Universidad Nacional Autónoma de México

Facultad de Ingeniería

Administración de Redes

Proyecto Final

Profesor: Ing. Juan José García Romero

Grupo: 01

Integrantes:

- Bote Sánchez Cristian
- Jimenez Cervantes Angel Mauricio
- Reyes Romero Luis Fernando

Semestre: 2025-2
Fecha de entrega: 13 - Mayo - 2025

1. Introducción

En el contexto tecnológico actual, las organizaciones enfrentan una transformación constante en sus formas de trabajo. La digitalización, el trabajo remoto, la movilidad laboral y la necesidad de colaboración en tiempo real han elevado las exigencias sobre las infraestructuras de red. Las oficinas modernas ya no son entornos estáticos: requieren redes dinámicas que se adapten con rapidez, seguridad y eficiencia a las necesidades cambiantes de sus usuarios.

Las redes híbridas, que integran tecnologías cableadas e inalámbricas, han surgido como la solución ideal para estos entornos. Su capacidad para ofrecer estabilidad en dispositivos fijos y flexibilidad en dispositivos móviles proporciona a las empresas una plataforma robusta, escalable y administrable.

De igual forma, el cumplimiento de normativas y estándares en el diseño e implementación del cableado estructurado es fundamental para garantizar el rendimiento, la seguridad y la escalabilidad de una red. Estas directrices, como las establecidas por la ANSI/TIA, ISO/IEC y otras entidades internacionales, definen criterios técnicos precisos sobre instalación, materiales, disposición de cables, conectores, etiquetado y pruebas de validación. Seguir estas normas no solo asegura una infraestructura organizada y profesional, sino que también facilita el mantenimiento, reduce interferencias, minimiza el riesgo de fallos y permite futuras actualizaciones sin necesidad de rehacer la instalación desde cero. En definitiva, respetar estos estándares es esencial para asegurar una red confiable, eficiente y alineada con las mejores prácticas de la industria.

Este documento presenta el diseño, implementación y documentación completa de una red híbrida en un entorno corporativo que abarca dos niveles de oficinas, contemplando conectividad cableada de alta velocidad, acceso inalámbrico seguro, segmentación por VLANs, telefonía IP, monitoreo de red, y una infraestructura física basada en normativas internacionales. El objetivo final es proporcionar una solución de conectividad integral, segura y preparada para el futuro.

2. Objetivo General

Diseñar e implementar una red híbrida (alámbrica e inalámbrica) que garantice conectividad continua, segura, estable y escalable para todos los usuarios y dispositivos distribuidos en las áreas laborales, ejecutivas, comunes y técnicas de la oficina corporativa. Se busca, además, facilitar la administración, mejorar la eficiencia operativa y permitir futuras ampliaciones sin rediseñar por completo la infraestructura.

3. Alcance del Proyecto

Este proyecto abarca:

- Análisis de necesidades de conectividad por área.
- Diseño lógico y físico de red.
- Instalación de cableado estructurado categoría 6 y 6A.
- Instalación de puntos de acceso inalámbrico de alto rendimiento.
- Segmentación de la red mediante VLANs.
- Instalación y configuración de dispositivos activos (switches, routers, servidor, UPS).
- Incorporación de telefonía IP con QoS y VLAN dedicada.
- Implementación de mecanismos de seguridad física y lógica.
- Documentación técnica detallada, incluyendo planos, etiquetas, y procedimientos de mantenimiento.

No se incluyen actividades de mantenimiento futuro ni integración con sistemas de terceros externos al entorno de red implementado.

4. Requerimientos del Cliente

Este apartado detalla los requerimientos específicos proporcionados por el cliente en cuanto al diseño e implementación de la red híbrida. Estos requerimientos se dividen en funcionales y no funcionales, abarcando aspectos relacionados con la conectividad

cableada e inalámbrica, seguridad, administración, escalabilidad, tiempos de entrega, normatividad y apariencia física de la instalación. Cada uno de estos elementos es esencial para garantizar que la solución tecnológica propuesta cumpla con las expectativas operativas, técnicas y organizacionales del entorno corporativo.

4.1 Requerimientos Funcionales

Los requerimientos funcionales definen las características y capacidades que debe tener la red para asegurar un funcionamiento eficaz y adaptado a las necesidades del cliente. Se incluyen especificaciones detalladas para la red cableada e inalámbrica, así como medidas de seguridad, herramientas de administración y lineamientos de escalabilidad. Estos requisitos permiten diseñar una infraestructura robusta, segura y preparada para soportar la carga actual y futura de dispositivos y servicios.

Red Cableada

La red cableada será la base de la infraestructura de conectividad del edificio, proporcionando conexiones estables y de alto rendimiento para los puestos de trabajo, impresoras multifuncionales y equipos críticos. Se establece que cada escritorio debe contar con al menos un puerto RJ-45 activo, gestionado desde switches administrables para permitir control y segmentación de tráfico. Además, los servidores estarán ubicados en una VLAN protegida con acceso limitado al personal autorizado, lo que refuerza la seguridad y la eficiencia operativa de la red.

Red Inalámbrica

Para garantizar movilidad y conectividad total en el entorno laboral, se requiere cobertura inalámbrica integral en todas las áreas del edificio, incluyendo oficinas, salas comunes y zonas de tránsito. Se especifica una velocidad mínima garantizada por punto de acceso y la segmentación en dos redes: una empresarial, segura y priorizada, y otra para invitados, aislada de los recursos internos. Esto permitirá una experiencia de usuario fluida sin comprometer la seguridad de la red principal. Por ello, se van a cubrir los siguientes puntos:

- Se requiere **cobertura WiFi completa** en todas las áreas: oficinas privadas, salas de juntas, áreas comunes, sanitarios y recepción.
- La capacidad mínima por punto de acceso será de **150 Mbps reales** para permitir la conexión simultánea de múltiples dispositivos.
- Se deben configurar dos redes inalámbricas:
    - **Red empresarial**: con autenticación WPA3, acceso a recursos internos y tráfico priorizado.
    - **Red de invitados**: aislada del resto de la red, con acceso exclusivo a internet.

Seguridad

La seguridad de la red es un pilar fundamental en el diseño solicitado. Se implementarán mecanismos como filtrado por dirección MAC, segmentación mediante VLANs, políticas de acceso restringido y configuración avanzada del router con firewall, NAT y registros de actividad. Estas medidas están orientadas a proteger la infraestructura contra accesos no autorizados, amenazas internas y externas, y garantizar la integridad de los datos y servicios.

Administración

La red debe ser completamente administrable de forma remota para facilitar el mantenimiento proactivo y la respuesta ante incidencias. Se exige la integración de herramientas de monitoreo como Zabbix o PRTG, capaces de generar alertas automáticas y brindar visibilidad del estado de la red. Además, se requiere un documento de respaldo con contraseñas, configuraciones y diagramas que permita una gestión organizada y profesional de la infraestructura.

Escalabilidad

La solución debe estar preparada para el crecimiento futuro sin necesidad de rediseñar su estructura. Se especifica que la red debe ser capaz de admitir al menos 20 dispositivos adicionales, y debe contemplarse un plan de expansión documentado para una posible ampliación física del edificio, como la inclusión de un tercer piso o puntos

de acceso adicionales. Esta previsión asegura que la inversión en infraestructura sea sostenible a largo plazo.

4.2 Requerimientos No Funcionales

Los requerimientos no funcionales establecen condiciones clave para la entrega, operación y presentación de la red, que no están directamente relacionadas con funciones técnicas pero son igualmente críticas para el éxito del proyecto. Se incluye un plazo máximo de implementación de 30 días hábiles, una disponibilidad operativa del 99.9%, y criterios estéticos que aseguren una instalación profesional y visualmente ordenada. Además, se exige cumplimiento estricto de normativas internacionales y nacionales, lo cual respalda la calidad, seguridad y compatibilidad de la solución implementada.

5. Justificación Técnica y Normativa

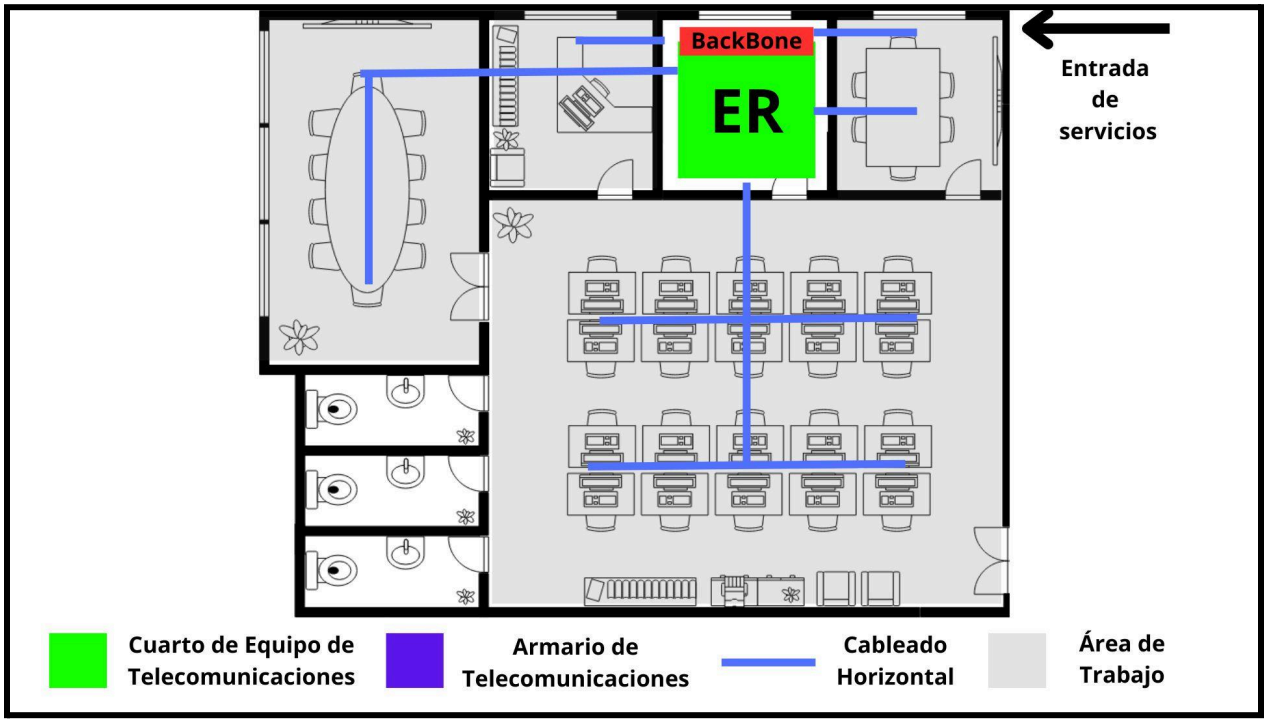
El uso de cableado estructurado basado en normas TIA/EIA-568 e ISO/IEC 11801 asegura una infraestructura robusta, organizada y con alta capacidad de crecimiento. Se identificaron e implementaron los **subsistemas clave** del cableado:

- ***Entrada de servicios:*** Es el punto donde los servicios externos de telecomunicaciones (como Internet, telefonía o redes privadas) ingresan al edificio desde el proveedor. Facilita la transición entre la red del proveedor y la infraestructura interna del cliente. Garantiza una conexión segura y ordenada con las redes externas, permitiendo la integración de servicios fundamentales para la operación del negocio.
- ***Cuarto de telecomunicaciones:*** Es el espacio principal donde se centraliza la gestión de la red, alojando equipos como switches, servidores, UPS, racks y sistemas de monitoreo. Actúa como el núcleo de la infraestructura de red, desde donde se distribuyen las conexiones hacia el resto del edificio. Su correcta organización y condiciones ambientales aseguran el rendimiento continuo y la seguridad de los equipos críticos de la red.

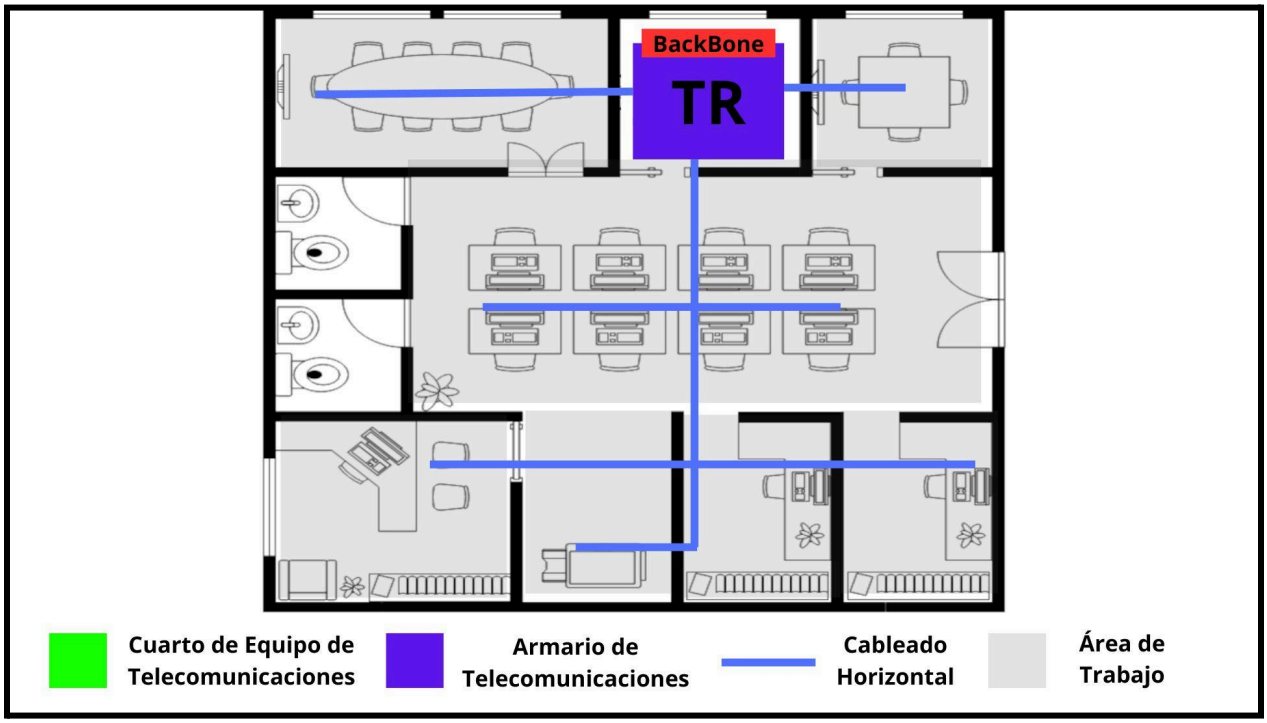
- ***Armarios de telecomunicaciones:*** Son cuartos secundarios ubicados en cada piso del edificio que albergan equipos de red intermedios (como switches de acceso y patch panels). Distribuyen el cableado hacia las áreas de trabajo dentro de cada nivel del edificio. Además, permiten una estructura modular y organizada, facilitando el mantenimiento, escalabilidad y control por zonas.
- ***Cableado Backbone:*** Es el cableado principal que interconecta los cuartos de telecomunicaciones, típicamente usando fibra óptica o cable UTP de alta categoría. Transporta datos a alta velocidad entre los distintos niveles de red, desde la entrada de servicios hasta los armarios de piso. Su rendimiento y capacidad son fundamentales para asegurar una transmisión rápida y confiable entre las distintas partes de la red.
- ***Cableado Horizontal:*** Es el cableado que va desde los armarios de telecomunicaciones hasta las áreas de trabajo, usualmente utilizando cables UTP categoría 6 o superior. Proporciona conectividad directa a los usuarios finales. De igual forma, es la base para que cada dispositivo en el área de trabajo tenga acceso a la red con calidad y sin interferencias.
- ***Áreas de trabajo:*** Son los puntos donde los usuarios se conectan a la red mediante dispositivos como computadoras, teléfonos IP, impresoras, entre otros. Facilita la interacción del usuario con los servicios de red. Una conexión confiable en estas áreas garantiza la productividad del personal y el funcionamiento continuo de las operaciones.

Con base en lo anterior, es fundamental identificar cada uno de los subsistemas de la red, ya que esto permite ubicar su posición dentro de la infraestructura y facilita su correcta implementación, cumpliendo con todas las normativas aplicables al cableado estructurado. Los subsistemas considerados para nuestros planos son:

Subsistemas para el piso 1



Subsistemas para el piso 2



Por otra parte, la normatividad en redes se refiere al conjunto de estándares, lineamientos y buenas prácticas establecidos por organismos internacionales como ANSI/TIA, ISO/IEC e IEEE, los cuales regulan el diseño, instalación, operación y mantenimiento de infraestructuras de telecomunicaciones. Su propósito principal es asegurar que las redes sean seguras, eficientes, interoperables y escalables, independientemente del fabricante o proveedor. Cumplir con estas normativas garantiza un rendimiento óptimo, reduce fallas, facilita el diagnóstico de problemas y permite que la red pueda adaptarse fácilmente a futuras actualizaciones tecnológicas. Además, proporciona una base sólida para la compatibilidad entre equipos y asegura que la infraestructura esté alineada con las expectativas y necesidades del entorno corporativo actual.

Dicho lo anterior, En este proyecto de cableado estructurado podemos observar que las normas y estándares que se deben de cumplir son los siguientes:

- ***ANSI/TIA-568 (Estándares de Cableado para Edificios Comerciales):*** Define los requisitos para el diseño e instalación de sistemas de cableado estructurado para edificios comerciales y data centers.
- ***ISO/IEC 11801:*** Especifica los estándares internacionales para cableado de telecomunicaciones dentro de edificios comerciales.
- ***ANSI/TIA-569 (Estándar de Edificios Comerciales para Recorridos y Espacios de Telecomunicaciones):*** Establece las pautas para los espacios y las rutas de telecomunicaciones en edificios comerciales.
- ***ANSI/TIA-606A (Normas de Administración de Infraestructura de Telecomunicaciones en Edificios Comerciales):*** Establece las prácticas para la administración y documentación de la infraestructura de telecomunicaciones en edificios comerciales. Incluye normas para el etiquetado de cables, paneles, gestión de registro y la planificación del cableado.
- ***ANSI/TIA-607 (Requisitos de Puesta a Tierra y Conexionado de Sistemas de Telecomunicaciones en Edificios Comerciales):*** Este estándar establece los lineamientos para el sistema de puesta a tierra y conexión equipotencial de los sistemas de telecomunicaciones, incluyendo bastidores, racks, cableado y

demás componentes metálicos. Su objetivo es proteger tanto al personal como a los equipos frente a descargas eléctricas, interferencias electromagnéticas (EMI) y sobretensiones, lo cual es vital para garantizar la seguridad, el rendimiento y la durabilidad de la infraestructura de red.

- ***ISO/IEC 14763-2:*** Describe los requisitos para la instalación y pruebas del cableado estructurado.
- ***ISO 27001:*** Relacionado con la seguridad de la información en las infraestructuras de red.

Normas para la configuración de la red:

- ***IEEE 802.3 (Ethernet):*** Define las tecnologías de red Ethernet, asegurando la compatibilidad entre otros dispositivos para la transmisión de datos por cable.
- ***IEEE 802.11 (Wi-Fi):*** Establece estándares para redes inalámbricas, garantizando una interoperabilidad entre dispositivos como Access Points y clientes.
- ***RFC 2131 (Protocolo DHCP):*** Especifica cómo se asignan direcciones IP dinámicamente, lo que es esencial para configurar un servidor DHCP que administre eficientemente las direcciones de red.
- ***RFC 1034 y RFC 1035 (DNS):*** Definen cómo funciona el sistema de nombres de dominio (DNS), clave para la resolución de nombres en la red.
- ***RFC 5424:*** Define la estructura, severidad y niveles del protocolo Syslog, utilizado para el envío de mensajes de registro desde dispositivos a un servidor central.
- ***SIP (Session Initiation Protocol – RFC 3261):*** Protocolo ampliamente utilizado para establecer, modificar y finalizar sesiones multimedia como llamadas VoIP.
- ***RTP (Real-time Transport Protocol – RFC 3550):*** Protocolo para la transmisión de audio y video en tiempo real sobre IP.
- ***RFC 959:*** Define el protocolo FTP estándar para transferencia de archivos.
- ***RFC 2228:*** Extensiones de seguridad para FTP (como FTP Secure o FTPS).
- ***SMTP (Simple Mail Transfer Protocol – RFC 5321):*** Para envío de correos.

- ***IMAP (Internet Message Access Protocol – RFC 3501):*** Para acceso a correos desde el servidor.
- ***POP3 (Post Office Protocol v3 – RFC 1939):*** Para descarga de correos al cliente.
- ***MIME (Multipurpose Internet Mail Extensions – RFCs 2045–2049):*** Para el envío de contenido multimedia por correo.

Como podemos observar los beneficios específicos al usar estás normas y estándares en un proyecto de cableado estructurado nos asegura que los componentes del sistema, como switches, cables y Access Points, funcionen correctamente entre sí. De igual forma, estándares como TIA/EIA-568 nos garantizan que el cableado estructurado soporte las velocidades necesarias de acuerdo a las necesidades del cliente.

Por otra parte, normas como ISO/IEC 27001 y 802.1X nos aseguran que los datos y accesos a la red estén protegidos. Asimismo, el uso de estos estándares nos ayudan a la facilitación de futuras expansiones sin necesidad de rediseñar toda la red. Además, de evitar problemas legales, debido a que estamos cumpliendo con normativas nacionales e internacionales.

6. Diseño General de la Red

La red se estructura bajo el modelo jerárquico de tres capas:

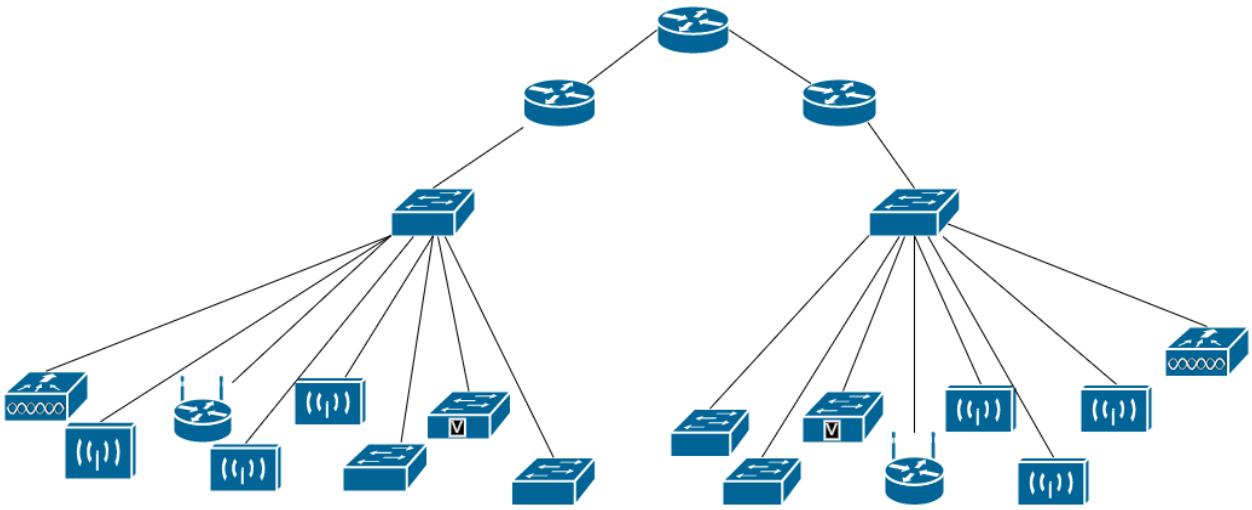
- **Capa de acceso**: Conecta los dispositivos finales a switches de acceso.
- **Capa de distribución**: Conecta las distintas VLANs y gestiona políticas.
- **Capa de núcleo**: Enlace troncales entre pisos y red de backbone.

Además, se implementó **EIGRP** para un enrutamiento dinámico eficiente, lo que permite una rápida convergencia, control granular del tráfico y mejor escalabilidad.

El diseño de la red se considera óptimo porque sigue el modelo jerárquico de tres capas, una arquitectura ampliamente reconocida por su eficiencia, escalabilidad y facilidad de administración. La capa de acceso permite la conexión directa de los

dispositivos finales mediante switches, facilitando la gestión local y el control de acceso. La capa de distribución actúa como un punto de agregación para las VLANs, permitiendo aplicar políticas de seguridad, control de tráfico y segmentación lógica de la red, lo que mejora tanto el rendimiento como la seguridad. Por último, la capa de núcleo proporciona conectividad troncal de alta velocidad entre los distintos pisos del edificio, funcionando como columna vertebral de la red y garantizando una comunicación rápida y confiable entre todas las áreas. Complementando esta estructura, la implementación del protocolo EIGRP (Enhanced Interior Gateway Routing Protocol) permite un enrutamiento dinámico altamente eficiente, con tiempos de convergencia reducidos, control granular del tráfico y una gran capacidad de adaptación a cambios en la topología de red. Esta combinación de diseño estructurado y protocolo de enrutamiento avanzado asegura una red robusta, flexible y preparada para el crecimiento futuro.

A Continuación se muestra la topología diseñada.



7. Componentes Principales

Componente	Detalles Técnicos

Cableado estructurado	Categoría 6/6A, patch panels RJ-45, organizadores y canalización etiquetada
Switches	Switches Cisco Catalyst de la serie 9300
PBX	JMV de RingCentral o 3cx
Router principal	Catalyst de la serie 8300-1N1S-6T
Servidores	DNS, DHCP, VoIP, Syslog, NTP, FTP, correo electrónico
UPS	Tripp Lite 1000VA para respaldo eléctrico
Puntos de acceso (APs)	Cisco Aironet 4800 Series Access Points y Router Wi-Fi* 6 AX3000 2,4 GHz y 5 GHz
Software de monitoreo	Zabbix para alerta, control y visualización de tráfico Cisco Meraki para una gestión más sencilla.
Aire acondicionado	Tipo mini-split, con capacidad para mantener temperatura del SITE

Computadoras	Lenovo ThinkCentre M70s Gen 5 (Intel) SFF
Teléfonos	Teléfono IP Cisco serie 8800

8. Red Inalámbrica y Cableada

La red implementada combina infraestructura cableada e inalámbrica para ofrecer una conectividad integral, segura y eficiente en todo el entorno corporativo. Cada estación de trabajo cuenta con al menos un puerto RJ-45 activo conectado a switches administrables, asegurando un rendimiento constante y baja latencia para tareas críticas. Adicionalmente, se ha garantizado cobertura WiFi completa en todos los espacios del edificio, incluyendo oficinas, salas de juntas, áreas comunes y zonas de tránsito. Para optimizar el uso y seguridad de la red, se implementaron dos redes inalámbricas diferenciadas por piso: una red empresarial con acceso a los recursos internos y altos estándares de seguridad, y una red de invitados aislada, exclusivamente para acceso a internet. Como se mencionó anteriormente, se instalaron dos redes inalámbricas por piso:

- **Red empresarial:** La segmentación de la red inalámbrica en dos entornos lógicos responde a una necesidad crítica de seguridad y control. La red empresarial está diseñada para uso interno del personal autorizado, con autenticación robusta bajo el estándar WPA 3, que ofrece protección contra ataques de diccionario y asegura la confidencialidad incluso en redes públicas. Esta red permite el acceso a recursos como servidores, impresoras, aplicaciones internas y servicios críticos, y su tráfico puede ser priorizado mediante QoS (Calidad de Servicio) para mantener la eficiencia operativa.
- **Red de invitados:** Está red se encuentra completamente aislada de la infraestructura interna y restringida únicamente al acceso a internet, evitando así cualquier posible punto de entrada a la red corporativa. Esta segmentación no

solo previene accesos no autorizados, sino que también protege la confidencialidad de la información y reduce la superficie de ataque en caso de dispositivos comprometidos conectados por visitantes o usuarios externos. Ambas redes operan en bandas 2.4 GHz y 5 GHz, garantizando compatibilidad y rendimiento según el tipo de dispositivo y la densidad de usuarios.

9. Servicios y Segmentación de Red

Para asegurar un control eficiente del tráfico, una administración segura de los recursos y una mejor calidad de servicio, la red ha sido diseñada con una segmentación lógica mediante VLANs (Redes de Área Local Virtual) y la implementación de servicios esenciales para el funcionamiento de una red empresarial moderna. Esta estructura permite aislar el tráfico según su función dentro de la organización, al mismo tiempo que se habilitan servicios clave como VoIP, correo electrónico, sincronización horaria y acceso remoto, todos pensados para mejorar la operatividad, el rendimiento y la seguridad de la red.

Segmentación por VLANs

El uso de VLANs (Virtual Local Area Networks) permite dividir una red física en varias redes lógicas, aislando el tráfico entre distintos grupos de usuarios y servicios, incluso cuando comparten el mismo hardware de red. Esta segmentación mejora significativamente la seguridad, al evitar que usuarios sin privilegios accedan a recursos sensibles, y optimiza el rendimiento de la red al reducir el dominio de broadcast. En el diseño implementado, cada VLAN se asignó a una función específica (usuarios comunes, salas de juntas, ejecutivos, VoIP, etc.), lo que facilita la gestión, permite aplicar políticas diferenciadas por tipo de dispositivo y asegura la calidad del servicio en aplicaciones sensibles como la telefonía IP.

VLANs por funcionalidad:

VLAN	Nombre	Función
10	Usuarios	Dispositivos comunes
20	Salas reuniones	Tráfico administrativo
30	Salas de conferencias	Trabajo colaborativo
40	Oficinas ejecutivas	Conexiones privilegiadas
50	VoIP	Segmentación y QoS para voz
99	Administración	Gestión, servidores, switches

Servicios configurados:

La red empresarial se complementa con una serie de servicios configurados que permiten cubrir las necesidades operativas clave de los usuarios y administradores

- **VoIP**: permite llamadas internas entre extensiones con calidad de voz asegurada gracias a la segmentación en VLAN y la aplicación de QoS. Como llamadas

entre extensiones (ej. 54001 a 64005) con calidad garantizada.

- **DNS y HTTPS**: Facilitan la navegación web con páginas personalizadas, útiles para pruebas o entornos educativos (ej. simulan Google y Facebook).

- **Correo electrónico**: El uso de este servicio permite la comunicación ágil entre empleados sin necesidad de servicios externos (ej. Mauricio, Fernando).

- **FTP**: Se emplea para el intercambio de archivos entre estaciones de trabajo y servidores (ej. AspectosProyecto.txt).

- **Syslog y NTP**: Donde, Syslog registra eventos importantes en la red, esencial para tareas de auditoría y diagnóstico, mientras que NTP mantiene sincronizados los relojes de los dispositivos, crucial para la trazabilidad y seguridad..

- **SSH/Telnet**: Permiten la administración remota de routers y switches, garantizando acceso seguro y centralizado a los equipos de red.

---

10. Seguridad y Buenas Prácticas

La seguridad de una red no solo depende de los dispositivos implementados, sino también de las políticas, configuraciones y prácticas que se aplican de forma proactiva para proteger la infraestructura contra accesos no autorizados, fallos operativos y amenazas internas o externas. En este proyecto se han incorporado medidas de seguridad a nivel lógico y físico para asegurar la integridad, confidencialidad y disponibilidad de la información y los servicios. Desde protocolos de acceso remoto seguros como SSH, hasta el uso de contraseñas cifradas, segmentación de red, y restricciones de acceso físico, cada elemento ha sido configurado conforme a buenas prácticas de ciberseguridad y gestión de redes.

Políticas de Administración

Las políticas de administración son un conjunto de normas, procedimientos y lineamientos diseñados para garantizar el uso adecuado, seguro y eficiente de los recursos tecnológicos dentro de una organización. Estas políticas permiten mantener la operatividad de la red, definir responsabilidades, estandarizar procesos, y facilitar tanto el mantenimiento como la escalabilidad de la infraestructura. Son fundamentales para prevenir malas prácticas, gestionar adecuadamente el presupuesto tecnológico, y asegurar que el sistema evolucione conforme a las necesidades del negocio, sin comprometer la seguridad ni el rendimiento.

Políticas Generales de Servicios

1. Todos los servicios implementados deben estar documentados con su configuración y responsables asignados.
2. Cada nuevo servicio debe pasar por una fase de pruebas antes de ser desplegado en producción.
3. Todos los servicios deben estar protegidos mediante autenticación y control de acceso.
4. Se debe realizar un respaldo semanal automático de servicios críticos como DNS, correo, FTP y VoIP.
5. La disponibilidad mínima de los servicios debe ser del 99.9% durante horas laborales.
6. Cualquier cambio o interrupción en un servicio debe ser notificado con al menos 24 horas de anticipación.
7. Los registros de eventos (logs) deben almacenarse al menos por 90 días.
8. Solo personal autorizado puede realizar configuraciones o actualizaciones sobre los servicios activos.
9. Cada servicio debe tener configurada su supervisión mediante herramientas como Zabbix o PRTG.
10. Los servicios inactivos o no utilizados deben ser dados de baja para evitar vulnerabilidades.

Políticas de Software

1. Todo software debe contar con licencia vigente y respaldo legal.
2. Se prohíbe el uso de software pirata o no autorizado dentro de la infraestructura de red.
3. El software debe mantenerse actualizado según las recomendaciones del proveedor.
4. Las actualizaciones deben realizarse fuera del horario laboral para evitar interrupciones.
5. Solo personal del área de TI puede instalar o desinstalar software en equipos críticos.
6. Se debe llevar un inventario actualizado de las versiones de software instaladas en cada equipo.
7. No se permite el uso de software de uso personal en equipos corporativos.
8. El antivirus y antimalware deben estar instalados y actualizados en todos los equipos conectados a la red.
9. El acceso a software administrativo o de gestión estará limitado a usuarios con roles definidos.
10. Las pruebas de software nuevo deben realizarse en un entorno aislado antes de su implementación general.

Políticas de Hardware

1. Cada componente de hardware debe registrarse en un inventario detallado (modelo, serie, ubicación).
2. La instalación o sustitución de hardware debe ser realizada únicamente por personal certificado.
3. Se debe realizar mantenimiento preventivo cada seis meses en servidores, switches y equipos críticos.
4. Todo equipo debe contar con etiquetas de identificación visibles y en buen estado.

5. Los equipos fuera de servicio deben almacenarse en un lugar seguro y etiquetarse como "Fuera de operación".
6. Los puertos de red no utilizados deben permanecer desactivados por seguridad.
7. El cableado estructurado debe cumplir con los estándares TIA/EIA y estar canalizado adecuadamente.
8. No se permite el uso de extensiones eléctricas caseras en equipos de red o servidores.
9. Se debe contar con respaldo energético (UPS) para los cuartos de telecomunicaciones.
10. El hardware obsoleto debe ser reemplazado según los ciclos de vida definidos (3-5 años).

Políticas de Seguridad

1. Todos los accesos remotos deben hacerse mediante SSH, VPN o protocolos cifrados.
2. Las contraseñas deben renovarse cada 90 días y cumplir con políticas de complejidad.
3. El acceso a VLANs críticas debe estar restringido solo a usuarios con privilegios altos.
4. Se deben aplicar listas de control de acceso (ACLs) en routers y switches de distribución.
5. Los puntos de acceso inalámbricos deben utilizar cifrado WPA3 y SSID oculto donde aplique.
6. Los equipos de red deben contar con nombre, IP estática y estar registrados en DNS.
7. Port Security debe estar habilitado en los switches para limitar el número de dispositivos por puerto.
8. El acceso físico a cuartos de telecomunicaciones debe estar controlado con cerraduras electrónicas.
9. Los logs del sistema (Syslog) deben ser revisados semanalmente para detectar incidentes.

10. Toda política de seguridad debe revisarse anualmente o tras una brecha de seguridad.

Políticas de Ejercicio Presupuestal

1. Toda compra de equipo o software debe estar respaldada por una justificación técnica.
2. Las inversiones tecnológicas deben alinearse con el plan de crecimiento de la red.
3. Se debe contar con una reserva presupuestal del 10% para emergencias tecnológicas.
4. No se realizarán compras fuera de los periodos presupuestales establecidos sin aprobación ejecutiva.
5. Todo contrato con proveedores debe incluir cláusulas de soporte técnico y garantía.
6. El ciclo de reemplazo de equipos debe definirse según obsolescencia y rendimiento.
7. Las solicitudes de adquisición deben incluir al menos dos cotizaciones comparativas.
8. Los recursos asignados a TI deben revisarse trimestralmente para ajustar gastos operativos.
9. Las inversiones deben priorizar seguridad, escalabilidad y compatibilidad con la red existente.
10. Se deben generar informes anuales del ejercicio presupuestal con indicadores de rendimiento (ROI).

SITE

El SITE, también conocido como cuarto de telecomunicaciones o cuarto de servidores, es un espacio físico especializado dentro de una infraestructura de red donde se centralizan los equipos críticos de conectividad y procesamiento, como switches de distribución, routers, servidores, racks, paneles de parcheo, UPS y sistemas de monitoreo. Por lo general, se ubica en un punto estratégico del edificio que permita

minimizar el cableado backbone y garantizar condiciones ambientales óptimas. La importancia del SITE radica en que funciona como el corazón operativo de la red, ya que concentra el flujo de datos, permite la segmentación lógica de la red, y asegura el desempeño, la estabilidad y la continuidad del servicio. Por ello, protegerlo física y lógicamente con políticas de seguridad y buenas prácticas es fundamental para garantizar la disponibilidad y confidencialidad de toda la infraestructura tecnológica de la organización.

Políticas de Seguridad para el SITE

1. El acceso físico al SITE debe estar restringido exclusivamente al personal autorizado mediante cerradura electrónica, lector biométrico o tarjeta de acceso.
2. El área debe contar con cámaras de vigilancia con grabación continua y respaldo de al menos 30 días.
3. Se debe llevar un registro de entrada y salida de personal, incluyendo fecha, hora y motivo de acceso.
4. El cuarto debe permanecer cerrado en todo momento; no se permite el acceso sin supervisión.
5. El SITE debe contar con sensores de temperatura, humo y humedad conectados a un sistema de alerta temprana.
6. Todos los equipos del SITE deben estar conectados a un sistema de energía ininterrumpida (UPS) y a una toma de tierra adecuada.
7. Está prohibido el almacenamiento de objetos ajenos al funcionamiento de red (archivos, cajas, mobiliario).
8. No se permite el uso de dispositivos de almacenamiento externo no autorizados dentro del SITE.
9. La infraestructura de red debe tener configurado acceso lógico mediante SSH y autenticación robusta.
10. Se deben realizar inspecciones de seguridad física y lógica del SITE al menos cada trimestre.

Buenas Prácticas en el SITE

1. Mantener una temperatura controlada entre 19 °C y 21 °C con ventilación o aire acondicionado adecuado.
2. Etiquetar correctamente todos los cables, puertos, equipos y paneles para facilitar la administración.
3. Utilizar canaletas y organizadores de cableado para evitar desorden y facilitar el mantenimiento.
4. Disponer de iluminación suficiente y señalización visible de emergencias y salidas.
5. Contar con un extintor tipo CO2 o para equipos electrónicos accesible dentro o cerca del SITE.
6. Hacer respaldos periódicos de la configuración de switches, routers y servidores.
7. Documentar cualquier cambio de configuración, conexión o reemplazo dentro del cuarto.
8. Usar racks con cerradura para resguardar switches y servidores que no requieren manipulación frecuente.
9. Establecer rutinas de mantenimiento mensual preventivo (limpieza, revisión de UPS, ventilación, etc.).
10. Auditar el acceso y revisar los registros de cámaras y logs de red de forma regular.

Rack

El rack es un gabinete metálico diseñado para alojar y organizar equipos de red, servidores, sistemas de almacenamiento, fuentes de energía y cableado estructurado de manera segura y eficiente. Su principal función es centralizar los dispositivos críticos de la infraestructura tecnológica, facilitando el mantenimiento, la ventilación, el orden del cableado y el aprovechamiento del espacio vertical. Los racks se dividen en unidades de medida llamadas UR (Unidades de Rack), donde cada UR equivale a 1.75 pulgadas de altura. Para una correcta distribución de los equipos, se siguen criterios de peso, tamaño y frecuencia de manipulación. En la parte superior del rack se colocan dispositivos livianos y de manipulación poco frecuente, como switches, routers, KVMs y patch panels, los cuales usualmente ocupan 2 UR. En la zona intermedia se ubican

equipos de tamaño medio y uso moderado como servidores, arreglos de discos y UPS, que requieren entre 4 y 8 UR. Finalmente, en la parte inferior se instalan los dispositivos más pesados, como estaciones de trabajo (workstations) que ocupan entre 6 y 8 UR, para mantener la estabilidad del rack. Además, por norma de organización y ventilación, se recomienda dejar al menos 1 UR libre entre equipos para evitar saturación y mejorar la circulación del aire. Esta disposición no solo mejora la estética y accesibilidad, sino que también prolonga la vida útil de los equipos y reduce riesgos operativos.

Por otra parte, debemos de tener en cuenta que la instalación de una red de datos genera un impacto ambiental significativo debido a las diversas etapas de su ciclo de vida: fabricación, instalación, operación y desecho final de los equipos tecnológicos. Durante la producción de componentes como cables, switches, routers y servidores, se extraen grandes cantidades de materiales como cobre, aluminio, plásticos y tierras raras, cuya minería y procesamiento consumen enormes recursos de energía y agua, además de causar deforestación y contaminación. Adicionalmente, la fabricación de estos dispositivos emite gases de efecto invernadero, agravando el cambio climático.

En la etapa de instalación, el transporte de materiales y equipos desde las fábricas hasta el sitio genera emisiones de carbono, mientras que el proceso mismo puede producir residuos como recortes de cables, embalajes plásticos y sobrantes de materiales, que suelen terminar en vertederos si no se gestionan adecuadamente. Durante el uso de la red, el consumo constante de electricidad por parte de dispositivos como switches, Access Points y servidores contribuye al aumento de la huella de carbono. Esto es especialmente crítico en centros de datos, responsables de hasta el 2% del consumo energético mundial. Además, el calor generado por estos equipos requiere sistemas de enfriamiento, que a su vez consumen más energía.

Finalmente, al llegar al final de su vida útil, los equipos de red se convierten en residuos electrónicos, un problema ambiental grave. Muchos de estos dispositivos contienen sustancias tóxicas como plomo, mercurio y cadmio, que pueden filtrarse en el suelo y al

agua si no se gestionan correctamente. Sin embargo, solo un pequeño porcentaje de estos residuos es reciclado de manera adecuada, lo que incrementa el problema.

Para mitigar estos impactos, es esencial adoptar medidas como el uso de equipos con certificaciones de eficiencia energética, la planificación de diseños de red sostenibles que optimicen el uso de materiales, el reciclaje adecuado de residuos y la alimentación de la infraestructura con energía renovable. Además, prolongar la vida útil de los dispositivos mediante mantenimiento preventivo y actualizaciones de software contribuye a reducir su impacto ambiental. A través de estas acciones, es posible minimizar los efectos negativos de la instalación de redes de datos y avanzar hacia un entorno más sostenible.

---

11. Administración y Monitoreo

- El sistema se administra desde una **interfaz web central** (Switches Cisco Catalyst de la serie 9300).
- Se emplea **Zabbix/Meraki** para visualización en tiempo real, con notificaciones por eventos.
- Documentación completa: topología lógica y física, contraseñas iniciales, respaldos.

---

12. Resultados de Implementación

Las pruebas de funcionamiento mostraron:

- Éxito en **comunicaciones entre dispositivos por ping** desde diferentes VLANs y pisos.
- Asignación dinámica correcta vía **DHCP desde routers**.
- Visualización de páginas HTTPS mediante DNS.
- Funcionamiento estable de VoIP entre pisos.
- Envío y recepción de **correos electrónicos internos** y uso de servidor FTP.
- **Accesos SSH y Telnet** confirmados y operativos.

Se anexó el repositorio GitHub del proyecto:
https://github.com/Mauricio658/ProyectoFinal_TeoriaAdministraci-nRedes.git

---

13. Mantenimiento Preventivo y Futuro

El mantenimiento dentro de una infraestructura de red es un conjunto de actividades programadas que buscan preservar el funcionamiento óptimo de todos los componentes físicos y lógicos del sistema. Es especialmente importante porque reduce el riesgo de fallos inesperados, prolonga la vida útil de los equipos y mantiene la disponibilidad de los servicios. El mantenimiento preventivo permite anticiparse a posibles incidentes mediante inspecciones y verificaciones periódicas, mientras que el mantenimiento evolutivo contempla la documentación y preparación para el crecimiento futuro de la red. En un entorno profesional, estas prácticas son esenciales para sostener el rendimiento, la seguridad y la escalabilidad de la infraestructura tecnológica. A continuación, se detallan las principales acciones contempladas para asegurar el buen estado actual y la evolución futura de la red.

Mantenimiento Preventivo

1. Realizar inspección trimestral del cableado estructurado para detectar desgaste, daño físico o conexiones sueltas.
2. Verificar cada tres meses el estado operativo de las UPS, asegurando el nivel de carga, funcionalidad de las baterías y correcto flujo de energía.
3. Controlar la temperatura y humedad del SITE con sensores especializados y registros automáticos.
4. Revisar periódicamente los logs de eventos de switches, routers y servidores para detectar fallos o comportamientos anómalos.
5. Actualizar el firmware de los dispositivos de red conforme a las recomendaciones del fabricante.
6. Realizar respaldos automáticos semanales de configuraciones de red y respaldos mensuales de información crítica.
7. Limpiar filtros de ventilación, rejillas y componentes físicos del SITE para asegurar una buena circulación del aire.
8. Verificar la integridad del sistema de puesta a tierra del cuarto de telecomunicaciones.
9. Validar que las etiquetas, señalización y documentación estén actualizadas en racks y paneles.
10. Realizar pruebas de conectividad y rendimiento por VLAN para detectar congestión o latencia.

Mantenimiento Evolutivo y Futuro

1. Mantener un plan de expansión actualizado que contemple la posible inclusión de nuevos pisos o áreas de trabajo.
2. Reservar espacio físico y lógico en los racks y switches para al menos 20 dispositivos adicionales.
3. Evaluar trimestralmente la capacidad de los puntos de acceso inalámbrico y planificar nuevos AP si la demanda lo requiere.

4. Documentar todo cambio físico o lógico en la red inmediatamente después de su ejecución.
5. Realizar estudios de cobertura WiFi anualmente para garantizar la calidad del servicio inalámbrico.
6. Verificar la escalabilidad del direccionamiento IP y la disponibilidad de VLANs en crecimiento.
7. Reemplazar o actualizar equipos que hayan alcanzado su ciclo de vida útil recomendado.
8. Evaluar anualmente el ancho de banda contratado vs. el consumo real para futuras adecuaciones.
9. Identificar cuellos de botella o puntos críticos y documentar soluciones previstas.
10. Reentrenar al personal de TI cada 12 meses en las mejores prácticas y protocolos actualizados.

Propuesta Económica

Para poder calcular el costo del proyecto se deben de tomar en cuenta varias cosas. Una de ellas es el tipo de contenedor o el medio por donde va ir el cable, la opción que nosotros recomendamos es el uso de:

- Bandejas portacables:
- Tipo: Bandejas de malla metálica.
- Medidas: 54/100 mm
- Capacidad máxima: 86 Cables Cat6
- Uso: Se colocarán en los trayectos principales del cableado horizontal para sostener y organizar los cables de red, asegurando una instalación limpia y sin interferencias. Además, las bandejas de malla permiten una buena ventilación y accesibilidad para futuras modificaciones o mantenimientos.

Para bajar el cable de la propia canaleta se puede hacer uso de canaletas o tubos conduit. Para mayor facilidad nosotros vamos a usar canaletas. Sin embargo, es muy

importante tener en cuenta que la capacidad máxima de una canaleta es del 40%, este porcentaje es recomendado por EIA/TIA-569-A para el diseño de sistemas de cableado estructurado.

- Tipo: Canaletas de PVC con tapas desmontables.
- Medidas: 52/100 mm
- Uso: Se utilizarán para canalizar los cables en los espacios visibles, como a lo largo de las paredes en áreas de trabajo. Las canaletas permiten una fácil instalación y mantenimiento, y ayudan a mantener una estética limpia en el entorno de oficina

Otra parte fundamental para el cálculo del costo del proyecto es el uso de los racks. Cada piso debe de contar con un rack de 32U como ya se había mencionado anteriormente.

- Tipo: Rack de 32U con cerradura.
- Uso: El rack se utilizará para alojar los equipos de red, como los switches y los paneles de parcheo, en el cuarto de telecomunicaciones (TR). Este tipo de rack garantiza una buena organización y accesibilidad para los equipos, así como seguridad física al contar con cerraduras para evitar accesos no autorizados.

También debemos de tener en cuenta que necesitamos alrededor de 4600 [mts] de cable UTP cat6. Así como, los conectores RJ-45 cat6. Los conectores RJ-45, son los terminadores más utilizados en redes de datos, especialmente para cables de par trenzado. Cada cable contará con dos conectores RJ-45, uno en cada extremo. En total tenemos una cantidad de 153 nodos en todo el edificio contando los APs. La planta baja cuenta con 35 nodos, el primer, segundo y tercer piso cuentan con 29 nodos y el cuarto piso cuenta con 31 nodos. Esto quiere decir que necesitamos 306 conectores.

De igual forma, necesitamos las placas de pared, ya que, son esenciales para proporcionar un punto de conexión limpio y ordenado en cada nodo de red. En este proyecto, se utilizarán placas de pared compatibles con los estándares del cableado estructurado, específicamente diseñadas para soportar cables de categoría 6 y las

conexiones RJ-45. vamos a usar una placa de pared por cada nodo. Entonces, necesitamos 153 placas de pared.

Como elemento adicional se recomienda el uso de una unidad UPS (Sistema de Alimentación Ininterrumpida) para proteger los equipos críticos de la red ante posibles fallos en el suministro eléctrico. Es decir, en caso de un corte de energía, permitirá a los sistemas que continúen funcionando durante un tiempo determinado, lo cual es esencial para evitar la pérdida de datos o interrupciones en los servicios.

Para las bandejas portacables vamos a usar 100 mts por cada piso. Entonces, en total vamos a usar una cantidad de 500 mts.

Para las canaletas se venden por pieza. Entonces debemos de encontrar una que se adapte a nuestras necesidades. Anteriormente, mencionamos que el total de nodos son 153, entonces necesitamos 153 canaletas.

Dispositivos o Material	***Precio***
Cable (4600 mts)	84,878.56 MXN
Bandejas portacable (500 mts)	30,000 MXN
Canaletas (153 pzas)	9,534.96 MXN
Racks 32 U (5 racks)	77,485.15 MXN
Conectores RJ-45	1347 MXN
Placas de pared	17,633 MXN
Switches	38,000 MXN
Puntos de Acceso	28,800 MXN
Sistema de Alimentación Ininterrumpida	15,000 MXN
Mano de obra	40,000 MXN
TOTAL	***342,678.67 MXN***

Cada bobina de cable tiene 305 mts y tiene un precio de 5,304.91 MXN de la marca CONDUMEX. Necesitamos alrededor de 16 bobinas para tener la cantidad necesaria de cable, dándonos un precio de 84,878.56 MXN.

Para la bandeja portacable nos da un valor de 30,000 MXN.

Las canaletas tienen un precio de 62.32 MXN por pieza. Necesitas un total de 153 pzas. Dándonos un total de 9,534.96 MXN.

Para los racks de 32U encontramos que el precio de estos racks están alrededor de 15,497.03 MXN. Como vamos a utilizar uno en cada piso debemos de tener 5 en total dándonos un precio total de 77,485.15 MXN.

La caja de los conectores cuestan 429 MXN y trae 100 piezas. Nosotros estimamos un total de 306 conectores. Podemos comprar 3 botes de 100 piezas y las piezas faltantes las podemos conseguir de forma individual. Esto nos da un costo de 1347 MXN.

Para las placas de pared encontramos un precio de dos placas de pared por 229 MXN. Necesitamos 153 placas de paredes y eso nos da un precio de 17,633 MXN.

---

14. Conclusiones

Este proyecto ha demostrado la viabilidad y necesidad de contar con una red híbrida moderna. La integración de servicios esenciales, el diseño basado en normas, la segmentación inteligente y la administración remota forman una infraestructura lista para los desafíos tecnológicos actuales y futuros. La topología escalable, la seguridad

aplicada, y los servicios funcionales permiten a la empresa operar con alta disponibilidad, eficiencia y control.

15. Referencias

ALCIONE. (S/F). *BANDEJA P/CABLE 3MT 54X100MM ZINCADO*. https://www.alcione.mx/bandeja-p-3-cable-3mt-54x100mm-zincado-cf054--3%3D100%20ez#:~:text=%24555.

ALCIONE. (S/F). *CANALETA DE PVC C/TAPA DE 17X20X2500MM 1 VIA BLANCO*. https://www.alcione.mx/canaleta-de-pvc-c-3-tapa-de-17x20x2500mm-1-via-1720tmk

Amazon. (S/F), Iwillink *Placa de Pared Ethernet, Placa de Pared Keystone Jack de 1 puerto con Conector RJ45 Keystone en Línea, Placa de Pared Hembra a Hembra Cat6 Keystone, Color Azul, Paquete de 2*. https://www.amazon.com.mx/Iwillink-Ethernet-Keystone-Conector-Paquete/dp/B09NVQJGXK/ref=asc_df_B09NVQJGXK/

Argüello, F. (2025, marzo 3). *Cómo Instalar Cableado Seguro Según NFPA 70*. Felipe Argüello. https://www.infoteknico.com/cableado-seguro/

Blog, B. (Last updated Jan 16, 2025 | Published on May 24 2023). Normas de marcado y etiquetado UL 969. *Boyd | Trusted Innovation*. https://es.boydcorp.com/blog/ul-marking-and-labeling-standards.html

Cisco networking academy. (s/f-a). Netacad.com. Recuperado el 1 de abril de 2025, de https://www.netacad.com/launch?id=5846d097-8c60-4c85-a958-72a67ab938c9&tab=curriculum&view=b04986b6-c9af-557a-87de-45062681d376

Cisco networking academy. (s/f-b). Netacad.com. Recuperado el 1 de abril de 2025, de https://www.netacad.com/launch?id=5846d097-8c60-4c85-a958-72a67ab938c9&tab=curriculum&view=a2b89d4b-53bf-5cc5-b59c-f8f4ecc241af

CIVINET SAS. (S/F). *Cableado Estructurado: 10 Recomendaciones para una Instalación Exitosa*. https://www.civinetsas.com/cableado-estructurado-10-recomendaciones/

EBAY. (S/F). *Server Rack 32U Network Cabinet 24" depth Data Server Cabinet - BONUS INCLUDED*. https://www.ebay.com/itm/

Elton, P. A. M. (2024, junio 17). *Estándar ANSI/TIA 568A Y 568B Cableado Estructurado*. SILYMX. https://sily.mx/blogs/base-de-conocimientos-noticias/estandar-ansi-tia-568a-y-568b-cableado-estructurado

INCOM. (S/F). 66766645 - Cable UTP Cat 6 para uso exterior (305 m). https://incom.mx/collections/cable-cat-6/products/cable-utp-cat-6-para-uso-exterior-305-m-marca-condumex-66766645

Martínez, R. (S/F). El armario de comunicaciones de una red local. ADR formación. https://www.adrformacion.com/knowledge/administracion-de-sistemas/el_armario_de_comunicaciones_de_una_red_local.html

Microsoft. (2023, marzo 08). Protocolo de configuración dinámica de host (DHCP). https://learn.microsoft.com/es-es/windows-server/networking/technologies/dhcp/dhcp-top

PC DOMINO. (S/F). Bote C/ 100 Conectores RJ45, P/ Cable Cat 6, Uso Interior, INTELLINET 502344. https://pcdomino.com/products/bote-c-100-conectores-rj45-p-cable-cat-6-uso-interior-intellinet-502344

Sanchez, D. (2023, junio 07). Todo lo que hay que saber del Cableado Estructurado para Redes. ITA TECH. https://ita.tech/todo-lo-que-hay-que-saber-del-cableado-estructurado

Stokes, H. (2024, octubre 02). ¿Qué es una sala IDF y qué hace?. The Network Installers.https://thenetworkinstallers.com/es/blog/habitaci%C3%B3n-de-las-FDI/

Telefónica. (2023, septiembre 13). ¿Cómo afecta la tecnología al medioambiente?. https://www.telefonica.com/es/sala-comunicacion/blog/afecta-tecnologia-medioambiente/

(S/f). Auditoriainterna.es. Recuperado el 1 de abril de 2025, de https://auditoriainterna.es/iso-11801/