UNIVERSIDAD DE EL SALVADOR

FACULTAD MULTIDISCIPLINARIA ORIENTAL

DEPARTAMENTO DE INGENIERÍA Y ARQUITECTURA

SECCIÓN DE INGENIERÍA DE SISTEMAS INFORMÁTICOS.

INFORME FINAL DEL CURSO DE ESPECIALIZACION:

DISEÑO Y ADMINISTRACIÓN DE INFRAESTRUCTURA DE REDES EMPRESARIALES DE ALTA DISPONIBILIDAD

TITULO DEL INFORME FINAL:

"PROPUESTA DE MEJORA PARA LA INFRAESTRUCTURA DE RED DE LA FACULTAD MULTIDISCIPLINARIA ORIENTAL DE LA UNIVERSIDAD DE EL SALVADOR"

PARA OPTAR AL GRADO ACADEMICO DE:

INGENIERÍA DE SISTEMAS INFORMÁTICOS.

PRESENTADO POR:

BRYAN ALEXANDER MATA CÁCERES	N.º CARNET MC19038
ELIAN FRANCISCO TREMINIO PARADA	N.º CARNET TP20007
VICTORIA GABRIELA VELASQUEZ ORELLANA	N.º CARNET VV19020

DOCENTE ASESOR:

ING. DIEGO ARMANDO HERRERA FLORES

3 DE OCTUBRE DEL 2025

SAN MIGUEL, EL SALVADOR, CENTROAMERICA

UNIVERSIDAD DE EL SALVADOR

AUTORIDADES

MSC. JUAN ROSA QUINTANILLA

RECTOR

DRA. EVELYN BEATRIZ FARFÁN MATA

VICERRECTORA ACADÉMICO

MSC. ROGER ARMANDO ARIAS ALVARADO

VICERECTOR ADMINISTRATIVO

LIC. PEDRO ROSALIO ESCOBAR CASTANEDA

SECRETARIO GENERAL

LIC. CARLOS ALMILCAR SERRANO RIVERA

FISCAL GENERAL

UNIVERSIDAD DE EL SALVADOR

FACULTAD MULTIDISCIPLINARIA ORIENTAL

AUTORIDADES

MSC. CARLOS IVÁN HERNÁNDEZ FRANCO

DECANO

DRA. NORMA AZUCENA FLORES RETANA

VICEDECANA

LIC. CARLOS DE JESÚS SÁNCHEZ

SECRETARIO

ING. JOSÉ LUIS CASTRO CORDERO

JEFE DEL DEPARTAMENTO DE INGENIERÍA Y ARQUITECTURA

ING. MILAGRO ALICIA GONZALES DE REYES

COORDINADORA DEL PROCESO DE GRADO DEL DEPARTAMENTO DE INGENIERÍA Y ARQUITECTURA

Índice

Índice De Figuras

Índice De Tablas

1. Resumen

El presente proyecto de investigación titulado “Propuesta de mejora para la infraestructura de red de la Facultad Multidisciplinaria Oriental de la Universidad de El Salvador” tiene como objetivo diseñar un modelo de red actualizado que responda de manera eficiente a las demandas tecnológicas actuales y a los retos futuros de la comunidad universitaria. La investigación surge ante la necesidad de modernizar, optimizar y fortalecer la red institucional, garantizando mayor disponibilidad de los servicios, seguridad informática y facilidad de administración. La metodología empleada consistió en un análisis exhaustivo de la infraestructura existente, incluyendo un inventario técnico de los equipos de red, servidores y dispositivos de seguridad del centro de datos, así como la revisión de la distribución lógica de VLAN, telefonía IP y conectividad inalámbrica. Este diagnóstico permitió identificar fortalezas y debilidades críticas relacionadas con la segmentación, redundancia, administración de tráfico y seguridad. Como resultado, se propone una arquitectura de red jerárquica de tres capas (núcleo, distribución y acceso) que garantiza escalabilidad, redundancia y alta disponibilidad. La propuesta integra segmentación lógica mediante VLAN, un plan de direccionamiento IP coherente y servicios esenciales como DHCP, DNS, VPN, VoIP y Web, respaldados por mecanismos de alta disponibilidad y políticas de seguridad robustas basadas en firewalls perimetrales, autenticación centralizada y control de accesos. El diseño se validó mediante simulaciones en GNS3, comprobando la operatividad de los servicios, la conectividad entre VLAN y la eficacia de las políticas propuestas, junto con un plan técnico-económico sostenible y compatible con los equipos existentes

Palabras clave: Infraestructura de red; Red tipo campus; VLAN; Alta disponibilidad; Seguridad en redes.

1.1 Abstract

The present research project entitled “Proposal for the Improvement of the Network Infrastructure of Facultad Multidisciplinaria Oriental de la Universidad de El Salvador aims to design an updated network model that efficiently meets current technological demands and future challenges of the university community. This research arises from the need to modernize, optimize, and strengthen the institutional network, ensuring greater service availability, cybersecurity, and ease of administration. The applied methodology consisted of an exhaustive analysis of the existing infrastructure, including a detailed technical inventory of network equipment, servers, and data center security devices, as well as the review of VLAN logical distribution, IP telephony, and wireless connectivity. This diagnostic process identified both strengths and critical weaknesses related to segmentation, redundancy, traffic management, and security. As a result, a three-layer hierarchical network architecture (core, distribution, and access) is proposed, ensuring scalability, redundancy, and high availability. The proposal integrates logical segmentation through VLANs, a coherent IP addressing plan, and essential services such as DHCP, DNS, VPN, VoIP, and Web, supported by high-availability mechanisms and robust security policies based on perimeter firewalls, centralized authentication, and access control. The design was validated through GNS3 simulations, verifying service operability, inter-VLAN connectivity, and the effectiveness of the proposed security policies, along with a complementary technical-economic plan that considers cost-benefit ratio, sustainability, and compatibility with existing equipment.

Keywords: Network infrastructure; Campus network; VLAN; High availability; Network security.

2. Introducción

El presente proyecto tiene como propósito desarrollar una propuesta de mejora integral para la red institucional de la Facultad Multidisciplinaria Oriental de la Universidad de El Salvador. Esta propuesta busca modernizar la infraestructura tecnológica, optimizar el rendimiento, garantizar la seguridad y eficientizar el uso de los recursos informáticos como consecuencia de la reestructuración de la red. Para lograrlo, se plantea el diseño de una red de tipo campus, basada en una arquitectura jerárquica de tres capas: acceso, distribución y núcleo. Esta arquitectura integrará servicios esenciales como DNS, DHCP, VPN, VoIP y Web.

La propuesta se fundamenta en un análisis detallado de la situación actual de la red de la facultad multidisciplinaria oriental de la Universidad de El Salvador; un levantamiento técnico de los equipos y servicios existentes, y el diseño de una solución escalable, segura y alineada con los conocimientos obtenidos durante el curso de pre-especialización acerca de las mejores prácticas en redes de computadoras. Esta mejora no solo permitirá soportar el crecimiento institucional, sino también ofrecer una experiencia tecnológica más eficiente y confiable para estudiantes, docentes y personal administrativo.

El diseño estará basado en parámetros rigurosos de investigación, incluyendo la creación de un inventario detallado de los equipos de red y sus respectivos servicios, organizados por departamentos y aulas, con esquemas y observaciones documentadas minuciosamente mediante fotografías. Asimismo, se propondrá una segmentación lógica mediante vlans, debidamente documentadas con su identificador (ID), nombre, rango de direcciones IP y función específica. Además, se realizará un presupuesto del equipamiento requerido para implementar la propuesta presentada, en caso la Facultad así lo requiriera. Además de implementar una arquitectura jerárquica de tres capas, se incluirán mecanismos de alta disponibilidad y redundancia, considerando factores como el presupuesto, la tolerancia a fallos y la complejidad de la infraestructura. Se propondrán opciones que integren servidores en clúster, máquinas virtuales replicadas o una combinación de ambas, según las necesidades de los distintos servicios.

En concordancia con los objetivos planteados, este proyecto no se limita únicamente al rediseño estructural de la red, sino que también contempla aspectos fundamentales como la documentación precisa de los recursos actuales, la evaluación técnica y funcional de los elementos existentes, y la justificación económica de la propuesta de mejora. Asimismo, se enfatiza la implementación de políticas robustas de seguridad informática que aborden integralmente los principios de confidencialidad, integridad y disponibilidad, tanto en el acceso interno como externo a los servicios institucionales. Se validará el diseño propuesto mediante simulaciones en GNS3 permitirá anticipar el comportamiento real de la red y ajustar parámetros técnicos antes de una posible implementación. De esta manera, se garantiza que la propuesta responda de forma efectiva a las necesidades actuales y futuras de la Facultad, brindando una infraestructura sólida, escalable y preparada para afrontar los desafíos tecnológicos de una comunidad académica en constante crecimiento.

3. Objetivos

Objetivo general

- Diseñar y desarrollar una propuesta de mejora a la infraestructura de red para la Facultad Multidisciplinaria Oriental de la Universidad de El Salvador, orientada a optimizar la escalabilidad, redundancia, segmentación lógica y seguridad, mediante la implementación de buenas prácticas y arquitectura de red tipo campus con el fin de proveer de una red más estable, segura y eficiente para beneficio de los usuarios de la facultad.

Objetivos específicos

- Documentar la infraestructura de red actual, detallando sus activos, interfaces, direcciones IP y funciones específicas de cada componente.
- Identificar puntos de mejora en la infraestructura existente, con el fin de proponer optimizaciones que beneficien a la comunidad de la Facultad Multidisciplinaria Oriental.
- Implementar mecanismos y políticas de seguridad que garanticen la confidencialidad, integridad y disponibilidad de los recursos de red.
- Diseñar una nueva topología de red jerárquica con mejoras, enlaces redundantes y una arquitectura de tres capas (acceso, distribución y núcleo).
- Simular y validar el diseño propuesto utilizando GNS3, justificando la propuesta técnica y económicamente.
- Aplicar mecanismos de seguridad en la red, como control de acceso, firewall perimetral, autenticación centralizada y segmentación de tráfico.

4. Marco Teórico y Conceptual

El diseño y mejora de infraestructuras de red en instituciones académicas requiere una sólida base conceptual y técnica que permita entender los elementos clave involucrados. En este apartado se exponen los fundamentos teóricos necesarios para sustentar la propuesta, así como las definiciones operativas de los términos técnicos más relevantes del proyecto.

4.1 ¿Qué es una red informática?

Es un sistema interconectado de dispositivos electrónicos, como computadoras, servidores, dispositivos móviles y otros dispositivos, que se comunican entre sí para compartir recursos, transmitir datos y permitir la colaboración en línea. [1] A esta red también se le llama red de computadoras o red de ordenadores y pueden ser tanto redes locales que conectan dispositivos dentro de un área limitada, como redes globales, tal es el caso del Internet, que abarcan todo el mundo. Una red se compone de dispositivos llamados nodos, que se comunican entre sí mediante protocolos predefinidos. Estos protocolos permiten a los nodos comprenderse entre sí, por medio de un lenguaje compartido, permitiéndoles intercambiar información eficazmente.

4.2 Modelos de referencia

4.2.1 Modelo OSI

Este modelo se basa en una propuesta desarrollada por la Organización Internacional de Normas (ISO) como el primer paso hacia la estandarización internacional de los protocolos utilizados en las diversas capas. Este modelo se revisó en 1995 y se le llama Modelo de referencia OSI (Interconexión de Sistemas Abiertos, del inglés Open Systems Interconnection) de la ISO, puesto que se ocupa de la conexión de sistemas abiertos; [2] esto es, sistemas que están abiertos a la comunicación con otros sistemas. Para abreviar, lo llamaremos modelo OSI.

Es un marco conceptual o una plantilla que sirve como estándar para entender, diseñar o evaluar un sistema, proceso o concepto, ofreciendo estandarización, estructura y una base para la comparación. Estos modelos se aplican en diversos campos, como la ingeniería de software para la comunicación, en redes para la estandarización de la comunicación (ej., OSI y TCP/IP), o en gestión de procesos (BPM) para definir flujos de valor genéricos.

El modelo OSI tiene siete capas. Los principios que se aplicaron para llegar a las siete capas se pueden resumir de la siguiente manera:

1. Se debe crear una capa en donde se requiera un nivel diferente de abstracción.
2. Cada capa debe realizar una función bien definida.
3. La función de cada capa se debe elegir teniendo en cuenta la definición de protocolos estandarizados internacionalmente.
4. Es necesario elegir los límites de las capas de modo que se minimice el flujo de información a través de las interfaces.
5. La cantidad de capas debe ser suficiente como para no tener que agrupar funciones distintas en la misma capa; además, debe ser lo bastante pequeña como para que la arquitectura no se vuelva inmanejable.

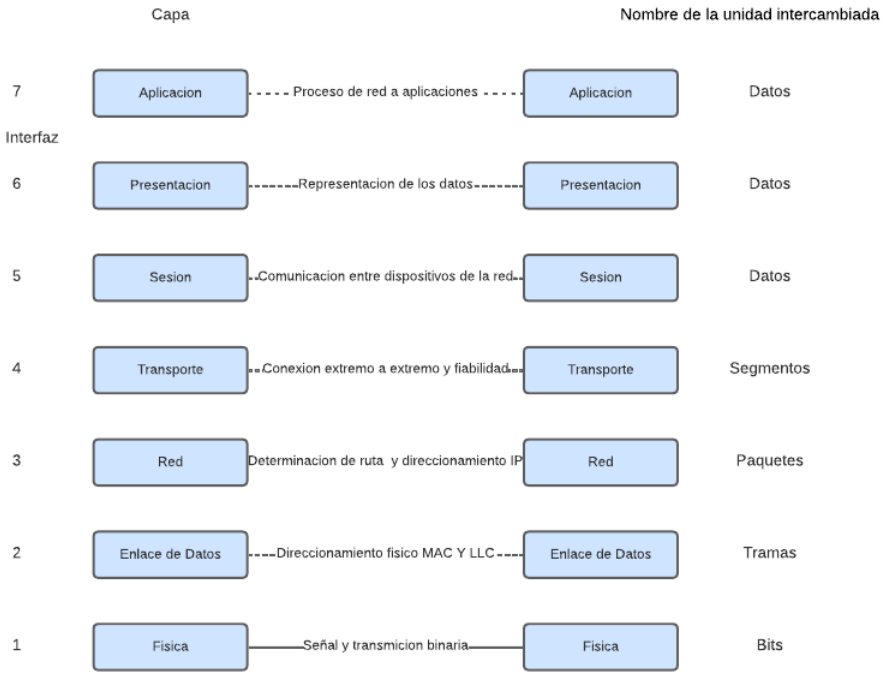

Figura 1: El modelo de referencia OSI

A continuación, estudiaremos cada capa del modelo en orden, empezando por la capa inferior

4.2.1.1. La capa física

La capa física se relaciona con la transmisión de bits puros a través de un canal de transmisión. Los aspectos de diseño tienen que ver con la acción de asegurarse que cuando uno de los lados envíe un bit 1 el otro lado lo reciba como un bit 1, no como un bit 0. [3]

4.2.1.2 La capa de enlace

La tarea principal de esta capa es transformar un medio de transmisión puro en una línea de comunicación que, al llegar a la capa de red, aparezca libre de errores de transmisión. Logra esta tarea haciendo que el emisor fragmente los datos de entrada en tramas de datos (típicamente, de algunos cientos o miles de bytes) y transmitiendo las tramas de manera secuencial. Si el servicio es confiable, el receptor confirma la recepción correcta de cada trama devolviendo una trama de confirmación de recepción. [4]

Otra cuestión que surge en la capa de enlace de datos (y en la mayoría de las capas superiores) es cómo hacer que un transmisor rápido no sature de datos a un receptor lento. Por lo general se necesita un mecanismo de regulación de tráfico que indique al transmisor cuánto espacio de búfer tiene el receptor en ese momento. Con frecuencia, esta regulación de flujo y el manejo de errores están integrados.

4.2.1.3 La capa de red

La capa de red controla la operación de la subred. Una cuestión clave de diseño es determinar cómo se encaminan los paquetes desde el origen hasta el destino. Las rutas se pueden basar en tablas estáticas que se "codifican" en la red y rara vez cambian, aunque es más común que se actualicen de manera automática para evitar las fallas en los componentes. También se pueden determinar el inicio de cada conversación; por ejemplo, en una sesión de terminal al iniciar sesión en una máquina remota. [5]

Por último, pueden ser muy dinámicas y determinarse de nuevo para cada paquete, de manera que se pueda reflejar la carga actual en la red. Si hay demasiados paquetes en la subred al mismo tiempo, se interpondrán en el camino unos con otros y formarán cuellos de botella. El manejo de la congestión también es responsabilidad de la capa de red, en conjunto con las capas superiores que adaptan la carga que colocan en la red. Otra cuestión más general de la capa de red es la calidad del servicio proporcionado (retardo, tiempo de tránsito, variaciones, etcétera). Cuando un paquete tiene que viajar de una red a otra para llegar a su destino, pueden surgir muchos problemas. El direccionamiento utilizado por la segunda red puede ser distinto del que utiliza la primera. La segunda red tal vez no acepte el paquete debido a que es demasiado grande.

Los protocolos pueden ser diferentes, etc. Es responsabilidad de la capa de red solucionar todos estos problemas para permitir la interconexión de redes heterogéneas. En las redes de difusión, el problema de encaminamiento es simple, por lo que con frecuencia la capa de red es delgada o incluso inexistente.

4.2.1.4 La capa de transporte

La función básica de la capa de transporte es aceptar datos de la capa superior, dividirlos en unidades más pequeñas si es necesario, pasar estos datos a la capa de red y asegurar que todas las piezas lleguen correctamente al otro extremo. Además, todo esto se debe realizar con eficiencia y de una manera que aísle las capas superiores de los inevitables cambios en la tecnología de hardware que se dan con el transcurso del tiempo. [5] La capa de transporte también determina el tipo de servicio que debe proveer a la capa de sesión y, en última instancia, a los usuarios de la red. El tipo más popular de conexión de transporte es un canal punto a punto libre de errores que entrega los mensajes o bytes en el orden en el que se enviaron. Sin embargo, existen otros posibles tipos de servicio de transporte, como el de mensajes aislados sin garantía sobre el orden de la entrega y la difusión de mensajes a múltiples destinos.

El tipo de servicio se determina al establecer la conexión (cabe mencionar que es imposible lograr un canal libre de errores; lo que se quiere decir en realidad con este término es que la tasa de errores es lo bastante baja como para ignorarla en la práctica). La capa de transporte es una verdadera capa de extremo a extremo; lleva los datos por toda la ruta desde el origen hasta el destino. En otras palabras, un programa en la máquina de origen lleva a cabo una conversación con un programa similar en la máquina de destino mediante el uso de los encabezados en los mensajes y los mensajes de control.

4.2.1.5 La capa de sesión

capa de sesión permite a los usuarios en distintas máquinas establecer sesiones entre ellos. Las sesiones ofrecen varios servicios, incluyendo el control del diálogo (llevar el control de quién va a transmitir), el manejo de tokens (evitar que dos partes intenten la misma operación crítica al mismo tiempo) y la sincronización (usar puntos de referencia en las transmisiones extensas para reanudar desde el último punto de referencia en caso de una interrupción). [6]

4.2.1.6 La capa de presentación

A diferencia de las capas inferiores, que se enfocan principalmente en mover los bits de un lado a otro, la capa de presentación se enfoca en la sintaxis y la semántica de la información transmitida. Para hacer posible la comunicación entre computadoras con distintas representaciones internas de datos, podemos definir de una manera abstracta las estructuras de datos que se van a intercambiar, junto con una codificación estándar que se use “en el cable”. La capa de presentación maneja estas estructuras de datos abstractas. [6]

4.2.1.7 La capa de aplicación

La capa de aplicación contiene una variedad de protocolos que los usuarios necesitan con frecuencia. Un protocolo de aplicación muy utilizado es HTTP (Protocolo de Transferencia de Hipertexto, del inglés HyperText Transfer Protocol), el cual forma la base para la World Wide Web. Cuando un navegador desea una página web, envía el nombre de la página que quiere al servidor que la hospeda mediante el uso de HTTP. Después el servidor envía la página de vuelta. Hay otros protocolos de aplicación que se utilizan para transferir archivos, enviar y recibir correo electrónico y noticias. [6]

4.2.2 El modelo de referencia TCP/IP

Es un conjunto de protocolos de comunicación que define el funcionamiento de internet y otras redes. Se organiza en cuatro capas: Aplicación (interacción con el usuario), Transporte (garantiza una comunicación confiable y establece la conexión), Internet (determina las rutas de los datos a través de la red, utilizando el Protocolo de Internet o IP), y Acceso a la Red (maneja el hardware y los medios de comunicación de la red). Este modelo es crucial para la transmisión fiable de datos en paquetes, y fue desarrollado por el Departamento de Defensa de EE. UU. en los años 70. [7]

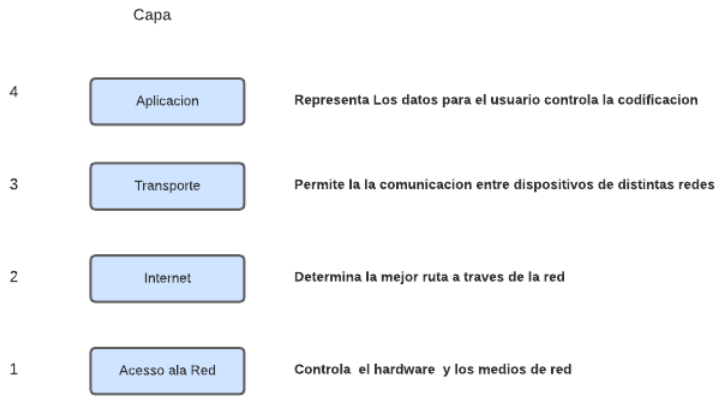

Figura 2: Modelo de referencia TCPI/IP

4.2.2.1 La capa de Acceso a la Red

Todos estos requerimientos condujeron a la elección de una red de conmutación de paquetes basada en una capa sin conexión que opera a través de distintas redes. La capa más baja en este modelo es la capa de Acceso a la red; ésta describe qué enlaces (como las líneas seriales y Ethernet clásica) se deben llevar a cabo para cumplir con las necesidades de esta capa de interred sin conexión. En realidad, no es una capa en el sentido común del término, sino una interfaz entre los hosts y los enlaces de transmisión. [7]

4.2.2.2 La capa de internet

Define un formato de paquete y un protocolo oficial llamado IP (Protocolo de Internet, del inglés Internet Protocol), además de un protocolo complementario llamado ICMP (Protocolo de Mensajes de Control de Internet, del inglés Internet Control Message Protocol) que le ayuda a funcionar. La tarea de la capa de interred es entregar los paquetes IP a donde se supone que deben ir. Aquí el ruteo de los paquetes es sin duda el principal aspecto, al igual que la congestión (aunque el IP no ha demostrado ser efectivo para evitar la congestión). [7]

4.2.2.3 La capa de transporte

Por lo general, a la capa que está arriba de la capa de internet en el modelo TCP/IP se le conoce como capa de transporte; y está diseñada para permitir que las entidades pares, en los nodos de origen y de destino, lleven a cabo una conversación, al igual que en la capa de transporte de OSI. Aquí se definieron dos protocolos de transporte de extremo a extremo. El primero, TCP (Protocolo de Control de la Transmisión, del inglés Transmission Control Protocol), es un protocolo confiable orientado a la conexión que permite que un flujo de bytes originado en una máquina se entregue sin errores a cualquier otra máquina en la internet. Este protocolo segmenta el flujo de bytes entrante en mensajes discretos y pasa cada uno a la capa de internet En el destino, el proceso TCP receptor vuelve a ensamblar los mensajes recibidos para formar el flujo de salida. El TCP también maneja el control de flujo para asegurar que un emisor rápido no pueda inundar a un receptor lento con más mensajes de los que pueda manejar. [8]

4.2.2.4 La capa de aplicación

El modelo TCP/IP no tiene capas de sesión o de presentación, ya que no se consideraron necesarias. Las aplicaciones simplemente incluyen cualquier función de sesión y de presentación que requieran. La experiencia con el modelo OSI ha demostrado que esta visión fue correcta: estas capas se utilizan muy poco en la mayoría de las aplicaciones. [8]

4.2.3 ¿Qué es un protocolo de red?

Es un conjunto de reglas que rigen el formato y el significado de los paquetes o mensajes que intercambian las entidades iguales en una capa. Las entidades utilizan protocolos para implementar sus definiciones de servicios. Pueden cambiar sus protocolos a voluntad, siempre y cuando no cambien el servicio visible para sus usuarios. De esta manera, el servicio y el protocolo no dependen uno del otro. [9]
Entre sus elementos a considerar se encuentran:

4.2.3.1 Protocolos de la Capa de Aplicación

- ***Protocolo de transferencia de hipertexto (HTTP, HyperText Transfer Protocol)***
  HTTP se implementa mediante dos programas: un programa cliente y un programa servidor. Ambos programas, que se ejecutan en sistemas terminales diferentes, se comunican entre sí intercambiando mensajes HTTP. HTTP define la estructura de estos mensajes y cómo el cliente y el servidor intercambian los mensajes. [10]

- ***Protocolo de transferencia de hipertexto Seguro (HTTPS HyperText Transfer Protocol Secure)***
  Es una extensión de HTTP con funciones de seguridad adicionales proporcionadas por Transport Layer Security (TLS) o su predecesor, Secure Sockets Layer (SSL). HTTPS cifra los datos transmitidos entre clientes y servidores, garantizando la confidencialidad, integridad y autenticidad. [10]

- ***El protocolo de transferencia de archivos (FTP, File Transfer Protocol)***
  Se utiliza para enviar archivos de un sistema a otro bajo el control del usuario. Se permite transmitir archivos tanto de texto como en binario. Además, el protocolo permite controlar el acceso de los usuarios. Cuando un usuario solicita la transferencia de un archivo, FTP establece una conexión TCP con el sistema destino para intercambiar mensajes de controlSSH.

- ***Telnet***
  Es el protocolo estándar para proporcionar servicios de emulación de terminal a través de una red TCP/IP, permitiendo la comunicación entre un cliente y un servidor mediante un canal confiable.

- ***SMTP (Simple Mail Transfer Protocol)***
  Es un protocolo de la capa de aplicación usado para la transferencia de correo electrónico en redes TCP/IP, diseñado para enviar mensajes desde un cliente de correo hacia un servidor o entre servidores de correo.

- ***IMAP (Internet Message Access Protocol)***
  Es un protocolo de la capa de aplicación que permite a un cliente de correo electrónico acceder y manipular mensajes almacenados en un servidor, ofreciendo funcionalidades avanzadas como organización en carpetas, búsqueda de mensajes y sincronización entre múltiples dispositivos.

- ***DNS (Domain Name System)***
  Es un sistema distribuido y jerárquico de la capa de aplicación que traduce nombres de dominio legibles por humanos en direcciones IP utilizadas por las computadoras en redes TCP/IP.

- ***DHCP (Dynamic Host Configuration Protocol)***
  Es un protocolo cliente-servidor que asigna dinámicamente direcciones IP y otros parámetros de configuración de red a los hosts, facilitando la administración de redes grandes.

- ***LDAP (Lightweight Directory Access Protocol)***
  Es un protocolo ligero para acceder y mantener servicios de directorio distribuidos sobre una red TCP/IP, utilizado comúnmente para autenticar usuarios y gestionar recursos.

- ***NTP (Network Time Protocol)***
  Es un protocolo que permite sincronizar la hora de las computadoras en Internet, funcionando en una arquitectura cliente-servidor o en jerarquía de servidores de tiempo.

4.2.3.2 Protocolos en la Capa de Transporte

Capa responsable de la entrega confiable de datos extremo a extremo, control de flujo, control de errores y segmentación de datos.

- ***TCP (Transmission Control Protocol)***
  Protocolo de transporte confiable orientado a conexión que garantiza la entrega ordenada y sin errores de los datos.

- ***UDP (User Datagram Protocol)***
  Protocolo de transporte sin conexión que proporciona un servicio de datagramas simple y rápido sin garantías de entrega.

4.2.3.3 Protocolos en la Capa de Red

Capa responsable del enrutamiento de paquetes a través de múltiples redes, direccionamiento lógico y determinación de rutas óptimas.

- **IP (IPv4/IPv6)**
  Protocolo de internet que proporciona direccionamiento lógico y enrutamiento de paquetes. IPv6 es la versión expandida con direcciones de 128 bits. [7]

- **ICMP (Internet Control Message Protocol)**
  Protocolo de control y error para IP que proporciona mecanismos de diagnóstico y reporte de errores [7]

- **IGMP (Internet Group Management Protocol)**
  Es un protocolo de red que permite a los dispositivos en una red (hosts) informar a un router de multidifusión sobre su interés en recibir transmisiones de multidifusión [7]

- **GRE (Generic Routing Encapsulation)**
  Protocolo de túnel que puede encapsular una amplia variedad de protocolos de capa de red dentro de túneles punto a punto. [9]

- **OSPF (Open Shortest Path First)**
  Protocolo de enrutamiento de estado de enlace que utiliza el algoritmo de Dijkstra para determinar rutas óptimas. [9]

4.2.3.4 Capa de Enlace de Datos

Capa responsable de la transmisión confiable de datos entre nodos adyacentes, detección de errores y control de acceso al medio.

- **STP (Spanning Tree Protocol)**
  Protocolo que previene bucles en topologías de red redundantes mediante la creación de un árbol de expansión. [11]

4.2.4 Elementos de una red

Las redes informáticas están constituidas principalmente por computadoras interconectadas, lo cual requiere de la participación de ciertos tipos de elementos, como son:

- **Clientes o terminales.** Son el conjunto de computadoras interconectadas que permiten a los usuarios acceder a la red informática. A menudo se las conoce también como “máquinas de trabajo”, ya que dependen de la presencia de un operador humano.
- **Servidores.** Son computadoras conectadas a la red en las que no opera ningún usuario, sino que se dedican a procesar el flujo de datos de la red, atendiendo a las peticiones de los terminales.
- **Elementos de hardware.** Son los dispositivos y periféricos que permiten el establecimiento de la comunicación en red, como son las tarjetas de red, módems y enrutadores, o antenas repetidoras, en el caso de las redes inalámbricas.
- **Elementos de software.** Son los programas requeridos para administrar el hardware de comunicaciones, como es el Sistema Operativo de Redes (también llamado NOS o Network Operating System), y los protocolos de comunicación, como TCP/IP.
- **Medios físicos de transmisión.** Son los elementos encargados de la transmisión física de la información, ya sea el cableado o las ondas electromagnéticas. [12]

4.2.5 Clasificación de redes (LAN, MAN, WAN).

- **Redes LAN**. Su nombre proviene del inglés Local Area Network ("Red de Área Local"), ya que se trata de las redes de menor envergadura y alcance, como las que se pueden instalar en un hogar o una oficina.
- **Redes MAN**. Su nombre proviene del inglés Metropolitan Area Network ("Red de Área Metropolitana"), pues se trata de redes de tamaño mediano, óptimas para un campus universitario o el edificio de una biblioteca o una empresa de varios pisos.
- **Redes WAN.** Su nombre proviene del inglés Wide Area Network ("Red de Área Amplia"), pues se trata de redes de gran tamaño y alcance, que pueden abarcar un país o incluso el planeta entero, como ocurre con internet

4.2.6 Topologías De Red

Las topologías de red son muy importantes en las comunicaciones ya que permiten estructurar los diferentes nodos que se encuentran en una organización, empresa, casa, universidades, escuelas, de acuerdo al funcionamiento que se pretenda implementar. Dependiendo de la forma en que estos nodos están interconectados, y de las características de estos nodos, obtendremos una red más o menos compleja, con mayor o menor rendimiento, además de condicionar otros aspectos, como la forma en que se implementan las posibles políticas de seguridad, sobre la misma. Cuando nos referimos a una determinada topología, podemos utilizarla para representar la forma de conexionado y el flujo físico de los datos, como, por ejemplo: punto a punto y punto a multipunto; o también podemos abstraernos al movimiento lógico de la información, sin importar la forma en que están conectados los elementos físicos que realizan la tarea de transportarla, como, por ejemplo: peer-to-peer [12]

4.2.6.1 Topología de red difusión

Las redes de difusión tienen un solo canal de difusión compartido por todas las máquinas de la red. Los mensajes cortos (paquetes) que envía una máquina son recibidos por todas las demás. Un campo de dirección dentro del paquete especifica a quién se dirige; al recibir un paquete, una máquina verifica el campo de dirección; y si el paquete está dirigido a ella, lo procesa; si está dirigido a otra máquina lo ignora. Los sistemas de difusión generalmente también ofrecen la posibilidad de dirigir un paquete a todos los destinos colocando un código especial en el campo de dirección; cuando se transmite un paquete con este código, cada máquina lo recibe y lo procesa, y este modo de operación se le llama difusión.

Algunos sistemas de difusión también contemplan la transmisión a un subconjunto de las máquinas, algo conocido como multidifusión. Las redes de difusión se dividen en estáticas y dinámicas, dependiendo de cómo

se asigna el canal. Una asignación estática típica, divide los intervalos discretos y ejecuta un algoritmo de asignación cíclica, permitiendo a cada máquina transmitir únicamente cuando llega su turno.

La asignación estática, desperdicia la capacidad del canal cuando una máquina no tiene nada que decir durante su segmento asignado, por lo que muchos sistemas intentan asignar el canal dinámicamente. [12]

Los métodos de asignación dinámica, pueden ser centralizados o descentralizados

- En el método de asignación de canal centralizado hay una sola entidad, la cual determina quién es la siguiente.
- En el descentralizado no existe una unidad central, cada máquina debe decidir por sí misma si transmite o no.

Sus características son:

- Empleadas en redes locales
- Software de admisión es simple porque no requiere de algoritmos de routing y el control de errores es de extremo a extremo.
- Se requiere reconocer la dirección destino
- Existe el único medio de transmisión, es decir solo hay un canal de comunicación. Los principales retrasos: espera de ganar el canal.
- El medio de transmisión puede ser totalmente pasivo, es decir solo está conduciendo la información.
- Se necesitarán duplicar las líneas en caso en que se requiera asegurar la funcionalidad ante fallas.
- Aumenta el costo, para poder asegurar más tarjetas de red.

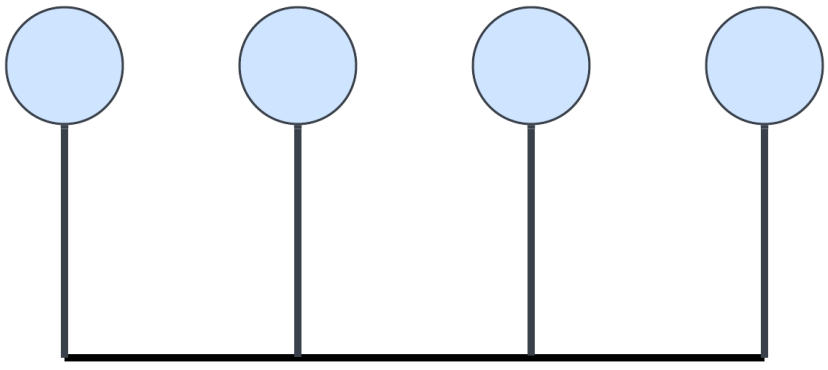

Figura 3: Topología De Red Punto A Punto

4.2.6.2 Topología De Red Punto A Punto

Las redes punto a punto (llamadas a veces de igual a igual) proporcionan muchas características avanzadas y la flexibilidad requerida hasta por las instalaciones más exigentes; la función general de todas las redes punto a punto es la misma: Que los nodos de la red compartan dispositivos como son las impresoras y lo más importante que es la información, la cual está contenida en las unidades de disco.

Al evaluar las redes punto a punto, son varios los factores que determinan si este tipo de red satisface nuestras necesidades. Basadas principalmente en cable y en cada conexión intervienen solo dos equipos [12]

Se dividen en:

- Simplex: inútil en redes de computadores (monodireccional).
- Semi-dúplex (Half-duplex): envía datos cada vez en un sentido.
- Dúplex (Full-duplex): envía datos en los dos sentidos a la vez.

Sus características son:

- Empleadas en redes WAN
- Los algoritmos de routing son complejos, se necesitan 2 niveles de control de errores.
- Se distribuye el mensaje a la estación indicada.
- Existen varias líneas de comunicación.
- El principal retraso es debido a la retransmisión del mensaje entre nodos intermedios.
- Medio de transmisión: nodos intermedios
- La redundancia es inherente siempre que el número de conexión de cada nodo sea mayor de 2

Figura 4: Ejemplo de la Topología Punto a Punto

4.2.6.3 Topologías De Redes Multipunto

En una red multipunto sólo existe una línea de comunicación cuyo uso está compartido por todas las terminales en la red, y la información fluye de forma bidireccional y es discernible para todas las terminales de la red. Lo típico es que en una conexión multipunto las terminales compiten por el uso del medio (línea) de forma que el primero que lo encuentra disponible lo acapara, aunque también puede negociar su uso. [12]

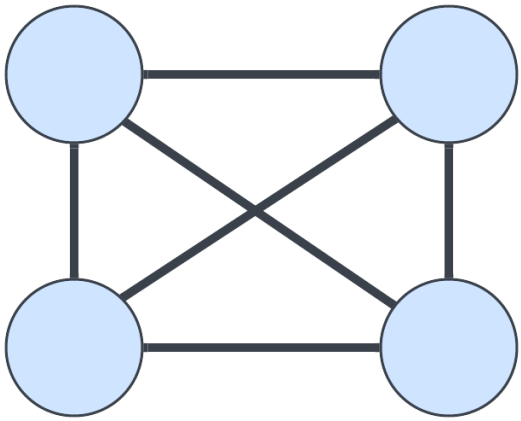

Figura 5: Ejemplo de redes multipunto

4.2.6.4 Topología en bus

La topología en bus tiene todos sus nodos conectados directamente a un cable central y lineal, donde físicamente cada dispositivo está conectado a un cable común, el cable o canal propaga las señales en ambas direcciones, de manera que todos los dispositivos puedan ver todas las señales de todos los demás dispositivos.

Esta característica puede ser ventajosa si se requiere que todos los dispositivos obtengan esa información, pero podría representar una desventaja debido al tráfico y podrían presentarse colisiones que afecten a la red. [12]

Las ventajas de la topología en canal o bus son:

- La facilidad de incorporar o quitar dispositivos de la red.
- Se requiere una menor cantidad de cableado que en otras topologías.

Su principal desventaja es:

- La ruptura del cableado hace que se rompa toda la comunicación dentro de la red que se encuentra conectado.

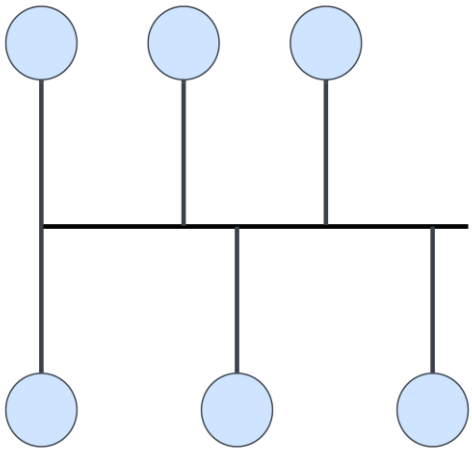

Figura 6: Ejemplo de la topología tipo bus

4.2.6.5 La Topología En Estrella

La topología en estrella se caracteriza por tener todos sus nodos conectados a un controlador central: donde todas las transacciones pasan a través del nodo central, siendo éste el encargado de gestionar y controlar todas las comunicaciones, por este motivo, el fallo de un nodo en particular es fácil de detectar y no daña el resto de la red, pero un fallo en el nodo central desactiva la red completa. [12]

Las ventajas de la topología en estrella son:

- Facilidad para incorporar o eliminar dispositivos de la red.
- La ruptura del cableado de un dispositivo, solo afecta a éste.
- Se detecta con facilidad alguna desconexión.

Las desventajas que presenta, son las siguientes:

- La cantidad de cableado requerido es superior a cualquier otra topología.
- Una falla en el hub o switch afecta a toda la red.

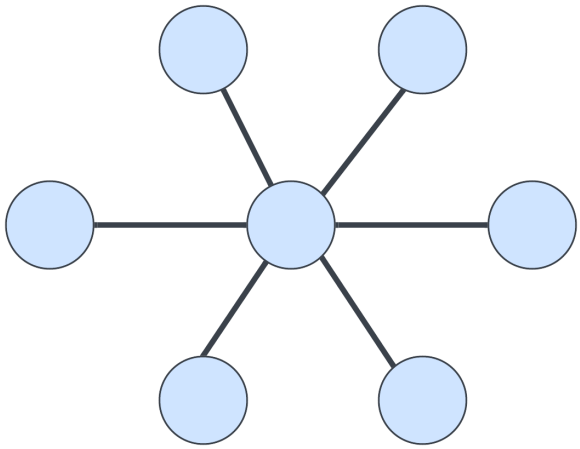

Figura 7: Ejemplo de la topología tipo estrella

4.2.6.6 Topología En Anillo

La topología en anillo se caracteriza por un camino unidireccional cerrado que conecta todos los nodos, dependiendo del control de acceso al medio, se dan nombres distintos a esta topología: Bucle; se utiliza para designar aquellos anillos en los que el control de acceso está centralizado (una de las estaciones se encarga de controlar el acceso a la red). [12]

La principal ventaja en redes con topología en anillo, es la estabilidad con respecto al tiempo que tardan las señales en llegar a su destino, sin que se presenten colisiones.
La desventaja que tiene esta topología es que la ruptura en la conexión de un dispositivo, tira toda la red.

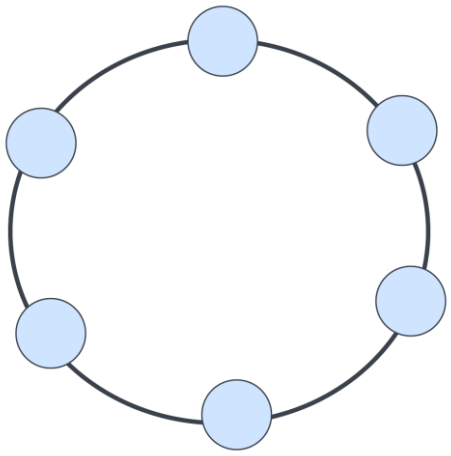

Figura 8: Ejemplo de la topología tipo anillo

4.2.6.7 Topología En Malla O Total

En esta topología, de uso común en redes tipo WAN, todos los nodos de la red están interconectados entre sí, formando una malla de conexiones similar a una tela de araña. La redundancia de conexiones busca que siempre exista un camino viable entre un nodo y otro [12]

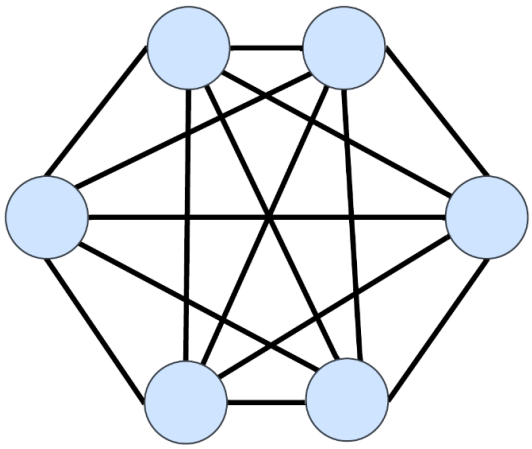

Figura 9: Ejemplo de la topología tipo malla

4.2.6.8 Tipos de topología hibrida o mixta

Como su nombre lo indica, es una combinación de dos o más topologías de red diferentes, para adaptar la red a las necesidades del cliente, de este modo, podemos combinar las topologías que deseemos, obteniendo infinitas variedades, las cuales, deben ajustarse a la estructura física del lugar en donde estará la red y los equipos que estarán conectados en dicha red. En una topología mixta, se combinan dos o más topologías para formar un diseño de red completo, esta combinación puede darse en diferentes tipos de redes, LAN, MAN y WAN, dependiendo del diseño y funcionamiento que presente cada una de ellas. [12]

Ventajas Las redes híbridas o mixtas

Ofrecen múltiples posibilidades para la transmisión de datos entre nodos de la red; el fallo de cualquier componente simple de hardware (tal como una impresora o un cable) no afecta al rendimiento de la red, y en tal caso, la red híbrida evita el nodo/cable afectado y desplaza los datos a una ruta de transmisión alternativa. Las redes híbridas son versátiles y pueden adaptarse a una amplia variedad de requerimientos y tamaños de red.

Desventajas

Una red híbrida requiere más cableado entre sus nodos que otros tipos de redes; las inconsistencias y errores en los nodos individuales de una red híbrida son a menudo difíciles de aislar y reparar.

Las redes híbridas eficientes requieren puntos o centros inteligentes de concentración; los concentradores inteligentes están diseñados para proporcionar aislamiento de fallos y procesamiento automáticos. Constantemente escanean la red, recogen información sobre todos los nodos, detectan errores, aíslan los nodos defectuosos y convierten el tráfico de red a rutas alternas.

Los concentradores inteligentes, aunque eficientes, son más caros que los pasivos y los activos. Las redes híbridas de gran tamaño comúnmente requieren varios concentradores inteligentes

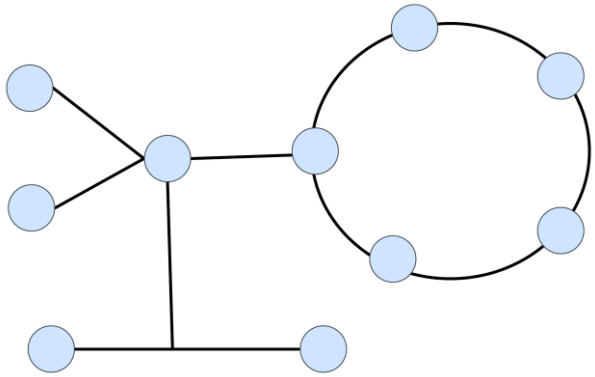

Figura 10: Ejemplo de la topología hibrida o mixta

4.2.6.9 Una topología en estrella extendida

Conecta estrellas individuales entre sí mediante la conexión de hubs o switches. Esta topología puede extender el alcance y la cobertura de la red. [12]

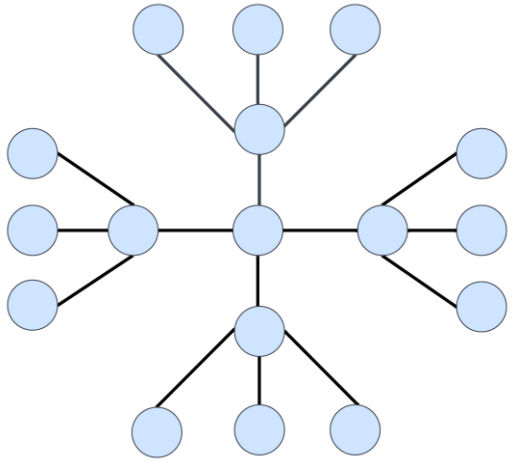

Figura 11: Ejemplo de la topología de estrella extendida

4.2.6.10 Topología de red jerárquica - árbol

Es la topología de red en la que los nodos están colocados en forma de árbol, y desde una visión topológica, la conexión en árbol es parecida a una serie de redes en estrella interconectadas salvo en que no tiene un nodo central. Tiene un nodo de enlace troncal, generalmente ocupado por un hub o switch, desde el que se ramifican los demás nodos; es una variación de la red en bus, la falla de un nodo no implica interrupción en las comunicaciones, y se comparte el mismo canal de comunicaciones. La topología en árbol puede verse como una combinación de varias topologías en estrella. Tanto la de árbol como la de estrella son similares a la de bus cuando el nodo de interconexión trabaja en modo difusión, pues la información se propaga hacia todas las estaciones, solo que en esta topología las ramificaciones se extienden a partir de un punto raíz (estrella), a tantas ramificaciones como sean posibles, según las características del árbol. [12]

Los problemas asociados a las topologías anteriores radican en que los datos son recibidos por todas las estaciones sin importar para quién vayan dirigidos.

Ventajas de Topología de Árbol

- El Hub o switch central al retransmitir las señales amplifica la potencia e incrementa la distancia a la que puede viajar la señal.
- Se permite conectar más dispositivos gracias a la inclusión de concentradores secundarios.
- Cableado punto a punto para segmentos individuales.
- Soportado por multitud de vendedores de software y de hardware.

Desventajas de Topología de Árbol

- Se requiere mucho cable.
- La medida de cada segmento viene determinada por el tipo de cable utilizado.
- Si se viene abajo el segmento principal todo el segmento se viene abajo con él.

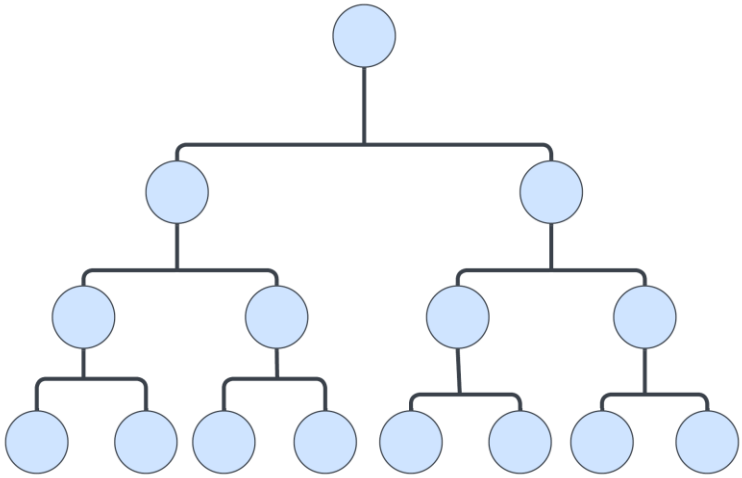

Figura 12: Ejemplo de la topología tipo árbol

4.3 Infraestructura de red de computadoras

Es el conjunto de componentes físicos (hardware) y lógicos (software) que permiten la conexión de dispositivos y la comunicación de datos en redes informáticas, como Internet o las redes locales de una empresa. Incluye elementos como el cableado estructurado, switches, routers, firewalls y software de gestión, que son esenciales para el flujo de información, la seguridad, el rendimiento y la escalabilidad de los sistemas de TI.

4.3.1 Componentes físicos de una infraestructura de red

Para que la comunicación en red sea operativa, en primer lugar, es necesario interconectar los equipos entre ellos. Frecuentemente se utiliza una interfaz por cable, como un cable conectado a una tarjeta de red o a un módem. También se puede utilizar la interfaz inalámbrica a través de comunicaciones inalámbricas, que utilizan los infrarrojos, el láser o las ondas de radio. [13]

Los componentes físicos de una infraestructura de red son todos aquellos elementos tangibles que permiten la transmisión de datos y la conectividad entre los dispositivos interconectados. Entre los más relevantes se encuentran:

- **Switches (conmutadores):** Los switches son piezas de construcción clave para cualquier red. Conectan varios dispositivos, como computadoras, Access points inalámbricos, impresoras y

servidores; en la misma red dentro de un edificio o campus. Un switch permite a los dispositivos conectados compartir información y comunicarse entre sí. [14]

- **Routers (enrutadores):** un router funciona como un distribuidor, que dirige el tráfico y elige la ruta más eficiente para que la información, en forma de paquetes de datos, Además de conectar varias redes, el router también permite que los dispositivos en red y varios usuarios accedan a Internet. [15]
- **Cableado estructurado:** El cableado estructurado se refiere al medio de transmisión de datos guiados, cada uno cuenta con diferente nicho en términos de ancho de banda, retardo, costo y facilidad de instalación y mantenimiento. Algunos de los más utilizados son, par trenzado, coaxial, fibra óptica. [16]
- **Servidores:** poderosas computadoras dedicadas a servicios específicos, a esto se le denomina servidores. Entre ellos podemos encontrar servicios como, WEB, HOST, Correo Electrónico, entre muchos otros. [16]
- **Puntos de acceso inalámbrico (Access Points):** Un access point inalámbrico (WAP) es un dispositivo de red que permite que los dispositivos con capacidad inalámbrica se conecten a una red cableada. [17]
- **Firewall (cortafuegos):** dispositivo o software de seguridad que actúa como un filtro de paquetes. Inspecciona todos y cada uno de los paquetes entrantes y salientes. Los paquetes que cumplen cierto criterio descrito en reglas formuladas por el administrador de la red se reenvían en forma normal. Los que fallan la prueba simplemente se descartan. [18]
- **AC (Access Controller o Controlador de Acceso WLAN):** tiene como objetivo principal poder centralizar todo el control de los puntos de acceso, de esta forma estará evitándose delegar un control para cada uno de estos puntos. Por lo tanto, la AP ya no va a funcionar de forma automática sino pasará a convertirse en lo que se llama un AP ligero "LWAP", para ello contará con la colaboración del protocolo de control y aprovisionamiento para los puntos de Acceso Inalámbricos **"CAPWAP"** [19]
- **IDS (Intrusion Detection System):** Un sistema de detección de intrusiones es una herramienta de seguridad de red que monitorea el tráfico de red y los dispositivos para detectar actividades maliciosas conocidas, actividades sospechosas o infracciones a las políticas de seguridad. Puede ayudar a acelerar y automatizar la detección de amenazas en la red alertando a los administradores de seguridad sobre amenazas conocidas o potenciales, o enviando alertas a una herramienta de seguridad centralizada. [20]
- Racks y gabinetes de comunicaciones: estructuras metálicas donde se instalan switches, routers, servidores, paneles de parcheo y equipos de protección, asegurando organización y ventilación adecuada.
- Paneles de parcheo (Patch Panels): elementos intermedios donde terminan los cables de red estructurados, permitiendo una administración ordenada de conexiones.

- Sistemas de cableado de fibra óptica: necesarios para interconectar edificios, gabinetes de distribución o el backbone de la red, ofreciendo mayor ancho de banda y menor latencia que el cobre. [21]

4.3.2 Componentes lógicos de una Infraestructura de red

Los componentes lógicos de una red comprenden todos aquellos elementos no físicos que regulan, controlan y permiten el funcionamiento eficiente de la comunicación de datos. Entre ellos destacan:

- Protocolos de red: son reglas y estándares que determinan cómo se comunican los dispositivos dentro de una red. Algunos de los más utilizados son:
  - ✓ IP (Internet Protocol): direccionamiento y envío de datos entre redes.
  - ✓ TCP/UDP: control de transmisión de datos.
  - ✓ HTTP/HTTPS: transferencia de contenido web.
  - ✓ DNS, DHCP, SNMP, FTP, SMTP: protocolos específicos para servicios de red.
- VLANs (Virtual Local Area Networks): segmentaciones lógicas dentro de la red que permiten separar grupos de dispositivos según su función (administrativos, docentes, estudiantes, laboratorios, voz, servidores, invitados). Mejoran la seguridad, reducen el dominio de broadcast y facilitan la administración del tráfico.
- **Protocolos de enrutamiento:** permiten que los routers o switches de capa 3 determinen la mejor ruta para enviar paquetes entre diferentes redes. Pueden ser:
  - ✓ **Estáticos:** configurados manualmente, adecuados para redes pequeñas o enlaces fijos.
  - ✓ **Dinámicos:** actualizan rutas automáticamente según cambios en la red. Entre los más usados están **RIP** (sencillo pero limitado), **EIGRP** (rápida convergencia), **OSPF** (eficiente y escalable, ideal para campus) y **BGP** (utilizado para interconexión con proveedores de Internet).
- **Protocolos de redundancia y disponibilidad:**
  - ✓ **HSRP/VRRP:** permiten crear una puerta de enlace virtual redundante para asegurar la continuidad en caso de falla de un router o switch.
  - ✓ **LACP (Link Aggregation Control Protocol):** protocolo que agrupa múltiples enlaces físicos en un único enlace lógico para aumentar la capacidad y la tolerancia a fallos.
  - ✓ **STP/RSTP (Spanning Tree Protocol):** previenen bucles de capa 2 en topologías con enlaces redundantes.
- Servicios de red: funciones operadas por servidores que facilitan la administración y operación de la red. Los más comunes son:
  - ✓ DHCP: asignación automática de direcciones IP.
  - ✓ DNS: resolución de nombres de dominio.

- ✓ AAA (RADIUS/TACACS+): control de autenticación, autorización y contabilización.
- ✓ VPN: acceso remoto seguro.
- ✓ VoIP: comunicación de voz a través de IP.
- ✓ Servidor web: alojamiento de plataformas y sistemas.

- Direccionamiento IP: esquema de asignación de direcciones únicas a cada dispositivo dentro de la red. Se puede usar direccionamiento IPv4 **(**como 192.168.1.1) o IPv6, y se organiza mediante subredes y máscaras. Este componente es esencial para la segmentación, el enrutamiento y el control del tráfico.
- Topologías y políticas de red: definen la estructura lógica de la red (estrella, anillo, malla, árbol) y las reglas de operación, como políticas de calidad de servicio (QoS), control de ancho de banda, y listas de control de acceso (ACLs)

4.3.3 La importancia de la infraestructura de red

Todas las tecnologías que te permiten ofrecer experiencias significativas a los clientes dependen de una infraestructura de red confiable, adaptable y centrada en la seguridad. Estas pueden ser los enrutadores, los conmutadores, los servidores, las entidades virtuales, las máquinas virtuales, el software de infraestructura, los microservicios y las aplicaciones modernas. La infraestructura de red posibilita la conexión y la comunicación entre las aplicaciones en todos los niveles, y también con tus clientes.

- Confiable, adaptable y centrada en la seguridad tiene mucho que ofrecer:
- Mejora la seguridad, ya que restringe el acceso según las funciones y la aplicación.
- Funciona como base para ofrecer mejores experiencias a los usuarios.
- Posibilita la prestación de servicios de red y permite que los proveedores de servicios de telecomunicaciones dejen de lado el hardware especializado para adoptar los sistemas de software open source. [22]

4.4 ¿Qué es una red de área de campus (CAN)?

Una red de área de campus (CAN) es una red informática que abarca un área geográfica limitada. Las CAN interconectan varias redes de área local (LAN) dentro de un campus educativo o corporativo. La mayoría de las CAN se conectan a la Internet pública.

Las CAN son más pequeñas que las redes de área metropolitana (MAN) y que las redes de área amplia (WAN), que se extienden por grandes áreas geográficas. Normalmente, la organización propietaria del campus también posee y opera todo el equipo, y la infraestructura de red para la CAN. En cambio, las MAN y las WAN pueden combinar infraestructuras operadas por varios proveedores diferentes.

En facultades, universidades y otras instituciones educativas, las CAN proporcionan acceso a Internet a estudiantes y profesores. Las CAN también permiten que los usuarios conectados compartan rápidamente

archivos y datos dentro de la red: como los datos no tienen que salir de la CAN, los usuarios experimentan una latencia mucho menor que cuando envían y reciben datos dentro de una MAN o WAN.

4.4.1 ¿Cuáles son las ventajas de seguridad de las CAN?

Una CAN la suele gestionar íntegramente un equipo de TI interno, lo que le da un alto grado de control sobre la red. Los equipos de TI pueden aplicar políticas de seguridad en toda la red con mucha más facilidad que si el campus utilizara varias redes desconectadas. Por ejemplo, el equipo de TI puede instalar y gestionar los firewalls para proteger los datos dentro de la CAN. El departamento de TI también puede gestionar el acceso a la red estableciendo requisitos de inicio de sesión, bloqueando los dispositivos no seguros y estableciendo otras garantías de control de acceso. [23]

4.4.2 Modelo jerárquico de tres capas

El modelo jerárquico de redes es una arquitectura ampliamente recomendada para diseñar infraestructuras de red escalables, organizadas, seguras y de fácil mantenimiento. Esta estructura se divide en tres capas funcionales: acceso, distribución y núcleo (core), cada una con responsabilidades y características específicas. Este modelo permite aislar funciones críticas, facilitar la implementación de políticas, optimizar el rendimiento y mejorar la disponibilidad de la red. A continuación, se describen sus tres capas principales:

a. Capa de acceso

Es la capa más cercana al usuario final y representa el punto de entrada a la red. Aquí se conectan los dispositivos terminales como computadoras, impresoras, teléfonos IP y puntos de acceso inalámbrico.

Funciones principales:

- Conectar usuarios y dispositivos finales a la red.
- Aplicar políticas básicas de seguridad (ACLs, autenticación 802.1X).
- Definir VLANs para segmentación lógica.
- Ofrecer conectividad mediante switches gestionables.

Características técnicas:

- Uso de switches de capa 2.
- Puede implementar PoE (Power over Ethernet) para alimentar dispositivos como cámaras o teléfonos IP.
- Generalmente, incluye redundancia hacia la capa de distribución.

b. Capa de distribución

Actúa como intermediaria entre la capa de acceso y el núcleo. Su principal función es agregar y gestionar el tráfico proveniente de múltiples switches de acceso.

Funciones principales:

- Enrutamiento entre VLANs.
- Aplicación de políticas de control y seguridad más avanzadas.
- Gestión del tráfico de múltiples segmentos de red.
- Filtrado y priorización de datos (QoS).
- Proveer redundancia y enlaces troncales hacia el núcleo.

Características técnicas:

- Uso de switches de capa 3 (con capacidad de enrutamiento).
- Conectividad redundante hacia acceso y core.
- Es ideal para implementar servicios como AAA o DHCP relay.

c. Capa núcleo (core)

Es el corazón de la red. Su objetivo es proporcionar una conectividad de alta velocidad, altamente disponible y confiable entre todos los segmentos de la red, incluyendo enlaces hacia servidores, data centers y conexiones externas (como internet).

Funciones principales:

- Transportar grandes volúmenes de datos con la menor latencia posible.
- Interconectar todas las capas de distribución.
- Servir como punto de convergencia para servidores críticos o enlaces WAN.

Características técnicas:

- Alta capacidad de procesamiento y conmutación.
- Implementación de redundancia total (dual routers, enlaces agregados).
- Tolerancia a fallos con protocolos como HSRP, VRRP o GLBP.
- Generalmente, no se aplican políticas ni servicios en esta capa para evitar congestiones.

4.5 ¿Qué es una VLAN?

Una VLAN (Virtual Local Area Network) es una red lógica que permite agrupar dispositivos dentro de una misma red física como si estuvieran en redes separadas, con el fin de mejorar la seguridad, organización y eficiencia del tráfico de red. [24]

4.5.1 ¿Cómo funcionan las VLANs?

Las VLANs operan en la capa 2 del modelo OSI, la de enlace de datos, y lo hacen etiquetando las tramas de datos con identificadores únicos llamados VLAN IDs, que utilizan el estándar IEEE 802.1Q
Esto permite que los switches gestionen el tráfico de forma que únicamente los dispositivos pertenecientes a la misma VLAN puedan comunicarse directamente entre sí. Este aislamiento lógico es muy útil en entornos en los que se necesita separar el tráfico por razones de seguridad o eficiencia, como por ejemplo una empresa que desea dividir el acceso entre sus diferentes departamentos y evitar además posibles conflictos o brechas de seguridad. [24]

4.5.2 Tipos de VLAN y sus aplicaciones

Existen diferentes clases de red, cada una de ellas diseñada para satisfacer necesidades muy concretas dentro de una red.

- **VLAN de datos:** Destinadas al tráfico de datos estándar de los usuarios. Se utilizan para mejorar la organización y seguridad segmentando la red.
- **VLAN de voz:** Optimizadas para el tráfico de VoIP (Voice over IP), lo que garantiza una excelente calidad para las comunicaciones de este tipo.
- **VLAN de gestión:** Reservadas para el acceso y control de dispositivos de red como switches y routers, a los que proporcionan una capa extra de seguridad.
- **VLAN nativa:** Se utiliza en enlaces troncales entre switches para gestionar el tráfico no etiquetado. Es importante que la configuración de la red sea correcta para evitar problemas de seguridad y funcionamiento. [24]

4.5.3 Segmentación Lógica con VLANs

Una VLAN (Virtual Local Area Network) permite crear subredes lógicas dentro de una misma infraestructura física. Mediante la segmentación por VLANs, se puede agrupar a usuarios o servicios según su función, área o nivel de privilegio, lo que ayuda a:

- Reducir el tráfico de broadcast.
- Mejorar el rendimiento de la red.
- Aumentar la seguridad mediante el aislamiento de segmentos críticos.
- Aplicar políticas diferenciadas por grupo de usuarios.

4.6 Servicios Esenciales de Red

Una red moderna y funcional requiere de la integración de servicios fundamentales que aseguren la conectividad dinámica y segura de los dispositivos. Entre los más relevantes se encuentran:

- **DNS (Domain Name System):** servicio que traduce nombres de dominio a direcciones IP, facilitando el acceso a recursos de red.
- **DHCP (Dynamic Host Configuration Protocol):** asigna direcciones IP de manera automática y temporal a los dispositivos conectados.
- **VPN (Virtual Private Network):** permite la conexión remota segura a la red institucional a través de túneles cifrados.
- **VoIP (Voice over IP**): tecnología que transmite comunicaciones de voz mediante el protocolo IP, utilizando softphones o teléfonos IP.

Los servicios de red son necesarios para satisfacer las necesidades de conexión a internet de los usuarios de la facultad multidisciplinaria oriental, por lo cual es recomendable contar con una distribución de servicios propia, que permita a los estudiantes y usuarios contar con disponibilidad local de servicios de internet, así como una forma segura de interconectarse.

5. Investigación de la Infraestructura Actual

5.1 Inventario de Equipos de Red en el Data center

En el presente inventario se registran los equipos de red del Data Center**,** especificando sus características técnicas, ubicación, conectividad y responsables asignados. Cada ficha técnica resume la información esencial de los dispositivos, permitiendo un control organizado de los recursos y asegurando la disponibilidad de datos precisos para procesos de mantenimiento, soporte y auditoría.

Equipo: NCE	
ID	NCE
FECHA	21 de agosto del 2025
HORA	10:00 AM
NÚMERO DE SERIE	1021C6034988
MARCA	HUAWEI
MODELO	AirEngine9700-M1_6F0DD791

TIPO DE EQUIPO	Controlador de AP
SISTEMA OPERATIVO	Versatile Routing Platform
SERVICIO QUE BRINDA	Gestión de AC y AP, aprovisionamiento de WLAN
CONECTADO A	-
TIPO DE CONECTIVIDAD	Fibra óptica
UBICACIÓN	DATA CENTER
RESPONSABLE O ENCARGADO	Ing. Guadalupe Bermúdez
INTERFACES ACTIVAS	-
DIRECCIONES IP	172.17.24.X:18008
SUBREDES UTILIZADAS	172.17.24.0

Tabla 1: Ficha técnica del equipo NCE

Equipo: WAC	
ID	WAC
FECHA	21 de agosto del 2025
HORA	10:00 AM
NÚMERO DE SERIE	1021C6034988
MARCA	HUAWEI
MODELO	Wireless LAN AirEngine9700- M1
TIPO DE EQUIPO	Controlador de red
SISTEMA OPERATIVO	Versatile Routing Platform
SERVICIO QUE BRINDA	Gestión de AC y AP, aprovisionamiento de WLAN
CONECTADO A	-
TIPO DE CONECTIVIDAD	Fibra óptica
UBICACIÓN	DATA CENTER
RESPONSABLE O ENCARGADO	Ing. Guadalupe Bermúdez Bermúdez
INTERFACES ACTIVAS	-
DIRECCIONES IP	172.17.60.X MGMT 10.60.100.XCAPWAP
SUBREDES UTILIZADAS	-

Tabla 2: Ficha técnica del equipo WAC

Equipo: FIREWALL01_ETH_PORT_01	
ID	FIREWALL01_ETH_PORT_01
FECHA	21 de agosto del 2025
HORA	10:00 AM
NÚMERO DE SERIE	1021C0011920
MARCA	HUAWEI
MODELO	USG6610E-01
TIPO DE EQUIPO	Firewall perimetral
SISTEMA OPERATIVO	Versatile Routing Platform
SERVICIO QUE BRINDA	seguridad perimetral
CONECTADO A	-
TIPO DE CONECTIVIDAD	Fibra óptica
UBICACIÓN	DATA CENTER
RESPONSABLE O ENCARGADO	Ing. Guadalupe Bermúdez
INTERFACES ACTIVAS	-
DIRECCIONES IP	172.17.60.X:8443
SUBREDES UTILIZADAS	172.17.60.0

Tabla 3: Ficha técnica del equipo FIREWALL01_ETH_PORT_01

Equipo: FIREWALL02_ETH_PORT_02	
ID	FIREWALL02_ETH_PORT_02
FECHA	21 de agosto del 2025
HORA	10:00 AM
NÚMERO DE SERIE	1021C0011919
MARCA	HUAWEI
MODELO	USG6610E-02
TIPO DE EQUIPO	Firewall perimetral
SISTEMA OPERATIVO	Versatile Routing Platform
SERVICIO QUE BRINDA	seguridad perimetral
CONECTADO A	-

TIPO DE CONECTIVIDAD	Fibra Optica
UBICACIÓN	DATA CENTER
RESPONSABLE O ENCARGADO	Ing. Guadalupe Bermúdez
INTERFACES ACTIVAS	-
DIRECCIONES IP	172.17.60.X
SUBREDES UTILIZADAS	172.17.60.0

Tabla 4: Ficha técnica del equipo FIREWALL01_ETH_PORT_02

Equipo: ROUTER01_ETH_PORT	
ID	ROUTER01_ETH_PORT
FECHA	21 de agosto del 2025
HORA	10:00 AM
NUMERO DE SERIE	2102353HFW10MC100068
MARCA	HUAWEI
MODELO	SMGEdgeNE8KM1A
TIPO DE EQUIPO	Router de borde
SISTEMA OPERATIVO	Versatile Routing Platform
SERVICIO QUE BRINDA	Encaminamiento de tráfico WAN/LAN
CONECTADO A	-
TIPO DE CONECTIVIDAD	-
UBICACIÓN	DATA CENTER
RESPONSABLE O ENCARGADO	Ing. Guadalupe Bermúdez
INTERFACES ACTIVAS	-
DIRECCIONES IP	172.17.60.X/loop: 172.17.62.X
SUBREDES UTILIZADAS	172.17.60.0

Tabla 5: Ficha técnica del equipo ROUTER01_ETH_PORT

Equipo: ROUTER02_ETH_PORT	
ID	ROUTER02_ETH_PORT
FECHA	21 de agosto del 2025

HORA	10:00 AM
NUMERO DE SERIE	2102353HFW10MC100070
MARCA	HUAWEI
MODELO	SMGEdgeNE8KM1A
TIPO DE EQUIPO	Router de borde
SISTEMA OPERATIVO	Versatile Routing Platform
SERVICIO QUE BRINDA	Encaminamiento de tráfico WAN/LAN
CONECTADO A	-
TIPO DE CONECTIVIDAD	Fibra Óptica
UBICACIÓN	DATA CENTER
RESPONSABLE O ENCARGADO	Ing. Guadalupe Bermúdez
INTERFACES ACTIVAS	-
DIRECCIONES IP	172.17.60.X/loop: 172.17.62.X
SUBREDES UTILIZADAS	172.17.60.0

Tabla 6: Tabla 5: Ficha técnica del equipo ROUTER02_ETH_PORT

Equipo: ANTIDDOS01	
ID	ANTIDDOS01
FECHA	21 de agosto del 2025
HORA	10:00 AM
NÚMERO DE SERIE	1021C0011654
MARCA	HUAWEI
MODELO	1905_CLEANING
TIPO DE EQUIPO	Anti-DDoS
SISTEMA OPERATIVO	Huawei AntiDDoS OS
SERVICIO QUE BRINDA	Detección y mitigación de ataques DDoS
CONECTADO A	-
TIPO DE CONECTIVIDAD	Fibra óptica
UBICACIÓN	DATA CENTER
RESPONSABLE O ENCARGADO	Ing. Guadalupe Bermúdez

INTERFACES ACTIVAS	-
DIRECCIONES IP	172.17.60.X
SUBREDES UTILIZADAS	172.17.60.0

Tabla 7: Ficha técnica del equipo ANTIDDOS01

Equipo: ANTIDDOS02	
ID	ANTIDDOS02
FECHA	21 de agosto del 2025
HORA	10:00 AM
NÚMERO DE SERIE	1021C0011651
MARCA	HUAWEI
MODELO	Huawei S1905
TIPO DE EQUIPO	Anti-DDoS
SISTEMA OPERATIVO	Huawei AntiDDoS OS
SERVICIO QUE BRINDA	Detección y mitigación de ataques DDoS
CONECTADO A	-
TIPO DE CONECTIVIDAD	Fibra Óptica
UBICACIÓN	DATA CENTER
RESPONSABLE O ENCARGADO	Ing. Guadalupe Bermúdez
INTERFACES ACTIVAS	-
DIRECCIONES IP	172.17.60.X
SUBREDES UTILIZADAS	172.17.60.0

Tabla 8: Ficha técnica del equipo ANTIDDOS02

Equipo: SW_ACCESS_DC	
ID	SW_ACCESS_DC
FECHA	21 de agosto del 2025
HORA	10:00 AM
NUMERO DE SERIE	3G21C0046597

MARCA	HUAWEI
MODELO	S5736-S24UM4XC
TIPO DE EQUIPO	Switch de acceso
SISTEMA OPERATIVO	Versatile Routing Platform
SERVICIO QUE BRINDA	Conmutación capa 2/3
CONECTADO A	Biblioteca, Enlace de distribución Educación, Sistemas Informáticos, Posgrados, UESED, Ingeniería y Arquitectura, Decanato, laboratorio Realidad Virtual, académica, pantallas Aula de sociología, servidores, Enlace Firewalls
TIPO DE CONECTIVIDAD	Fibra Óptica
UBICACIÓN	DATA CENTER
RESPONSABLE O ENCARGADO	Ing. Guadalupe Bermúdez
INTERFACES ACTIVAS	14
DIRECCIONES IP	172.19.29.X
SUBREDES UTILIZADAS	172.19.29.0

Tabla 9: Ficha técnica del equipo SW_ACCESS_DC

Equipo: CONTROLADORA1	
ID	CONTROLADORA1
FECHA	21 de agosto del 2025
HORA	10:00 AM
NUMERO DE SERIE	-
MARCA	CISCO
MODELO	Cisco Controladora
TIPO DE EQUIPO	Contralador de AP cisco
SISTEMA OPERATIVO	Cisco IOS XE (WLC)
SERVICIO QUE BRINDA	Reconocimiento y gestión de AP cisco
CONECTADO A	-
TIPO DE CONECTIVIDAD	Fibra Óptica
UBICACIÓN	DATA CENTER

RESPONSABLE O ENCARGADO	Ing. Guadalupe Bermúdez
INTERFACES ACTIVAS	-
DIRECCIONES IP	172.16.0.X
SUBREDES UTILIZADAS	172.16.0.0

Tabla 10: Ficha técnica del equipo CONTROLADORA1

Equipo: CONTROLADORA2	
ID	CONTROLADORA2
FECHA	21 de agosto del 2025
HORA	10:00 AM
NÚMERO DE SERIE	FCL240200U2
MARCA	CISCO
MODELO	Cisco Controladora
TIPO DE EQUIPO	
SISTEMA OPERATIVO	Cisco IOS XE (WLC software)
SERVICIO QUE BRINDA	-
CONECTADO A	-
TIPO DE CONECTIVIDAD	Fibra OPTICA
UBICACIÓN	DATA CENTER
RESPONSABLE O ENCARGADO	Ing. Guadalupe Bermúdez
INTERFACES ACTIVAS	-
DIRECCIONES IP	172.16.16.X
SUBREDES UTILIZADAS	172.16.16.0

Tabla 11: Ficha técnica del equipo CONTROLADORA2

Equipo: DATACENTER	
ID	DATACENTER
FECHA	21 de agosto del 2025
HORA	10:00 AM
NUMERO DE SERIE	SOLO MONITOREO

MARCA	CISCO
MODELO	9800-L-F
TIPO DE EQUIPO	Controladora inalámbrica
SISTEMA OPERATIVO	Cisco IOS / IOS XE
SERVICIO QUE BRINDA	Gestión de WLAN
CONECTADO A	-
TIPO DE CONECTIVIDAD	Fibra Óptica
UBICACIÓN	DATA CENTER
RESPONSABLE O ENCARGADO	Ing. Guadalupe Bermúdez
INTERFACES ACTIVAS	-
DIRECCIONES IP	172.16.0.x
SUBREDES UTILIZADAS	172.16.0.0

Tabla 12: Ficha técnica del equipo DATACENTER (CISCO 9800-L-F)

Equipo: CORE DISTRIBUCIÓN 1	
ID	CORE DISTRIBUCIÓN 1
FECHA	21 de agosto del 2025
HORA	10:00 AM
NUMERO DE SERIE	102010022304
MARCA	HUAWEI
MODELO	S6730-H48X6C
TIPO DE EQUIPO	Switch de núcleo/distribución
SISTEMA OPERATIVO	Versatile Routing Platform
SERVICIO QUE BRINDA	Conmutación capa 3 (core)
CONECTADO A	A firewalla
TIPO DE CONECTIVIDAD	Fibra óptica
UBICACIÓN	DATA CENTER
RESPONSABLE O ENCARGADO	Ing. Guadalupe Bermúdez
INTERFACES ACTIVAS	15
DIRECCIONES IP	192.168.10.X
SUBREDES UTILIZADAS	92.168.10.0

Tabla 13: Ficha técnica del equipo CORE DISTRIBUCION 1

Equipo: SISTEMA DE SERVIDORES	
ID	SISTEMA DE SERVIDORES
FECHA	21 de agosto del 2025
HORA	10:00 AM
NÚMERO DE SERIE	FCW1943C168
MARCA	CISCO
MODELO	Cisco Catalyst 3850
TIPO DE EQUIPO	Switch para servidores
SISTEMA OPERATIVO	Cisco IOS XE
SERVICIO QUE BRINDA	Conmutación para sistemas/servidores
CONECTADO A	-
TIPO DE CONECTIVIDAD	Fibra optica
UBICACIÓN	DATA CENTER
RESPONSABLE O ENCARGADO	Ing. Guadalupe Bermúdez
INTERFACES ACTIVAS	
DIRECCIONES IP	192.168.10.X
SUBREDES UTILIZADAS	92.168.10.0

Tabla 14: Ficha técnica para el equipo SISTEMA DE SERVIDORES (CISCO CATALYST 3850)

Equipo: SISTEMAS	
ID	SISTEMAS
FECHA	21 de agosto del 2025
HORA	10:00 AM
NÚMERO DE SERIE	21980109364ELC008422
MARCA	HUAWEI
MODELO	S5735-L48T4X-A
TIPO DE EQUIPO	Switch de acceso/servidores
SISTEMA OPERATIVO	Versatile Routing Platform
SERVICIO QUE BRINDA	Switching

CONECTADO A	-
TIPO DE CONECTIVIDAD	Fibra Optica
UBICACIÓN	DATA CENTER
RESPONSABLE O ENCARGADO	Ing. Guadalupe Bermúdez
INTERFACES ACTIVAS	-
DIRECCIONES IP	192.168.10.X
SUBREDES UTILIZADAS	92.168.10.0

Tabla 15: Ficha técnica del equipo SISTEMAS (Huawei S5735-L48T4X-A)

5.2 Inventario de Equipos de Red en los departamentos

En la siguiente tabla se muestra el inventario de equipos de red ubicados en los diferentes departamentos de la institución**,** incluyendo datos como número de registro, nombre del equipo, ubicación física, marca, dirección IP, modelo y número de serie. La información se encuentra organizada de manera sistemática para identificar los dispositivos instalados en cada área académica o administrativa. Los datos mostrados a continuación fueron proporcionados por gestión y administración de la red, a cargo de: Ing. Guadalupe Bermúdez, responsable de la infraestructura de red de la Facultad Multidisciplinaria Oriental.

N	EQUIPO	UBICACION	MARCA	IP	MODELO	NUMERO DE SERIE
1	EDUCACIÓN	EDUCACIÓN	HUAWEI	192.168.10.X	S1720-52GWR-4X	21980106112SK5600010
1	Computo UESED	Cómputo UESED	HUAWEI	192.168.10.X	S1720-52GWR-4X	21980106112SK5600056
2	Servicios Al Publico	Servicios Al Publico	DAHUA	192.168.10.X	DH-S5600-48GT4XF	219801A2A59242Q0004C
3	Educación	Educación	HUAWEI	192.168.10.X	S1720-52GWR-4X	21980106112SK5600010
4	Académica	Académica	HUAWEI	192.168.10.X	S1720-52GWR-4X	21980106112SK5600081
5	Aulas Economía	Aulas Economía	CISCO	192.168.10.X	SF200-24	-
6	Economía	Economía	HUAWEI	192.168.10.X	S6730-H48X6C	-
7	Matemática	Matemática	HUAWEI	192.168.10.X	S6730-H48X6C	21980106112SK5600072
8	Agronomía	Agronomía	HUAWEI	192.168.10.X	S6730-H48X6C	21980106112SK5600042
9	Biología	Biología	CISCO	192.168.10.X	WS-C2960X-48TS-L	-
10	Postgrados	Postgrados	HUAWEI	192.168.10.X	S5735-L48T4X-A	21980109364ELC008861
12	Medicina	Medicina	HUAWEI	192.168.10.X	S1720-52GWR-4X	21980106112SK5600042

13	Bodega	Bodega	CISCO	192.168.10.X	SG350-10	-
14	CDI	CDI	CISCO	192.168.10.X	SF200-24	DNI204002CC
15	CC. Juridicas	CC. juridicas	HUAWEI	192.168.10.X	S1720-52GWR-4X	21980106112SK5600072
16	Residencia 2	Residencia 2	CISCO	192.168.10.X	SF200-24	DNI2040026P
17	Financiera	Financiera	DAHUA	192.168.10.X		219801A2A59242Q0000D
18	Química	Química	HUAWEI	192.168.10.X	S1720-52GWR-4X	21980106112SK5600025
19	Computo Redes 1	Computo Redes 1	CISCO	192.168.10.X	SF200-24	DNI22110F39
20	INGENIERÍA	INGENIERÍA	HUAWEI	192.168.10.X	S1720-52GWR-4X	21980106112SK5600004
21	Cómputo Redes 2	Cómputo Redes 2	CISCO	192.168.10.X	SF200-24	DNI22110F5E
22	Cómputo Redes 3	Cómputo Redes 3	CISCO	192.168.10.X	SF200-24	PSZ21471MLU
23	Residencia	Residencia	DLINK	192.168.10.X	SG350-10	PSZ21471MMO
24	UESED	OFICINA UESED	CISCO	192.168.10.X	DE-1210	F3XZ4FC001381
25	Financiera 2	Financiera 2	CISCO	192.168.10.X	SF200-24	DNI223405HG
26	Edificio Minerva	Edificio Minerva	HUAWEI	192.168.10.X	S1720-52GWR-4X	21980106112SK5600074
27	Sala De Internet	Sala De Internet	CISCO	192.168.10.X	SF200-24	DNI204302BG
28	Vigilancia Estacionamiento	Vigilancia Estacionamiento	CISCO	192.168.10.X	SF200-24	DNI223405HN
29	Aulas Ingles	Aulas Ingles	HUAWEI	192.168.10.X	S5735-L24T4X-A	
30	Aulas Educación	Aulas Educación	HUAWEI	192.168.10.X	S5735-L24T4X-A	2S2180007714
31	Aulas De Ingeniería	Aulas De Ingeniería	HUAWEI	192.168.10.X	S5735-L24T4X-A	2S2180007811
32	Aulas Agronomía	Aulas Agronomía	HUAWEI	192.168.10.X	S5735-L24T4X-A1	2S2180007728
33	Simulación Y Audiencias	Simulación Y Audiencias	HUAWEI	192.168.10.X	S5735-L48T4X-A	21980109364ELC008861
34	Sociología	Sociología	TP-LINK	192.168.10.X	TL-SG3452P	Y227022000412
35	Edificio Minerva Pantallas 1	Edificio Minerva	HUAWEI	192.168.10.X	S5731-S24P4X	-
36	Edificio Minerva Pantallas 2	EDIFICIO MINERVA	HUAWEI	192.168.10.X	S5731-S24P4X	-
37	Ciencias Juridicas	Aula Ccjj	Huawei	192.168.10.X	S5731-S24P4X	DM22B0020628

	Pantallas					
38	Aulas Sociologia Pantallas	Aula Sociología	Huawei	192.168.10.X	S5731-S24P4X	102285825322
39	Vigilancia Entrada	Caseta Vigilancia Entrada	Tp-Link	192.168.10.X	TL-SG3452P	Y2270A5000027

Tabla 16: Inventario de switches de la FMO

5.3 Distribución Lógica Actual Red De La FMO UES

Se presenta la distribución lógica actual de la red de la FMO-UES, en la cual se detallan las VLAN configuradas para cada área o servicio institucional. La información se organiza en columnas que muestran el nombre asignado a la VLAN, su identificador (ID-VLAN), la dirección de red y la máscara correspondiente. Este registro permite visualizar de manera estructurada la segmentación de la red, diferenciando entre VLAN destinadas a facultades, servicios administrativos, laboratorios, sistemas especializados y redes inalámbricas.

N.º	NOMBRE VLAN	ID-VLAN	VLAN	MÁSCARA
1	WIFI	1101	172.16.0.1	/20
2	ADMINISTRATIVOS	1102	192.168.30.1	/24
3	UESED	1103	192.168.8.1	/24
4	COMPUTO	1104	192.168.60.1	/24
5	AGRONOMÍA	1105	192.168.9.1	/24
6	ADMINISTRACIÓN	1106	192.168.10.1	/24
7	SERVIDORES	1107	192.168.7.1	/24
8	BIBLIOTECA	1108	192.168.11.1	/24
9	ACADÉMICA	1109	192.168.12.1	/24
10	POSTGRADO	1110	192.168.13.1	/24
11	SALA-INTERNET	1111	192.168.14.1	/24
12	ECONOMÍA	1112	192.168.15.1	/24
13	CCNN	1113	192.168.16.1	/24
14	MEDICINA	1114	192.168.17.1	/24
15	CCJJ	1115	192.168.18.1	/24
16	QUÍMICA	1116	192.168.19.1	/24

17	HUMANIDADES	1117	192.168.20.1	/24
18	INGENIERÍA	1118	192.168.21.1	/24
19	CÁMARAS	1119	192.168.22.1	/24
20	TELEFONÍA IP	1120	192.168.23.1	/24
21	AUDIOVISUALES	1121	192.168.24.1	/24
22	WIFI2	1122	172.16.1.1	/20
23	WIFI6	1123	IP PLAN	

Tabla 17: Distribución actual de Vlans en la FMO

5.4 Detalle de la telefonía IP de la FMO

Se presenta el detalle de la telefonía IP en la FMO-UES**,** con información relacionada a la ubicación de los equipos, extensiones, direcciones IP y, en algunos casos, los switches a los que se encuentran conectados. No obstante, se identifican algunos registros incompletos o con datos faltantes**,** lo cual sugiere la necesidad de una futura actualización del inventario para mantener la información más homogénea y precisa.

N.º	EQUIPO	UBICACIÓN	EXTENSIÓN	DIRECCIÓN IP	SWITCH
1	TELEFONO IP	SECRETARÍA DECANATO	9201	192.168.23.2	
2	TELEFONO IP	PLANIFICACIÓN	9202	192.168.23.3	
3	TELEFONO IP	POSGRADO	9203	192.168.23.4	
4	TELEFONO IP	PLANIFICACIÓN	9204	192.168.23.5	
5	TELEFONO IP	BIBLIOTECA	9205	192.168.23.6	
6	TELEFONO IP	SECRETARÍA VICEDECANATO	9206	192.168.23.7	
7	TELEFONO IP		9207	192.168.23.8	
8	TELEFONO IP	DECANATO	9208	192.168.23.9	
9	TELEFONO IP		9209	192.168.23.10	
10	TELEFONO IP		9210	192.168.23.11	
11	TELEFONO IP	PROCESOS TÉCNICOS BIBLIO 1	9211	192.168.23.12	192.168.10.8

12	TELEFONO IP	HEMEROTECA BIBLIO 2	9212	192.168.23.13	192.168.10.8
13	TELEFONO IP	BIBLIO 3	9213	192.168.23.14	192.168.10.8
14	TELEFONO IP	BIBLIO 4	9214	192.168.23.15	192.168.10.8
15	TELEFONO IP	BIBLIO 5	9215	192.168.23.16	192.168.10.8
16	TELEFONO IP		9216	192.168.23.17	
17	TELEFONO IP		9217	192.168.23.18	
18	TELEFONO IP			192.168.23.19	
19	TELEFONO IP		9219	192.168.23.20	
20	TELEFONO IP	FINANCIERA	9220	192.168.23.21	
21	TELEFONO IP	COLECTURÍA	9221	192.168.23.22	
22	TELEFONO IP	PROYECCIÓN SOCIAL	9222	192.168.23.23	
23	TELEFONO IP	DESARROLLO FÍSICO	9223	192.168.23.24	
24	TELEFONO IP	FINANCIERA	9224	192.168.23.25	
25	TELEFONO IP	FINANCIERA	9225	192.168.23.26	
26	TELEFONO IP		9226	192.168.23.27	
27	TELEFONO IP		9227	192.168.23.28	
28	TELEFONO IP		9228	192.168.23.29	
29	TELEFONO IP		9229	192.168.23.30	
30	TELEFONO IP	ADMINISTRACIÓN ACADÉMICA 1	9230	192.168.23.31	172.19.29.14
31	TELEFONO IP	ADMINISTRACIÓN ACADÉMICA 2	9231	192.168.23.32	172.19.29.14
32	TELEFONO IP	ADMINISTRACIÓN ACADÉMICA 3	9232	192.168.23.33	172.19.29.14
33	TELEFONO IP	ADMINISTRACIÓN ACADÉMICA 4	9233	192.168.23.34	172.19.29.14
34	TELEFONO IP	ADMINISTRACIÓN ACADÉMICA 5	9234	192.168.23.35	172.19.29.14
35	TELEFONO IP	ADMINISTRACIÓN ACADÉMICA 6	9235	192.168.23.36	172.19.29.14
36	TELEFONO IP	ADMINISTRACIÓ	9236	192.168.23.37	172.19.29.14

		N ACADÉMICA 7			
37	TELEFONO IP	ADMINISTRACIÓN ACADÉMICA 8	9237	192.168.23.38	172.19.29.14
38	TELEFONO IP	ADMINISTRACIÓN ACADÉMICA 9	9238	192.168.23.39	172.19.29.14
39	TELEFONO IP	ADMINISTRACIÓN ACADÉMICA 10	9239	192.168.23.40	172.19.29.14
40	TELEFONO IP	RECURSOS HUMANOS	9240	192.168.23.41	
41	TELEFONO IP		9241	192.168.23.42	
42	TELEFONO IP		9242	192.168.23.43	
43	TELEFONO IP		9243	192.168.23.44	
44	TELEFONO IP		9244	192.168.23.45	
45	TELEFONO IP	AGRONOMÍA	9245	192.168.23.46	
46			9246		
47			9247		
65		UNIDAD DE ESTUDIOS SOCIO	9265		
70		ADMINISTRACIÓN GENERAL	9270		
71		MATEMÁTICA	9271		
75		MEDICINA – ASISTENTE	9275		
80		SISTEMAS INFORMÁTICOS	9280		
91		INGENIERÍA Y ARQUITECTURA	9291		
92		CIENCIAS JURÍDICAS	9292		

Tabla 18: Detalle de la telefonía IP de la FMO

5.5 Diagrama de red del estado actual de la FMO

En el siguiente diagrama de red se muestra el estado actual de la FMO-UES, en el cual se representan los enlaces que conectan los diferentes edificios, departamentos y dependencias académicas y administrativas. Este esquema ofrece una visión general de la topología de la red y de la forma en que se organiza la infraestructura de comunicaciones de la institución.

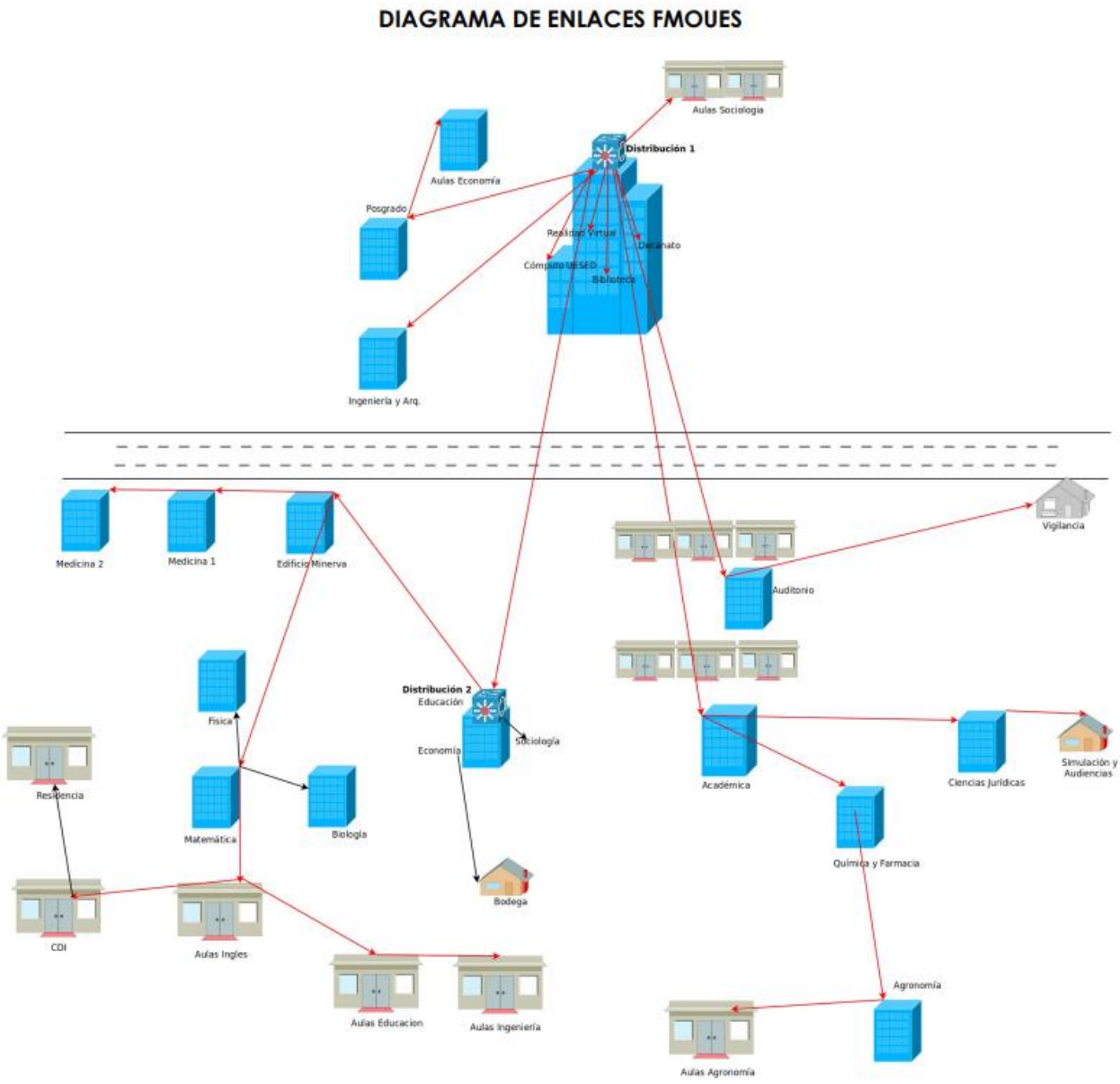

Figura 13: Diagrama de red des estado actual de la FMO

5.6 Diagrama de distribución de switches por marca de la FMO

El diagrama de distribución de switches por marca en la FMO muestra la organización de la infraestructura de red de la Facultad Multidisciplinaria Oriental, destacando las diferentes marcas de equipos que se encuentran instalados en las distintas áreas. En la parte superior se ubica el switch de núcleo (CORE), que concentra la conectividad principal y la distribuye hacia los diferentes edificios y dependencias. Desde este núcleo parten enlaces hacia los servidores y la telefonía, además de dos grandes ramas de distribución que abarcan tanto áreas académicas como administrativas.

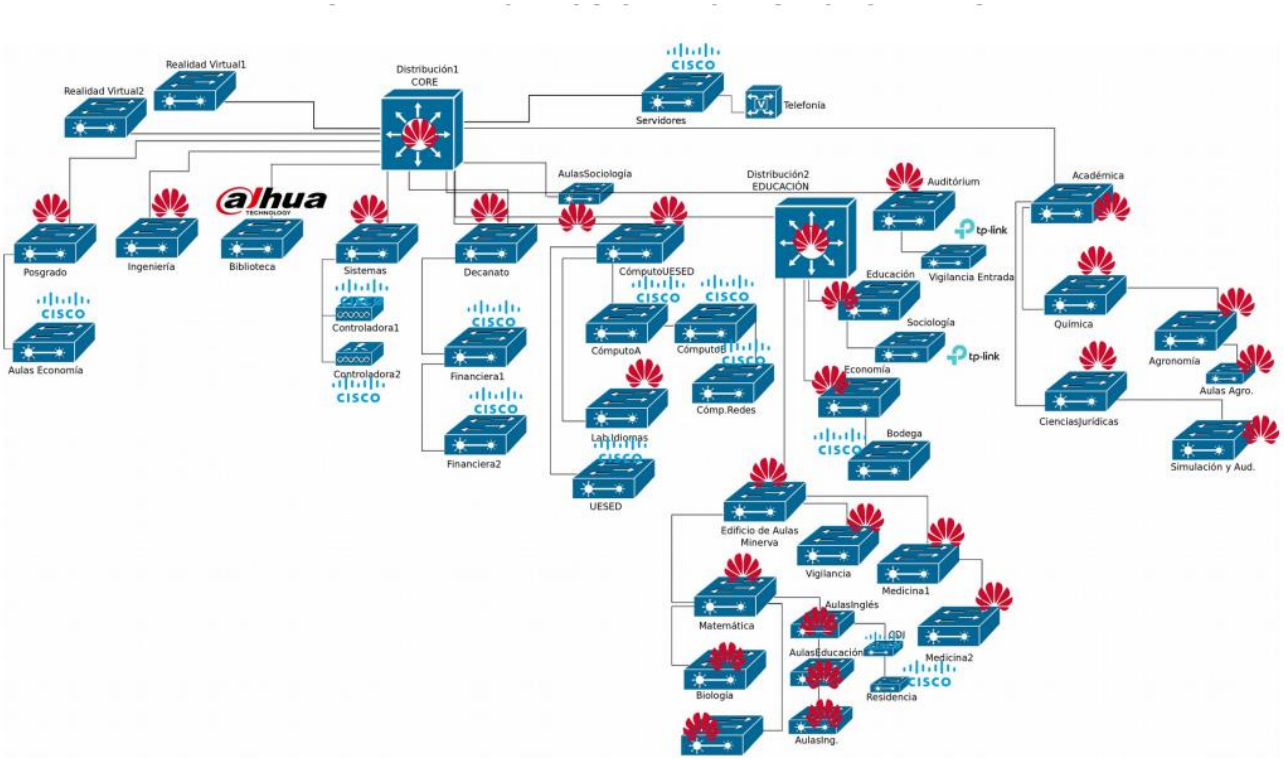

Figura 14: Diagrama de distribución por marcas

5.7 Diagrama enlaces principales de la FMO

El diagrama muestra los enlaces principales de la red de la FMO-UES, donde se representan las conexiones establecidas entre el proveedor de servicios de internet, los dispositivos de seguridad, los equipos de enrutamiento y los switches de núcleo y distribución. El esquema permite visualizar de manera general la estructura de interconexión que sostiene la red institucional en su capa principal.

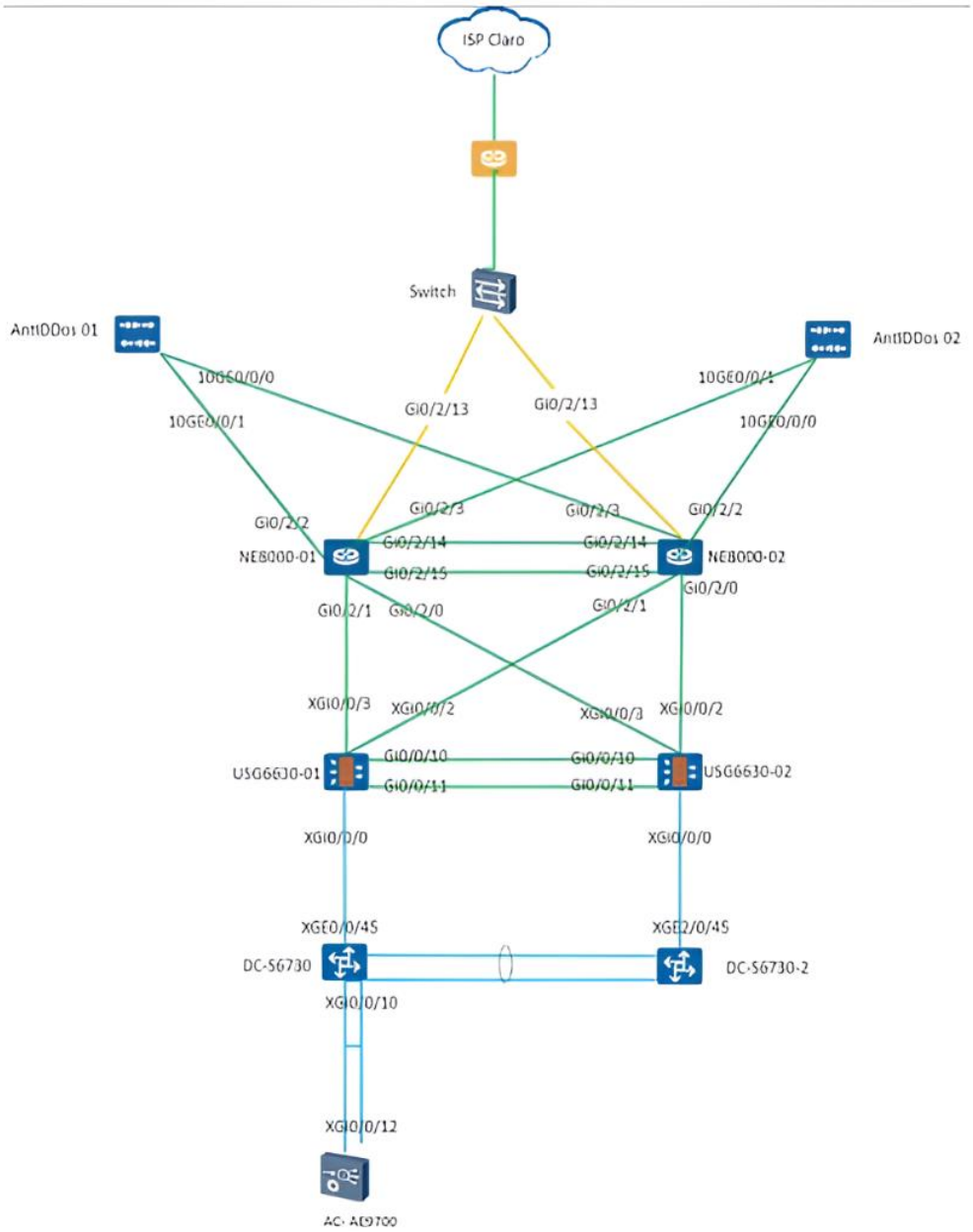

Figura 15: Diagrama de enlaces principales de la FMO

Parte II

6. Propuesta de Red Tipo Campus

6.1 Propuesta de enlaces para la Facultad Multidisciplinaria Oriental

Se presenta la propuesta de enlaces de red para la Facultad Multidisciplinaria Oriental (FMO-UES), la cual se estructura bajo el modelo jerárquico de tres capas: núcleo, distribución y acceso. Este enfoque responde a las necesidades de crecimiento, estabilidad y seguridad de la red institucional, organizando de manera lógica la interconexión de edificios, laboratorios, unidades académicas y áreas administrativas. A diferencia del diseño previo, donde la red presentaba una topología más dispersa y con limitaciones en su administración, la propuesta establece un esquema más claro, eficiente y preparado para la expansión futura.

Las ventajas principales de este diseño pueden resumirse en los siguientes aspectos:

1. **Organización estructural:** al adoptar la división en capas, se facilita la identificación de funciones específicas (enrutamiento, distribución de tráfico y acceso), lo que simplifica el mantenimiento y la administración de la red.
2. **Escalabilidad garantizada:** el modelo permite integrar nuevas áreas, servicios o tecnologías sin comprometer la estabilidad de la infraestructura existente.
3. **Mayor redundancia y continuidad operativa:** se reduce la dependencia de un único punto de fallo, incrementando la disponibilidad de los servicios y la confiabilidad de la red.
4. **Optimización del tráfico de datos:** la segmentación lógica de la red mejora la velocidad de respuesta, distribuye la carga de manera más eficiente y favorece el uso de recursos tecnológicos de forma equilibrada.
5. **Seguridad reforzada:** el diseño jerárquico posibilita la implementación de políticas de control en puntos estratégicos, protegiendo la red frente a accesos indebidos o vulnerabilidades.
6. **Facilidad de gestión:** la administración centralizada de los equipos se vuelve más ágil, reduciendo tiempos de respuesta en caso de incidencias y facilitando la labor del personal técnico.
7. **Adaptación a estándares internacionales:** al alinearse con las mejores prácticas de diseño de redes institucionales, se garantiza compatibilidad con futuras tecnologías y normativas.

En este contexto, la propuesta no solo moderniza la infraestructura actual, sino que también establece las bases para una red universitaria robusta, confiable y preparada para el futuro, convirtiéndose en una alternativa superior frente al esquema previo y aportando un valor estratégico a la gestión tecnológica de la FMO-UES.

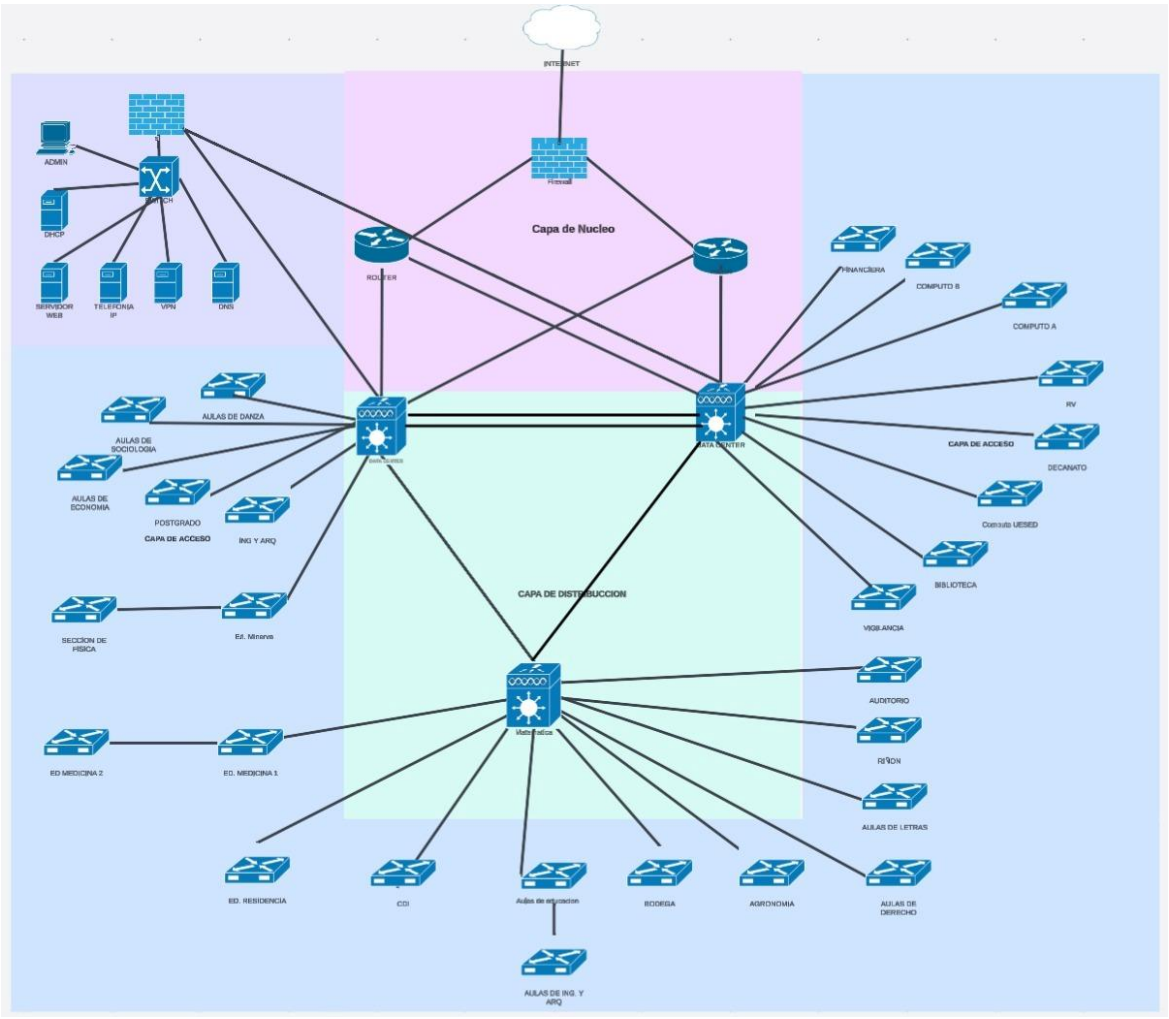

Figura 16: Diagrama de la propuesta de red

6.2 Lista de Equipos usados para la topología en GNS3

En la siguiente tabla presenta el inventario de los equipos y servicios empleados para la demostración práctica realizada en GNS3, donde se virtualizó la infraestructura de red institucional con fines académicos y de exposición. En este entorno se configuraron servidores críticos (DHCP, DNS, web, telefonía IP y VPN), dispositivos de seguridad (FortiGate), routers (Cisco y MikroTik) y switches de capa 2, además de clientes ligeros para pruebas de conectividad. Esta simulación permitió recrear de manera fiel la operación de la red de la FMO-UES, mostrando su funcionamiento en un escenario controlado y didáctico para la presentación.

ID	NOMBRE DEL EQUIPO	DISPOSITIVO	SISTEMA OPRATIVO/VERSION	DESCRIPCION	CANTIDAD	UBICACIÓN
1	Servidor DHCP	Máquina Virtual	Debian 13, GNU/Linux 13 (trixie)	Asignación automática de direcciones IP a los clientes de la red	1	Centro de datos
2	Dns-vm-1	Máquina virtual	Debian 13, GNU/Linux 13 (trixie)	Resolución de nombres de dominio, traduce direcciones web en direcciones IP.	1	Centro de datos
3	Asterisk	Máquina Virtual	Asterisk 18.16.0	Plataforma de telefonía IP (VoIP) para comunicación	1	Centro de datos
4	Fedora VPN	Servidor VPN	Fedora 17	Permitir conexiones remotas seguras de usuarios externos hacia la red.	1	Centro de datos
5	Servidor web	Máquina Virtual	Debian 13, GNU/Linux 13 (trixie)	Alojamiento de aplicaciones y páginas institucionales	1	Centro de datos
6	Router CISCO	CISCO C725	Cisco IOS Version 12.4(15)T14,	Enrutamiento principal de la red, conexión entre VLANs y hacia internet.	2	Centro de datos
7	FIREWALL	FORTIGATE 7.0.9 QEMU	FortiGate-VM64-KVM v7.0.9,build0444,	filtrado de tráfico y seguridad perimetral de la red.	1	Centro de datos
8	Microtik	Microtik QEMU	RouterOS version: 7.8 (stable)	Enrutamiento y control de tráfico en	3	Capa de distribución

				la capa de distribución.		
9	Conmutador L2	Cisco QEMU L2-adventerprisek9-m. 03.2017.qcow2	Cisco IOS version 15.2	Conmutación de nivel 2, interconexión de equipos en la red local.	4	Capa de Acesso
10	Puppy_linux	Puppy Linux Qemu	Versión 9.6	Escritorio de usuario	1	Área de trabajo

Tabla 19: Lista de equipos usados en la topología GNS3

6.3 Propuesta de segmentación VLANS de la FMO

Se presenta la propuesta de segmentación de VLANs para la red de la FMO-UES, donde se asignan subredes específicas a las distintas áreas académicas, administrativas y de servicios. En cada registro se detallan el nombre de la VLAN, el identificador (ID), el número de hosts soportados, la notación CIDR correspondiente, así como la red y el rango de direcciones utilizables. Esta planificación responde a la necesidad de contar con un direccionamiento más eficiente, ordenado y seguro dentro de la infraestructura institucional.

Entre las ventajas principales de la propuesta se destacan:

- **Optimización del direccionamiento IP:** al definir rangos precisos para cada VLAN se evita el desperdicio de direcciones y se aprovecha mejor el espacio disponible.
- **Reducción de dominios de broadcast:** cada área cuenta con su propia subred, disminuyendo la saturación de la red y mejorando el rendimiento general.
- **Mayor seguridad y control:** la segmentación permite aplicar políticas de filtrado, ACLs y controles específicos según el departamento o servicio.
- **Escalabilidad:** la asignación por subredes facilita el crecimiento de la red y la incorporación de nuevos equipos o servicios sin afectar la estructura existente.
- **Gestión centralizada y organizada:** la documentación clara de rangos IP y VLANs simplifica las tareas de administración y resolución de incidencias.
- **Separación lógica de servicios críticos:** VLANs especiales para servidores, cámaras, telefonía IP o audiovisuales aseguran que estos sistemas operen de manera estable y con menor riesgo de interferencia.

- **Mejores prácticas institucionales:** el diseño propuesto se alinea con estándares de ingeniería de redes utilizados en campus universitarios modernos.

En este sentido, la segmentación propuesta constituye una mejora significativa frente al esquema anterior, al ofrecer una red más ordenada, segura, eficiente y preparada para la expansión futura de la FMO-UES.

N	**NOMBRE DE LA VLAN**	**ID VLAN**	**HOSTS**	**CIDR**	**RED**	**PRIMERA UTILIZABLE**	**ÚLTIMA UTILIZABLE**
1	ADMINISTRATIVOS	1010	62	/26	192.168.10.0	192.168.10.1	192.168.10.62
2	UESED	1011	64	/26	192.168.10.64	192.168.10.65	192.168.10.126
3	COMPUTO	1012	128	/25	192.168.10.128	192.168.10.129	192.168.10.254
4	AGRONOMÍA	1013	32	/27	192.168.11.0	192.168.11.1	192.168.11.30
5	ADMINISTRACIÓN	1014	32	/27	192.168.11.32	192.168.11.33	192.168.11.62
6	BIBLIOTECA	1015	32	/27	192.168.11.64	192.168.11.65	192.168.11.94
7	ACADÉMICA	1016	32	/27	192.168.11.96	192.168.11.97	192.168.11.126
8	POSTGRADO	1017	32	/27	192.168.11.128	192.168.11.129	192.168.11.158
9	SALA-INTERNET	1018	32	/27	192.168.11.160	192.168.11.161	192.168.11.190
10	ECONOMÍA	1019	64	/26	192.168.11.192	192.168.11.193	192.168.11.254
11	CCNN	1020	64	/26	192.168.12.0	192.168.12.1	192.168.12.62
12	MEDICINA	1021	128	/25	192.168.12.64	192.168.12.65	192.168.12.126
13	CCJJ	1022	64	/26	192.168.12.128	192.168.12.129	192.168.12.190
14	QUÍMICA	1023	64	/26	192.168.12.192	192.168.12.193	192.168.12.254
15	HUMANIDADES	1024	64	/26	192.168.13.0	192.168.13.1	192.168.13.62
16	INGENIERÍA	1025	64	/26	192.168.13.64	192.168.13.65	192.168.13.126
17	SERVIDORES	1126	32	/27	192.168.13.128	192.168.13.129	192.168.13.142
18	CAMARA	1127	128	/25	192.168.14.0	192.168.14.1	192.168.14.126
19	TELEFONÍA IP	1128	128	/25	192.168.14.128	192.168.14.129	192.168.14.254
20	AUDIOVISUALES	1129	16	/28	192.168.15.0	192.168.15.1	192.168.15.14

Tabla 20: Propuesta de segmentación de VLANS de la FMO

6.3.1 Propuesta de segmentación VLANS de Wifi por departamento

Se presenta la propuesta de segmentación de VLANs de WiFi por departamento en la FMO-UES, en la que se asignan rangos de direcciones IP independientes para cada departamento. En el registro se detalla el nombre de la VLAN, su identificador (ID), el número de hosts soportados, la notación CIDR utilizada, así como la red asignada y las direcciones IP utilizables. Esta propuesta permite organizar de forma eficiente el servicio inalámbrico, otorgando a cada área un espacio de red propio y controlado.

Entre las ventajas principales de esta segmentación se destacan:

- **Mejor administración del servicio WiFi**, al contar cada facultad con una VLAN dedicada.
- **Optimización del rendimiento**, ya que se reduce la congestión en un único dominio de broadcast.
- **Mayor seguridad y aislamiento**, al evitar que el tráfico de una facultad impacte en otra.
- **Escalabilidad garantizada**, permitiendo ampliar los rangos IP en caso de mayor demanda de usuarios.
- **Orden y trazabilidad**, lo que facilita identificar y resolver incidencias en puntos de acceso específicos.

De esta manera, la segmentación propuesta proporciona una infraestructura inalámbrica más robusta, organizada y alineada con las necesidades de conectividad de cada departamento.

N	NOMBRE DE LA VLAN	ID	HOSTS	CIDR	RED	PRIMERA UTILIZABLE	ÚLTIMA UTILIZABLE
1	WIFI	1200	2046	/21	192.168.30.0	192.168.30.1	192.168.37.254
2	Wifi_Medicina	1270	510	/23	192.168.38.0	192.168.38.1	192.168.39.254
3	Wifi_Agronomia	1210	254	/24	192.168.40.0	192.168.40.1	192.168.40.254
4	Wifi_Economia	1220	254	/24	192.168.41.0	192.168.41.1	192.168.41.254
5	Wifi_CN_Matematica	1230	254	/24	192.168.42.0	192.168.42.1	192.168.42.254
6	Wifi_Ciencias_Humanidades	1240	254	/24	192.168.43.0	192.168.43.1	192.168.43.254
7	Wifi_Arq_Ing	1250	254	/24	192.168.44.0	192.168.44.1	192.168.44.254
8	Wifi_Jurisprudencia_CS	1260	254	/24	192.168.45.0	192.168.45.1	192.168.45.254
9	Wifi_Quimica_Farmacia	1280	254	/24	192.168.46.0	192.168.46.1	192.168.46.254

Tabla 21: Segmentación de Vlans de Wifi por departamento

6.3.2 Propuesta de segmentación del área del centro de datos

Se presenta la propuesta de segmentación del área del centro de datos en la FMO-UES, donde se asignan direcciones IP específicas a los servidores críticos que soportan los servicios institucionales. En ella se incluyen el servidor web, DHCP, VoIP, VPN y DNS, cada uno con su dirección de red, máscara correspondiente y gateway común. Esta organización garantiza que los servicios esenciales del centro de datos cuenten con una asignación ordenada, controlada y homogénea de direcciones**,** lo que facilita su administración y refuerza la estabilidad operativa de la red.

DISPOSITIVO	DIRECCION DE RED	MASCARA	GATEWAY
Servidor Web	192.168.16.134	255.255.255.192	192.168.16.132
Servidor DHCP	192.168.16.135	255.255.255.192	192.168.16.132
Servidor Voip	192.168.16.136	255.255.255.192	192.168.16.132
Servidor VPN	192.168.16.137	255.255.255.192	192.168.16.132
Servidor DNS	192.168.16.138	255.255.255.192	192.168.16.132

Tabla 22: Propuesta de segmentación del centro de datos

6.3.3 Propuesta de direccionamiento de la red del

Se presenta la propuesta de direccionamiento para el centro de datos de la red de la FMO-UES, en la cual se definen las interfaces, direcciones de red, máscaras y gateways de los principales dispositivos que conforman la infraestructura. Se incluyen equipos como MikroTik, Fortigate y routers Cisco, organizados en diferentes segmentos y enlaces punto a punto para garantizar la correcta comunicación entre la capa de acceso, distribución y núcleo. Esta planificación permite establecer un esquema de direccionamiento claro y homogéneo, que facilita la administración de la red y asegura la conectividad entre los distintos servicios y VLANs.

DISPOSITIVO	INTERFAZ	DIRECCION DE RED	MASCARA DE RED	GATEWAY
Microtik	Bridge-LAN	192.168.16.132	255.255.255.192	192.168.16.132
Fortigate	Port1	192.168.137.2	255.255.255.0	-
	Port2	192.168.16.131	255.255.255.192	192.168.16.131
	Port3	10.0.0.2	255.255.255.252	10.0.0.1

	Port4	10.0.10.2	255.255.255.252	10.0.10.1
Router 1	Fa0/0	10.0.0.1	255.255.255.252	-
	Fa0/1	10.0.1.1	255.255.255.252	-
	Fa1/0	10.0.2.1	255.255.255.252	-
	Fa2/0	10.10.11.1	255.255.255.252	-
Router 2	Fa0/0	10.0.10.1	255.255.255.252	-
	Fa0/1	10.0.1.2	255.255.255.252	-
	Fa1/0	10.0.3.1	255.255.255.252	-
	Fa2/0	10.10.12.1	255.255.255.252	-
Microtik 1	Ether1	10.0.0.2	255.255.255.252	-
	Ether2	10.10.11.2	255.255.255.252	-
	Bond-mt1	10.0.4.1	255.255.255.252	-
Microtik 2	Ether1	10.0.10.2	255.255.255.252	-
	Ether2	10.10.12.2	255.255.255.252	-
	Bond-mt2	10.0.4.2	255.255.255.252	-

Tabla 23: Direccionamiento de la red

6.4 Materiales y tecnologías

6.4.1 Materiales

Se presenta los materiales adicionales propuestos para fortalecer la infraestructura de red de la FMO-UES, considerando que la universidad ya dispone de la mayoría de los equipos necesarios. En este listado se incluyen dispositivos estratégicos como un firewall Fortigate con soporte para servicios avanzados de seguridad y un switch Cisco SG200-26 de 24 puertos, los cuales contribuirán a optimizar la gestión del tráfico y reforzar la protección de la red. Estos materiales se detallan con su respectiva descripción técnica, cantidad requerida, proveedor y costo estimado, a fin de facilitar su adquisición e integración al diseño planteado

ID	NOMBRE	DESCRIPCION	CANTIDAD	PROVEEDOR	PRECIO	IMAGEN
1	Fortigate	Fortinet FortiGate-50G Firewall for Branch and Small Offices with 1-Year FortiGuard AI-Powered Unified Threat Protection Services (FG-50G-BDL-950-12) Enlace de compra: Fortinetfortigate 50g Firewall For Branch And Small Offices With 1 | Desertcart El Salvador	1	desertcart	$2,206.60	
2	Switch Cisco	El conmutador Cisco SG200-26 (SLM2024T-NA) es un conmutador inteligente Gigabit Ethernet asequible de 24 puertos, que incluye dos puertos mini-GBIC **Enlace de compra:** Switch Cisco SG200-26 Gigabit Ethernet Smart Switch 10/100/1000 | Grupo Servitech | Soluciones Informáticas y Tecnológicas de El Salvador	1	Servitech	$352.00	

Tabla 24: Materiales para la instalación

En La siguiente tabla se presenta los equipos de red considerados como alternativas al firewall FortiGate, detallando sus características técnicas, cantidad requerida, proveedor sugerido y precio estimado. Se incluyen dos dispositivos principales:

ID	NOMBRE	DESCRIPCIÓN	CANTIDAD	PROVEEDOR	PRECIO	IMAGEN
1	**Cisco Firepower 1010**	Firewall de próxima generación, 8 Gbps, soporte para VPN, IPS, inspección de aplicaciones, filtrado web. Enlace de compra: https://a.co/d/ceVP7P6	1	Cisco Partner	$1,950.00 aprox.	
2	**MikroTik CCR2004-1G-12S+2XS**	Router/firewall de alto rendimiento, 12 puertos SFP+, throughput hasta 10 Gbps, soporte de VPN y reglas dinámicas. **Enlace de compra:** MikroTik Routers and Wireless - Products: CCR2004-1G-12S+2XS	1	MikroTik / Servitech	$850.00 aprox.	

Tabla 25: Materiales para instalación alternativos a Fortigate

La tabla muestra dos alternativas de switches administrables de 24 puertos de diferentes marcas. Se compara un modelo de Cisco con un precio aproximado de $380.00 y otro de TP-Link con un costo de $290.00, ofreciendo así opciones de distinta marca y presupuesto para la instalación.

ID	NOMBRE	DESCRIPCIÓN	CANTIDAD	PROVEEDOR	PRECIO	IMAGEN
4	**Cisco CBS250-24T-4G**	Switch administrable, 24 puertos Gigabit + 4 uplinks SFP, VLANs, QoS, ACLs, administración web/CLI. **Enlace de compra** https://a.co/d/5x3lnei	1	Cisco Partner	$380.00 aprox.	

5	**TP-Link JetStream T1600G-28TS**	TP-LINK T2700G-28TQ Jetstream Conmutador administrado Gigabit apilable L2+ de 28 puertos Enlace de compra: https://a.co/d/58GQR9I	1	TP-Link	$228.00 aprox.	

Tabla 26: Materiales para instalación alternativos a Switch

6.4.1 Justificación

6.4.1.1 Justificación Técnica

La Facultad Multidisciplinaria Oriental de la Universidad de El Salvador cuenta actualmente con una infraestructura de red y equipamiento tecnológico que han permitido el desarrollo de actividades académicas y administrativas de forma efectiva. Sin embargo, a partir de la investigación realizada, se identificaron áreas de mejora necesarias para responder al crecimiento de la comunidad universitaria y a la demanda de servicios digitales cada vez más robustos y seguros.

Entre los principales retos detectados se encuentran: limitaciones en la segmentación lógica de la red, falta de redundancia en algunos enlaces críticos, ausencia de una arquitectura jerárquica plenamente definida y carencias en políticas de seguridad informática que garanticen la confidencialidad, integridad y disponibilidad de la información institucional. Estos aspectos limitan la escalabilidad y la continuidad de los servicios tecnológicos frente a un entorno académico en constante expansión.

El proyecto plantea un rediseño basado en un modelo de red jerárquica de tres capas (acceso, distribución y núcleo), implementando segmentación lógica mediante VLANs, integración de servicios críticos (DNS, DHCP, VPN, VoIP y Web) y políticas de seguridad perimetral con autenticación centralizada. Esta propuesta permitirá optimizar el control del tráfico, mejorar la eficiencia y garantizar la disponibilidad de servicios bajo estándares de buenas prácticas.

Un factor diferenciador es la posibilidad de involucrar a estudiantes de la carrera de Ingeniería de Sistemas Informáticos en el desarrollo del proyecto, ya sea a través de horas sociales, prácticas profesionales o proyectos de aula. Esto no solo potencia su formación práctica, sino que permite a la institución contar con apoyo adicional en labores de implementación y monitoreo, fortaleciendo al mismo tiempo el vínculo entre academia y gestión tecnológica.

Finalmente, para garantizar la sostenibilidad del proyecto, se recomienda que al menos dos profesionales de la institución cuenten con certificaciones reconocidas internacionalmente (Cisco CCNA/CCNP, Fortinet NSE, Mikrotik MTCNA, entre otras), lo que asegurará la correcta administración de la red, el soporte a los servicios críticos y la gestión de la seguridad informática bajo altos estándares.

Perfiles técnicos sugeridos para la administración de la red

- **Administrador de Red 1 (Perfil de Infraestructura y Routing):**
  Profesional con certificación Cisco CCNA o CCNP, experiencia **en** diseño y gestión de redes LAN/Campus, conocimientos en enrutamiento dinámico (OSPF, EIGRP), administración de VLANs, configuración de switches de capa 2/3 y manejo de protocolos de redundancia (HSRP, VRRP, STP). Encargado del núcleo de la red y la conectividad con proveedores externos.
- **Administrador de Red 2 (Perfil de Seguridad y Servicios):**
  Profesional con certificación Fortinet NSE o Mikrotik MTCNA, con competencias en firewalls perimetrales, políticas de seguridad, segmentación lógica, VPN, servidores DNS/DHCP y VoIP. Encargado de la gestión de seguridad, monitoreo de accesos, soporte a usuarios y administración de los servicios críticos que soporta la red institucional.

6.4.1.2 Justificación Económica

La Universidad de El Salvador, a través de la Facultad Multidisciplinaria Oriental (FMO-UES), ya dispone de un presupuesto institucional respaldado por la Ley de Presupuesto de la Nación, el cual contempla partidas específicas para el fortalecimiento de la infraestructura tecnológica y la modernización institucional. Este soporte financiero constituye la base para garantizar la factibilidad del proyecto y respalda la adquisición de equipos, servicios y materiales contemplados en la propuesta.

El análisis costo–beneficio demuestra que la inversión en equipos de red de nivel empresarial (firewalls Fortinet, switches gestionables L2/L3, routers de núcleo, controladores inalámbricos y servidores) es una decisión estratégica, dado que proporcionan alta disponibilidad, redundancia y seguridad perimetral, garantizando la continuidad de los procesos académicos y administrativos. Además, los costos de implementación se compensan con la reducción de incidencias críticas en la red, la disminución de pérdidas por caídas de servicios y el aprovechamiento de licenciamientos centralizados.

Asimismo, se contemplan alternativas de equipos (Tablas 25 y 26), lo que otorga flexibilidad económica y asegura la viabilidad del proyecto frente a posibles variaciones del mercado tecnológico.

En términos de sostenibilidad financiera, la justificación se fortalece considerando que:

- La segmentación lógica mediante VLANs optimizará el uso del hardware existente, reduciendo la necesidad de nuevas adquisiciones en el mediano plazo.
- La propuesta incluye la incorporación de servicios críticos (DNS, DHCP, VoIP, VPN y Web), lo que permitirá disminuir los costos asociados a hardware físico y facilitar la escalabilidad futura.
- La arquitectura jerárquica de tres capas (acceso, distribución y núcleo) estandariza la gestión de la red, reduciendo gastos operativos y minimizando los tiempos de mantenimiento correctivo.
- Los mecanismos de redundancia (OSPF, enlaces troncales y firewalls en alta disponibilidad) asegurarán la continuidad de los servicios críticos, evitando pérdidas de productividad académica y administrativa.

Un elemento adicional de relevancia es la participación de estudiantes de Ingeniería de Sistemas en horas sociales, prácticas profesionales o proyectos de aula, lo cual representa un apoyo significativo en la fase de implementación y monitoreo de la red. Esta estrategia no solo fortalece la formación académica de los estudiantes, sino que también se traduce en un ahorro de costos operativos para la institución, al reducir la dependencia de servicios externos.

En consecuencia, el proyecto es económicamente viable con base en el presupuesto institucional y, además, constituye una inversión estratégica de alto impacto para la FMO-UES, ya que no solo moderniza su infraestructura tecnológica, sino que también garantiza eficiencia, confiabilidad y sostenibilidad a largo plazo.

6.4.2 Tecnologías

En esta sección se describen las tecnologías utilizadas en la simulación del proyecto dentro del entorno GNS3, las cuales permitieron recrear de manera práctica y controlada la infraestructura de red propuesta para la FMO-UES. Se seleccionaron imágenes y software de fabricantes reconocidos como Cisco, MikroTik, Fortinet y sistemas basados en GNU/Linux (Debian, Fedora, entre otros), con el objetivo de emular el comportamiento de los equipos físicos presentes en un entorno de producción gracias a la facilidad, versatilidad y la compatibilidad de las imágenes de virtualización con sistemas operativos de código abierto como las distribuciones de Linux.

La utilización de estas tecnologías en GNS3 permitió probar la segmentación en VLANs, la asignación de direccionamiento IP, la configuración de servicios críticos (DNS, DHCP, VPN, VoIP y Web) y las políticas de seguridad perimetral, todo ello sin necesidad de recurrir a hardware físico. De esta forma, la simulación proporcionó un laboratorio virtual robusto, en el que se validó la factibilidad y el correcto funcionamiento del diseño de red antes de su implementación real.

6.4.2.1 Router Cisco 7200

El Cisco 7200 Series es una línea de routers modulares de alto rendimiento diseñados para entornos de red empresariales y proveedores de servicios. Ofrecen capacidades avanzadas de enrutamiento, seguridad y servicios integrados, con soporte para múltiples interfaces WAN y LAN. La serie incluye modelos como el Cisco 7204VXR y el Cisco 7206VXR, que permiten una amplia variedad de configuraciones y actualizaciones para adaptarse a las necesidades específicas de cada implementación. [25]

6.4.2.2 Justificación de por qué se usó el router Cisco 7200

El Cisco 7200 Series se seleccionó por su alto rendimiento y flexibilidad, lo que lo hace ideal para redes universitarias o empresariales con múltiples servicios. Su arquitectura modular permite adaptar interfaces WAN/LAN, soportar enrutamiento avanzado, VPNs, seguridad integrada y QoS, y escalar según la demanda de tráfico. Además, su reputación de fiabilidad y estabilidad garantiza que los servicios críticos (correo, servidores, plataformas educativas) permanezcan disponibles, minimizando interrupciones. Por estas características, es un equipo adecuado para consolidar la red y manejar la conectividad de forma segura y eficiente.

6.4.2.3 Fortigate 7.0.9

FortiGate es una familia de firewalls de nueva generación (NGFW) desarrollados por la empresa Fortinet. Estos dispositivos combinan funciones clásicas de firewall con servicios avanzados de seguridad como inspección profunda de paquetes (DPI), prevención de intrusiones (IPS), filtrado web, control de aplicaciones, protección contra malware y gestión de VPNs. Se utilizan en redes empresariales y de campus porque permiten centralizar la seguridad, segmentar VLANs y garantizar que el tráfico entre usuarios, servidores e internet esté protegido. [26]

6.4.2.4 Justificación de por qué se usó Fortigate 7.0.9

La elección de FortiGate 7.0.9 en la implementación de la red se justifica por varios factores técnicos y de seguridad. En primer lugar, FortiGate es un firewall de nueva generación (NGFW) que permite no solo el filtrado tradicional de paquetes, sino también la inspección profunda de tráfico (DPI), la gestión de VPNs seguras y la integración con sistemas de prevención de intrusiones (IPS). Esto resulta indispensable para una red de tipo campus, donde coexisten múltiples VLANs y servicios críticos que requieren segmentación y protección confiable.

La versión 7.0.9 fue seleccionada debido a su estabilidad comprobada y soporte extendido por parte de Fortinet, garantizando compatibilidad con las últimas actualizaciones de seguridad y parches. Además, esta versión

ofrece mejoras en rendimiento y administración frente a versiones anteriores, optimizando el manejo de tráfico en entornos de alta densidad de usuarios.

Otro aspecto fundamental es la facilidad de integración con equipos de distintos fabricantes (como MikroTik, Cisco o servidores Debian), lo cual se adapta a la heterogeneidad de nuestra red. Asimismo, FortiGate 7.0.9 incorpora un sistema de políticas centralizadas que facilita la aplicación de reglas de seguridad de manera uniforme en todas las VLANs y subredes, reduciendo riesgos de configuración manual y errores humanos.

6.4.2.5 Cisco IOSvL2

Cisco IOSvL2 es una imagen virtual del sistema operativo IOS de Cisco, diseñada para emular un switch de capa 2 dentro de entornos virtualizados como GNS3, EVE-NG o VMware.

Con IOSvL2 se pueden realizar prácticas de configuración de redes en switching, incluyendo:

- Creación y gestión de VLANs.
- Configuración de troncales 802.1Q.
- Implementación de Spanning Tree Protocol (STP).
- Configuración de EtherChannel.
- Pruebas de conectividad en laboratorios de simulación.

Es muy utilizado en el ámbito académico y profesional porque permite replicar el comportamiento de switches Cisco reales, sin necesidad de contar con hardware físico, lo que facilita el aprendizaje.

6.4.2.6 Justificación de por qué se usó Cisco IOSvL2

La inclusión de Cisco IOSvL2 en el diseño de la red responde a la necesidad de contar con una plataforma de simulación confiable y flexible para la implementación de funciones de conmutación de capa 2. Este software, desarrollado por Cisco, permite emular un switch con funcionalidades completas de switching, incluyendo creación y administración de VLANs, configuración de enlaces troncales (802.1Q).
La principal justificación para su uso radica en que IOSvL2 posibilita replicar el comportamiento de un switch físico Cisco dentro de entornos virtualizados como GNS3 o EVE-NG, reduciendo significativamente los costos de adquisición de hardware y proporcionando flexibilidad para pruebas y escenarios de laboratorio. Esto es especialmente útil en una red de tipo campus, donde la segmentación en múltiples VLANs y la administración centralizada de enlaces resultan fundamentales.

6.4.2.7 Mikrotik

Mikrotik es una empresa letona fundada en 1996 para desarrollar enrutadores y sistemas ISP inalámbricos. MikroTik proporciona hardware y software para la conectividad a Internet en la mayoría de los países del mundo. [27]

6.4.2.8 Justificación de por qué se usó Mikrotik

La implementación de MikroTik dentro de la red se justifica principalmente por su versatilidad, bajo costo y amplia gama de funcionalidades avanzadas, que permiten cubrir múltiples necesidades sin requerir hardware adicional. A través de su sistema operativo RouterOS, es posible habilitar servicios de ruteo dinámico (OSPF, BGP, RIP), segmentación de tráfico mediante VLANs, gestión de firewall, NAT y servidores integrados de DHCP y DNS, así como la creación de túneles VPN para asegurar la comunicación entre diferentes segmentos de la red.

Una de las razones clave para su elección es que MikroTik ofrece una relación costo-beneficio muy favorable, en comparación con otros fabricantes de equipos de red. Esto facilita contar con dispositivos de alto rendimiento para laboratorios académicos, pruebas en entornos virtualizados y despliegues en campo, sin necesidad de una gran inversión. Asimismo, su software es altamente configurable y flexible, lo que permite adaptarlo a redes pequeñas, medianas y complejas, como las de tipo campus.

Otro factor relevante es su capacidad de interoperabilidad con otros equipos de distintos fabricantes (Cisco, Fortinet, servidores Linux/Debian, etc.), lo cual garantiza una integración adecuada en entornos heterogéneos. Además, MikroTik es una herramienta muy utilizada en la formación profesional de ingenieros en redes, dado que permite realizar prácticas de configuración y administración reales, preparando a los estudiantes para escenarios de producción.

En conclusión, el uso de MikroTik en la red aporta flexibilidad, eficiencia económica y funcionalidad avanzada, asegurando una administración centralizada y escalable que contribuye al correcto funcionamiento de la infraestructura propuesta.

6.4.2.9 Bind9

BIND9 (Berkeley Internet Name Domain, versión 9) es uno de los servidores DNS más utilizados en el mundo. Fue desarrollado por el Internet Systems Consortium (ISC) y se considera el estándar de facto para la implementación de servicios de resolución de nombres en sistemas Unix y Linux. [28]

- Con BIND9, un servidor puede desempeñar funciones críticas como:
- Servidor autoritativo: responde por dominios configurados directamente en su base de datos.
- Servidor recursivo o caché: busca y almacenas respuestas de otros DNS para optimizar consultas de clientes.
- Soporte para DNSSEC: añade seguridad mediante la validación criptográfica de respuestas DNS.
- Soporte para IPv4 e IPv6.
- Gestión avanzada de zonas: primarias, secundarias y reversas.

Es ampliamente usado en redes empresariales, proveedores de internet, universidades y laboratorios académicos, debido a su robustez, flexibilidad y a que es software libre y de código abierto.

6.4.2.10 Justificación de por qué se usó Bind9

La elección de BIND9 como servidor DNS en nuestra red se fundamenta en su estabilidad, flexibilidad y adopción global como estándar de facto en la administración de servicios de nombres. Al ser un software de código abierto, desarrollado y mantenido por el Internet Systems Consortium (ISC), BIND9 ofrece una solución robusta y segura sin costos de licenciamiento, lo cual representa una ventaja significativa en entornos académicos y de producción.

Entre las principales razones para su implementación se encuentra su capacidad de funcionar tanto como servidor autoritativo encargado de resolver directamente las consultas de dominios internos como servidor recursivo o de caché, lo que permite optimizar la resolución de nombres hacia internet y mejorar los tiempos de respuesta para los usuarios de la red. Además, BIND9 cuenta con soporte para DNSSEC, lo que garantiza mayor seguridad en la resolución de nombres mediante validación criptográfica, un aspecto fundamental para proteger contra ataques como cache poisoning o suplantación de DNS.

6.4.2.11 Asterisk – FreePBX

FreePBX es una plataforma de administración gráfica basada en web que funciona sobre el motor de telefonía Asterisk, y permite configurar y gestionar de manera sencilla un sistema de centralita telefónica (PBX) VoIP. [29]

Características principales de FreePBX

- Facilita la administración de Asterisk a través de una interfaz amigable, sin necesidad de editar manualmente los archivos de configuración.

- Permite crear y administrar extensiones SIP/IAX, troncales hacia proveedores de telefonía IP, planes de marcado, buzones de voz, colas de llamadas y menús IVR (respuesta de voz interactiva).
- Ofrece módulos adicionales para grabación de llamadas, reportes, control de llamadas, seguridad, integración con CRM y soporte para call centers.
- Es software libre de código abierto, desarrollado inicialmente por la comunidad y actualmente mantenido por Sangoma Technologies.
- Se utiliza ampliamente en empresas, instituciones educativas y laboratorios, porque es escalable, personalizable y de bajo costo en comparación con centralitas propietarias.

6.4.2.12 Justificación de por qué se usó FreePBX

La elección de FreePBX como plataforma de gestión de telefonía IP en nuestra red se justifica por su facilidad de administración, escalabilidad y bajo costo, lo que la convierte en una herramienta ideal para entornos educativos y empresariales. Al estar basado en Asterisk, FreePBX hereda todas las capacidades de un sistema de PBX de código abierto, pero con el valor agregado de una interfaz gráfica amigable que simplifica la configuración y el control del sistema.

Una de las razones principales para su implementación es que permite a los administradores crear y gestionar extensiones, troncales, planes de marcado, buzones de voz y menús IVR de manera intuitiva, reduciendo el tiempo y la complejidad en comparación con la configuración manual de Asterisk. Además, ofrece la posibilidad de añadir módulos adicionales para funciones avanzadas como colas de llamadas, grabación, reportes y seguridad, lo que lo hace adaptable a distintos niveles de necesidad en la red.
Otro aspecto clave es su costo-beneficio, ya que FreePBX es software libre, con actualizaciones constantes y soporte por parte de la comunidad y de Sangoma Technologies. Esto lo convierte en una alternativa accesible frente a soluciones propietarias de telefonía IP, sin sacrificar estabilidad ni seguridad. Asimismo, su interoperabilidad con teléfonos VoIP, routers y firewalls de distintos fabricantes (incluyendo MikroTik y FortiGate en nuestra red) asegura una integración transparente en entornos heterogéneos.

6.4.2.13 ISC-DHCP-SERVER

El ISC DHCP Server (Internet Systems Consortium DHCP Server) es un servidor de protocolo DHCP (Dynamic Host Configuration Protocol) de código abierto desarrollado por el Internet Systems Consortium (ISC). Su función principal es asignar direcciones IP y parámetros de red de forma automática a los dispositivos de una red, evitando la configuración manual en cada host. [30]

Características principales:

- **Asignación dinámica de IPs**: entrega direcciones IP de un rango predefinido a los clientes que se conectan.
- **Asignación estática (reservas)**: permite asociar direcciones IP específicas a direcciones MAC concretas.
- **Configuración de parámetros adicionales**: como máscara de subred, puerta de enlace (gateway), servidores DNS, servidores NTP, etc.
- **Soporte para IPv4 e IPv6**.
- **Alta personalización** a través de archivos de configuración (/etc/dhcp/dhcpd.conf en sistemas Linux).
- Es ampliamente usado en universidades, empresas y laboratorios porque es gratuito, confiable y compatible con entornos heterogéneos.

En una infraestructura con múltiples VLANs y subredes, como la que estás diseñando, el ISC DHCP Server permite centralizar la entrega de direcciones IP y asegurar que cada dispositivo en la red tenga conectividad adecuada sin intervención manual.

6.4.2.14 Justificación de por qué se usó ISC-DHCP-SERVER

La adopción de ISC DHCP Server en la red se justifica por la necesidad de contar con un servicio de asignación automática y centralizada de direcciones IP, lo cual garantiza una administración más eficiente y ordenada de los recursos de red. En un entorno de tipo campus, donde existen múltiples VLANs y subredes, resulta inviable realizar configuraciones manuales en cada dispositivo; por ello, ISC DHCP Server se convierte en una solución esencial.

Entre sus principales ventajas destacan su flexibilidad y robustez, ya que permite configurar tanto asignaciones dinámicas (IPs dentro de un rango predefinido) como asignaciones estáticas (reservas de IPs para dispositivos críticos). Asimismo, soporta la distribución de parámetros adicionales como gateway predeterminado, máscara de subred, servidores DNS y NTP, lo cual asegura que cada cliente de la red pueda conectarse y comunicarse de manera adecuada.

Otro motivo importante para su implementación es que se trata de una herramienta open source mantenida por el Internet Systems Consortium (ISC), ampliamente probada y utilizada en redes empresariales y educativas a nivel mundial. Su compatibilidad con sistemas Linux/Debian facilita la integración con otros servicios de red (como BIND9 para DNS), y su estabilidad garantiza un funcionamiento confiable incluso en redes con alta densidad de usuarios.

6.4.2.15 Open VPN

OpenVPN es un software de código abierto que implementa técnicas de red privada virtual (VPN, Virtual Private Network) para crear conexiones seguras y cifradas a través de redes públicas como Internet. [31]

Características principales de OpenVPN

- Utiliza protocolos de seguridad como SSL/TLS para autenticar y cifrar el tráfico.
- Es compatible con IPv4 e IPv6.
- Permite tanto acceso remoto seguro (usuarios que se conectan a una red corporativa desde fuera) como conexiones sitio a sitio (túneles entre redes distintas).
- Es multiplataforma: funciona en Linux, Windows, macOS, Android y iOS.
- Puede usarse con autenticación basada en usuario/contraseña, certificados digitales y llaves precompartidas.
- Soporta integración con firewalls y políticas de seguridad avanzadas.

Importancia en redes

- Se usa para que empleados o estudiantes accedan a la red interna de forma segura desde internet.
- Protege la comunicación en redes Wi-Fi públicas, evitando espionaje o robo de datos.
- Permite interconectar sucursales o campus universitarios de manera segura a través de túneles cifrados.

6.4.2.16 Justificación de por qué se usó OpenVPN

La elección de OpenVPN en la red se justifica por su capacidad de proporcionar conexiones seguras y cifradas entre distintos segmentos de red y usuarios externos, lo cual es fundamental en un entorno de tipo campus. En este escenario, donde se requiere acceso remoto a recursos internos (servidores, aplicaciones y servicios), OpenVPN permite establecer túneles seguros a través de internet, garantizando la confidencialidad e integridad de los datos transmitidos.

Entre sus principales ventajas destacan que es un software de código abierto, con una amplia comunidad de soporte y mejoras continuas, lo cual asegura transparencia y confiabilidad en su implementación. Asimismo, ofrece flexibilidad en los métodos de autenticación, ya sea mediante certificados digitales, credenciales de usuario o llaves precompartidas, adaptándose a diferentes niveles de seguridad según las necesidades de la red.

6.4.2.17 Apache Web Server

Apache HTTP Server (conocido comúnmente como Apache Web Server) es un servidor web de código abierto desarrollado y mantenido por la Apache Software Foundation. Es uno de los servidores más usados a nivel mundial para publicar sitios web y aplicaciones en internet o intranets. [32]

Características principales de Apache Web Server

- Servidor HTTP/HTTPS: entrega páginas web y contenidos estáticos (HTML, imágenes, CSS, etc.) y dinámicos (PHP, Python, Perl, etc.).
- Multiplataforma: funciona en Linux, Windows, macOS y otros sistemas operativos.
- Módulos extensibles: su arquitectura modular permite añadir funciones como autenticación, balanceo de carga, seguridad, compresión de contenido, reescritura de URLs, entre otros.
- Compatibilidad con lenguajes y frameworks: se integra fácilmente con PHP, Python, Java, Perl, Ruby, y con bases de datos como MySQL o PostgreSQL.
- Seguridad y cifrado: soporta HTTPS mediante SSL/TLS.
- Alto grado de configuración: a través de archivos como httpd.conf y .htaccess.
- Uso en producción y desarrollo: es ampliamente adoptado tanto en empresas como en universidades, ya que permite desde alojar páginas institucionales hasta aplicaciones educativas o de investigación.

6.4.2.18 Debian 13 Trixie

Debian 13 (con nombre en clave “Trixie”) es la próxima versión estable de la distribución GNU/Linux Debian, desarrollada por la comunidad del Proyecto Debian.

Debian es un sistema operativo libre y de código abierto basado en el kernel de Linux, ampliamente utilizado en servidores, estaciones de trabajo y entornos académicos. Se caracteriza por su estabilidad, seguridad y gran cantidad de paquetes de software disponibles (más de 60,000 en sus repositorios oficiales). [33]

Características de Debian 13 “Trixie”

- Será la sucesora de Debian 12 “Bookworm” (lanzada en junio de 2023).
- Actualmente se encuentra en desarrollo, con lanzamientos periódicos de versiones de prueba (testing).
- Como es tradición en Debian, el nombre proviene de un personaje de la película Toy Story.
- Se espera que incluya:
    - ✓ Kernel de Linux más actualizado.
    - ✓ Mejoras en compatibilidad con hardware reciente.

- ✓ Paquetes actualizados (servidores web, bases de datos, entornos gráficos, etc.).
- ✓ Herramientas reforzadas para seguridad y administración de sistemas.

6.4.2.19 Justificación de por qué se usó Debian13 (Trixie)

La selección de Debian 13 "Trixie" como sistema operativo base en nuestra red se justifica por su estabilidad, seguridad y versatilidad, características que lo convierten en una de las distribuciones GNU/Linux más confiables para entornos de servidores y redes complejas. Debian es reconocido mundialmente por ser un sistema operativo libre, de código abierto y con una comunidad activa, lo que garantiza soporte constante y disponibilidad de actualizaciones a largo plazo.

En este proyecto, Debian 13 fue utilizado como plataforma principal para la implementación de servicios críticos como DNS (BIND9), DHCP (ISC DHCP Server), servidores web (Apache) y telefonía IP (FreePBX/Asterisk). Su robustez asegura que dichos servicios funcionen de manera estable, incluso en un escenario de múltiples VLANs y alta densidad de usuarios, como el de una red de campus.

6.5 Propuesta de Segmentación WiFi

6.5.1 ¿Por qué segmentar la red del CAMPUS?

Dentro de la red de la universidad, conviven distintos tipos de usuarios y servicios: estudiantes conectados vía WiFi, personal administrativo en la red cableada, centros de cómputo, telefonía IP, cámaras de seguridad, servicios críticos y demás necesidades de red institucionales. Todos los dispositivos haciendo tráfico muchos de ellos en simultaneo generan una demanda de ancho de banda, seguridad y prioridad.

Si la red no está segmentada, todo ese tráfico viaja en el mismo espacio de direcciones y de broadcast, esto ocasiona:

- **Saturación del ancho de banda** en horas pico (colisiones, retransmisiones, lentitud).
- **Riesgo de seguridad** debido a que los equipos usuarios comparten dominio de red con los servidores críticos.
- **Dificultad para gestionar y priorizar tráfico**, por ejemplo, darle más prioridad a voz, plataformas académicas frente a descargas o streaming.

6.5.1.1 Beneficios de la segmentación de red.

La segmentación en VLANS y subredes permite dividir la red en zonas lógicas, de manera que cada una tenga sus propias políticas de prioridad, seguridad y control de ancho de banda. Esto nos facilita:

1. **Optimizar el uso de los 500 Mb/s disponibles,** evitando que un grupo de usuarios sature el servicio.
2. **Asegurar la continuidad de servicios críticos** tales como servidores, telefonía o administración.
3. **Mejora en la seguridad** al aislar el tráfico sensible de usuarios no confiables.
4. **Escalar la red** más fácilmente, gracias a que cada zona cuesta con su propia VLAN y políticas sin afectar a otra.

Se puede concluir que segmentar la red no es solo una mejora en el rendimiento, sino que se torna un requisito esencial de seguridad y gestión para soportar el crecimiento de usuarios y servicios en pro del desarrollo del campus.

6.5.2 Segmentación de la red.

A partir de la creación de la VLAN para los puntos de acceso WiFi preestablecidas en el documento, se sugiere:

1. Usar SSID separadas:
    a. Académico / Institucional – VLAN institucional Priorizar
    b. Estudiantes – VLAN con Rage Limit
    c. Invitado – VLAN guest, aislada con captive portal.

2. Control Centralizado
    - Los AP Huawei AirEngine usan CAPWAP – Utilizar la controladora en DC
    - Activar Load Balancing y band steering
    - Ajustar los canales y potencia por zona para evitar solapamiento, en especial en áreas como Biblioteca y Auditorios.

3. Redundancia y cableado
    a. Asegurar que cada switch de acceso WiFi6 tenga uplinks redundates al core de distribución.
    b. Monitorear el uso real de cada AP desde la controladora para conocer el tráfico real medio en tráfico de hora pico.

6.5.2.1 Árboles de cola

Un árbol de colas, es una forma de dividir el ancho de banda en “ramas” jerárquicas. Nuestro árbol parte desde el enlace a Internet (500 Mb/s) y se va dividiendo en ramas más pequeñas, como, por ejemplo: [34]

1. Clase de Tráfico: institucional, estudiantes, invitados.

2. Zonas o VLAN: Biblioteca, auditorio, medicina, departamentos, etc.
3. Usuarios Individuales: Cada dispositivo en nuestra red.

Existen diferentes tipos de Árboles de Cola, entre ellos:

1- HTB (Hierarchical Token Bucket) [35]

   a. Organizado general de la red.
   b. Define cuanto ancho de banda mínimo se garantiza a cada rama y cuánto puede llegar a usar si hay disponibilidad.
   c. Divide el internet en zonas, clases y servicios.

2- PCQ (Per Connection Queue) [35]

   a. Se encarga de repartir justamente entre los usuarios
   b. Evita la saturación y acaparamiento de la red en descargas desde un solo dispositivo.

3- Colas Simples /Shapers [35]

   a. Son limites directos a cierto tipo de tráfico
   b. Sirven para reservar ancho de banda fijo a VoIP o servicios críticos.

6.5.2.2 Distribución sugerida

Con el conocimiento recopilado acerca de la red, específicamente sobre la distribución de AP's Wifi de Huawei, así como el tráfico promedio determinado por zona según consultas al personal de gestión de los mismos, podemos resaltar tres zonas claves las cuales categorizaremos a continuación:

- **Zonas de alta densidad:** Biblioteca, Auditorios, Medicina – Mayor Cuota
- **Zonas Académicas:** Aulas, Ingenierías y Arq, Idiomas, Agronomía, Economía, etc – Reparto Medio.
- **Zonas Administrativas:** Administración, Vigilancia, CDI – Menor Cuota (Prioridad en VoIP/Servicios).

Para efectos prácticos tomaremos como base los siguientes datos:

- **Concurrencia Realista (En horas pico)**: 600 Usuarios en la red Wifi
- **Ancho de Banda**: 500 Mb/s
- **Reserva para red cableada**: 150 Mb (30%)
- **Disponibilidad para Puntos de Acceso Wifi**: 350 Mb/s

Por la versatilidad y facilidad de aplicación se recomienda el uso de Colas Simples (Simple Queues) con ella podremos:

- Limitar el ancho de banda por usuario.
- Ajustar equitativamente el uso del ancho de banda de cada zona o Vlan.
- Es flexible y escalable en cuanto al número de usuarios en simultaneo.

Zona	APs aproximadas	Usuarios horas pico	% de WiFi (350 Mb/s)	Cuota (Mb/s)	Rate-limit por usuario
Biblioteca	50	200	30%	105	1–2 Mb/s
Auditorios	30+	150	25%	87.5	1–1.5 Mb/s
Medicina	30–35	120	20%	70	1.5–2 Mb/s
Áreas académicas (Departamentos)	100+	100	20%	70	1–1.5 Mb/s
Admin/Oficinas/Vigilancia/CDI	40+	30	5%	17.5	2–3 Mb/s
TOTAL, WiFi	≈250	~600	100%	**350**	—

Tabla 27: Distribución Wifi

6.6 Propuesta de segmentación de telefonía en la FMO

El nuevo esquema de numeración y gestión de extensiones presenta diversas ventajas en comparación con la estructura anterior. Estas se pueden resumir en los siguientes puntos:

1. **Numeración ordenada y continua**
   El rango de extensiones **1001–1035** se encuentra organizado de forma secuencial, lo que facilita la asignación, la memorización y la administración del sistema. A diferencia del esquema anterior (9201–9292), que contenía huecos y extensiones sin asignar, el nuevo modelo ofrece claridad y uniformidad.
2. **Identificación precisa de dependencias y usuarios**
   Cada extensión cuenta con un nombre descriptivo que corresponde directamente al área o dependencia institucional (ejemplo: *Secretaría Decanato, Biblioteca, Recursos Humanos*). Esto reduce la ambigüedad y permite una rápida localización de los puntos de comunicación.
3. **Uso de protocolo moderno (PJSIP)**
   Todas las extensiones están configuradas bajo el protocolo PJSIP, el cual proporciona mayor

eficiencia en el manejo de recursos, mejor seguridad en la autenticación y compatibilidad con dispositivos y aplicaciones modernas de VoIP.

4. **Escalabilidad del sistema**

   La numeración continua y estandarizada permite crecer de manera ordenada (1036, 1037, etc.), garantizando que nuevas extensiones puedan incorporarse sin romper la lógica del esquema actual

N.º	EQUIPO	UBICACIÓN	EXTENSIÓN
1	TELEFONO IP	Secretaria_Decanato	1001
2	TELEFONO IP	Planificacion	1002
3	TELEFONO IP	Oficina_Postgrado	1003
4	TELEFONO IP	Oficina_Planificacion	1004
5	TELEFONO IP	Biblioteca	1005
6	TELEFONO IP	Secretaria_vicedecanato	1006
7	TELEFONO IP	Disponible	1007
8	TELEFONO IP	Oficina_Decano	1008
9	TELEFONO IP	Disponible	1009
10	TELEFONO IP	Disponible	1010
11	TELEFONO IP	Procesos_tecnicos	1011
12	TELEFONO IP	Biblioteca_2	1012
13	TELEFONO IP	Biblioteca_3	1013
14	TELEFONO IP	Biblioteca_4	1014
15	TELEFONO IP	Biblioteca_5	1015
16	TELEFONO IP	Financiera	1016
17	TELEFONO IP	Financiera_2	1017
18	TELEFONO IP	Financiera_3	1018
19	TELEFONO IP	Colecturia	1019
20	TELEFONO IP	Proyeccion_social	1020
21	TELEFONO IP	Desarrollo_fisico	1021
22	TELEFONO IP	Administracion_academica	1022
23	TELEFONO IP	Administracion_academica_2	1023
24	TELEFONO IP	Administracion_academica_3	1024
25	TELEFONO IP	Administracion_academica_4	1025
26	TELEFONO IP	Administracion_academica_5	1026

27	TELEFONO IP	Recursos_humanos	1027
28	TELEFONO IP	Agronomia	1028
29	TELEFONO IP	Unidad_de_Estudio_Socioeconomico	1029
30	TELEFONO IP	Administracion_General	1030
31	TELEFONO IP	Matematica	1031
32	TELEFONO IP	Medicina_Asistente	1032
33	TELEFONO IP	SIDESI	1033
34	TELEFONO IP	Ingenieria_Arquitectura	1034
35	TELEFONO IP	Ciencias_Juridicas	1035

Tabla 28: Propuesta de segmentación de telefonía en la FMO

6.7 Políticas de Seguridad en la Red

Con el propósito de proteger la infraestructura tecnológica y garantizar un uso adecuado de los recursos de red, se han definido una serie de reglas de seguridad**.** Estas reglas permiten o bloquean ciertos accesos según el tipo de usuario, el servicio y la necesidad institucional. A continuación, se describen de manera sencilla:

N.º	Nombre de la regla	Explicación	Acción
1	**Bloquear SSH Externo**	Se evita que personas externas a la institución intenten conectarse de forma remota a los equipos.	Bloqueado
2	**Acceso a servidores internos**	Solo el personal autorizado puede entrar a los servidores para tareas de mantenimiento y gestión.	Permitido
3	**Proteger el núcleo de la red**	Los usuarios normales (WiFi o laboratorios) no pueden acceder al “centro” de la red donde se administra.	Bloqueado
4	**Bloqueo de VLAN Cómputo**	Los equipos de los laboratorios de cómputo no tienen permiso para entrar a la red administrativa.	Bloqueado
5	**WiFi solo con Internet**	Los usuarios de la red inalámbrica solo tienen acceso a Internet, no a áreas administrativas.	Permitido
6	**Bloquear programas P2P**	Se bloquean descargas con programas como BitTorrent o eMule, que consumen mucho internet y son inseguros.	Bloqueado
7	**Bloquear descargas inseguras**	Se bloquean conexiones antiguas (ej. Telnet, FTP) que no usan seguridad.	Bloqueado
8	**Acceso administrativo**	Solo la red administrativa puede entrar a los equipos de red para configurarlos.	Permitido

9	**DNS y DHCP**	Los usuarios sí pueden obtener dirección IP e información de navegación desde los servidores internos.	Permitido
10	**Contenido restringido**	Se bloquean páginas de ocio (ejemplo: streaming o redes sociales) en ciertos horarios o áreas.	Bloqueado
13	**Bloqueo de ping externo**	Se evita que atacantes externos puedan "probar" la red con herramientas como ping o traceroute.	Bloqueado
14	**Bloqueo de streaming en WiFi**	Se limita el uso de YouTube, Netflix o Twitch en WiFi para priorizar actividades académicas.	Bloqueado

Tabla 29: Políticas de seguridad

7. Metodología de Trabajo

Para el desarrollo de la investigación se aplicó una metodología basada en trabajo de campo y recopilación de información técnica, que permitió conocer el estado actual de la infraestructura de red de la Facultad Multidisciplinaria Oriental de la Universidad de El Salvador.

1. Entrevista con la encargada del Data Center

Se realizó una entrevista semiestructurada con la Ing. Guadalupe Bermúdez, responsable del centro de datos. Este proceso tuvo como objetivo obtener información directa sobre el funcionamiento de la infraestructura de red, los equipos instalados, los servicios implementados y las principales dificultades que enfrenta la facultad en cuanto a administración y seguridad de la red. La entrevista permitió recopilar datos cualitativos que complementaron la revisión documental y el levantamiento técnico.

2. Visita Técnica al Data Center

Posteriormente, se llevó a cabo una visita técnica a las instalaciones del Data Center, en la cual se verificó in situ la disposición de los equipos de red, su estado, las conexiones activas y las condiciones físicas de operación. Durante la visita se procedió a:
Inspeccionar racks, switches, routers, controladoras inalámbricas y servidores.

- Identificar la ubicación y distribución de los equipos.
- Registrar las direcciones IP, interfaces activas y subredes en uso.
- Verificar las políticas de seguridad física y lógica implementadas.

3. Recolección y Organización de la Información

La información obtenida en la entrevista y en la visita técnica fue complementada con la documentación institucional y registros técnicos disponibles. Se elaboraron fichas técnicas de cada equipo, con datos como marca, modelo, número de serie, sistema operativo, servicios que brindan y subredes utilizadas.

4. Sistematización para el Análisis

Los datos recolectados fueron organizados en inventarios y diagramas que representan tanto la topología lógica como la física de la red.
Esta sistematización permitió:

- Identificar fortalezas y debilidades de la infraestructura existente.
- Determinar los puntos críticos de mejora.
- Diseñar una propuesta de modernización escalable y segura

8. Conclusiones

- La infraestructura de red actual de la Facultad Multidisciplinaria Oriental presenta limitaciones importantes que afectan la eficiencia, seguridad y escalabilidad de los servicios. Se identificaron carencias en la organización lógica y en la actualización de equipos, lo que justifica la necesidad de una propuesta de mejora.
- El diseño de red basado en el modelo jerárquico de tres capas (acceso, distribución y núcleo) es una alternativa viable para optimizar la comunicación entre departamentos, mejorar la administración de recursos y facilitar la incorporación de nuevas tecnologías.
- La segmentación de la red mediante VLANs es clave para aumentar la seguridad, reducir la congestión y dar orden al tráfico de datos. Separar funciones académicas, administrativas y de servicios genera un entorno más estable y confiable para estudiantes, docentes y personal.
- La integración de servicios esenciales como DNS, DHCP, VPN, VoIP y autenticación centralizada, junto con políticas de seguridad robustas, asegura la protección de la información y la disponibilidad de los recursos institucionales.
- La validación en entornos simulados (GNS3**)** permitió comprobar la viabilidad técnica del diseño antes de implementarlo, lo que evidencia que las mejoras pueden aplicarse de manera ordenada, minimizando riesgos y costos innecesarios.
- En general, la propuesta demuestra que invertir en una red moderna, escalable y segura no es un gasto, sino una apuesta estratégica que impacta positivamente en la calidad académica y administrativa de la institución

9. Recomendaciones

- Actualizar la infraestructura con equipos que soporten tecnologías de alta disponibilidad, redundancia y segmentación lógica.
- Implementar políticas de seguridad más estrictas, incluyendo control de acceso, firewall perimetral, autenticación centralizada y segmentación de tráfico, para resguardar la confidencialidad, integridad y disponibilidad de los recursos.
- Mantener un monitoreo constante de la red para detectar anomalías, optimizar el rendimiento y prever fallas.
- Capacitar al personal técnico y administrativo en el uso de las nuevas tecnologías, protocolos de seguridad y gestión de recursos de red.
- Planificar la expansión futura de la red considerando el crecimiento institucional, con un diseño escalable que facilite la incorporación de más usuarios, dispositivos y servicios.
- Asegurar sostenibilidad económica, evaluando siempre la relación costo–beneficio en cada adquisición tecnológica.
- Se recomienda que el cableado estructurado de la red de la FMO-UES sea migrado progresivamente a fibra óptica**,** ya que actualmente no todos los enlaces cuentan con esta tecnología. La implementación de fibra óptica garantizará mayor velocidad de transmisión, menor latencia, mayor estabilidad en la conectividad y una infraestructura más confiable, preparada para responder a las demandas actuales y futuras de los servicios académicos y administrativos.

10. **Referencias**

[1] J. DORDOIGNE, «Redes informáticas actuales,» de *Redes informáticas Nociones Fundamentales (8a edición)*, Ediciones ENI, 2020, p. 26.

[2] TANENBAUM, ANDREW S., «Modelo OSI,» de *Redes de Computadoras*, PEARSON, 2012, pp. 37,38.

[3] TANENBAUM, ANDREW S., «Capa física,» de *Redes de Computadoras*, PEARSON, 2012, p. 36.

[4] A. TANEMBAUM, «La capa de enlace,» de *Redes de Computadoras*, Pearson, 2012, p. 183.

[5] TANENBAUM, ANDREW S., «La capa de red,» de *Redes de Computadoras*, PEARSON, 2012, p. 37.

[6] TANENBAUM, ANDREW S., «La capa de sesión, La capa de presentación, La capa de aplicación,» de *Redes de Computadoras* , PEARSON, 2012, p. 38.

[7] TANENBAUM, ANDREW S., «El modelo de referencia TCP/IP,» de *Redes de Computadoras*, PEARSON, 2012, p. 39.

[8] TANENBAUM, ANDREW S., «Capa de Transporte,» de *Redes de Computadoras*, PEARSON, 2012, p. 40.

[9] TANENBAUM, ANDREW S., «La relación entre servicios y protocolos,» de *Redes de Computadora*, PEARSON, 2012, p. 34.

[10] M. Mozilla, «Generalidades del protocolo HTTP,» de *Mozilla Developer Network, [En línea], Available: https://developer.mozilla.org/es/docs/Web/HTTP/Guides/Overview*.

[11] A. F. Behrouz A. Forouzan y s. Chung Fegan, «Data Communications and Networking,» de *Data Communications and Networking*, United States, McGraw-HilI, 2007.

[12] E. Equipo editorial, «Red - Qué es, tipos de red, topología y elementos,» Equipo editorial, Etecé,, 15 Febreo 2025. [En línea]. Available: https://concepto.de/red-2/. [Último acceso: 31 julio 2025].

[13] J. Dordoeigne, Redes Informáticas (Nociones Fundamentales) 4a edicion, ENI, 2013.

[14] I. CISCO Systems, «CISCO,» CISCO Systems, Inc., [En línea]. Available: https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/network-switch-how.html. [Último acceso: 24 8 2025].

[15] CISCO, CISCO Systems, Inc., [En línea]. Available: https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/network-switch-vs-router.html#~switches. [Último acceso: 24 8 2025].

[16] A. S. Tanenbaum, «Redes de Computadoras,» de *Quinta Edición*, Pearson, 2012, pp. 82 -87.

[17] CISCO, CISCO Sytems, Inc., [En línea]. Available: https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/what-is-access-point.html?dtid=osscdc000283&linkclickid=srch#~tipos-de-access-points. [Último acceso: 24 08 2025].

[18] A. S. Tanenbaum, «Redes de Computadoras,» PEARSON, 2012, p. 703.

[19] I. P. a. Paso, InternetPasoaPaso.com, [En línea]. Available: https://internetpasoapaso.com/wireless-lan-controller/. [Último acceso: 24 8 2025].

[20] IBM, IBM, [En línea]. Available: https://www.ibm.com/mx-es/think/topics/intrusion-detection-system. [Último acceso: 24 8 2025].

[21] D. E. Peralta y L. E. Martin, «Redes de información y comunicación I,» de *Redes de información y comunicación I* , Catamarca, Editorial Científica Universitaria de la, 2021, pp. 81-89.

[22] «Red Hat,» 30 7 2025. [En línea]. Available: https://www.redhat.com/es/partners/network-infrastructure.

[23] «cloudflare,» [En línea]. Available: https://www.cloudflare.com/es-es/learning/network-layer/what-is-a-campus-area-network/. [Último acceso: 30 7 30].

[24] E. D. C. D. GoDaddy, «VLAN: Qué es y cómo optimizar las redes locales,» 26 11 2024. [En línea]. Available: https://www.godaddy.com/resources/latam/seguridad/vlan-que-es. [Último acceso: 30 7 2025].

[25] C. Systems, «Cisco 7200 VXR Routers—The New Benchmark for Secure WAN and MAN Services Aggregations,» Cisco Systems, [En línea]. Available: https://www.cisco.com/c/dam/en/us/products/collateral/security/router-security/prod_brochure0900aecd804718b9.pdf. [Último acceso: 13 septiembre 2025].

[26] fortinet, «www.fortinet.com,» [En línea]. Available: https://www.fortinet.com/products/next-generation-firewall. [Último acceso: 29 septiembre 2025].

[27] Mikrotik, «mikrotik.com,» [En línea]. Available: https://mikrotik.com/aboutus. [Último acceso: 29 09 2025].

[28] I. S. Consortium, «ISC,» [En línea]. Available: https://www.isc.org/bind/. [Último acceso: 29 09 2025].

[29] S. Technologies, «freepbx,» [En línea]. Available: www.freepbx.org. [Último acceso: 29 09 2025].

[30] I. S. Consortium, «isc.org,» [En línea]. Available: https://www.isc.org/dhcp. [Último acceso: 29 09 2025].

[31] O. VPN, «OpenVPN,» [En línea]. Available: https://openvpn.net/. [Último acceso: 30 09 2025].

[32] Apache Software Foundation, «Apache Software Foundation,» [En línea]. Available: https://httpd.apache.org/. [Último acceso: 30 09 2025].

[33] D. Project, «Debian,» [En línea]. Available: https://www.debian.org/releases/trixie. [Último acceso: 30 09 2025].

[34] MikroTik, «MikroTik Wiki,» [En línea]. Available: https://wiki.mikrotik.com/wiki/Manual:Queue_Tree. [Último acceso: 30 09 2025].

[35] MikroTik, «MikroTik Wiki,» [En línea]. Available: https://help.mikrotik.com/docs/display/ROS/Queues. [Último acceso: 30 09 2025].

[36] A. S. Tanenbaum y D. J. Wetherall , «Redes de computadoras,» de *Redes de computadoras*, mexico, PEARSON EDUCACIÓN, 2012, pp. 35-45.

[37] Mozilla, Generalidades del protocolo HTTP, MDN Web Docs, 2025.

11. Anexos

Se presenta la topología de red implementada en GNS3 como parte de la simulación práctica de la propuesta de diseño para la FMO-UES. En este esquema se representan de manera integrada los servidores, equipos de seguridad, routers, switches de acceso y distribución, así como las distintas VLAN asignadas a áreas académicas y administrativas. El diagrama permite visualizar cómo se interconectan los diferentes dispositivos virtualizados y físicos dentro del laboratorio, recreando la infraestructura planteada en un entorno controlado para su análisis y demostración.

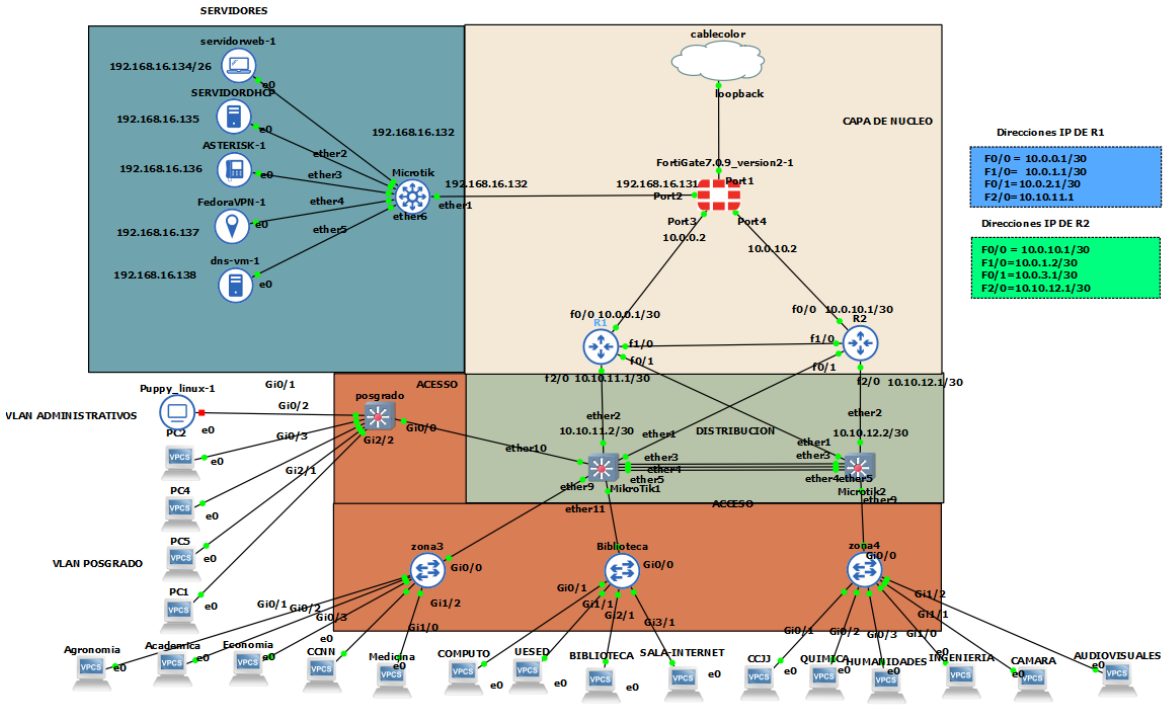

Figura 17: Topología en GNS3

San Miguel, 8 de agosto del 2025

Ingeniera Ligia Astrid Hernández Bonilla
Jefa de la Unidad de Sistemas Informáticos
Universidad de El Salvador FMO

Presente.

Estimada Ingeniera Astrid:

Reciba un cordial saludo de parte del grupo de estudiantes del curso de Pre-Especialización denominado **"Diseño Y Administración De Infraestructura De Redes Empresariales De Alta Disponibilidad"**

Por medio de la presente, solicitamos respetuosamente su autorización para realizar un levantamiento técnico de la infraestructura tecnológica de red de la Facultad, como parte de nuestras actividades académicas y con el objetivo de realizar nuestro proyecto final de la Pre-Especialización.

Este trabajo consistirá en recolectar información detallada sobre los equipos instalados en el data center incluyendo como mínimo los siguientes aspectos por dispositivo:

- Marca, modelo y número de serie.
- Tipo de equipo (switch, router, firewall, servidor, entre otros).
- Sistema operativo o firmware instalado.
- Interfaces físicas activas.
- Direcciones IP asignadas y subredes configuradas.
- Servicios brindados (por ejemplo, DHCP, DNS, NAT, etc.).
- Conectividad con otros dispositivos de red.

Asimismo, solicitamos su permiso para realizar un inventario de los equipos tecnológicos presentes en las siguientes áreas de la Facultad:

- Departamentos administrativos.

- Aulas de clase.
- Laboratorios.
- Biblioteca.
- Oficina de coordinación y dirección.

Este trabajo podrá complementarse con esquemas, planos o fotografías con anotaciones técnicas, que permitan representar de forma clara la ubicación y conectividad de los dispositivos.

Agradecemos de antemano su atención y quedamos atentos a cualquier indicación adicional que estime conveniente.

Sin más por el momento, nos despedimos con el mayor de los respetos.

Atentamente,

Nombre: Victoria Gabriela Velásquez Orellana
Carné: VV19020

Nombre: Angela Emeli Gómez López
Carné: GL16004

Nombre: Leonel Osmín Gutiérrez Ortez
Carné: GO16004

Nombre: Débora María Martínez Méndez
Carné: MM15187

Nombre: Jose Noe Saravia Chavarria
Carné: SC13037

Nombre: José Manuel Silva Paiz
Carné: SP19002

Nombre: Elian Francisco Treminio Parada

Carné: TP20007

Nombre: Bryan Alexander Mata Cáceres

Carné: MC19038

Estudiantes del Diplomado de Pre-especialización denominado: "Diseño Y Administración De Infraestructura De Redes"

Ingeniería en Sistemas Informáticos

Universidad de El Salvador – FMO

Ingeniera Ligia Astrid Hernández Bonilla

Figura 18: Carta de permiso aprobada para la visita técnica

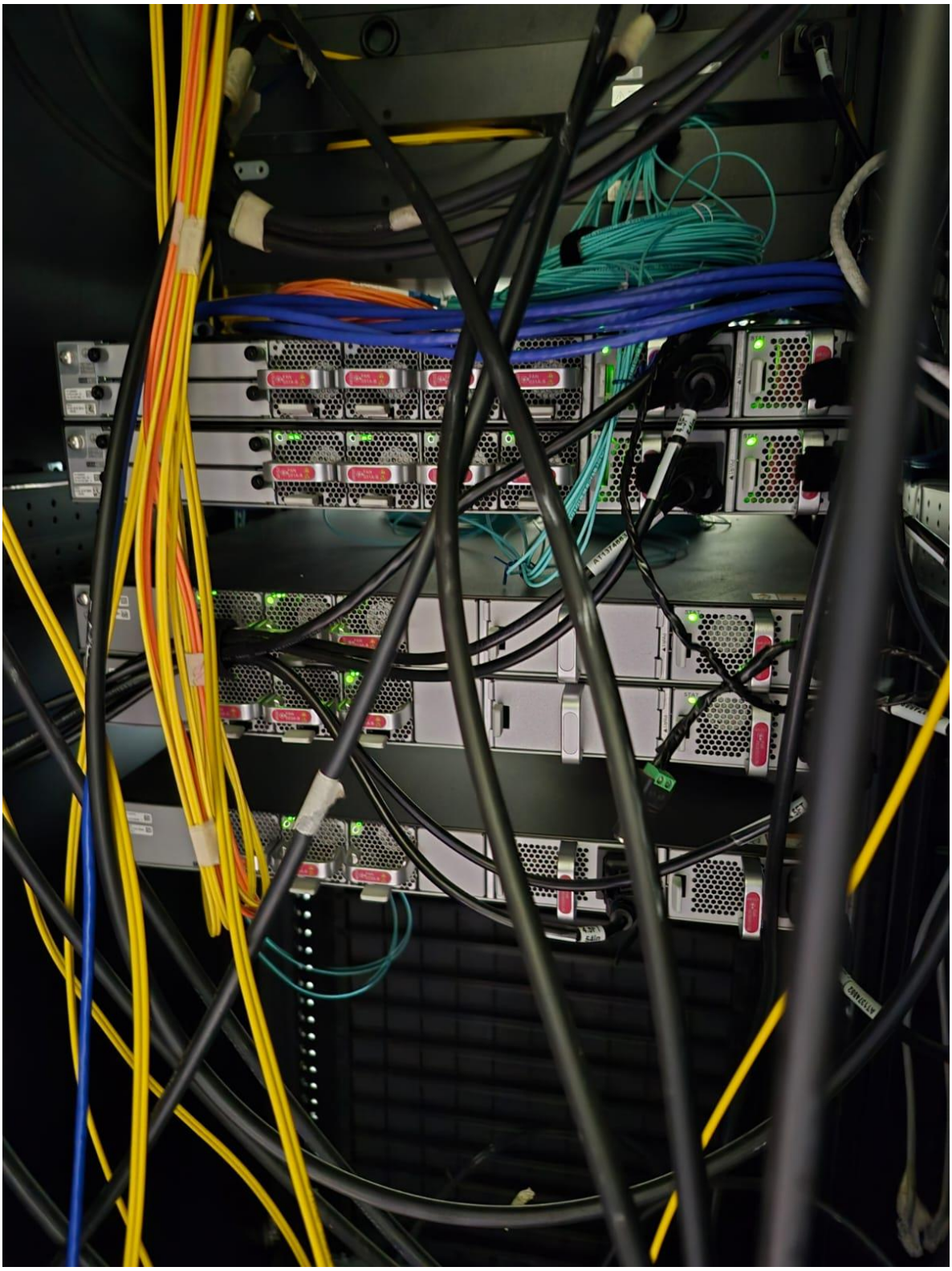

Figura 19: Evidencia de la visita técnica al centro de datos

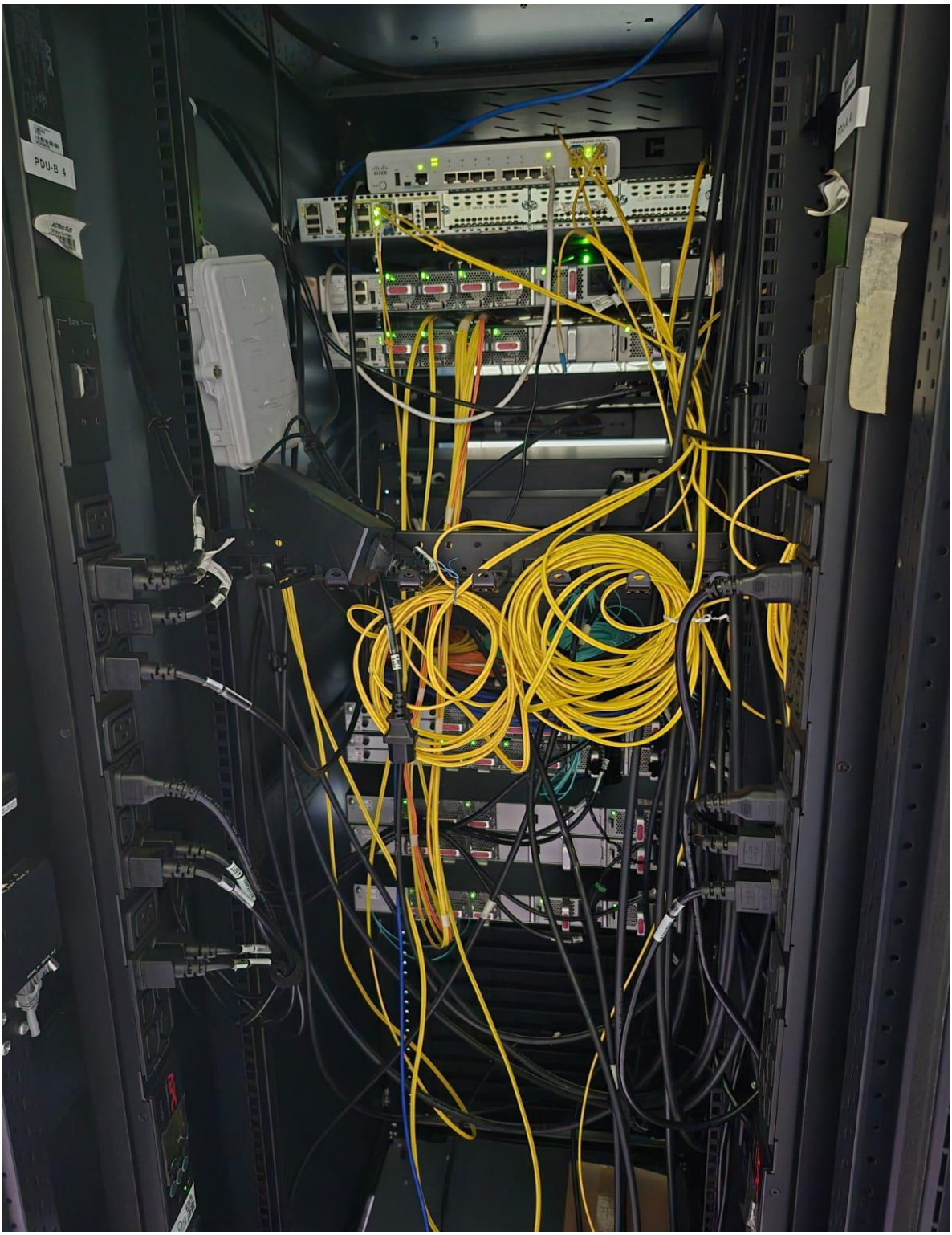

Figura 20: Equipos del centro de datos 1

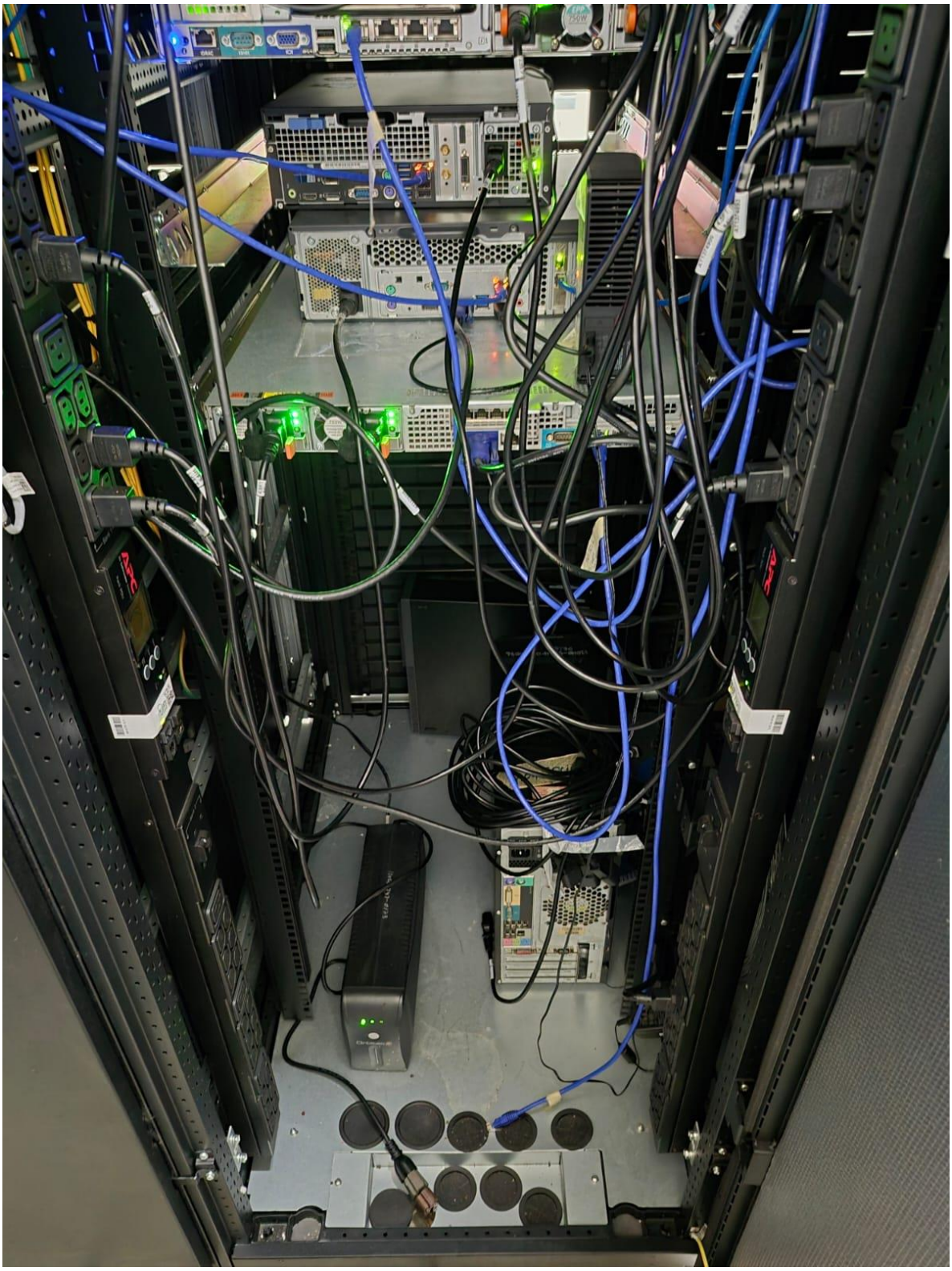

Figura 21: Equipos del centro de datos 2

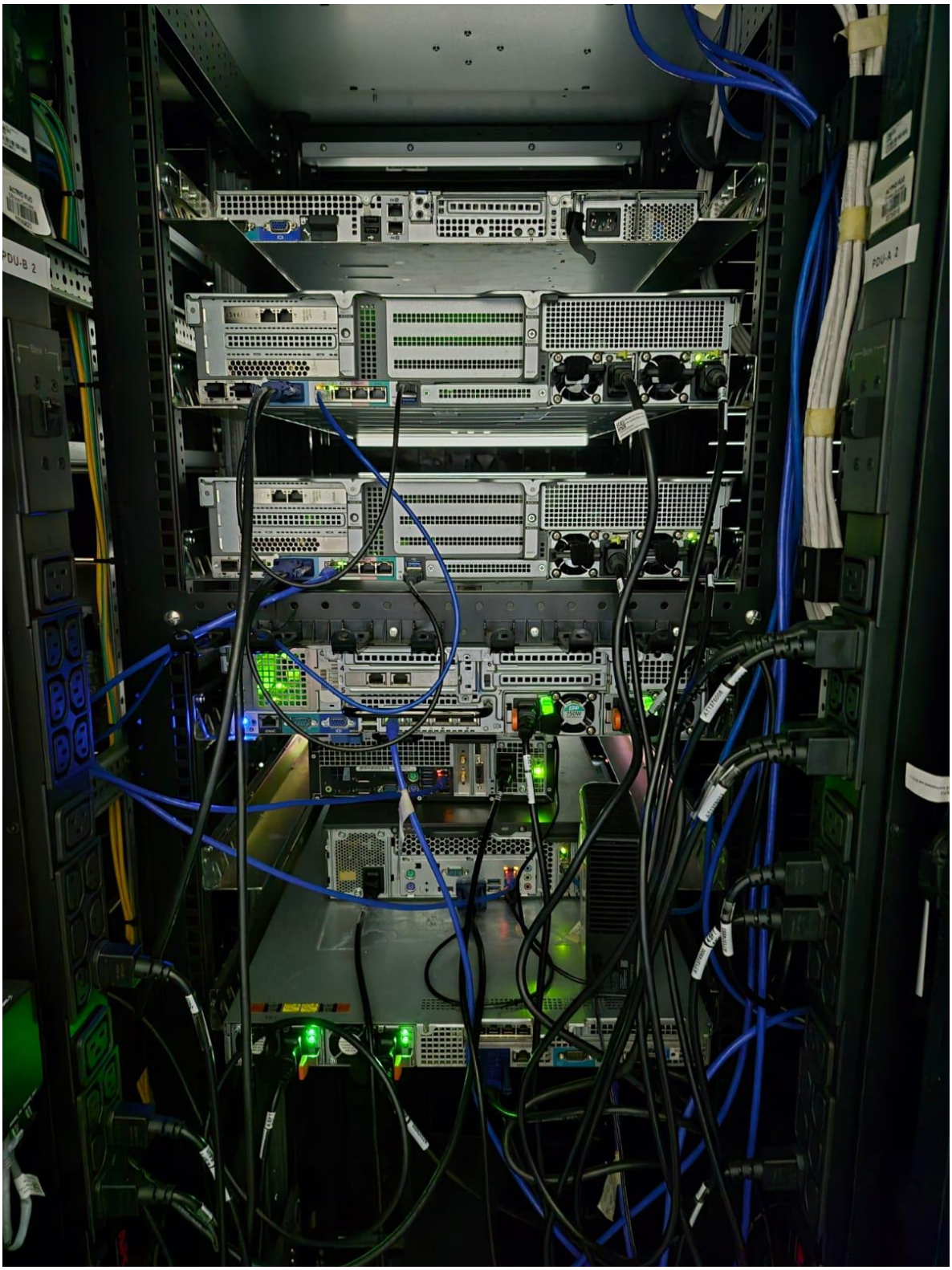

Figura 22: Equipos del centro de datos 3

Figura 23: Evidencia de reuniones de trabajo 1

Figura 24: Evidencia de reuniones de trabajo 2