una instalación ordenada, segura y con capacidad de crecimiento, se implementarán los siguientes elementos:

- Canaletas de PVC tipo industrial de 60×40 mm, instaladas en pared y techo según la ubicación de los puestos de trabajo.
- Se utilizarán bandejas porta cables metálicos en los tramos principales, especialmente en el MDF, para gestionar el alto volumen de cables.

- Se mantendrá una separación mínima de 30 cm entre canalizaciones eléctricas y de datos, tal como indica la norma, con el fin de evitar interferencias electromagnéticas que puedan afectar el rendimiento de la red.
- Las canalizaciones estarán sobredimensionadas con al menos un 25% de capacidad libre, permitiendo futuras expansiones sin requerir remodelaciones físicas.

Adicionalmente, se evitarán curvas cerradas en los recorridos de canalización, y se respetarán los radios de giro necesarios para mantener la integridad física del cableado. Las canaletas estarán cerradas y bien fijadas a estructuras sólidas para evitar movimientos o desgaste.

Canaletas de Superficie:

Para la instalación del cableado en paredes y techos, se emplearán canaletas de superficie rígidas. El modelo sugerido es el Panduit T-70 Surface Raceway, conocido por su durabilidad y capacidad de organización. Estas canaletas proporcionan una ruta protegida para los cables, asegurando que se mantengan ordenados y protegidos contra el desgaste físico y posibles interferencias. Además, su diseño modular facilita la instalación y permite modificaciones futuras con relativa facilidad.

Figura III.1.28: Canaleta pequeña
Fuente: Panduit

Bandejas Porta cables:

Para soportar y organizar grandes volúmenes de cables, se utilizarán bandejas porta cables como las Chatsworth Universal Cable Runway. Estas bandejas abiertas son ideales para la organización de cables en áreas de alto tráfico, como salas de servidores y centros de datos. Las bandejas permiten un fácil acceso a los cables para el mantenimiento y la gestión, y su diseño robusto asegura que los cables se mantengan en su lugar sin riesgo de enredos o daños.

Figura III.1.29: Bandejas porta cables
Fuente: Electro Instalador

III.1.3.6.4. Gestión de Cableado

Paneles de Conexión (Patch Panels)

Los paneles de conexión, también conocidos como patch panels, son esenciales para la gestión y organización del cableado de red en Cosaalt. Estos paneles, que se montan en racks, permiten terminar y organizar los cables de red de manera eficiente. El modelo sugerido para este proyecto es el Panduit DP48688TGY, un panel de alta calidad que proporciona múltiples puertos RJ45 para conectar y gestionar el cableado. Cada cable de red proveniente de dispositivos finales se termina en el patch panel, lo que facilita la administración de las conexiones y permite realizar cambios rápidos y sencillos en la configuración de la red. La organización centralizada en los patch panels mejora la

flexibilidad y la capacidad de adaptación, ya que permite identificar y gestionar fácilmente cada conexión, reduciendo el tiempo necesario para el mantenimiento y la resolución de problemas.

Figura III.1.30: Panel de conexión
Fuente: Tienda mia

Patch Cords

Para la interconexión de dispositivos dentro de los racks y la conexión de dispositivos a rosetas y paneles de conexión, se utilizarán patch cords de categoría 6A con conectores RJ45 en ambos extremos. El modelo recomendado es el Panduit UTP28X, conocido por su alta calidad y rendimiento. Estos cables cortos se utilizarán de dos medidas de 0.5, 2 y 1 metros de longitud. Los patch cords permiten conexiones rápidas y fiables entre los dispositivos y los paneles de conexión, facilitando la organización dentro de los racks y asegurando una conectividad robusta y de alto rendimiento. Además, su uso adecuado ayuda a minimizar el desorden y los enredos de cables, lo que es fundamental para mantener un entorno de red limpio y manejable.

En el MDF se instalarán 50 patch cords de 0.5 m para interconexiones entre patch panels y switches. Para los 2 IDFs se utilizarán 38 patch cords de 0.5 m para la misma conexión.

Para la conexión de los servidores al switch de servidores se utlizara 10 patch cords de 1 m de longitud.

Además, se utilizarán 12 patch cords de 2 metros para conectar equipos que anteriormente se encontraban conectados de forma inalámbrica y que ahora pasarán a conexión física, mejorando la estabilidad del servicio.

Figura III.1.31: cable de conexión corto
Fuente: Fromm Electric

III.1.3.7. Equipos de conectividad

III.1.3.7.1. Firewall perimetral

Este firewall sirve para dar seguridad a la red, también garantizar la disponibilidad de la red de Cosaalt de esta manera se considera indispensable con un dispositivo de control de tráfico entrante y saliente de la red.

Teniendo en cuenta que Cosaalt ya cuenta con un dispositivo capaz para manejar la seguridad como lo es Uniper SSG-20 será reutilizable para la nueva red de datos y se dará las siguientes características del equipo:

- Protección firewall

- Sistema de filtrado
- Análisis de antivirus
- Alta disponibilidad de contenidos
- Interfaces: 2 X 1000 Base-T RJ-45
- 20 puertos de RJ-45
- Almacenamiento interno de 32 GB

Figura III.1.32: firewall
Fuente: Juniper Network

III.1.3.7.2. Router

Para la selección del router a utilizar en el diseño se mantendrá con los que cuenta actualmente Cosaalt por su capacidad para aguantar la propuesta, el router mikrotik ccr1009-7g-1c-1s+ y el router D-LINK DSR-1000AC.

MIKROTIK ccr1009-7g-1c-1s+

- Procesador de 9 cores 1.2 GHz.
- 2 GB RAM.
- 128 MB de Almacenamiento.
- 7 puertos Gigabit.
- 1 puerto Combo.
- 1 puerto SFP+

Figura III.1.33: Router mokrotic ccr1009-7g-1c-1s+
Fuente: Tectel Bolivia

TP-LINK TL-R600VPN

- 1 puerto WAN Gigabit y 4 puertos de red local Gigabit: conectividad por cable de alta velocidad
- Soporta los protocolos VPN IPsec/PPTP, hasta 20 túneles VPN IPsec y 16 túneles VPN PPTP soportados simultáneamente
- Cortafuegos SPI y protección contra ataques DoS para proteger la red de las amenazas de Internet más comunes
- Incluye protección profesional contra rayos de hasta 4000 V para mantener a salvo su inversión. (TP-LINK, TP-LINK, s.f.).

Figura III.1.34: Router TL-R600VPN
Fuente: TP-LINK

III.1.3.7.3. Switches

La selección de switches se realizó tomando en cuenta la escalabilidad, para lo cual se consideró necesario adquirir 3 switches con 48 puertos para la planta baja, primer piso y el segundo piso. Además, se requerirá un switch más para que trabaje como principal.

Los switches solicitados serán: 3 switches TP-Link T3700G-52TQ y 1 switch D-link Dgs-3130-30ts

3 switches de 48 Puertos:

TP-Link T3700G-52TQ. Tipo de interruptor: Gestionado, Capa del interruptor: L2/L3. Puertos tipo básico de conmutación RJ-45 Ethernet: Gigabit Ethernet (10/100/1000), Cantidad de puertos

básicos de conmutación RJ-45 Ethernet: 48, Cantidad de puertos USB 2.0: 2, Puerto de consola: RJ-45. Tabla de direcciones MAC: 32000 entradas, Capacidad de conmutación: 176 Gbit/s. Estándares de red: IEEE 802.1D, IEEE 802.1Q, IEEE 802.1p, IEEE 802.1s, IEEE 802.1w, IEEE 802.1x, IEEE 802.3ab, IEEE.... Montaje en rack, Factor de forma: 1U. (Informatica, s.f.)

Figura III.1.35: Switch Tp-link de 48 puertos
Fuente: Ultima Informática

1 Switch de 24 Puertos: D-link Dgs-3130-30ts

- Gestionado L3 Administración basada en web
- Calidad de servicio (QoS) soporte
- Cantidad de puertos básicos de conmutación RJ-45 Ethernet: 24
- Soporte 10G 10BASE-T, 10GBASE-T, 100BASE-T, 1000BASE-T
- Tabla de direcciones MAC: 16384 entradas Capacidad de conmutación: 168 Gbit/s
- Lista de Control de Acceso (ACL)
- Apilable
- CC

D-Link DGS-3130-30TS/E. Tipo de interruptor: Gestionado, Capa del interruptor: L3. Puertos tipo básico de conmutación RJ-45 Ethernet: Gigabit Ethernet (10/100/1000), Cantidad de puertos básicos de conmutación RJ-45 Ethernet: 24, Cantidad de puertos USB 2.0: 1. Tabla de direcciones MAC: 16384 entradas, Capacidad de conmutación: 168 Gbit/s. Estándares de red: IEEE 802.1D, IEEE

802.1Q, IEEE 802.1p, IEEE 802.1s, IEEE 802.1v, IEEE 802.1w, IEEE 802.1x, IEEE.... Conector eléctrico: Conector de alimentación AC-in (Informatica I. , s.f.)

Figura III.1.36: Switch D-link de 24 puertos
Fuente: INNOVA Informática

Los switches con los que cuenta Cosaalt son:

TP-Link T2600G-28TS

- Conexiones Gigabit Ethernet en todos los puertos proporcionando velocidad total de transferencia de datos
- Funcionalidades L2+ —— Enrutamiento Estático, ayuda a enrutar el tráfico interno para una mayor eficiencia de uso en los recursos de red
- Vinculación Puerto-MAC-IP, ACL, Seguridad por Puerto, Defensa DoS, Control de Tormentas, DHCP Snooping, Autenticación 802.1X y Radius que proporciona robustas estrategias de seguridad
- QoS L2/L3/L4 y IGMP snooping que optimiza aplicaciones de voz y vídeo
- Soporta IPv6 con dual stack IPv4/IPv6, MLD snooping, IPv6 neighbor discovery
- Web, CLI (Puerto de Consola, Telnet, SSH), SNMP, RMON e Imagen Dual que aportan múltiples políticas de gestión. (TP-LINK, s.f.)

Figura III.1.37: Switch Tp-link de 24 puertos
Fuente: tp-link

D-LINK DGS-3630-28SC

- Alto rendimiento, flexibilidad, tolerancia a fallas y funciones avanzadas de software para PYMES, PYME, grandes empresas e ISP.
- 20 x puertos SFP 4 x Combo 10/100/1000BASE-T/SFP puertos 4 x 10G SFP+ con protección contra sobretensiones de 6 kV en todos los puertos de acceso RJ-45 soporte de fuente de alimentación redundante (RPS)
- Switch Resource Management (SRM) para una gestión flexible de los recursos del sistema Soporte VPN MPLS L2VPM/L3 Soporte completo del protocolo de enrutamiento L3 que incluye OSPF, BGP e ISIS para conmutador habilitado para SDN IPv4/IPv6, compatible con Openflow 1.3
- Los switches administrados apilables Gigabit L3 de la serie DGS-3630 combinan 4 puertos integrados de apilamiento/enlace ascendente 10G, protección contra sobretensiones integrada de 6kV, gestión inteligente de recursos de conmutadores e imágenes de software actualizables
- Alta disponibilidad y flexibilidad: incluye tecnología de apilamiento, que permite combinar múltiples switches para formar una sola pila física o virtual. Escale su red utilizando solo un cable de apilamiento y sin necesidad de apilar módulos. (AMAZON, s.f.)

Figura III.1.38: Switch D-link de 24 puertos
Fuente: Amazon

III.1.3.7.4. Servidores

En cuanto a los servidores, también se tomarán en cuenta los que ya tiene Cosaalt.

Servidor Dell:

Marca y Modelo: Dell PowerEdge R740

Servidor rack con procesadores Intel Xeon, gran capacidad de memoria y almacenamiento, adecuado para aplicaciones críticas.

Figura III.1.39: Servidor Dell
Fuente: open Support

Servidor IBM:

Marca y Modelo: IBM System x3650 M5

Servidor de alto rendimiento con procesadores Intel Xeon, diseñado para cargas de trabajo intensivas y alta disponibilidad.

Figura III.1.40: Servidor IBM
Fuente: Lenovo Press

III.1.3.8. Seguridad física

Para la propuesta de ed para Cosaalt, se integran medidas específicas para asegurar tanto la infraestructura de red como el acceso físico a los componentes críticos, conforme a las recomendaciones de las normas ANSI/TIA-942 y TIA/EIA-606-B.

Protección del MDF

La ubicación anterior del MDF no cumplía con los requisitos mínimos de seguridad física, ya que se encontraba expuesto a accesos no controlados, presencia de ventanas y riesgos ambientales. Por ello, se propuso su reubicación a un ambiente cerrado en la planta baja, donde se aplicarán las siguientes medidas:

- Acceso restringido únicamente a personal autorizado de TI, mediante cerraduras o control de acceso físico.
- Eliminación de ventanas o puntos de exposición al polvo, humedad o fluctuaciones térmicas.
- Instalación de ventilación controlada, manteniendo la temperatura entre 18 °C y 27 °C y humedad relativa entre 40% y 60%.
- Implementación de una UPS, para proteger los equipos de red frente a interrupciones eléctricas.
- Montaje en racks cerrados y metálicos de 19", los cuales brindan organización, circulación de aire y seguridad física a los switches, servidores, firewall y router.

Protección del cableado y canalización

- Todo el cableado estructurado será canalizado mediante canaletas cerradas y bandejas porta cables metálicos, evitando cables sueltos, enredados o expuestos.
- Las canaletas de datos estarán separadas 30 cm o más de las eléctricas, para evitar interferencia electromagnética, cumpliendo con TIA/EIA-569-C.
- En zonas de tránsito, las canaletas estarán aseguradas a muros o techos, evitando contacto accidental del personal.

Identificación y etiquetado

Para facilitar la gestión y reducir errores en intervenciones técnicas:

- Se aplicará un sistema de etiquetado normalizado, conforme a la norma TIA/EIA-606-B, donde cada punto de red, cable, patch panel, switch y puerto estará correctamente identificado con códigos alfanuméricos.
- La codificación seguirá un esquema por piso – rack – puerto – VLAN, lo cual permitirá trazabilidad y control.

Resguardo de puntos críticos

- Los servidores, firewall, y equipos de red centrales estarán montados en racks con paneles frontales cerrados y con control de acceso físico.
- El access points se ubicarán en áreas elevadas y protegidas contra manipulación.
- Se asegurará que los switches de acceso en cada piso estén dentro de áreas restringidas o cajas metálicas cerradas, si se encuentran expuestos.

III.1.4. Aplicación de normas y estándares técnicos en el diseño de red

El diseño de la nueva arquitectura de red para Cosaalt se basa no solo en las necesidades funcionales identificadas durante el análisis de requerimientos, sino también en el cumplimiento de normas y estándares técnicos reconocidos internacionalmente. Esto garantiza una solución estructurada, escalable, segura y alineada con buenas prácticas de la industria.

III.1.4.1. Norma ANSI/TIA-568-C: Cableado estructurado

Esta norma define los criterios técnicos y de instalación para sistemas de cableado estructurado en edificios comerciales. Establece los tipos de cables, conectores, distancias máximas, topologías y métodos de terminación.

En la propuesta se utiliza cable UTP categoría 6A, que permite velocidades de hasta 10 Gbps, cumpliendo con los requerimientos de rendimiento y futuro crecimiento. Se consideran las distancias

recomendadas, márgenes de curvatura, el uso de patch cords y paneles de parcheo en el MDF, conforme a esta norma.

- Se usó cable UTP categoría 6A de 8.3 mm, cumpliendo con el soporte para 10 Gbps.
- Se respetó el radio mínimo de curvatura de 33 mm en canaletas y bandejas.
- Se instalaron 32 patch cords de 0.5 m en el MDF, 12 de 2 m y 10 de 1 m para reemplazar conexiones inalámbricas.
- Las longitudes no superan los 90 m de cableado horizontal, más 10 m en patch cords.

III.1.4.2. Norma ANSI/TIA-569-C: Rutas y espacios de telecomunicaciones

La norma TIA-569 establece las especificaciones para la planificación de canaletas, bandejas porta cables, racks, espacios técnicos (como el MDF) y condiciones físicas necesarias para una instalación profesional y segura.

En el diseño se propone la remodelación del MDF para eliminar factores de riesgo como ventanas, accesos no controlados y falta de ventilación. Además, se planifica el uso de canaletas y cable canal para mantener orden y facilitar el mantenimiento del sistema de cableado.

- Se estableció una separación de 30 cm entre cables de red y eléctricos para evitar interferencias.
- Se usaron bandejas porta cables y canaletas cerradas para separar tipos de cable.
- Se planificó una canalización con capacidad de crecimiento del 25%, permitiendo ampliaciones futuras.

III.1.4.3. Norma ANSI/TIA-606-B: Administración del cableado

Esta norma establece los lineamientos para la identificación y documentación de componentes del sistema de cableado estructurado.

En la propuesta se contempla el etiquetado de cables, puertos, patch panels y puntos de red, así como la elaboración de planos y registros técnicos que permitirán una administración efectiva del sistema, facilitando el mantenimiento, la solución de fallos y futuras expansiones.

- Todos los cables y puertos fueron etiquetados con codificación por piso, rack y VLAN (ejemplo: 2F-R1-V20-12).
- Se elaboró un plano de red detallado con la ubicación de cada switch, puerto y punto de red.
- Se gestionó un registro de conexiones físicas y lógicas para facilitar mantenimiento y control.

III.1.4.4. Modelo OSI: Referencia para diseño lógico

El diseño de red sigue el modelo OSI como guía para organizar la estructura lógica.

- En capa 2 (Enlace de Datos) se aplican VLANs para segmentar la red por áreas funcionales (comercial, técnica, administrativa, impresoras, etc.), reduciendo la congestión y mejorando la seguridad.
- En capa 3 (Red) se implementa enrutamiento entre VLANs y un plan de direccionamiento IP escalable y jerárquico, lo que facilita la administración y futuras ampliaciones.

III.1.4.5. Seguridad: Principios basados en la norma ISO/IEC 27001

Aunque esta norma no se aplica directamente en su totalidad, se consideraron sus principios para reforzar la seguridad de la red, tales como:

- Segmentación de red mediante VLANs.
- Control de acceso lógico usando listas de control de acceso (ACLs).
- Seguridad perimetral mediante la incorporación de un firewall FortiGate para inspección profunda de paquetes (DPI), filtrado de contenido, y control de aplicaciones.

- Seguridad inalámbrica mediante WPA2-Enterprise con autenticación basada en RADIUS.

III.1.4.6. Norma ANSI/TIA-942: Infraestructura de centros de datos

Esta norma proporciona directrices específicas para el diseño físico de centros de datos, incluyendo cuartos de telecomunicaciones como el MDF.

En el análisis inicial, se identificó que el MDF actual de la empresa no cumple con varios de estos requerimientos: está expuesto a factores ambientales (ventanas, temperatura) y no cuenta con organización ni seguridad física adecuada.

- El MDF fue evaluado y se recomendó su remodelación o reubicación en planta baja, eliminando ventanas y mejorando el control ambiental.
- Se especificó el uso de racks metálicos, sistemas de ventilación, y UPS.
- Se garantizó que solo el personal autorizado acceda al MDF, siguiendo controles de seguridad física.

Estas mejoras siguen las recomendaciones de ANSI/TIA-942, asegurando condiciones óptimas para la operación continua de los equipos críticos de red.

III.1.5. Fase 4: Probar, Optimizar y Documentar el Diseño

III.1.5.1. Probar el diseño de red

Para garantizar la conectividad en la red, se realizaron pruebas de ping entre los dispositivos desde una PC a las vlans utilizando en Router principal configurado como Router-on-a-Syick.

- Prueba 1: Ping desde uns PCa la VLAN 10 (192.25.3.1).
  Resultado: Latencia mínima (<1 ms) y sin pérdida de paquetes.

- Prueba 2: Ping desde una PC a La VLAN 50 (192.25.3.161).
  Resultado: Latencia mínima (<1 ms) y sin pérdida de paquetes.
- Prueba 3: Conexión del Switch principal al Router principal
  Conclusión: La configuración Trunk funciona correctamente, asegurando comunicación entre los dispositivos.

III.1.5.2. Optimización del Diseño de Red

Ajustes de Ancho de Banda

- Redistribución: Se incrementó el ancho de banda de VLAN 10 y VLAN 20 de 20 Gbps a 25 Gbps cada una, reduciendo 5 Gbps asignados a VLAN 60.
- Justificación: La carga de trabajo en Access Points no requiere tanto ancho de banda, mientras que las áreas comerciales y administrativas manejan mayor tráfico de datos.

Propuesta de escalabilidad

- **Aumento de enlaces:** Propuesta de enlaces adicionales con fibra óptica entre el MDF y switches de piso para soportar futuros incrementos de usuarios.

III.1.5.3. Documentación del diseño

Toda la documentación se fue realizando a lo largo del documento, desde los diagramas lógicos y físicos, hasta la configuración del diseño de red propuesto.

Se presentaron los diagramas lógicos y físicos finales:

Diagrama lógico: Muestra las VLANs, asignaciones IP y rutas de red.

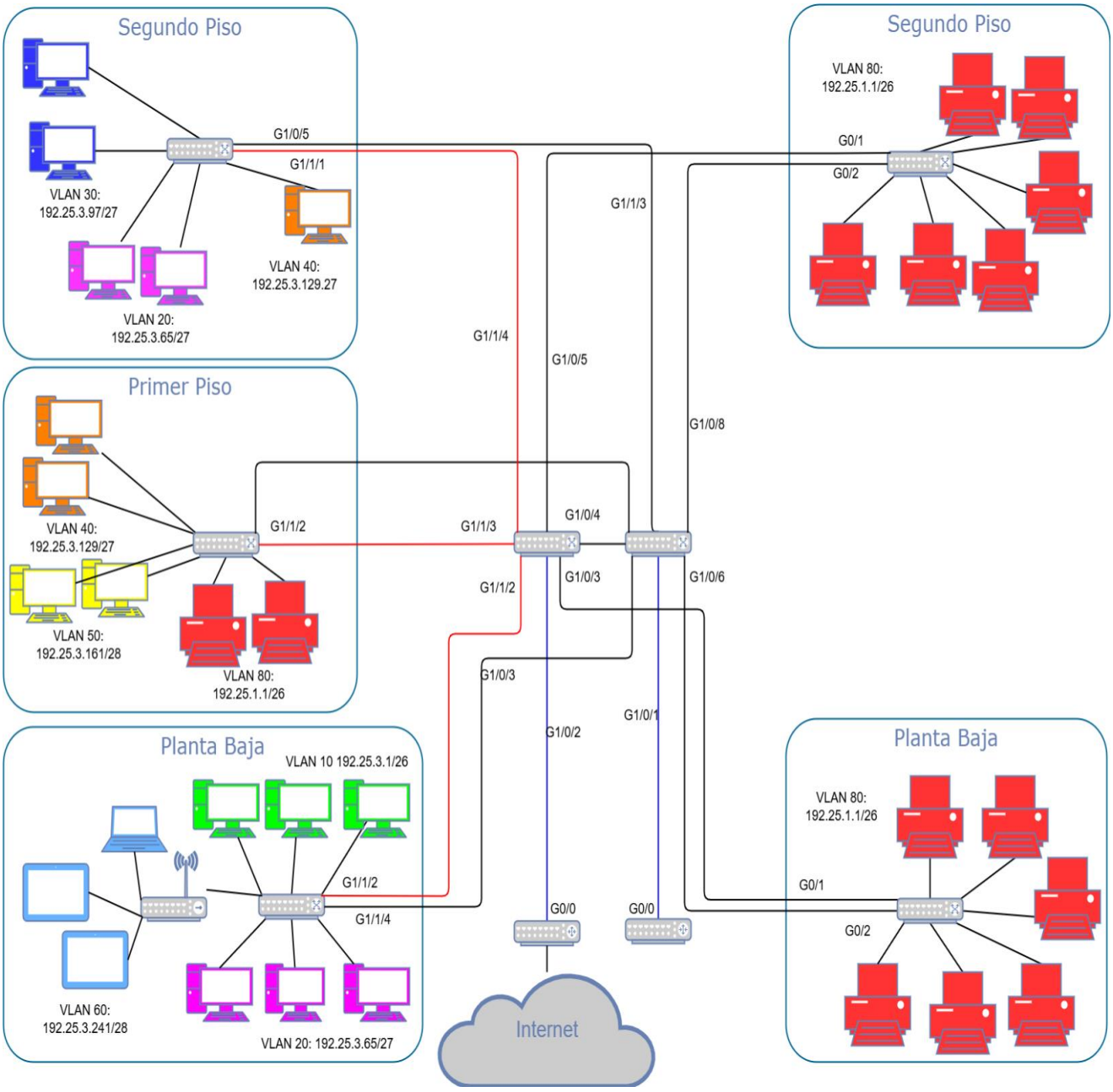


Figura III.1.41: Diagrama lógico
Fuente: Elaboración propia

Diagrama físico: Incluye la ubicación de dispositivos, conexiones y tipo de cables.

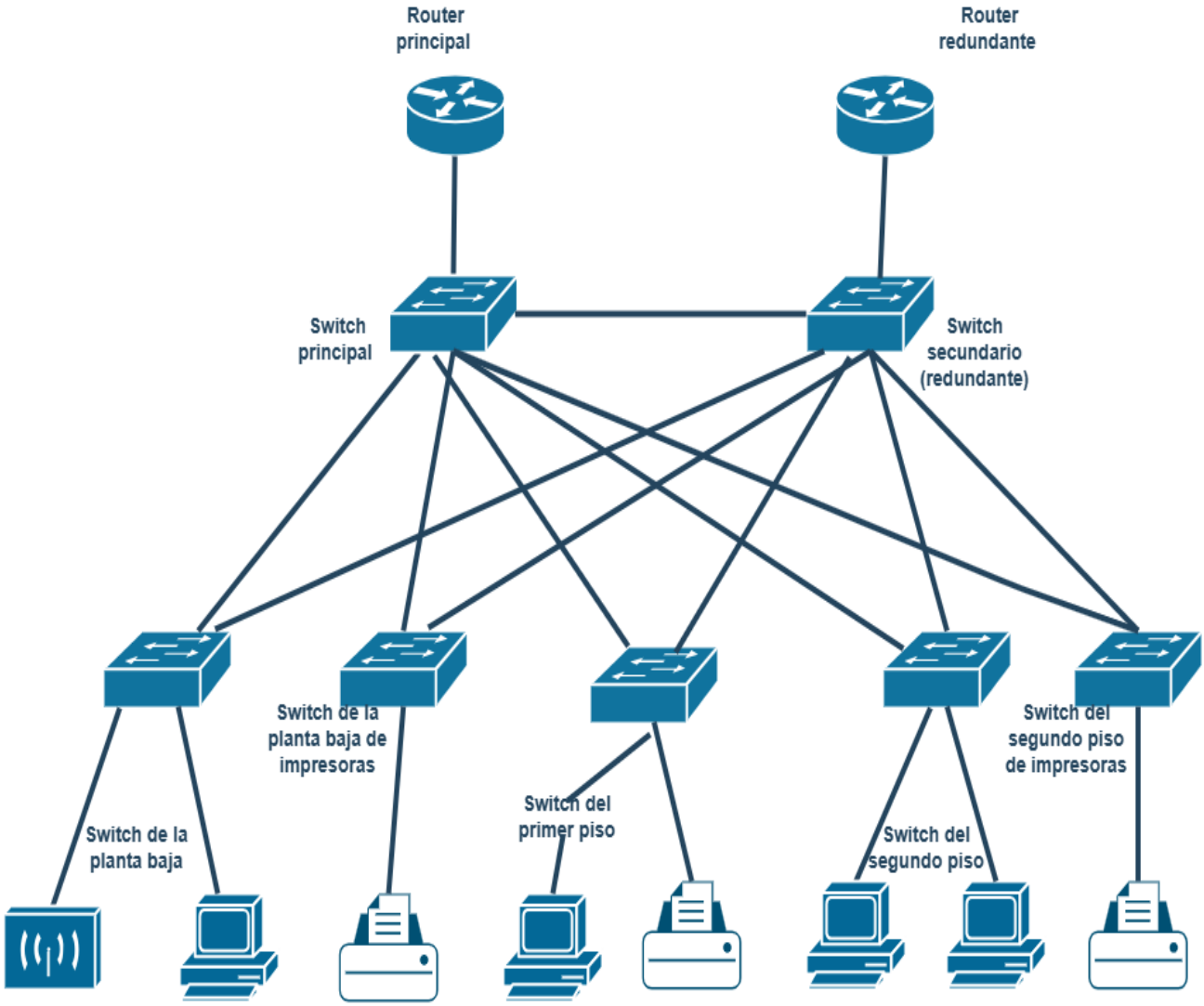


Figura III.1.42: Diagrama físico
Fuente: Elaboración propia

III.1.6. Simulación

Para esta fase se utilizó 3 herramientas para obtener una simulación de forma clara, estas son Cisco, Packet Tracer, Sketchup y GNS3. Cada una con un propósito diferente, Packet Tracer para la simulación de la red en términos de configuración de routing y switching, sketch para visualizar la estructuración del cableado en 3D observando de forma más clara la organización del cableado

estructurado y GNS3 para la simulación del Firewall de forma realista dado que Packet Tracer no cuenta con una configuración de forma clara de un Firewall.

III.1.6.1. Packet Tracer

Para comenzar con la simulación en cisco Packet Tracer lo primero que hay que hacer es armar el diseño de red que se necesita, seguido de la configuración de los switches, routers y otros dispositivos de red. Se asignaron direcciones IP, se crearon VLANs y se implementaron protocolos como RSTP (para redundancia) y LACP (para la agregación de enlaces).

En la siguiente imagen se puede observar cómo fue diseñada la primera ventada del diseño físico

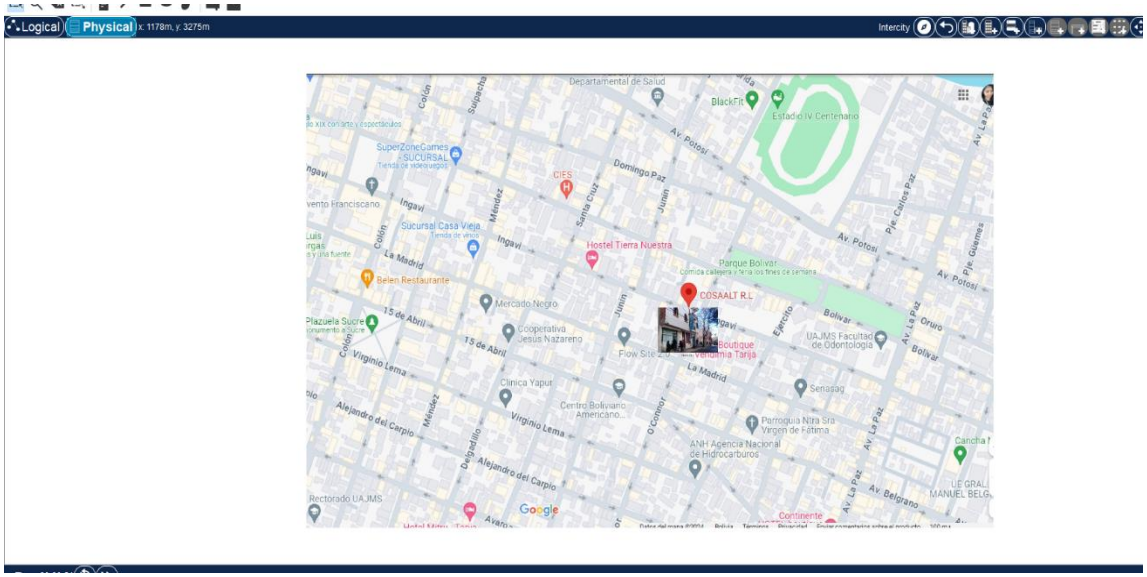


Figura III.1.43: simulación física en Packet Tracer 1
Fuente: Elaboración propia

En esta imagen se pude observar el edificio de Cosaalt, dando a conocer la forma en la que se conecta cada piso.

Figura III.1.44: Simulación física en Packet Tracer 2
Fuente: Elaboración propia

Simulación lógico y físico del diseño de la red

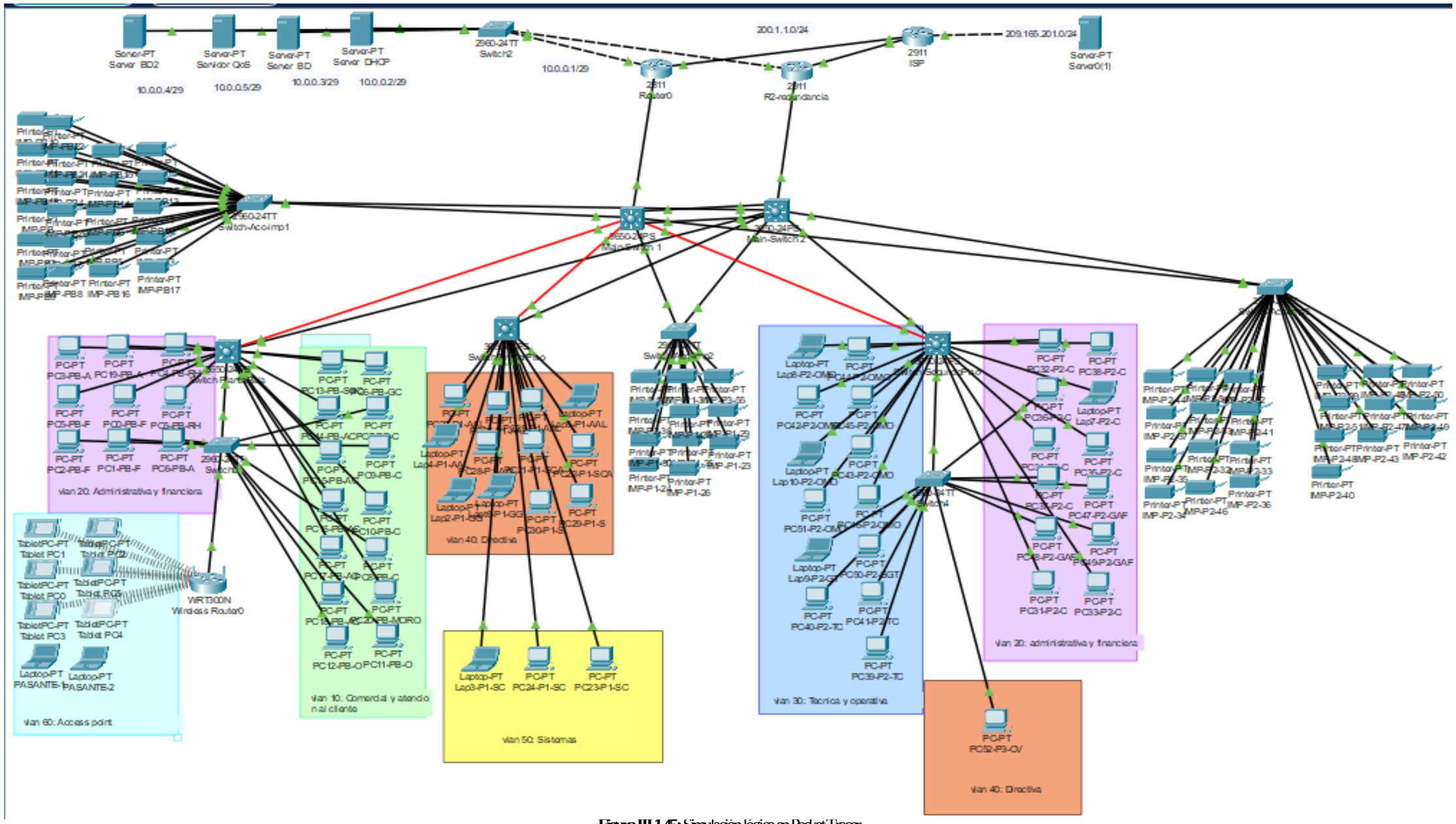


Figura III.145: Simulación lógica en Packet Tracer
Fuente: Elaboración propia

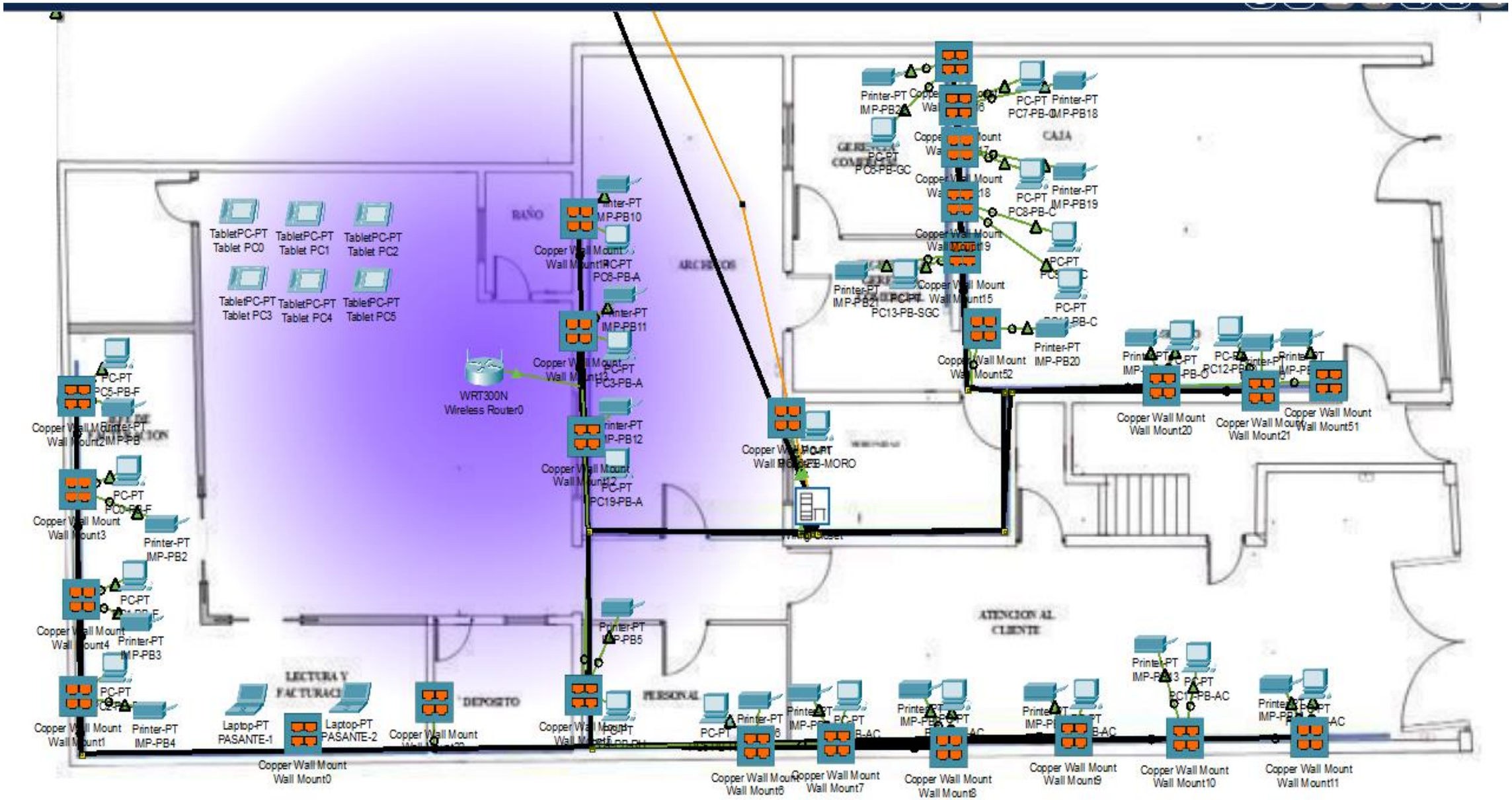


Figura III.1.46: Simulación física de la planta baja
Fuente: Elaboración propia

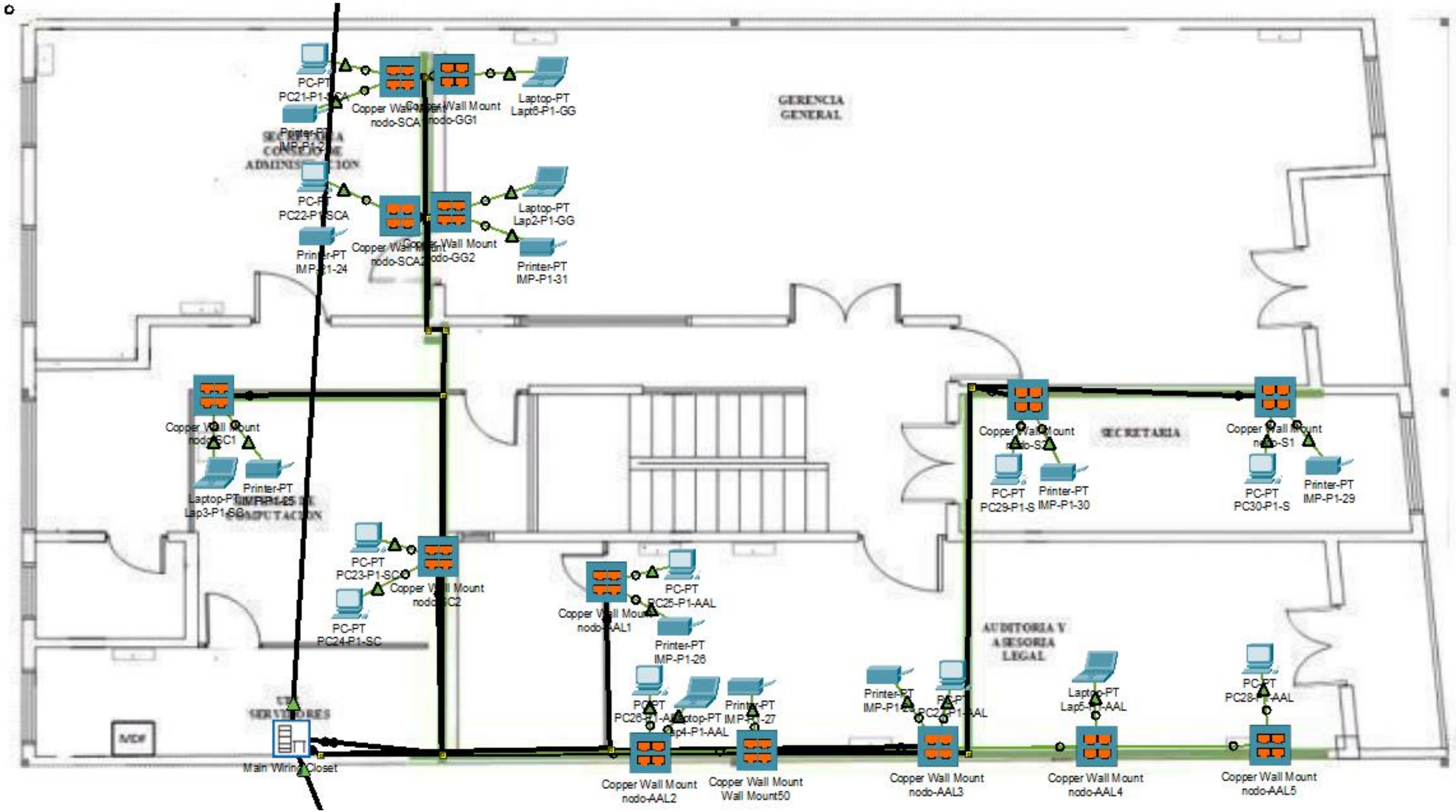


Figura III.147: Simulación física del primer piso
Fuente: Elaboración propia

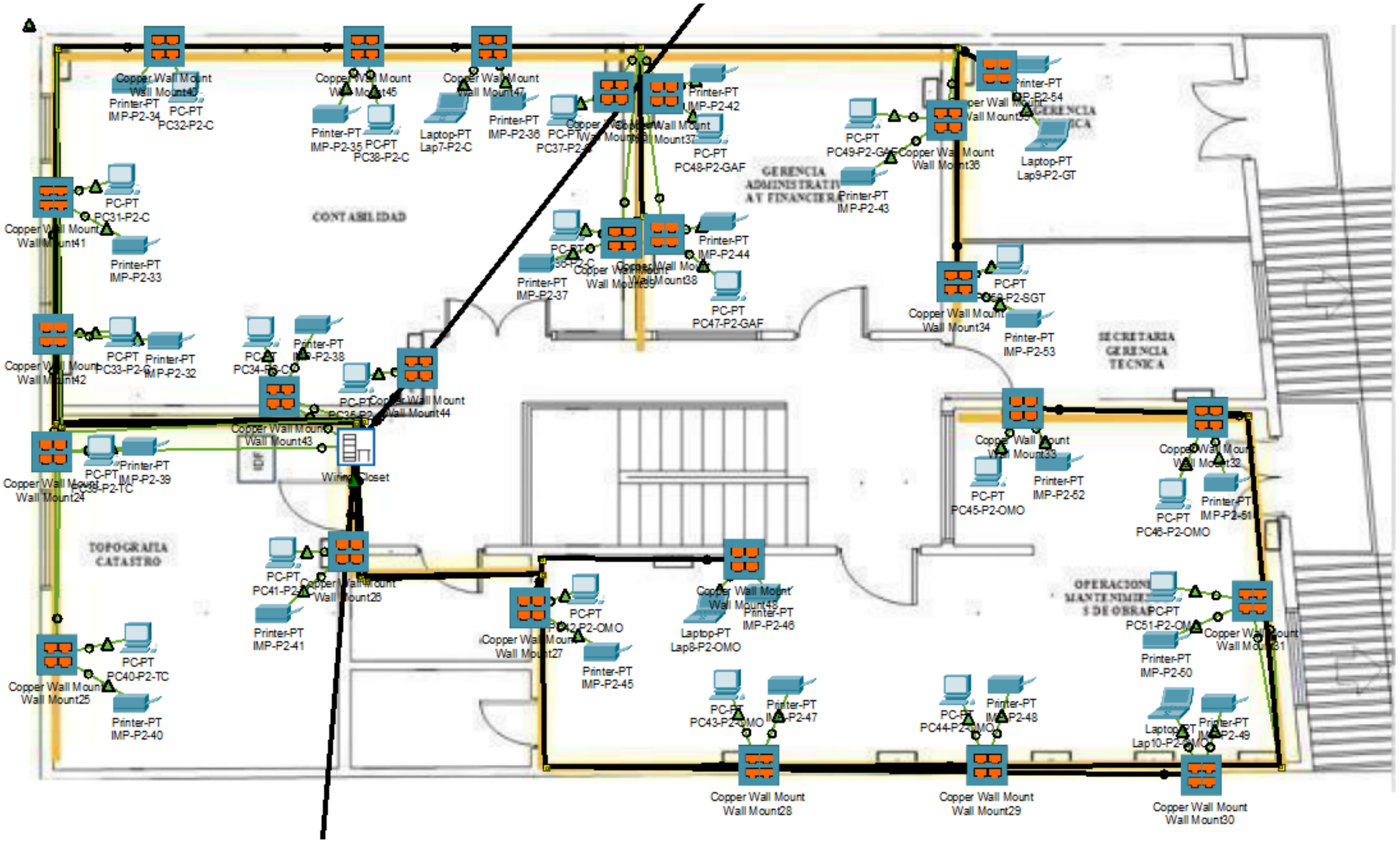


Figura III.148: Simulación física del segundo piso
Fuente: Elaboración propia

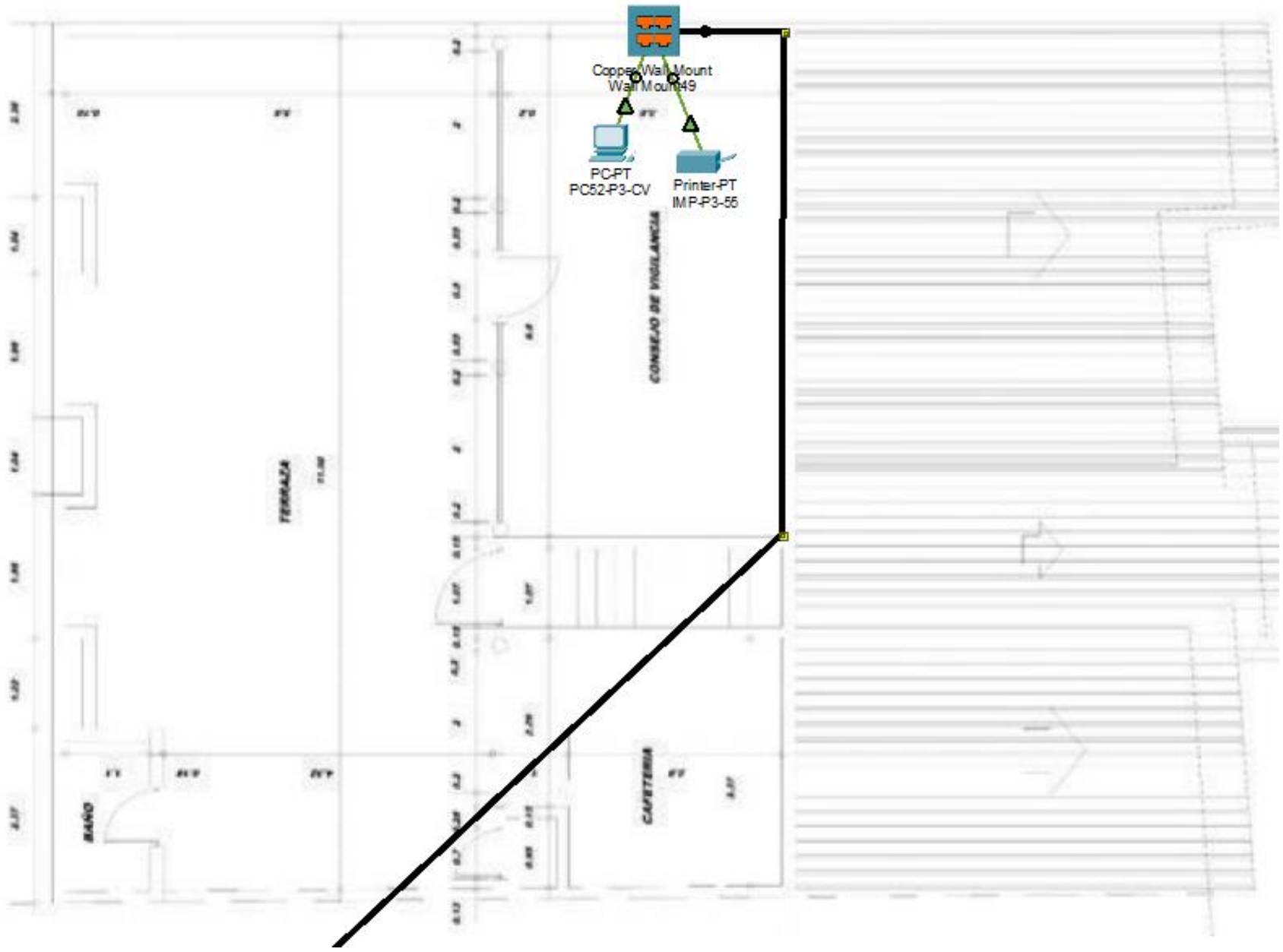


Figura III.149: Simulación física del tercer piso
Fuente: Elaboración propia

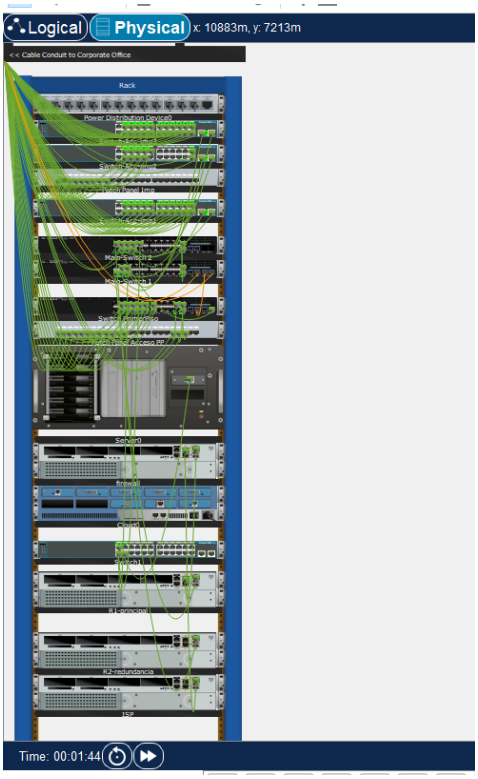

Logical
Physical
x: 10883m, y: 7213m
<< Cable Conduit to Corporate Office
Rack
Power Distribution Devices
Main Switch2
Main Switch1
Servers
Switch1
Switch2
ISP
Time: 00:01:44

Figura III.1.50: Simulación del Rack del MDF
Fuente: Elaboración propia

Configuración del Access point con la contraseña detallada anteriormente

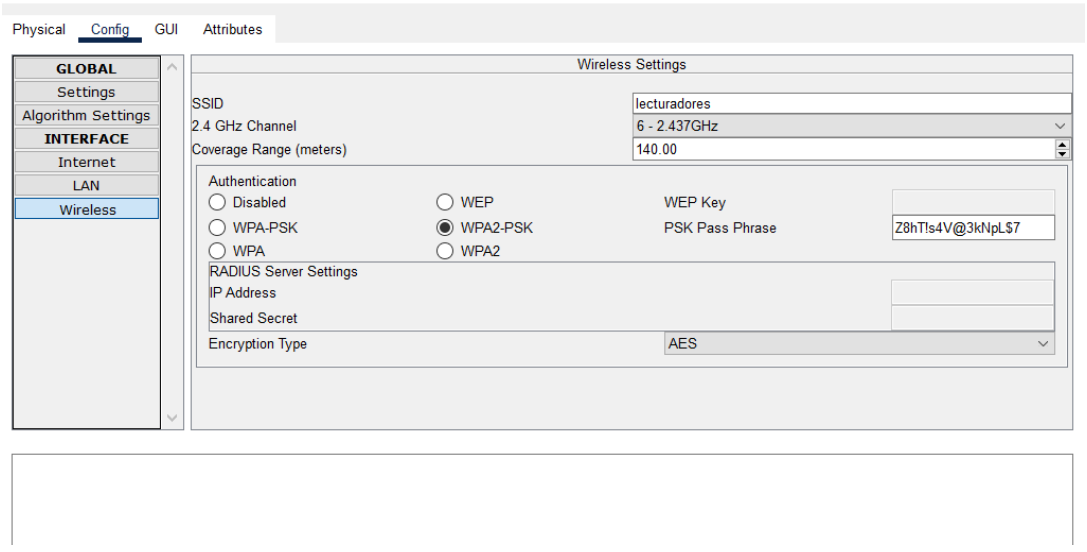


Figura III.1.51: Configuración access point
Fuente: Elaboración propia

III.1.6.2. Scketchup

se utilizó para modelar la estructura física de la red. SketchUp maneja modelado 3D, su enfoque en diseño tridimensional es adecuado para representar diagramas de cableado y topología física. Lo primero que se debe hacer es colocar los planos con medidas para poder levantar las paredes de forma exacta y con las medidas correctas

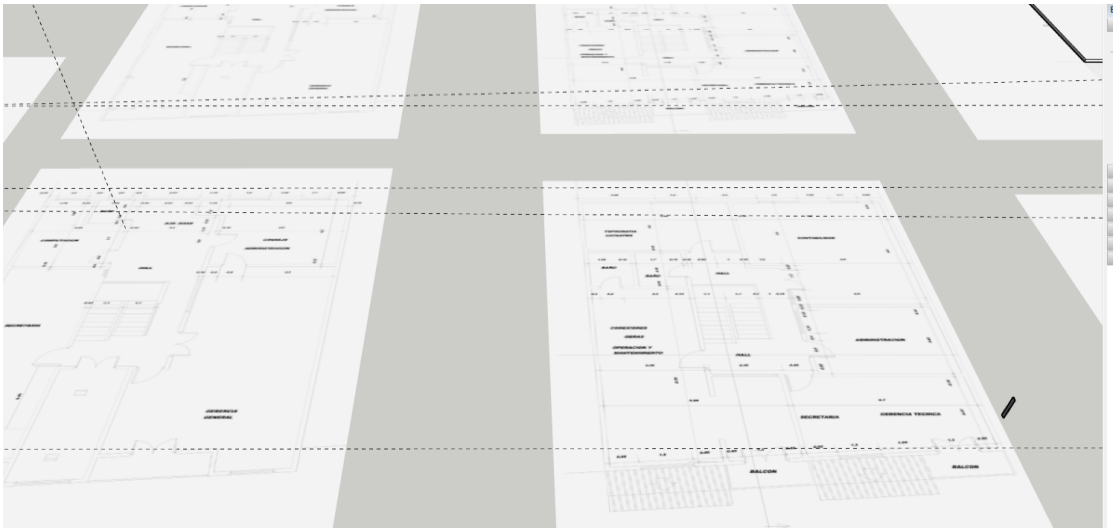


Figura III.1.52: Diseño en Scketchup
Fuente: Elaboración propia

Luego con el plano abajo dibujamos el contorno y levantamos un piso

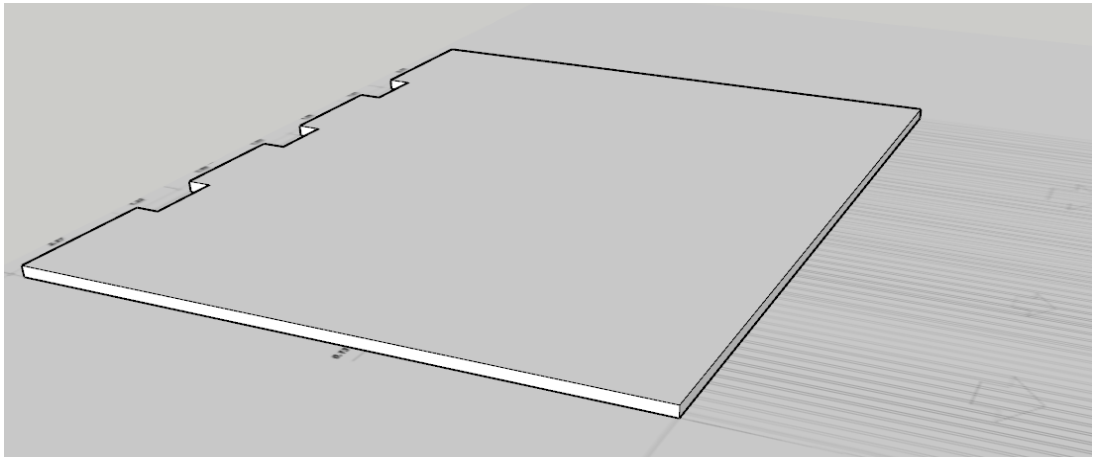


Figura III.1.53: simulación de piso en Scketchup
Fuente: Elaboración propia

Seguido de eso levantamos paredes volviendo a marcar los lugares donde se encuentran paredes en nuestro plano

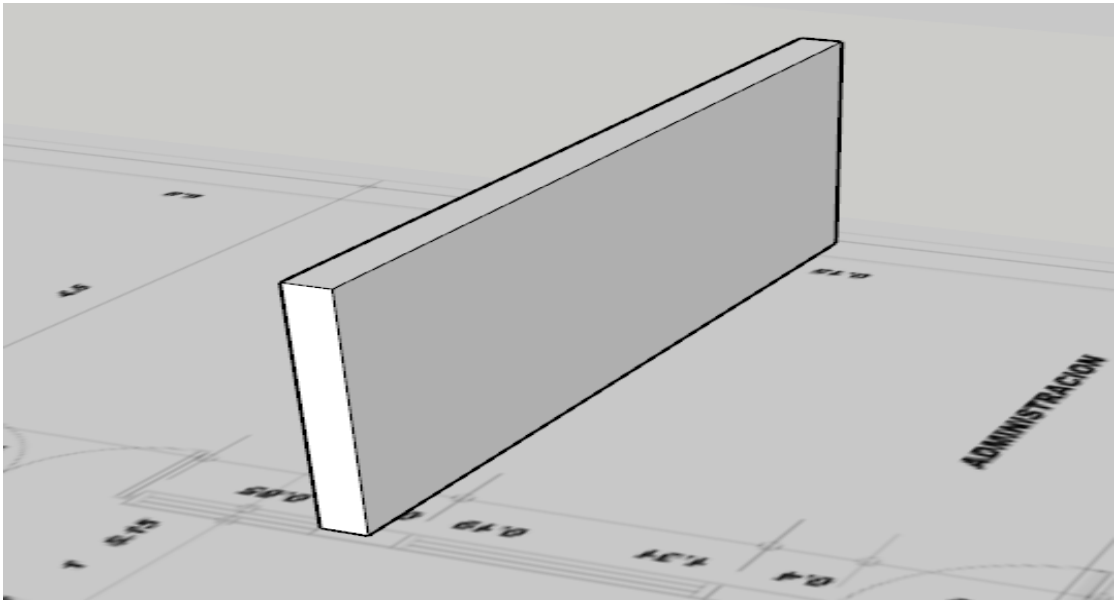


Figura III.1.54: Simulación de paredes en Scketchup
Fuente: Elaboración propia

Y armamos un escenario lo más parecido a la institución en la que estamos trabajando

Figura III.1.55: Simulación del edificio de Cosaalt en Scketchup
Fuente: Elaboración propia

Finalmente, colocamos el cableado junto a todos los dispositivos ya explicados

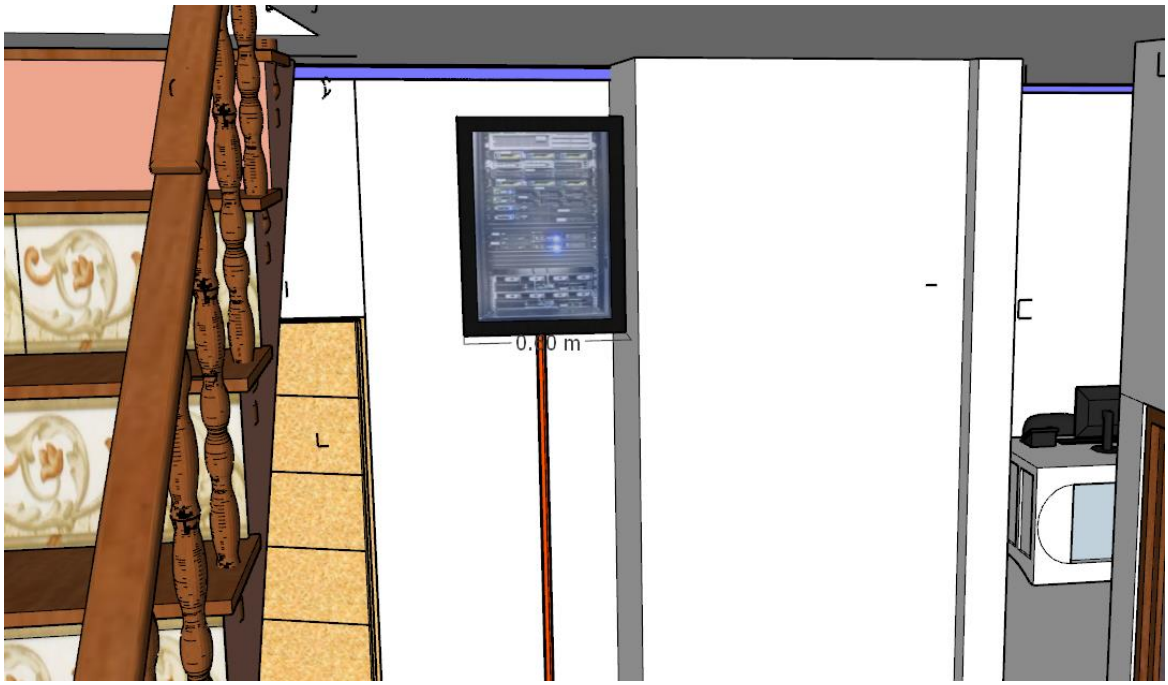


Figura III.1.56: Simulación de rack en Scketchup
Fuente: Elaboración propia

Figura III.1.57: Simulación de rosetas y canaletas en Scketchup
Fuente: Elaboración propia

III.1.6.3. GNS3

GNS3 es una plataforma avanzada que simula entornos de red con mayor realismo. Fue utilizada para trabajar específicamente con el firewall Juniper SSG-20, que no está disponible en Packet Tracer.

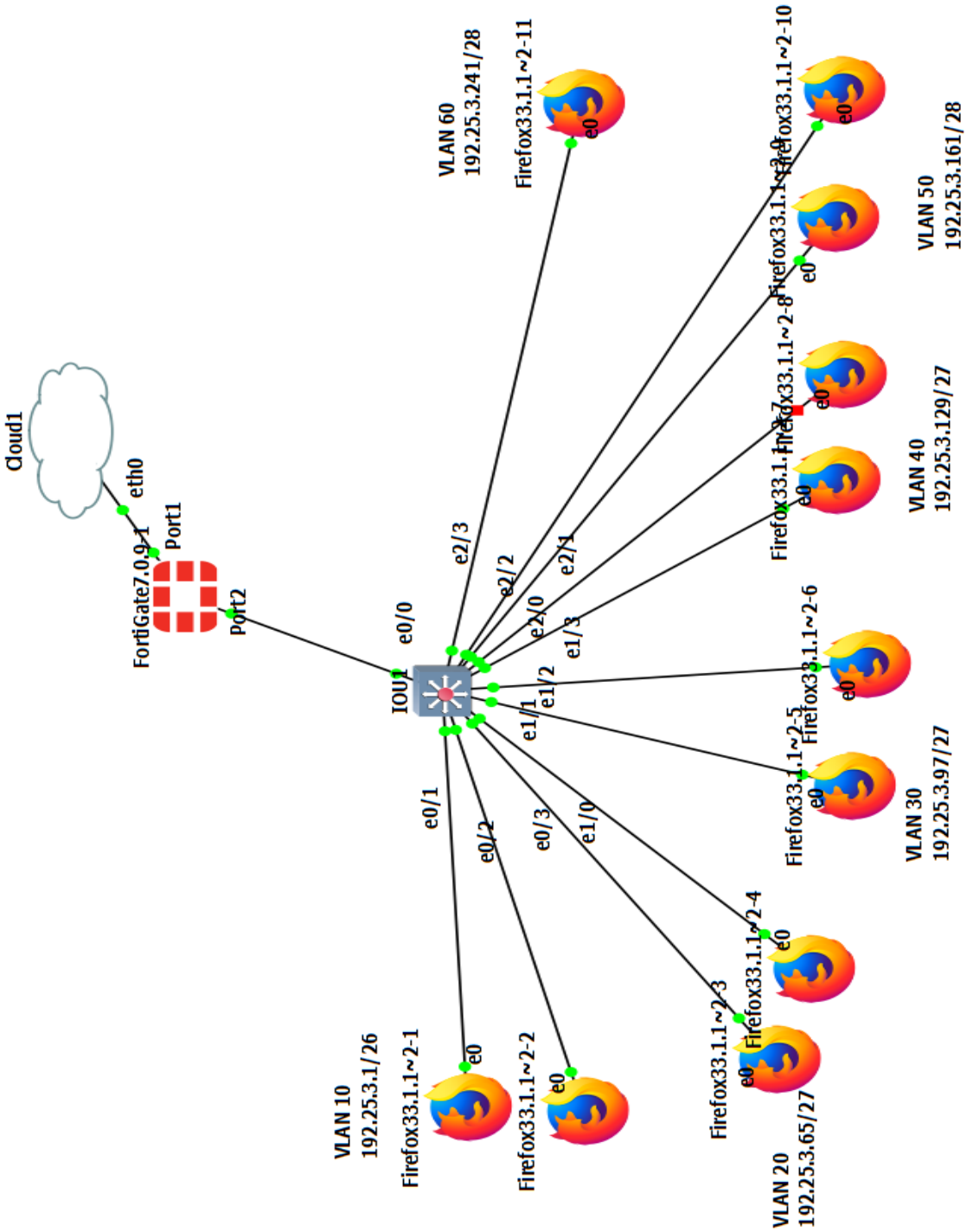


Figura III.1.58: Simulación en GNS3
Fuente: Elaboración propia

Creación de interfaces y VLANs

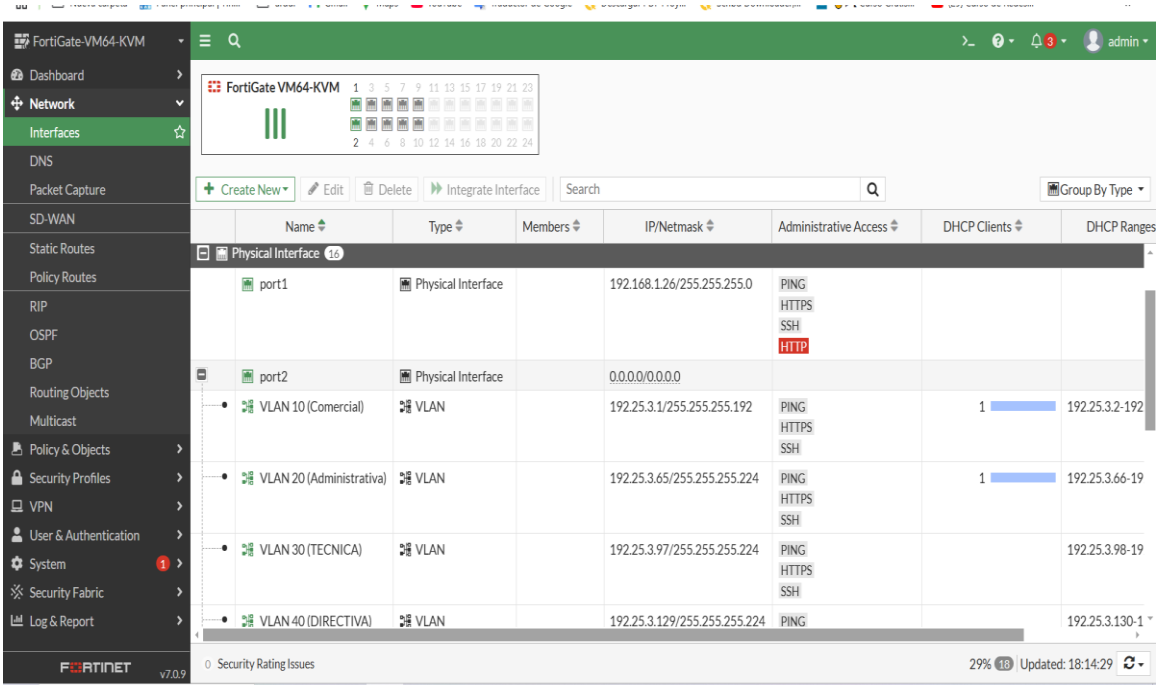


Figura III.1.59: Asignación de las interfaces a los puertos
Fuente: Elaboración propia

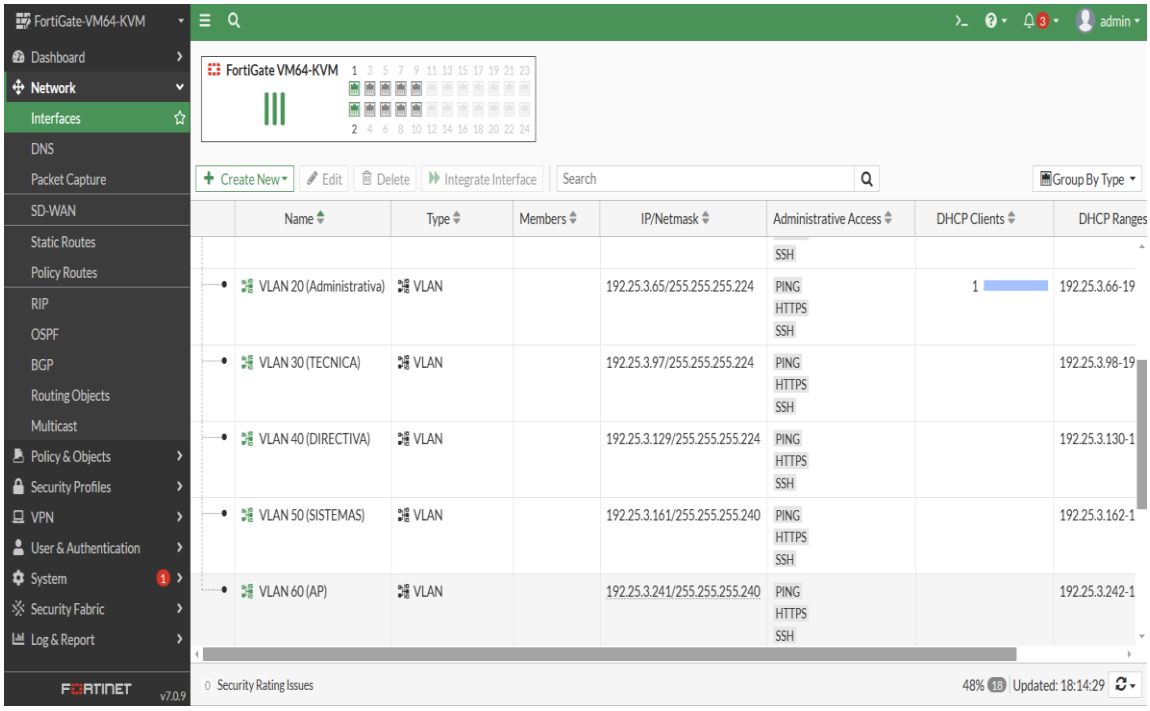


Figura III.1.60: Asignación de puertos
Fuente: Elaboración propia

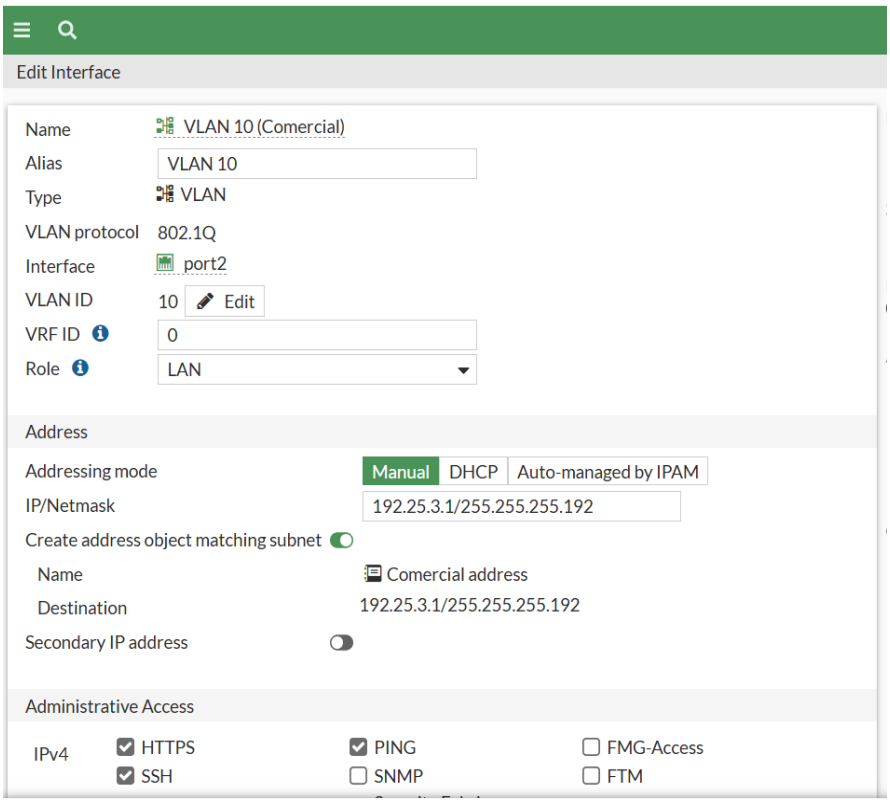


Figura III.1.61: Configuración de la VLAN 10
Fuente: Elaboración propia

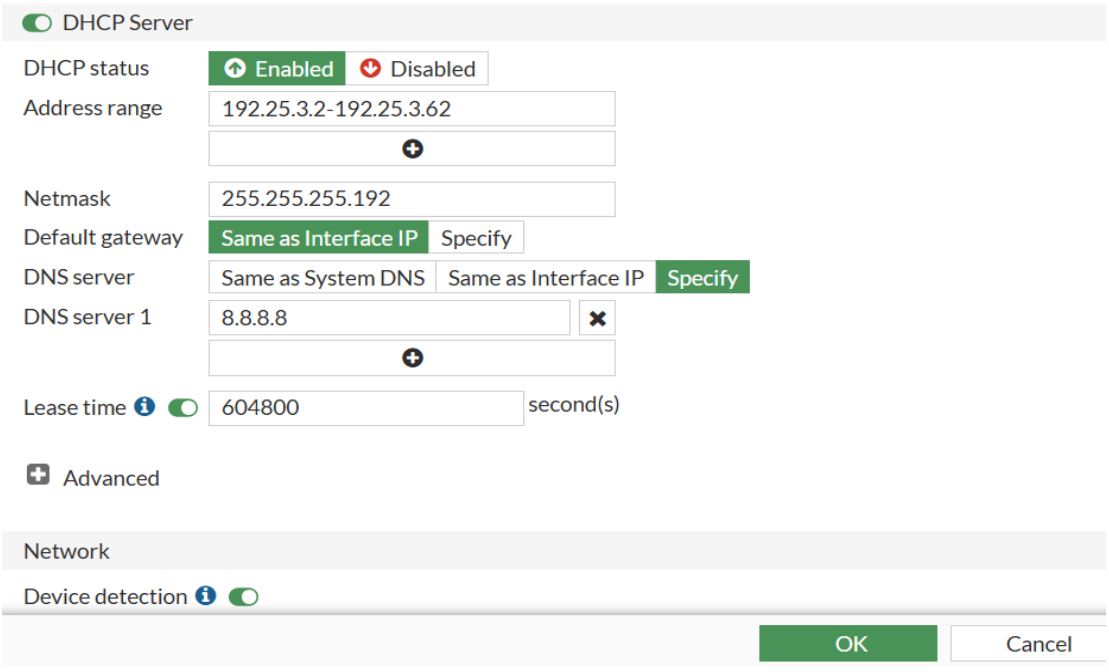


Figura III.1.62: Configuración del DHCP
Fuente: Elaboración propia

Creación de políticas de seguridad

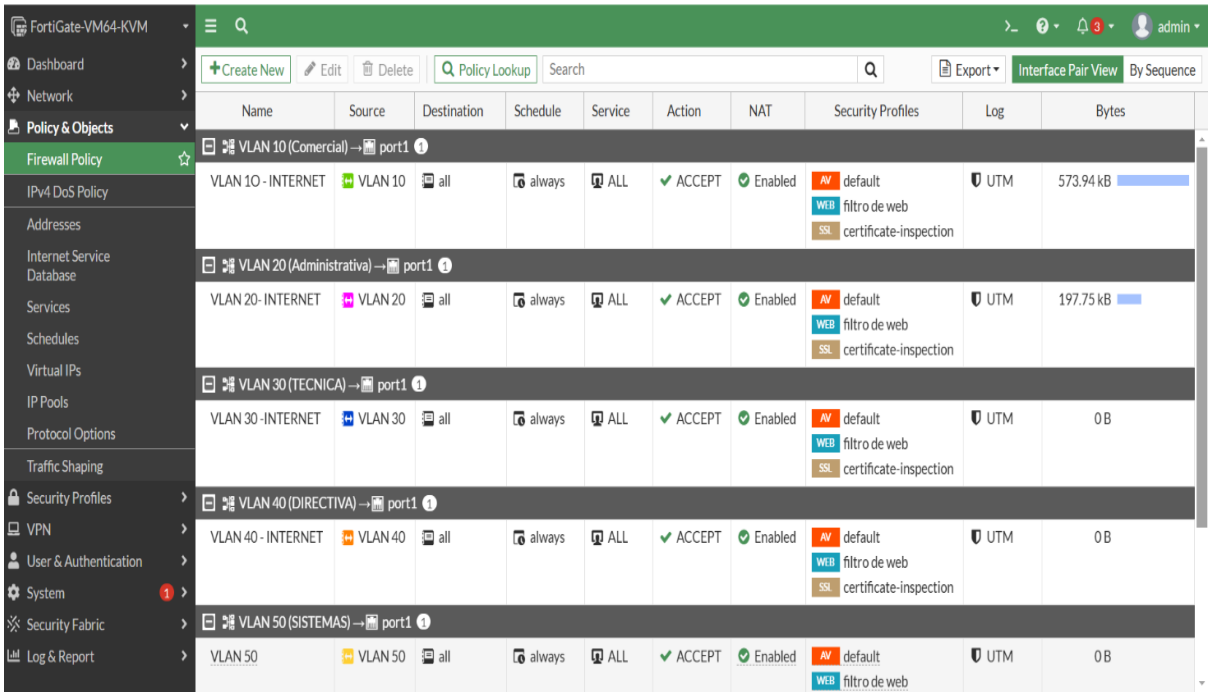


Figura III.1.63: Configuración de las políticas de seguridad (ACLs)
Fuente: Elaboración propia

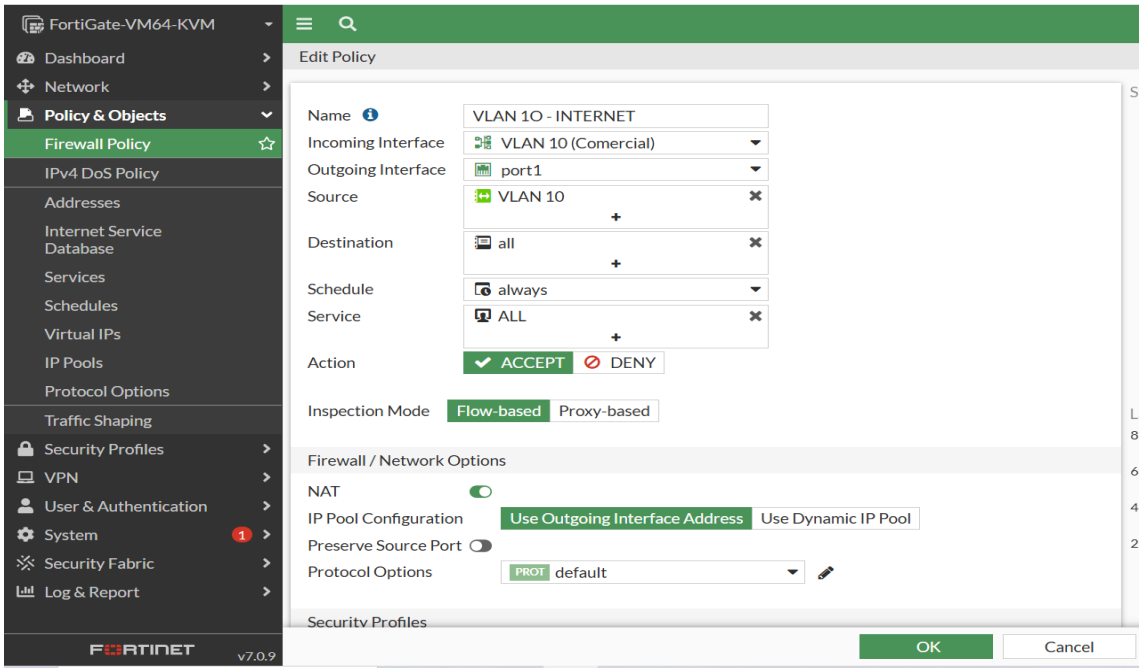


Figura III.1.64: Configuración de la política de seguridad para la VLAN 10
Fuente: Elaboración propia

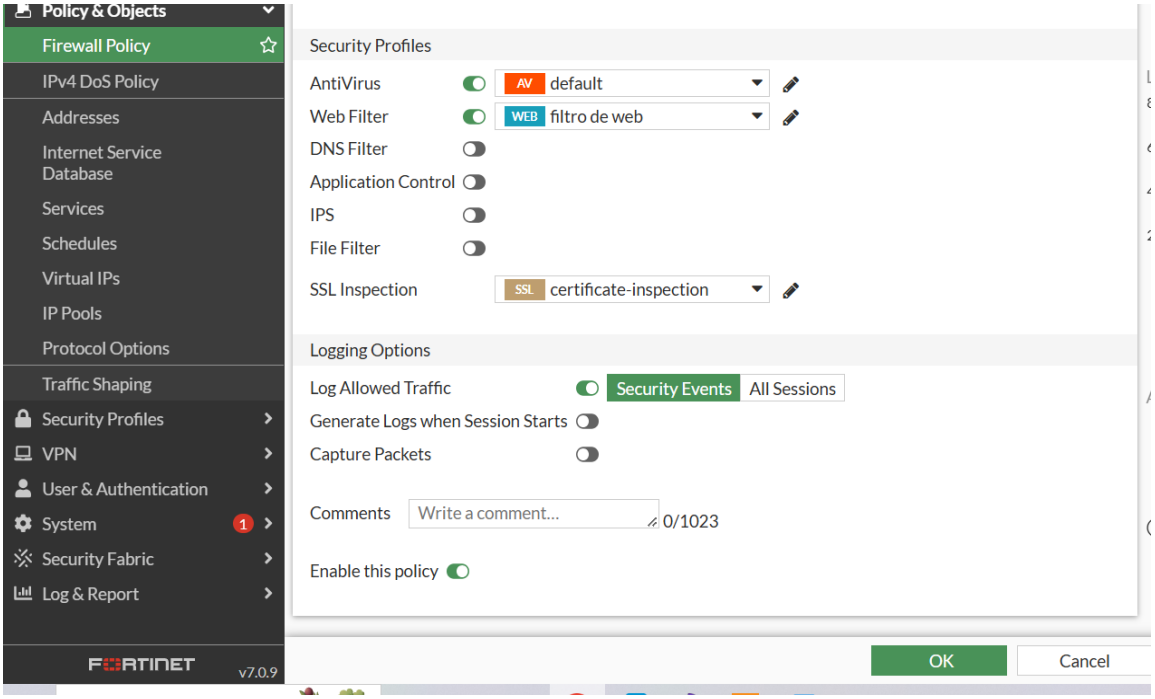


Figura III.1.65: Configuración de la política de seguridad para la VLAN 10 para la web
Fuente: Elaboración propia

III.2. Componente 2: Propuesta técnica de red documentada, validada y presentada ante las autoridades de COSAALT.

III.2.1. Introducción

El segundo componente del proyecto tiene como propósito la elaboración y presentación de una propuesta técnica detallada para la implementación de una nueva infraestructura de red en Cosaalt, una organización que busca modernizar su tecnología para responder a las demandas actuales y futuras. Este componente incluye una descripción técnica de los diseños, especificaciones y análisis realizados.

El problema que presenta la Cooperativa de agua y alcantarillado “Cosaalt”, es que no cuenta con una buena arquitectura de red y con equipos adecuados para ello, lo cual no permite la

comunicación óptima entre los usuarios de la red. Esto trae inconvenientes al instante del crecimiento tecnológico. La infraestructura existente se caracteriza por:

- Conexiones inestables debido a la falta de capacidad en los switches de piso.
- Una asignación manual de direcciones IP que aumenta la probabilidad de errores.
- Limitada cobertura inalámbrica en algunos pisos.
- Ausencia de medidas de redundancia que garanticen la alta disponibilidad.

III.2.2. Justificación técnica y organizacional

La presentación formal de la propuesta de red a los responsables de TI y a la gerencia general de COSAALT se justifica tanto desde una perspectiva técnica como organizacional.

Desde el punto de vista técnico, la red actual presenta limitaciones que afectan su rendimiento, seguridad y escalabilidad. A través del análisis realizado en la fase de diagnóstico, se identificaron problemas como la asignación manual de direcciones IP, falta de segmentación por VLANs, conexiones inalámbricas inestables en pisos con saturación de puertos, y la inexistencia de mecanismos de redundancia. Por estas razones, la validación de la nueva arquitectura propuesta por el personal encargado permite asegurar que las soluciones planteadas (VLANs, enrutamiento por subinterfaces, HSRP, protocolos de switching, entre otros) se alineen con la realidad operativa y técnica de la institución.

En términos organizacionales, la participación activa del personal técnico y de la gerencia general es esencial para garantizar la aceptación institucional de la propuesta, su viabilidad en una futura implementación, y el compromiso con los procesos de mejora tecnológica. La socialización también permite obtener retroalimentación directa de quienes administran o hacen uso de la red, enriqueciendo el diseño final mediante aportes prácticos y realistas.

III.2.3. Análisis de necesidades

Tras una exhaustiva evaluación, se identificó las necesidades actuales de la red y he identificado áreas clave que requieren atención. Estos incluyen la demanda creciente de ancho de banda, la necesidad de una mayor seguridad cibernética.

- Crecimiento no planificado y falta de documentación
- Incumplimiento de la norma ANSI/TIA 942 para cableado físico
- Desorganización y condiciones del cuarto del MDF
- Problemas de conectividad y velocidad de internet
- Uso inalámbrico ineficiente para equipos de trabajo fijo
- Falta de filtrado de paquetes en el firewall
- Diseño de red no adaptado a necesidades y falta de escalabilidad

III.2.4. Objetivo General

Presentar la propuesta de red de datos a los encargados de TI de manera clara y detallada, asegurando su comprensión y aceptación para la implementación y gestión futura de la infraestructura

III.2.4.1. Objetivos específicos

- Explicar la estructura lógica y física de la red, incluyendo la asignación de VLANs, configuraciones de routers y switches, y la integración de dispositivos existentes.
- Asegurar que el personal técnico entienda los beneficios a corto y largo plazo de la propuesta.
- Diseñar una propuesta de red escalable, eficiente y segura.

III.2.5. Metodología

La elaboración de esta propuesta se basó en la metodología Top-Down, partiendo de las necesidades organizacionales hacia la definición técnica de la red. Para ello:

- Se utilizaron simuladores como Cisco Packet Tracer para modelar la red lógica y validar su funcionalidad.
- Se complementó con diagramas tridimensionales en herramientas como SketchUp para ilustrar el diseño físico.
- Se incluyeron análisis técnicos que identificaron problemas clave y las soluciones propuestas para resolverlos.

III.2.6. Actividades desarrolladas

1.Elaboración de la propuesta técnica documentada:

Se estructuró un documento formal que incluye el análisis de la red actual, el diseño lógico y físico propuesto, la segmentación mediante VLANs, el direccionamiento IP planificado, la aplicación de protocolos de redundancia (HSRP), agregación de enlaces (EtherChannel), así como estrategias de seguridad, administración y escalabilidad de la red.

2.Simulación técnica en Packet Tracer y GNS3:

La propuesta fue validada mediante simulación en los entornos de Cisco Packet Tracer y GNS3. En Packet Tracer se modeló la estructura de red interna, configurando los routers, switches, VLANs, servidores y dispositivos finales. En GNS3 se simularon elementos adicionales como el firewall, la nube ISP y servicios como NAT y DNS para probar salida a Internet y accesos externos controlados.

3.Desarrollo del manual de configuración:

Se redactó un manual técnico que contiene paso a paso todas las configuraciones necesarias de routers, switches y servidores, incluyendo comandos, topologías, y criterios de verificación, con el fin de facilitar la implementación futura de la red.

4.Presentación de la propuesta al personal de COSAALT:

Se llevó a cabo la exposición del diseño técnico ante el personal responsable del área de TI y la gerencia general. Durante esta presentación se explicó la justificación del rediseño, las mejoras técnicas propuestas, los resultados de las simulaciones, y los beneficios esperados para la institución.

5.Obtención de retroalimentación y validación:

Como resultado de la exposición, se obtuvo retroalimentación positiva, incluyendo observaciones y sugerencias, las cuales fueron consideradas para fortalecer aún más la propuesta. Finalmente, se entregó una carta de conformidad firmada por el Gerente General, validando la calidad y pertinencia técnica del diseño.

III.2.7. Presentación de la propuesta

III.2.7.1. Detalles de la explicación

La propuesta fue explicada a los responsables técnicos de Cosaalt mediante un enfoque didáctico, abarcando los siguientes puntos clave:

Diseño físico de la red:

- Se presentó un plano a escala que ilustra la ubicación de los MDF e IDFs, los trayectos de cableado horizontal y vertical, así como la posición de los equipos.
- Se incluyó un cálculo detallado del cableado necesario en base al diseño propuesto, priorizando el uso de cables Cat 6 y fibra óptica.

Diseño lógico de la red:

- Se detallaron las VLANs recomendadas y su asignación de ancho de banda en función de las necesidades de cada área.
- Se presentó una simulación funcional del tráfico segmentado para demostrar la eficacia de la propuesta en la mejora de la conectividad y la reducción de colisiones.

Recursos y equipamiento:

- Se describieron las características de los equipos sugeridos, incluyendo switches gestionables, routers y servidores, asegurando su compatibilidad con los requerimientos actuales y futuros.
- Se propusieron configuraciones específicas para garantizar la seguridad y la redundancia.

III.2.7.2. Métodos de Presentación

Para garantizar una comprensión clara y detallada de la propuesta, se emplearon:

Diagramas interactivos generados en herramientas de diseño en 3D.

Documentos técnicos con especificaciones detalladas, destacando los beneficios esperados.

Simulaciones prácticas realizadas en Cisco Packet Tracer, evidenciando los resultados esperados en términos de conectividad y rendimiento.

III.2.7.3. Protocolos y Tecnologías Seleccionadas

Se describirán los principales protocolos de switching (RSTP, LACP) y routing (HSRP, Router-on-a-Stick) implementados, detallando cómo estos optimizan la conectividad y mejoran la redundancia.

III.2.7.4. Estrategias de Seguridad y Administración

- Configuración del firewall para proteger la red contra accesos no autorizados.

- Implementación de políticas de seguridad mediante ACLs y segmentación de VLANs.
- Monitoreo proactivo utilizando herramientas de administración centralizadas para prevenir problemas.

III.2.8. Beneficios de la propuesta

Estabilidad y rendimiento:

Segmentación de la red mediante VLANs que optimiza el uso del ancho de banda y mejora la estabilidad de las conexiones.

Uso de enlaces redundantes y protocolos de switching avanzados para garantizar alta disponibilidad.

Automatización y simplicidad:

Implementación de DHCP para asignación automática de direcciones IP, reduciendo errores administrativos.

Mayor cobertura:

Incorporación de puntos de acceso estratégicamente ubicados para garantizar señal estable en todas las áreas del edificio.

Seguridad mejorada:

Las estrategias propuestas minimizarán riesgos de intrusión y protegerán los datos sensibles.

Escalabilidad:

Diseño adaptable para integrar sistemas futuros, como SCADA y medidores inteligentes, sin necesidad de reemplazar equipos.

III.2.9. Conclusión

El éxito de la red dependerá de la correcta comprensión y adopción por parte del equipo técnico.

Esta propuesta no solo soluciona los problemas actuales, sino que también establece una base sólida para el crecimiento tecnológico futuro de Cosaalt y optimizando sus procesos.

La participación del personal de TI y la gerencia permitió reforzar la pertinencia del rediseño, garantizar su aplicabilidad real y asegurar el compromiso institucional. La documentación técnica elaborada, así como la simulación detallada de la red, aportan un valor significativo como productos concretos del proyecto.

CAPÍTULO IV:

CONCLUSIONES Y RECOMENDACIONES

IV.1. Conclusiones

La falta de una correcta estructuración, planificación en la red de datos son los primordiales motivos que justifican la elaboración de este proyecto, para superar estas falencias, se realizó el rediseño usando la tecnología Top-Down.

La implementación de DHCP en el router ayuda a administrar y automatizar el proceso de asignación de IPs hacia los equipos de la red local.

La información que se obtuvo de algunos trabajadores ayudo de gran manera para comprobar que Cosaalt tenía distintos problemas en cuanto a la red de datos, tales como, escasez de seguridad en la conexión a internet, mal servicio de red inalámbrico, falta de etiquetado en los servidores y switch de cada piso.

Mediante la segmentación de VLANs de una misma subred se logra evitar que el tráfico dentro de Cosaalt se congestione. Además, ayuda a administrar la red agrupándola por áreas.

Actualizar los puntos de acceso inalámbrico y ubicarlos estratégicamente en las instalaciones resuelve los problemas de cobertura y garantiza una conexión estable para todos los trabajadores.

Diseñar la red pensando en el futuro permitirá a cosaalt incorporar sistemas avanzados como SCADA y medidores inteligentes, asegurando que la red se adapte a las necesidades tecnológicas en crecimiento.

IV.2. Recomendaciones

Para garantizar el buen funcionamiento de la red se debe mejorar o reubicar la infraestructura en la que se encuentra el MDF, debido a que no se encuentra en buenas condiciones y no cuanta con la seguridad necesaria.

Se recomienda que los encargados del TI participen en capacitaciones periódicas para informarse de tecnologías emergentes y tener un buen uso de la red de datos y el mini data center, para evitar inconvenientes.

Se recomienda mantener la documentación actualizada de cada cambio o aumento de equipos realizados en la red, para evitar confusiones, cableado de red innecesario y sobre todo para evitar el retraso reparaciones en la red.

Reemplazar cables antiguos y organizar el cableado nuevamente facilitará el mantenimiento y reducirá problemas de conexión.

Invertir en switches y routers modernos con capacidades avanzadas asegura el soporte para las nuevas demandas de la red.