Introducción

La Empresa Tarijeña del Gas “EMTAGAS” es un pilar fundamental en la ciudad de Tarija, y para continuar brindando servicios confiables y seguros, es esencial que la infraestructura de tecnología de la información esté a la altura de los desafíos actuales. Este proyecto de rediseño de la red LAN se presenta con el propósito de transformar la infraestructura de red en una base sólida que respalde las operaciones críticas y las necesidades cambiantes de la Organización.

En un mundo donde la tecnología desempeña un papel fundamental en la prestación de servicios de calidad, el rediseño de la red se presenta como una iniciativa estratégica para elevar la empresa al siguiente nivel. En esta propuesta, exploraremos en detalle cómo se planeará para lograrlo, aprovechando tecnologías de vanguardia y estrategias de seguridad sólidas para garantizar un rendimiento excepcional y la protección de los activos más valiosos: los datos y la confianza de los trabajadores.

La red actual de la infraestructura ha servido satisfactoriamente, pero enfrenta limitaciones en términos de rendimiento, seguridad y escalabilidad. El crecimiento de la empresa y la creciente demanda de servicios requieren una infraestructura de red robusta que pueda respaldar las operaciones críticas y laborales del día a día. Este proyecto se presenta como propuesta de solución para abordar estos desafíos, explorando a detalle los capítulos y componentes claves del rediseño de red LAN.

CAPÍTULO I

DEFINICIÓN DEL PROYECTO

Capítulo I: Definición del proyecto

I.1. Descripción del proyecto

I.1.1. Antecedentes

1. La empresa EMTAGAS fue fundada el 14 de octubre de 1988, es la entidad prestadora de servicios de gas domiciliario en el departamento de Tarija que actualmente requiere de una organización administrativa para la operación y mantenimiento de los indicados servicios.

2. Fue creada como una Empresa Pública de Servicios y de carácter social; por lo tanto, es una Empresa sin fines de lucro. La política y el objetivo fundamental de EMTAGAS es que toda familia que habita en el departamento de Tarija cuente con el servicio de gas domiciliario mediante el plan para todos.

3. La empresa Tarijeña del Gas está conformada por la gobernación autónoma del Departamento de Tarija, Yacimiento Petrolíferos Fiscales Boliviano y la Honorable Alcaldía Municipal de Tarija.

I.1.2. Justificación del Proyecto

4. Justificación con base en dos aspectos:

5. Tecnológico: el diseño de una red WLAN y mejoramiento de la red LAN, esto permitirá la mejora en cuanto a transmisión y comunicación de datos entre sus áreas, trayendo consigo un mejor servicio para la comunidad

6. Operativa: El personal encargado del TI de la red LAN, se mantiene informado para la configuración de la nueva tecnología.

I.1.3. Planteamiento del problema

7. Inadecuación de la infraestructura de la red LAN de EMTAGAS frente a los desafíos tecnológicos actuales.

I.1.4. Objetivos

I.1.4.1. Objetivo General

8. Mejoramiento del desempeño de la red LAN para la empresa Tarijeña del Gas EMTAGAS.

I.1.4.2. Objetivos Específicos

- Red LAN de EMTAGAS rediseñado.
- Socializar a los trabajadores sobre la propuesta de la red LAN de EMTAGAS.

I.1.5. Resultados Esperados

- Concluir con la propuesta del diseño de la red LAN, proponiendo un mejoramiento en las actividades internas de EMTAGAS.
- Informar a los trabajadores y encargados del TI de EMTAGAS Tarija, sobre la propuesta del mejoramiento de la red de la misma infraestructura.

I.1.6. Beneficiarios

1.1.6.1. Beneficiarios Directos

9. Los beneficiarios directos son los trabajadores de la empresa, también denominados usuarios, que están directamente relacionados y en contacto con los equipos existentes en las oficinas.

1.1.6.2. Beneficiarios indirectos

10. Los beneficiarios indirectos son los clientes, ya que estos no están conectados a la red, pero son beneficiados por el adecuado uso del servicio de red de la empresa EMTAGAS.

I.1.7. Presupuesto General

Categoría	Descripción	Costo
Hardware y Software	Equipos de red (enrutadores, switches, servidores, etc.).	60,000 Bs.
	Telefonía IP y sistemas relacionados	15,000 Bs.
	Software de seguridad (firewalls, soluciones de autenticación).	25,000 Bs.
Infraestructura de conectividad	Fibra óptica y cableado UTP.	25,000 Bs.
Centro de Datos	Equipamiento y acondicionamiento del centro de datos, incluyendo racks y sistemas de refrigeración.	15,000 Bs.
Costos de seguridad	Implementación de medidas de seguridad, incluyendo hardware y software de seguridad, control de acceso físico, y sistemas de monitoreo.	25,000 Bs.
Total, del presupuesto		140,000 Bs.

Tabla 1 *Presupuesto general*

Fuente: *Elaboración propia*

I.2 Matriz del marco lógico (MM.)

Resumen Narrativo del Proyecto	**Indicadores**	**Medios de Verificación**	**Supuestos**
Fin Contribuir a mejorar el “servicio al cliente” de la Empresa Tarijeña del Gas (EMTAGAS)	A dos años de finalizado el proyecto, se ha incrementado al menos en un 90% el número de clientes de EMTAGAS, que catalogan al “servicio al cliente” como excelente.	Se plantea que, si el proyecto fuera implementado, se realizarían encuestas al inicio y a los dos años de su finalización, con el fin de medir el impacto en la percepción del servicio al cliente.	Se mantiene la Infraestructura y la estructura orgánica de la empresa de EMTAGAS
Objetivo General (Propósito) Mejoramiento del desempeño de la red LAN para la empresa Tarijeña del gas EMTAGAS	**Criterio de Mejora:** Disponibilidad de la Red (Uptime) **Indicador:** "Al finalizar el proyecto, las simulaciones del diseño propuesto	Documento formal de aprobación de la propuesta de los servicios por el encargado de sistema de la Empresa EMTAGAS Tarija.	Compromiso y apoyo continuo del encargado de sistemas de la Empresa EMTAGAS Tarija en la definición de requerimientos y entrega

	para la red LAN de EMTAGAS demuestran una disponibilidad potencial incrementada en un 40% en comparación con el estado actual, garantizando la operación continua de los servicios críticos durante el horario operativo."		de manera oportuna la información.
Objetivos Específicos (Componentes) 1. Red LAN de EMTAGAS rediseñado	1.1 Al finalizar el proyecto se ha cumplido con los servicios disponibles de acuerdo a la ERS IEEE830.	1.1 Documento formal de aprobación de la propuesta del rediseño de la red, por parte del docente. 2.1 A través de una carta de conformidad de la explicación del	1.1 Disponibilidad de recursos digitales para la simulación de equipos de red en la propuesta de rediseño.

2. Socialización al personal del TI sobre la propuesta de red LAN- de EMTAGAS. .	2.1 Al finalizar el proyecto se ha explicado la propuesta para el uso y la configuración de la red.	proyecto hacia el encargado del TI de EMTAGAS	2.1 Asistencia del personal del TI de EMTAGAS
Actividades Componente 1: 1.1 Diseño del cableado estructurado (horizontal y vertical).	1.1.1 Propuesta de diseño de topología de red (estrella). 1.1.2 Propuesta de acomodación del cableado UTP Ethernet Cat. 7A. y de rosetas. 1.2.1 Propuesta de políticas de seguridad para el firewall Fortinet.	1.1.1 Documento formal de la propuesta de diseño 1.1.2 Documento formal de la propuesta de acomodación de cableado y de las rosetas. 1.2.1 Documento formal de la propuesta de políticas de seguridad y de los estándares de	1.1.1 Acceso a la información técnica sobre la red actual y cooperación del personal del TI de EMTAGAS. 1.2.1 Acceso a la configuración del

1.2 Configuración en el firewall (Fortinet), para cubrir la seguridad necesaria.	1.2.2 Propuesta de estándares de acceso a sitios web y programas de ejecución.	acceso a sitios web y programas de ejecución.	firewall de la simulación de red.
1.3 Elaboración de VLANs en la restructuración de la red LAN – WLAN.	1.3.1 Propuesta de configuración de VLANs en los Switches. 1.3.2 Simulación de conectividad y segregación de VLANs.	1.3.1 Documento formal de la propuesta de configuración de VLANs. 1.3.2 Capturas de la simulación de conectividad y pruebas de VLANs.	1.3.1 Equipos de simulación adecuados y la vinculación para la simulación de red.
1.4 Propuesta de implementación de armarios IDF.	1.4.1 Propuesta de instalación de nuevos racks y switches para incremento de IDF.	1.4.1 Documento formal de la propuesta de instalación de racks. 1.5.1 Documento formal de la propuesta de metodología de registro.	1.4.1 Disponibilidad de espacio y recursos

1.5 Propuesta de registro de equipos en la red LAN. 1.6 Propuesta de añadir una red WLAN.	1.5.1 Propuesta de metodología para registro de equipos en la red (tablas de direccionamiento). 1.5.2 Validación de conectividad de equipos registrados en la simulación. 1.6.1 Propuesta de integración de una nueva red WLAN. 1.6.2 Simulación de cobertura y rendimiento de la red WLAN.	1.5.2 Reporte de validación de conectividad de equipos en la simulación. 1.6.1 Documento formal de la propuesta de integración de red WLAN. 1.6.2 Reporte de simulación de cobertura y rendimiento de la red WLAN. 2.1.1 A través de un listado de asistencia a los encargados del TI y trabajadores de EMTAGAS	financieros para la propuesta. 1.5.1 Acceso a herramientas de gestión de red y cooperación del personal de IT y usuarios finales. 1.6.1 Equipos de simulación adecuados y conocimiento técnico para la simulación de red.

Componente 2: 2.1 Organizar sesiones de presentación de la propuesta de red para el personal encargado de IT y trabajadores de EMTAGAS	2.1.1 Preparar un ambiente (virtual o presencial), y materiales de explicación (presentación de propuesta)		2.1 Disponibilidad del tiempo de los encargados del TI y trabajadores de EMTAGAS.

Tabla 2 *Matriz de marco lógico (MML)*

Fuente: *Elaboración propia*

I.2.1. Cronograma de actividades

Actividad	Nro. de Días	Fecha inicio	Fecha fin
1 ANALISIS DE REQUERIMIENTOS	47	14/2/2024	18/4/2024
1.2 Analizar metas del negocio	10	14/2/2024	27/2/2024
1.3 Analizar metas técnicas	10	28/2/2024	12/3/2024
1.4 Analizar red existente	10	13/3/2024	26/3/2024
1.5 Analizar tráfico existente	17	27/3/2024	18/4/2024
2 DESARROLLAR DISEÑO LOGICO	100	19/4/2024	5/9/2024
2.1 Diseñar topología de red	20	19/4/2024	16/5/2024
2.2 Diseñar modelos de direccionamiento y hostnames	20	17/5/2024	13/6/2024
2.3 Seleccionar protocolos para Switching y Routing	20	14/6/2024	11/7/2024
2.4 Desarrollar estrategias de seguridad	20	12/7/2024	8/8/2024
2.5 Desarrollar estrategias de administración de red	20	9/8/2024	5/9/2024
3 DESARROLLO DEL DISEÑO FISICO	30	6/9/2024	17/10/2024
3.1 Seleccionar tecnologías y dispositivos para redes de campus	15	6/9/2024	26/9/2024
3.2 Seleccionar tecnologías y dispositivos para redes empresariales	15	27/9/2024	17/10/2024
4 SIMULACION DE LA RED	35	18/10/2024	5/12/2024
4.1 Probar diseño de red	15	18/10/2024	7/11/2024
4.2 Optimizar el diseño de red	10	8/11/2024	21/11/2024
4.3 Documentar resultados emulados	10	22/11/2024	5/12/2024

Tabla 3 *Cronograma de actividades*

Fuente: *Elaboración propia*

Diagrama de Gantt

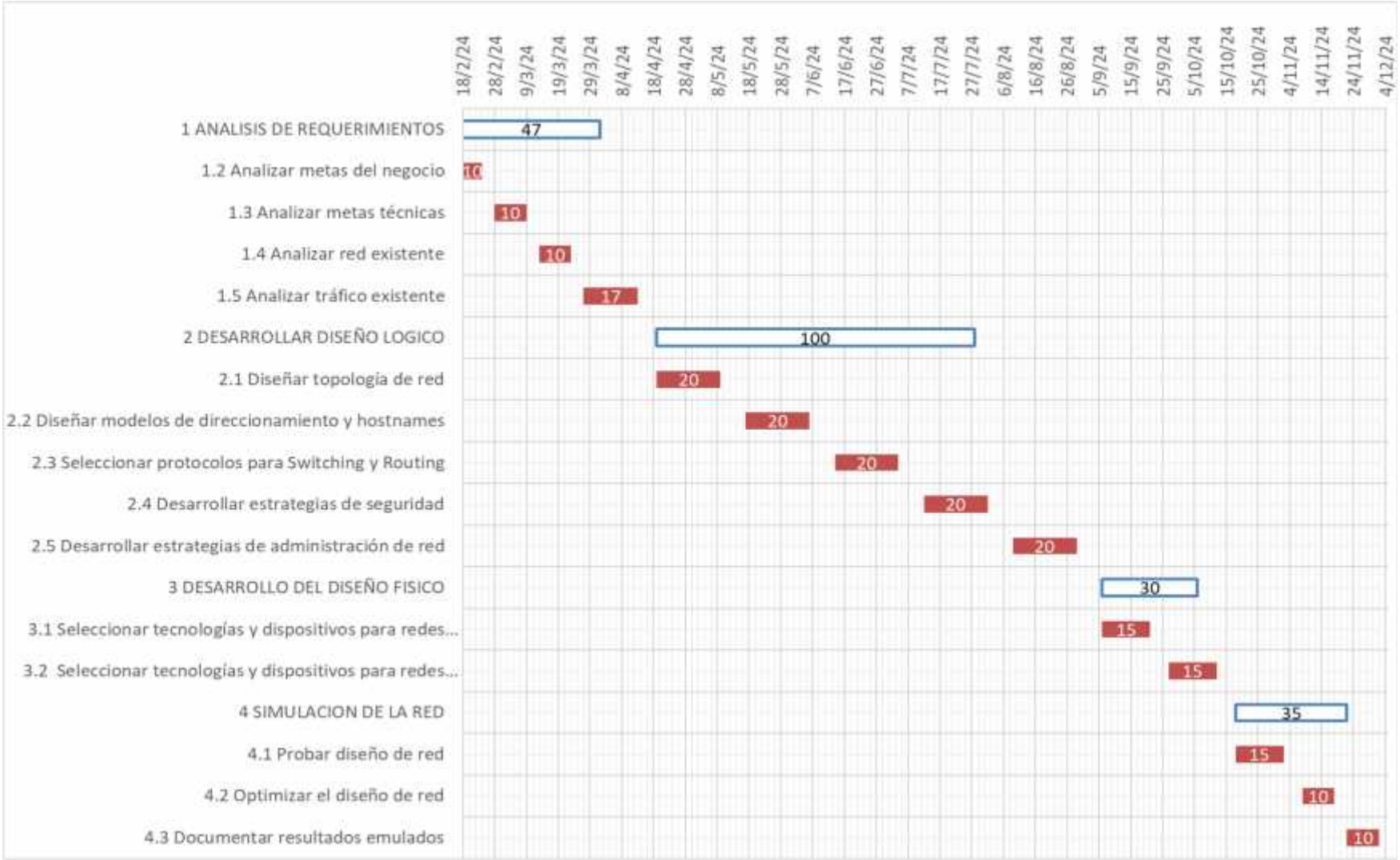


Figura 1: *Diagrama de Gantt*

Fuente: *Elaboración propia*

I.2.2. Árbol de Problemas

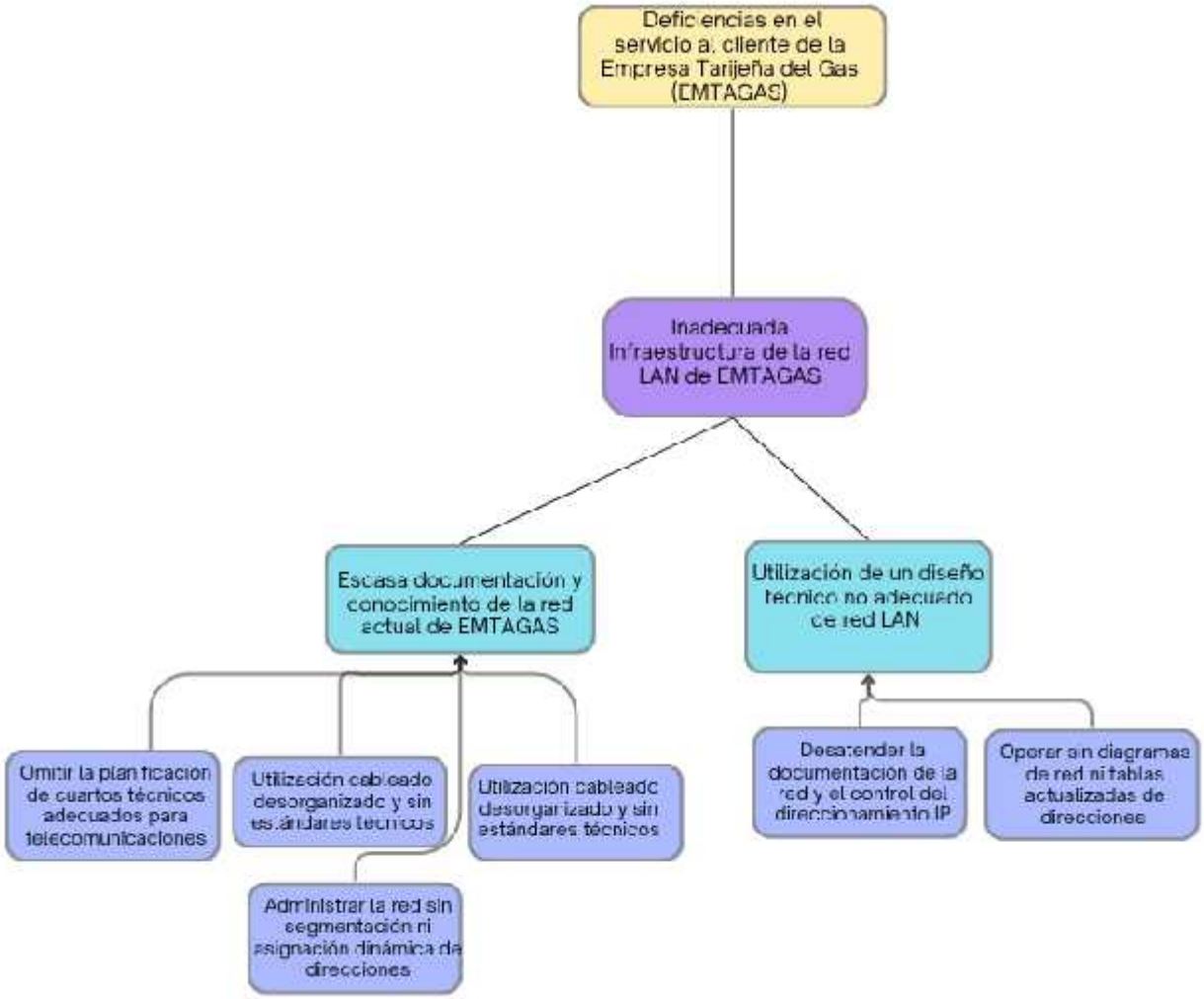


Figura 2: *Árbol de problemas*

Fuente: Elaboración propia

I.2.3. Árbol de Objetivos

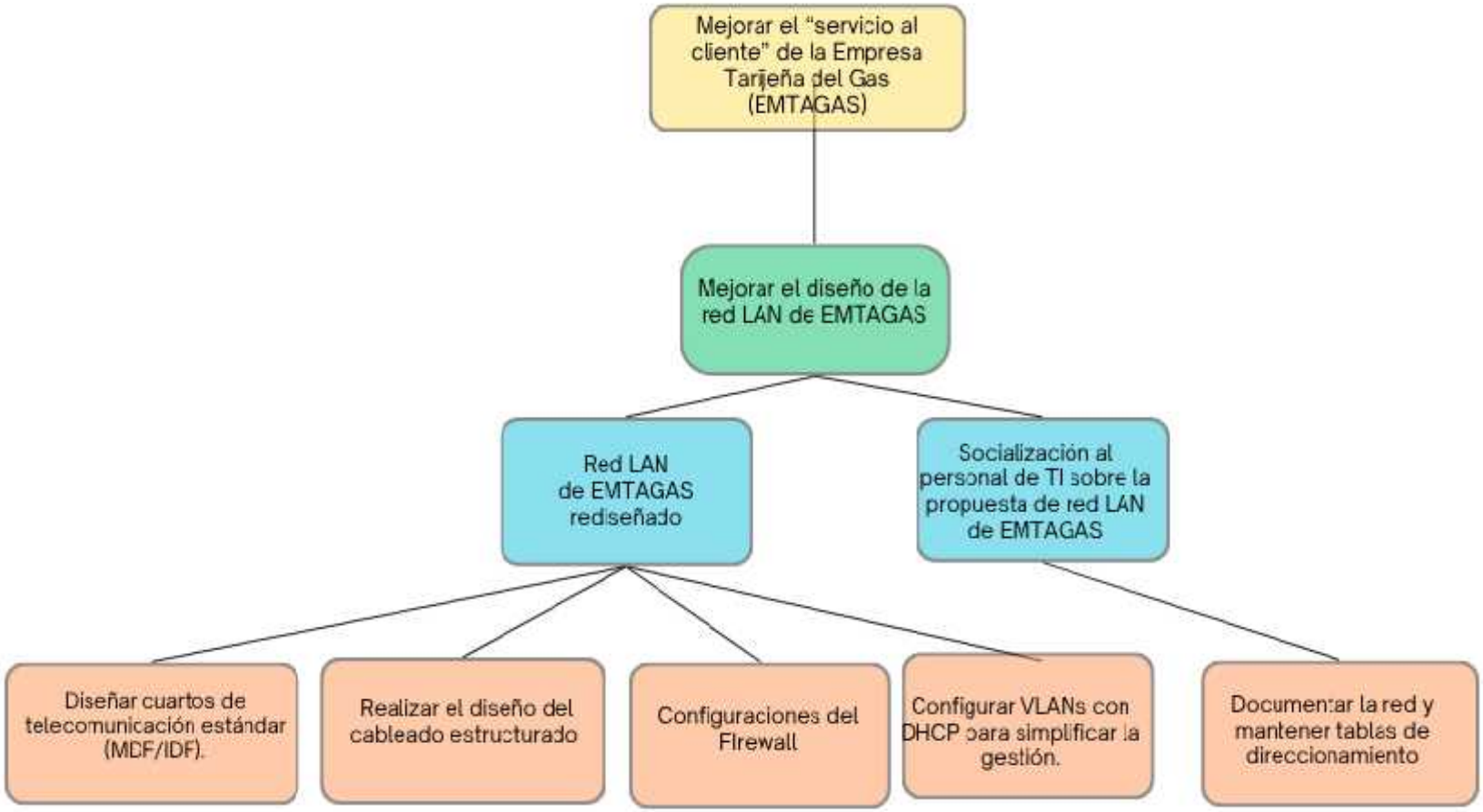


Figura 3: *Árbol de objetivo*

Fuente: *Elaboración propia*

I.3. Metodología

I.3.1. Metodología TOP-DOWN

11. La metodología Top-Down, también conocida como "arriba hacia abajo" en español, es un enfoque que se utiliza en diversos campos, incluyendo la programación, el diseño de sistemas y redes. La metodología Top-Down es un enfoque jerárquico que se utiliza para diseñar sistemas y resolver problemas complejos. Comienza con un diseño de alto nivel y se descomponga gradualmente en componentes más pequeños y detallados. Esto proporciona una estructura clara para la planificación y ejecución de proyectos, permitiendo un enfoque gradual y una visión general del sistema desde el principio.

12. El enfoque “top-down” es esencial en proyectos de redes porque asegura que la infraestructura de red se construya teniendo en cuenta los objetivos comerciales, lo que resulta en soluciones que son más efectivas y estratégicas para la organización.

Se tomarán en cuenta 4 puntos de la metodología, estos puntos son:

13. 1.— Análisis de Requerimientos.

- Analizar metas del negocio.
- Analizar metas técnicas.
- Analizar red existente.
- Analizar tráfico existente.

14. 2.— Diseño Lógico.

- Diseñar topología de red.
- Diseñar modelos de direccionamiento y hostnames.
- Seleccionar protocolos para Switching y Routing.
- Desarrollar estrategias de seguridad.

- Desarrollar estrategias de administración de red.

15. 3.— Desarrollar Diseño Físico.

- Seleccionar tecnologías y dispositivos para redes de campus.
- Seleccionar tecnologías y dispositivos para redes empresariales.

16. 4.— Pruebas del diseño.

- Probar el diseño de red.
- Optimizar el diseño de red.
- Documentar el diseño.

Capítulo II

Marco Teórico

Capítulo II Marco Teórico

II.1. Redes de Comunicación de Datos

II.1.1. Introducción

17. Una red de comunicación es básicamente un conjunto o sistema de equipos informáticos conectados entre sí, por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos con la finalidad de compartir datos, información, recursos y ofrecer servicios.

18. Entre las principales características para definir su funcionalidad están:

- Velocidad
- Seguridad de la red
- Confiabilidad
- Escalabilidad
- Disponibilidad

II.1.1.2. Modelos de Protocolos y de Referencias

19. Un elemento fundamental para la comprensión de los procesos involucrados en la transmisión de datos sobre medios de networking son los modelos teóricos que permiten explicar e informar la función de cada uno de los elementos que intervienen en la comunicación.

20. Muchos son los modelos desarrollados con este propósito: el modelo Apple Talk, el modelo Novell Netware, el modelo TCP/IP, el modelo OSI, etc. La mayoría de ellos tienen un elemento en común: Son modelos de capas que se dividen las diferentes tareas en los módulos independientes conectados por interfaces; de esta forma, facilitan la comprensión de los procesos y, por sobre todo, el desarrollo de nuevas tecnologías (Acosta, 2012)

21. De esta multiplicidad de modelos, dos son los que importan: el modelo TCP/IP y el modelo OSI.

II.1.1.3. Modelo TCP/IP

22. El modelo TCP/IP es un modelo en capas desarrollado inicialmente para facilitar el establecimiento de comunicaciones de extremo a extremo.

23. Es el modelo de aplicación en Internet. Por este motivo es el más difundido y muchos de los protocolos originales del Internet refieren a este modelo de capas. (FORTINET, FORTINET, 2024)

24. En la actualidad sigue siendo de gran aplicación, aunque en términos generales se prefiere el modelo OSI para el estudio y análisis.

25. Más allá de su utilidad como modelo, también se suele denominar TCP/IP a un conjunto de protocolos que trabajan a partir de la implementación del protocolo TCP, capa de transporte y protocolo IP en la capa de internet. (Gerometta, 2017, pág. 52).

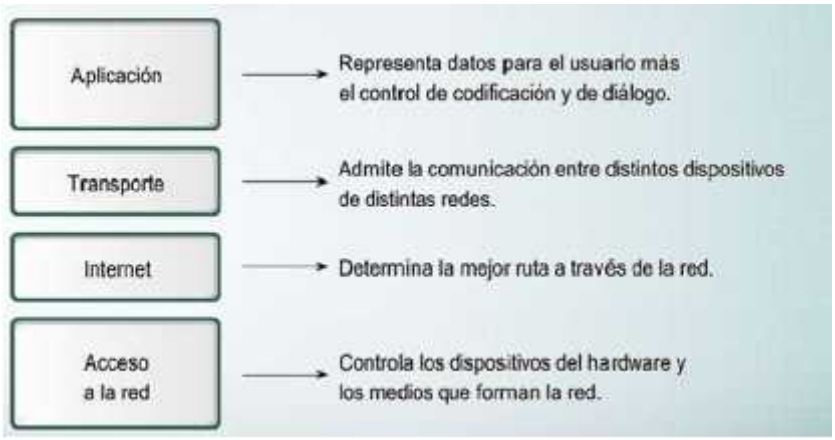


Figura 4: *Modelo TCP/IP*

Fuente: (elcuadernodejhonny, 2014)

II.1.1.4. Modelo OSI

26. Fue creado por la ISO a principios de la década de 1980 para solucionar los problemas generados por el desarrollo e implementación de diferentes modelos propietarios diseñados por diferentes fabricantes (IBM, 2020)

27. Es el modelo de arquitectura primaria para redes. Describe cómo los datos y la información de la red fluyen desde una terminal, a través de los medios de red, hasta otra terminal.

28. Divide el proceso global en grupos lógicos más pequeños de procesos a los que denomina “capas” o “layers”. Por este motivo se habla de una “arquitectura de capas” (Gerometta, 2019).

Figura 5: *Modelo OSI*

Fuente: (castro, 2018)

II.1.1.5. Comparación entre los modelos OSI Y TCP/IP

29. Una de las principales diferencias es que OSI es un modelo conceptual que no se utiliza prácticamente para la comunicación, mientras que TCP/IP se utiliza para establecer una conexión y comunicarse a través de la red. (Sheldon, 2021).

30. El modelo TCP/IP fue desarrollado antes que el modelo OSI, y, por lo tanto, las capas difieren. Con respecto al diagrama que vemos a continuación, se ve claramente que el Modelo TCP/IP tiene cuatro capas que son: interfaz de red, Internet, transporte y Capa de Aplicación. (FORTINET, FORTINET, 2022).

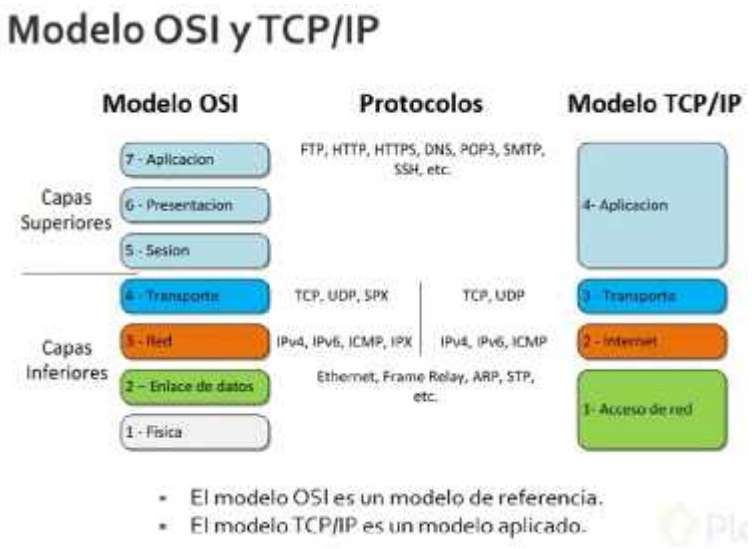


Figura 6: *Modelo OSI Y TCP/IP*

Fuente: (Ortiz, 2022)

II.1.2. Hardware para redes LAN-WLAN

31. Para hacer posible la conexión entre sí y la conectividad a Internet de los equipos informáticos conectados a tu red LAN o red Wifi se necesitan una serie de dispositivos hardware que

constituyen la infraestructura de la red informática: armarios rack, routers, switches, puntos de acceso Wifi, patch panels, latiguillos, cableado de red, canaletas y rosetas, entre otros. (COMUNICATIONS).

II.1.2.1. Racks de comunicaciones

32. Los armarios rack son unas estructuras metálicas que se utilizan para centralizar en un solo lugar los principales componentes hardware de la red informática y de comunicaciones del recinto, por ejemplo (routers, switches, patch panels, grabadores CCTV, etc.). (Luz, 2024).

Figura 7: *Racks de comunicaciones*

Fuente: (DOYSON, 2022)

II.1.2.2. Router

33. Un router o enrutador es un dispositivo hardware que se utiliza para conectar una red informática local (LAN) con otras redes informáticas. En el contexto del recinto es básicamente el dispositivo que gestiona la conectividad a Internet, siendo el encargado de recibir, transmitir, analizar y reenviar los paquetes de datos desde y hacia el exterior de tu red local. (Cloudflare, 2024).

34. Dado que son la puerta de entrada a tu red local, los routers son fundamentales a nivel de seguridad informática, y es muy importante configurarlos correctamente, disponer de un firewall

potente que te proteja de ataques externos, y disponer de una visión muy clara de qué puertos de conexión están abiertos al exterior y quién puede utilizarlos.

Figura 8: *Router*

Fuente: (amazon, 20222)

II.1.2.3. Switch

35. Un switch o conmutador es el dispositivo hardware que gestiona la comunicación interna entre todos los equipos conectados a tu red informática local. Cuando recibe un mensaje, el switch no lo transmite a toda la red, sino que verifica a qué sistema o puerto debe enviarlo, conectando de forma directa al emisor y al receptor del mensaje, y aumentando de este modo la velocidad efectiva de la red. (Blog, 2023).

36. Los switches disponen de fuente de alimentación, varios puertos RJ45 (uno por cada dispositivo que quieras conectar a la red) y luces de conexión que te permiten confirmar que los puertos están funcionando correctamente. (COMMUNICATIONS, 2021).

Figura 9: *Switch*

Fuente: (manuals.plu, 2020)

II.1.2.4. Servidor

El servidor es aquel o aquellas computadoras que van a compartir recursos hardware y software con los demás equipos de la red. (Paessler, 2024).

Figura 10: *Servidor*

Fuente: (tecnozero, 2020)

II.1.2.5. Gateway

37. Es un hardware y software que permite que se conecten dos redes locales entre sí. Un puente interno es el que se instala en un servidor de la red, y un puente externo es el que se hace sobre una estación de trabajo de la misma red. Los puentes también pueden ser locales o remotos. Los puentes locales son los que conectan a redes de un mismo edificio, usando tanto conexiones internas como externas. Los puentes remotos conectan redes distintas entre sí, llevando a cabo la conexión a través de redes públicas, como la red telefónica, RDSI o red de conmutación de paquetes. (Unlimited).

Figura 11: *Gateway*

Fuente: (tieline, s.f.)

II.1.2.6. Tarjeta de Red PCI

38. Tarjeta de red: también se denomina NIC(Network interface Card). Básicamente, realiza la función de intermediario entre la computadora y la red de comunicación. En ella se encuentran grabados los protocolos de comunicación de la red. La comunicación con la computadora se realiza normalmente a través de las ranuras de expansión de que este dispone, ya sea ISA, PCI o PCMCIA. Aunque algunos equipos disponen de este adaptador integrado directamente en la placa base. (Citelia)

Figura 12: *Tarjeta de red PCI*

Fuente: (aten, 2020)

II.1.2.7. Medio de Conexión

39. Constituido por el cableado y conectores que enlazan los componentes de la red. Los medios físicos más utilizados son el cable de par trenzado, cable coaxial y la fibra óptica.

Figura 13: *Medio de Conexión*

Fuente: (rockwellautomation., 2019)

II.1.2.8. Patch panels

40. Los patch panels (paneles de conexión) son un elemento hardware que se compone de un conjunto de puertos de entrada o de salida, y que se utiliza para organizar y clasificar la conexión del cableado exterior de un armario rack con los dispositivos instalados dentro del rack. (John, 2021)

41. En lugar de conectar directamente el cableado con los diferentes dispositivos que hay en el rack, cada cable se conecta con su correspondiente puerto en el patch panel, facilitando la clasificación y el etiquetado de cada conexión. Como cada puerto dispone de dos caras, una vez el cable exterior está conectado, podemos conectar el puerto del patch panel al puerto correspondiente del dispositivo final al que debe conectarse mediante latiguillos.

42. La utilización de patch panels es especialmente útil en redes de alta densidad de cableado, pues facilita la modularidad y escalabilidad futura de las conexiones, permite un acabado estético y organizado del cableado de red, y facilita la detección y corrección de problemas técnicos que puedan surgir con la red informática. (SYSRACKS, 2024).

Figura 14: *Patch Panels*

Fuente: (cl.rsdelivers., 2019)

II.1.2.9. Rosetas

43. Las rosetas RJ45 son las placas que se instalan en la pared o en la mesa, en cada puesto de trabajo, para permitir conectar los diferentes equipos informáticos a la red local, usando un cable Ethernet. (WIKIPEDIA, WIKIPEDIA La enciclopedia libre, 2023).

Figura 15: *Roseta Rj45*

Fuente: (kualitek, s.f.)

II.1.2.10. Puntos de acceso wifi

44. Los puntos de acceso Wifi (access points en inglés) son dispositivos hardware que crean una red de área local inalámbrica (WLAN) en oficinas y edificios, donde se pueden conectar equipos informáticos necesarios (ordenadores, impresoras, tablets, teléfonos móviles…).

45. El punto de acceso inalámbrico se conecta al router o al switch mediante un cable Ethernet, y proyecta una señal Wifi con un alcance que depende de las características de cada modelo.

Figura 16: *Puntos de acceso Wifi*

Fuente: (opensupport., s.f.)

II.1.3. Red LAN

46. Definición: Red de Área Local (LAN) (Local Área Network) Red de comunicación entre ordenadores situados en el mismo edificio o en edificios cercanos, de forma que permite a sus usuarios el intercambio de datos y la compartición de recursos. (Wikipedia, s.f.).

Figura 17: *Red Lan*

Fuente: (forum.huawei, forum.huawei, 2023)

II.1.3.1. Topologías de red.

II.1.3.1.1. Topología Bus.

47. Usa solo un cable backbone que debe terminarse en ambos extremos. Todos los hosts se conectan directamente a este backbone. Su funcionamiento es simple y es muy fácil de instalar, pero es muy sensible a problemas de tráfico, y un fallo o una rotura en el cable interrumpe todas las transmisiones. Esto hace que se dificulte el mantenimiento de la red. (Wikipedia, s.f.).

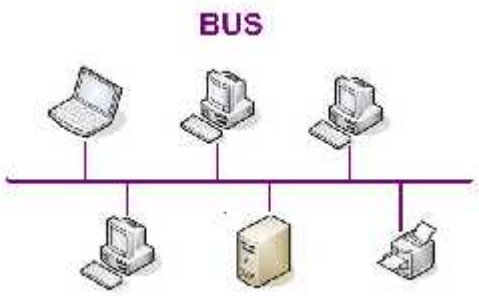


Figura 18: *Topología Bus*

Fuente: (goconqr, goconqr, 2020)

II.1.3.1.2. Topología Anillo.

48. Conecta los nodos punto a punto, formando un anillo físico y consiste en conectar varios nodos a una red que tiene una serie de repetidores. Cuando un nodo transmite información a otro, la información pasa por cada repetidor hasta llegar al nodo deseado. El problema principal de esta topología es que los repetidores son unidireccionales (siempre van en el mismo sentido). Después de pasar los datos enviados a otro nodo por dicho nodo, continúa circulando por la red hasta llegar de nuevo al nodo de origen, donde es eliminado. Esta topología no tiene problemas por la congestión de tráfico, pero si hay una rotura de un enlace, se produciría un fallo general en la red. *(Wikipedia, s.f.)*

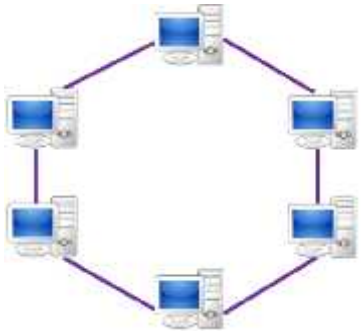


Figura 19: *Topología Anillo*

Fuente: (goconqr, goconqr, 2020)

II.1.3.1.3. Topología estrella.

49. Conecta todos los nodos con un nodo central. El nodo central conecta directamente con los nodos, enviándoles la información del nodo de origen, constituyendo una red punto a punto. Si falla un nodo, la red sigue funcionando, excepto si falla el nodo central, que las transmisiones quedan interrumpidas. (wikipedia, 2024).

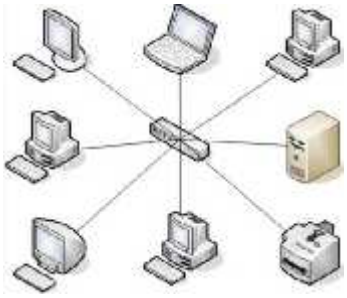


Figura 20: *Topología Estrella*

Fuente: (forum.huawei, forum.huawei, 2015)

II.1.3.1.4. Topología en estrella extendida

50. Conecta estrellas individuales entre sí mediante la conexión de concentradores (hubs) o switches. Esta topología puede extender el alcance y la cobertura de la red. (WordPress, 2017).

Figura 21: *Topología Estrella Extendida*

Fuente: (construiryadministrarred27estrella, s.f.)

II.1.3.1.5 Topología de Malla

51. Se implementa para proporcionar la mayor protección posible para evitar una interrupción del servicio. El uso de una topología de malla en los sistemas de control en red de una planta nuclear sería un ejemplo excelente. En esta topología, cada host tiene sus propias conexiones con los demás hosts. *(Wikipedia, s.f.)*

Figura 22: *Topología en Malla*

Fuente: (Locales., s.f.)

II.1.3.1.6. Topología de Árbol

52. Tiene varias terminales conectadas de forma que la red se ramifica desde un servidor base. Un fallo o rotura en el cable interrumpe las transmisiones. *(Wikipedia, s.f.).*

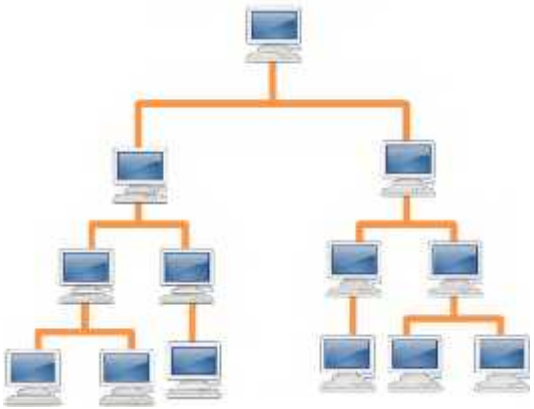


Figura 23: *Topología de árbol*

Fuente: (redesinalambricasycableadas.wordpress, 2014)

II.1.3.1.7. Topología Mixta

53. Es aquella en la que se aplica una mezcla entre alguna de las otras topologías: bus, estrella o anillo. Principalmente, las podemos encontrar dos topologías mixtas: Estrella-Bus y Estrella-Anillo. Los cables más utilizados son el cable de par trenzado, el cable coaxial y la fibra óptica. *(Wikipedia, s.f.).*

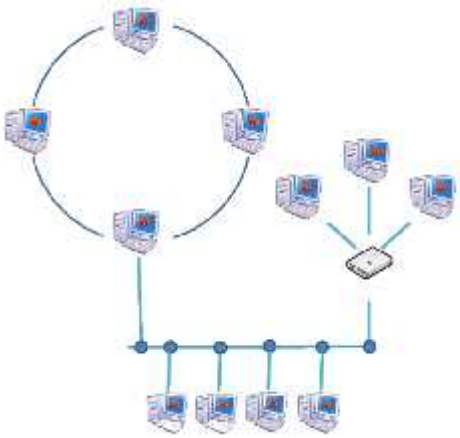


Figura 24: *Topología mixta*

Fuente: (redesybasededatoss.wordpress., s.f.)

II.1.4. Red WLAN

54. Una red de área local inalámbrica, también conocida como **WLAN** (del inglés *wireless local area network*), es una red inalámbrica de comunicación para distancias cortas y funciona mediante ondas de radio o infrarrojas. Con los rápidos avances de Internet, ya no era necesario utilizar cableado como las redes tradicionales. *(Wikipedia, s.f.).*

Figura 25: *Red WLAN*

Fuente: (Chávez, 2014)

II.1.4.1 Topología Inalámbrico

55. Las LAN inalámbricas pueden acomodar varias topologías de red. El estándar 802.11 identifica dos modos principales de topología inalámbrica: modo Ad hoc y modo Infraestructura. Tetherin o Anclaje a red también es un modo en ocasiones usado para proveer un acceso inalámbrico rápido. (Brito, 2018).

II.1.4.1.1. Modo Ad hoc

56. Es cuando dos dispositivos se conectan de forma inalámbrica de igual a igual (P2P) sin utilizar AP o routers inalámbricos. Los ejemplos incluyen clientes inalámbricos que se conectan directamente entre sí mediante Bluetooth o wifi Direct. El estándar IEEE 802.11 se refiere a una red ad hoc como un conjunto de servicios básicos independientes / Independent Basic Service Set (IBSS). (Cuellar, 2021).

Figura 26: *Modo Ad hoc*

Fuente: (Walton, ccnadesdecero, s.f.)

II.1.4.1.2. Modo infraestructura

57. Esto ocurre cuando los clientes inalámbricos se interconectan a través de un router inalámbrico o AP, como en las WLAN. Los AP se conectan a la infraestructura de red utilizando el sistema de distribución por cable, como Ethernet.

Figura 27: *Modo Infraestructura*

Fuente: (Walton, ccnadesdecero, 2021)

II.1.4.2. Estándares IEEE 802.11

A lo largo del camino, la Wi-Fi Alliance desarrolló una convención de nomenclatura ("Wi-Fi #") para ayudar al público en general a distinguir mejor entre las distintas implementaciones de IEEE 802.11:

- IEEE 802.11™ es el estándar pionero de Wi-Fi de 2,4 GHz mencionado anteriormente, de 1997, y aún se conoce con esa nomenclatura. Este estándar y sus modificaciones posteriores constituyen la base de las redes inalámbricas Wi-Fi y representan los protocolos de redes informáticas inalámbricas más utilizados a nivel mundial. (IEEE, 2023).
- IEEE 802.11b™, o Wi-Fi 1, se introdujo en el mercado en 1999 con el anuncio de Apple. También operaba a 2,4 GHz, pero para reducir la interferencia de hornos microondas, teléfonos inalámbricos, monitores de bebés y otras fuentes, y para lograr velocidades de datos más altas, incorporó esquemas de modulación denominados modulación de espectro ensanchado por secuencia directa/codificación complementaria por código (DSSS/CCK). Wi-Fi 1 permitió comunicaciones inalámbricas a distancias de unos 38 m en interiores y unos 140 m en exteriores. (IEEE, 2023).
- IEEE 802.11a™, o Wi-Fi 2, también introducido en 1999, fue el sucesor de IEEE 802.11b. Fue la primera especificación Wi-Fi en incorporar un esquema de modulación multiportadora (OFDM) para soportar altas velocidades de datos, a diferencia del diseño de portadora única de Wi-Fi 1. Admitía el funcionamiento a 5 GHz y su ancho de banda de 20 MHz admitía múltiples velocidades de datos. (IEEE, 2023).

- IEEE 802.11g™, o Wi-Fi 3, se introdujo en 2003. Permitió velocidades de datos más rápidas, de hasta 54 Mbit/s, en la misma banda de frecuencia de 2,4 GHz que IEEE 802.11b, gracias a un esquema de modulación multiportadora OFDM y otras mejoras. Esto resultó atractivo para el mercado general, ya que los dispositivos de 2,4 GHz eran más económicos que los de 5 GHz. (IEEE, 2023).
- IEEE 802.11n™, o Wi-Fi 4, se introdujo en 2009 para ofrecer compatibilidad con las bandas de frecuencia de 2,4 GHz y 5 GHz, con velocidades de datos de hasta 600 Mbit/s, múltiples canales dentro de cada banda y otras características. El rendimiento de datos de IEEE 802.11n permitió el uso de redes WLAN en lugar de redes cableadas, una característica importante que posibilitó nuevos casos de uso y redujo los costos operativos para usuarios finales y organizaciones de TI. (IEEE, 2023).
- IEEE 802.11ac™, o Wi-Fi 5, se introdujo en 2013 para soportar velocidades de datos de hasta 3,5 Gbit/s, con un ancho de banda aún mayor, canales adicionales, mejor modulación y otras características. Fue el primer estándar Wi-Fi que permitió el uso de la tecnología MIMO (múltiples entradas/múltiples salidas), lo que permitió usar múltiples antenas tanto en dispositivos emisores como receptores para reducir errores y aumentar la velocidad. (IEEE, 2023).

II.1.4.3. Seguridad en redes WLAN

58. Los protocolos de cifrado analizan los principales métodos de protección para redes inalámbricas: WEP (obsoleto), WPA, WPA2 y WPA3, además del uso de autenticación mediante RADIUS, certificados digitales o portales cautivos. Este punto es crucial en el diseño de seguridad de red.

II.1.4.3.1 Protocolos de cifrado: WEP, WPA, WPA2, WPA3

59. Protocolo WEP

WEP, desarrollado en 1997, fue diseñado para proteger las redes inalámbricas mediante cifrado y restricción de acceso. Sin embargo, su dependencia del cifrado RC4 inseguro y la autenticación de clave compartida hizo que las redes fueran vulnerables a ataques. Si bien WEP inicialmente proporcionaba un cifrado similar al de las redes cableadas, sus vulnerabilidades fueron ampliamente explotadas por hackers, lo que lo volvió obsoleto. (Maine, 2024).

La discontinuación del protocolo generó alternativas más robustas, como WPA (Acceso Protegido Wi-Fi). A pesar de sus defectos, la simplicidad y la amplia adopción de WEP inicialmente llamaron la atención, pero sus vulnerabilidades inherentes finalmente eclipsaron sus beneficios, lo que resaltó la importancia de actualizar constantemente los estándares de seguridad inalámbrica. (Maine, 2024).

Protocolo WPA

WPA, lanzado en 2003, surgió como un sucesor eficaz de WEP, corrigiendo sus deficiencias. WPA utiliza el cifrado del protocolo de integridad de clave temporal (TKIP) para mejorar la gestión de claves y las comprobaciones de integridad. Ofrece dos modos: WPA-Personal para redes domésticas y WPA-Enterprise para empresas que utilizan servidores RADIUS. (Maine, 2024).

El cifrado de 128 bits de WPA ofrece mayor protección que los estándares de cifrado más débiles de WEP; sin embargo, sigue siendo comparativamente más débil que WPA2, lo que genera posibles fallos y problemas de compatibilidad. Además, la adopción de WPA puede requerir modificaciones de hardware, lo que supone un problema para los usuarios con equipos antiguos. (Maine, 2024).

Protocolo WPA2

WPA2, lanzado en 2004, es el estándar de seguridad inalámbrica más popular que utiliza la técnica de cifrado AES para ofrecer una seguridad robusta. Sus ventajas sobre WPA incluyen una mejor administración y una menor vulnerabilidad a ataques. WPA2 se ha adoptado ampliamente como estándar de la industria, lo que garantiza la interoperabilidad de los dispositivos. (Maine, 2024).

Sin embargo, vulnerabilidades como el ataque de reinstalación de clave (KRACK) constituyen un riesgo de seguridad. Si bien es apropiado para la mayoría de las redes domésticas, surgen dificultades en entornos empresariales, donde los ataques sofisticados son más comunes. Además, los equipos antiguos sin compatibilidad con WPA2 pueden requerir actualizaciones. A pesar de estos problemas, WPA2 sigue siendo fundamental para la seguridad de las redes inalámbricas, pero se están realizando esfuerzos continuos para abordar las crecientes amenazas y vulnerabilidades. (Maine, 2024).

Protocolo WPA3

WPA3, lanzado en 2018, ofrece mayor cifrado, protección contra ataques de fuerza bruta por diccionario y una configuración más sencilla de dispositivos mediante Wi-Fi Easy Connect. A pesar de estas mejoras, su aceptación generalizada es lenta. WPA3 se presenta en tres tipos: WPA3-Personal para uso doméstico, WPA3-Enterprise para entornos organizacionales y Wi-Fi Enhanced Open para redes sin protección por contraseña. (Maine, 2024).

Si bien mejora la seguridad general de la red, presenta desventajas como la complejidad de implementación, la baja adopción por parte de los usuarios y problemas de compatibilidad con dispositivos y equipos más antiguos. A pesar de sus beneficios, la implementación completa de WPA3 aún no se ha producido, lo que indica una transición lenta de los protocolos de seguridad antiguos a este estándar más moderno. (Maine, 2024).

II.1.4.3.2 Autenticación: 802.1X, RADIUS, portal cautivo

60. El estándar IEEE 802.1X para el control de acceso a la red basado en puertos y protege las LAN Ethernet del acceso no autorizado de usuarios. Bloquea todo el tráfico hacia y desde un suplicante (cliente) en la interfaz hasta que las credenciales del suplicante se presenten y coincidan en el servidor de autenticación (un servidor RADIUS). Cuando se autentica el suplicante, el conmutador deja de bloquear el acceso y abre la interfaz al solicitante. Lea este tema para obtener más información.

La autenticación 802.1X funciona mediante el uso de una entidad de acceso al puerto del autenticador (el conmutador) para bloquear el tráfico de entrada de un suplicante (dispositivo final) en el puerto hasta que las credenciales del solicitante se presenten y coincidan en el servidor de autenticación (un servidor RADIUS). Cuando se autentica, el conmutador deja de bloquear el tráfico y abre el puerto al solicitante. (NETWORKS, 2025).

II.1.4.4. Control de acceso y gestión de usuarios

II.1.4.4.1. Filtros MAC

El filtro MAC es una tecnología utilizada en routers inalámbricos para evitar el acceso no autorizado a las redes. La dirección MAC es un identificador único que se asigna a cada dispositivo en una red. Un router inalámbrico utiliza una dirección MAC para identificar el dispositivo y determinar a qué red debe conectarse. (cudy, 2024).

El acceso inalámbrico se puede filtrar utilizando las direcciones de Control de acceso a medios (MAC) de los dispositivos inalámbricos que transmiten dentro de su red inalámbrica. Puede permitir o impedir que computadoras y dispositivos inalámbricos específicos accedan a su Wi-Fi. Este artículo lo guiará sobre cómo configurar un filtro MAC inalámbrico, permitiendo o impidiendo el acceso a su red inalámbrica. (belkin, s.f.).

II.1.4.4.2. VLAN’s dinámicas

La configuración de una WLAN mediante VLAN dinámicas permite asignar diferentes usuarios a diferentes VLAN en función de la contraseña proporcionada al conectarse al SSID. (JUNIPER, JUNIPER driven by mist AI, 2020)

Se necesita un Servidor RADIUS con nombre de usuario/contraseña y asignaciones de VLAN configuradas, además de un Conmutador conectado al AP configurado con las VLAN correctas.

Las interfaces de suscriptor VLAN dinámicas que se crean con base en el identificador de línea de acceso (ALI) son útiles en configuraciones con una combinación de sesiones de suscriptores DHCP y PPPoE en el mismo hogar. (JUNIPER, JUNIPER NETWORKS, 2023).

Cuando usa VLAN de servicio (S-VLAN) para llevar un servicio a muchos suscriptores (1:N), cada suscriptor u hogar puede tener diferentes tipos de tráfico en varias VLAN. El nodo de acceso incrusta la ALI en paquetes de control DHCP y PPPoE. Para identificar todas las sesiones de suscriptor para un suscriptor individual o un hogar, puede usar el ALI. La capacidad de identificar de manera única a los suscriptores simplifica la aplicación de servicios, como cos y filtros, a suscriptores individuales u hogares. (JUNIPER, JUNIPER NETWORKS, 2023).

Dado que una S-VLAN corresponde a un servicio en lugar de a un suscriptor individual, el enrutador usa la ALI en paquetes de control DHCP y PPPoE en lugar de la encapsulación de VLAN para identificar de manera única a los suscriptores y facilitar la aplicación de servicios basados en suscriptores. Las ALIs incluyen el identificador de circuito del agente (ACI) y el identificador remoto de agente (ARI). (JUNIPER, JUNIPER NETWORKS, 2023).

II.1.4.4.3. QoS y priorización de tráfico

Para minimizar la posibilidad de que se descarte el tráfico de mayor prioridad cuando se produce una congestión, puede habilitar y configurar el sistema VELOS para que priorice el tráfico de mayor prioridad sobre otros tipos de tráfico. La función de calidad de servicio (QoS) permite configurar la ponderación de los tipos de paquetes, según el campo 802.1p o DSCP, para garantizar que un porcentaje de un tipo de tráfico determinado se procese y no se descarte cuando haya un alto volumen de tráfico. (F5, s.f.).

Esta función habilita las colas de QoS, también llamadas prioridades de tráfico. Hay ocho colas de QoS por puerto en los sistemas VELOS. Se pueden asignar valores 802.1p o DSCP a cada cola, de modo que, al entrar un paquete, se clasifique en una de las colas según su valor 802.1p o DSCP. Posteriormente, se puede asignar un porcentaje de ponderación a cada cola y, al salir, el sistema garantiza que el tráfico saliente se componga según el porcentaje asignado a cada cola. Esta medición solo se realiza cuando el sistema está congestionado, y el tráfico no se descarta cuando no está congestionado. (F5, s.f.).

II.1.4.5. Ventajas y desventajas de las WLAN

Ventajas de la red de área local inalámbrica (WLAN):

- Es un tipo de comunicación confiable.
- Como WLAN reduce los cables físicos, es una forma de comunicación versátil.
- La WLAN también reduce el valor de propiedad.
- Es más fácil destacar o eliminar una estación de trabajo.
- Proporciona una alta velocidad gracias a la cobertura de área pequeña.
- También moverás la estación de trabajo manteniendo la conectividad.
- Para su propagación no se requiere la luz solar directa.

- La dirección de conectividad suele ser cualquier lugar, es decir, conectarás dispositivos en cualquier dirección a menos que estén dentro del alcance del punto de acceso.
- Fácil instalación y no necesitará cables adicionales para la instalación.
- Las redes WLAN suelen ser útiles en situaciones de desastre, como terremotos e incendios. Una red inalámbrica puede conectar a las personas en cualquier desastre.
- Es económico debido al área pequeña de acceso.
- La cantidad de energía que requiere es mayor ya que utiliza transmisor; por lo tanto, la duración de la batería de las computadoras portátiles puede verse afectada. (geeksforgeeks, 2022).

Desventajas de la red de área local inalámbrica (WLAN):

- WLAN requiere licencia.
- Es un área limitada para esconderse.
- Las agencias gubernamentales pueden controlar el flujo de señales de WLAN y también pueden limitarlo si es necesario. Esto afectará la transferencia de datos desde los dispositivos conectados a la web.
- Si la cantidad de dispositivos conectados aumenta, la tasa de transferencia de datos disminuye.
- La WLAN utiliza una frecuencia que puede interferir con otros dispositivos que también utilizan esta frecuencia.
- Si hay lluvia o tormentas la comunicación puede interferir.
- Debido a la baja seguridad, los atacantes pueden obtener acceso a los datos transmitidos.

- Las señales también podrían verse afectadas por el medio ambiente en comparación con el uso de fibra óptica.
- Las radiaciones de las redes WLAN suelen ser perjudiciales para el medio ambiente.
- La WLAN es más cara que los cables y concentradores porque se trata de puntos de acceso.
- Las señales pueden obtenerse de las señales más cercanas mediante puntos de acceso.
- Es necesario variar la tarjeta de red y el punto de acceso cuando cambia el estándar.
- Sigue siendo necesario un cable LAN que actúa como columna vertebral de la WLAN.
- La velocidad de transferencia de datos es menor que la de la conexión por cable porque la WLAN utiliza mucha frecuencia.
- Las posibilidades de errores son altas.
- La comunicación no es segura y usuarios no autorizados pueden acceder a ella. (geeksforgeeks, 2022).

II.1.5. Cableado Estructurado

61. El cableado estructurado se define como el conjunto de cables, conectores, canalizaciones y dispositivos que componen la infraestructura de telecomunicaciones interior de un edificio o recinto.

62. Su función es transportar señales desde unos dispositivos (emisores) a otros (receptores) con el objetivo de crear la red de área local del mismo.

63. Esta estructura contiene una combinación de cables trenzados (UTP/STP/FTP), fibras ópticas (FO) y/o cables coaxiales que deben cumplir ciertos estándares universales para que puedan ser fácilmente entendidos por instaladores y administradores de redes. (WIKIPEDIA, WIKIPEDIA La enciclopedia libre, 2023).

II.1.5.1. Elementos del Cableado Estructurado

64. A la hora de realizar una instalación de cableado estructurado se debe de tener en cuenta los elementos a conectar, las características y el diseño del lugar en el que se va a instalar y el crecimiento futuro de dicha instalación, por lo que la cantidad de cables a colocar ha de satisfacer necesidades de ampliación futuras.

65. Los principales elementos del cableado estructurado son:

II.1.5.1.1. Cableado horizontal

66. Se refiere al cableado o sistema de distribución que corre horizontalmente entre el techo y el suelo, se compone de dos elementos básicos: rutas y espacios horizontales que se encargan de, además de distribuir y soportar el cableado horizontal, conectar el hardware entre la salida del área de trabajo y el cuarto de telecomunicaciones, según se define en la norma EIA/TIA 568.

67. La longitud máxima de cable desde el punto de terminación en el cuarto de telecomunicaciones hasta la terminación en la toma del área de trabajo no puede superar los 90 metros. Esta distancia máxima de cableado horizontal de 90 metros se denomina enlace permanente, porque está instalada en la estructura del edificio. Los medios horizontales se ejecutan desde un patch panel en el cuarto de telecomunicaciones a un Jack de pared en cada área de trabajo. (ASCENTOPTICS, 2024)

68. Según el tipo de categorías se identifica el tipo de cable y su función principal.

Categoría	**Máxima velocidad (Teórica)**	**Ancho de banda (MHz)**	**Aplicaciones**	**Notas**

Cat. 1	—	< 1 MHz	Líneas telefónicas y módem de banda ancha.	No descrito en las recomendaciones del EIA/TIA. No es adecuado para sistemas modernos.
Cat. 2	—	4 MHz	Cable para conexión de antiguos terminales como el IBM 3270.	No descrito en las recomendaciones del EIA/TIA. No es adecuado para sistemas modernos.
Cat. 3	10 Mbps	16 Mbps Clase C.	10BASE-T and 100BASE-T4 Ethernet	Descrito en la norma EIA/TIA-568. No es adecuado para transmisión de datos mayor a 16 Mbit/s. Usado en telefonía.
Cat. 4	20 Mbps	20 MHz	16 Mbit/s Token Ring	No es usado comúnmente.
Cat. 5	100 Mbps	100 MHz Clase D	10BASE-T, 100BASE-TX y 1000BASE-T Ethernet	Usado en conexiones Ethernet entre dispositivos de red
Cat. 5 e	1000 Mbps	100 MHz Clase D	100BASE-TX y 1000BASE-T Ethernet	Mejora del cable de categoría 5.

Cat. 6	1000 Mbps	250 MHz Clase E.	1000BASE-T Ethernet	Transmite a 1000 Mbps. Cable más comúnmente instalado en Finlandia según la norma SFS-EN 50173-1.
Cat. 6a	10 000 Mbps	250 MHz (500 MHz según otras fuentes) Clase E	10GBASE-T Ethernet	Estándar mejorado probado a 500 MHz. Puede extenderse hasta 100 metros. Estandarizado según las normas ISO/IEC 11801, segunda edición (2008) y ANSI/TIA-568-C.1 (2009).
Cat. 7	10 000 Mbps	600 MHz, Clase F	Para servicios de telefonía, televisión por cable y Ethernet 1000BASE-T en el mismo cable.	Cable blindado bajo estándar ISO/IEC 11801, pero no reconocido por EIA/TIA.
Cat. 7a	10 000 Mbps	1000 MHz, Clase F	Para servicios de telefonía, televisión por cable y Ethernet	Cable S/FTP (pares blindados, cable blindado trenzado) de 4 pares, bajo el estándar ISO/IEC

			1000BASE-T en el mismo cable.	11801, pero no reconocido por EIA/TIA.
Cat. 8	40.000 Mbps	2000 MHz	40 GBASE-T Ethernet o 1000BASE-T para servicios de telefonía, televisión por cable y Ethernet en el mismo cable.	Cable S/FTP (pares blindados, cable blindado trenzado) de 4 pares. Descrito por las normas ANSI/TIA-568-C.2-1 e ISO/IEC 11801-1:2017
Cat. 9	—	25000 MHz	Norma en creación por la UE.	Cable S/FTP (pares blindados, cable blindado trenzado) de 8 pares con Mylar y poliamida.
Cat. 10	—	75000 MHz	Norma en creación por la G.E.R.A. (RELATIONSHIP BETWEEN COMPANIES ANONYMA G) e IEEE.[*cita requerida*]	

Tabla 4 *Categorías de cable UTP*

Fuente: Elaboración propia

II.1.5.1.2. Cableado vertical

69. También conocido como backbone o cableado troncal, proporciona las interconexiones entre de entrada y servicios del edificio, cuartos de equipos y cuartos de telecomunicaciones.

70. Este cableado es el encargado de realizar la conexión vertical entre los diferentes pisos de un edificio, estableciendo los medios de transmisión, puntos principales e intermedios de conexión cruzada y terminaciones mecánicas necesarias.

71. La norma EIA/TIA 568 prevé la necesidad de ubicar la transmisión de cableado vertical a horizontal, en habitaciones independientes, llamadas armarios de telecomunicaciones, al menos una por piso. (COMPUhelp, 2023).

72. Los tipos de cables que se utilizan generalmente para este tipo de cableado son:

- Multipar UTO y STP
- Fibra Óptica Multimodo y Monomodo
- Las distancias máximas para transmitir vos de este tipo de cables son:
- UTP 800 metros
- STP 700 metros
- Fibra MM 62.5/125um 2000 metros.

II.1.5.1.3. Cuarto de comunicaciones

73. Se conoce así a la sala en la que se alojan y centralizan todos los elementos que componen el sistema de telecomunicaciones: los cables, accesorios de conexión, dispositivos de protección y demás equipos necesarios para conectar el edificio a los servicios externos. (Llamas, 2023)

74. Estos cuartos se deben diseñar de acuerdo con la norma EIA/TIA-569.

II.1.5.2. Organismos y normas

II. 1.5.2.1. Organismos

75. Actualmente, existen diversos organismos implicados en la elaboración de los diferentes estándares de cableado estructurado. Estos organismos son:

76. **TIA** (Telecommunications Industry Association)**,** se fundó en 1985 después de la separación del monopolio de AT&T. Se encarga de desarrollar normas de cableado industrial para varios productos de las telecomunicaciones.

77. **ANSI** (American National Standards Institute)**,** se trata de una organización sin ánimo de lucro que supervisa el desarrollo de estándares para productos, servicios, procesos y sistemas en los Estados Unidos. ANSI es miembro de la Comisión Electrotécnica Internacional (IEC) y de la Organización Internacional para la Estandarización (ISO). ANSI/TIA desarrollan en conjunto los estándares para EE. UU.

78. **EIA** (Electronic Industries Alliance), es una organización compuesta por la asociación de las compañías electrónicas y de alta tecnología de los EE. UU. cuya misión es promover el desarrollo de mercado y la competitividad de la industria de alta tecnología.

79. **ISO** (International Standards Organization), es una organización no gubernamental a nivel mundial. Se encarga de desarrollar los estándares internacionales y tiene una red de representantes de estándares nacionales. Los estándares nacionales son miembros de ISO y representan a ISO en sus países.

80. **IEEE** (Instituto de Ingenieros Eléctricos y de Electrónica), es una asociación de ingenieros a nivel mundial que se dedica a establecer normativas con relación a áreas técnicas.

II.1.5.2.2. Normas

81. ANSI/TIA/EIA-568-B: Cableado de Telecomunicaciones en Edificios Comerciales sobre cómo instalar el cableado.

82. **TIA/EIA 568-B1,** Requerimientos generales.

83. **TIA/EIA 568-B2,** Componentes de cableado mediante par trenzado balanceado.

84. **TIA/EIA 568-B3**, componentes de cableado, fibra óptica.

85. **ANSI/TIA/EIA-569-A**, Normas de Recorridos y Espacios de Telecomunicaciones en edificios comerciales sobre cómo enrutar el cableado.

86. **ANSI/TIA/EIA-570-A**, Normas de Infraestructura Residencial de Telecomunicaciones.

87. **ANSI/TIA/EIA-606-A,** Normas de Administración de Infraestructura de Telecomunicaciones en edificios comerciales.

88. **ANSI/TIA/EIA-607,** Requerimientos para instalaciones de sistemas de puesta a tierra de Telecomunicaciones en Edificios Comerciales.

89. **ANSI/TIA/EIA-758,** Norma Cliente-Propietario de cableado de Planta Externa de Telecomunicaciones.

II.1.5.3. Fibra Óptica

II.1.5.3.1. Introducción a la Fibra Óptica

90. La fibra óptica es un medio de transmisión de datos que utiliza luz pulsada para enviar información a través de fibras delgadas de vidrio o plástico. Es ampliamente utilizada en redes de telecomunicaciones debido a sus ventajas en términos de velocidad, capacidad y resistencia a interferencias electromagnéticas. (WIKIPEDIA, WIKIPEDIA La enciclopedia libre, 2024).

II.1.5.3.2. Componentes de la Fibra Óptica

91. Núcleo:

92. Es el núcleo central de la fibra donde se propaga la luz. Está compuesto por vidrio o plástico de alta pureza y tiene un índice de refracción mayor que el revestimiento para facilitar la reflexión interna total.

93. Revestimiento:

94. Capa que rodea al núcleo y tiene un índice de refracción menor que el núcleo. Ayuda a guiar la luz a lo largo del núcleo mediante reflexión interna total y protege el núcleo de daños físicos.

95. Cubierta:

96. Capa externa que protege la fibra contra daños mecánicos y ambientales. Puede ser de diferentes materiales como polietileno o PVC. (Noori, 2024).

II.1.5.3.3. Principios de Funcionamiento

97. Reflexión Interna Total:

98. Fenómeno óptico por el cual la luz se refleja dentro del núcleo de la fibra en ángulos específicos, permitiendo que la señal óptica se transmita a largas distancias sin degradación significativa.

99. Modulación de luz:

100. Proceso mediante el cual se modula la luz para transportar información. Las señales eléctricas se convierten en señales ópticas mediante diodos emisores de luz (LED) o láseres, y viceversa en el receptor. (SLIDESHARE, 2019).

II. 1.5.3.4. Tipos de Fibra Óptica

101. Fibra Monomodo (Single Mode):

102. Diseñada para transmitir un solo modo de luz, adecuada para largas distancias y altas velocidades. Tiene un núcleo más delgado (~9 micrómetros).

103. Fibra Multimodo (Multimode):

104. Permite la transmisión de múltiples modos de luz, adecuada para distancias más cortas y aplicaciones LAN. Tiene un núcleo más grueso (~50-62.5 micrómetros). (Telefonica, 2024).

II.1.5.3.5. Aplicaciones de la Fibra Óptica

105. **Telecomunicaciones:** Redes de banda ancha, transmisión de voz y datos de alta velocidad.

106. **Redes Corporativas:** Conexiones entre edificios, centros de datos y campus universitarios.

107. **Aplicaciones especiales:** Medicina (endoscopios), sensores industriales, comunicación submarina.

Capítulo III Componentes

III.1. Componente 1:

Red LAN de EMTAGAS rediseñado

III.1. Componente 1: Red LAN de EMTAGAS rediseñado

III.1.1. Análisis de Requerimientos

III.1.1.1. Analizar metas del negocio

III.1.1.1.1 Visión

108. Fue creada como una Empresa Pública de Servicios y de carácter social; por lo tanto, es una Empresa sin fines de lucro.

109. La política y el objetivo fundamental de EMTAGAS es que toda familia que habita en el Departamento de Tarija cuente con el servicio de gas domiciliario, con el Plan Gas Para Todos (EMTAGAS,2021).

III.1.1.1.2. Misión

110. Ser una empresa eficiente, eficaz, moderna y transparente, líder en el desarrollo del sector energético, a través de la integración del Departamento de Tarja mediante el uso y consumo del gas natural, brindando un servicio continuo y de calidad a las familias, con el compromiso y esfuerzo de sus recursos humanos. (EMTAGAS,2021).

III.1.1.2. Analizar metas técnicas

111. Con las metas técnicas se busca un diseño de red utilizando VLANs y fibra óptica con la finalidad de mejorar la red de datos de la empresa EMTAGAS. Para el diseño de red propuesto, se tomaron en cuenta la seguridad, rendimiento, escalabilidad, flexibilidad, adaptabilidad, gestión y administración de la red.

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

III.1.1.2.1. Seguridad

113. **Firewall:** Es necesario que la red de datos y los servicios de la empresa EMTAGAS se mantengan a través de un sistema de seguridad, evitando que usuarios no autorizados provenientes

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

114. **Diseño y seguridad del cableado estructurado:** Además de la protección lógica proporcionada por los firewalls, se propone mejorar la seguridad física de la infraestructura de red mediante un diseño robusto de cableado estructurado. Esto incluye el uso de materiales resistentes y métodos de instalación que minimizan el riesgo de interferencia y manipulación no autorizada. Asimismo, se considera la propuesta de implementar políticas de gestión de acceso físico y de control de ingreso a los cuartos de comunicación IDF y MDF, donde se centraliza y distribuye el tráfico de red.

115. **Mejora de la seguridad en los cuartos de comunicación IDF y MDF:** Los cuartos de comunicación IDF y MDF representan puntos críticos de la infraestructura de red, donde se encuentran concentrados los equipos y conexiones fundamentales. Para fortalecer la seguridad en estos puntos, se propone implementar medidas adicionales como cámaras de vigilancia, sistemas de control de acceso con tarjetas de identificación, cerraduras biométricas y sensores de movimientos y contra incendios. Estas medidas no solo protegen los activos físicos, sino que también aseguran que solo personal autorizado pueda acceder y manipular los componentes de red esenciales.

III.1.1.2.2. Rendimiento y escalabilidad

116. El objetivo principal en esta área del proyecto es mejorar tanto el rendimiento actual como la capacidad de adaptación futura de la red LAN de EMTAGAS, asegurando que pueda satisfacer las demandas crecientes de datos y aplicaciones en un entorno empresarial dinámico.

117. **Aumento de la velocidad de transferencia de datos:** Se busca incrementar significativamente la velocidad de transferencia de datos dentro de la red LAN para mejorar la eficiencia operativa y la experiencia de los trabajadores de EMTAGAS. Esto implica la evaluación o

análisis, y posible actualización de los equipos de red, como switches y routers, para soportar velocidades más altas y tecnologías avanzadas de transmisión de datos.

118. **Propuesta de implementación de fibra óptica:** Una medida clave para mejorar la capacidad de ancho de banda y la fiabilidad de la red es la implementación de tecnología de fibra óptica. Esta tecnología permite velocidades de transmisión mucho más rápidas que el cableado tradicional de cobre, lo que es crucial para soportar aplicaciones intensivas en datos y garantizar tiempos de respuesta rápidos y consistentes.

119. **Segmentación de la red mediante VLANs:** Para optimizar el rendimiento y la gestión de tráfico, se propone la implementación de VLANs (Virtual Local Area Networks). Estas VLANs permiten segmentar la red lógicamente, agrupando usuarios y recursos de manera lógica y eficiente. Esto no solo mejora la seguridad y la administración de la red, sino que también optimiza el flujo de datos al reducir el tráfico innecesario y mejorar la calidad del servicio (QoS) para aplicaciones críticas.

III.1.1.2.3. Gestión de la red

120. **Políticas de calidad de servicio (QoS):** Se establecerán políticas de QoS para priorizar el tráfico de red según las necesidades del negocio. Esto asegura que aplicaciones críticas como VoIP y videoconferencia tengan prioridad en el ancho de banda, garantizando una experiencia de usuario consistente y de alta calidad.

III.1.1.3. Analizar red existente

121. Para el análisis de la red actual de la empresa EMTAGAS se realizó una visita a la empresa con una entrevista al encargado del área de sistemas y preguntando sobre el funcionamiento de la red, gracias a la entrevista se obtuvo información de la red actual de datos, la empresa no contiene exactamente toda la documentación de las IP de la empresa. En cuanto a la seguridad, no tienen una segmentación de VLAN, ya que en la empresa trabajan con cuentas bancarias.

122. La empresa EMTAGAS cuenta con la banda ancha de la empresa es de 100 Mbps dedicado. Este servicio lo obtiene de Entel con fibra óptica hasta el TI con una suma de pago de Bs 7.900 mensual. Cabe mencionar que no tienen una norma de cableado estructurado. La empresa usa cualquier tipo de cable UTP y de distintas categorías como ser 6A y 5E.

III.1.1.3.1. Estructura de la Red Actual

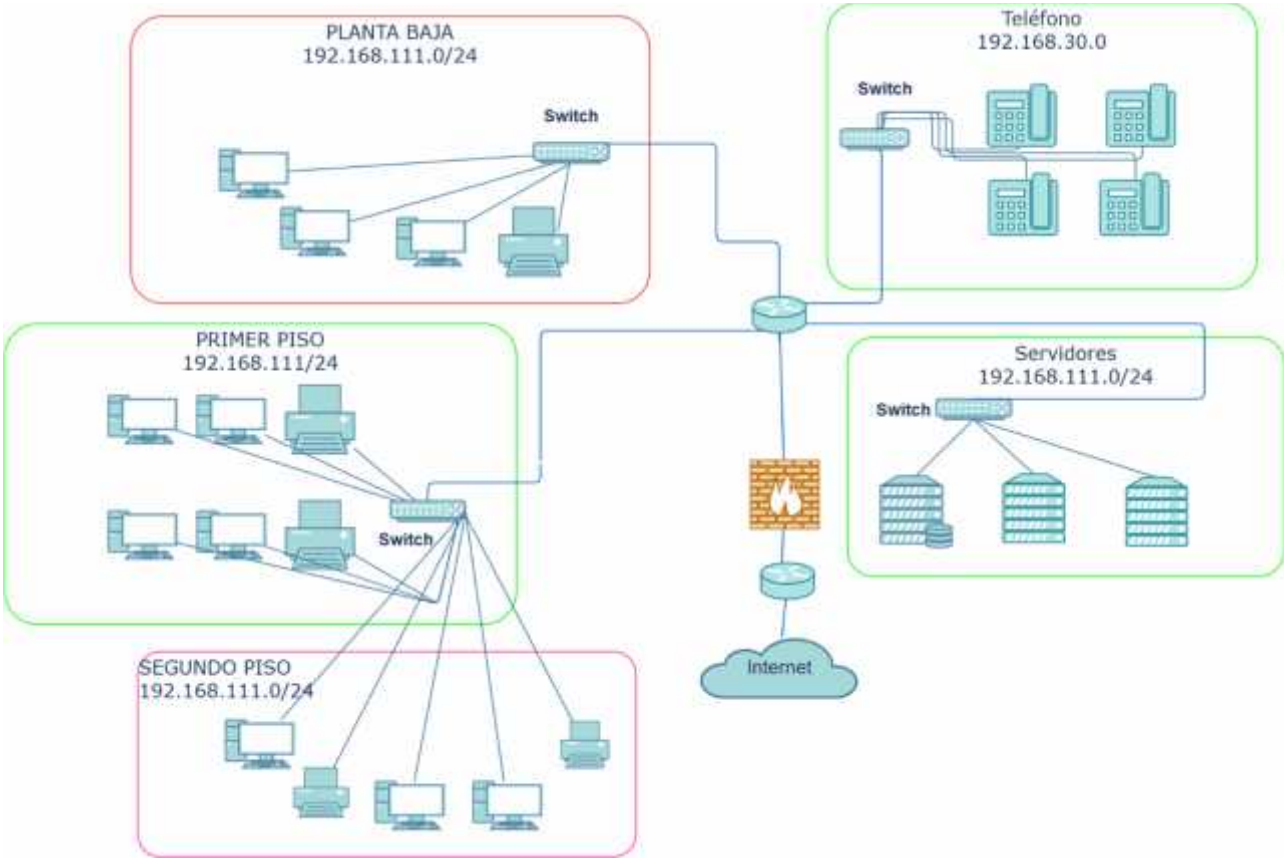


Figura 28: *Estructura de red actual de EMTAGAS*

Fuente: Elaboración propia

123. La figura proporciona una visión clara de cómo se estructuran los componentes de la red de EMTAGAS, se muestra la cantidad de equipos de red que están en uso y la forma en la que se conectan.

124. EMTAGAS para el vínculo entre pisos usa cable UTP cat 6A y UTP cat 5E, la red actual se inicia desde el router del proveedor de Entel el cual brinda el servicio de internet de 100Mbps, que es distribuida por todos los pisos del edificio principal de EMTAGAS.

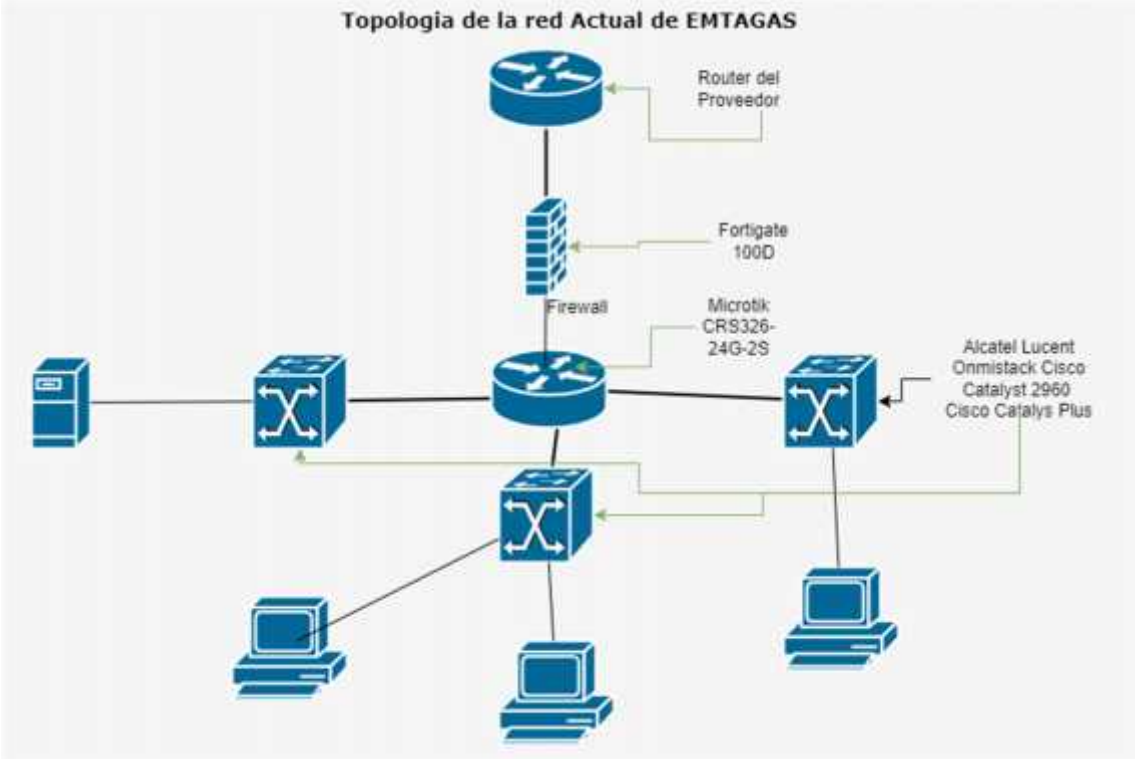


Figura 29: *Topología de red actual de EMTAGAS*

Fuente: Elaboración propia

125. Con el crecimiento de la institución y la expansión de algunas oficinas, ha surgido la necesidad de equipos de switches y otros equipos, por el cual la empresa cuenta con un diseño lógico de topología cascada, donde los dispositivos dependen uno del otro, el núcleo de esta topología se encuentra ubicada en el primer piso, donde se encuentra los dispositivos críticos para la red.

III.1.1.3.2. Especificación de los equipos actuales de la red

126. La infraestructura incluye una variedad de dispositivos, como router, switches, servidor, telefonía ip, firewall.

127. Tabla de los equipos de comunicación de la red actual de la empresa

Nro.	Equipo	Modelo	Cantidad
1	Firewall	Fortinet 100D	1
2	Router/Switch	Microtik CRS326-246-25+RM	
3	Switch	Cisco Catalyst 2960 serie	1
4	Switch	Cisco Catalyst plus series si-poe-8	1
5	Switch	Alcatel Lucent omnistack LS6248P	3
6	Router	Microtik hex series	1
7	Router	Cisco 890 series	1
8	Servidor	HP dl38065	1
9	Servidor	Dell poweredge VRTX	1

Tabla 5 *Especificación de equipos de la red de EMTAGAS*

Fuente: Elaboración propia

128. Los equipos de videovigilancia, telefonía y otros de la empresa EMTAGAS.

Nro.	Equipo	Modelo	Cantidad
1	Central	Central IP Alcatel lucent omnipex Enterprice	1

2	UPS	UPS rackeable	1
3	Dvr	Dahua 3204 hf 32 canales	1

Tabla 6 *Equipos de vigilancia de la red actual de EMTAGAS*

Fuente: Elaboración propia

III.1.1.3.3. Tabla de direccionamientos de la red actual

129. Con la información recolectada y la entrevista al encargado de sistemas, nos dio la información de la tabla de la red actual, ya que todas las IP son estáticas en la siguiente tabla.

130. Tabla genérica de las direcciones de red actual de EMTAGAS.

Nro.	Dispositivos	Dirección de la red	Mascara	Gateway	Host
1	Usuarios	192.168.111.0	255.255.255.0	192.168.111.1	10-70
2	Servidores	192.168.111.0	255.255.255.0	192.168.111.1	10-20
3	Teléfono	192.168.30.0	255.255.255.0	192.168.30.1	10-50

Tabla 7 *Tabla de expresión genérica del direccionamiento de la red actual de EMTAGAS*

Fuente: Elaboración propia

131. Tabla de direcciones asignada de manera estática.

N°	APELLIDOS Y NOMBRES	CARGO	RED
RED LOCAL EMTAGAS			IP
1	Leyton Romero Fernando	Gerente General	192,168,111,111
2	Espinoza Heredia Betty Alcira	Jefe Auditoría Interna	192,168,111,112

3	Vargas Fernandez America	Auxiliar de Auditoría Interna	192,168,111,113
4	Del Carpio Silos Mateo Wilfredo	Jefe de Planificación	192,168,111,114
5	Angola Vidaurre Elizabeth	Secretaria Gerencia General	192,168,111,115
6	Lisarazu Velasquez Blanca Rosio	Director Jurídico	192,168,111,116
7		Asesor Legal	192,168,111,117
8	Condori Choque Zulma Jhovanna	Asesor Legal	192,168,111,118
9	Uriburu Tirao Francis Clara	Auxiliar Legal	192,168,111,119
10	Morales Paz Susana Lily	Secretaria Jurídica	192,168,111,120
11	Vargas Rivera Jose Luis	Director Técnico	192,168,111,121
12	Figueroa Olarte Maria Cristina	Enc. De Obras Civiles	192,168,111,122
13		Técnico Proyectista	192,168,111,123
14	Figueroa Espinoza Yamil	Técnico en Cartografía	192,168,111,124
15	fotocopiadora	dirección comercial	192,168,111,125

16	Mamani Vega Zulema	Secretaria Dir. Técnica	192,168,111,126
17	Leyton Ale Nayu Sandra	Jefe de Recursos Humanos	192,168,111,127
18	Gonzales Ruiz Jaime Fernando	Tec. Medio Enc. Activos Fijos	192,168,111,128
19	Teran Rodriguez Edwin Cristobal	Jefe de Adquisiciones	192,168,111,129
20	Delfin Finn Bismarck Noe	Auxiliar de Recursos Humanos	192,168,111,130
21	Sanchez Krayasichs Alberto	Tec. Superior Enc. De Servicios Grals.	192,168,111,131
22	Gonzales Ruiz Jaime Fernando	Tec. Medio Enc. Activos Fijos	192,168,111,132
23	Diaz Jesús Orlando	Encargado de Almacenes	192,168,111,133
24	Maita Montesinos Cristina Consuelo	Secretaria Dir. Administrativa	192,168,111,134
25	Leyton Antezana Horacio Pablo	Oficial Comunicación	192.168.111.135
26	Teran Rodriguez Edwin Cristobal	máquina virtual	192,168,111,136
27		consultor	192,168,111,137

28		consultor	192,168,111,138
29	Torrez Farfan Willan Alberto	Jefe de Operaciones	192,168,111,139
30		consultor	192,168,111,140
31	Vaca Valdez Carla Alejandra	Técnico Adjunto	192,168,111,141
32	Baldiviezo Alvarado Mario Luis	Técnico Medio I	192,168,111,142
33	Vargas Fernandez America	Portátil	192,168,111,143
34		consultor	192,168,111,144
35		Técnico Proyectista	192,168,111,145
36	Vaca Valdez Carla Alejandra	Impresora	192,168,111,146
37	impresora	Adriana Buitrago	192.168.111.146
38		consultor	192,168,111,147
39		consultor	192,168,111,148
40		consultor	192,168,111,149
41		Portátil	192,168,111,150
42		consultor	192,168,111,151

43	Borja Paita Oscar	Técnico Medio II	192,168,111,152
44	Miranda Vega Mauricio	Auxiliar Administrativo de Almacenes	192,168,111,13
45		consultor	192,168,111,154

Tabla 8 *Tabla de direccionamiento local de la red actual de EMTAGAS*

Fuente: Elaboración propia

N°	**APELLIDOS NOMBRES**	**Y**	**CARGO**	**RED**
RED CONTABILIDAD				**IP**
46	Vidal Mauricio Lopez	Sergio	Director Administrativo y Financiero	192,168,111,71
47	Miranda Rosmery	Armella	Contador General	192,168,111,72
48	Añazgo Ramirez Luis Grover		Jefe de Presupuestos	192,168,111,73
49	López Martinez Shirley		Responsable de Ingresos	192,168,111,74
50	Cardozo Urzagaste Marlene Zulma		Encargada de Tributación	192,168,111,75

51	Diaz Jesus Orlando	Jefe de Tesorería	192,168,111,76
52	Torrez Murguia Elizabeth	Responsable de Egresos	192,168,111,77
53			192,168,111,78
54	Vaca Solano Mario Santos	Auxiliar Tesorería	192,168,111,79
55	switch	Cisco Servidores	192,168,111,80
56	switch	Cisco Red Facturación	192,168,111,81
57	Teran Rodriguez Edwin Cristobal	impresora	192,168,111,82
58			192,168,111,83
59	Cardozo Urzagaste Marlene Zulma	impresora	192,168,111,94

Tabla 9 *Tabla de direccionamiento de red en el área de contabilidad de EMTAGAS*

Fuente: Elaboración propia

N°	APELLIDOS Y NOMBRES	CARGO	RED
RED FACTURACION			IP
60	Del Carpio Silos Mateo Wilfredo	Director Comercial	192,168,111,41
61	Quiroga Araoz Paola Ninet	Enc. Cred y Morosidad	192,168,111,42
62	Colodro Herrera Rene Fernando	Tec. Instrumentista	192,168,111,43
63	Martinez De los Rios Walter	Encargado de Facturación	192,168,111,44
64	Martinez De los Rios Walter	Encargado de Facturación	192,168,111,45
65	Alvarado Romero Sandro Simon Aldo	Técnico Senior de ODECO	192,168,111,46
66	Molina Aranda Luis	Enc. De Medidores	192,168,111,47
67	inactivo		192,168,111,48
68	Gaite Alvarado Blanca Jheny	Auxiliar de Facturación	192,168,111,49
69		Lecturadora III	192,168,111,50
70	Buitrago Frigerio Adriana	Encargada de ODECO	192,168,111,51
71	Yolanda Cruz	Técnico_Odeco	192,168,111,52
72	inactivo		192,168,111,53
73	Pacheco Siles Ernesto Osmar	Cajero I	192,168,111,54
74	Ortiz Fernandez Sandro Petri	Cajera II	192,168,111,55
75		Resp. Eval.-Control	192,168,111,56

		Inst. Internas	
76	inactivo		192,168,111,57
77		Técnico_odeco_II	192,168,111,58
78	Mamani Vega Zulema	Secretaria de Comercial	192,168,111,59
79	Colodro Rene	Consultor	192,168,111,60
80	Martinez De los Rios Walter	portátil envy	192,168,111,61
81		Consultor	192,168,111,65
82		analista de facturación	192,168,111,66
83		Encargada Reg. San Lorenzo	192,168,111,93

Tabla 10 *Tabla de direccionamiento de red en el área de facturación de EMTAGAS*

Fuente: Elaboración propia

N°	**APELLIDOS Y NOMBRES**	**CARGO**	**RED**
	ADMINISTRADOR		**IP**
	FORTINET 100D	FIREWALL	192,168,111,1
	DVR AJHUA	SERVIDOR VIGILANCIA	192,168,111,10
80	Willma Mendieta	Encargada Archivos	192,168,111,27

81	Tapia Duran Raúl Hernan	Encargado de Sistemas	192,168,111,28
82	BarriosCuenca Walter Antonio	auxiliar de Sistemas	192,168,111,29
83	Servidor Antivirus	Servidores	192,168,111,30
84	Servidor Biometrico	Servidores	192,168,111,31
85			192,168,111,32
86	Servidor Wifi	Servidores	192,168,111,33
87	DNS	Servidores	192,168,111,34
88	pasante sistemas		192,168,111,35
89	servidor wifi2	Servidores	192,168,111,36
90	Cari Alicia	Encargada de Centralita	192,168,9,102

Tabla 11 *Tabla de direccionamiento de red en el área de administración de EMTAGAS*

Fuente: Elaboración propia

III.1.1.3.4. Distribución de los MDF y IDF

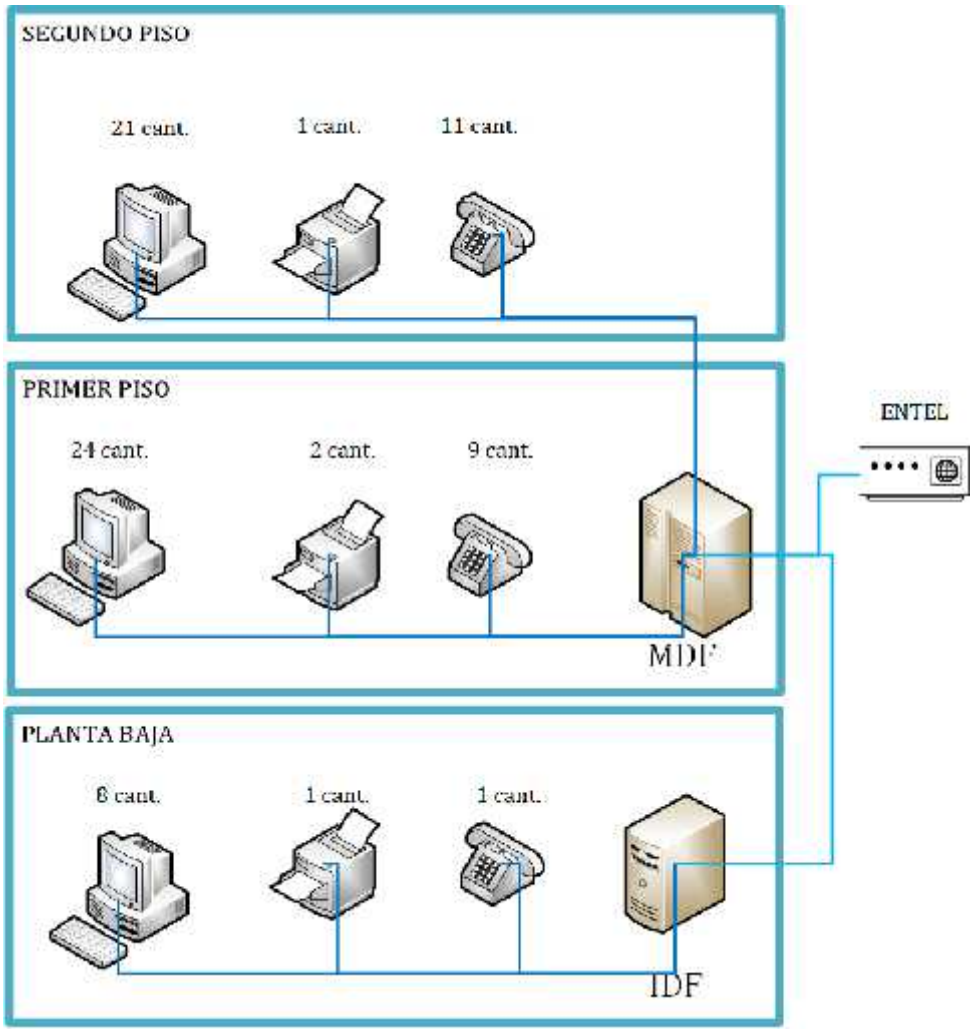


Figura 30: *Distribución de los cuartos de comunicación MDF y IDF*

Fuente: Elaboración propia

132. La red informática de EMTAGAS se encuentra distribuida en dos pisos que conforma la empresa esta cuenta con un solo IDF y un MDF, emplea únicamente el enrutamiento estático para enlazar los dispositivos que conforma la infraestructura, como ser los equipos de escritorio, dispositivos compartidos (impresoras) y dispositivos de comunicación y colaboración (teléfonos IP),

cuenta con los siguientes dispositivos: 53 equipos de escritorios, 4 impresoras, 21 teléfonos, 3 interfaces Router, 4 switches y 1 servidor.

133. El IDF está situado en la planta baja y el MDF en el primer piso, estableciendo una conexión vertical de los puntos de conexión, en estos pisos se alberga los cuartos de telecomunicación, el principal está ubicada en el primer piso, está equipado el MDF con un solo aire de acondicionamiento, el diseño del MDF no cuenta con el estándar óptimo de seguridad y protección. El cuarto está ubicado de forma provisional dentro del área de la dirección técnica, está asegurada por una puerta de madera y deteniendo el ingreso una fila de asientos metálicos, también no contiene algún censor de ingreso y de incendio por lo cual no cumple con la política de seguridad física para un MDF. Así el MDF está expuesto a acceso no autorizados y a incendios no controlado, por lo cual expone la integridad de los datos y la continuidad operativa.

134. El cuarto presenta un exceso de cables mal organizados que esto tiende a tener fallos de conexión y operativo.

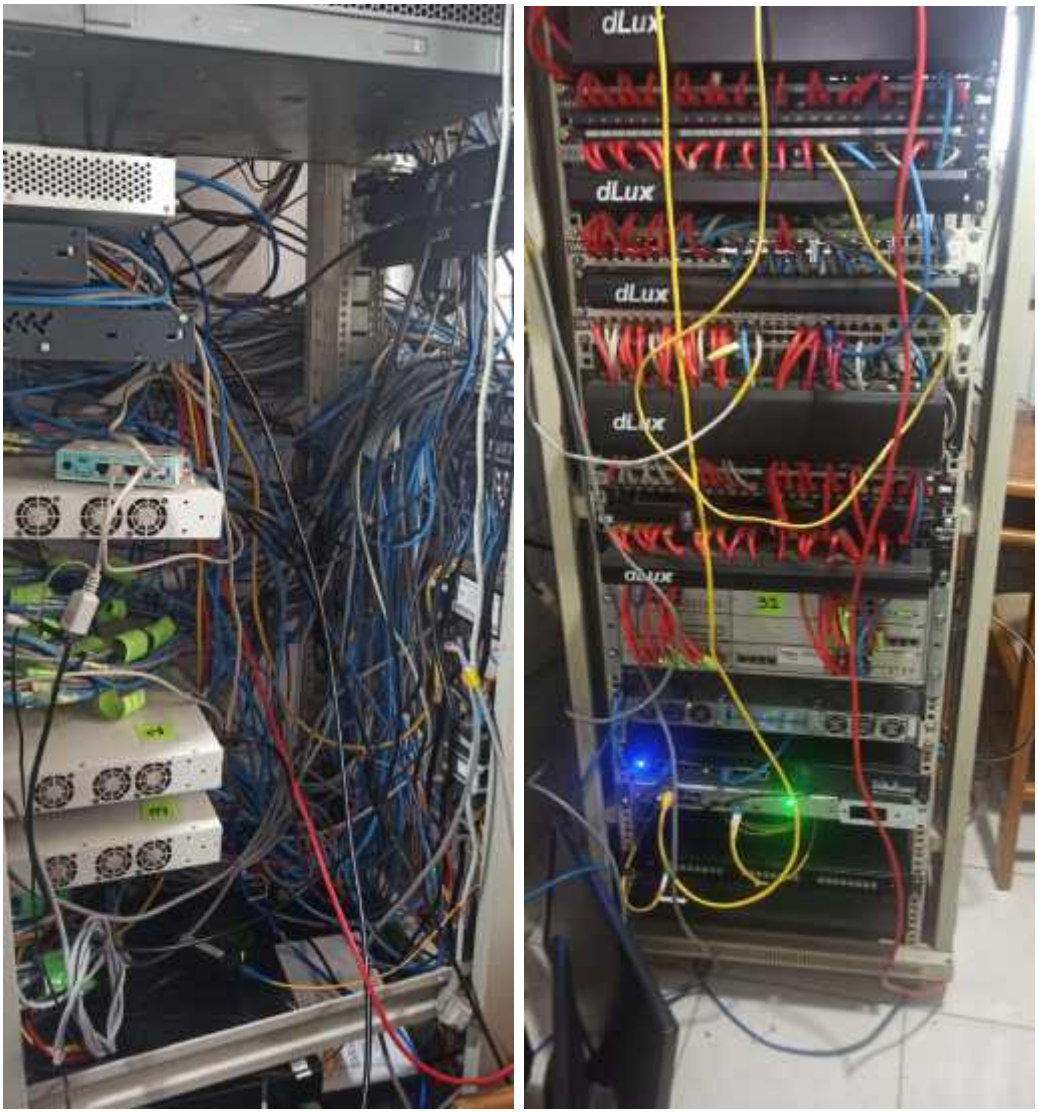


Figura 31: *Parte interna del MDF actual de EMTAGAS*

Fuente: Elaboración propia

135. En esta imagen se puede visualizar el cableado del Rack en el MDF

Figura 32: *Parte exterior del MDF de EMTAGAS*

Fuente: Elaboración propia

136. En esta imagen visualizamos el estado del MDF ubicado en el primer piso.

Figura 33: *IDF actual de EMTAGAS*

Fuente: Elaboración propia

137. En esta imagen se puede notar el estado de la ubicación del IDF de la planta baja. Está claro que faltan normas de seguridad en los cuartos de comunicación tanto en el MDF como en el IDF.

Figura 34: *Estructura del cableado de red actual de EMTAGAS*

Fuente: Elaboración propia

138. Se puede visualizar en la imagen, que la empresa no se cumple con la totalidad las normas del cableado estructurado.

139. Cabe mencionar que la empresa cuenta con cámaras analógicas y telefonía, pero están desprendidas de la red de datos.

III.1.1.4. Analizar tráfico existente

140. Para el análisis del tráfico existente por privacidad no se pudo analizar, ya que en la empresa tienen cajas de pagos y cuentas de la misma empresa.

141. Se hizo un cálculo estimado para el tráfico existente.

Nro.	Actividad en línea	Ancho de banda necesario	Usuarios	Ancho de banda actual	Ancho de banda del proveedor
1	Navegación web, email, redes sociales	1 Mbps	58	0,26 Mbps	15 Mbps
2	videoconferencias	1.5 Mbps	58	0,26 Mbps	15 Mbps
3	Streaming de música	0.5	58	0,26 Mbps	15 Mbps

Tabla 12 *Análisis del tráfico existente de la red de EMTAGAS*

Fuente: Elaboración propia

III.1.2. Diseño Lógico

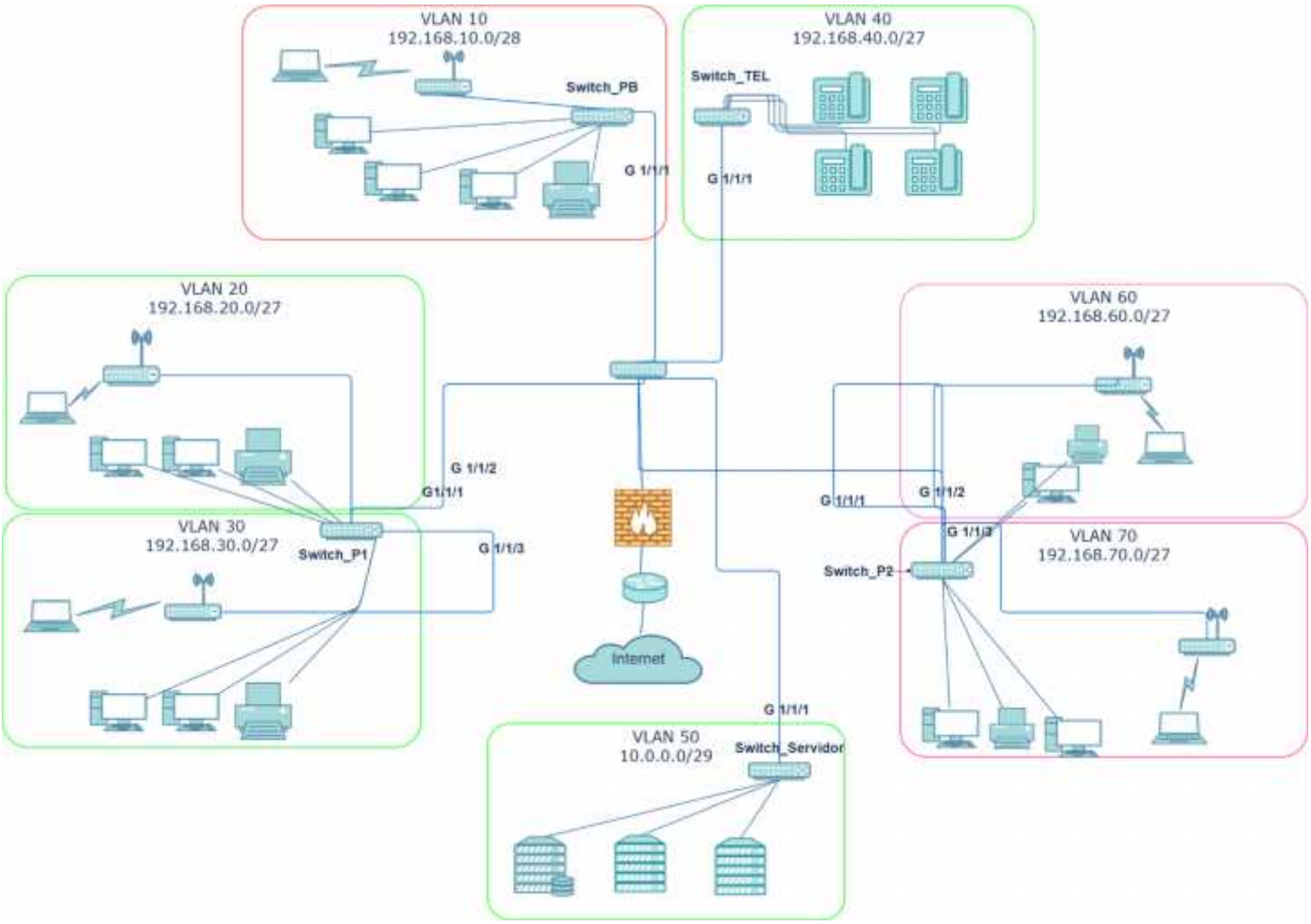


Figura 35: *Propuesta de red del diseño lógico de EMTAGAS*

Fuente: Elaboración propia

III.1.2.1. Diseñar topología de red

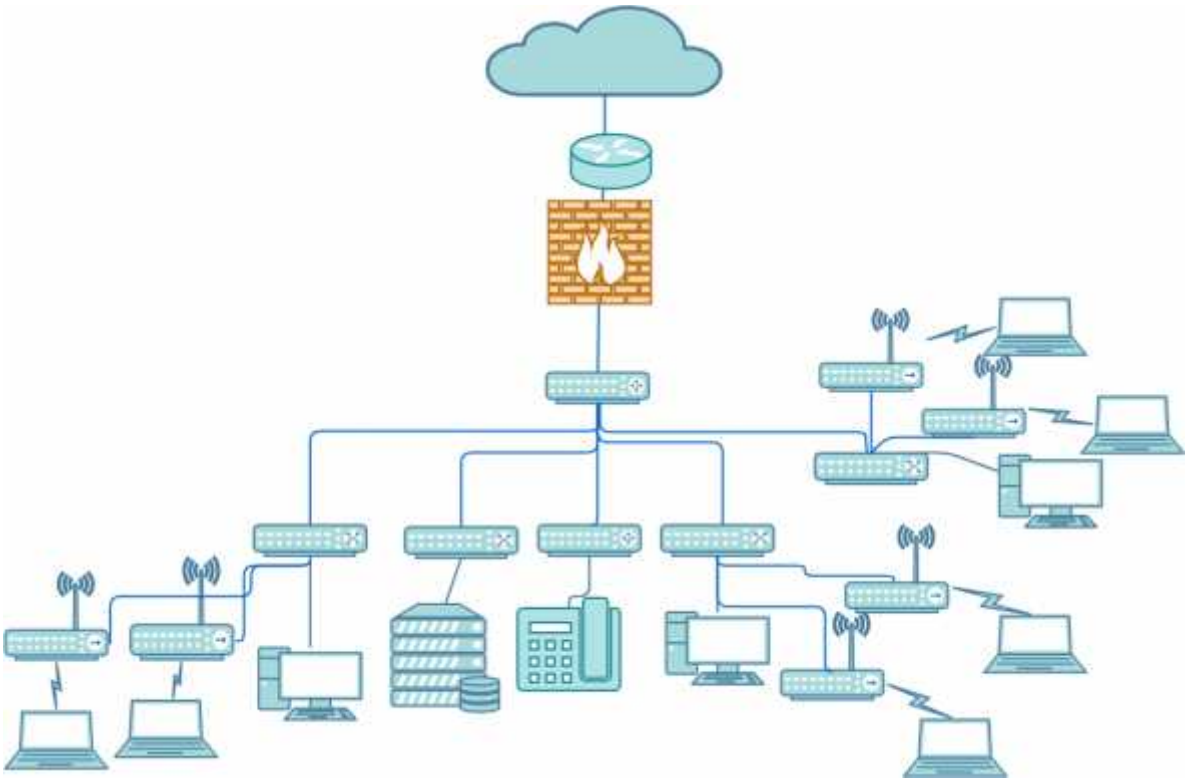


Figura 36: *Topología de red propuesta para EMTAGAS*

Fuente: Elaboración propia

142. . Considerando que EMTAGAS tiene varias áreas de operación, se opta por una topología de red en estrella, con la facilidad de administración y la capacidad de aislar problemas de red, ya que un fallo en un nodo no afecta a los demás.

143. Esta Topología implica un núcleo central donde convergen todas las conexiones de red, conectado a través de enlaces de fibra óptica para garantizar altas velocidades de transferencia y baja latencia, donde por cada piso se propone un switch de acceso local para gestionar el tráfico interno de manera eficiente.

III.1.2.2. Selección de tecnología

III.1.2.2.1. VLAN (Red de Área Local Virtual)

144. La implementación de VLAN permite segmentar la red en subredes lógicas independientes, lo que brinda mayor seguridad y eficiencia en la gestión del tráfico de datos. Para el establecimiento y configuración de las VLAN, se utilizará el protocolo IEEE 802.1Q, que permite etiquetar y clasificar el tráfico de red en las diferentes VLAN.

III.1.2.2.2. Fibra Óptica

145. La utilización de fibra óptica como medio de transmisión ofrece una alta capacidad de ancho de banda y una menor pérdida de señal en comparación con los cables de cobre tradicionales. En fibra óptica, se utilizará el protocolo Ethernet 1000BASE-SX, para establecer la comunicación de datos a través de estos medios.

III.1.2.2.3. Redes inalámbricas (Wi-Fi)

146. En el caso de las redes Wi-Fi, se utilizarán protocolos como IEEE 802.11 para establecer la comunicación inalámbrica entre los dispositivos.

III.1.2.2.4. Protocolos de red

147. Se utilizarán protocolos estándar como TCP/IP (Protocolo de Control de Transmisión/Protocolo de Internet), que es el conjunto de protocolos utilizados en Internet para la comunicación de datos. TCP/IP incluye protocolos como IP (Protocolo de Internet) para la entrega de paquetes de datos y TCP (Protocolo de Control de Transmisión) para garantizar la entrega confiable de datos. Además, se empleará el protocolo DHCP (Protocolo de Configuración Dinámica de Host) para asignar direcciones IP de manera automática y SNMP (Protocolo Simple de Administración de Red) para la gestión y monitoreo de la red.

III.1.2.2.5. Firewalls y Seguridad de Red

148. En el uso de un dispositivo Fortinet, se trata de un firewall de próxima generación que proporciona seguridad integral para la red. Los firewalls Fortinet utilizara una variedad de protocolos

y tecnologías de seguridad, como IPsec (Protocolo de Seguridad de Internet), SSL/TLS (Capa de Conexión Segura/Protocolo de Seguridad de Transporte), IPS (Sistema de Prevención de Intrusiones) y antivirus integrado, entre otros. Estos protocolos y tecnologías ayudarán a proteger la red contra amenazas y ataques, así como a controlar el tráfico de datos entrante y saliente.

III.1.2.2.6. Segmentación de la Red

149. El direccionamiento estará dividido en siete subredes que serán las siguientes sub redes: Caja-Odeco, Dirección Técnica, Dirección Comercial, Dirección Administrativa, Dirección Legal, Telefonía y la de servidores.

150. Se trabajará con clase C de direcciones IP, que se asignaran dinámicamente.

III.1.2.2.7. Cableado estructurado

Nro.	Especificaciones	Cat 5	Cat 5e	Cat 6	Cat 6a
1	Frecuencia	100 MHz	100 MHz	250 MHz	500 MHz
2	Atenuación (min a 100Mhz)	22 db	22db	19.8 db	--
3	Perdida de retorno (min A 100 MHz)	16 db	20.1 db	20.1 db	8db
4	Redes soportadas	100 Base-T	1000 Base-Tx	1000 Base-Tx	10 Gbase

Tabla 13 *Categoría del cable UTP propuesto*

Fuente: Elaboración propia

151. Para el diseño físico utilizaremos el cable UTP 6A con un diámetro exterior de 8.3 mm también cuenta con un radio de curvatura fija de 33 mm cable tiene que estar con temperatura de 10 C° a 60 C° también permite trabajar con una velocidad de Ethernet hasta 10 Gbps, ya que este cable soportara a futuras bandas anchas.

152. Cabe mencionar que la distancia más larga de punto a punto de todo el diseño es de 75 mts.

153. También todo el cableado estructurado estará bajo la norma TIA/EIA-568-B Intenta definir las normas que permitan el diseño y aplicación de sistemas de cableado estructurado para edificios comerciales, y entre los edificios y entornos de campus.

154. Todo el cableado estará bajo el cable canal y rosetas, también a cada final de un punto de red contará con un patch cord para llegar al equipo final.

155. Al llegar el cable al patch panel, se dejará una largura de cable de 8mts para que a futuro se pueda alargar el punto de red o, cuando hubiera fallas, se pueda hacer el reponchado del punto.

III.1.2.3. Diseño de cableado de red

III.1.2.3.1. Planta baja

156. La planta baja está conformada por las siguientes áreas: Caja, ODECO.

157. La cantidad de dispositivos en esta es de 8 máquinas de escritorios, 1 teléfono y 1 impresora. Todos estos equipos conectados al IDF de la planta baja.

Figura 37: *Diseño de la elaboración del IDF planta baja, vista 3D*

Fuente: Elaboración propia

Figura 38: *Diseño del cableado UTP de la planta baja, vista 3D*

Fuente: Elaboración propia

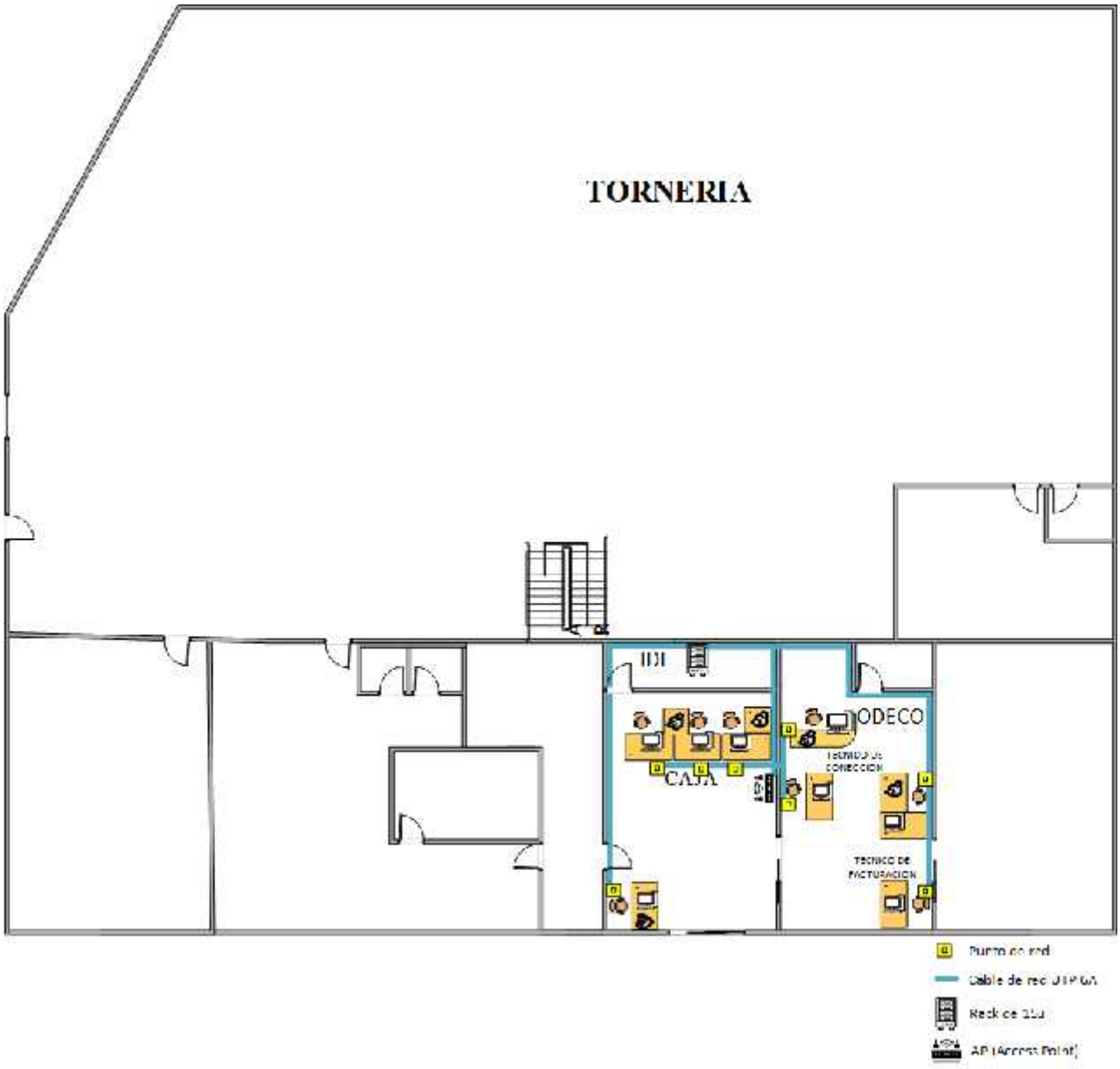


Figura 39: *Diseño de cableado UTP planta baja, vista 2D*

Fuente: Elaboración propia

III.1.2.3.2. Primer Piso

158. El primer piso está conformado por las siguientes áreas: Dirección Comercial, Dirección Técnica, Recursos Humanos, Facturación, Recuperación de Carpetas.

159. La cantidad de dispositivos en esta es de 22 máquinas de escritorios, 10 teléfonos y cuenta con 19 impresoras que solo 2 de ellas se encuentran conectadas a la red, todos estos equipos conectados en el MDF.

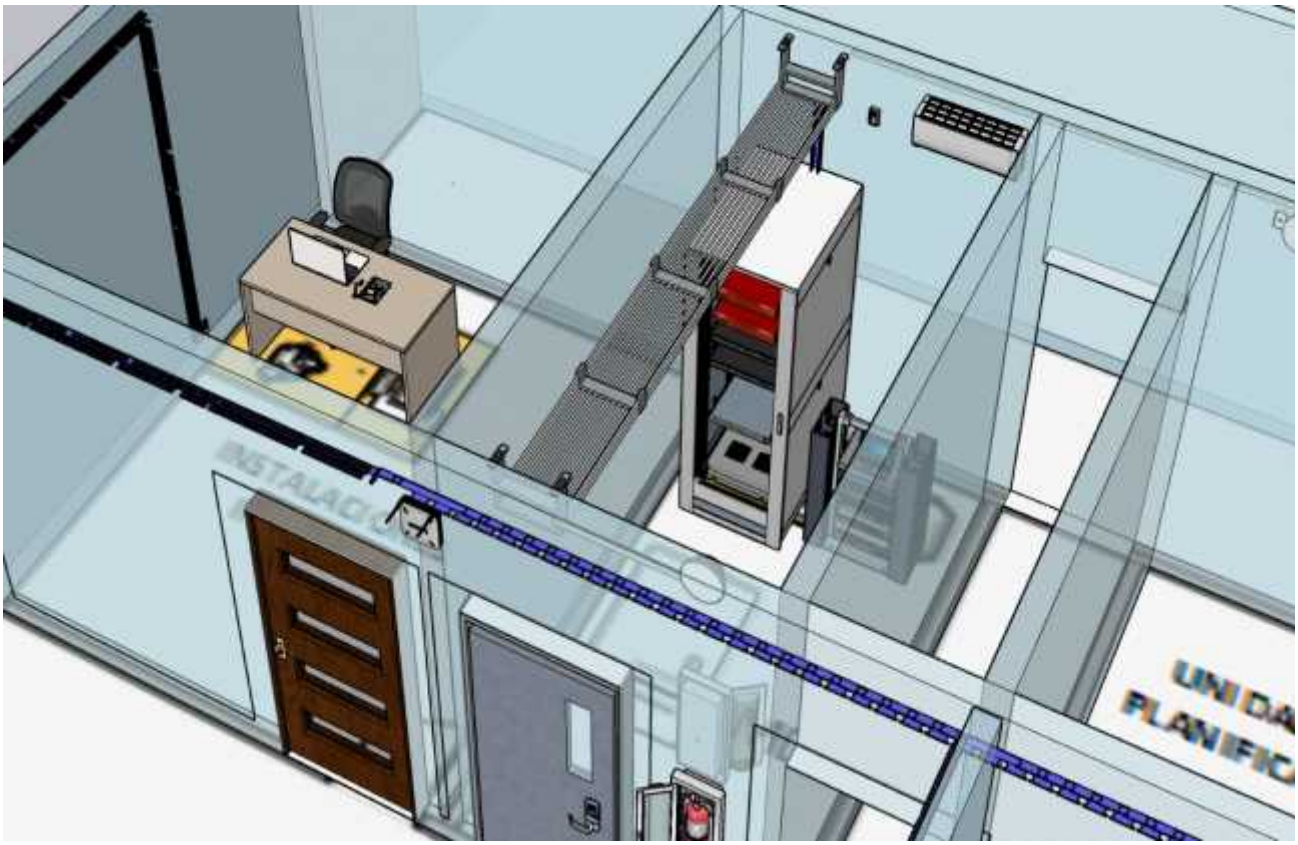


Figura 40: *Diseño del MDF del primer piso, vista 3D*

Fuente: Elaboración propia

160. En el primer piso está ubicado el MDF de la empresa, donde llegan todos los puntos de red de la planta baja: primer piso y segundo piso.

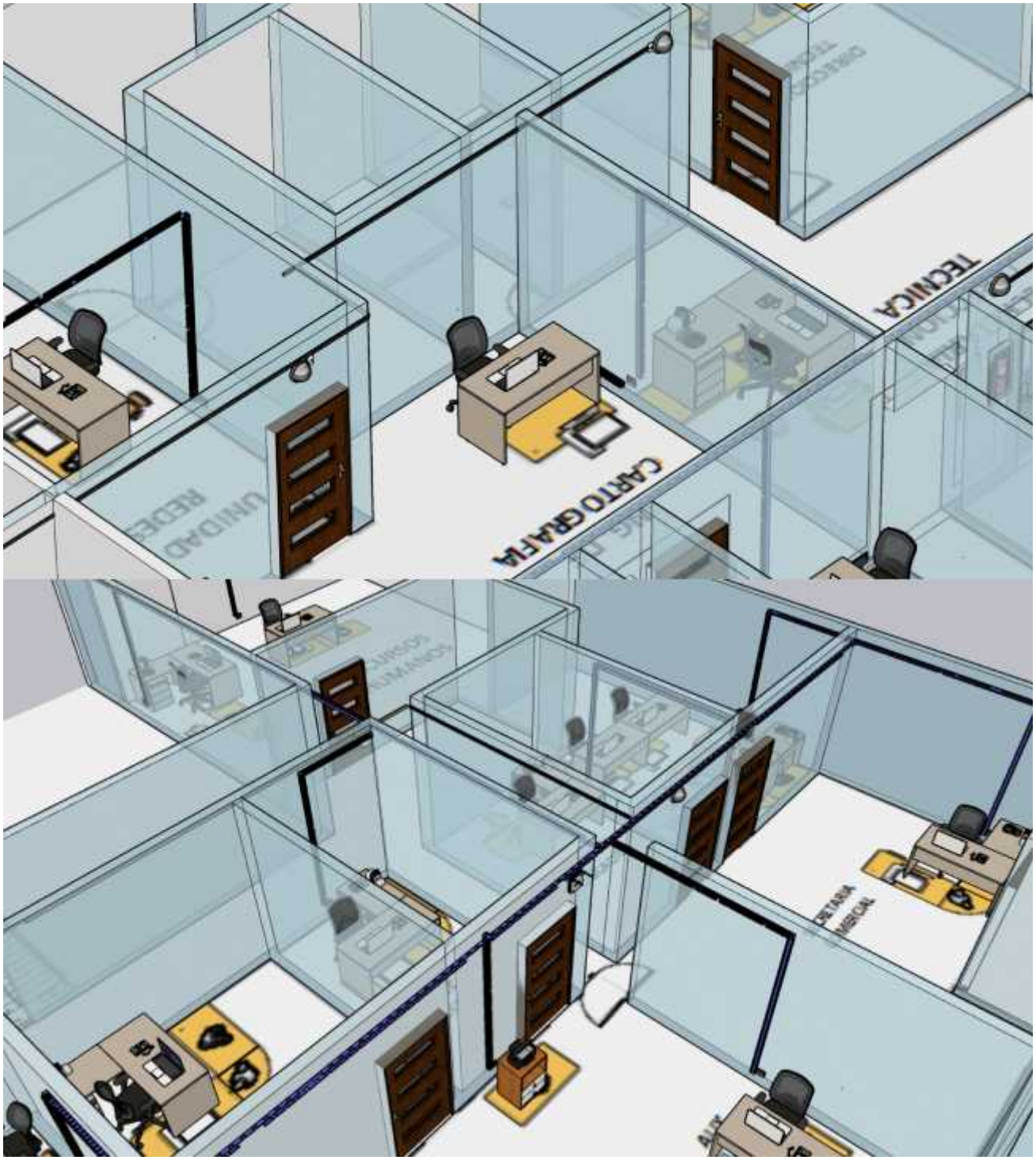


Figura 41: *Diseño del cableado UTP del primer piso, vista 3D*

Fuente: Elaboración propia

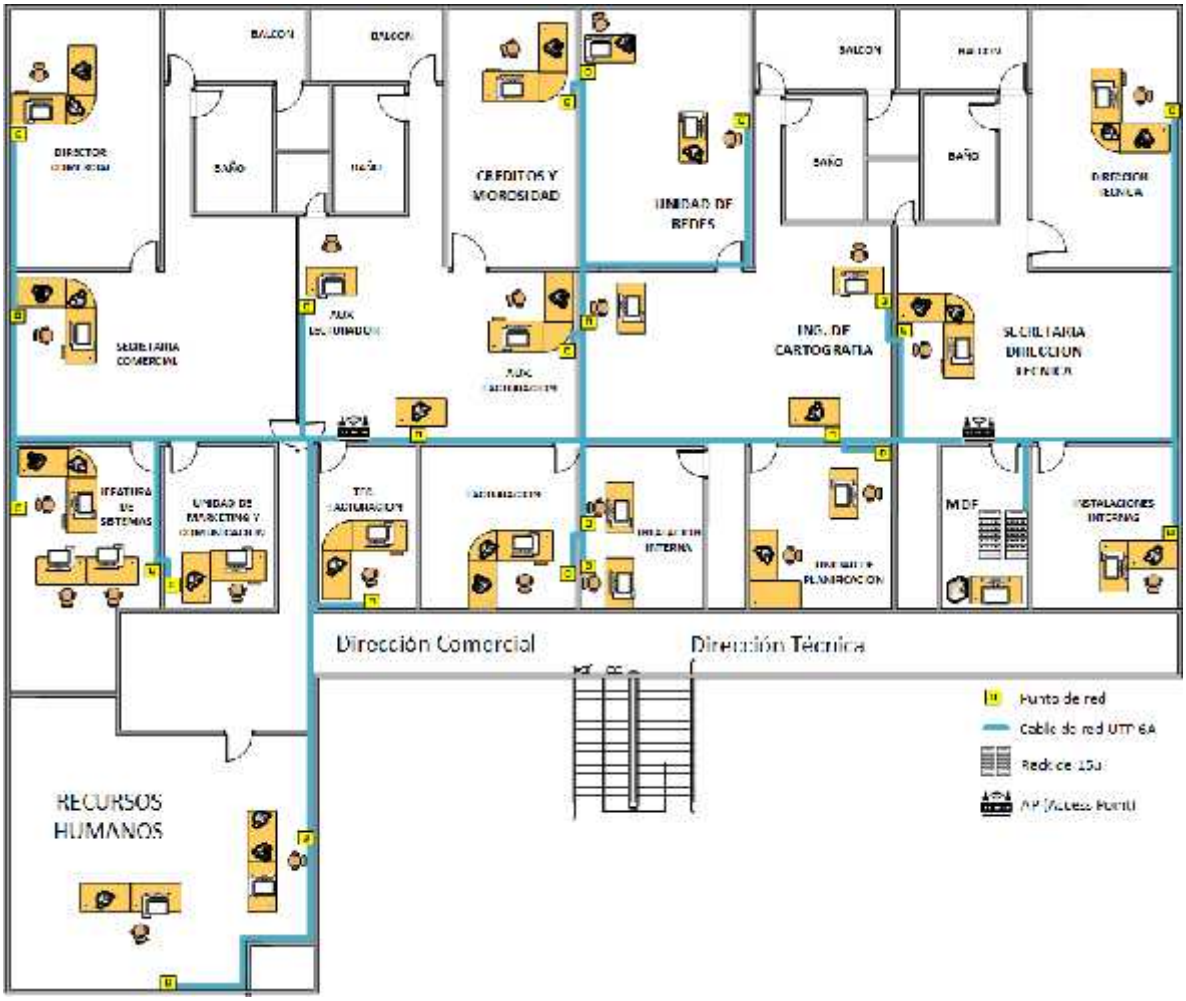


Figura 42: *Diseño del cableado UTP primer piso, vista 2D*

Fuente: Elaboración propia

III.1.2.3.3. Segundo Piso

161. El segundo piso conformad por las siguientes áreas: Gerencia General, Dirección Jurídica, Dirección Administrativa y Financiera.

162. La cantidad de dispositivos en esta planta es de 21 máquinas de escritorios, 11 teléfonos y cuenta con 21 impresoras, donde una sola se encuentra conectada a la red, todos estos equipos conectados en el IDF.

163. En el segundo piso se ubicará el IDF propuesto, para distribución de nuevos puntos de red y control de esa área.

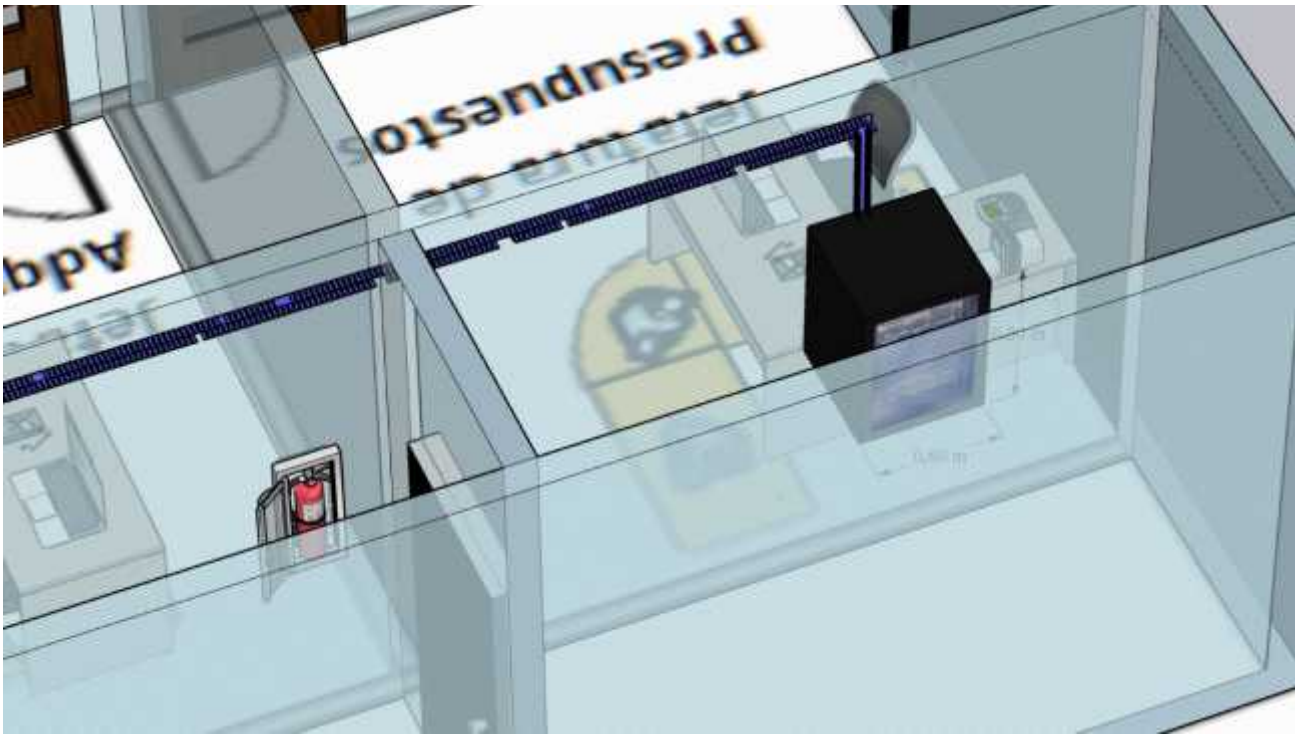


Figura 43: *Diseño del IDF del segundo piso, visto 3D*

Fuente: Elaboración propia

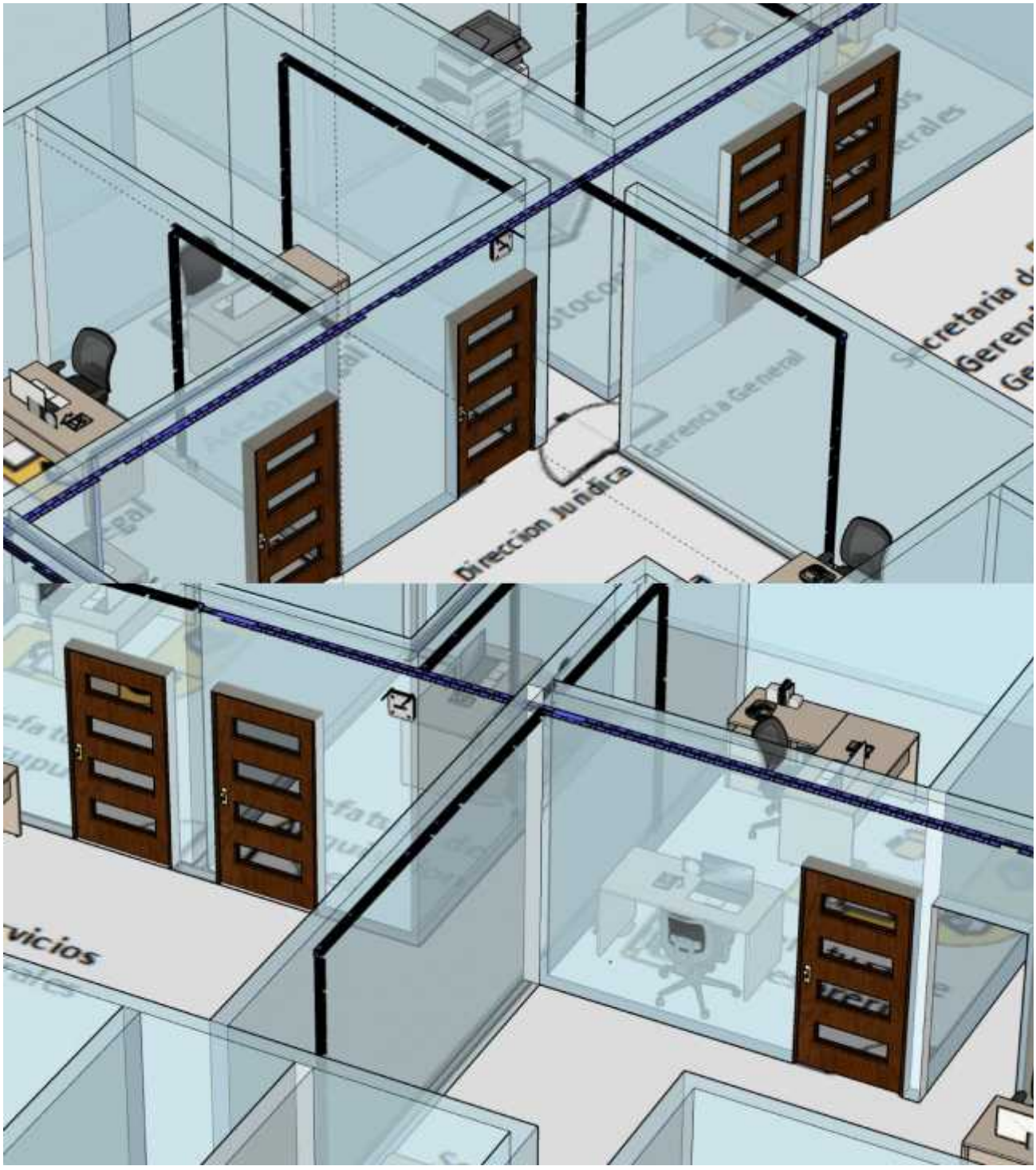


Figura 44: *Diseño del cableado UTP segundo piso, visto 3D*

Fuente: Elaboración propia

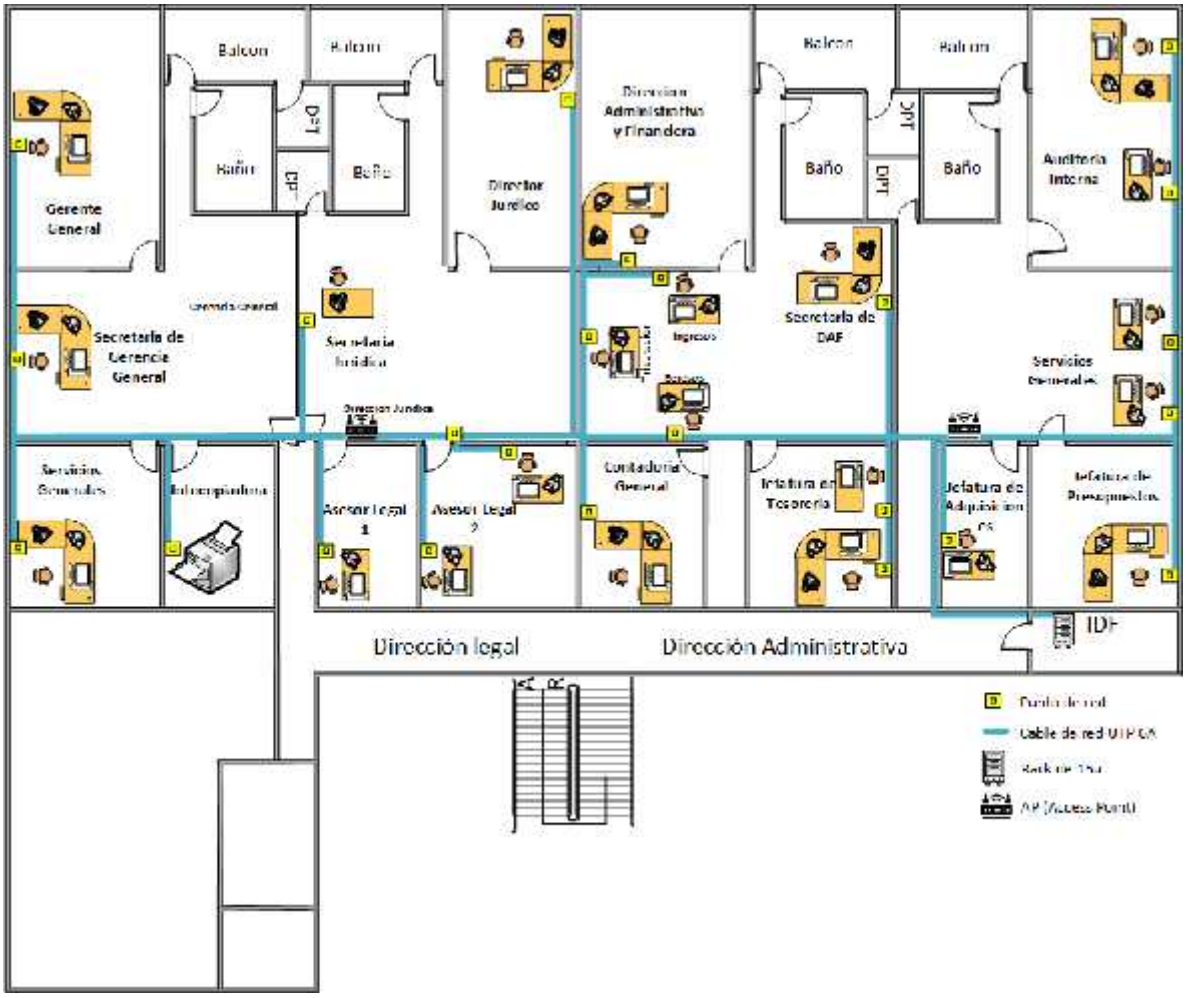


Figura 45: *Diseño de cableado UTP segundo piso, vista 2D*

Fuente: Elaboración propia

III.1.2.4. Diseñar modelos de direccionamiento y hostnames

III.1.2.4.1. Tabla de Direccionamiento IP

164. Tabla de La cantidad total de host que vamos a utilizar, para lo cual consideraremos todos los equipos que requieran un direccionamiento IP.

- 53 equipos de escritorio
- 4 impresoras
- 21 teléfonos
- 6 interface Router
- 1 servidor Archivos, DHCP
- 1 servidor Web, aplicación

165. Una vez definida la cantidad total de puntos, que en nuestro caso son 85 dispositivos que estarán conectados en la red, para lo cual determinaremos el direccionamiento dividiendo la red en siete subredes que serán: Caja-Odeco, Dirección Técnica, Dirección Comercial, Dirección Administrativa, Dirección Legal, Telefonía y la de servidores.

166. Se trabajará con clase C de direcciones IP, que se asignaran dinámicamente direcciones IP.

167. Servidores

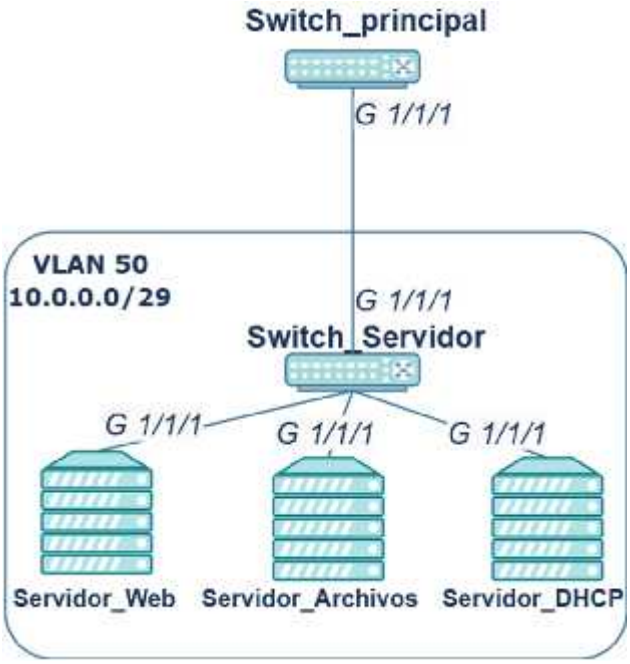


Figura 46: *Switch-servidor diseño lógico*

Fuente: Elaboración propia

168. Tabla de direccionamiento IP del switch servidor

Dispositivo	Dirección IPV4	Mascara de subred	Gateway
Servidor_DHCP_VLAN10	192.168.10.2	255.255.255.240	192.168.10.1
Servidor_DHCP_VLAN20	192.168.20.2	255.255.255.224	192.168.20.1
Servidor_DHCP_VLAN30	192.168.30.2	255.255.255. 224	192.168.30.1
Servidor_DHCP_VLAN60	192.168.60.2	255.255.255.224	192.168.60.1
Servidor_DHCP_VLAN70	192.168.70.2	255.255.255.224	192.168.70.1
Servidor ARCHIVOS	10.0.0.5	255.255.255.248	10.0.0.1
Servidor WEB, APLICACIÓN	10.0.0.6	255.255.255.248	10.0.0.1

Tabla 14 *Tabla de direccionamiento IP propuesto en el Switch-servidor*

Fuente: Elaboración propia

169. Asignación de puertos en el switch del servidor

Puertos (Interfaces)	Asignación	Red
Fa 0/2	VLAN 10,20,30,60,70	192.168.10.0/28, 192.168.20.0/27, 192.168.30.0/27, 192.168.60.0/27, 192.168.70.0/27
Fa 0/3-12	VLAN 50	192.168.50.0/29

Tabla 15 *Asignación de puertos, Switch servidor*

Fuente: Elaboración propia

Planta Baja

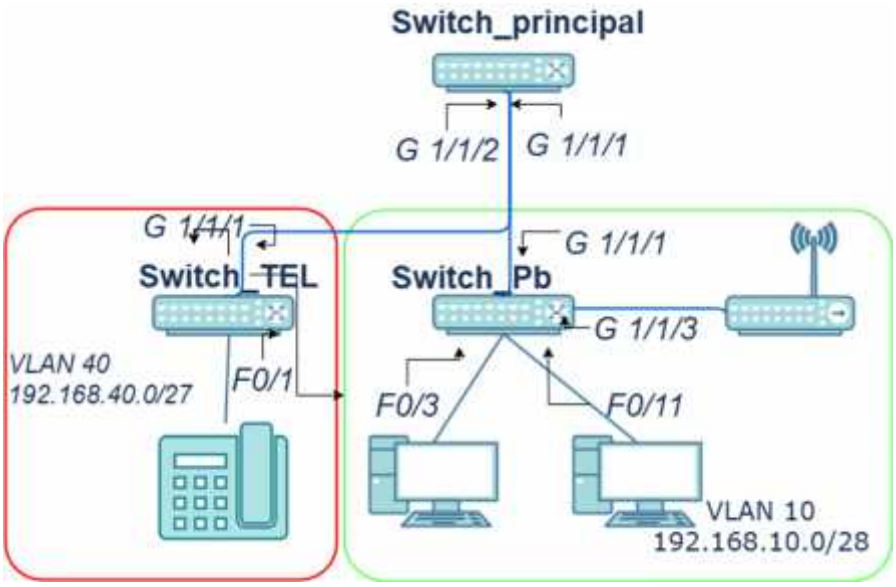


Figura 47: *Switch de planta baja-diseño lógico*

Fuente: Elaboración propia

170. Tabla de direccionamiento IP del switch planta baja

Dispositivo	Dirección IPV4	Mascara de subred	Gateway
PC0-PB-Cj - Printer0-PB-OD	192.168.10.2 - 192.168.10.16	255.255.255.240	192.168.10.1
IP Phone0-PB-AsisFono	192.168.40.2 - 192.168.40.30	255.255.255.224	192.168.40.1

Tabla 16 *Tabla de direccionamiento IP propuesto en el Switch-Planta Baja*

Fuente: Elaboración propia

171. Asignación de puertos en el switch de planta baja

Puertos (Interfaces)	Asignación	Red
F0/3-24	VLAN 10	192.168.10.0/28

Tabla 17 *Asignación de puertos Switch Planta Baja*

Fuente: Elaboración propia

172. Asignación de puertos en el switch de teléfono

Puertos (Interfaces)	Asignación	Red
Fa 0/2-Fa 0/24	VLAN 40	192.168.40.0/27

Tabla 18 *Asignación de puertos Switch de Teléfono*

Fuente: Elaboración propia

Primer Piso

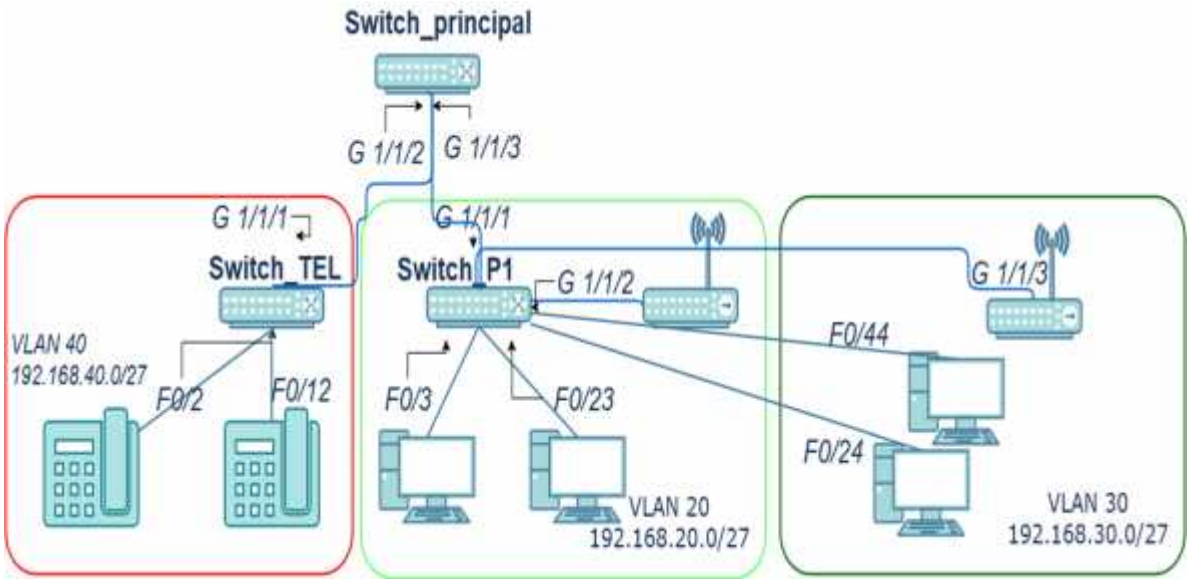


Figura 48: *Switch de primer piso-diseño lógico*

Fuente: Elaboración propia

173. Tabla de direccionamiento IP del switch principal

Dispositivo	Dirección IPV4	Mascara de subred	Gateway
PC8-P1-inst_Inter – PC17-P1-	192.168.20.2 - 192.168.20.30	255.255.255.224	192.168.20.1
PC18-P1-creMoro–PC30-P1-RHumanos	192.168.30.2 - 192.168.30.30	255.255.255.224	192.168.30.1
IP Phone1-P1 - IP Phone10-P1	192.168.40.3 – 192.168.40.30	255.255.255.224	192.168.40.1

Tabla 19 *Rango de direcciones IP para las PCs del Primer Piso*

Fuente: Elaboración propia

Asignación de Puertos

Switch Primer Piso

Puertos (Interfaces)	Asignación	Red
Fa 03-23	VLAN 20	192.168.20.0/27
Fa 0/24-44	VLAN 30	192.168.30.0/27

Tabla 20 *Asignación de puertos Switch Primer piso.*

Fuente: Elaboración propia

Switch de Teléfono

Puertos (Interfaces)	Asignación	Red
Fa 0/3-Fa 0/14	VLAN 40	192.168.40.0/27

Tabla 21 *Asignación de puertos Switch de Telefono.*

Fuente: Elaboración propia

Switch Segundo Piso

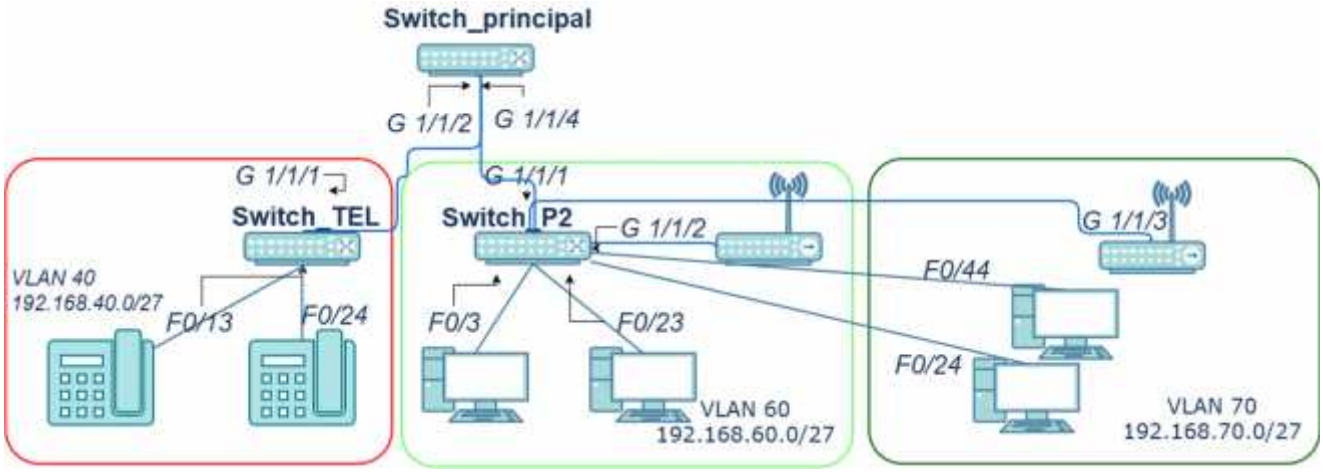


Figura 49: *Switch de segundo piso-diseño lógico*

Fuente: Elaboración propia

o

Dispositivo	**Dirección IPV4**	**Mascara de subred**	**Gateway**
PC31-P1-inst_Inter – PC17-P1-	192.168.20.10 - 192.168.20.40	255.255.255.192	192.168.20.1
IP Phone1-P1 - IP Phone10-P1	192.168.40.10 – 192.168.40.30	255.255.255.224	192.168.40.1

Tabla 22 *Rango de direcciones IP para las PCs del segundo piso.*

Fuente: Elaboración propia

Asignación de Puertos

Switch Segundo Piso

Puertos (Interfaces)	Asignación	Red
F0/3-23	VLAN 60	192.168.60.0/27
F0/24-44	VLAN 70	192.168.70.0/27

Tabla 23 *Asignación de puertos Switch de segundo piso.*

Fuente: Elaboración propia

Switch de Teléfono

Puertos (Interfaces)	Asignación	Red
Fa 0/13-Fa 0/24	VLAN 40	192.168.40.0/27

Tabla 24 *Asignación de puertos Switch de Telefonos.*

Fuente: Elaboración propia

Selección de protocolos Switching y Routing

174. En la selección de protocolos de switching y routing se considera los siguientes protocolos:

175. **VTP**, este permite centralizar y simplificar la administración en un dominio de VLAN, pudiendo crear, borrar y renombrar las mismas, reduciendo así la necesidad de configurar la misma VLAN.

176. **IEEE 802.1Q**, este protocolo se encarga de añadir 4 bytes al encabezado de las tramas, para así asociarlo con la información de la VLAN a la que pertenece. Y el protocolo VTP (VLAN Trunking Protocol), este protocolo nos ayudará a administrar las VLAN en toda la red, dándonos la posibilidad de cambiar el nombre, crear nuevas VLAN y eliminarlas. Se creará VLAN por cada área

de piso, una VLAN para servidores y una VLAN para solo teléfonos. Se crearán enlaces troncales para cada switch que van directamente conectando al switch de capa 3.

177. ANSI/TIA/EIA-569

178. Esta Norma señala las especificaciones necesarias, el diseño de las instalaciones y la infraestructura requeridas en el cableado horizontal y vertical de telecomunicaciones para edificios.

179. Cuenta tres conceptos fundamentales relacionados con telecomunicaciones y edificios:

- Los edificios son dinámicos. Reconoce que existirán cambios y los tiene en cuenta en sus recomendaciones para el diseño de las canalizaciones de telecomunicaciones.
- Los sistemas de telecomunicaciones son dinámicos. Reconoce este hecho siendo tan independiente como sea posible de proveedores y tecnologías de equipo.
- Telecomunicaciones es más que “voz y datos”. Incluye otros conceptos, incorpora otros sistemas tales como control ambiental, seguridad, audio, televisión, alarmas y sonido.

180. La Norma identifica seis componentes en la infraestructura:

- Instalaciones de Entrada
- Sala de Equipos
- Canalizaciones de “Montantes” (“Back-bone”)
- Salas de Telecomunicaciones
- Canalizaciones horizontales
- Áreas de trabajo

181. Esta normativa nos ayudará a considerar el tendido de canalización para el cableado de red, tomando en cuenta los siguientes campos: ubicación, tamaño, ambiente, electricidad,

distanciamiento, ductos bajo piso, ductos sobre piso, ductos aparentes, bandejas, ductos sobre cielo raso y ductos perimetrales.

III.1.2.5. Desarrollar estrategias de seguridad

182. La seguridad de Red es de vital importancia cuando se habla de empresas e instituciones, considerando el flujo de la información que presenta la empresa EMTAGAS es necesario implementar estrategias de seguridad y aplicarlas en las áreas donde se presente la discreción en la información, y son en estas áreas son más propensas a los ataques de usuarios maliciosos, la importancia de las estrategias de seguridad es dar solución a las vulnerabilidades que están presente. La propuesta de mi estrategia de seguridad serán las siguientes:

183. **Firewalls,** permite crear una barrera entre la red local o interna con las redes externas (Internet). Se usará un conjunto de reglas definidas para permitir o bloquear el tráfico; muy aparte, también se hace un control del consumo del ancho de banda. Dándonos la facilidad de bloquear tales sitios que no convalidan con el trabajo en dichas áreas, por ejemplo, páginas web maliciosas, redes sociales, etc.

184. **Segmentación de la red:** se implementará una red VLAN con 4 redes, una red para cada piso y una para los servidores. La segmentación nos ayudará a clasificar el tráfico de red en distintas categorías y facilitará la aplicación de políticas de seguridad. Las clasificaciones se basan en la identidad de los EndPoints, no solo en las direcciones IP. Puede asignar derechos de acceso basados en roles, ubicación y demás, de modo que se otorgue el nivel de acceso correcto a las personas adecuadas y se contengan y reparen los dispositivos sospechosos.

185. **Control de acceso**, ayudará a que no todos los usuarios deben tener acceso a la red, para evitar posibles ataques. Se reconocerá a todos los usuarios y dispositivos en donde se podrán aplicar las políticas de seguridad. Se podrá bloquear a dispositivos de EndPoints que no cumplen las políticas o proporcionarles acceso limitado, todo esto con el control de acceso a la red (NAC).

186. **Control de Acceso Físico:** Limitación el acceso físico a los equipos y dispositivos de la LAN. Utilizando tarjetas de acceso y control de puertas para evitar intrusiones no autorizados.

187. **Seguridad en la Capa Física**: Ocultar el SSID de la WLAN para dificultar el acceso no autorizado. Utilizando el cifrado WPA3 para proteger las comunicaciones inalámbricas.

188. **Aislamiento de Clientes:** Configuración de WLAN para aislar a los clientes, de modo que no puedan comunicarse entre sí, lo que reduce el riesgo de ataques internos.

189. **Red de Invitados:** Si es aplicable, se creará una red WLAN separada para invitados con acceso limitado a recursos internos y una contraseña única.

190. **Monitoreo de Tráfico WLAN:** Utilizaremos herramientas de monitoreo para supervisar el tráfico WLAN y detectar actividad sospechosa.

191. **Seguridad del correo electrónico**, el gateways del correo electrónico es el principal vector de amenaza para las infracciones a la seguridad, se implementará una aplicación de seguridad de correo electrónico bloquea los ataques entrantes y controla los mensajes salientes para prevenir la pérdida de datos sensibles.

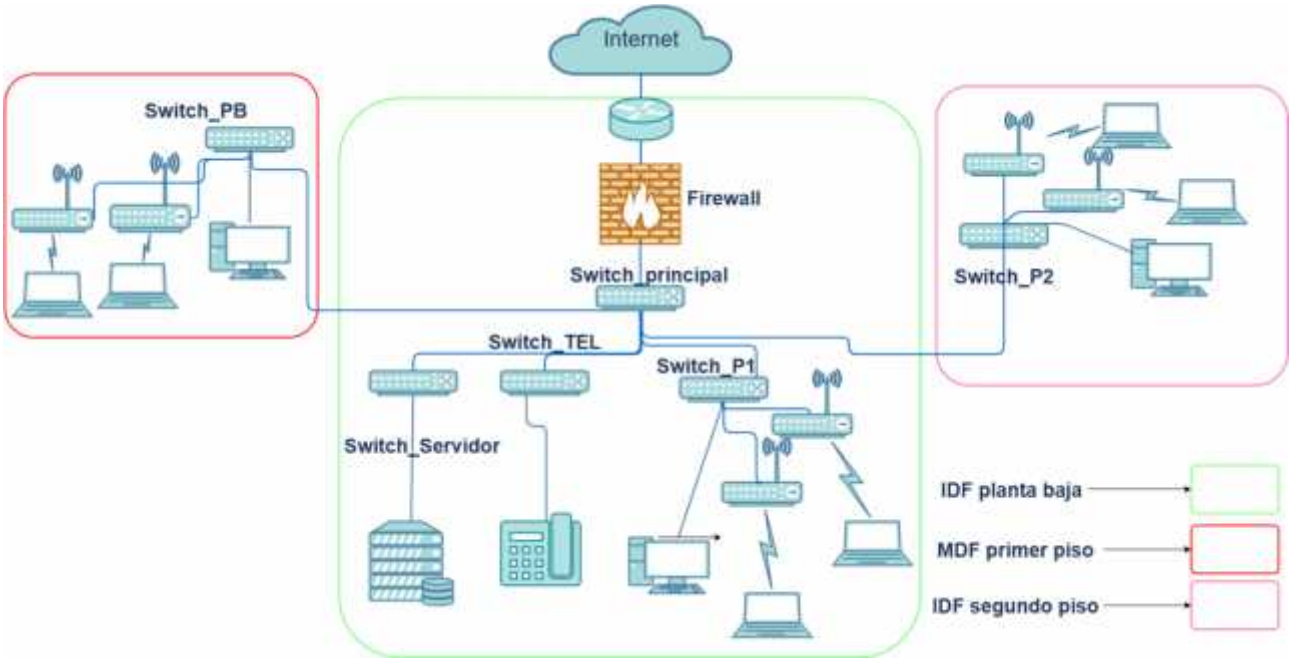
192. **Seguridad web,** dará un bloqueo a las amenazas web y bloquea el acceso a sitios web maliciosos, protegerá el gateway web en las instalaciones o la nube

III.1.2.6. Desarrollar estrategias de administración de red

193. En la red se implementaron las siguientes estrategias de administración de red:

- Administración los equipos por áreas o subredes asignando host-name a cada uno.
- Optimizar el ancho de banda por subred.
- Implementar protocolos en la implementación de vlans esta es otra forma de administrar la red debido a que se están implementando diferentes protocolos que son el IEEE 802.1Q, el STP y el VTP, que, como vimos anteriormente, son importantes cuando hacemos uso de las vlans.

- Aplicar un modelo de direccionamiento, el direccionamiento es una función clave de los protocolos de capa de Red que permite la transmisión de datos entre hosts de la misma red o en redes diferentes. El Protocolo de Internet versión 4 (IPv4) ofrece direccionamiento jerárquico para paquetes que transportan datos.
- Implementar Host-names a los equipos.



III.1.3. Desarrollar Diseño Físico

Figura 50: *Diseño físico de la red*

Fuente: Elaboración propia

Diseño físico planta baja

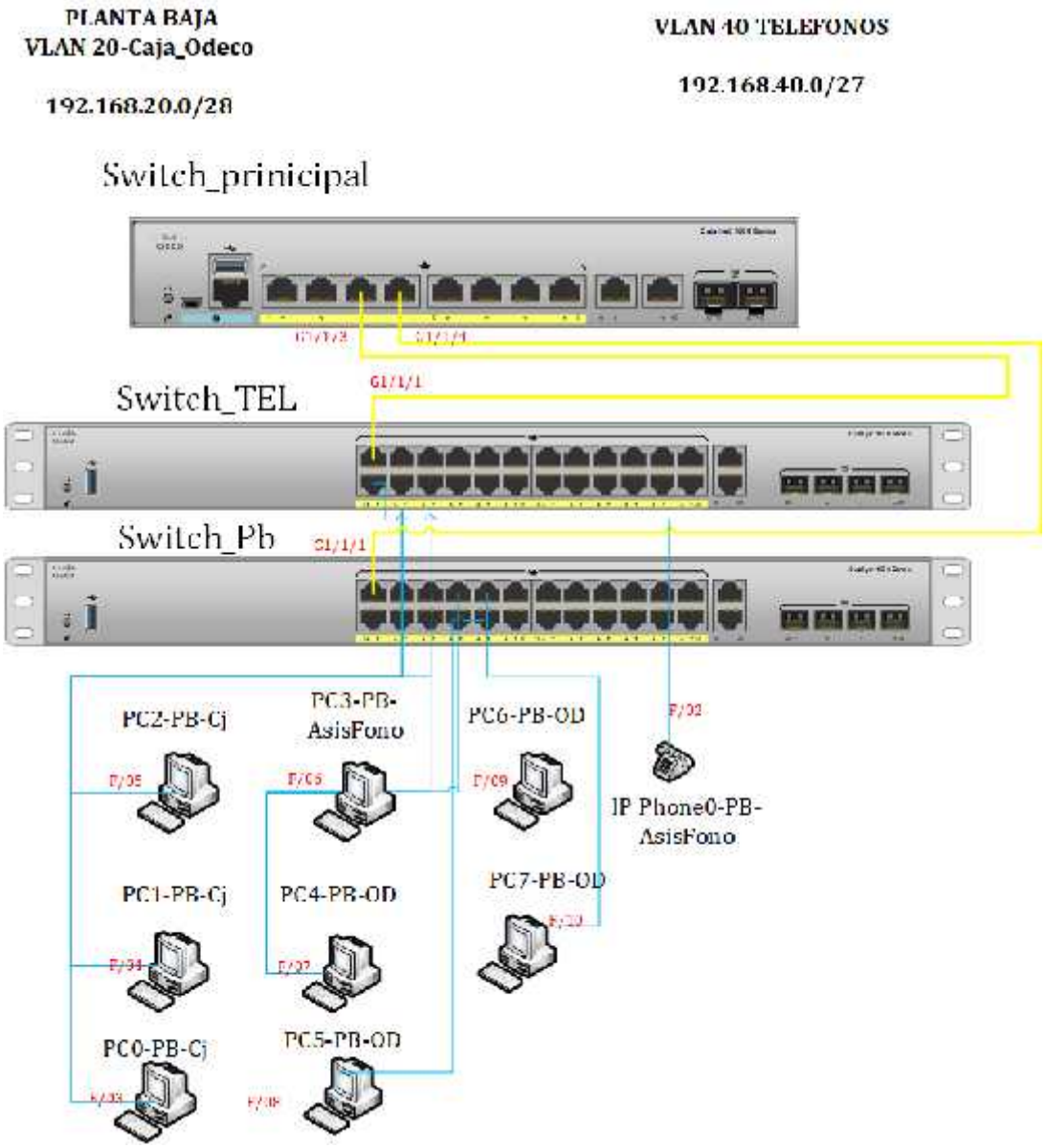


Figura 51: *Diseño físico planta baja*

Fuente: Elaboración propia

Diseño físico primer piso

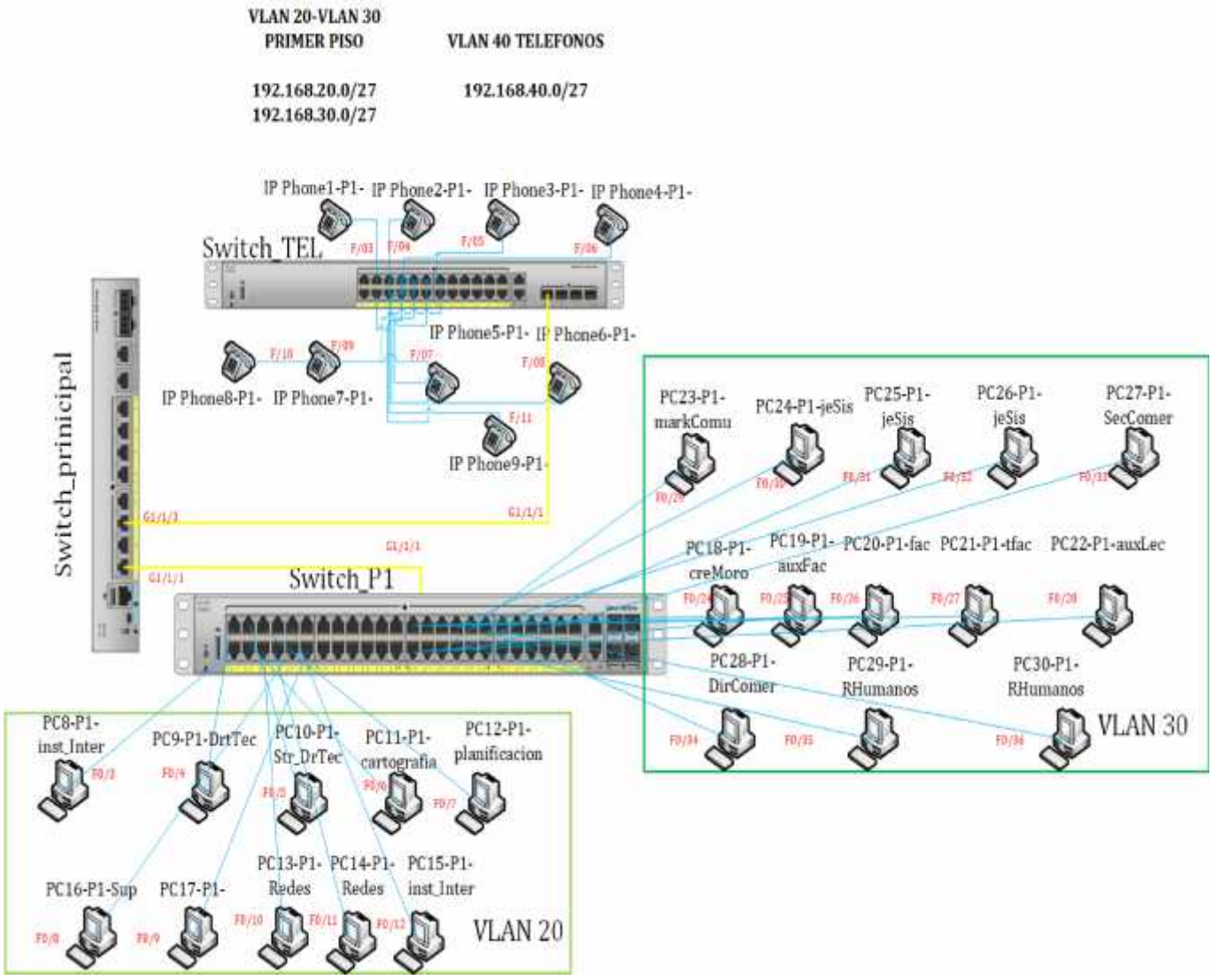
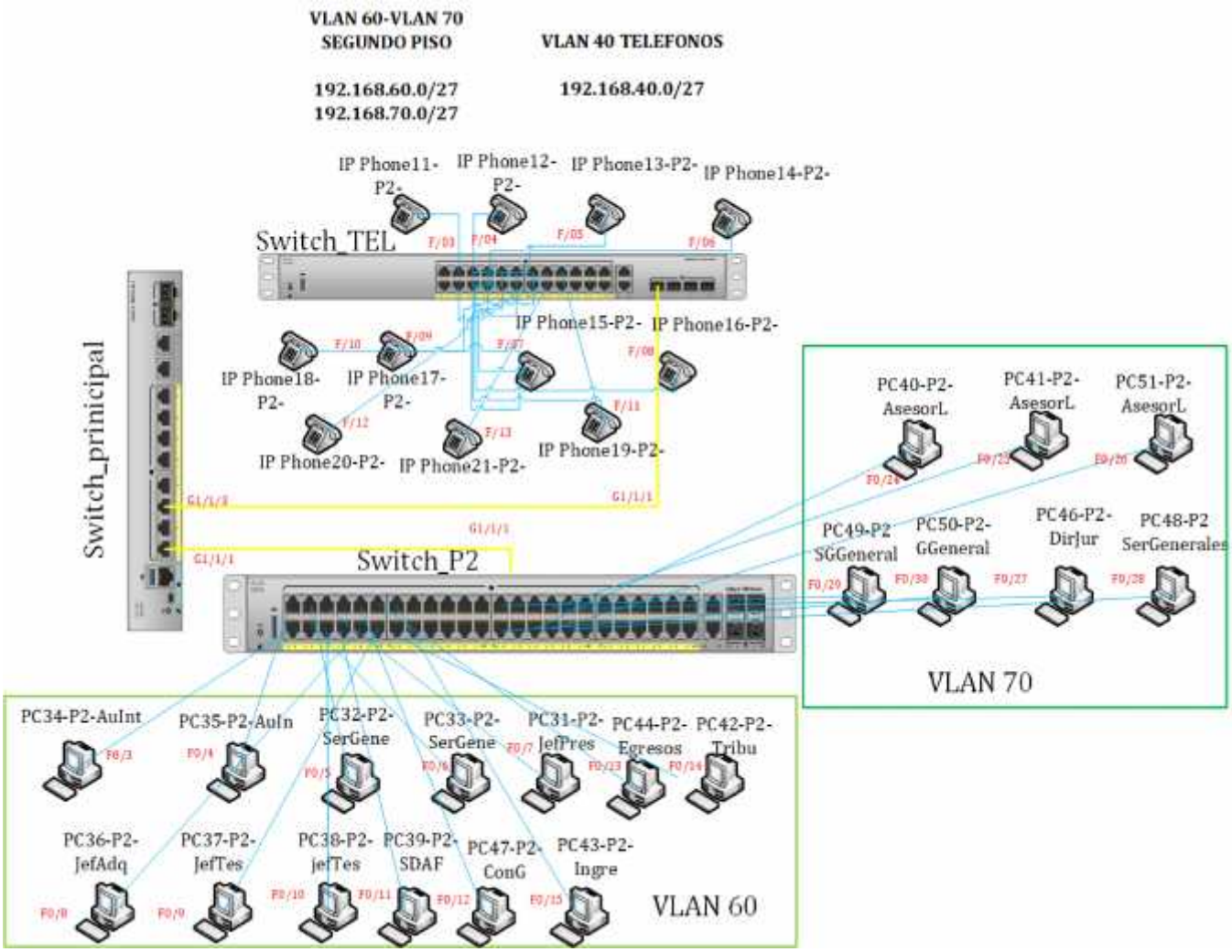


Figura 52: *Diseño físico primer piso*

Fuente: Elaboración propia

Diseño físico segundo piso



194.

Figura 53: *Diseño físico segundo piso*

Fuente: Elaboración propia

195.

III.1.3.1. Seleccionar tecnologías y dispositivos para redes de campus

III.1.3.1.1. Firewall perimetral

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

197. Teniendo en cuenta que este dispositivo firewall Fortinet FortiGate-100D será reutilizable para la nueva red de datos y se dará las siguientes características del equipo:

- Protección Firewall.
- Sistema de filtración.
- Análisis de antivirus.
- Alta disponibilidad de contenidos.
- Interfaces 2x1000Base-T RJ-45 (WAN).
- 20 puertos de RJ-45.
- Almacenamiento interno de 32 GB.

Figura 54: *Fortinet*

Fuente: (TIMIX)

III.1.3.1.2. Router Switch

198. Este dispositivo tiene la función de un arranque dual que permite elegir qué sistema operativo usar: el Router OS o SWOS. Para este equipo se utilizará como un router, ya que tiene las características de una capa 3.

199. También este dispositivo Mikrotik CRS326-24G-25 será reutilizable, ya que la empresa cuenta con este dispositivo y lo tiene funcionando como un router. Se dará las respectivas

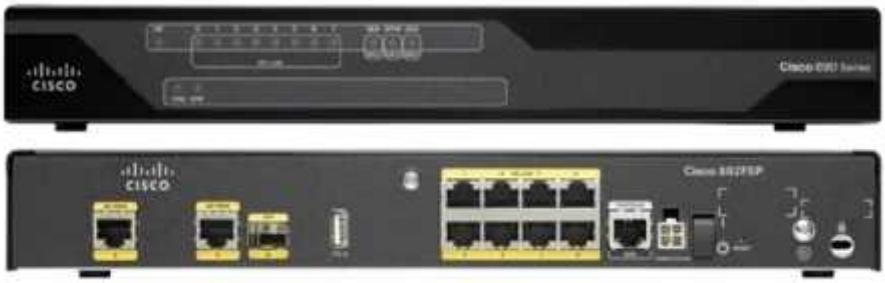
especificaciones de este dispositivo.

- Tamaño de RAM 512 MB
- Almacenamiento 16 GB
- Temperatura probada de -40 a 60 grados
- 24 puertos de Ethernet
- 2 puertos SFP
- Puerto de consola RJ45

Figura 55: *Mikrotik CRS326-24G-25*

Fuente: (MIKROTIC)

Router



200. También este dispositivo Router: Cisco 890 Series será reutilizable, ya que la empresa cuenta con este dispositivo y lo tiene funcionando como un switch. Se dará las respectivas especificaciones de este dispositivo.

- Puertos: Varían según el modelo, típicamente 8 x Gigabit Ethernet, 1 x SFP.
- Rendimiento: Hasta 25 Mbps VPN throughput.
- Soporte VLAN: Sí.
- Seguridad: Firewall integrado, VPN, filtrado de contenido.
- Otras características: WAN inalámbrica opcional, gestión avanzada con Cisco IOS.

Figura 56: *Router CISCO 890*

Fuente: (CISCO, CISCO, 2022)

III.1.3.1.3. Switch's

201. Los siguientes dispositivos serán reutilizables, ya que la empresa cuenta con este dispositivo y se encuentra en buen estado. Se dará las respectivas especificaciones de este dispositivo.

Switch: Cisco Catalyst 2960 Series

- **Puertos:**
  - Variantes con 24 o 48 puertos Gigabit Ethernet
  - Opciones con puertos SFP para fibra óptica

- **VLANs:** Soporte para VLANs 802.1Q

- **Rendimiento:**
  - Capacidad de conmutación: Hasta 216 Gbps (según modelo)
  - Capacidad de reenvío: Hasta 107.1 Mbps (según modelo)

- **Funciones adicionales:**
  - PoE/PoE+ en modelos seleccionados
  - Administración avanzada de red con Cisco IOS

Figura 57: *Switch Catalyst 2960*

Fuente: (CISCO, CISCO, 2019)

202. **Switch: Cisco Catalyst Plus Series si-poe-8**

- **Puertos:**
  - 8 puertos Gigabit Ethernet con PoE/PoE+
  - 2 puertos uplink SFP para fibra óptica
  - **VLANs:** Soporte para VLANs 802.1Q

- **Rendimiento:**
  - Capacidad de conmutación: 20 Gbps
  - Capacidad de reenvío: 14.88 Mbps

- **Funciones adicionales:**
- Potencia PoE total: Hasta 124 W
- Administración basada en web y CLI

Figura 58: *Switch Cisco Catalyst Plus Series si-poe-8*

Fuente: (CISCO, tonitrus)

Switch: Alcatel Lucent Omnistack LS6248P

203. **Puertos:**

- 48 puertos Gigabit Ethernet
- 4 puertos SFP para fibra óptica
- **VLANs:** Soporte para VLANs 802.1Q

204. **Rendimiento:**

- Capacidad de conmutación: 176 Gbps
- Capacidad de reenvío: 130 Mbps

205. **Funciones adicionales:**

- PoE en todos los puertos
- Administración avanzada con OmniVista

Figura 59: *Switch Alcatel Lucent Omnistack LS6248P*

Fuente: (Alcatel, 2025)

III.1.3.1.4. Servidores

206. Los siguientes servidores serán reutilizables, ya que la empresa cuenta con este dispositivo y se encuentra en buen estado. Se dará las respectivas especificaciones de este dispositivo

207. **Servidor: HP DL38065**

- **Procesador:** Soporta hasta 2 procesadores Intel Xeon E5-2600 v4.
- **Memoria:** Hasta 3 TB de RAM DDR4.
- **Almacenamiento:** Soporte para SAS/SATA/SSD, hasta 12 bahías de 3.5” o 24 de 2.5”.
- **Red:** Soporte para tarjetas de red con puertos SFP, UTP Cat6A.

208. **Otras características:** Gestión con iLO, redundancia de fuentes de poder y ventiladores.

Figura 60: *Servidor HP DL38065*

Fuente: (HP)

Servidor: Dell Power Edge VRTX

- **Procesador:** Soporta hasta 4 nodos de servidor, cada uno con hasta 2 procesadores Intel Xeon.
- **Memoria:** Hasta 1.5 TB  de RAM por nodo.
- **Almacenamiento:** Soporte para SAS/SATA/SSD, hasta 25 bahías de 2.5”.
- **Red:** Soporte para tarjetas de red con puertos SFP, UTP Cat6A.
- **Otras características:** Chasis de torre/rack, almacenamiento compartido, gestión con iDRAC

Figura 61: *Servidor Dell Power Edge VRTX*

Fuente: (DELL)

III.1.3.1.5. AP (puntos de acceso inalámbrico)

209. Tomando en cuenta los equipos de la empresa, los puntos de Acceso Inalámbricos (APs) recomendados son:

210. **Ubiquiti UniFi AP AC Pro**

211. **Características:**

- Dual-band (2.4 GHz y 5 GHz).
- Velocidades de hasta 450 Mbps en 2.4 GHz y 1300 Mbps en 5 GHz.
- Soporte para VLANs.
- Alimentación PoE.
- Gestión centralizada a través de UniFi Controller.

212. **Cisco Aironet 1830 Series**

213. **Características:**

- Dual-band.
- Velocidades de hasta 867 Mbps en 5 GHz y 400 Mbps en 2.4 GHz.
- Soporte para VLANs.
- Alimentación PoE.
- Gestión avanzada a través de Cisco Wireless LAN Controller.

214. **Aruba Instant On AP22**

215. **Características:**

- Dual-band.
- Velocidades de hasta 574 Mbps en 2.4 GHz y 1200 Mbps en 5 GHz.
- Soporte para VLANs.
- Alimentación PoE.
- Gestión a través de la aplicación móvil y portal web.

216. Para la propuesta de implementación Wifi en la red de EMTAGAS, se propone agregar puntos de acceso inalámbricos como los Ubiquiti UniFi AP AC Pro, Cisco Aironet 1830 Series, o Aruba Instant On AP22. Estos APs pueden conectarse a tus switches PoE existentes, y con la configuración adecuada de VLANs y gestión centralizada, tendrás una red inalámbrica eficiente y bien integrada para la infraestructura cableada.

217. El APs, que propongo usar, es **Ubiquiti UniFi AP AC Pro** por el soporte de protocolos que este equipo tiene:

- IEEE 802.11 a/b/g/n/ac
- IEEE 802.1Q (VLAN Tagging)
- IEEE 802.3af (PoE)
- IEEE 802.11r (Fast Roaming)
- IEEE 802.11i (WPA3)
- IEEE 802.11k/v (Radio Resource Management)
- IEEE 802.11 e (QoS)

Figura 62: *AP Ubiquiti UniFi*

Fuente: (Ubiquiti)

III.1.3.1.6. Fibra Óptica

218. Para las conexiones dentro de la misma se propone Fibra óptica multimodo (Multimode), preferiblemente OM4 para soportar mayores velocidades y distancias.

219. El Multimodo (Multimode) tiene:

- **Usos:** Ideal para distancias cortas, típicamente dentro de edificios o campus.
- **Características:** Tiene un núcleo más grande (50 o 62.5 micrones) y es más adecuado para distancias cortas debido a la dispersión modal.
- **Aplicaciones:** Conexiones entre switches y servidores dentro de un mismo edificio o campus.

220. Se propone el uso del Protocolo y Transceptor.

- 10GBASE-SR (10 Gigabit Ethernet)
- **Velocidad:** 10 Gbps.
- **Distancia:** Hasta 400 metros con fibra OM4.
- **Transceptores:** SFP+ 10GBASE-SR.

Figura 63: *Cable de fibra*

Fuente: (PVL)

III.1.3.1.7. Cable UTP

221. Se reutilizará el cable de UTP Cat. 6ª para las conexiones entre equipos finales con los cuartos de Comunicación (IDFs y MDF).

Figura 64: *Cable UTP*

Fuente: (Steren)

III.1.4. Pruebas del diseño a través de la simulación

222. Para esta fase se utilizaron 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 #D observando de forma más clara la organización del cableado estructurado y GNS3 para la simulación del Firewall de forma realista dado que PacketTracer no cuenta con una configuración de forma clara de un Firewall. Y el uso de Sketchup para la visualización de la propuesta de cableado estructurado, localización de los cuartos de comunicación y la ubicación de los Aps.

III.1.4.1. PacketTracer

Para comenzar con la simulación en Cisco Packet Tracer lo primero que hay que hacer es armar el diseño de red que se necesita

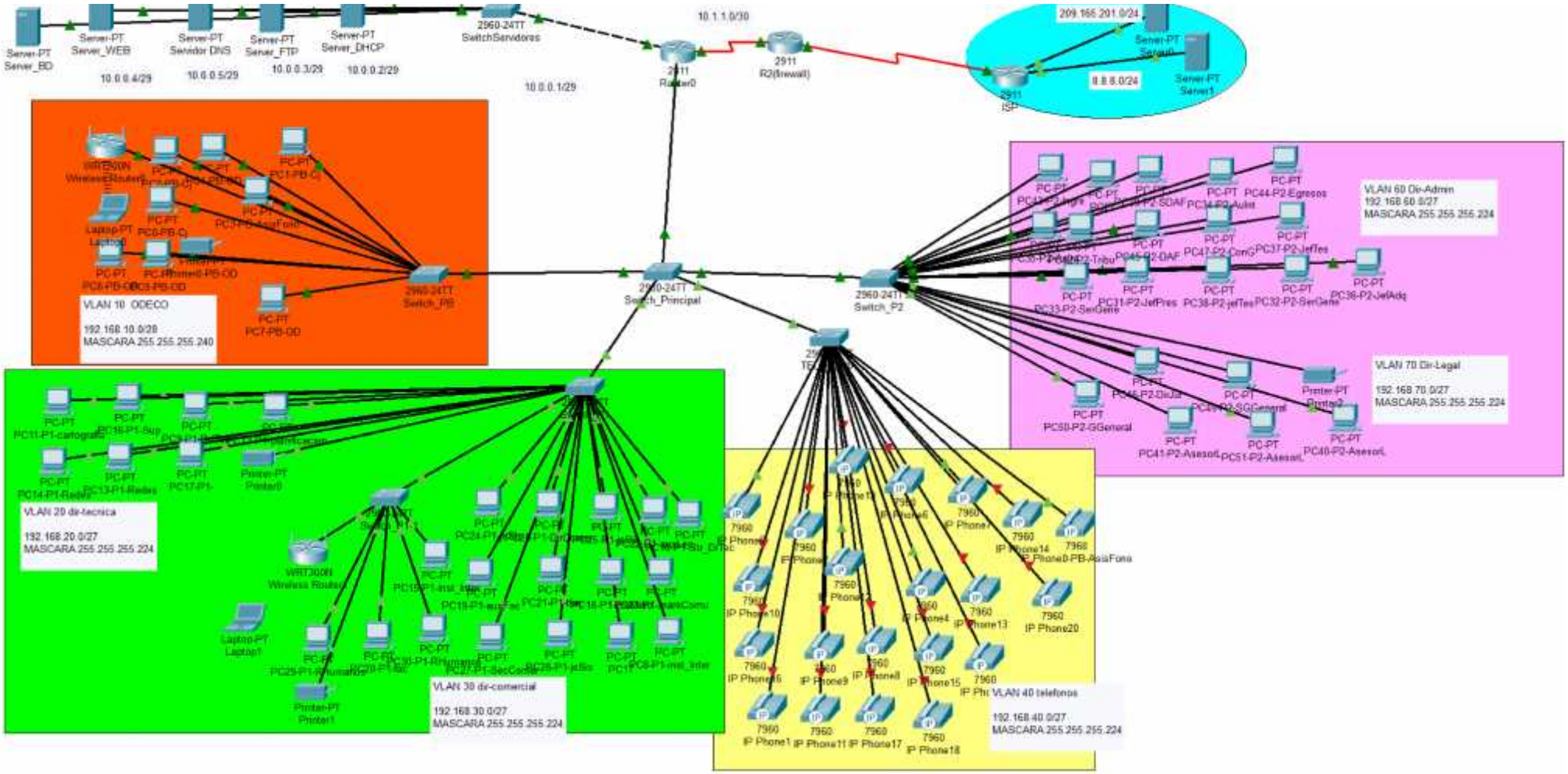


Figura 65: *Simulación lógica del diseño de la red en Packet Tracer*

Fuente: Elaboración propia

III.1.4.1.1. Diseño físico simulado en packet tracer

Planta baja

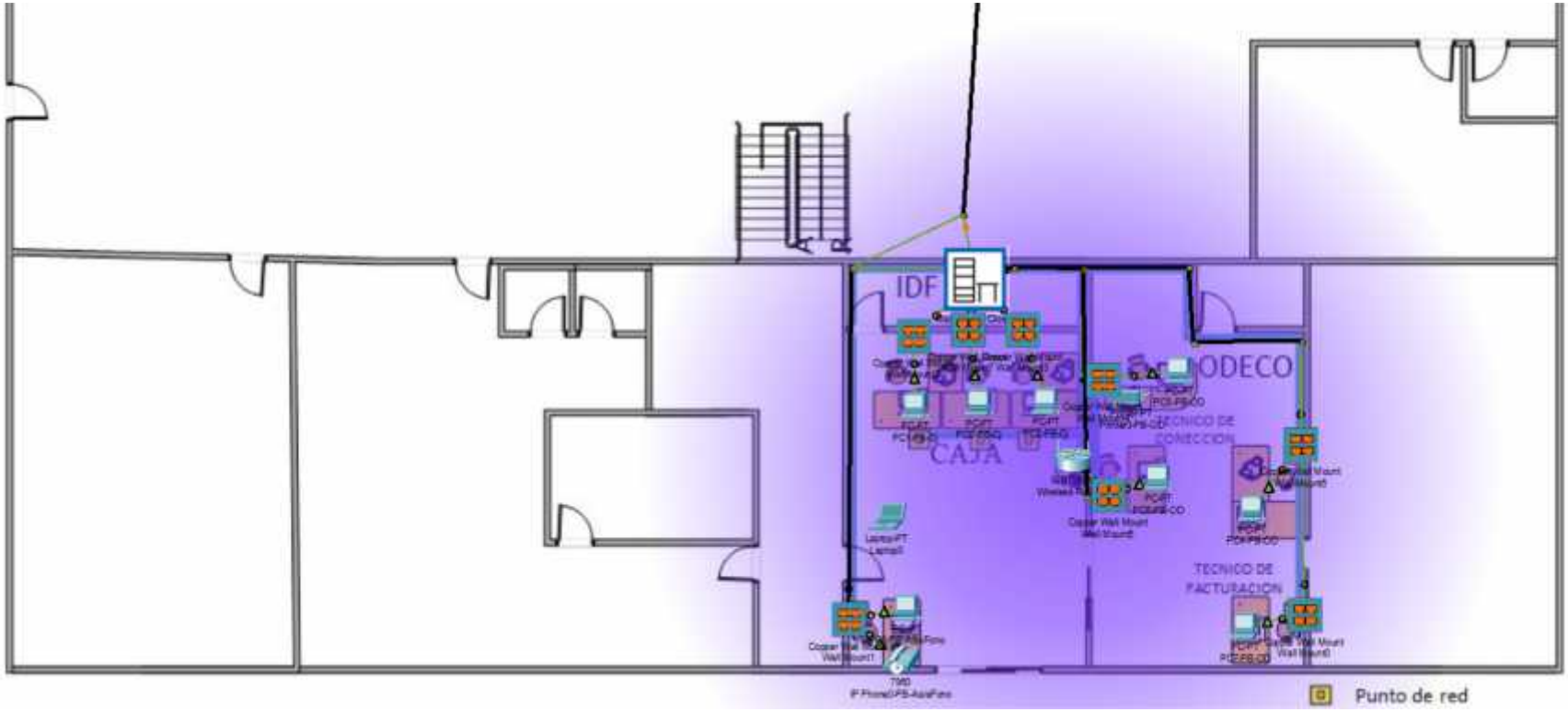


Figura 66: *Simulación física del diseño de la red en Packet Tracer*

Fuente: Elaboración propia

IDF de la planta baja

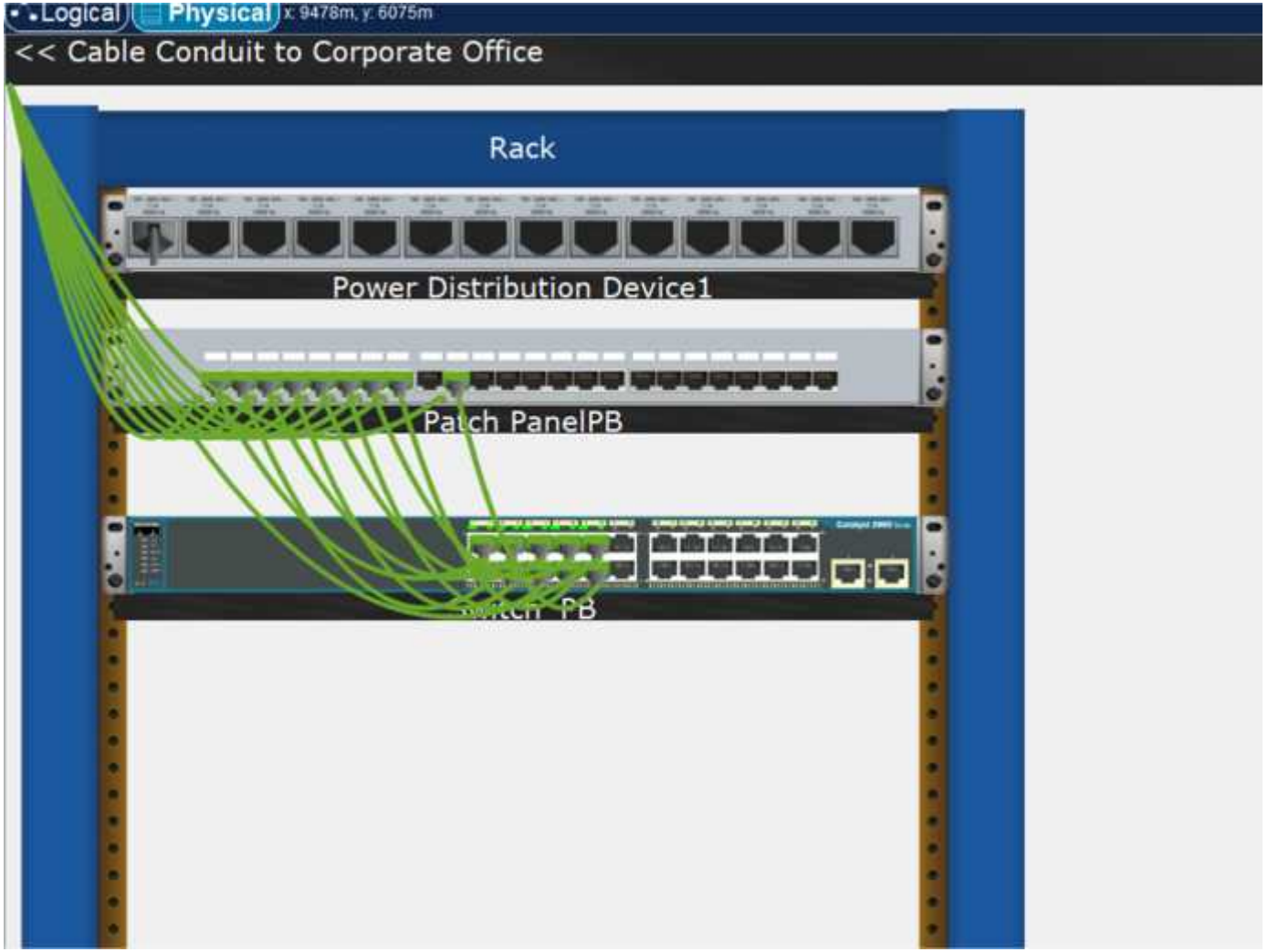


Figura 67: *Simulación del rack de la planta baja en Packet Tracer*

Fuente: Elaboración propia

Primer piso

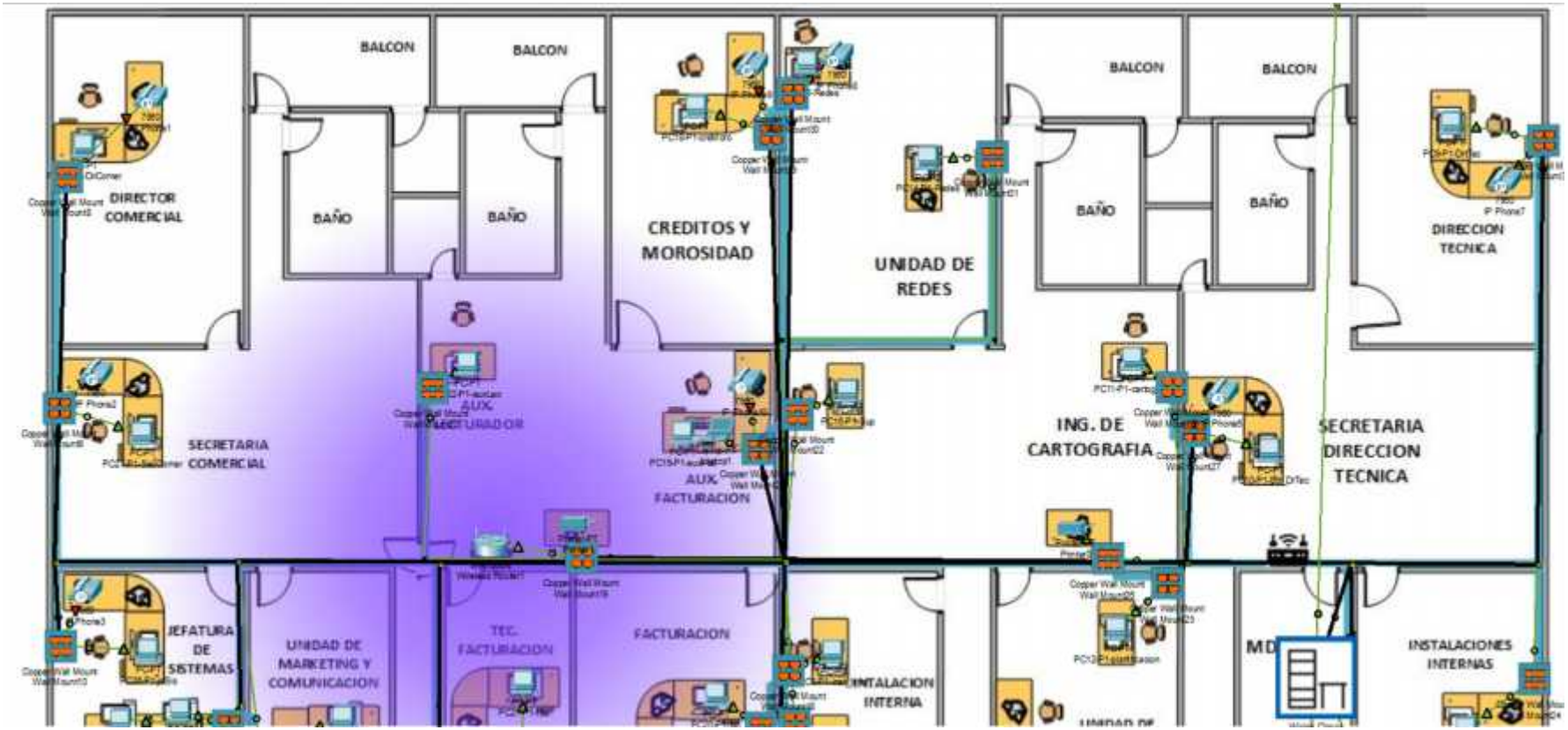


Figura 68: *Simulación física del primer piso en Packet Tracer*

Fuente: Elaboración propia

MDF primer piso

Figura 69: *Simulación del rack del primer piso en Packet Tracer*

Fuente: Elaboración propia

Segundo Piso

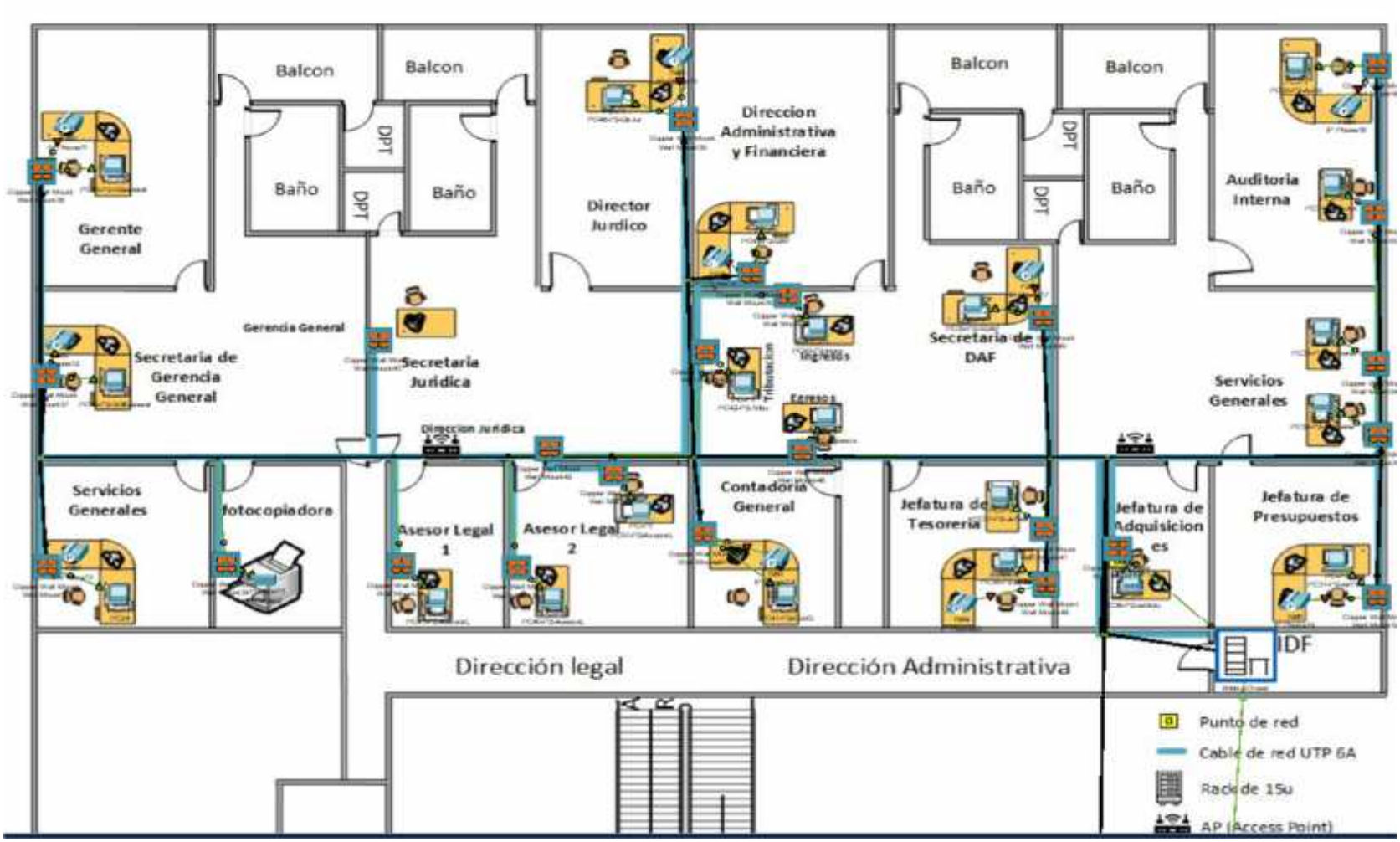


Figura 70: *Simulación física del segundo piso en Packet Tracer*

Fuente: Elaboración propia

IDF del segundo Piso

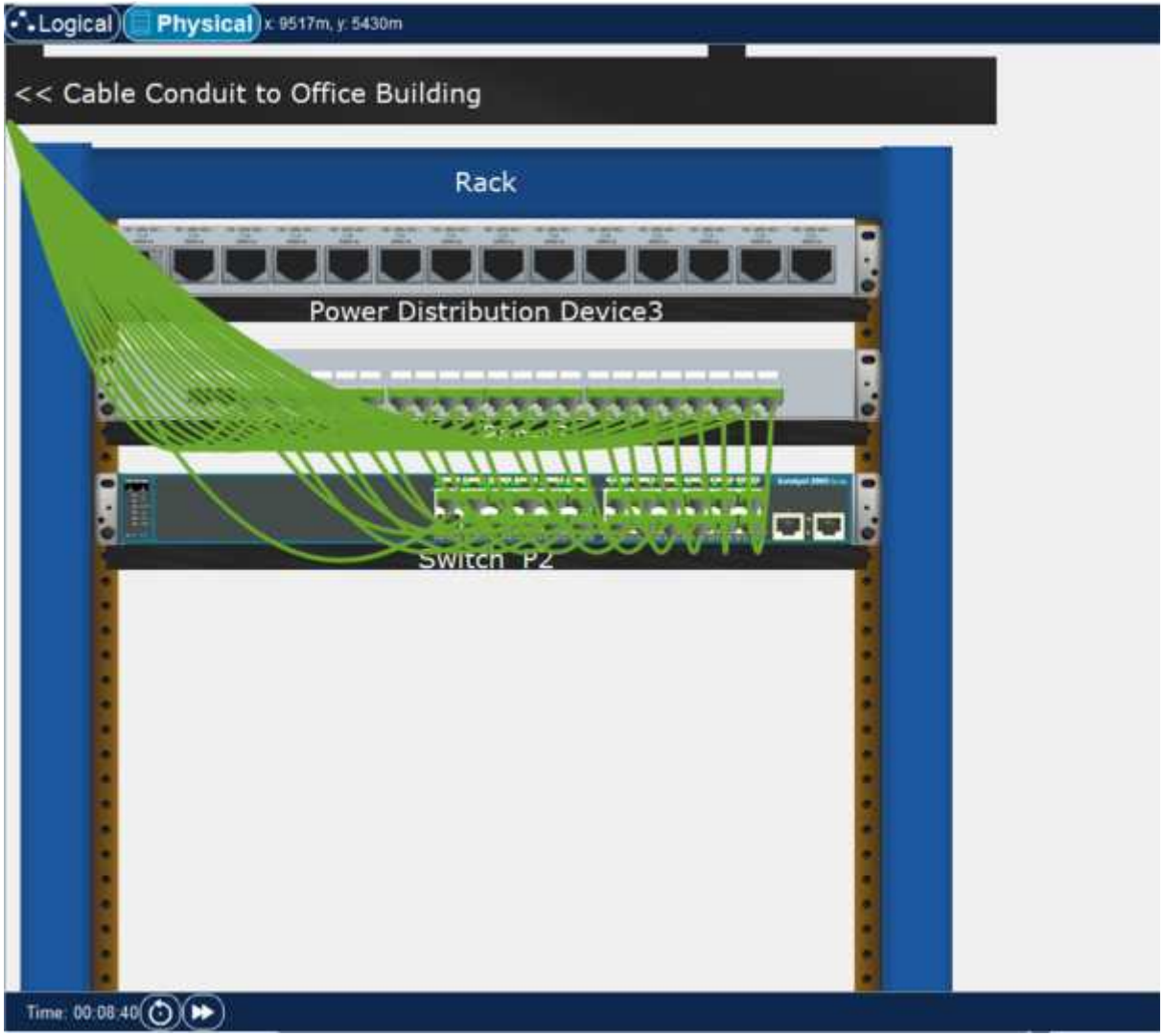


Figura 71: *Simulación del rack del segundo piso en Packet Tracer*

Fuente: Elaboración propia

223. Luego de armado el diseño, vamos a configurar los equipos para que tengan conexión y cumplan con lo mencionado en el diseño.

III.1.4.1.2. CONFIGURACIÓN DE ROUTER

224. Esta sección describe la configuración básica de la interfaz FastEthernet1/0 de un router. Este procedimiento se realiza para asignar una dirección IP a la interfaz, habilitarla y preparar la conectividad con otros dispositivos en la red.

Configuración de interfaces fastethernet

225. Se realizaron asignaciones de direcciones IP a diferentes interfaces FastEthernet. Estas configuraciones permiten al router interactuar con redes locales específicas.

226. **Interface FastEthernet1/0:**

- Dirección IP: `192.168.40.1`
- Máscara de red: `255.255.255.224`

227. **Propósito:** Representa una subred con hasta 30 hosts.

228. **Interface FastEthernet0/0:**

- Dirección IP: `10.0.0.1`
- Máscara de red: `255.255.255.248`

229. **Propósito:** Esta subred es más pequeña, con capacidad para 6 hosts, típicamente usada para enlaces entre routers o switches.

Comandos utilizados:

```
Interface fastethernet 0/0

ip address 10.0.0.1 255.255.255.248

no shutdown
```

```
Interface fastethernet 1/0

ip address 192.168.40.1 255.255.255.224

no shutdown
```

Configuración del Sistema de telefonía

230. El router está configurado para actuar como un sistema de telefonía IP utilizando Cisco CallManager Express (CME)**.**

Comando utilizado:

```
telephony-service

max-ephones 22
```

```
max-dn 22

auto assign 1 to 22
```

max-ephones: Define un máximo de 22 teléfonos IP (ephones).

max-dn: Define un máximo de 22 números de directorio (DNs).

auto assign: Asigna automáticamente los directorios numéricos a los teléfonos.

Configuración de un número de directorio (ephone-dn), comando utilizado:

```
ephone-dn 22

number 1022
```

ephone-dn 22: Crea un número de directorio para el ephone con ID 22.

number 1022: Asigna el número telefónico 1022 al directorio.

III.1.4.1.3. CONFIGURACIÓN BÁSICA DEL SWITCH PRINCIPAL

- **Asignación del nombre al switch**

El switch fue renombrado como **Switch_Principal** para identificarlo dentro de la red.

Comando utilizado:

```
hostname Swirch_Principal
```

- **Creación de las VLANs**

Para organizar la red, se crearon las siguientes VLANs:

VLAN 10 ODECO:

```
vlan 10
 name odeco
```

VLAN 20 Dirección técnica:

```
vlan 20
name dir.Tecnica
```

VLAN 30 Dirección comercial:

```
vlan 30
name dir.Comercial
```

VLAN 40 Telefonos:

```
vlan 40

name teléfonos
```

VLAN 50 servidores:

```
vlan 50

name servidores
```

VLAN 60 Dirección administrativa:

```
vlan 60

name dir.Admin
```

VLAN 70 Dirección legal:

```
vlan 70

name dir.Legal
```

- **Configuración de los puertos en trunk del switch**

Para que el switch pueda enviar y recibir tráfico de múltiples VLANs a través de un único puerto, se configuraron varios puertos en modo trunk.

Puerto FastEthernet 1/1 configurado para la conexión del router al switch principal, comandos utilizados:

```
interface FastEthernet 1/1

switchport mode trunk
```

```
switchport trunk allowed vlan 10,20,30,40,50
```

Puerto FastEthernet 0/6 configurado para la conexión del switch principal al switch del primer piso para la VLAN 10, comandos utilizados:

```
interface FastEthernet 0/6

switchport mode trunk

 switchport trunk allowed vlan 10
```

Puerto FastEthernet 0/2 configurado para la conexión del switch principal al switch del segundo piso para las VLANs 20 y 30, comandos utilizados:

```
interface FastEthernet 0/2

switchport mode trunk

switchport trunk allowed vlan 20,30
```

Puerto FastEthernet 0/5 configurado para la conexión del switch principal al switch del segundo piso para las VLANs 60 y 70, comandos utilizados:

```
interface FastEthernet 0/5

switchport mode trunk

switchport trunk allowed vlan 60,70
```

Puerto FastEthernet 0/7 configurado para la conexión del switch principal al switch del segundo piso para las VLANs 40, comandos utilizados:

```
interface FastEthernet 0/7

switchport mode trunk
```

```
switchport trunk allowed vlan 40
```

III.1.4.1.4 CONFIGURACION DEL SWITCH DE LA PLANTA BAJA

- **Configuración inicial del switch**

Para identificar este switch como parte del Primer Piso, se cambió su nombre a Switch_PB.

Comando utilizado:

```
hostname Switch_PB
```

- **Creación de VLANs**

VLAN 10 (odeco): Se creó la VLAN 10 para segmentar los dispositivos del Primer Piso.

Comando utilizado:

```
vlan 10

name odeco
```

- **Configuración de los puertos**

Configuración del Puerto Trunk (FastEthernet 0/24) este puerto conecta Switch_P1 con el Switch Principal y permite el tráfico de la VLAN 20.

Comando utilizado:

```
interface fastEthernet 0/24

switchport mode trunk

switchport trunk allowed vlan 10
```

Configuración de Puertos de Acceso (FastEthernet 0/1-23), los puertos 0/1 al 0/23 se configuraron como puertos de acceso y se asignaron a la VLAN 20 para conectar dispositivos finales.

Comando utilizado:

```
interface range fastEthernet 0/1-23

switchport mode access

switchport access vlan 10
```

III.1.4.1.5. CONFIGURACION DEL SWITCH DEL PRIMER PISO

- **Configuración inicial del switch**

Para identificar este switch como parte del Primer Piso, se cambió su nombre a Switch_P1.

Comando utilizado:

```
hostname Switch_P1
```

- **Creación de VLANs**

VLAN 20 (dir.Tecnica), VLAN 30 (dir.Comercial): Se creó la VLAN 20 y 30 para segmentar los dispositivos del Primer Piso.

Comando utilizado:

```
vlan 20

name dir.Tecnica
```

```
vlan 30

name dir.Comercial
```

- **Configuración de los puertos**

Configuración del Puerto Trunk (FastEthernet 0/24) este puerto conecta Switch_P1 con el Switch Principal y permite el tráfico de la VLAN 20.

Comando utilizado:

```
interface fastEthernet 0/24

switchport mode trunk

switchport trunk allowed vlan 20,30
```

Configuración de Puertos de Acceso (FastEthernet 0/1-12), los puertos 0/1 al 0/12 se configuraron como puertos de acceso y se asignaron a la VLAN 20 para conectar dispositivos finales.

Comando utilizado:

```
interface range fastEthernet 0/1-12

switchport mode access

switchport access vlan 20
```

Configuración de Puertos de Acceso (FastEthernet 0/13-23), los puertos 0/13 al 0/24 se configuraron como puertos de acceso y se asignaron a la VLAN 30 para conectar dispositivos finales.

Comando utilizado:

```
interface range fastEthernet 0/13-23

switchport mode access
```

switchport access vlan 30

CONFIGURACION DEL SWITCH DEL SEGUNDO PISO

- **Configuración inicial del switch**

Para identificar este switch como parte del Segundo Piso, se cambió su nombre a Switch_P2.

Comando utilizado:

```
hostname Switch_P2
```

- **Creación de VLANs**

VLAN 60 (dir.Admin), VLAN 70 (dir.Legal): Se creó la VLAN 60 y 70 para segmentar los dispositivos del Segundo Piso.

Comando utilizado:

```
vlan 60

name dir.Admin
```

```
vlan 70

name dir.Legal
```

- **Configuración de los puertos**

Configuración del Puerto Trunk (FastEthernet 0/24) este puerto conecta Switch_P1 con el Switch Principal y permite el tráfico de la VLAN 20.

Comando utilizado:

```
interface fastEthernet 0/24
```

switchport mode trunk

```
switchport trunk allowed vlan 60,70
```

Configuración de Puertos de Acceso (FastEthernet 0/1-12), los puertos 0/1 al 0/12 se configuraron como puertos de acceso y se asignaron a la VLAN 70 para conectar dispositivos finales.

Comando utilizado:

```
interface range fastEthernet 0/1-12

switchport mode access

switchport access vlan 70
```

Configuración de Puertos de Acceso (FastEthernet 0/13-23), los puertos 0/13 al 0/23 se configuraron como puertos de acceso y se asignaron a la VLAN 60 para conectar dispositivos finales.

Comando utilizado:

```
interface range fastEthernet 0/13-23

switchport mode access

switchport access vlan 60
```

III.1.4.1.6. CONFIGURACION DEL SWITCH TELEFONIA

- **Configuración inicial del switch**

Para identificar este switch como parte de telefonia, se cambió su nombre a Switch_TELEFONIA.

Comando utilizado:

```
hostname Switch_TELEFONIA
```

- **Creación de VLANs**

VLAN 40 (TELEFONIA): Se creó la VLAN 40 para segmentar los teléfonos que se encuentran en todos los pisos

Comando utilizado:

```
vlan 40
```

```
name TELEFONIA
```

- **Configuración de los puertos**

Configuración del Puerto Trunk (FastEthernet 0/24) este puerto conecta Switch_TELEFONIA con el Switch Principal y permite el tráfico de la VLAN 40.

Comando utilizado:

```
interface fastEthernet 0/24

switchport mode trunk

switchport trunk allowed vlan 40
```

Configuración de Puertos de Acceso (FastEthernet 0/1-23), los puertos 0/1 al 0/23 se configuraron como puertos de acceso y se asignaron a la VLAN 40 para conectar dispositivos finales.

Comando utilizado:

```
interface range fastEthernet 0/1-23
```

switchport mode access

switchport access vlan 40

III.1.4.1.7. Pruebas y medios de verificación

Prueba de conectividad entre dispositivos

Desde un dispositivo final (PC) a las VLANs

VLAN 10

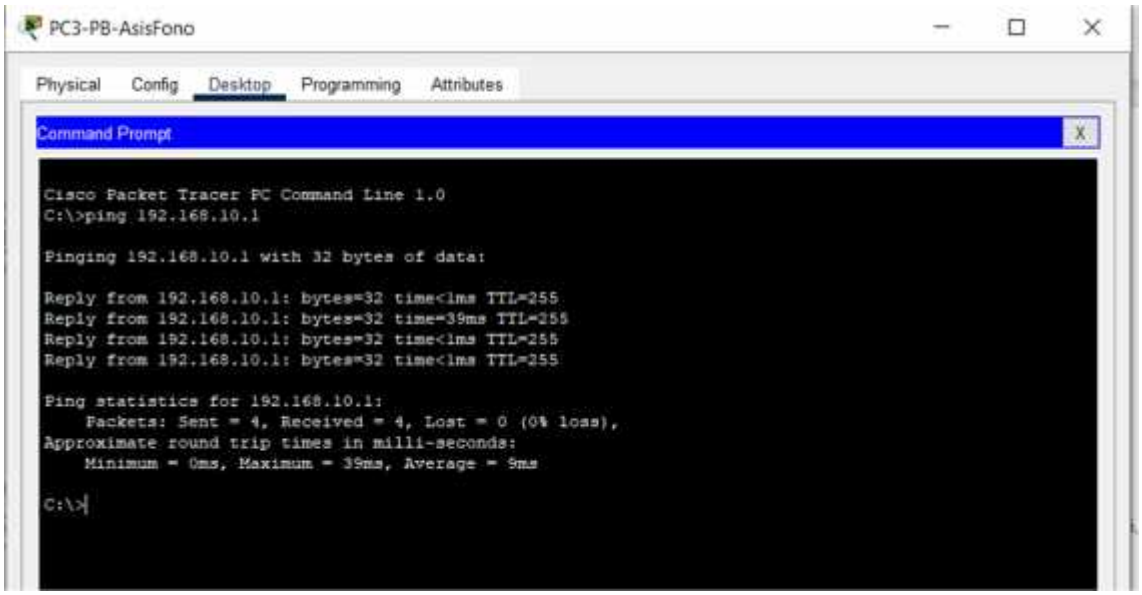


Figura 72: *Prueba de ping desde una PC a la VLAN 10*

Fuente: Elaboración propia

VLAN 20

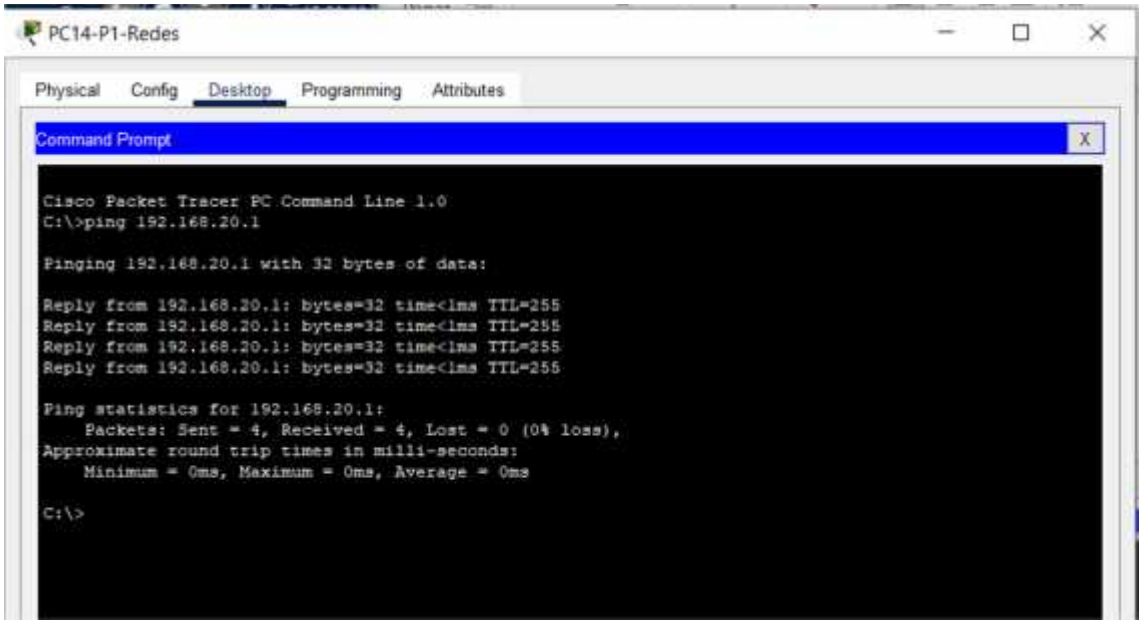


Figura 73: *Prueba de ping desde una PC a la VLAN 20*

Fuente: Elaboración propia

VLAN 30

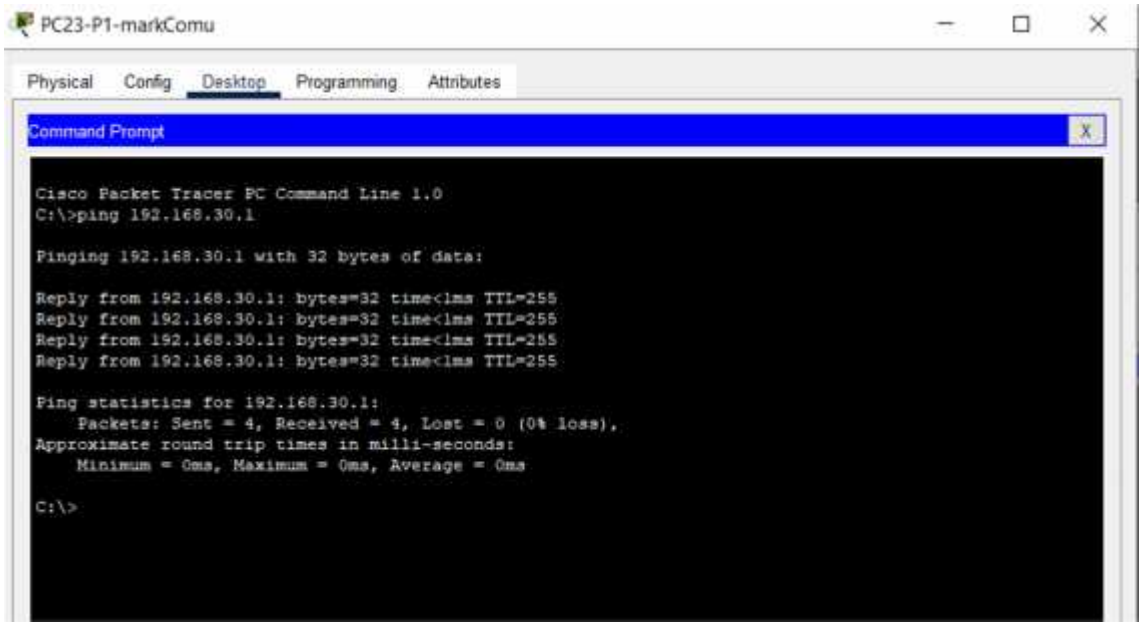


Figura 74: *Prueba de ping desde una PC a la VLAN 30*

Fuente: Elaboración propia

VLAN 60

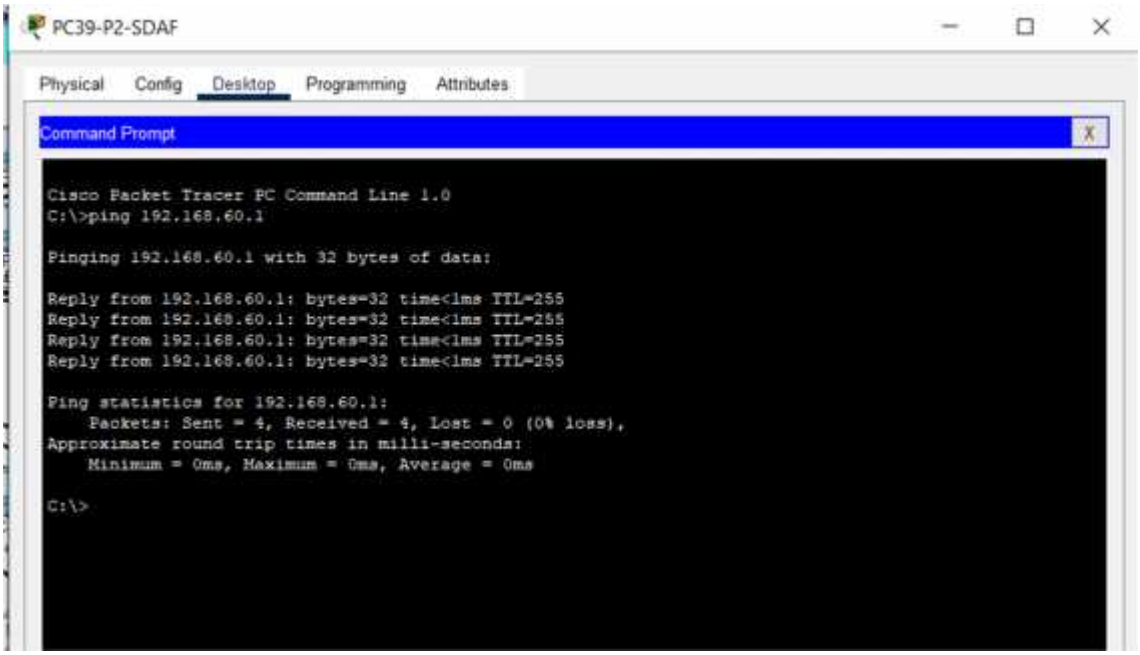


Figura 75: *Prueba de ping desde una PC a la VLAN 60*

Fuente: Elaboración propia

VLAN 70

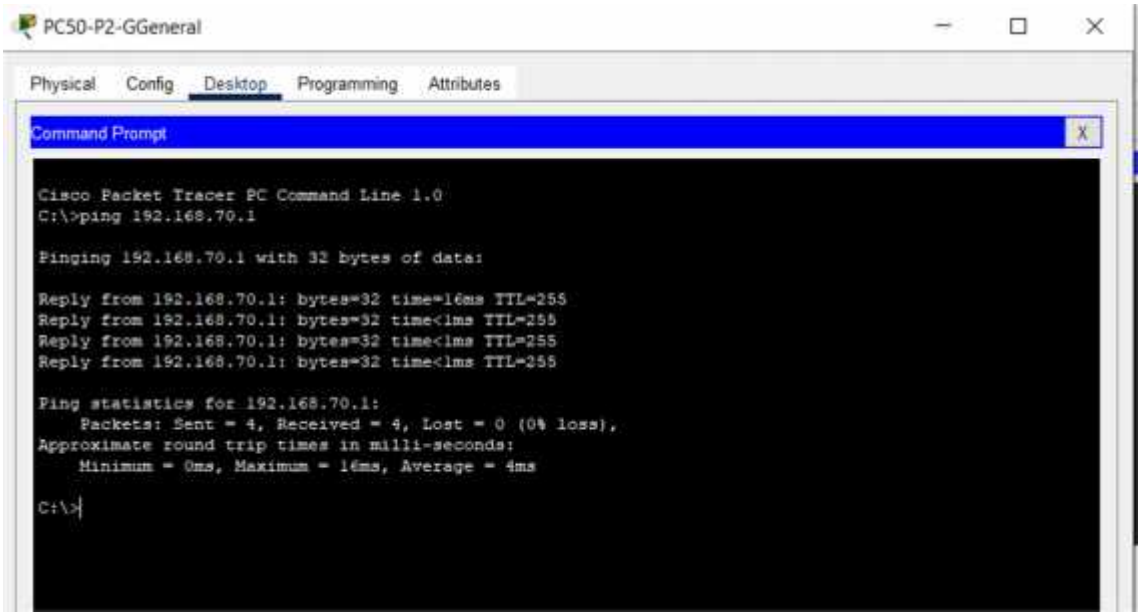


Figura 76: *Prueba de ping desde una PC a la VLAN 70*

Fuente: Elaboración propia

Pruebas de configuración de VLANs y Troncales

Validación de la correcta segmentación y propagación de VLANs en el Switch

Switch principal

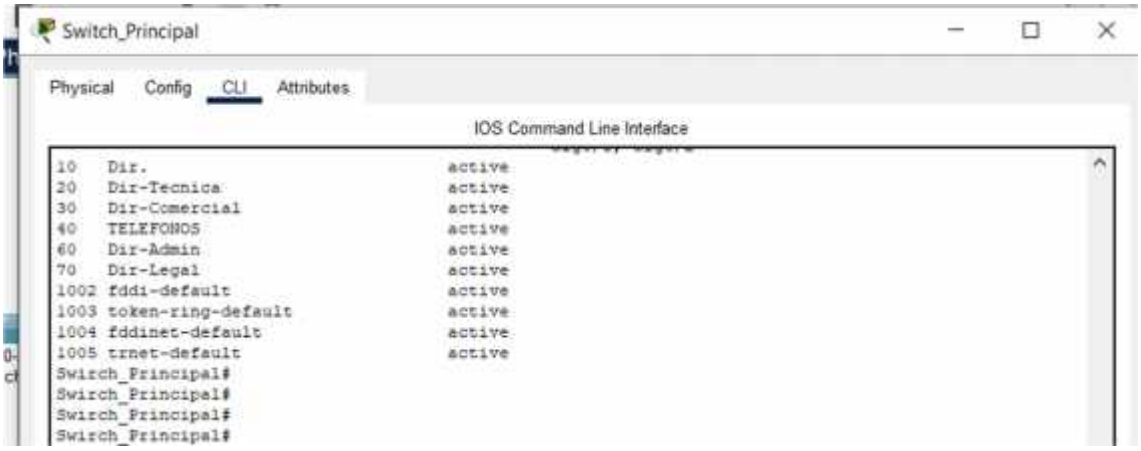


Figura 77: *Prueba de la creación de VLANs en el Switch-principal*

Fuente: Elaboración propia

Switch de planta Baja

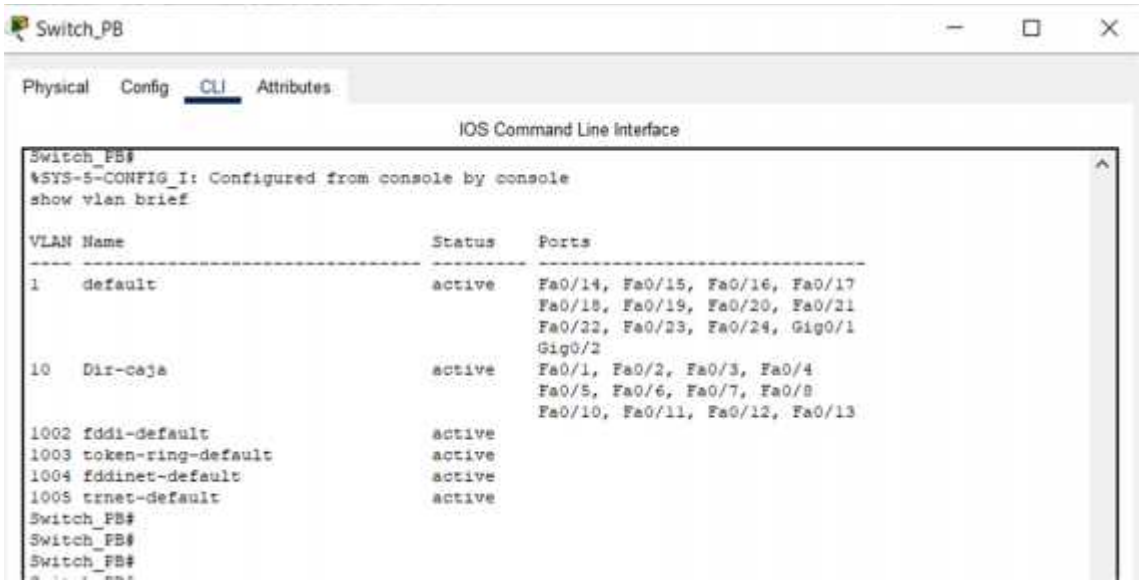


Figura 78: *Prueba de la creación de VLANs en el Switch-PB*

Fuente: Elaboración propia

Switch del primer piso

Figura 79: *Prueba de la creación de VLANs en el Switch-P1*

Fuente: Elaboración propia

Switch del Segundo Piso

Figura 80: *Prueba de la creación de VLANs en el Switch-P2*

Fuente: Elaboración propia

Validación de enlaces troncales en el Switch principal

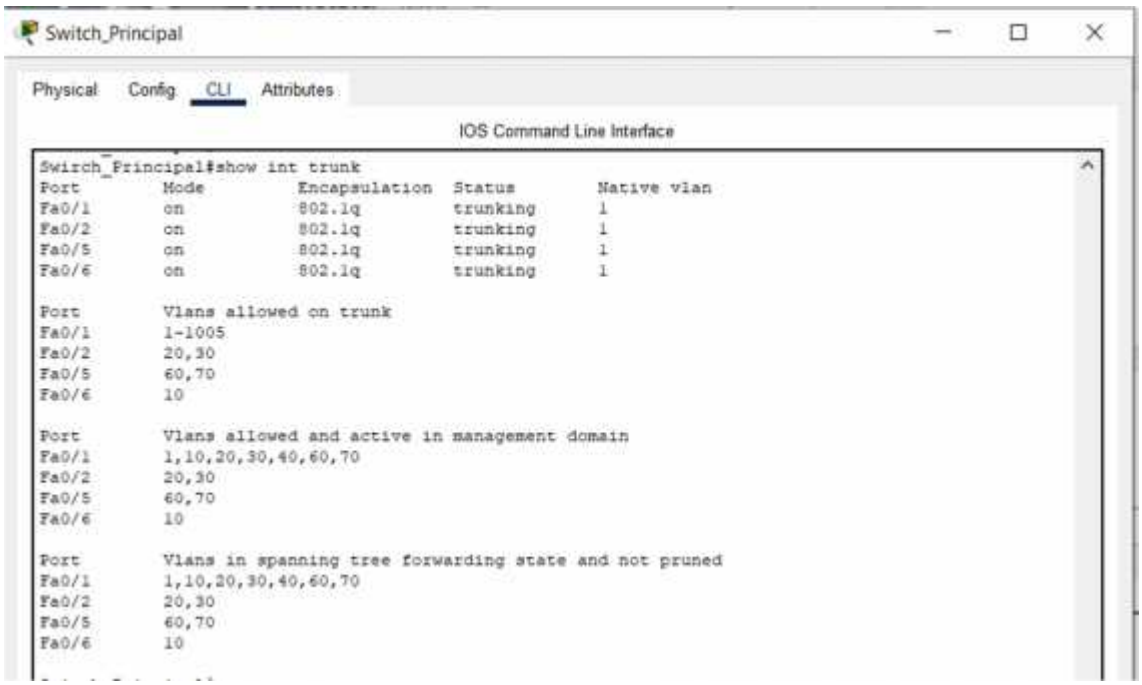


Figura 81: *Prueba de enlaces troncales en el Switch-principal*

Fuente: Elaboración propia

Prueba de asignación de DHCP

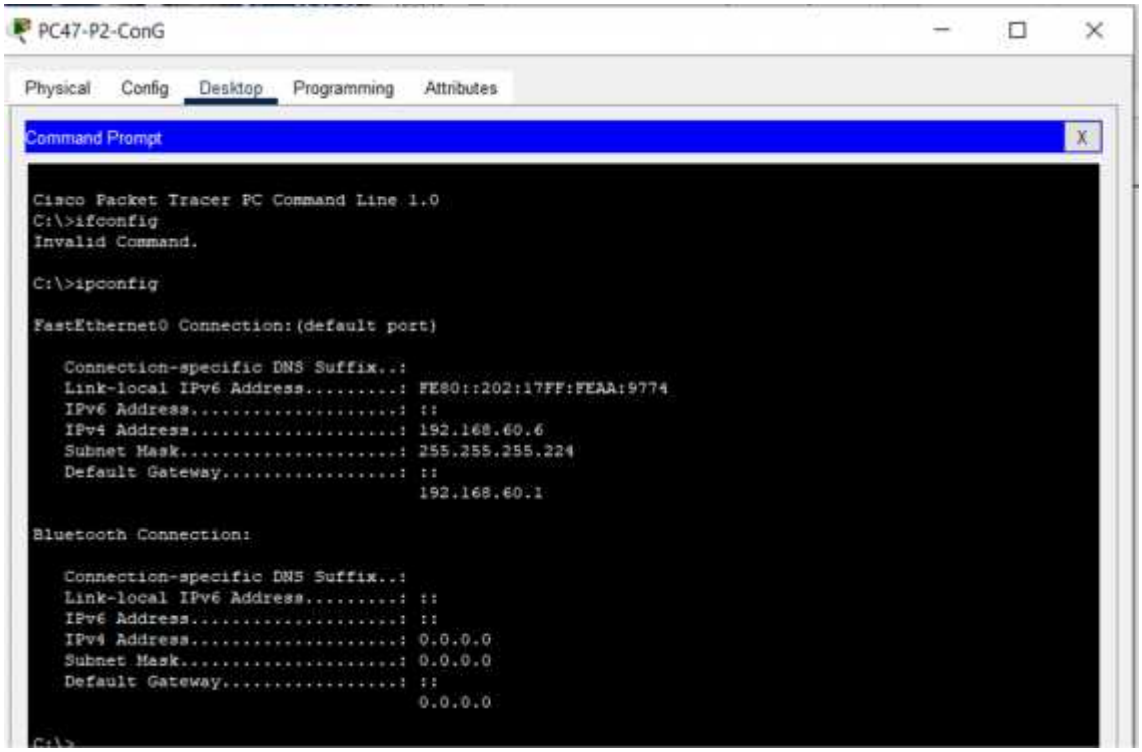


Figura 82: *Prueba de asignación de DHCP en el servidor mediante ping a una PC*

Fuente: Elaboración propia

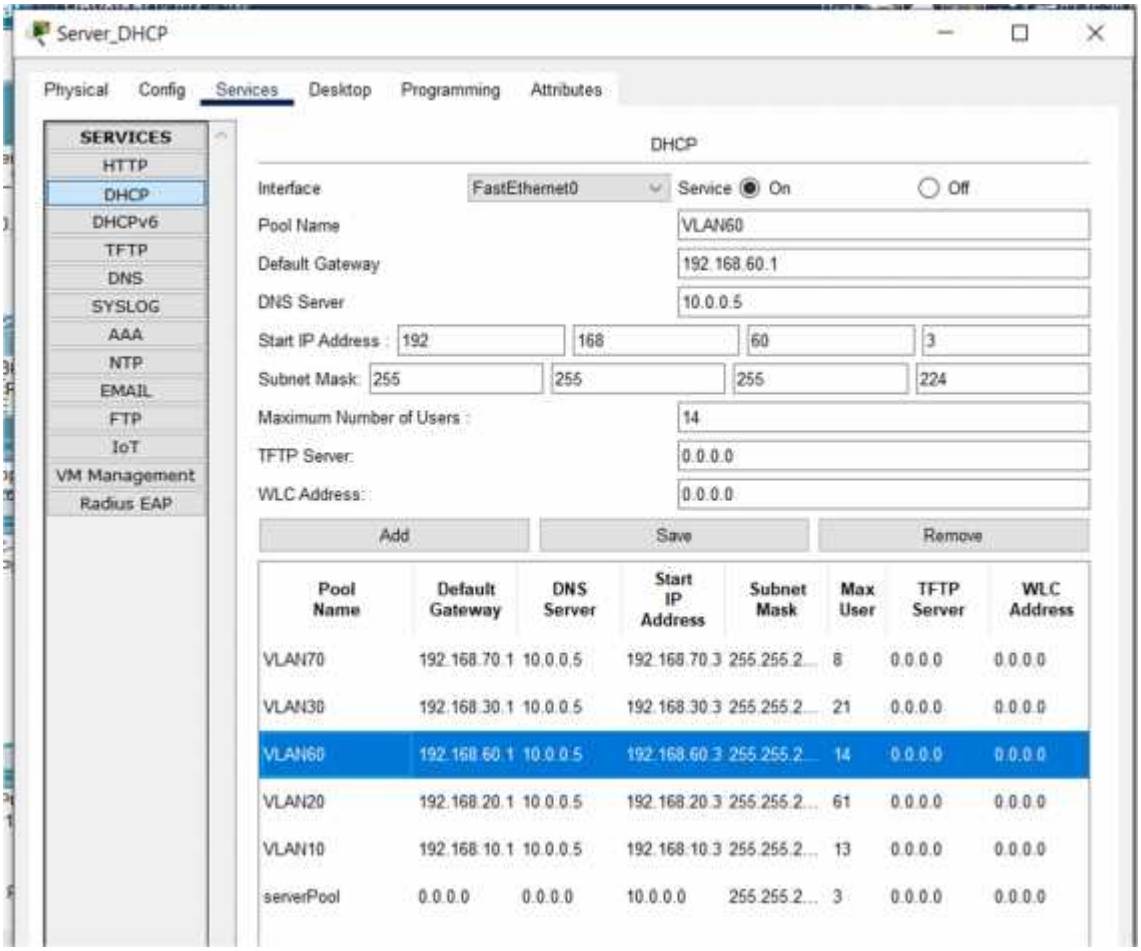


Figura 83: *Prueba de asignación de DHCP en el servidor*

Fuente: Elaboración propia

Prueba de conectividad a internet

Figura 84: *Prueba de conectividad a internet desde una PC*

Fuente: Elaboración propia

Prueba de acceso a internet de todas las Vlans

Figura 85: *Prueba de asignación de ACL para el acceso a internet en el router*

Fuente: Elaboración propia

III.1.4.1.8. Listado de comandos de verificación

231. Router

- *Show ip interface brief*: muestra un resumen del estado de todas las interfaces del router
- *show running-config:* permite revisar toda la configuración actual aplicada al router.
- *show cdp neighbors:* Confirma qué dispositivos están conectados directamente al router.
- *show access-lists:* muestra las ACL configuradas en el dispositivo.
- *show running-config | include access-group:* confirma en qué interfaces se han aplicado las ACLs.
- *show ip dhcp binding:* confirma las direcciones IP asignadas por el servidor DHCP.
- Switch
- *show interfaces status:* verifica el estado de los puertos del switch (administrativo y operativo).
- *show vlan brief:* confirma qué VLANs están creadas y a qué puertos están asignadas.
- *show interfaces trunk:* verifica los puertos configurados como troncales y las VLANs permitidas.
- *show cdp neighbors:* confirma qué dispositivos están conectados directamente al switch.
- *show vlan id <vlan-id>:* confirma qué puertos están asignados a una VLAN específica.

III.1.4.1.9. Lista de ACLs que se utilizaron

Permite que solo la VLAN 10 acceda hacia internet

- *R2(config)# access-list 1 permit 192.168.10.0 0.0.0.15* (Permitir solo la red VLAN 10)
- *R2(config)# access-list 1 deny any* (Denegar cualquier otra red)
- *R2(config)# access-list 1 permit any* (Permitir el resto del tráfico)
- *R2(config)# interface s0/0/1* (En la interfaz que conecta a Internet)
- *R2(config-if)# ip access-group 1 in* (Aplicar ACL 1 en el tráfico entrante)

Esto permite que solo los dispositivos de la **VLAN 10** puedan acceder a Internet, pero bloquea el acceso de otras VLANs hacia Internet.

Eliminación de una acl:

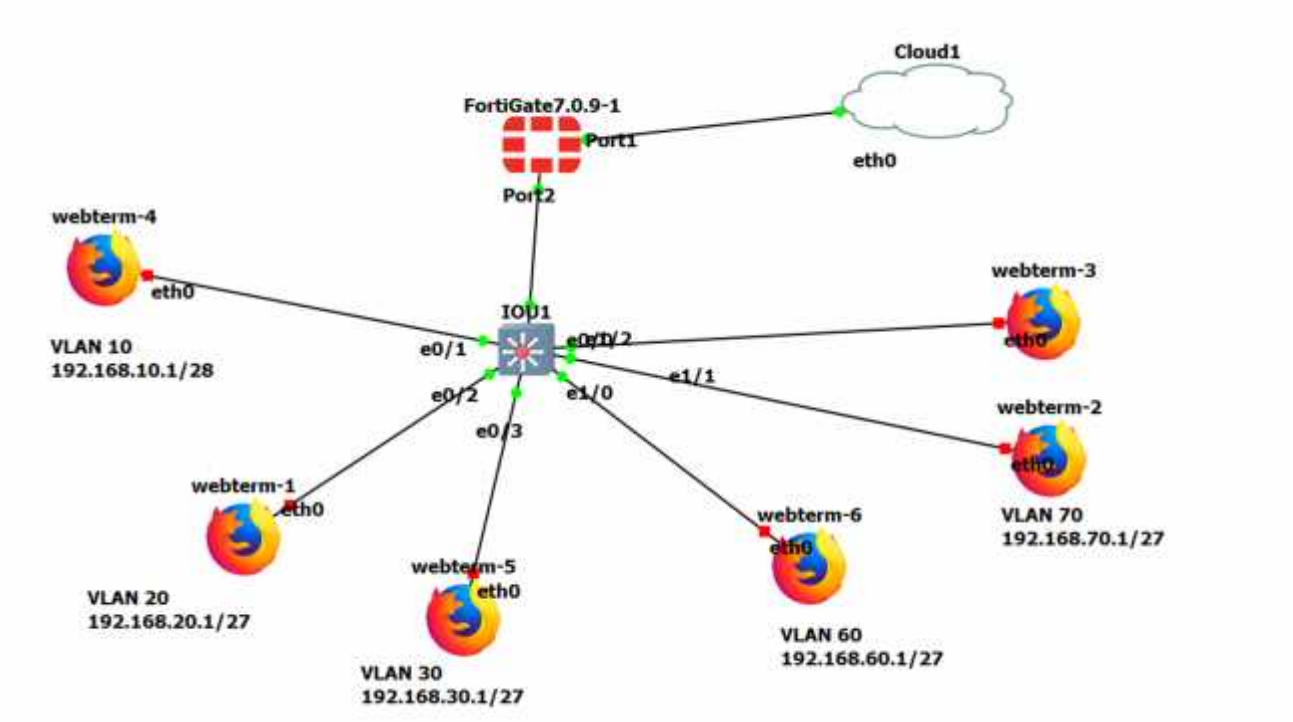
no access-list <número de grupo>

Quitar una acl de la interfaz:

Interface < puerto>

no ip access-group <número de grupo> in

III.1.4.2. Simulación en GNS3



232. Con el uso de la herramienta GNS3, se realizó la simulación de las políticas de seguridad aplicado en el firewall FortiGate.

233. Como primer paso a entender la simulación procederemos a la explicación de las configuraciones realizadas en la simulación, con el propósito de demostrar las políticas de seguridad que se pueden crear, para un mayor control y acceso a internet.

III.1.4.2.1. Creación de VLAN en el Firewall FortiGate

234. Descripción general de la creación de las VLAN's en el firewall

235. Crear una VLAN asignándole un identificador único es decir el ID, en este caso se debe asignar el número 10, se debe definir el nombre de la VLAN, como ser **"VLAN 10 (ODECO)".**

236. Asignación de interfaz, parámetros de IP y habilitación del DHCP

237. A continuación, se debe asignar una interfaz lógica a la **“VLAN 10 (ODECO)”**, esta interfaz será la puerta de enlace para los dispositivos que conformen a la **“VLAN 10 (ODECO)”,** en este caso será **“port2”.**

238. Se debe asignar la dirección **IP** a la interfaz **“VLAN 10 (ODECO)”**, con la **IP 192.168.10.1/28** con la **máscara 255.255.255.240**.

239. Habilitar el servicio **DHCP** dentro del equipo como servidor con el rango de dirección **192.168.10.2-192.168.10.14** con mascara **255.255.255.240**, y la habilitación del **DNS server 8.8.8.8.**

240. De la misma manera se debe configurar las demás VLAN’s, es decir: **VLAN 20(Dir-Técnica), VLAN 30(Dir-Comercial), VLAN 40(Dir-Tecnica), VLAN 60(Dir-Admin), VLAN 70(Dir-Legal).**

241. Ahora veremos como se crea en un firewall Fortigate.

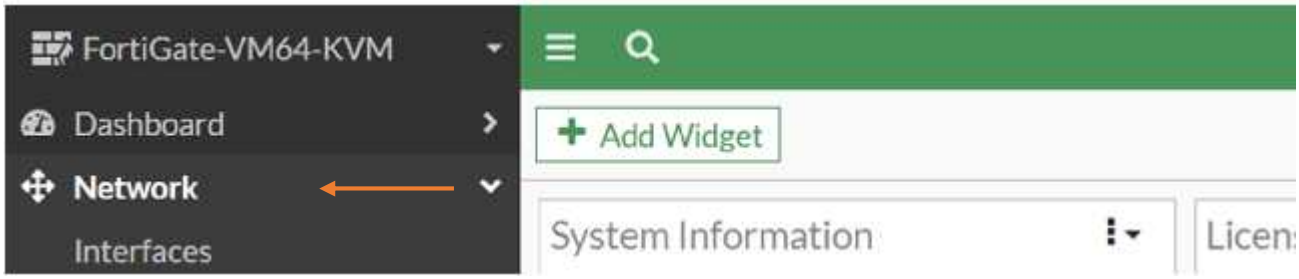


Figura 86: *Creación de interfaces en el FortiGate*

Fuente: Elaboración propia

242. Dirigirse a Network > Interfaces.

Crear una interfaz existente:

- **Name: VLAN_10**, ingresamos un nombre

- **Interface:** port2, selecciona la interfaz física que se conecta al switch, en este caso en la simulación es el puerto2.
- **VLAN ID: 10**, ingresamos un valor entero indicando el vlan correspondiente
- **IP/Netmask:** 192.168.10.1/28, se asigna un rango de IP,
- **DHCP Server**: Habilita el servidor DHCP
- **IP Range**: 192.168.10.2 – 192.168.10.31, se establece un rango

Y por último damos clic en **OK** para guardar.

En la simulación seria de esta forma:

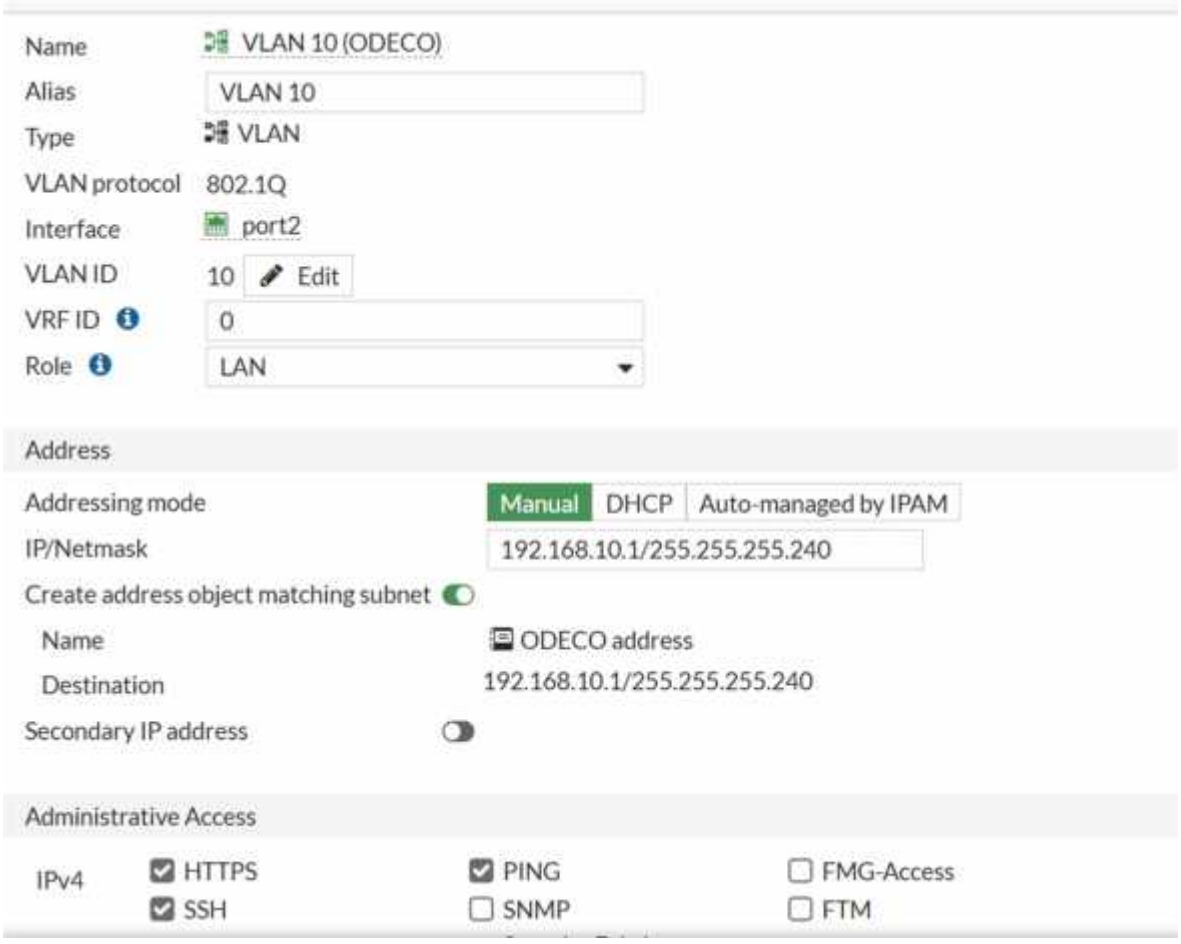
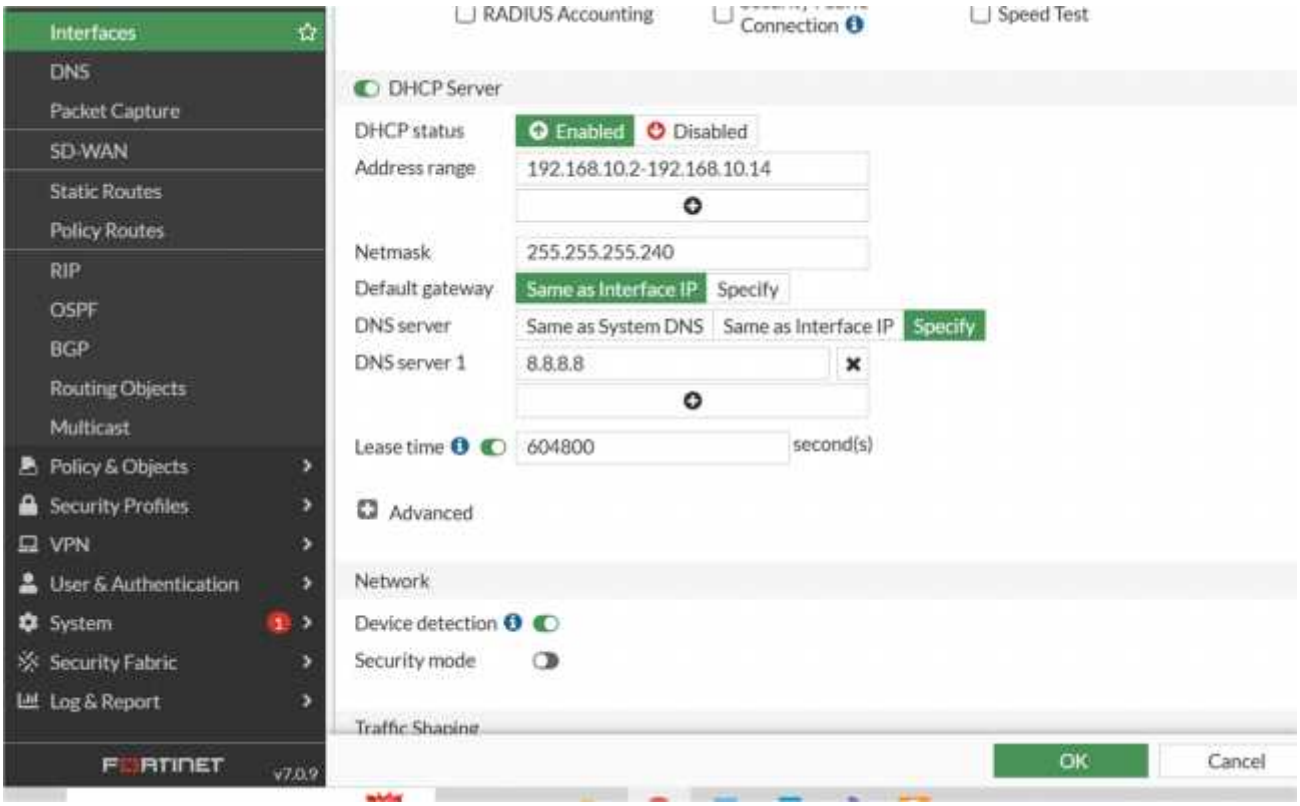


Figura 87: *Creación de la VLAN 10 con su dirección de red en el FortiGate*



Fuente: Elaboración propia

Figura 88: *Asignación de DHCP en el FortiGate*

Fuente: Elaboración propia

De la misma manera se deben crear las demás VLAN’s necesarias para la demostración, de tal forma se forma de esta manera.

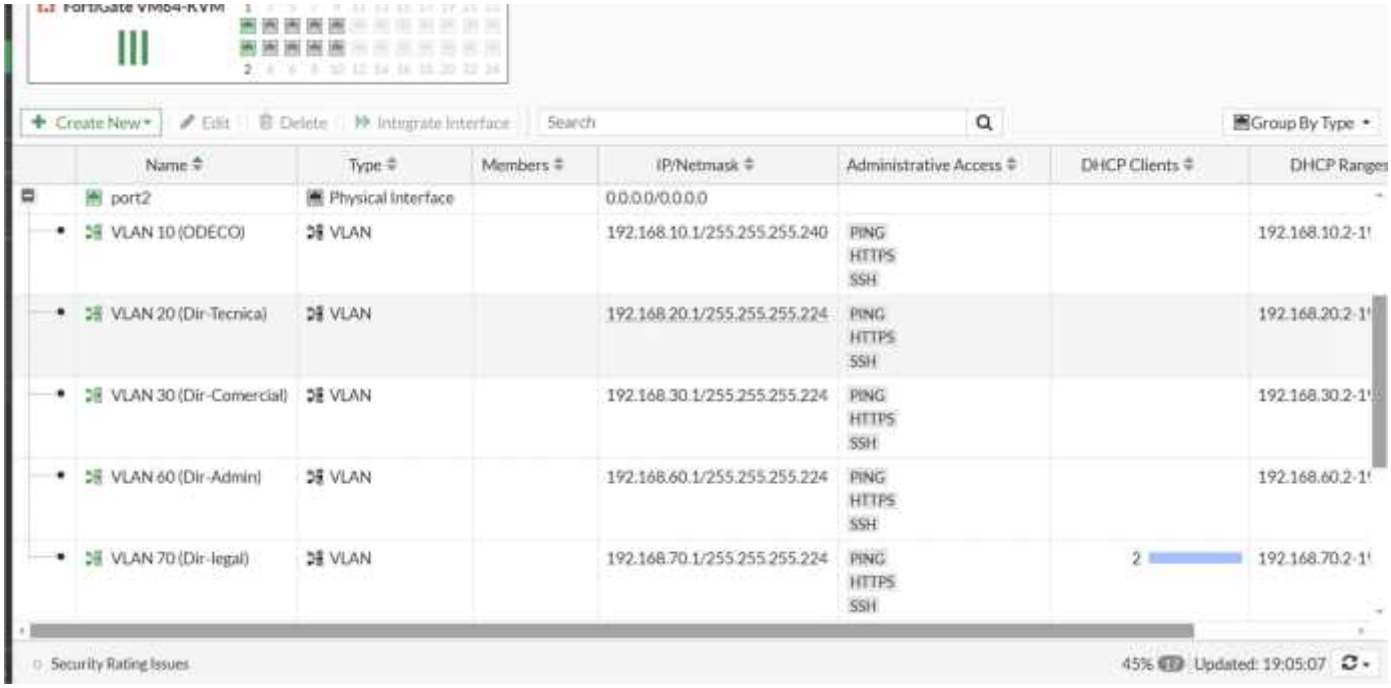


Figura 89: *VLANs con DHCP asignado en el FortiGate*

Fuente: Elaboración propia

243. Acabado de la creación de VLAN en la interfaz port2, se procede a crear el grupo de direcciones, habilitando un límite de IP, con la idea de no tener direcciones innecesarias.

III.1.4.2.2. Configuración de un grupo de direcciones IP

244. Descripción general de creación de objetos de dirección IP para todas las VLAN's en un firewall

245. Se debe crear objetos de red para todas las VLAN's, para agrupar dispositivos que tendrán acceso limitado a la red, se debe definir un rango de direcciones IP que representan a los dispositivos de las VLAN's.

246. Crear el nombre del objeto como ser **“vlan 10”**, asignar el un tipo de rango como ser **“IP range”**, asignamos el rango de **IP 192.168.10.2-192.168.10.32** y asignar el interfaz correspondiente en este caso deber ser **“VLAN 10 (ODECO)’’**.

247. De la misma forma se debe realizar los grupos para las **vlan20, vlan30, vlan40, vlan50, vlan60, vlan70.**

248. Grupo de dirección sin restricción en la red.

249. Crear un objeto de red que será asignado al gerente general de EMTAGAS, el objeto deberá ser con el nombre de **“vlan70_vip”**, asignar el tipo de IP fija o estática como ser **192.168.70.2/32** y asignar el interfaz correspondiente, es decir la interfaz **VLAN 70(Dir-Legal).**

250. **Creación de objetos de dirección IP para todas las VLAN’s en Fortigate**

Segmentaremos las IP que estarán restringidas y las que estarán sin restricciones.

Dirigirse a Policy & Objects > Addresses.

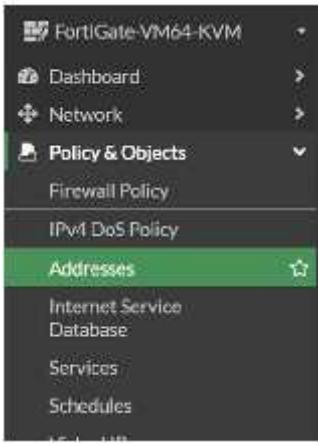


Figura 90: *Paso 1 para la configuración de direcciones IP*

Fuente: Elaboración propia

Creamos objetos de direcciones para todas las VLAN’s:

- **Name:** VLAN10
- Type: IP Range

FIREWALL_AUTH_PORTAL_ADDRESS	0.0.0.0/0	
SSLVPN_TUNNEL_ADDR1	10.212.134.200 - 10.212.134.210	
all	0.0.0.0/0	
none	0.0.0.0/32	
vlan 10	192.168.10.2 - 192.168.10.32	VLAN 10 (ODECO)
vlan 20	192.168.20.2 - 192.168.20.32	VLAN 20 (Dir-Tecnica)
vlan 30	192.168.30.2 - 192.168.30.32	VLAN 30 (Dir-Comercial)
vlan 60	192.168.60.2 - 192.168.60.32	VLAN 60 (Dir-Admin)
vlan 70	192.168.70.3 - 192.168.70.32	VLAN 70 (Dir-legal)
vlan 70_vip	192.168.70.2/32	VLAN 70 (Dir-legal)

- Range: 192.168.10.2-192.168.10.32

2.2 Y por último damos clic en **OK** para guardar

En la simulación se visualizaría de la siguiente manera.

Figura 91: *Paso 2 para la configuración de direcciones IP*

Fuente: Elaboración propia

Figura 92: *Comprobación de la configuración de direcciones IP*

Fuente: Elaboración propia

III.1.4.2.3. Configurar filtrado de contenido y aplicaciones

251. Descripción genérica de la configuración del filtrado Web en firewall

252. Para aplicar los controles de debe acceder al módulo de perfiles de seguridad, desde allí podremos definir políticas específicas para la inspección y control tanto del tráfico web como del uso de aplicaciones.

253. Configuración del Filtrado Web (Web Filtering)

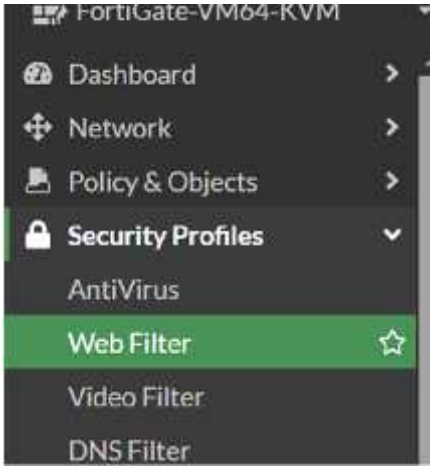
254. Se debe crear un nuevo perfil con el nombre de filtrado web, dentro del perfil, seleccionamos la categorías de sitios web a bloquear, como ser (Redes sociales, contenido para adultos, juegos en línea, servicios de streaming y anuncios y reastreadores).

255. En la parte de bloqueo de url o filtro de url se debe añadir los siguientes url: www.yotube.com, www.facebook.com, www.tiktok.com, www.instagram.com.

256. Configuración de Filtrado web en Fortigate

Se debe crear perfiles para bloquear páginas y aplicaciones.

Filtrado Web:

Dirigirse a Security 

Profiles > Web Filter.

Figura 93: *Paso 1 para la configuración de filtrado web*

Fuente: Elaboración propia

Creamos un perfil con estas configuraciones:

- Blocked Categories: Selecciona las categorías de páginas web que deseas bloquear.
- Static URL Filter, habilitamos para ingresar página que no queremos que sean utilizadas por las VLAN's.

Y por último damos clic en **OK** para guardar

En la simulación se muestra de la siguiente forma.

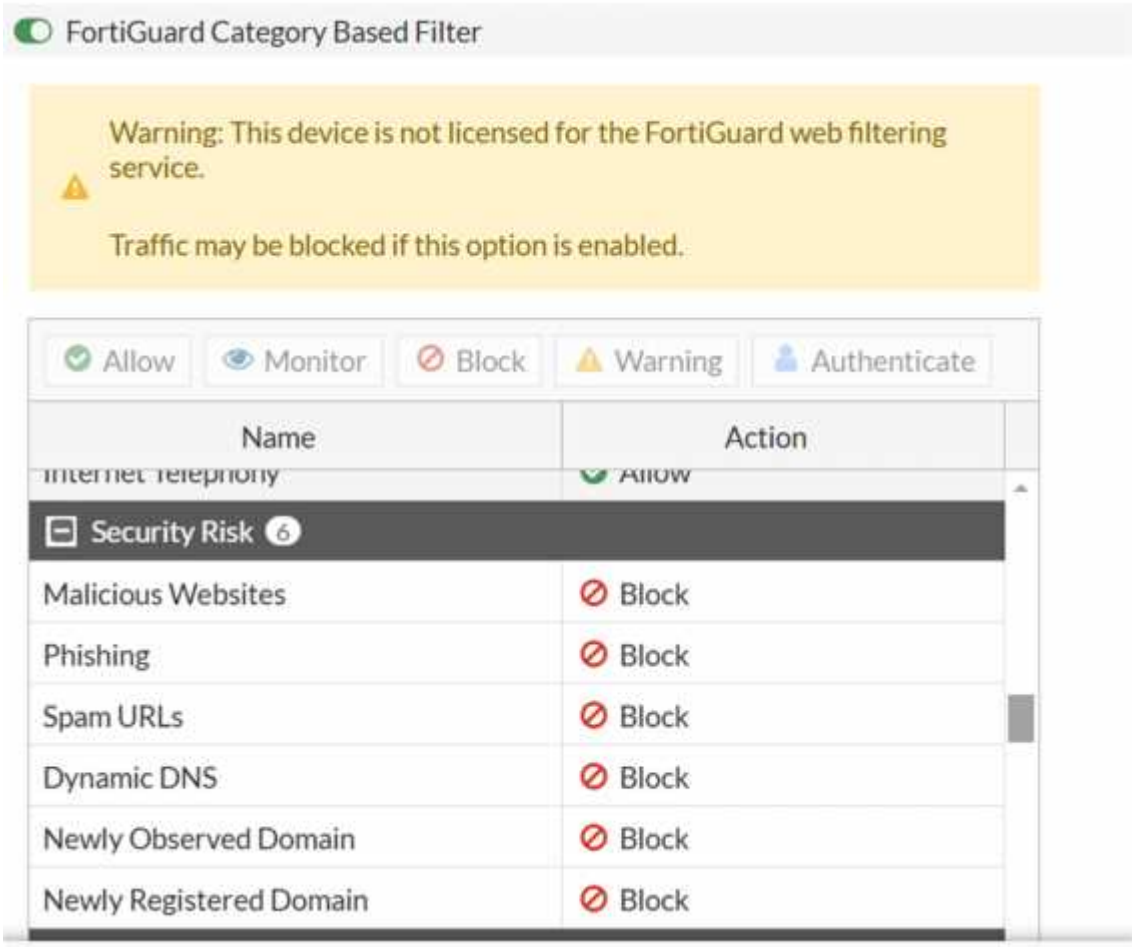


Figura 94: *Paso 2 para la configuración de filtrado web*

Fuente: Elaboración propia

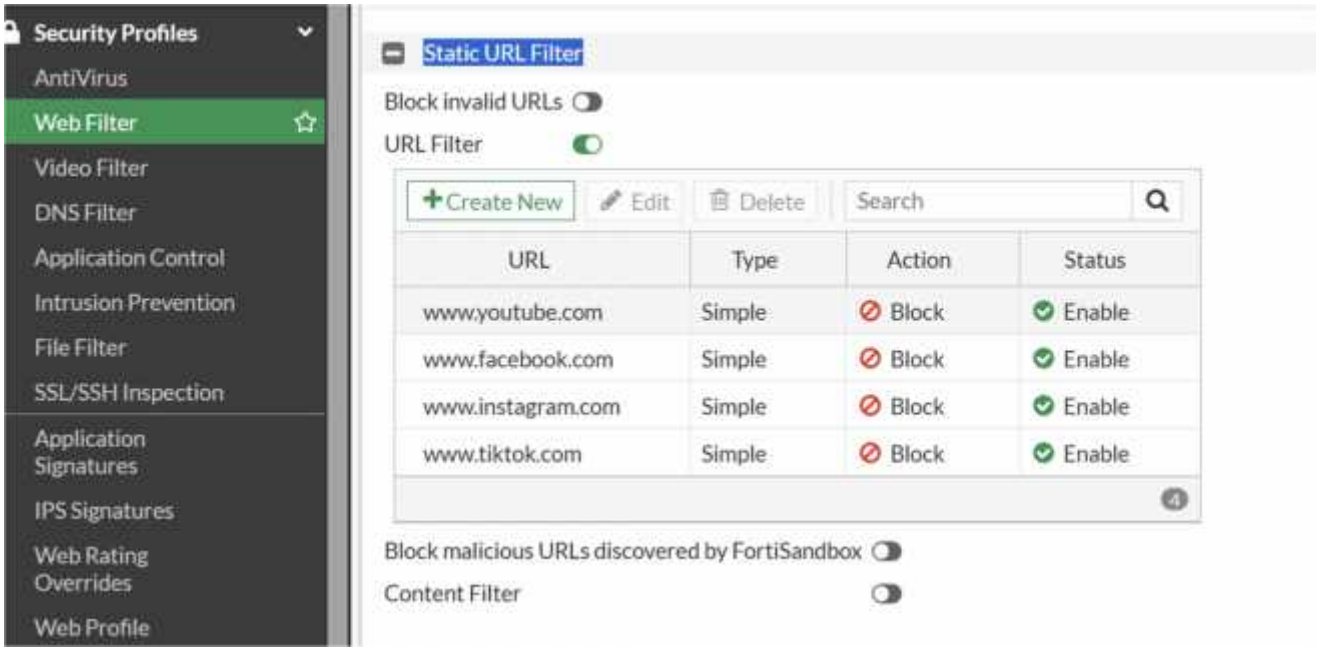


Figura 95: *Comprobación de la configuración de filtrado web para cada VLAN*

Fuente: Elaboración propia

III.1.4.2.4. Filtrado de Aplicaciones

257. Descripción genérica de la configuración del filtrado de Aplicaciones en firewall

258. Configuración del Filtrado de Aplicaciones (Application Control)

259. Se debe crear un nuevo perfil con el nombre de filtrado de aplicaciones, dentro del perfil añadimos las aplicaciones a bloquear, como ser (VPNs no autorizados, Redes sociales, Plataformas de mensajería personal (WhatsApp, Telegram, etc.), juegos en línea).

260. Una vez creados, los perfiles de filtrado web y control de aplicaciones se pueden vincular a reglas de acceso o políticas de firewall, según los grupos de direcciones IP o VLANs

configuradas previamente. Así, se garantizamos que los filtros se apliquen de forma selectiva, permitiendo excepciones cuando sea necesario.

Configuración de control de aplicaciones en Fortigate

Dirigirse a Security Profiles > Application Control.

Figura 96: *Configuración de filtrado de aplicaciones*

Fuente: Elaboración propia

Creamos un perfil con las siguientes configuraciones:

- Block Applications: Añade las aplicaciones que deseas restringir.

Y por último damos clic en **OK** para guardar

En la simulación se muestra de la siguiente forma.

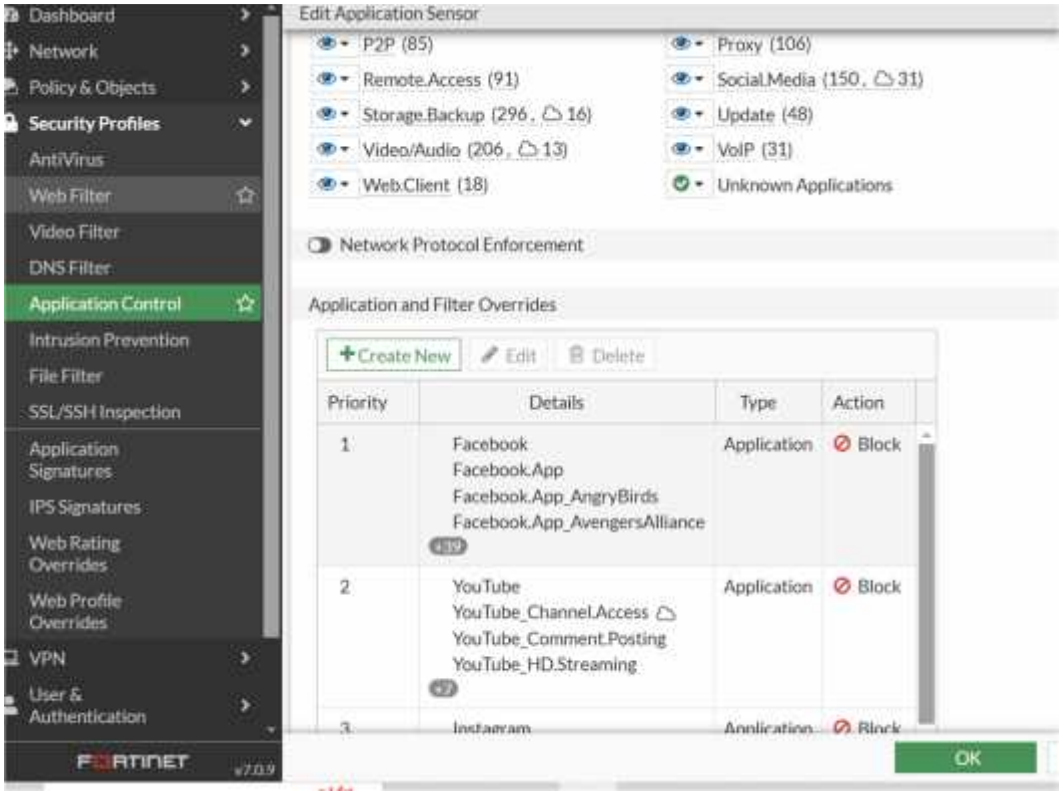


Figura 97: *Comprobación de la configuración de filtrado de aplicaciones*

Fuente: Elaboración propia

III.1.4.2.5. Creación de las políticas de seguridad en el firewall

En este es muy crucial tener bien planteadas las políticas de seguridad, por esta razón se consideró proponer en base al uso y el acceso a las páginas web como también el uso de aplicaciones.

261. Configurar políticas, aplicar las reglas de restricción, que está regla consiste en la habilitación de internet a todas las VLAN'S, habilitando los filtros web, control de aplicaciones y activación del antivirus, con el fin de tener un seguridad y control de acceso que recurren los usuarios.

Explicación genérica de la creación de políticas de seguridad en firewalls

262. Estas políticas especifican condiciones como la interfaz de entrada, la dirección IP de origen, el destino, los servicios permitidos y la aplicación de perfiles de seguridad.

263. Para gestionar de forma efectiva el acceso a Internet desde una red segmentada (por ejemplo la VLAN), se pueden definir múltiples políticas según el nivel de restricción deseado para distintos grupos de usuarios.

264. Habilitación de acceso a Internet a todas las VLAN's

265. Política 1 Acceso Restringido (VLAN 10-INTERNET)

266. Esta política está diseñada para aplicar restricciones de contenido y aplicaciones a los usuarios comunes dentro de una red segmentada.

267. Primero debemos encontrarnos en el módulo de política de seguridad del firewall.

268. **Parámetros generales de la política:** debemos cumplir estos pasos para generar la política de seguridad, se debe crear de la siguiente forma

269. **Nombre**: ingresamos el nombre de la política de seguridad "**VLAN 10-INTERNET**

270. **Interfaz de entrada (Incoming):** Aquí es la interfaz virtual correspondiente al grupo de red, en este caso usaremos el grupo ya creado anteriormente que es la interfaz **"VLAN 10(ODECO)".**

271. **Interfaz de salida (Outgoing):** Aquí la interfaz que conecta a la red externa o Internet que en este case será el **"port1"** del firewall ya que por esta interfaz se conectara a la red de Internet.

272. Dirección de origen (Source): Aquí va el objeto de direcciones que agrupa a los usuarios restringidos que creamos con anterioridad, en este caso asignamos al objeto correspondiente que es la **"vlan10"**.

273. **Destino (Destination):** En esta etapa debemos permitir todos los destinos **(any o all),** permitiendo el acceso a cualquier dirección.

274. **Servicio:** Aquí debemos configurar de manera **(all)** permitimos todos los servicios, sujeto a los filtros definidos.

275. **Acción**: Aquí configuramos en **Accept** que indica aceptar tráfico que cumpla con esta condición.

276. **Perfiles de seguridad:** En este paso activamos los perfiles de filtrado web y control de aplicaciones previamente configurados, con el fin de limitar el contenido y bloquear el uso de aplicaciones no autorizadas.

277. Activamos si en caso está disponible la función del **antivirus**.

278. Habilitamos y relacionamos el perfil de control de páginas web seleccionando el **filtro web,** creado anteriormente.

279. Habilitamos y relacionamos el perfil de control de aplicaciones seleccionando el **filtrado de aplicaciones**, creado anteriormente**.**

280.

281. Esta política asegura que los usuarios estándar puedan acceder a Internet, pero bajo una supervisión y un control adecuado.

282. De la misma manera se debe crear las políticas de seguridad con el fin de tener acceso a Internet de las demás VLAN's, es decir: **VLAN 20(Dir-Técnica), VLAN 30(Dir-Comercial), VLAN 40(Dir-Tecnica), VLAN 60(Dir-Admin), VLAN 70(Dir-Legal).**

283. Política 2: Acceso sin Restricciones (VLAN 70_VIP)

284. Esta segunda política está destinada a un dispositivo o usuario específico (por ejemplo, un gerente o administrador) que requiere acceso total sin filtros.

285. Parámetros generales de la política:

286. **Nombre**: ingresamos el nombre de la política de seguridad **“VLAN 70_VIP’’**

287. **Interfaz de entrada (Incoming):** Aquí es la interfaz virtual correspondiente al grupo de red, en este caso usaremos el grupo ya creado anteriormente que es la interfaz **“VLAN 70(Dir-Legal)”.**

288. **Interfaz de salida (Outgoing):** Aquí la interfaz que conecta a la red externa o Internet que en este case será el **“port1”** del firewall ya que por esta interfaz se conectara a la red de Internet.

289. Dirección de origen (Source): Aquí va el objeto de direcciones que agrupa a los usuarios restringidos que creamos con anterioridad, en este caso asignamos al objeto correspondiente que es la **“vlan 70_vip”**.

290. **Destino (Destination):** En esta etapa debemos permitir todos los destinos **(any o all),** permitiendo el acceso a cualquier dirección.

291. **Servicio:** Aquí debemos configurar de manera **(all)** permitimos todos los servicios, sujeto a los filtros definidos.

292. **Acción**: Aquí configuramos en **Accept** que indica aceptar tráfico que cumpla con esta condición.

293. **Perfiles de seguridad:** En esta política, no se aplican perfiles de filtrado, permitiendo así acceso libre a todos los recursos disponibles.

294. Ahora veremos la configuración de la creación de las políticas de seguridad en un firewall FORTIGATE.

Política 1: Acceso a Internet a VLAN’s

Diríjase a Policy & Objects > IPv4 Policy.

Configura la política:

- **Name:** VLAN10_Internet
- **Incoming Interface:** VLAN_10
- **Outgoing Interface:** port 1
- **Source:** VLAN10
- **Destination:** all
- **Service:** all
- **Action:** Accept
- Security Profiles: Habilita Web Filter y Application Control.

295. Este tipo de política de Seguridad es aplicado en las VLAN propuesta para la red, ya que sin esta existencia de esta política seria imposible que exista comunicación hacia el internet, en la simulación se observaría de esta forma las políticas de red.

Figura 98: *Configuración de políticas de seguridad*

Fuente: Elaboración propia

296. De esta forma se visualiza las políticas de seguridad creada para cada VLAN, con el fin que estas VLAN’s accedan al internet.

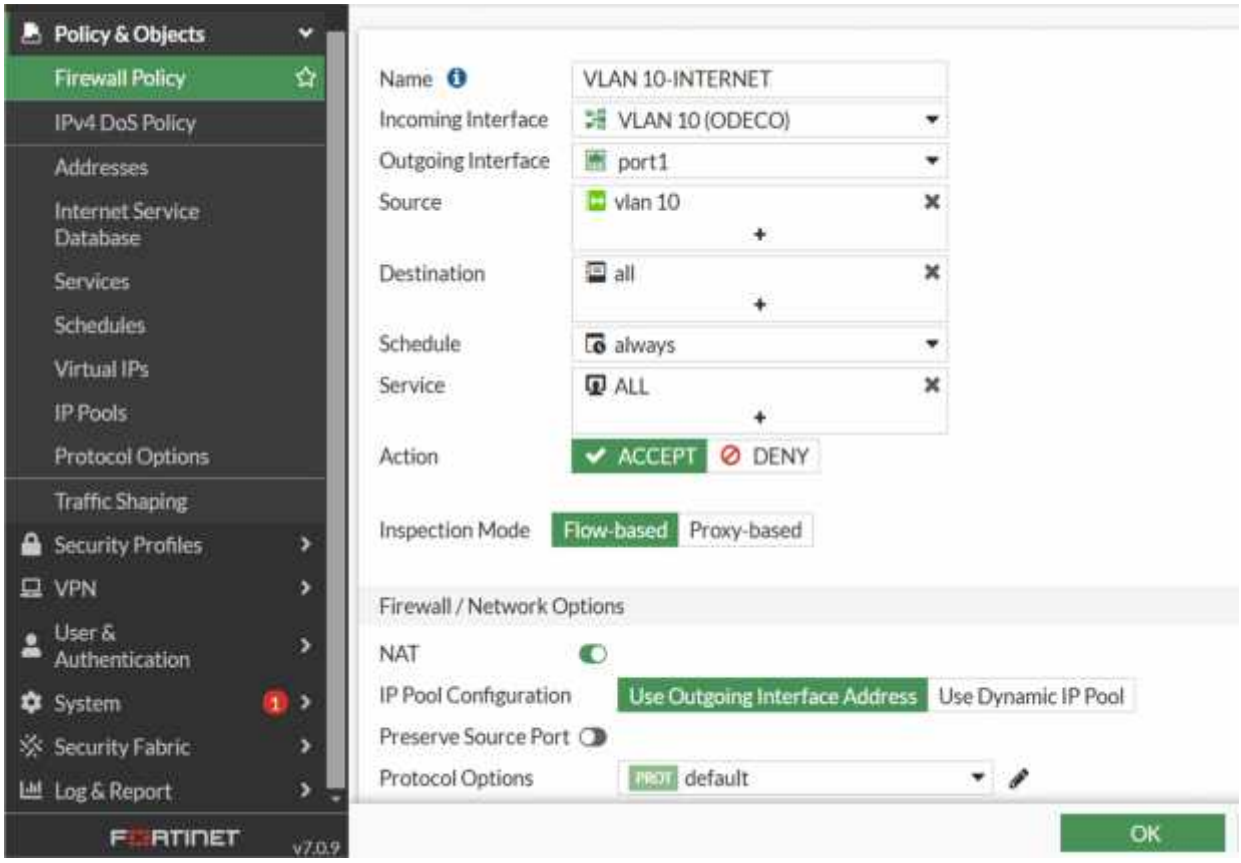


Figura 99: *Configuración de las políticas de seguridad para la VLAN 10*

Fuente: Elaboración propia

De esta forma se visualiza los pasos para la creación de la política de red.

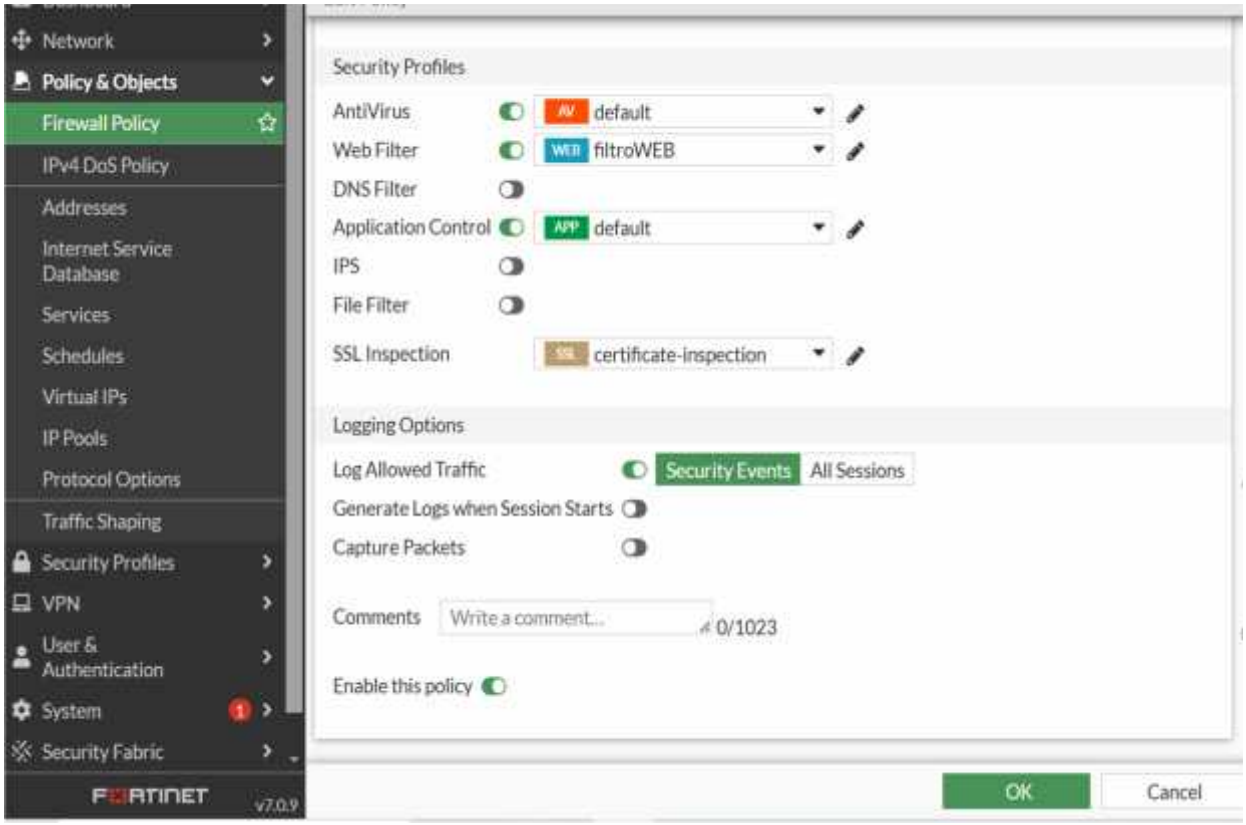


Figura 100: *Visualización de la configuración completa de las políticas de seguridad*

Fuente: Elaboración propia

297. Observamos que podemos aquí habilitar el uso del antivirus que por defecto trae el FortiGate, como el filtrado de las páginas y aplicaciones.

- Se creo un apolítica especial, para solo el gerente de EMTAGAS, que esta política trata de crear una dirección dentro de la VLAN 70, en la cual, sin desordenar la topología de la red, exista privilegio sobre el gerente general de la empresa, dicho privilegio consiste en el que no exista ni una restricción de páginas y aplicaciones en su ip que el utilice.

298. Dicho esto se debe realizar una reserva de IP en el DHCP y con esto podremos tener una IP especial solo para el gerente general,para esto procederemos a registrar la dirección MAC del equipo que simulara el uso de la máquina del gerente, ahora procedemos a realizar los pasos de configuración.

III.1.4.2.6. configuración en la interfaz en la VLAN 70

299. Para garantizar que el gerente siempre reciba la misma IP, hacemos una reserva en el servidor DHCP.

300. Ve a Network > DHCP Server.

301. Encontrar el servidor DHCP correspondiente a la VLAN 70 y selecciona **Edit**.

302. En la sección Reserved Addresses:

- Damos clic en **+ Add**.

303. Especifica:

- **MAC Address**: La dirección MAC del dispositivo del gerente (puedes encontrarla en su equipo o en el monitor de DHCP del FortiGate).
- **IP Address**: Asigna la IP fija deseada, por ejemplo, 192.168.70.2
- Guarda los cambios.

304. Dicho esto, visualizamos en la simulación.

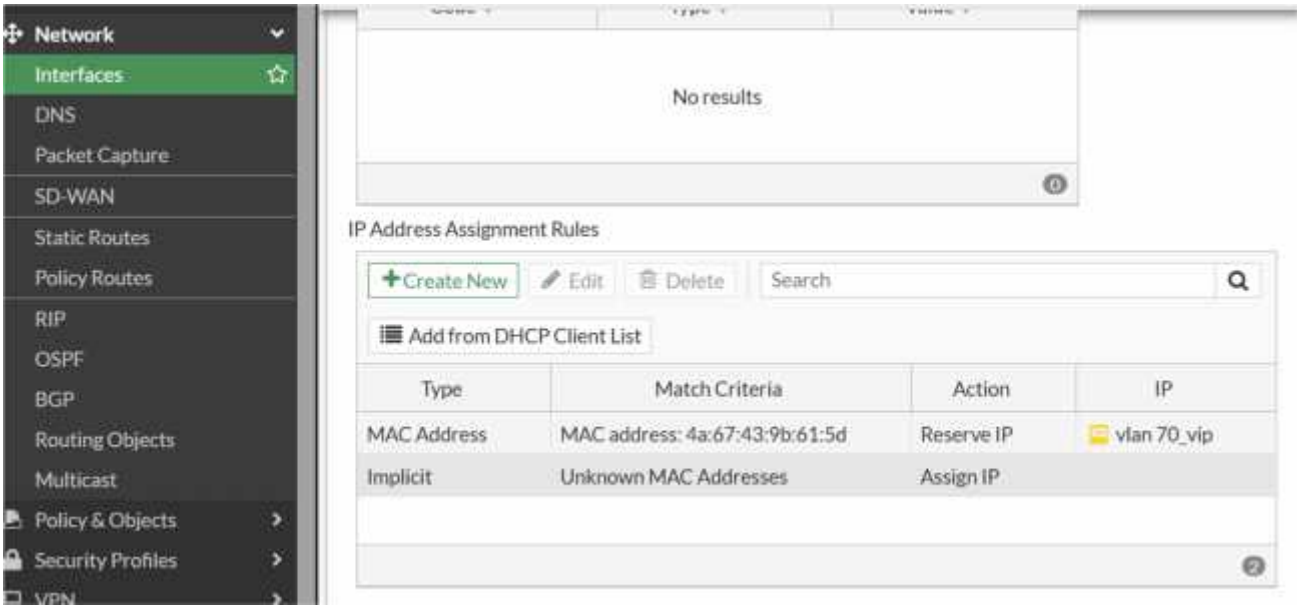


Figura 101: *Configuración de la interfaz para la VLAN 70*

Fuente: Elaboración propia

305. Como observamos en la imagen se registró el MAC del equipo del gerente y con una IP asignada solo a él.

III.1.4.2.7. Configuración del objeto de direcciones IP

306. Creamos una dirección para permitir el tráfico según sea necesario.

307. Nos dirigimos a **Policy & Objects > Addresses**.

308. Crea dos objetos de direcciones:

309. **Sin Restricción**:

- **Name**: VIP_Manager
- **Type**: Subnet/IP
- **Address**: 192.168.70.2

310. De esta forma seria en la simulación.

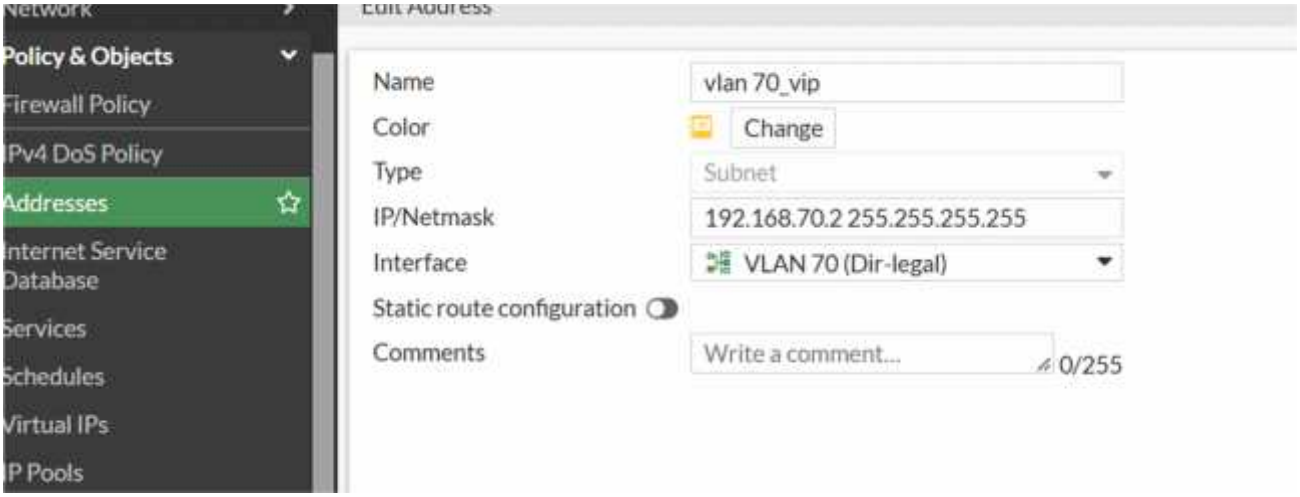


Figura 102: *Configuración de la dirección IP para la VLAN 70*

Fuente: Elaboración propia

Como indica en la imagen llamamos a ese grupo de dirección de privilegio, como vlan 70_vip.

III.1.4.2.8. configuración de la política de seguridad en el firewall

Diríjase a Policy & Objects > IPv4 Policy.

- **Name**: VLAN70_VIP.
- **Incoming Interface**: VLAN_70.
- **Outgoing Interface**: pot1, es el puerto que este de salida hacia el INTERNET.
- **Source**: vlan 70_vip
- **Destination**: all.
- **Service**: all.
- **Action**: Accept.
- Security Profiles**:** Dejamos deshabilitados los perfiles de seguridad.

Y de esta forma se visualizaremos en la simulación.

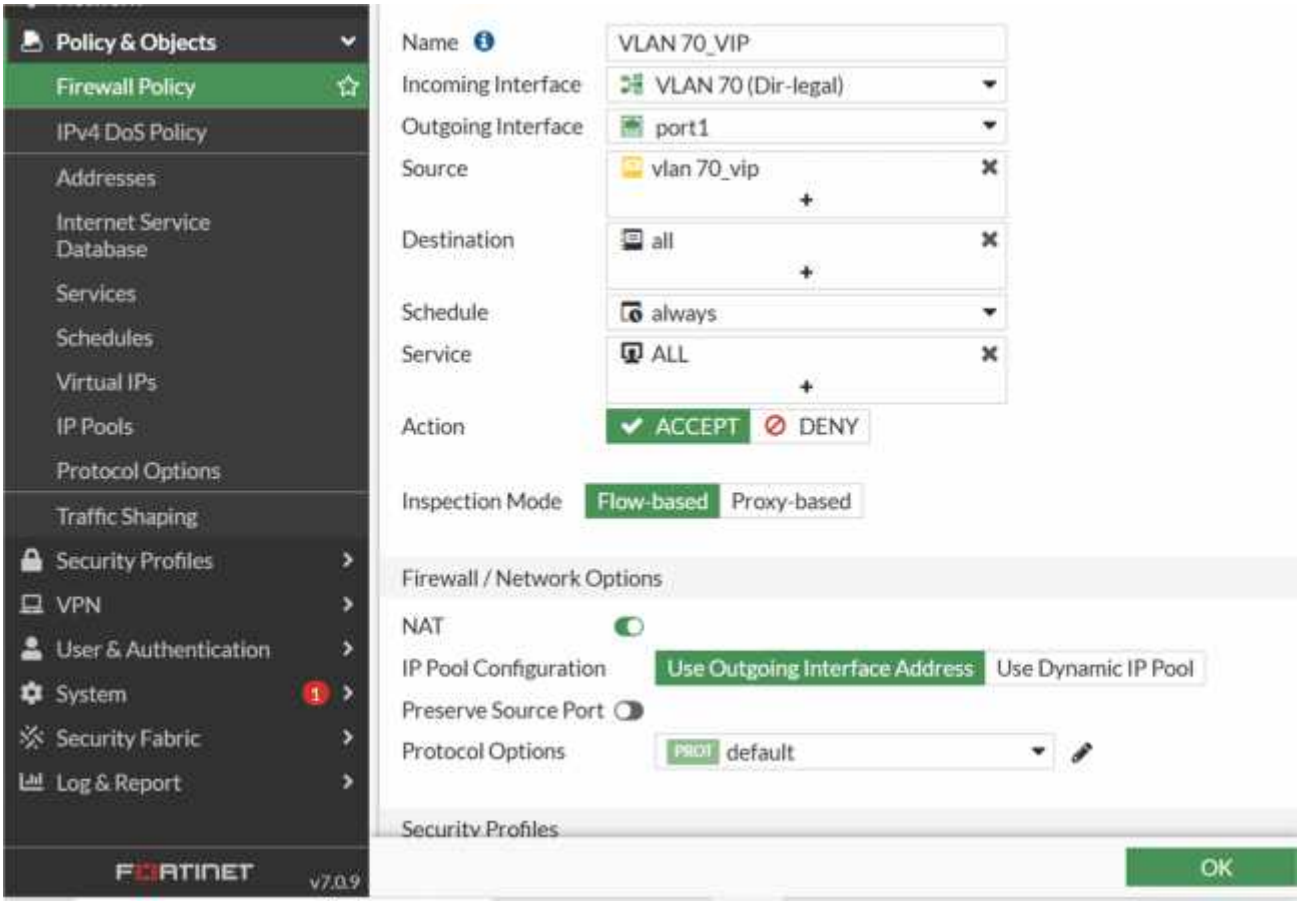


Figura 103: *Configuración de las políticas de seguridad para la VLAN 70*

Fuente: Elaboración propia

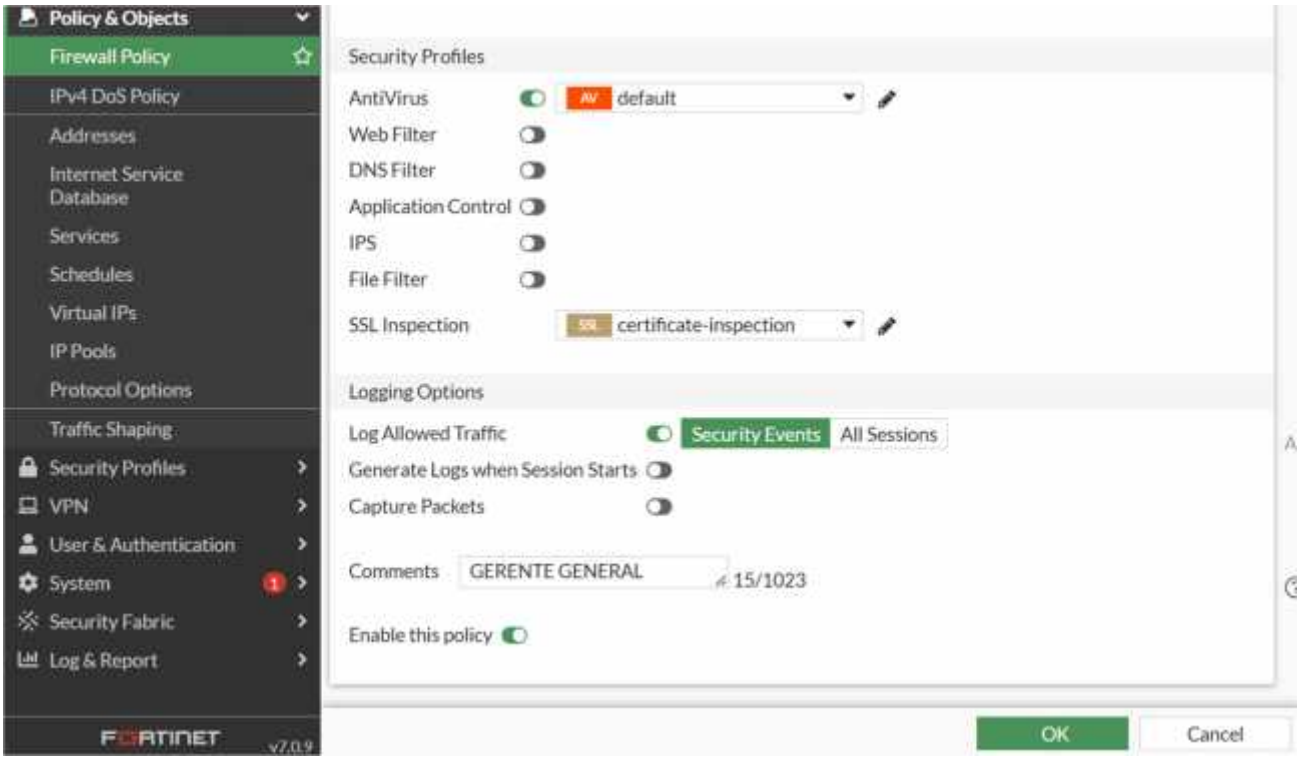


Figura 104: *Política de seguridad de acceso a internet*

Fuente: Elaboración propia

Y es así que se crea otra política de seguridad, de acceso a internet sin ninguna restricción de páginas web.

III.1.4.3. Sketchup

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

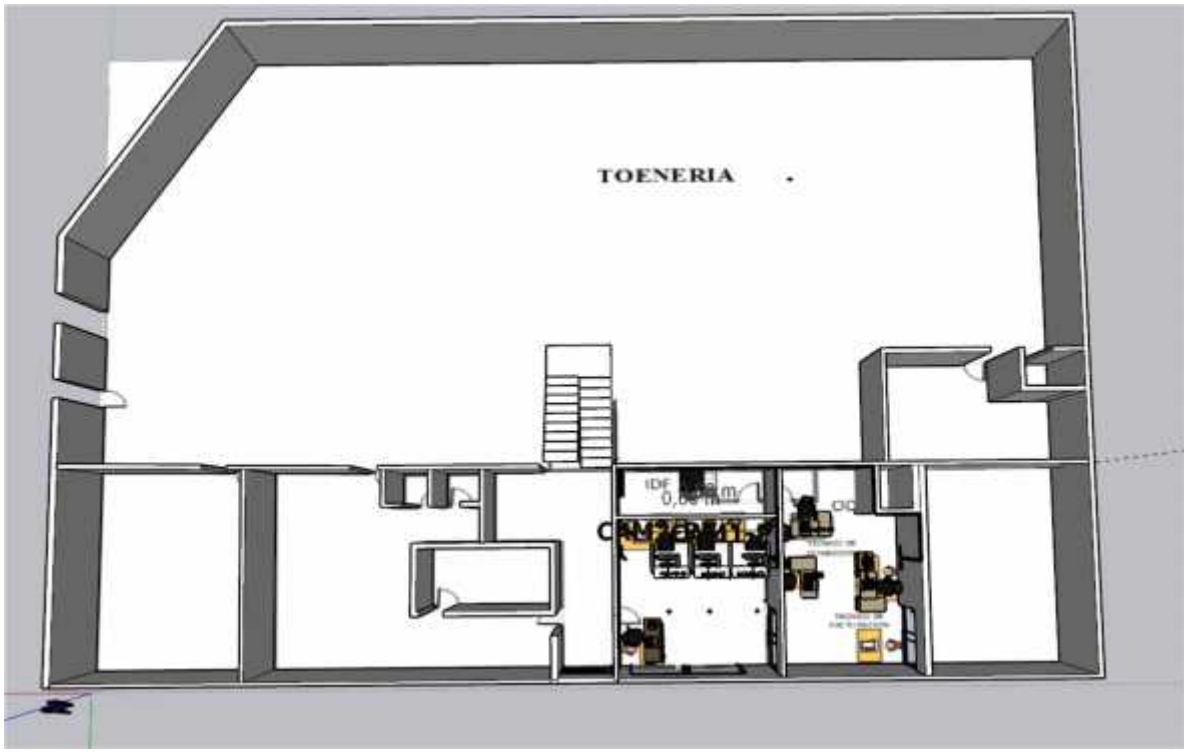


Figura 105: *Plano en 3D de la planta baja de ENTAGAS en Sketchup*

Fuente: Elaboración propia

Se usa el plano para levantar el plano de 2d a 3d.

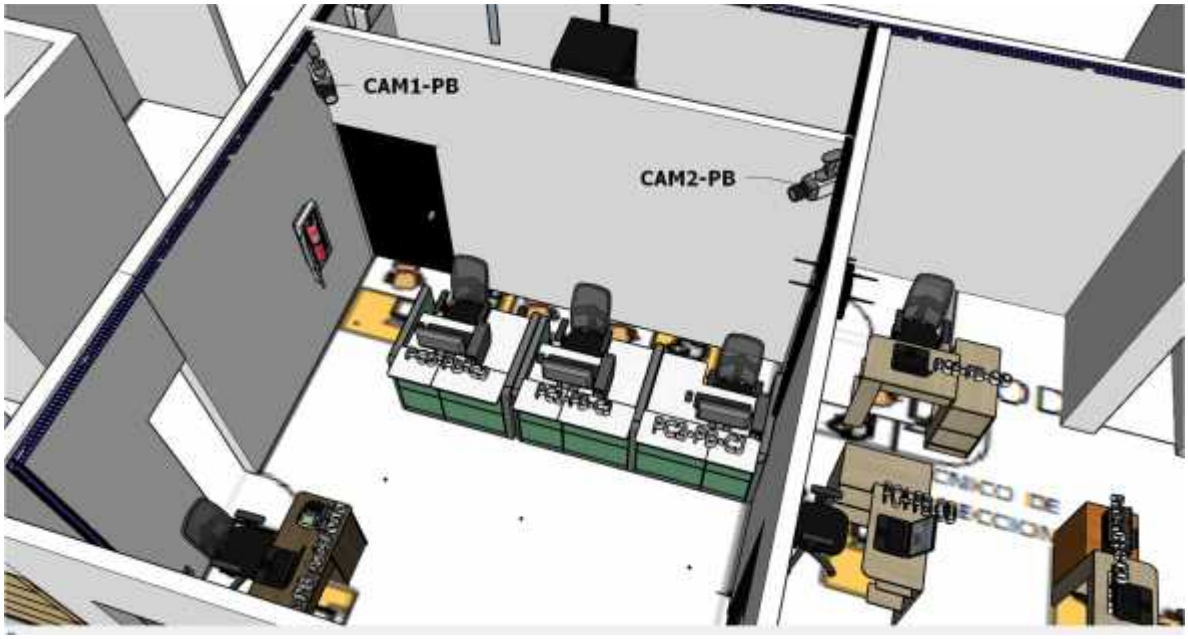


Figura 106: *Plano en 3D de las canaletas de la planta baja de ENTAGAS en Sketchup*

Fuente: Elaboración propia

Se graficó canaletas, que este hace referencia al cableado estructurado, tanto en planta baja como en las demás plantas

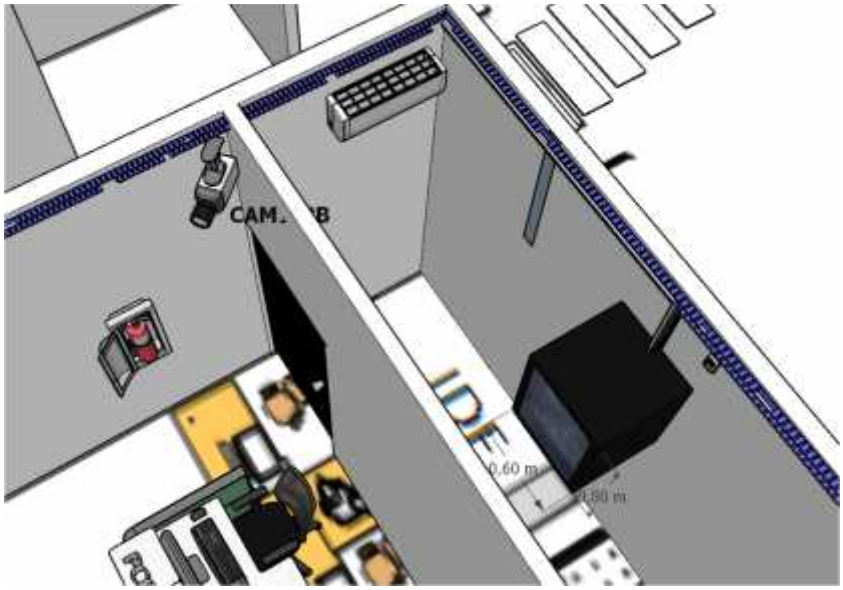


Figura 107: *Vista en 3D del Rack de la planta baja*

Fuente: Elaboración propia

También hace la referencia de cómo deben estar armados los cuartos de comunicación (IDF).

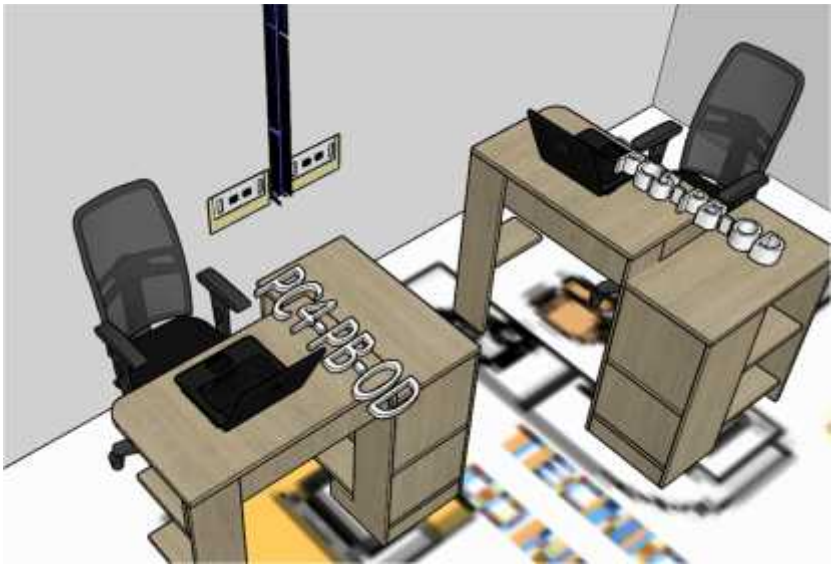


Figura 108: *Vista de las rosetas de la planta baja*

Fuente: Elaboración propia

III.2. Componente 2:

Socialización a los trabajadores

del TI en la propuesta de red LAN.

III.2. Componente 2: Socialización a los trabajadores del TI en la propuesta de red LAN.

III.2.1. Introducción del Proyecto

311. EMTAGAS se enfrenta a desafíos significativos en la gestión de su infraestructura de TI, la cual es fundamental para mantener la calidad y seguridad de nuestros servicios. Este proyecto propone un rediseño de la red LAN-WLAN para abordar estos desafíos y garantizar un funcionamiento más eficiente y seguro.

312. En respuesta a las crecientes demandas de eficiencia y seguridad, este proyecto de red aborda múltiples aspectos. Planeando implementar una infraestructura de red de alto rendimiento que se basará en tecnologías de vanguardia, incluyendo fibra óptica, cableado UTP, segmentación de redes mediante VLANs, y la incorporación de telefonía IP para una comunicación más eficiente.

313. Además, este proyecto aborda la creación de servidores web, de bases de datos y de archivos para una mejor gestión de datos. Para garantizar la integridad y confidencialidad de la información, se implementarán estrategias de seguridad de red, que incluyen segmentación de red, firewalls, autenticación y autorización avanzadas, monitoreo continuo y control de acceso físico. También se establecerán rutinas de copias de seguridad para garantizar la disponibilidad y recuperación de datos en caso de cualquier eventualidad.

314. La administración de la red se optimizará mediante la creación de IDFs (Armarios de Distribución Intermedios) por piso y un MDF (Armario de Distribución Principal) en la segunda planta. Esto facilitará una administración centralizada y una gestión más eficaz en la infraestructura de red.

III.2.2. Objetivos del Proyecto

- Mejorar la eficiencia operativa: Aumentar la velocidad de transferencia de datos en un 40% para optimizar la operación y respuesta a los clientes.
- Garantizar la seguridad de los datos: Fortalecer la seguridad de la red para proteger los datos críticos de la empresa y garantizar la integridad de la operación de servicios de gas.
- Facilitar la escalabilidad: Proporcionar una infraestructura de red que permita una fácil expansión y escalabilidad de los servicios de gas en el futuro.

III.2.3. Alcance del Proyecto

315. Este proyecto abordará el rediseño de la red LAN-WLAN en nuestras instalaciones centrales, incluyendo oficinas administrativas y centros de control. No incluirá las instalaciones de campo.

III.2.4. Diseño de la Nueva Red

316. **Infraestructura de conectividad:** Se implementará una infraestructura híbrida que combina fibra óptica para la troncal principal y cableado UTP para la conectividad de usuarios.

317. **Segmentación de red mediante VLANs:** Se establecerán VLANs para segmentar la red en función de los departamentos y los grupos de usuarios.

318. **Telefonía IP:** Implementaremos una solución de telefonía IP para una comunicación más eficiente.

III.2.5. Beneficios del rediseño

319. **Mejora en la eficiencia operativa.** Con una mayor velocidad de transferencia de datos, los empleados pueden acceder y compartir información de manera más rápida, mejorando la respuesta a los clientes.

320. **Seguridad Reforzada:** La implementación de estrategias de seguridad de red reducirá el riesgo de ataques cibernéticos y protegerá los datos críticos de la empresa.

321. **Facilitación de Escalabilidad:** La infraestructura de red escalable permitirá a la empresa crecer de manera eficiente sin interrupciones en la operación.

III.2.6. Presupuesto

Categoría	Descripción	Costo
Hardware y Software	Equipos de red (enrutadores, switches, servidores, etc.).	60,000 Bs.
	Telefonía IP y sistemas relacionados	15,000 Bs.
	Software de seguridad (firewalls, soluciones de autenticación).	25,000 Bs.
Infraestructura de conectividad	Fibra óptica y cableado UTP.	25,000 Bs.
Centro de Datos	Equipamiento y acondicionamiento del centro de datos, incluyendo racks y sistemas de refrigeración.	15,000 Bs.
Costos de seguridad	Implementación de medidas de seguridad, incluyendo hardware y software de seguridad, control de acceso físico, y sistemas de monitoreo.	25,000 Bs.
Total, del presupuesto		140,000 Bs.

Tabla 25 *Tabla de presupuestos*

Fuente: Elaboración propia

III.2.7. Seguridad y Condiciones Específicas

322. A continuación, se detallan las consideraciones de seguridad y las condiciones específicas:

323. Segmentación de red.

324. Se implementará una sólida segmentación de red para garantizar que los departamentos y sistemas críticos estén aislados y protegidos de posibles amenazas internas. Cada VLAN se configurará para tener reglas de acceso específicas.

325. Firewalls y Protección Perimetral:

326. Se desplegarán firewalls de próxima generación en los puntos de entrada a la red para controlar el tráfico y detectar y bloquear amenazas cibernéticas. Se establecerán políticas de filtrado de paquetes para reforzar la seguridad.

327. Control de Acceso Físico:

328. Se establecerán políticas y procedimientos para controlar el acceso físico a las áreas de red críticas, como los armarios de distribución intermedios (IDFs) y el armario de distribución principal (MDF). Solo el personal autorizado tendrá acceso a estos lugares.

329. Condiciones Específicas para el Centro de Datos:

330. El centro de datos debe cumplir con las condiciones específicas de temperatura, humedad y seguridad. Se instalarán sistemas de enfriamiento y protección contra incendios adecuados.

331. Acceso restringido a Datos Confidenciales:

332. El acceso a datos confidenciales estará restringido a empleados autorizados. Se establecerán políticas de acceso y permisos detallados.

333. Conformidad con las regulaciones:

334. El proyecto debe asegurarse de cumplir con todas las regulaciones pertinentes, como las relacionadas con la seguridad de datos y la privacidad.

Capitulo IV

Conclusiones y Recomendaciones

Capitulo IV Conclusiones y recomendaciones

IV.1. Conclusiones

335. En resumen, la propuesta de red LAN para la empresa EMTAGAS representa un paso significativo en la evolución de nuestra infraestructura tecnológica. Después de una evaluación exhaustiva de las necesidades actuales y futuras de nuestra organización, hemos diseñado un proyecto que aprovecha tecnologías de vanguardia y estrategias de seguridad sólidas para alcanzar nuestros objetivos.

336. Este proyecto busca mejorar el rendimiento, la seguridad y la confiabilidad de la red, lo que se traducirá en un impacto positivo en las operaciones y en la satisfacción de los trabajadores. La implementación de fibra, cableado UTP, VLANs, telefonía IP, servidores, y estrategias de seguridad de red y de administración, se combina para crear una infraestructura tecnológica robusta y segura.

337. La creación de Intermediate Distribution Frames (IDFs) por piso y un Main Distribution Frame (MDF) en la segunda planta garantiza la distribución eficiente de la red en toda la organización, permitiendo la escalabilidad y el crecimiento futuro.

338. Esperamos que este proyecto sea bien recibido y que pueda avanzar hacia la ejecución de este emocionante proyecto de red. La infraestructura tecnológica renovada fortalecerá el recinto, brindando un servicio de alta calidad en un entorno seguro y eficiente.

IV.2 Recomendaciones

339. **Participación del Personal Clave:** La colaboración y la comunicación efectiva son fundamentales. Recomendamos involucrar a los equipos de TI, seguridad de la información y otros departamentos relevantes en el proceso. La participación de expertos internos garantizará una implementación más fluida y una comprensión compartida de los objetivos del proyecto.

340. **Evaluación de Riesgos Continua:** A lo largo del proyecto, se deben llevar a cabo evaluaciones de riesgos continuas. Esto garantizará que cualquier riesgo potencial se identifique y aborde de manera oportuna, minimizando interrupciones no planificadas y garantizando la seguridad de la red y los datos.

341. **Formación del Personal:** La introducción de nuevas tecnologías y procesos puede ser un cambio significativo. Recomendamos la implementación de programas de formación para el personal afectado por el proyecto. Esto les permitirá adaptarse a las nuevas tecnologías y procedimientos de manera eficaz.

342. **Gestión de Cambios Efectiva:** Establecer un proceso sólido de gestión de cambios es esencial. Recomendamos la creación de un equipo de gestión de cambios dedicado que supervise la transición y comunique los cambios a todos los interesados. Esto minimizará la resistencia al cambio y garantizará una adopción exitosa.

343. **Pruebas y validación rigurosas:** Antes de la implementación completa, se deben realizar pruebas exhaustivas en un entorno de pruebas. Esto incluye pruebas de seguridad, pruebas de rendimiento y pruebas de recuperación de desastres. Recomendamos no pasar a la fase de implementación completa hasta que se hayan completado y validado con éxito todas las pruebas.

344. **Mantenimiento y actualizaciones regulares:** Una vez que la red esté en funcionamiento, es fundamental mantenerla y actualizarla de manera regular. Esto garantizará que la red siga siendo segura y eficiente a medida que evolucionan las tecnologías y las necesidades de la organización.

345. **Cumplimiento Normativo:** Asegurarse de que la red cumpla con las regulaciones y normativas aplicables en la industria de servicios de gas es esencial. Recomendamos llevar a

cabo auditorías de cumplimiento periódicas para garantizar que estemos operando dentro de los marcos legales.