

**UNIVERSIDAD DE EL SALVADOR  
FACULTAD MULTIDISCIPLINARIA ORIENTAL  
DEPARTAMENTO DE INGENIERÍA Y ARQUITECTURA  
SECCIÓN DE INGENIERÍA DE SISTEMAS INFORMÁTICOS**



**MODALIDAD DE CURSO O DIPLOMADO**

DIPLOMADO DE PRE-ESPECIALIZACIÓN DISEÑO Y ADMINISTRACIÓN DE INFRAESTRUCTURA DE REDES EMPRESARIALES DE ALTA DISPONIBILIDAD.

**TÍTULO**

PROPUESTA DE NUEVA INFRAESTRUCTURA DE RED DE LA UNIVERSIDAD DE EL SALVADOR, FACULTAD MULTIDISCIPLINARIA ORIENTAL.

**NOMBRE DE AUTOR:**

JOSÉ MANUEL SILVA PAIZ	SP19002
ANGELA EMELI GÓMEZ LÓPEZ	GL16004
DÉBORA MARÍA MARTÍNEZ MÉNDEZ	MM15187

**PARA OPTAR AL TÍTULO DE**

INGENIERO DE SISTEMAS INFORMÁTICOS

**CATEDRÁTICO ASESOR**

ING. DIEGO ARMANDO HERRERA FLORES

**OCTUBRE 2025, SAN MIGUEL, EL SALVADOR, CENTROAMÉRICA.**

**UNIVERSIDAD DE EL SALVADOR**

**AUTORIDADES:**



MSC. JUAN ROSA QUINTANILLA

**RECTOR:**

DRA. EVELYN BEATRIZ FARFÁN

**VICERECTORA ACADEMICA:**

MSC. ROGER ARMANDO ARIAS ALVARADO

**VICERRECTOR ADMINISTRATIVO:**

LIC. PEDRO ROSALÍO ESCOBR CASTANEDA

**SECRETARIO GENERAL:**

LIC. CARLOS AMILCAR 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**

INGA. MILAGRO ALICIA GONZÁLES DE REYES

**COORDINADOR DE PROCESOS DE GRADO DE INGENIERÍA DE SISTEMAS INFORMÁTICOS**

# ÍNDICE

1. INTRODUCCIÓN.....	1
2. OBJETIVOS.....	2
2.1. Objetivo general .....	2
2.2. Objetivos específicos.....	2
3. MARCO TEÓRICO Y CONCEPTUAL.....	3
3.1. Componentes de red de computadoras .....	3
3.1.1. Tipos de Redes. ....	3
3.2. Topología de Red .....	3
3.2.1 Tipos de Topología de red.....	3
3.3. Infraestructura de Red. ....	7
3.3.1. La Importancia de la Infraestructura de Red .....	8
3.3.2. Red de Área de Campus (CAN). ....	8
3.4. Modelo de diseño Jerárquico.....	9
3.4.1. Modelo de Capa 3.....	9
3.5. Diseño Jerárquico.....	10
3.6. Administración de redes informáticas.....	10
3.6.1. Tipos de Subneteo .....	11
3.7. Componentes de una red. ....	11
3.7.1. Dispositivos Finales.....	11
3.7.2. Dispositivos Intermedios.....	12
3.7.3. Medios de comunicación dentro de las redes.....	15
3.7.4. Sistemas Operativos .....	18
4. ANÁLISIS DE INFRAESTRUCTURA ACTUAL.....	19
4.1. Inventario de equipo de DataCenter.....	19
4.2. Inventario de Oficinas de Coordinación y Dirección .....	20

4.3. Inventario por Departamentos y Aulas .....	21
4.4. Descripción de Precios de Infraestructura Actual .....	28
4.5. Plan para Wifi 6 .....	30
4.7. Distribución de puntos de acceso Wifi 6 .....	33
5. PROPUESTA DE MEJORA Y DISEÑO DE RED .....	55
5.1. Planteamiento de la propuesta .....	55
5.1.1. Soluciones propuestas según el diagnóstico .....	55
5.1.2. Beneficios de las soluciones propuestas .....	56
5.2. Topología de Red .....	56
5.2.1. Topología Física por Zona .....	57
5.2.2. Topología Física Biblioteca .....	58
5.2.3. Topología Lógica Biblioteca .....	59
5.3. Segmentación Lógica .....	61
6. JUSTIFICACIÓN TÉCNICA Y ECONÓMICA. ....	68
6.1. Justificación Técnica .....	68
6.2. Justificación Económica .....	69
7. METODOLOGÍA DE TRABAJO .....	72
8. CONCLUSIÓN Y RECOMENDACIONES .....	73
REFERENCIAS .....	74
ANEXOS Y DIAGRAMAS .....	75

## INDICE DE TABLAS

<b>Tabla 1: Inventario de Equipos de Red en el DataCenter.</b> .....	19
<b>Tabla 2: Oficinas de Coordinación y Dirección.</b> .....	20
<b>Tabla 3: Departamentos Administrativos</b> .....	22
<b>Tabla 4: Aulas de Clases</b> .....	23
<b>Tabla 5: Laboratorios</b> .....	25
<b>Tabla 6: Biblioteca.</b> .....	26
<b>Tabla 7: Servicios Generales.</b> .....	26
<b>Tabla 8: Servicios Estudiantiles.</b> .....	27
<b>Tabla 9: Descripción de Precios de Infraestructura Actual.</b> .....	28
<b>Tabla 10: Distribución Lógica de Red.</b> .....	28
<b>Tabla 11: Plan para Wifi 6</b> .....	30
<b>Tabla 12: Distribución por VLAN Por Zonas.</b> .....	31
<b>Tabla 13: Distribución de VLAN Zona 2.</b> .....	33
<b>Tabla 14: Distribución de Puntos de Acceso Wifi 6 para oficinas de Admin. Académica.</b> .....	34
<b>Tabla 15: Distribución de Puntos de Acceso Wifi 6 para aulas de Educación.</b> .....	35
<b>Tabla 16: Distribución Puntos de Acceso Wifi 6 para Auditorium PP1.</b> .....	36
<b>Tabla 17: Distribución de Puntos de Acceso Wifi 6 para Auditorium PP2.</b> .....	36
<b>Tabla 18: Distribución de puntos de Acceso Wifi 6 Para Biblioteca Unidad Financiera.</b> .....	37
<b>Tabla 19: Distribución de puntos de Acceso Wifi 6 para Biblioteca Vice-Decano.</b> .....	38
<b>Tabla 20: Distribución de puntos de Acceso Wifi 6 para Biblioteca Área de Servidores.</b> .....	38
<b>Tabla 21: Distribución de puntos de Acceso Wifi 6 para Biblioteca Sala de Estudio.</b> .....	39
<b>Tabla 22: Distribución de puntos de Acceso Wifi 6 para Biblioteca Laboratorio de Redes.</b> .....	41
<b>Tabla 23: Distribución de puntos de Acceso Wifi 6 para caseta de vigilantes Entrada Principal.</b> .....	42
<b>Tabla 24: Distribución de puntos de Acceso Wifi 6 para Caseta de Vigilancia de Parqueo Principal.</b> .....	42
<b>Tabla 25: Distribución de puntos de Acceso Wifi 6 para Centro de Desarrollo Infantil (CDI).</b> .....	42
<b>Tabla 26: Distribución de puntos de Acceso Wifi 6 para Ciencias Jurídicas Sala de Simulación de Audiencia.</b> .....	43

<b>Tabla 27: Distribución de puntos de Acceso Wifi 6 para Laboratorio de Química y Farmacia.....</b>	<b>44</b>
<b>Tabla 28: Distribución de puntos de Acceso Wifi 6 para el Edificio Riñón.....</b>	<b>44</b>
<b>Tabla 29: Distribución de puntos de Acceso Wifi 6 para Edificio del Riñón Nivel 2.....</b>	<b>45</b>
<b>Tabla 30: Distribución de puntos de Acceso Wifi 6 para Medicina 1/ Nivel.....</b>	<b>45</b>
<b>Tabla 31: Distribución de puntos de Acceso Wifi 6 para Medicina 1 / Nivel 2.....</b>	<b>46</b>
<b>Tabla 32: Distribución de puntos de Acceso Wifi 6 para Medicina 2 / Nivel 2.....</b>	<b>48</b>
<b>Tabla 33: Distribución de puntos de Acceso Wifi 6 para Medicina 2 / Nivel 2.....</b>	<b>49</b>
<b>Tabla 34: Distribución de puntos de acceso Wifi 6 para aulas de Agronomía. ....</b>	<b>50</b>
<b>Tabla 35: Distribución de puntos de Acceso Wifi 6 para Agronomía Oficinas.....</b>	<b>51</b>
<b>Tabla 36: Distribución de puntos de Acceso Wifi 6 para Aulas de Economía.....</b>	<b>51</b>
<b>Tabla 37: Distribución de puntos de Acceso Wifi 6 para Aulas de Inglés.....</b>	<b>52</b>
<b>Tabla 38: Distribución de puntos de Acceso Wifi 6 para Aulas de Ingeniería y Arquitectura.....</b>	<b>53</b>
<b>Tabla 39: Distribución de puntos de Acceso Wifi 6 para Aulas de Ingeniería y Arquitectura.....</b>	<b>53</b>
<b>Tabla 40: Segmentación Lógica. ....</b>	<b>61</b>
<b>Tabla 41: Direcciones IP utilizadas en switches L3 para capa de núcleo.....</b>	<b>64</b>
<b>Tabla 42: Dirección de VLANs en switches. ....</b>	<b>66</b>
<b>Tabla 43: Direcciones IP en servidores. ....</b>	<b>66</b>
<b>Tabla 44: Direcciones IP firewall.....</b>	<b>67</b>
<b>Tabla 45: Equipos Propuestos.....</b>	<b>69</b>
<b>Tabla 46: Medidas de Fibra Óptica. ....</b>	<b>70</b>

## INDICE DE FIGURA

<b>Figura 1: Topología de Red Punto a Punto</b> .....	4
<b>Figura 2: Topología de Red en Bus</b> .....	4
<b>Figura 3: Topología de Red en Estrella</b> .....	5
<b>Figura 4: Topología de Red en Anillo Círculo</b> .....	5
<b>Figura 5: Topología de Red en Malla</b> .....	6
<b>Figura 6: Topología de Red en Árbol</b> .....	6
<b>Figura 7: Topología de Red Híbrida o Mixta.</b> .....	7
<b>Figura 8: Topología de Red Doble Anillo.</b> .....	7
<b>Figura 9: Modelo Jerárquico de Capa 3</b> .....	10
<b>Figura 10: Servidor.</b> .....	12
<b>Figura 11: Estación de Trabajo</b> .....	12
<b>Figura 12: Repetidor</b> .....	13
<b>Figura 13: Bridges</b> .....	13
<b>Figura 14: Switch</b> .....	14
<b>Figura 15: Routers</b> .....	14
<b>Figura 16: Brouters</b> .....	15
<b>Figura 17: Firewall</b> .....	15
<b>Figura 18: Conexión Fibra Óptica.</b> .....	16
<b>Figura 19: Cable Coaxial.</b> .....	16
<b>Figura 20: Par Trenzado</b> .....	17
<b>Figura 21: Topología de Red Por Zonas</b> .....	57
<b>Figura 22: Topología Física Biblioteca.</b> .....	58
<b>Figura 23: Topología Lógica Biblioteca.</b> .....	59
<b>Anexo 1: Topología de Enlace Principal</b> .....	75
<b>Anexo 2: Topología Física Actual.</b> .....	76
<b>Anexo 3: Enlaces Principales Ubicados en El Datacenter.</b> .....	77

## RESUMEN

El presente proyecto se presenta como una propuesta para la mejora de la infraestructura de red de la Universidad de El Salvador, Facultad Multidisciplinaria Oriental, a partir de una investigación y análisis detallado de la red actual. En el marco teórico se abordan los conceptos fundamentales de redes para presentar un contexto de sistemas de comunicaciones, describiendo los principales tipos de topología como estrella, bus, malla, anillo e híbrida, así como la descripción de los principales equipos y medios de comunicación empleados, entre ellos switches, routers, firewalls, fibra óptica y enlaces inalámbricos. La propuesta plantea una infraestructura jerárquica de tres capas que integre enlaces redundantes, segmentación mediante VLANs y medidas de seguridad avanzadas, incluyendo firewalls, autenticación y filtrado. Además, busca garantizar la escalabilidad de la red, permitiendo su crecimiento y adaptación a futuros servicios. En la parte económica se determinó que para implementar esta propuesta se necesita un presupuesto de \$17,417.52, considerando la adquisición de nuevos switches y 10 km de fibra óptica monomodo, con el objetivo de asegurar alta disponibilidad y continuidad operativa. Como resultado de la investigación, se identificaron aspectos que pueden optimizarse para incrementar la eficiencia y confiabilidad de la red, tales como la incorporación de redundancia en enlaces y equipos, la actualización de la segmentación lógica, el fortalecimiento de la seguridad y el control de acceso. Actualmente, algunos edificios cuentan con un único enlace hacia un switch de distribución, lo que puede afectar la continuidad del servicio ante una interrupción. Aunque los switches de distribución están configurados en stack para respaldo, el proceso de conmutación aún se realiza manualmente, generando tiempos de recuperación mayores.

Palabras claves: redundancia, infraestructura, segmentación, VLANs, autenticación, filtrado.

## ABSTRACT

This project presents a comprehensive proposal to enhance the network infrastructure of the University of El Salvador, Eastern Multidisciplinary Faculty, through an in-depth investigation and analysis of the existing network environment. The theoretical framework addresses the fundamental principles of computer networking, providing an overview of communication systems and describing the main network topologies—such as star, bus, mesh, ring, and hybrid—as well as the primary networking devices and transmission media used, including switches, routers, firewalls, optical fiber, and wireless links. The proposed solution introduces a three-layer hierarchical architecture designed to incorporate redundant links, VLAN-based segmentation, and advanced security mechanisms such as firewalls, authentication, and traffic filtering. Furthermore, the design emphasizes scalability, ensuring that the network can accommodate future growth and evolving service demands. From an economic standpoint, the implementation of this proposal requires an estimated budget of \$17,417.52, which includes the acquisition of new switches and 10 kilometers of single-mode optical fiber to guarantee high availability and operational continuity. The findings of this study reveal several areas for improvement to increase network efficiency and reliability, including the integration of redundancy in links and equipment, enhancement of logical segmentation, and strengthening of security and access control policies. Currently, some buildings are connected through a single link to a distribution switch, which poses a risk to service continuity in the event of a failure. Although the distribution switches are configured in a stack for redundancy, the switchover process remains manual, resulting in extended recovery times.

**Keywords:** redundancy, infrastructure, segmentation, VLANs, authentication, filtering.

## 1.INTRODUCCIÓN.

En la actualidad, la infraestructura de red es fundamental para cualquier organización moderna, ya sea del sector educativo, empresarial, gubernamental o de servicios. En todos estos entornos, los procesos operativos, administrativos, de comunicación y gestión dependen directamente de una conectividad estable, segura y de alto rendimiento. En un escenario donde las tecnologías de la información evolucionan de forma acelerada y las demandas de conectividad crecen exponencialmente, mantener una red alineada con los estándares actuales representa un desafío constante. Este contexto también alcanza a las instituciones de educación superior, donde las redes deben atender no solo las necesidades académicas y administrativas, sino también las demandas de investigación y servicios para la comunidad estudiantil. Por ello, resulta indispensable evaluar y proponer un nuevo diseño, optimizando las redes existentes con un enfoque estratégico y técnico que garantice su continuidad operativa, seguridad y escalabilidad.

La Universidad de El Salvador, Facultad Multidisciplinaria Oriental no es ajena a esta realidad. El incremento de usuarios, dispositivos y aplicaciones, junto con la creciente demanda de servicios digitales de alta calidad, ha puesto en evidencia las limitaciones de su infraestructura actual. En particular, ciertas áreas dependen de la conectividad de otras, lo que provoca que una interrupción en un punto específico afecte de forma encadenada a múltiples sectores. Ante este panorama, se plantea el desarrollo de una propuesta integral de reestructuración que considere las necesidades presentes y la proyección de crecimiento institucional, con el objetivo de lograr una red más eficiente, segura y resiliente.

El documento tiene como finalidad presentar una propuesta de reestructuración de la infraestructura de red en un entorno general para la Universidad de El Salvador, Facultad Multidisciplinaria Oriental. Como punto de partida, se llevará a cabo un diagnóstico exhaustivo de la infraestructura actual, identificando fortalezas, limitaciones y puntos de mejora. Los resultados de este análisis servirán como base para el diseño de una red que responda a las necesidades de conectividad, seguridad y rendimiento de la institución.

El documento, incluirá una topología de red simulada, ya que la simulación es una herramienta clave para evaluar y validar el diseño planteado. Este proceso permitirá comprobar aspectos como el rendimiento, la segmentación y las medidas de seguridad, garantizando que la propuesta sea sólida tanto a nivel técnico como conceptual para futuras implementaciones.

Uno de los pilares del diseño será asegurar la disponibilidad y seguridad de la red, incorporando mecanismos de alta disponibilidad y redundancia que permitan la continuidad operativa ante posibles fallos. Asimismo, se implementarán políticas de seguridad y control de acceso para proteger los recursos críticos frente a amenazas internas y externas, integrando medidas como autenticación, segmentación de tráfico, filtrado de paquetes y monitoreo en tiempo real. Todo el diseño seguirá principios reconocidos en la ingeniería de redes, con una estructura jerárquica y criterios que equilibren los requerimientos técnicos con las condiciones económicas, de manera que la propuesta sea viable, segura y sostenible a largo plazo.

## **2. OBJETIVOS**

### **2.1. Objetivo general**

Desarrollar una propuesta de mejora de la infraestructura de red en la Universidad de El Salvador, Facultad Multidisciplinaria Oriental, basada en una investigación exhaustiva previa orientada a encontrar puntos de mejora en la infraestructura de red actual y de esa manera desarrollar una propuesta integral, segura y moderna para la Universidad de El Salvador, Facultad Multidisciplinaria Oriental, que permita mejorar la conectividad, incrementar la disponibilidad y optimizar el rendimiento de los servicios de redes en el campus y los centros de cómputos, para satisfacer las necesidades de la comunidad universitaria.

### **2.2. Objetivos específicos.**

1. Analizar la estructura de la red actual, los equipos, topología, esquemas de direccionamiento y los servicios que están siendo utilizados en la Universidad de El Salvador, Facultad Multidisciplinaria Oriental.
2. Crear inventario técnico de los dispositivos conectados a la red especificando cada área: Equipos de Red en DataCenter, Departamentos administrativos, Aulas de clases, Laboratorios, Biblioteca, Oficina de coordinación y dirección.
3. Diseñar una nueva topología jerárquica que implemente las capas de acceso, distribución y núcleo, que permita mayor escalabilidad, facilidad de administración y control de tráfico en la red.
4. Definir criterios técnicos y económicos para la selección de equipos de red, garantizando un equilibrio entre rendimiento, seguridad y viabilidad financiera.
5. Proponer mecanismos de seguridad, alta disponibilidad y redundancia, incluyendo segmentación mediante VLANs, control de acceso y monitoreo.
6. Elaborar la documentación técnica de la propuesta de actualización de la infraestructura de red, incluyendo diagramas y descripciones detalladas que faciliten su administración y mantenimiento para una posible implementación futura.

### 3. MARCO TEÓRICO Y CONCEPTUAL.

#### 3.1. Componentes de red de computadoras

##### ¿Qué es red de computadoras?

Es un conjunto de dispositivos informáticos, compuestos por hardware y software interconectados entre sí por medio de una estructura cableada o inalámbrica que permiten integrar a todos sus elementos como una sola red [1]. Una red de computadoras no solo se conecta a los equipos físicamente, esto permite que compartan información, programas y recursos; los dispositivos pueden comunicarse entre sí de manera rápida y eficiente, gracias a la utilización de tecnologías como redes inalámbricas. El propósito de una red es facilitar tareas como el acceso compartido en internet, el uso de aplicaciones en línea, transferencia de archivos, la comunicación en tiempo real y la administración centralizada de servicios.

##### 3.1.1. Tipos de Redes.

1. **Redes de área Local:** Son redes de propiedad privada que operan dentro de un solo edificio, como en una casa, oficina o fábricas. La red LAN tiene restricciones en cuanto a su tamaño. Existen dos tipos principales de redes LAN: Alámbricas e inalámbricas. Las redes LAN inalámbricas cuentan con un estándar llamado IEEE 802.11 mejor conocido como wifi, este estándar define como los dispositivos se comunican dentro de una red local. Las redes alámbricas utilizan el estándar 802.3, conocido como ethernet. Este estándar determina cómo los dispositivos se comunican entre sí, mediante cables de cobre o fibra óptica dentro del área local.
2. **Redes de Área Metropolitana MAN:** Generalmente abarca una ciudad o una ciudad metropolitana, interconectando varias redes locales. La televisión por cable constituye una red MAN; sin embargo, los recientes avances en el acceso inalámbrico a internet de alta velocidad han dado lugar a otro tipo de red, la cual se estandarizó como IEEE 802.16 y se conoce comúnmente como WIMAX (Banda ancha inalámbrica).
3. **Redes de Área Amplia WAN:** Abarca una extensa área geográfica, por lo general un país o continente. La red WAN se constituye a partir de otras redes más pequeñas. [2].

#### 3.2. Topología de Red

La topología de red se define como una forma de comunicación usada por las computadoras que conforman una red, ya sea LAN, WAN o MAN, para intercambiar datos. En otras palabras, la manera en que está diseñada la red, sea en el plano físico o lógico [3].

La topología de red informática es fundamental para determinar cómo se transmiten los datos dentro de la red, lo que influye directamente en su rendimiento y eficiencia. Conocer la topología permite entender mejor el flujo de datos, identificar posibles puntos de falla y optimizar el rendimiento de la red. Básicamente, es como un mapa que organiza todo dentro de la red para que la comunicación sea clara y rápida.

##### 3.2.1 Tipos de Topología de red.

Conocer los tipos de topología es realmente importante porque cada una representa una manera distinta de cómo se enlazan las computadoras, los servidores y demás equipos dentro de una red. Conocer estas topologías nos ayuda a entender mejor cómo viaja la información y cómo se mantiene la comunicación entre los dispositivos.

##### 3.2.1.1. Topología de Red Punto a Punto.

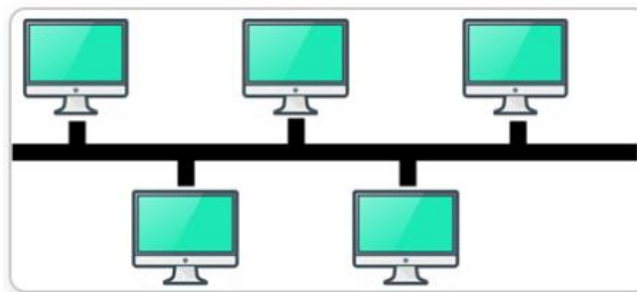
Una topología punto a punto conecta dos nodos directamente entre sí, también es conocida como "point to point", abreviadamente, PTP, es el modelo básico de la telefonía convencional. El nodo en un extremo coloca las ramas en los medios y el nodo en el otro extremo las saca de los medios del circuito punto a punto [3]. La topología punto a punto ofrece una forma eficiente y directa de transmitir información siendo ideal para conexiones específicas y controladas dentro de una red, pero presenta restricciones cuando se necesita ampliar la red o integrar más equipo; si uno de los dos dispositivos falla, la comunicación se interrumpe por completo.



*Figura 1: Topología de Red Punto a Punto*

### **3.2.1.2. Topología de Red en Bus.**

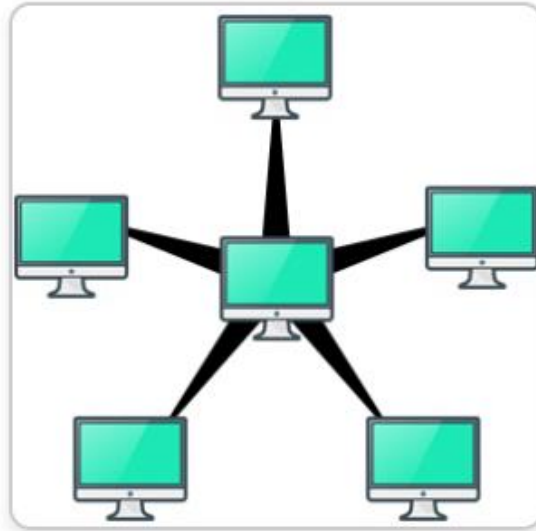
En la topología de bus todos los nodos o computadoras están conectados a un circuito común llamado bus. La información que se envía de una computadora a otra viaja directa o indirectamente, si existe un controlador que enruta los datos al destino correcto [3]. La topología en bus se utiliza principalmente en redes pequeñas, donde todos los dispositivos comparten un único medio de transmisión. Básicamente hay un cable principal al que se conectan los nodos y cada uno se encarga de enviar y recibir información, haciendo que los datos viajen por el cable hasta llegar al dispositivo de destino.



*Figura 2: Topología de Red en Bus*

### **3.2.1.3. Topología de Red en Estrella.**

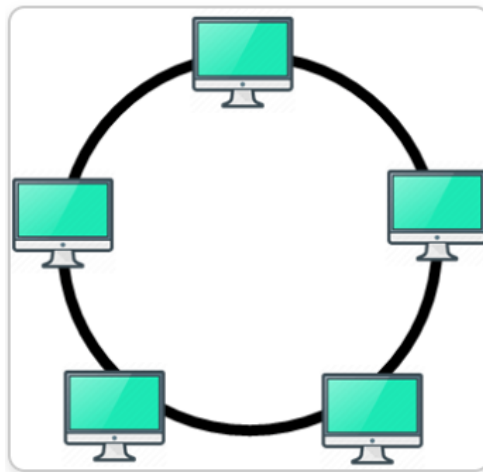
Reduce la posibilidad de fallo de red conectando todos los nodos a un nodo central. Cuando se aplica a una red basada en la topología estrella este concentrador central reenvía todas las transmisiones recibidas de cualquier nodo periférico a todos los nodos periféricos de la red, algunas veces incluso al nodo que lo envió [3]. Esta topología en estrella es muy útil porque permite que todos los dispositivos de red se conecten a un nodo central, lo que garantiza fiabilidad, escalabilidad y un control centralizado, siempre y cuando se cuente con un switch central redundante para reducir el riesgo de una caída total dentro del campus.



*Figura 3: Topología de Red en Estrella*

#### **3.2.1.4. Topología de Red de Anillo o Círculo.**

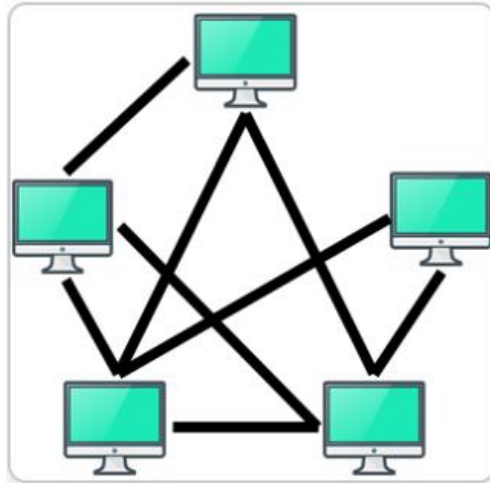
Una red en anillo es una topología de red en la que cada estación tiene una única conexión de entrada y otra de salida. Cada estación tiene un receptor y un transmisor que hace la función de traductor, pasando la señal a la siguiente estación [3]. La topología en anillo conecta los dispositivos de forma secuencial, de manera que los datos viajan en una sola dirección pasando por cada computadora o equipo hasta llegar a su destino. Para controlar la transmisión se utiliza un mecanismo llamado token, que permite que la información circule sin interferencias ni pérdidas, lo que hace que la red sea más organizada y confiable. Este tipo de red se utiliza mucho en redes de fibra óptica porque permite un control más ordenado del flujo de datos.



*Figura 4: Topología de Red en Anillo Círculo*

#### **3.2.1.5. Topología de Red en Malla**

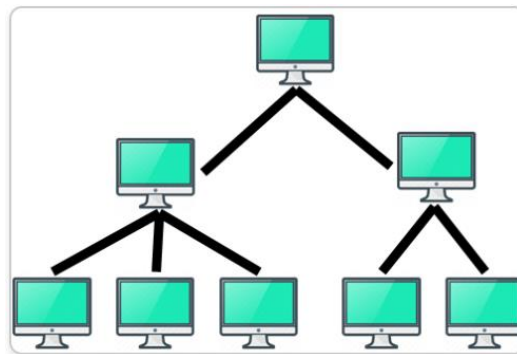
La topología de red en malla es una topología en la que cada nodo está conectado a todos los nodos. De esta manera es posible llevar los mensajes de un nodo a otro por distintos caminos [3]. La topología de red en malla conecta cada dispositivo o nodos están conectados directamente con más de un nodo, lo que crea diferentes caminos para enviar datos. Esto la hace muy confiable, porque si un enlace se daña, la información puede seguir circulando por otra ruta, y así la comunicación no se verá afectada.



*Figura 5: Topología de Red en Malla*

### 3.2.1.6. Topología de Red de Árbol

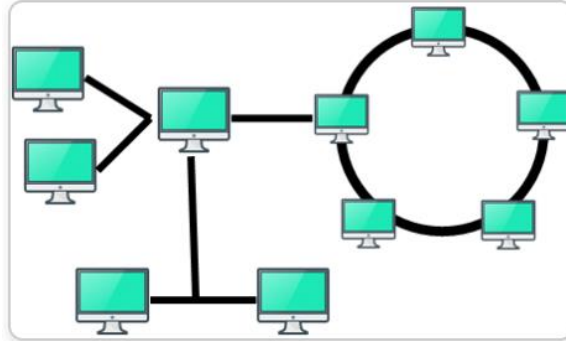
También conocida como topología jerárquica puede ser vista como una colección de redes en estrella ordenadas en una jerarquía. Este árbol tiene nodos periféricos individuales (por ejemplo, hojas) que requieren transmitir a y recibir de otro nodo solamente y no necesitan actuar como repetidores o regeneradores [3]. La topología en árbol, también llamado jerárquica, se organiza alrededor de un nodo principal, que suele ser un switch o un router, del cual dependen los nodos secundarios. De estos nodos se conectan las computadoras, impresoras o servidores, formando niveles que se pueden imaginar como varias redes en estrella ordenadas jerárquicamente. Se usan mucho en universidades y organizaciones grandes porque permite crecer la red fácilmente, mantenerla ordenada y que funcione de manera eficiente.



*Figura 6: Topología de Red en Árbol*

### 3.2.1.7. Topología de Red Híbrida o Mixta.

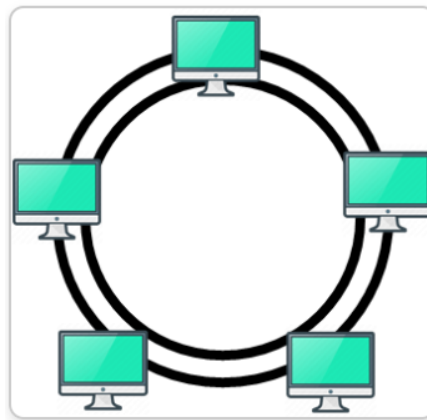
Topología híbrida, las redes pueden utilizar diversas tipologías para conectarse, como por ejemplo en estrella. La topología híbrida es una de las más frecuentes y se deriva de la unión de varios tipos de topologías de red, de aquí el nombre de híbridas [3]. La topología híbrida combina diferentes tipos de redes, como la topología de estrella - estrella, en árbol, bus - estrella. Es muy usada porque permite diseñar redes más flexibles y adaptarse a las necesidades de las organizaciones, aprovechando lo mejor de cada topología, aunque su implementación suele tener un costo más elevado debido a su complejidad de combinar varias topologías.



*Figura 7: Topología de Red Híbrida o Mixta.*

### 3.2.1.8. Topología de Red Doble Anillo.

Una topología en anillo doble consta de dos anillos concéntricos, donde cada Host de la red está conectado a ambos anillos, aunque los dos anillos no están conectados directamente entre sí [3]. La topología en anillo doble usa dos anillos que van uno dentro del otro, y cada computadora o dispositivo de la red está conectado a los dos al mismo tiempo. Aunque los anillos no se conectan entre sí, estos sirven para que, si la otra falla, pueda seguir transmitiendo la información. Esta configuración permite que los datos viajen en ambas direcciones mediante el paso de token, creando así redundancia y tolerancia a fallos. Aunque la topología doble anillo es más confiable que la topología de anillo simple, es más difícil de implementar, ya que requiere de más cableado y equipos, aumentando la complejidad y costos de instalaciones.



*Figura 8: Topología de Red Doble Anillo.*

### 3.3. Infraestructura de Red.

La infraestructura de red es una parte de la infraestructura de la TI que incluye el hardware, el software, los sistemas y los dispositivos que posibilitan el flujo de los datos en toda la empresa para conectar a los usuarios, los dispositivos, las aplicaciones y el Internet, entre otras cosas.

Sin una infraestructura de red ni prácticas de seguridad adecuadas, se podrían generar una mala experiencia para los usuarios y ataques a la red que perjudicarán la productividad y la eficiencia del personal. Para ofrecer un rendimiento predecible y una experiencia uniforme a los usuarios, deben contar con una infraestructura de red confiable, adaptable y centrada en la seguridad [4].

### **3.3.1. 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. Entre estos están: 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 partners y clientes [4].

Una infraestructura de red, segura y flexible es fundamental para que los sistemas digitales de hoy operen sin problemas. Para los usuarios, esto significa tener acceso confiable y protegido a lo que necesitan, evitando problemas como la pérdida de datos o intrusiones. Además, mejora cómo se usan los servicios en línea, ofreciendo conexiones más rápidas, estables y con menos demoras. A su vez, esto ayuda a los proveedores a ser más ágiles, adoptando soluciones de código abierto, mejorando la eficiencia en sus operaciones y adaptándose mejor a las nuevas tecnologías y a las exigencias del mercado.

### **3.3.2. 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. 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 [5].

Así mismo, en Cisco [6], destaca la planificación de la infraestructura de red en el campus universitario debe tener contemplado tanto el diseño de cableado como el inalámbrico, asegurando aspectos claves como la cobertura, seguridad, disponibilidad y escalabilidad, esto es indispensable para responder todas las necesidades actuales futuras de conectividad.

En una red de campus, tener una buena gestión de la red interna permite aplicar reglas de seguridad y control de todo lo que pasa dentro del campus, como quién puede conectarse y qué información se debe compartir. Este tipo de red tiene muchos puntos de conexión, porque cada edificio, laboratorio o aula necesita estar conectado. Por esta razón, se usa un sistema de cableado de alto rendimiento que pueden ser con cables de cobre o con fibra óptica.

En la actualidad, la mayoría de campus usa fibra óptica porque puede manejar mucho más ancho de banda, no presentan los problemas de los cables de cobre, ocupa menos espacio y es más rentable a largo plazo. Permite agregar nuevos sistemas o equipos de alto rendimiento sin tener cambios en toda la red, lo que da más flexibilidad a los usuarios y a los administradores.

#### **3.3.2.1. Ventajas de la seguridad del área de campus.**

Las redes de área de campus (CAN) presentan múltiples ventajas. Permiten una alta velocidad de transmisión de datos, alcanzando hasta 1 Mbps, lo que facilita la comunicación y efectividad entre dispositivos. Son también muy fiables, ya que pueden detectar y corregir errores de transmisión automáticamente, garantizando la integridad de la información. Además, su implementación y mantenimiento resulta relativamente económico, y su flexibilidad permite adaptarlas a diferentes aplicaciones y sistemas dentro del campus [7]. Las redes de campus, especialmente las inalámbricas, requieren de medidas de protección como cifrado, autenticación y control de acceso, para prevenir accesos no autorizados y garantizar la disponibilidad de los servicios.

#### **3.3.2.2. Desventajas de la seguridad del área de campus.**

Las redes de área de campus (CAN) también presentan algunas limitaciones. Una de ellas son las restricciones de distancia, ya que las señales se transmiten a través de un bus físico, lo que limita la separación máxima entre los dispositivos; en instalaciones que requieren mayor cobertura, se necesitan repetidores o extensores, lo que puede incrementar el costo [7].

### **3.4. Modelo de diseño Jerárquico.**

El modelo jerárquico permite organizar los diferentes componentes y niveles de red de manera estructurada, facilitando su administración, escalabilidad y confiabilidad. Este modelo desglosa la red en capas o grupos modulares, una jerarquía entre sí, y donde cada capa implementa una función específica, de esta manera se simplifica el diseño, administración e instalación de la red [2], [6].

#### **3.4.1. Modelo de Capa 3.**

El diseño de redes se utiliza el modelo de capa 3 como una forma organizada de estructurar la infraestructura. Este modelo divide la red en tres capas o niveles principales: donde se encuentran la capa de acceso, la capa de distribución y la capa de núcleo. Cada capa cumple una función específica que facilita la comunicación, el control de tráfico y la escalabilidad de red, logrando así un diseño más claro y eficiente.

Un diseño jerárquico incluye las siguientes 3 capas:

1. Capa de Acceso.
2. Capa de Distribución.
3. Capa núcleo (Core).

#### **Capa de Acceso:**

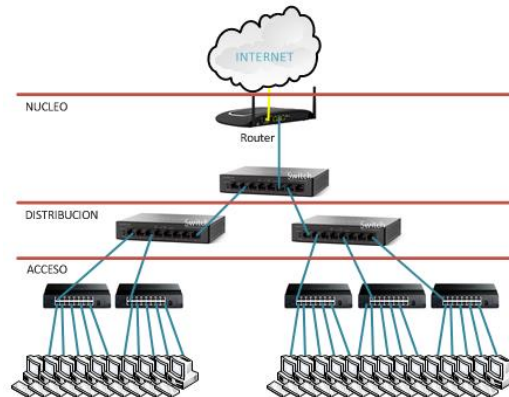
La capa de acceso permite a los dispositivos controlados por el usuario, dispositivos accesibles al usuario y otros dispositivos terminales conectarse en la red [6]. La capa de acceso es donde se conectan todos los equipos que usan los usuarios, como computadoras, impresoras, teléfonos IP, o incluso dispositivos móviles. Esta es la capa es la que permite que estos dispositivos puedan entrar y comunicarse dentro de la red.

#### **Capa de Distribución:**

La capa de distribución admite muchos servicios importantes. En una red donde la conectividad debe atravesar la LAN completa, ya sea entre distintos dispositivos de la capa de acceso o desde un dispositivo de la capa de acceso a la WAN [6]. La capa de distribución es la encargada de conectar y organizar todo el tráfico que viene desde la capa de acceso. Su función principal es permitir que los diferentes dispositivos de la red puedan comunicarse entre sí, sin importar en qué parte del campus o edificio estén ubicados. Esta capa es la que se encarga de enlazar la red local (LAN) con redes externas como WAN o internet.

#### **Capa Núcleo:**

Es una pieza fundamental de la red escalable y, aun así, es una de las más simples de diseñar [6]. La capa central dentro de una red es esencial porque garantiza que la comunicación sea rápida y confiable, permitiendo que la red pueda crecer sin perder eficiencia. Muchas veces es necesario usar varios switches de capa de distribución para que la red funcione mejor y sea más fácil de mantener, especialmente cuando los switches de acceso están en diferentes edificios, porque así se evita instalar mucha fibra óptica, que suele ser costosa. Por otro lado, contar con una capa de núcleo central hace que la red sea más ordenada, facilita la gestión de tráfico y permite agregar nuevos equipos o servicios en el futuro sin problemas.



**Figura 9: Modelo Jerárquico de Capa 3.**

### 3.5. Diseño Jerárquico.

Los diseños de LAN más grandes requieren una capa de distribución exclusiva para los servicios basados en la red frente a la necesidad de compartir la conectividad con los dispositivos de la capa de acceso. A medida que la densidad de los Routers WAN, los controladores WAAS, los dispositivos del perímetro de Internet y los controladores LAN inalámbricos crece, la capacidad de conectarse a un solo switch de la capa de distribución se hace difícil de administrar [6]. Cuando una red LAN crece mucho, ya no es suficiente que la capa de distribución solo comparta la conexión con los equipos de la capa de acceso. En estos casos, se necesita que esta capa se encargue de servicios más especializados de la red. Esto pasa porque mientras más aumenta la cantidad de dispositivos como: Routers para la conexión a la WAN, controladores de aplicaciones, equipos de seguridad en el perímetro de internet o controladores de redes inalámbricas, se vuelve más complicado administrarlos todos en un único switch. Por eso, la capa de distribución debe diseñarse de forma exclusiva para organizar este tipo de servicios y así mantener la red más estable y fácil de gestionar.

Existe una cantidad de factores que impulsan el diseño de red LAN con diversos módulos de capa de distribución:

1. La cantidad de puertos y ancho de banda del puerto que la plataforma de la capa de distribución puede proporcionar afecta el rendimiento y desempeño de la red.
2. La capacidad de recuperación de la red es un factor cuando todos los servicios LAN y basados en la red dependen de una única plataforma; independientemente del diseño de dicha plataforma, puede presentar un punto de falla único o un gran e inaceptable dominio de fallas.
3. La frecuencia y el control de cambios afectan a la capacidad de recuperación. Cuando todas las LAN, WAN y demás servicios de red se consolidan en una sola capa de distribución, los errores de configuración u operativos pueden afectar a todo el funcionamiento de la red.
4. La dispersión geográfica de los switches de acceso LAN entre distintos edificios en un campus más grande exigiría más interconexiones de fibra óptica a un núcleo fusionado único [6].

El modelo de capa tres puede aplicarse en nuevas propuestas para la infraestructura de red, ya que permite dividirla en niveles con funciones claras. Este enfoque hace que la red sea ordenada, estable y fácil de administrar, especialmente a medida crece la demanda tecnológica.

### 3.6. Administración de redes informáticas.

La administración de una red requiere de habilidades que permitan supervisar, comprobar, monitorizar y controlar los diversos componentes de hardware y software que la conforman, tanto locales como remotos [8]. La administración de redes se refiere al conjunto de actividades que se realizan para que una red funcione correctamente, manteniendo

un equilibrio entre eficiencia y seguridad. Para llevarlo a cabo, se necesitan conocimientos técnicos que permitan vigilar y comprobar el estado de los equipos y servicios que forman parte de la red.

Dentro de estas tareas están el monitoreo del tráfico, la supervisión de hardware como: switches, routers o servidores, y el control de software que gestiona la comunicación. Estas funciones no se limitan solo a los equipos locales, sino también a los que se encuentran conectados de forma remota.

El Subneteo, por ejemplo, es una técnica que permite dividir una red en subredes más pequeñas, facilitando la administración y optimizando el uso de los recursos.

**Subneteo de una red:** La función del Subneteo o Subnetting es dividir una red IP física en subredes lógicas (redes más pequeñas) para que cada una de ellas trabaje a nivel envío y recepción de paquetes como una red individual, aunque todas pertenezcan a la misma red física y al mismo dominio [9]. El Subneteo permite una mejor administración, control del tráfico y seguridad al segmentar la red por función. También mejora el rendimiento general, al reducir el tráfico de broadcast de nuestra red.

1. **Porción de Red:** En el caso que la máscara sea por defecto, una dirección con Clase, la cantidad de bits "1" en la porción de red, indican la dirección de red, es decir, la parte de la dirección IP que va a ser común a todos los hosts de esa red [9].
2. **Porción de Host:** La cantidad de bits "0" en la porción de host de la máscara, indican que parte de la dirección de red se usa para asignar direcciones de host, es decir, la parte de la dirección IP que va a variar según se vayan asignando direcciones a los hosts [9].

### 3.6.1. Tipos de Subneteo

1. **Subneteo Por clase:** genera una máscara común (fija) y una cantidad de hosts iguales a todas las subredes. Desaprovecha un gran número de direcciones.
2. **Subneteo de Máscara Variable VLSM:** (Variable Length Subnet Mask), toma una dirección de red o subred y la divide en subredes más pequeñas adaptando las máscaras según las necesidades de hosts de cada subred, generando una máscara diferente para las distintas subredes de una red [9].

### 3.7. Componentes de una red.

Los componentes de una red son los elementos que hacen que los dispositivos puedan comunicarse. Entre ellos se encuentran los dispositivos finales y los dispositivos intermedios, que cumplen funciones distintas dentro de la red. A continuación, se detalla estos dispositivos y cómo contribuyen al funcionamiento de la infraestructura de red.

#### 3.7.1. Dispositivos Finales.

Los dispositivos finales son los equipos que usamos los usuarios para conectarnos a la red y poder enviar o recibir información. Ejemplo de dispositivos finales podemos encontrar, las computadoras, laptops, impresoras. Son importantes porque representan el punto donde empieza o termina la comunicación dentro de la red.

##### 3.7.1.1. Servidor.

Es una computadora que, formando parte de una red, provee servicios a otras computadoras denominadas clientes. También se suele denominar con la palabra servidor a Una aplicación informática o programa que realiza algunas tareas en beneficio de otras aplicaciones llamadas clientes [10]. Un servidor es básicamente una computadora dentro de una red que se encarga de ofrecer servicios o recursos a otras computadoras, que se conocen como clientes. Estos servicios pueden ser muy variados, como almacenar archivos, administrar correo electrónico, manejar bases de datos o permitir el acceso a aplicaciones.



*Figura 10: Servidor.*

### **3.7.1.2. Estación de trabajo.**

Cuando una computadora se conecta a una red, la primera se convierte en un nodo de la última y se puede tratar como una estación de trabajo o cliente. Las estaciones de trabajo pueden ser computadoras personales, se encargan de sus propias tareas de procesamiento, así que cuanto mayor y más rápido sea el equipo, mejor [10]. Cuando una computadora se une a una red, automáticamente pasa a formar parte de ella y se considera un nodo. Este nodo puede funcionar como cliente o estación de trabajo, básicamente es una computadora dentro de la red que utiliza los recursos disponibles o que cumplen con ciertas funciones. Las estaciones de trabajo, como suelen ser computadoras personales, no dependen totalmente de la red para hacer procesos, sino que cada una realiza sus propias tareas.



*Figura 11: Estación de Trabajo.*

### **3.7.2. Dispositivos Intermedios.**

Los dispositivos intermedios son aquellos equipos que se encargan de dirigir y controlar cómo circula la información de datos dentro de la red. No los usamos como dispositivos finales, pero son muy importantes para que la información llegue al lugar correcto. Los ejemplos de dispositivos intermedios son los switches, Routers y firewalls, que ayudan a conectar los diferentes equipos, organizar el tráfico, asegurar que la comunicación sea eficiente y proteger la red de accesos no autorizados.

### 3.7.2.1. Repetidores.

Es un dispositivo electrónico que recibe una señal débil o de bajo nivel y la retransmite a una potencia o nivel más alto, de tal modo que se puedan cubrir distancias más largas sin degradación o con una degradación tolerable [10]. Un repetidor es un dispositivo de red que se utiliza cuando la señal empieza a perder fuerza debido a la distancia que recorre por el cableado o el medio de transmisión. Su función es recibir esa señal ya debilitada y volver a enviarla con más potencia, de modo que puede seguir transmitiendo sin perder calidad. Esto permite que la red cubra distancias más grandes sin que los datos lleguen dañados o se pierdan.



*Figura 12: Repetidor*

### 3.7.2.2. Bridges

Es un dispositivo de interconexión de redes de ordenadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Este interconecta dos segmentos de red (o divide una red en segmentos) haciendo el pasaje de datos de una red hacia otra, con base en la dirección física de destino de cada paquete [10]. Este dispositivo sirve para conectar dos segmentos de una misma red y permite que la información pase de un lado a otro. Trabaja en la capa 2 del modelo OSI, que es la capa de enlace de datos, y toma como referencia la dirección física MAC de cada paquete para decidir si lo deja pasar o no. El bridges o puente ayudan a gestionar y controlar el tráfico dentro de la red, evitando que haya demasiada congestión y haciendo más eficiente la comunicación.

**Se distinguen dos tipos de bridge:**

- **Locales:** sirven para enlazar directamente dos redes físicamente cercanas.
- **Remotos o de área extensa:** se conectan en parejas, enlazando dos o más redes locales, formando una red de área extensa, a través de líneas telefónicas.



*Figura 13: Bridges*

### 3.7.2.3. Switch.

Es un dispositivo digital de lógica de interconexión de redes de computadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes (bridges), pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red

[10]. Un switch es esencial para una infraestructura de red, porque garantiza seguridad y escalabilidad frente a tecnologías obsoletas. La función principal de los switches es conectar múltiples dispositivos a la LAN, que permite el intercambio de información eficiente segura y ordenada.



*Figura 14: Switch*

#### **3.7.2.4. Routers**

Es un enrutador, elemento que marca el camino más adecuado para la transmisión de mensajes en una red completa, esta toma el mejor camino para enviar los datos dependiendo del tipo de protocolo que esté cargado, cuenta con un procesador es el más robusto, tiene más procesadores y mucha más capacidad en sus respectivas memorias [10]. La función de los Routers es dirigir el tráfico de datos entre redes para que la información llegue al destino, ya que son el pilar de la conectividad interna y externa de un campus universitario o entidad, con la implementación de Routers se tendrá una infraestructura de red moderna escalable y confiable.



*Figura 15: Routers*

#### **3.7.2.5 Brouters**

Es un dispositivo de interconexión de redes de computadores que funciona como un bridge (puente de red) y como un enrutador. Un Brouters puede ser configurado para actuar como bridge para parte del tráfico de red, y como enrutador para el resto [10]. Es un dispositivo de red que combina las funciones de un bridge o de un Router, que puede trabajar como bridges, conectando segmentos de red y permitiendo que los datos pasen entre ellos basándose en direcciones MAC, también trabaja como Router, que dirige el tráfico de red utilizando direcciones IP.



*Figura 16: Routers*

### **3.7.2.6. Firewall.**

Es un elemento de seguridad que filtra el tráfico de red que a él llega, con un cortafuegos se puede aislar un ordenador de todos los otros ordenadores de la red excepto de uno o varios que son los que nos interesa que puedan comunicarse con él [10]. Es un sistema de seguridad de redes. Su función es controlar y filtrar el tráfico de datos que entra o sale dentro de un ordenador o red completa, basándose en las reglas que se configuran previamente. Con un firewall se puede decidir qué equipos o aplicaciones tienen permiso para comunicarse y cuáles no.



*Figura 17: Firewall*

### **3.7.3. Medios de comunicación dentro de las redes.**

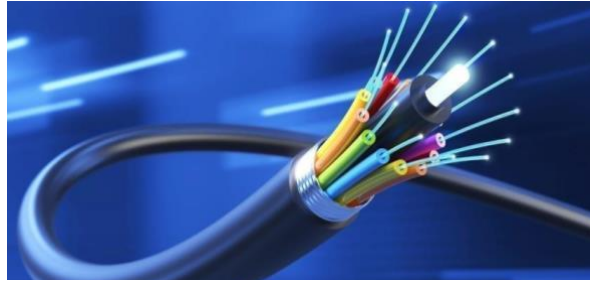
Los medios de comunicación constituyen el soporte a través del cual se transmite la información entre dos o más dispositivos. De manera general, los medios de transmisión o comunicación se dividen en medios guiados y no guiados. Los guiados hacen uso de canales físicos, como el cobre o la fibra óptica y los no guiados emplean espacios libres como medio de propagación, utilizando ondas electromagnéticas para transportar la información.

La elección de los medios de comunicación guiados o no guiados depende de factores como la distancia de transmisión, el ancho de banda requerido, el costo de implementación y el nivel de interferencia ambiental al que esté expuesto el sistema.

#### **3.7.3.1. Medios de Comunicación Guiados.**

##### **3.7.3.1.1. Conexión fibra óptica**

Permite transmitir la información a gran velocidad e impide la intervención de las líneas, como la señal es transmitida a través de luz, existen muy pocas posibilidades de interferencias eléctrica o emisión de señal, el cable consta de dos núcleos ópticos, uno interno y otro externo, que refractan la luz de forma distinta [10]. Es un medio de transmisión muy rápido y seguro. A diferencia de los cables tradicionales de cobre, la fibra óptica no transmite señal en forma eléctrica. La fibra óptica envía la información a gran velocidad, y está formado por dos núcleos: uno interno por donde viaja la luz con la información, y el otro externo que la refracta de manera diferente para mantenerla dentro del núcleo principal. Gracias a esta estructura la señal se conserva clara y puede recorrer largas distancias sin perder calidad.



**Figura 18: Conexión Fibra Óptica.**

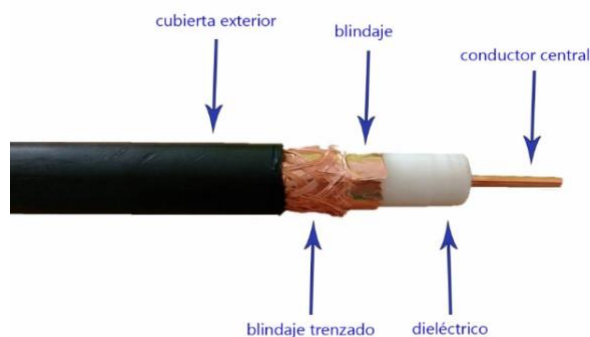
La fibra está encapsulada en un cable protector, ofrece las siguientes ventajas:

1. Alta velocidad de transmisión
2. No emite señales eléctricas o magnéticas, lo cual redundo en la seguridad
3. Inmunidad frente a interferencias y modulación cruzada.
4. Mayor economía que el cable coaxial en algunas instalaciones.
5. Soporta mayores distancias.

#### **3.7.3.1.2. Cable Coaxial.**

Un cable coaxial consiste en un alambre de cobre rígido como núcleo rodeado por un material aislante. El aislante está forrado con un conductor cilíndrico, que con frecuencia es una malla de tejido fuertemente trenzado. El ancho de banda posible depende de la calidad y longitud del cable, y de la relación señal a ruido de la señal de datos. Los cables modernos tienen un ancho de banda de cerca de 1 GHz. Los cables coaxiales solían ser ampliamente usados en el sistema telefónico para las líneas de larga distancia, pero en la actualidad han sido reemplazados por la fibra óptica en rutas de distancias considerables. Sin embargo, el cable coaxial aún se utiliza ampliamente en la televisión por cable y en las redes del área metropolitana. El cable coaxial para enviar datos, voz o videos, este cable está diseñado con varias capas que lo hacen eficiente y resistente a interferencias externas [11].

El centro tiene un alambre de cobre rígido, que funciona como núcleo y es el que transporta directamente la señal eléctrica. Este cable está rodeado por un material aislante, cuya función es proteger la señal para que no se pierda ni se mezcle con ruidos. Después lleva una cubierta de conductor cilíndrico, que suele ser una malla metálica trenzada, esta malla actúa como como blindaje reduciendo las interferencias externas y garantizando que la señal llegue con mejor calidad. El cable coaxial se usaba en líneas telefónicas de larga distancia, pero fue reemplazado por la fibra óptica, ya que esta última permite transmitir más datos con mayor velocidad y a mayores distancias sin pérdidas.

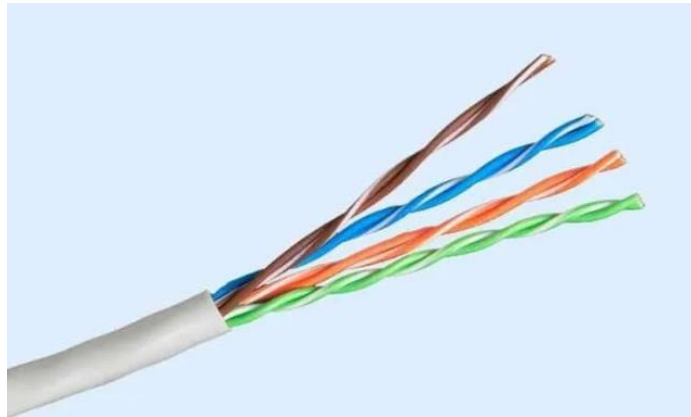


**Figura 19: Cable Coaxial.**

### 3.7.3.1.3. Par trenzado.

La aplicación más común del cable de par trenzado es en el sistema telefónico. Casi todos los teléfonos están conectados a la compañía telefónica mediante un cable de par trenzado. Los cables de par trenzado se pueden utilizar para transmisión tanto analógica como digital. El ancho de banda depende del grosor del cable y de la distancia que recorre; en muchos casos pueden obtenerse transmisiones de varios megabits/seg, en distancias de pocos kilómetros [11].

El par trenzado es uno de los más utilizados en telecomunicaciones y redes de computadoras. Este tipo de cable se compone de dos hilos de cobre entrelazados en forma de espiral, lo cual ayuda a reducir las interferencias externas y mantener la calidad de la señal. Una de las ventajas es que puede transmitir tanto señales analógicas, como señales digitales. En condiciones adecuadas el cable de par trenzado puede alcanzar transmisiones de varios megabits por segundos en distancia de algunos kilómetros.



*Figura 20: Par Trenzado.*

### 3.7.3.2. Medios de Comunicación No Guiados.

#### 3.7.3.2.1. Radiotransmisores.

Las ondas de radio son fáciles de generar, pueden viajar distancias largas y penetrar edificios sin problemas, y por ello su uso está muy generalizado en la comunicación, tanto en interiores como en exteriores. Las ondas de radio también son omnidireccionales, lo que significa que viajan en todas direcciones a partir de la fuente, por lo que no es necesario que el transmisor y el receptor se encuentren alineados físicamente [11].

La radiotransmisión es una forma de transmisión que funciona con ondas de radio para enviar información sin necesidad de cables. Un transmisor toma la señal (puede ser voz, datos o incluso videos) las convierte en ondas electromagnéticas y las envía al espacio. Estas ondas tienen la ventaja de recorrer largas distancias, pasar a través de edificios y propagarse en todas las direcciones. Por lo que no es obligatorio que el emisor y el receptor estén alineados.

#### 3.7.3.2.2. Transmisión por microondas

Por encima de los 100 MHz las ondas viajan en línea recta y, por lo tanto, se pueden enfocar en un haz estrecho. Concentrar toda la energía en un haz pequeño con una antena parabólica (como el tan familiar plató de televisión por satélite) produce una relación señal a ruido mucho más alta, pero las antenas transmisora y receptora deben estar bien alineadas entre sí [11].

La transmisión por microondas se utiliza cuando se trabaja con frecuencias mayores a los 100 MHz, ya que en este rango las ondas viajan de manera recta. esto permite dirigir las ondas en forma de un haz estrecho, usando antenas especiales, como las parabólicas que vemos en la televisión satelital. Al encontrar la señal en un haz tan preciso, se logra una mejor calidad de transmisión, ya que la energía no se dispersa y se obtiene una relación señal/ruido más alto.

### **3.7.3.2.3. Ondas infrarrojas y milímetros.**

Las ondas infrarrojas y milimétricas no guiadas se usan mucho para la comunicación de corto alcance. Todos los controles remotos de los televisores, grabadoras de vídeo y estéreos utilizan comunicación infrarroja. Estos controles son relativamente direccionales, económicos y fáciles de construir, pero tienen un inconveniente importante: no atraviesan los objetos sólidos. En general, conforme pasamos de la radio de onda larga hacia la luz visible, las ondas se comportan cada vez más como la luz y cada vez menos como la radio [11].

Estas ondas infrarrojo milimétricas, se usan en comunicaciones de corto enlace, siendo un ejemplo claro de los controles remotos de televisores, equipos de sonido o grabadoras, estos dispositivos funcionan como señal infrarroja, que son fáciles de implementar de bajo costo y bastante confiable, aunque requiere apuntar en la dirección del receptor, ya que no pueden atravesar objetos sólidos. Un detalle interesante es que a medida avanzamos en el espectro electromagnético desde las ondas de radio de gran longitud hasta la luz visible, las ondas empiezan a comportarse más como luz.

### **Transmisión por onda de luz.**

Una aplicación más moderna es conectar las VLANs de dos edificios por medio de láseres montados en sus azoteas. La señalización óptica coherente con láseres es inherentemente unidireccional, de modo que cada edificio necesita su propio láser y su propio fotodetector. Este esquema ofrece un ancho de banda muy alto y un costo muy bajo. También es relativamente fácil de instalar y, a diferencia de las microondas, no requiere una licencia de la FCC [11].

Transmisión por ondas de luz, consiste en usar láseres para enviar datos de un edificio a otro, sin necesidad de un cable. Por lo general, los láseres se instalan en las azoteas y funcionan como un enlace directo entre dos redes. Como la señal láser es coherente y direccional, no puede viajar en ambas direcciones en el mismo haz, por lo que cada edificio debe tener su propio láser transmisor y un fotodetector receptor para poder comunicarse de manera bidireccional.

### **Satélites de Comunicación**

Los satélites de comunicaciones tienen algunas propiedades interesantes que los hacen atractivos para muchas aplicaciones. En su forma más simple, un satélite de comunicaciones se puede considerar como un enorme repetidor de microondas en el cielo. Contiene numerosos transpondedores, cada uno de los cuales se encarga de una parte del espectro, amplifica la señal entrante y a continuación la retransmite en otra frecuencia para evitar interferencia con la señal entrante [11].

Un satélite de comunicación funciona como un repetidor que está en el espacio. Lo que hace es recibir señales de microondas que vienen desde la tierra, luego las amplía para que no se pierda la información y después las envía de nuevo, pero usando otra referencia para que no haya referencia con la señal que recibió al inicio.

### **3.7.4. Sistemas Operativos**

En el software de red se incluyen programas relacionados con la interconexión de equipos informáticos, es decir, programas necesarios para que las redes de computadoras funcionen. Entre otras cosas, los programas de red hacen posible la comunicación entre las computadoras, permiten compartir recursos (software y hardware) y ayudan a controlar la seguridad de dichos recursos [10]. Los softwares utilizados para la implementación de una red de campus son fundamentales ya que de ella depende la estabilidad, seguridad y eficiencia de toda la transmisión de datos. El software de red es la primera línea de defensa de ciberataque y si no cumple con estándares de calidad toda la información de dicha red podría ser vulnerada permitiendo accesos no permitidos, robo de datos o ataques de denegación de servicio.

#### 4. ANÁLISIS DE INFRAESTRUCTURA ACTUAL.

##### 4.1. Inventario de equipo de DataCenter.

El data center de la Universidad de El Salvador, Facultad Multidisciplinaria Oriental es el corazón de la infraestructura tecnológica de la institución, ya que ahí se encuentran los equipos de red más importante que permiten mantener la conectividad, la seguridad y la disponibilidad de distintos servicios. En este espacio se concentran equipos de alto rendimiento, preparados para responder a la creciente demanda de tráfico de datos y al uso simultáneo que hacen estudiantes, docentes y personal administrativo.

Dentro del inventario se incluyen controladores de red, switches de acceso y distribución, routers de núcleo, firewall de última generación y sistemas de protección Anti DDos, siendo la mayoría de marcas reconocidas como Huawei y Cisco. Los equipos analizados en este inventario evidencian que probablemente existen cuellos de botella en la infraestructura, derivados de la limitada disponibilidad de equipos destinados a la redundancia.

*Tabla 1: Inventario de Equipos de Red en el DataCenter.*

Nº	Marca/modelo	Nº Serie	Tipo de equipo	SO/Firmware	Ip/Subred	Conectividad
1	HUAWEI AirEngine9700- M1_6F0DD791	1021C6034988	AC (Access controller)	N/D	172.17.24.X:180 08	N/D
2	HUAWEI Wireless LAN AirEngine9700 M1	1021C6034988	AC	N/D	172.17.60.X MGMT 10.60. 100.CAPWAP	N/D
3	HUAWEI MGDC Edge USG6610E-01	1021C0011920	Firewall	N/D	172.17.60.X:844 3	N/D
4	HUAWEI SMGDCEdgeF W USG6610E- 01	1021C0011919	Firewall	N/D	172.17.60.X	N/D
5	HUAWEI SMIdgeN 8KM 1A	2102353HFW1 0MC100068	Router	Huawei VRP	172.17.60.X/loo k: 172.17.62.X	N/D
6	HUAWEI SMIdgeN 8KM 1A	2102353HFW1 0MC100070	Router	Huawei VRP	172.17.60.X/loo k: 172.17.62.X	N/D
7	HUAWEI S1905	1021C0011654	AntiDDoS	N/D	172.17.60.X	N/D
8	HUAWEI S1905	1021C0011651	AntiDDoS	N/D	172.19.29.X	N/D
9	HUAWEI S5736-	N/D	Switch de Acceso	Huawei VRP	172.16.0.X/24	N/D

	S24UM4XC					
10	CISCO CONTROLADORA	FCL240200U2	Controlador wifi	Cisco IOS XE	172.16.16.X	HUAWEI S5735-L48T4X-A (Data center)
11	CISCO C9800-L-F-K9	FCL240200U2	Controlador wifi	Cisco IOS XE	172.16.16.X	HUAWEI S5735-L48T4X-A (Data center)
12	CISCO 9800—L-F	N/D	Controlador wifi	Cisco IOS XE	172.16.0.X/24	N/D
13	HUAWEI S6730-H48X6C	102010022304	Switch de distribución	Huawei VRP	192.168.10.X	Conectado a firewall
14	CISCO CATALYST 3850	N/D	Servidor	Cisco IOS XE	192.168.10.X/24	HUAWEI S6730-H48X6C (Data center, Switch Distribucion)
15	HUAWEI S5735-L48T4X-A	21980109364E LC008422	Servidor	Huawei VRP	192.168.10.X/24	HUAWEI S6730-H48X6C (Data center, Switch Distribución)
16	HUAWEI S5736-S24UM4XC	3G21C0046597	Switch de acceso	Huawei VRP	172.19.29.X	N/D

#### 4.2. Inventario de Oficinas de Coordinación y Dirección

La siguiente tabla presenta el inventario de switches instalados en las oficinas de coordinación y dirección. En ella se detallan las principales características técnicas y de ubicación de cada dispositivo, con el objetivo de facilitar su identificación, control y gestión dentro de la infraestructura de red.

**Tabla 2: Oficinas de Coordinación y Dirección.**

Nº	Marca/modelo	Nº Serie	Tipo de equipo	SO/Firmware	Ip/Subred	Conectividad	Ubicación
1	HUAWEI S5735-L48T4X-A	21980109364ELC008270	Switch de acceso	HUAWEI S5735-L48T4X-A	192.168.10.X/24	HUAWEI S6730-H48X6C (Data center)	Decanato

2	HUAWEI S1720-52GWR-4X	21980106112SK5600081	Switch de acceso	Huawei VRP	192.168.10.X/24	N/D	Académica
3	CISCO SF200-24	219801A2A59242Q0000D	Switch de acceso	Cisco Small Business Firmware	192.168.10.X/24	HUAWEI S5735-L48T4X-A (Decanato)	Financiera 1
4	D'LINK DE-1210	F3XZ4FC001381	Switch de acceso	N/D	192.168.10.X/24	HUAWEI S1720-52GWR-4X (Cómputo UESED)	Oficina UESED
5	CISCO SF200-24	DNI223405HG	Switch de acceso	Cisco Small Business Firmware	192.168.10.X/24	CISCO SF200-24 (Financiera 1)	Financiera 2
6	HUAWEI S5736-S24UM4XC	3G21C0046822	Switch de acceso	Huawei VRP	172.19.29.X	Conectado a switch de acceso de edificio de aulas minerva	Jefatura de medicina 1
7	HUAWEI S5736-S24UM4XC	3G21C0046849	Switch acceso	Huawei VRP	172.19.29.X	HUAWEI S5736-S24UM4XC (Jefatura medicina 1)	Jefatura de medicina 2
8	HUAWEI S5736-S24UM4XC	3G21C0046537	Switch de acceso	Huawei VRP	172.19.29.X	N/D	Edificio Riñón 1
9	HUAWEI S5736-S24UM4XC	3G21C0046507	Switch de acceso	Huawei VRP	172.19.29.X	N/D	Edificio Riñón 2
10	HUAWEI S5736-S24UM4XC	3G21C0046511	Switch de acceso	Huawei VRP	172.19.29.X	Conectado a switch de acceso de Financiera 1	Unidad financiera
11	HUAWEI S5736-S24UM4XC	3G21C0046616	Switch de acceso	Huawei VRP	172.19.29.X	N/D	Vicedecanato
12	HUAWEI S5736-S24UM4XC	3G21C0046616	Switch de acceso	Huawei VRP	172.19.29.X	N/D	Oficinas de administración académica

### 4.3. Inventario por Departamentos y Aulas.

El inventario por departamento y aulas permite documentar y organizar equipos de red de acuerdo con su ubicación física y su función en la infraestructura de red. Este registro muestra datos esenciales como marcas y modelos, número de serie, tipo de equipos, sistema operativo, las direcciones IP, su conectividad y ubicación. De esta manera, se

garantiza un control eficiente de los dispositivos instalados, logrando facilitar la gestión del mantenimiento, la actualización tecnológica y la rápida identificación en casos de incidencia. De igual modo, este inventario contribuye a la planificación de red y a la seguridad informática, ya que ofrece una visión clara de donde se encuentran distribuidos los equipos en cada área académica y administrativa. Cabe señalar, que algunos casos, el campo de conectividad no muestra información detallada, ya que no todos los equipos tienen una relación documentada en la topología general de la red o funcionan de manera aislada en departamentos específicos.

**Tabla 3: Departamentos Administrativos**

N°	Marca/modelo	N° Serie	Tipo de equipo	SO/Firmware	IP/Subred	Conectividad	Ubicación
1	HUAWEI S1720-52GWR-4X	1980106112SK5600071	Switch de distribución	Huawei VRP	192.168.10.X/24	HUAWEI S6730-H48X6C (Data center)	Educación
2	HUAWEI S1720-52GWR-4X	21980106112SK5600010	switch de acceso	Huawei VRP	192.168.10.X/24	HUAWEI S1720-52GWR-4X(Educación)	Educación
3	HUAWEI S6730-H48X6C	N/D	Switch de acceso	Huawei VRP	192.168.10.X/24	HUAWEI S1720-52GWR-4X	Economía
4	HUAWEI S6730-H48X6C	21980106112SK5600072	Switch de acceso	Huawei VRP	192.168.10.X/24	Conectado al switch de acceso de Edificio de aulas minerva	Matemática
5	HUAWEI S6730-H48X6C	21980106112SK5600042	Switch de acceso	Huawei VRP	192.168.10.X/24	HUAWEI S1720-52GWR-4X(Química)	Agronomía
6	CISCO WS-C2960X-48TSL	N/D	Switch de acceso	Cisco IOS	192.168.10.X/24	HUAWEI S6730-H48X6C(matemática)	Biología
7	HUAWEI S5735-L48T4XA	21980109364ELC008861	Switch de acceso	Huawei VRP	192.168.10.X/24	N/D	Postgrado
8	HUAWEI S1720-52GWR-4X	21980106112SK5600042	Switch de acceso	Huawei VRP	192.168.10.X/24	N/D	Medicina
9	HUAWEI S1720-52GWR-	21980106112SK5	Switch de acceso	Huawei VRP	192.168.10.X/24	N/D	CC jurídica

	4X	600072					
10	HUAWEI S1720-52GWR- 4X	2198010 6112SK5 600025	Switch de acceso	Huawei VRP	192.168.10 .X/24	HUAWEI S5736- S24UM4XC (Administración Académica)	Química
11	HUAWEI S1720-52GWR- 4X	2198010 6112SK5 600004	Switch de acceso	Huawei VRP	192.168.10 .X/24	HUAWEI S6730- H48X6C (Data center)	Ingeniería
12	TP-LINK TL- SG3452P	Y227022 000412	Switch de acceso	TP Link JetStream OS	192.168.10 .X/24	HUAWEI S1720- 52GWR- 4X(Educación )	Sociología
13	HUAWEI S5736- S24UM4XC	3G21C00 46639	Switch de acceso	Huawei VRP	172.19.29. X	HUAWEI S6730- H48X6C(Mate mática)	Biología
14	HUAWEI S5736- S24UM4XC	3G21C00 46622	Switch de acceso	Huawei VRP	172.19.29. X	HUAWEI S6730- H48X6C(Mate mática)	Física
15	HUAWEI S5736- S24UM4XC	3G21C00 46603	Switch de acceso	Huawei VRP	172.19.29. X	HUAWEI S5736- S24UM4XC (Administración Académica)	Ciencias jurídicas
16	HUAWEI S5736- S24UM4XC	3G21C00 46860	Switch de acceso	Huawei VRP	172.19.29. X	HUAWEI S6730- H48X6C (Data center)	Postgrado

*Tabla 4: Aulas de Clases*

Nº	Marca/modelo	Nº Serie	Tipo de equipo	SO/Firmware	IP/Subred	Conectividad	Ubicación
1	HUAWEI S1720-52GWR- 4X	219801061 12SK5600 056	Switch de acceso	Huawei VRP	192.168.10 .X/24	HUAWEI S6730- H48X6C (Data center)	Cómputo UESED

2	CISCO SF200-24	N/D	Switch de acceso	Cisco Small Business Firmware	192.168.10.X/24	Conectado a switch acceso de Posgrado	Aulas de economía
3	HUAWEI S1720-52GWR-4X	21980106112SK5600074	Switch de acceso	Huawei VRP	192.168.10.X/24	HUAWEI S1720-52GWR-4X(Educación)	Edificio minerva
4	CISCO SF200-24	DNI 204302 BG	Switch de acceso	Cisco Small Business Firmware	192.168.10.X/24	N/D	Sala de internet
5	HUAWEI S5735-L24T4X-A	2S2180007582	Switch de acceso	Huawei VRP	92.168.10.X	HUAWEI S6730-H48X6C(Matemática)	Aulas inglés
6	HUAWEI S5735-L24T4X-A	2S2180007714	Switch de acceso	Huawei VRP	192.168.10.X/24	N/D	Aulas educación
7	HUAWEI S5735-L24T4X-A	2S2180007811	Switch de acceso	Huawei VRP	192.168.10.X/24	HUAWEI S5735-L24T4X-A (Aulas educación)	Aulas ingeniería
8	HUAWEI S5735-L24T4X-A1	2S2180007728	Switch de acceso	Huawei VRP	192.168.10.X/24	HUAWEI S6730-H48X6C(Agronomía)	Aulas Agronomía
9	HUAWEI S5731-S24P4X	N/D	Switch de acceso	Huawei VRP	192.168.10.X/24	N/D	Edificio minerva
10	HUAWEI S5731-S24P4X	N/D	Switch de acceso	Huawei VRP	192.168.10.X/24	N/D	Edificio minerva
11	HUAWEI S5731-S24P4X	DM22B0020628	Switch de acceso	Huawei VRP	192.168.10.X/24	N/D	Aula CCJJ
12	HUAWEI S5731-S24P4X	102285825322	Switch de acceso	Huawei VRP	192.168.10.X/24	HUAWEI S6730-H48X6C (Data center)	Aulas sociología
13	HUAWEI S5736-S24UM4XC	3G21C0046776	Switch de acceso	Huawei VRP	172.19.29.X	HUAWEI S5735-L24T4X-A (Aulas educación)	Aulas ingeniería
14	HUAWEI S5736-S24UM4XC	3G21C0046782	Switch de acceso	Huawei VRP	172.19.29.X	N/D	Aula 30 economía

15	HUAWEI S5736-S24UM4XC	3G21C004 6543	Switch de acceso	Huawei VRP	172.19.29.X	N/D	Minerva
16	HUAWEI S5736-S24UM4XC	3G21C004 6594	Switch de acceso	Huawei VRP	172.19.29.X	HUAWEI S6730-H48X6C(Matemática)	Aulas ingles
17	HUAWEI S5736-S24UM4XC	3G21C004 6598	Switch de acceso	Huawei VRP	172.19.29.X	HUAWEI S6730-H48X6C(Agronomía)	Aulas de Agronomía
18	HUAWEI S5736-S24UM4XC	3G21C004 6620	Switch de acceso	Huawei VRP	172.19.29.X	N/D	Aulas de educación

**Tabla 5: Laboratorios**

Nº	Marca/modelo	Nº Serie	Tipo de equipo	SO/Firmware	Ip/Subred	Conectividad	Ubicación
1	HUAWEI S5736-S24UM4XC	3G21C0046 851	Switch de acceso	Huawei VRP	172.19.29.X	N/D	Lab. de química
2	CISCO SF200-24	DNI 22110 F 39	Switch de acceso	Cisco Small Business Firmware	192.168.10.X/24	HUAWEI S1720-52 GWR-4X (Cómputo UESED)	Cómputo redes 1
3	CISCO SF200-24	DNI22110F5 E	Switch de acceso	Cisco Small Business Firmware	192.168.10.X/24	HUAWEI S1720-52 GWR-4X (Cómputo UESED)	Cómputo redes 2
4	CISCO SF200-24	PSZ21471M LU	Switch de acceso	Cisco Small Business Firmware	192.168.10.X/24	HUAWEI S1720-52 GWR-4X (Cómputo UESED)	Cómputo redes 3
5	HUAWEI S5735-L48T4X-A	2198010936 4ELC00886 1	Switch de acceso	Huawei VRP	192.168.10.X/24	HUAWEI S5736-S24UM4XC (Ciencias jurídicas)	Simulación y audiencia
6	HUAWEI S5736-S24UM4XC	3G21C0046 595	Switch de acceso	Huawei VRP	172.19.29.X	Conectado a switch de acceso cómputo A	laboratorio de redes

**Tabla 6: Biblioteca.**

C	Marca/modelo	N° Serie	Tipo de equipo	SO/Firmware	Ip/Subred	Conectividad	Ubicación
1	DAHUA DH-S5600-48GT4XF	219801A2 A59242Q0 004C	Switch de acceso	Dahua Switch OS	192.168.10.X/24	HUAWEI S6730-H48X6C (Data center)	Servicios al público
2	HUAWEI S5736-S24UM4XC	3G21C004 6630	Switch de acceso	Huawei VRP	172.19.29.X	N/D	Sala de estudio biblioteca

**Tabla 7: Servicios Generales.**

N°	Marca/modelo	N° Serie	Tipo de equipo	SO/Firmware	Ip/Subred	Conectividad	Ubicación
1	CISCO SG350-10	N/D	Switch de acceso	Cisco Small Business Firmware	192.168.10.X/24	HUAWEI S6730-H48X6C(Economía)	Bodega
2	CISCO SF200-24	DNI22340 5HN	Switch de acceso	Huawei VRP	192.168.10.X/24	HUAWEI S5736-S24UM4XC(Switch Auditorio)	Vigilancia estacionamiento
3	JETSTREAM TL-SG3452P	Y2270A5 000027	Switch de acceso	JetStream OS	192.168.10.X/24	Conectado a switch de acceso de edificio minerva	Caseta vigilancia
4	HUAWEI S5736-S24UM4XC	3G21C004 6506	Switch de acceso	Huawei VRP	172.19.29.X	N/D	Bodega medicina 2
5	HUAWEI S5736-S24UM4XC	3G21C004 6499	Switch de acceso	Huawei VRP	172.19.29.X	N/D	Bodega medicina 1
6	HUAWEI S5736-S24UM4XC	3G21C004 6633	Switch de acceso	Huawei VRP	172.19.29.X	N/D	Auditorium 1 Patch panel 2
7	HUAWEI S5736-S24UM4XC	3G21C004 6580	Switch de acceso	Huawei VRP	172.19.29.X	HUAWEI S6730-H48X6C (Data Center, Switch Distribución)	Auditorium 1 Patch panel 1

**Tabla 8: Servicios Estudiantiles.**

Nº	Marca/modelo	Nº Serie	Tipo de equipo	SO/Firmware	IP/Subred	Conectividad	Ubicación
1	CISCO SF200-24	DNI 204002 CC	Switch de acceso	Cisco Small Business Firmware	192.168.10 .X/24	Conectado a switch de acceso de aulas de inglés	CDI
2	CISCO SG350-10	PSZ21471M MO	Switch de acceso	Cisco Small Business Firmware	192.168.10 .X/24	CISCO SF200-24(CDI)	Residencia 1
3	CISCO SF200-24	DNI2040026 P	Switch de acceso	Cisco Small Business Firmware	192.168.10 .X/24	CISCO SF200-24(CDI)	Residencia 2

#### 4.4. Descripción de Precios de Infraestructura Actual

*Tabla 9: Descripción de Precios de Infraestructura Actual.*

Descripción	Marca	Modelo	Fecha	Precio
AntiDDoS	Huawei	ANTIDDOS 1905_Cleaning	25/07/2022	\$36504.97
AntiDDoS	Huawei	ANTIDDOS 1905_Cleaning	25/07/2022	\$36504.97
AP Indoor	Huawei	AIRENGINE 5761-21	25/07/2022	\$1443.35
AP Outdoor	Huawei	AIRENGINE 6760R-51E	25/07/2022	\$2717.17
AP Outdoor	Huawei	AIRENGINE 6760R-51E	25/07/2022	\$2717.17
Firewall	Huawei	USG6610GE	25/07/2022	\$26710.90
Firewall	Huawei	USG6610GE	25/07/2022	\$26710.90
Routers	Huawei	NETENGINE 8000 M1A	25/07/2022	\$9287.79
Routers	Huawei	NETENGINE 8000 M1A	25/07/2022	\$9287.79
Switches de acceso	Huawei	CLOUD ENGINE S536-S24UM4XC	25/07/2022	\$5092.76
Wireless controller	Huawei	AirEngine9700-M1	25/07/2022	\$19558.53

*Tabla 10: Distribución Lógica de Red.*

N°	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	CÓMPUTO	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
26	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	WIFI 6	1123	IP PLAN
----	--------	------	---------

#### 4.5. Plan para Wifi 6

El Plan para Wifi 6 presenta la organización lógica de la red mediante la asignación de VLANs a los diferentes servicios y áreas de la Universidad de El Salvador, Facultad Multidisciplinaria Oriental, cada VLAN tiene su identificador único (id VLANs) y un rango de dirección IP específico, lo que permite segmentar el tráfico de red y garantizar seguridad, control y mejor administración de los recursos.

En la tabla se observa que cada dependiente o servicio, como biblioteca, cómputo, administración, medicina, postgrado, entre otros, poseen su VLAN. Esto significa que el tráfico de cada área viaja de forma separada dentro de la misma infraestructura física, evitando interferencias con otros servicios y reduciendo riesgo de seguridad.

Los valores de las direcciones IP aparecen representadas por una “X” en el último octeto. Esto se debe a que la información que se nos compartió mediante una documentación omite números exactos por motivos de seguridad. Esta tabla muestra la forma en que la facultad segmenta la red mediante VLANs, asignando a cada unidad académica o administrativa un espacio de dirección IP propio, lo que contribuye a que la red sea más ordenada y segura. Sin embargo, aunque la red mantiene un nivel adecuado de organización y seguridad, presenta una limitación importante, algunas VLANs utilizan rangos de dirección IP excesivamente amplios en comparación con la cantidad real de dispositivos conectados. Esto genera un desperdicio de direcciones disponibles y reduce la eficiencia en la administración del direccionamiento IP dentro de la infraestructura.

**Tabla 11: Plan para Wifi 6**

N°	NOMBRE VLAN	ID -VLAN	VLAN	MÁSCARA
1	WIFI	1101	172.16.0.0.x	/20
2	ADMINISTRATIVOS	1102	192.168.30.x	/24
3	UESED	1103	192.168.8.x	/24
4	CÓMPUTO	1104	192.168.60.x	/24
5	AGRONOMÍA	1105	192.168.9.x	/24
6	ADMINISTRACIÓN	1106	192.168.10.x	/24
7	SERVIDORES	1107	192.168.7.x	/24
8	BIBLIOTECA	1108	192.168.11.x	/24
9	ACADÉMICA	1109	192.168.12.x	/24
10	POSTGRADO	1110	192.168.13.x	/24
11	SALA -INTERNET	1111	192.168.14.x	/24
12	ECONOMÍA	1112	192.168.15.x	/24
13	CCNN	1113	192.168.16.x	/24

14	MEDICINA	1114	192.168.17.x	/24
15	CCJJ	1115	192.168.18.x	/24
26	QUÍMICA	1116	192.168.19.x	/24
17	HUMANIDADES	1117	192.168.20.x	/24
18	INGENIERÍA	1118	192.168.21.x	/24
19	CÁMARAS	1119	192.168.22.x	/24
20	TELEFONÍA IP	1120	192.168.23.x	/24
21	AUDIOVISUALES	1121	192.168.24.x	/24
22	WIFI2	1122	172.16.1.x	/20
23	WIFI 6	1123	IP PLAN	

**Tabla 12: Distribución por VLAN Por Zonas.**

Ubicación	Administración		Servicio			Invitado	
	VLAN	SUBNET	DESC.	VLAN ID	SUBNET	VLAN	SUBNET
Biblioteca_DC	711	10.60.11.0	Red 1	811	10.61.11.0	921	10.62.21.0
			Red 2	812	10.61.12.0		
			Red 3	813	10.61.13.0		
			Red 4	814	10.61.14.0		
Medicina_1	712	10.60.12.0	Red 1	816	10.61.16.0	922	10.62.22.0
			Red 2	817	10.61.17.0		
			Red 3	818	10.61.18.0		
Medicina_2	713	10.60.13.0	Red 1	821	10.61.21.0	923	10.62.23.0
			Red 2	822	10.61.22.0		
			Red 3	823	10.61.23.0		
Aulas de Inglés	714	10.60.14.0	Red 1	826	10.61.26.0	924	10.62.24.0
Aulas Ingeniería	715	10.60.15.0	Red 1	831	10.61.31.0	925	10.62.25.0

			Red 2	832	10.61.32.0		
Edificio CCNN	716	10.60.16.0	Red 1	836	10.61.36.0	926	10.62.26.0
			Red 2	837	10.61.37.0		
Edificio Docentes Riñón	717	10.60.17.0	Red 1	841	10.61.41.0	927	10.62.27.0
			Red 2	842	10.61.42.0		
			Red 3	843	10.61.43.0		
Edificio Minerva	718	10.60.18.0	Red 1	846	10.61.46.0	928	10.62.28.0
			Red 2	847	10.61.47.0		
			Red 3	848	10.61.48.0		
Edificio Postgrado	719	10.60.19.0	Red 1	851	10.61.51.0	929	10.62.29.0
			Red 2	852	10.61.52.0		

**Tabla 13: Distribución de VLAN Zona 2.**

Ubicación	Administración		Servicio			Invitado	
	VLAN	SUBNET	DESC.	VLAN ID	SUBNET	VLAN	SUBNET
Edificio Agronomía	720	10.60.20.0	Red 1	856	10.61.56.0	930	10.62.30.0
			Red 2	857	10.61.57.0		
Edificio Académica	721	10.60.21.0	Red 1	861	10.61.61.0	931	10.62.31.0
			Red 2	862	10.61.62.0		
Ciencias Jurídicas	722	10.60.22.0	Red 1	866	10.61.66.0	932	10.62.32.0
			Red 2	867	10.61.67.0		
			Red 3	868	10.61.68.0		
Edificio Química	723	10.60.23.0	Red 1	871	10.61.71.0	933	10.62.33.0
Aulas Economía	724	10.60.24.0	Red 1	876	10.61.76.0	934	10.62.34.0
			Red 2	877	10.61.77.0		
Aulas Educación	725	10.60.25.0	Red 1	881	10.61.81.0	935	10.62.35.0
			Red 2	882	10.61.82.0		
Auditórium	726	10.60.26.0	Red 1	886	10.61.86.0	936	10.62.36.0
			Red 2	887	10.61.87.0		
			Red 3	888	10.61.88.0		

#### 4.7. Distribución de puntos de acceso Wifi 6

Actualmente, la Universidad de El Salvador, Facultad Multidisciplinaria Oriental cuenta con una red inalámbrica moderna con tecnología WiFi 6, disponible en edificios académicos, laboratorios, biblioteca y diferentes áreas comunes. Los puntos de acceso se administran desde un sistema central lo que permite un mejor manejo, seguro y con opción de inicio de sesión para la mayoría de los usuarios. Cabe destacar que, también se ha habilitado acceso para visitantes, quienes pueden conectarse sin necesidad de una credencial. La cobertura alcanza tanto en espacio interior como exterior, y gracias a las instalaciones de múltiples APs en aulas y auditorios, la red soporta un elevado número de conexiones simultáneas, la red está preparada para ampliarse según lo requiera la necesidad de conectividad futuras.

**Tabla 14: Distribución de Puntos de Acceso Wifi 6 para oficinas de Admin. Académica.**

<b>SWTICH NOMBRE: OFICINAS DE ADMINISTRACIÓN ACADÉMICA</b>				
<b>Interfaz para APs</b>	<b>Nombre</b>	<b>Tipo</b>	<b>Ubicación</b>	<b>Descripción de la ubicación o referencia</b>
MultiGE0/0/1	AP01	Outdoor	Admin Académica	Administración Académica pasillo de atrás en pared
MultiGE0/0/2	AP02	Outdoor	Admin Académica	Administración Académica Poste 3
MultiGE0/0/3	AP03	Outdoor	Admin Académica	Administración Académica Poste 1
MultiGE0/0/4	AP04	Outdoor	Admin Académica	Administración Académica Poste 2
MultiGE0/0/5	AP05	Outdoor	Admin Académica	Administración Académica pasillo de atrás en pared
MultiGE0/0/6	AP06	Indoor	Admin Académica	Administración Académica Oficina
MultiGE0/0/7	AP07	Outdoor	Admin Académica	Administración Académica pasillo de costado en pared

**Tabla 15: Distribución de Puntos de Acceso Wifi 6 para aulas de Educación.**

<b>SWTICH NOMBRE: AULAS DE EDUCACIÓN</b>				
<b>Interfaz para-APs</b>	<b>Nombre</b>	<b>Tipo</b>	<b>Ubicación</b>	<b>Descripción de la ubicación o referencia</b>
MultiGE0/0/1	AP02	Indoor	Aulas de Educación	Aulas de Educación
MultiGE0/0/2	AP03	Indoor	Aulas de Educación	Aulas de Educación
MultiGE0/0/3	AP04	Indoor	Aulas de Educación	Aulas de Educación
MultiGE0/0/4	AP07	Outdoor	Aulas de Educación	Aulas de Educación
MultiGE0/0/5	AP012	Outdoor	Auditorium	Pared por entrada de atrás
MultiGE0/0/6	AP013	Outdoor	Auditorium	Pared por entrada de atrás
MultiGE0/0/7	AP014	Indoor	Auditorium	Pabellón Norte pasillo frente a aula 3
MultiGE0/0/8	AP015	Indoor	Auditorium	Pabellón Norte pasillo frente a aula 4 ap.
MultiGE0/0/9	AP016	Indoor	Auditorium	Pabellón Norte Pasillo fuera de aula 5
MultiGE0/0/10	AP017	Indoor	Auditorium	Pabellón Norte Pasillo fuera de aula 6
MultiGE0/0/11	AP018	Indoor	Auditorium	Pabellón Norte Aula 06
MultiGE0/0/12	AP019	Indoor	Auditorium	Pabellón Norte Aula 05
MultiGE0/0/13	AP020	Indoor	Auditorium	Pabellón Norte Aula 05
MultiGE0/0/14	AP021	Indoor	Auditorium	Pabellón Sur Pasillo fuera de aula

				14/15
MultiGE0/0/15	AP022	Indoor	Auditorium	Pabellón Sur Pasillo fuera de aula 12 AP se callo.
MultiGE0/0/16	AP023	Indoor	Auditorium	Pabellón Sur Pasillo fuera de aula 11
MultiGE0/0/17	AP024	Indoor	Auditorium	Pabellón Sur Pasillo fuera de aula 9

**Tabla 16: Distribución Puntos de Acceso Wifi 6 para Auditorium PP1.**

<b>Switich Nombre: Auditorium PP1</b>				
<b>Interfaz para APs</b>	<b>Nombre</b>	<b>Tipo</b>	<b>Ubicación</b>	<b>Descripción de la ubicación o referencia</b>
MultiGE0/0/1	AP04	Outdoor	Auditorium	Butacas
MultiGE0/0/2	AP05	Outdoor	Auditorium	Butacas
MultiGE0/0/3	AP06	Outdoor	Auditorium	Pared por entrada
MultiGE0/0/4	AP07	Outdoor	Auditorium	Pared por entrada

**Tabla 17: Distribución de Puntos de Acceso Wifi 6 para Auditorium PP2.**

<b>Switich Nombre: Auditorium PP2</b>				
<b>Interfaz para APs</b>	<b>Nombre</b>	<b>Tipo</b>	<b>Ubicación</b>	<b>Descripción de la ubicación o referencia</b>
MultiGE0/0/1	AP01	Outdoor	Auditorium	Pabellón Norte pasillo de atrás
MultiGE0/0/2	AP02	Outdoor	Auditorium	Pabellón Norte pasillo de atrás
MultiGE0/0/3	AP03	Outdoor	Auditorium	Pabellón Norte pasillo de atrás
MultiGE0/0/4	AP04	Outdoor	Auditorium	Pabellón Norte pasillo de atrás
MultiGE0/0/5	AP05	Outdoor	Auditorium	Pabellón Norte Poste
MultiGE0/0/6	AP06	Indoor	Auditorium	Pabellón Sur Aula
MultiGE0/0/7	AP07	Indoor	Auditorium	Pabellón Sur Aula

MultiGE0/0/8	AP08	LIBRE	LIBRE	LIBRE
MultiGE0/0/9	AP09	Outdoor	Auditórium	Pabellón Norte Poste
MultiGE0/0/10	AP10	LIBRE	LIBRE	LIBRE
MultiGE0/0/11	AP11	Outdoor	Auditórium	Pabellón Sur Poste
MultiGE0/0/12	AP12	Outdoor	Auditórium	Pabellón Sur Poste
MultiGE0/0/13	AP13	Indoor	Auditórium	Pabellón Sur Aula
MultiGE0/0/14	AP14	Indoor	auditórium	Pabellón Sur Aula

**Tabla 18: Distribución de puntos de Acceso Wifi 6 Para Biblioteca Unidad Financiera.**

<b>Nombre: BIBLIOTECA UNIDAD FINANCIERA</b>					
<b>Interfaz para APs</b>	<b>Nombre</b>	<b>Switch Tipo</b>	<b>ESN</b>	<b>Ubicación</b>	<b>Descripción de la ubicación o referencia</b>
MultiGE0/0/1	AP40	Indoor	2102353VUT6RMB013525	Biblioteca	Unidad Financiera Pasillo frente
MultiGE0/0/2	AP41	Outdoor	2102353KCM6RMC001118	Biblioteca	Unidad Financiera fachada de edificio
MultiGE0/0/3	AP42	Outdoor	2102353KCM6RMC001014	Biblioteca	Unidad Financiera fachada de edificio
MultiGE0/0/4	AP43	Indoor	2102353VUT6RMB013521	Biblioteca	Unidad Financiera Oficina
MultiGE0/0/5	AP44	Indoor	2102353VUT6RMB013508	Biblioteca	Unidad Financiera Desarrollo Físico
MultiGE0/0/6	AP45	Indoor	2102353VUT6RMB011952	Biblioteca	Unidad Financiera Administración General
MultiGE0/0/7	AP47	Indoor	2102353VUT6RMB011949	Biblioteca	Unidad Financiera Proyección Social
MultiGE0/0/8	AP48	Indoor	2102353VUT6RMB011957	Biblioteca	Unidad Financiera Bodega

**Tabla 19: Distribución de puntos de Acceso Wifi 6 para Biblioteca Vice-Decano.**

<b>Switch Nombre: BIBLIOTECA VICE-DECANATO</b>					
<b>Interfaz para APs</b>	<b>Nombre</b>	<b>Tipo</b>	<b>ESN</b>	<b>Ubicación</b>	<b>Descripción de la ubicación o referencia</b>
MultiGE0/0/1	AP27	Indoor	2102353VUT6RMB012129	Biblioteca	Vice-Decanato secretaria
MultiGE0/0/2	AP43	Indoor	2102353VUT6RMB013527	Biblioteca	Vice-Decanato secretaria
MultiGE0/0/3	AP44	Indoor	2102353VUT6RMB013532	Biblioteca	Vice-Decanato Unidad de RRHH
MultiGE0/0/4	AP45	Indoor	2102353VUT6RMB013530	Biblioteca	Vice-Decanato Pasillo externo
MultiGE0/0/5	AP46	Indoor	2102353VUT6RMB013533	Biblioteca	Vice-Decanato Pasillo
MultiGE0/0/6	AP47	Indoor	2102353VUT6RMB013534	Biblioteca	Vice-Decanato Pasillo
MultiGE0/0/7	AP48	Indoor	2102353VUT6RMB013523	Biblioteca	Vice-Decanato Sala de Junta directiva
MultiGE0/0/8	AP01	Indoor	2102353VUT6RMB012738	Biblioteca	Vice-Decanato Unidad de RRHH
MultiGE0/0/9	AP02	Indoor	2102353VUT6RMC001020	Biblioteca	Vice-Decanato Departamento de proceso técnico
MultiGE0/0/10	AP03	Indoor	2102353VUT6RMC001071	Biblioteca	Vice-Decanato oficina del Decano

**Tabla 20: Distribución de puntos de Acceso Wifi 6 para Biblioteca Área de Servidores.**

<b>Switich Nombre: BIBLIOTECA ÁREA DE SERVIDORES</b>					
<b>Interfaz para APs</b>	<b>Nombre</b>	<b>Tipo</b>	<b>ESN</b>	<b>Ubicación</b>	<b>Descripción de la Ubicación o Referencia</b>
MultiGE0/0/1	AP01	Indoor	2102353VUT6RMB013526	Biblioteca	Data Center pasillo poniente Dpto. Infor.

MultiGE0/0/2	AP02	Indoor	2102353VUT6RMB013529	Biblioteca	Data Center Reparación y Mantenimiento EQ
MultiGE0/0/3	AP03	Indoor	2102353VUT6RMC001200	Biblioteca	Data Center Sala de Conferencia 1
MultiGE0/0/4	AP04	Indoor	2102353VUT6RMC001201	Biblioteca	Data Center Sala de Conferencia 1
MultiGE0/0/5	AP05	Indoor	2102353VUT6RMC001193	Biblioteca	Data Center Pasillo sala de conferencia
MultiGE0/0/6	AP06	Indoor	2102353VUT6RMC001154	Biblioteca	Data Center Sala de conferencia
MultiGE0/0/7	AP07	Indoor	2102353VUT6RMC001009	Biblioteca	Data Center Proceso Técnico
MultiGE0/0/8	AP08	Indoor	2102353VUT6RMC001006	Biblioteca	Data Center
MultiGE0/0/9	AP09	Indoor	2102353VUT6RMC001016	Biblioteca	Data Center
MultiGE0/0/10	AP10	Outdoor	2102353KCM6RMC001010	Biblioteca	Data Center externo en Fachada
MultiGE0/0/11	AP11	Outdoor	2102353KCM6RMC001304	Biblioteca	Data Center externo en Fachada
MultiGE0/0/12	AP12	Outdoor	2102353KCM6RMC001300	Biblioteca	Data Center pasillo interno
MultiGE0/0/13	AP13	Outdoor	2102353KCM6RMC001311	Biblioteca	Data Center pasillo interno

**Tabla 21: Distribución de puntos de Acceso Wifi 6 para Biblioteca Sala de Estudio.**

<b>Switich Nombre: BIBLIOTECA SALA DE ESTUDIOS</b>					
<b>Interfaz para-APs</b>	<b>Nombre</b>	<b>Tipo</b>	<b>ESN</b>	<b>Ubicación</b>	<b>Descripción de la ubicación o referencia</b>

MultiGE0/0/1	AP21	Indoor	2102353VUT6RMB013483	Biblioteca	Biblioteca Sala de Estudio
MultiGE0/0/2	AP22	Indoor	2102353VUT6RMB013484	Biblioteca	Biblioteca Sala de Estudio
MultiGE0/0/3	AP23	Indoor	2102353VUT6RMB013472	Biblioteca	Biblioteca Sala de Estudio
MultiGE0/0/4	AP24	Indoor	2102353VUT6RMB013473	Biblioteca	Biblioteca Sala de Estudio
MultiGE0/0/5	AP25	Indoor	2102353VUT6RMB013388	Biblioteca	Biblioteca Sala de Estudio
MultiGE0/0/6	AP26	Indoor	2102353VUT6RMB013481	Biblioteca	Biblioteca Sala de Estudio
MultiGE0/0/7	AP27	Indoor	2102353VUT6RMB013477	Biblioteca	Biblioteca Oficina videoteca
MultiGE0/0/8	AP28	Indoor	2102353VUT6RMB012726	Biblioteca	Biblioteca Pasillo de afuera
MultiGE0/0/9	AP29	Indoor	2102353VUT6RMB012729	Biblioteca	Biblioteca Pasillo de afuera
MultiGE0/0/10	AP30	Outdoor	2102353KCM6RMC001310	Biblioteca	Data Center parte de atrás del Edificio
MultiGE0/0/11	AP31	Outdoor	2102353KCM6RMC001112	Biblioteca	Biblioteca Zona verde en poste
MultiGE0/0/12	AP32	Outdoor	2102353KCM6RMC001308	Biblioteca	Biblioteca Zona verde en poste
MultiGE0/0/13	AP33	Outdoor	2102353KCM6RMC001099	Biblioteca	Biblioteca Plaza Madrid
MultiGE0/0/14	AP34	Outdoor	2102353KCM6RMC001111	Biblioteca	Biblioteca Plaza Madrid

**Tabla 22: Distribución de puntos de Acceso Wifi 6 para Biblioteca Laboratorio de Redes.**

<b>Switch Nombre: BIBLIOTECA LABORATORIOS DE REDES</b>					
<b>Interfaz para APs</b>	<b>Nombre</b>	<b>Tipo</b>	<b>ESN</b>	<b>Ubicación</b>	<b>Descripción de la ubicación o referencia</b>
MultiGE0/0/1	AP16	Indoor	2102353VUT6RMB012720	Biblioteca	Lab. de Redes centro de cómputo 2
MultiGE0/0/2	AP17	Indoor	2102353VUT6RMB012725	Biblioteca	Lab. de Redes centro de cómputo 2
MultiGE0/0/3	AP18	Indoor	2102353VUT6RMB012731	Biblioteca	Lab. de Redes Pasillo fuera de idiomas
MultiGE0/0/4	AP34	Indoor	2102353VUT6RMB012727	Biblioteca	Lab. de Redes Cómputo 1
MultiGE0/0/5	AP35	Indoor	2102353VUT6RMB012696	Biblioteca	Lab. de Redes
MultiGE0/0/6	AP36	Outdoor	2102353KCM6RMC000653	Biblioteca	Lab. De Redes Zona verde en poste
MultiGE0/0/7	AP37	Outdoor	2102353KCM6RMC000646	Biblioteca	Lab. De Redes Zona verde en poste
MultiGE0/0/8	AP38	Outdoor	2102353KCM6RMC000801	Biblioteca	Lab. De Redes Zona verde en poste
MultiGE0/0/9	AP39	Outdoor	2102353KCM6RMC000691	Biblioteca	Lab. De Redes Zona verde en poste
MultiGE0/0/10	AP43	Indoor	2102353VUT6RMB012676	Biblioteca	Lab. de Redes Aula de Idiomas
MultiGE0/0/11	AP44	Indoor	2102353VUT6RMB012728	Biblioteca	Lab. de Redes Aula de Idiomas
MultiGE0/0/12	AP45	Indoor	2102353VUT6RMB013504	Biblioteca	Lab. de Redes Aula de Idiomas
MultiGE0/0/13	AP46	Indoor	2102353KCM6RMC001241	Biblioteca	Lab. de Redes Aula de Idiomas

**Tabla 23: Distribución de puntos de Acceso Wifi 6 para caseta de vigilantes Entrada Principal.**

<b>Switch Nombre: CASETA DE VIGILANCIA ENTRADA PRINCIPAL</b>				
<b>Interfaz para APs</b>	<b>Nombre</b>	<b>Tipo</b>	<b>Ubicación</b>	<b>Descripción de la ubicación o referencia</b>
MultiGE0/0/3	AP01	Outdoor	Caseta de Vigilancia	Poste de Entrada principal
MultiGE0/0/4	AP02	Outdoor	Caseta de Vigilancia	Poste de Entrada principal

**Tabla 24: Distribución de puntos de Acceso Wifi 6 para Caseta de Vigilancia de Parqueo Principal.**

<b>Switch Nombre: CASETA DE VIGILANCIA PARQUEO PRINCIPAL</b>				
<b>Interfaz para APs</b>	<b>Nombre</b>	<b>Tipo</b>	<b>Ubicación</b>	<b>Descripción de la ubicación o referencia</b>
MultiGE0/0/7	AP07	Indoor	vigilancia parqueo principal	Caseta de vigilancia
MultiGE0/0/8	N/D	N/D	N/D	N/D
MultiGE0/0/9	AP09	Outdoor	vigilancia parqueo principal	Poste frente a Caseta de vigilancia
MultiGE0/0/10	AP10	Outdoor	vigilancia parqueo principal	Poste frente a Caseta de vigilancia

**Tabla 25: Distribución de puntos de Acceso Wifi 6 para Centro de Desarrollo Infantil (CDI).**

<b>Switch Nombre: CENTRO DE DESARROLLO INFANTIL (CDI)</b>				
<b>Interfaz para APs</b>	<b>Nombre</b>	<b>Tipo</b>	<b>Ubicación</b>	<b>Descripción de la ubicación o referencia</b>

MultiGE0/0/1	AP01	Indoor	Centro Desarrollo Infantil (CDI)	Centro de Desarrollo Infantil (CDI) Aula
MultiGE0/0/2	AP02	Indoor	Centro de Desarrollo Infantil (CDI)	Centro de Desarrollo Infantil (CDI) Aula
MultiGE0/0/3	AP03	Outdoor	Centro de Desarrollo Infantil (CDI)	Centro de Desarrollo Infantil (CDI) Poste

**Tabla 26: Distribución de puntos de Acceso Wifi 6 para Ciencias Jurídicas Sala de Simulación de Audiencia.**

<b>Switch Nombre: CIENCIAS JURÍDICAS SALA DE SIMULACIONES DE AUDIENCIA</b>				
<b>Interfaz para APs</b>	<b>Nombre</b>	<b>Tipo</b>	<b>Ubicación</b>	<b>Descripción de la ubicación o referencia</b>
MultiGE0/0/1	N/D	N/D	N/D	N/D
MultiGE0/0/2	CJ-SS-InAP01 - AP02	Indoor	Ciencias Jurídicas	Sala de Simulaciones de Ciencias Jurídicas
MultiGE0/0/3	CJ-SS-InAP02 - AP03	Indoor	Ciencias jurídicas	Sala de Simulaciones Aula de Letras
MultiGE0/0/4	CJ-SS-OutAP03 - AP04	Outdoor	Ciencias jurídicas	Sala de Simulaciones Aula de Letras
MultiGE0/0/5	CJ-SS-OutAP04 - AP05	Outdoor	Ciencias jurídicas	Sala de Simulaciones Aula de Letras
MultiGE0/0/6	CJ-SS-InAP05 - AP06	Indoor	Ciencias jurídicas	Sala de Simulaciones Aula de Letras

**Tabla 27: Distribución de puntos de Acceso Wifi 6 para Laboratorio de Química y Farmacia.**

<b>Switch Nombre: LABORATORIO QUÍMICA Y FARMACIA</b>				
<b>Interfaz para APs</b>	<b>Nombre</b>	<b>Tipo</b>	<b>Ubicación</b>	<b>Descripción de la ubicación o referencia</b>
MultiGE0/0/1	AP17	Indoor	Ciencias Químicas	Lab. De Ciencias químicas Oficina
MultiGE0/0/2	AP18	Indoor	Ciencias Químicas	Lab. De Ciencias químicas
MultiGE0/0/3	AP19	Indoor	Ciencias Químicas	Lab. De Ciencias químicas Oficina
MultiGE0/0/4	AP20	Outdoor	Ciencias Químicas	Lab. De Ciencias químicas fachada del edificio
MultiGE0/0/5	AP21	Outdoor	Ciencias Químicas	Lab. De Ciencias químicas por entrada principal

**Tabla 28: Distribución de puntos de Acceso Wifi 6 para el Edificio Riñón.**

<b>Switch Nombre: EDIFICIO RIÑÓN</b>					
<b>Interfaz para APs</b>	<b>Nombre</b>	<b>Tipo</b>	<b>Ubicación</b>	<b>Descripción de la Ubicación o Referencia</b>	<b>Nivel</b>
MultiGE0/0/1	AP01	Indoor	Edificio Riñón	Riñón Oficina	1
MultiGE0/0/2	AP02	Indoor	Edificio Riñón	Riñón Oficina	1
MultiGE0/0/3	AP03	Indoor	Edificio Riñón	Riñón Oficina	1
MultiGE0/0/4	AP04	Indoor	Edificio Riñón	Riñón Oficina	1
MultiGE0/0/5	AP05	Indoor	Edificio Riñón	Riñón Oficina	1
MultiGE0/0/6	AP06	Indoor	Edificio Riñón	Riñón Pasillo	1
MultiGE0/0/7	AP07	Indoor	Edificio Riñón	Riñón Oficina	1

**Tabla 29: Distribución de puntos de Acceso Wifi 6 para Edificio del Riñón Nivel 2.**

Switch Nombre: EDIFICIO RIÑÓN 2					
Interfaz para APs	Nombre	Tipo	Ubicación	Descripción de la ubicación o referencia	Nivel
MultiGE0/0/1	AP19	Indoor	Edificio Riñón	Riñón Oficina	2
MultiGE0/0/2	AP20	Outdoor	Edificio Riñón	Riñón fachado de edificio	2
MultiGE0/0/3	AP21	Indoor	Edificio Riñón	Riñón Oficina de letras	2
MultiGE0/0/4	AP22	Indoor	Edificio Riñón	Riñón Oficina	2
MultiGE0/0/5	AP23	Indoor	Edificio Riñón	Riñón Pasillo	2
MultiGE0/0/6	AP24	Indoor	Edificio Riñón	Riñón pasillo	2
MultiGE0/0/7	AP25	Indoor	Edificio Riñón	Riñón Psicología	2
MultiGE0/0/8	AP26	Indoor	Edificio Riñón	Riñón Psicología	2
MultiGE0/0/9	AP27	Indoor	Edificio Riñón	Riñón Fisiología	2
MultiGE0/0/10	AP28	Outdoor	Edificio Riñón	Riñón fachado de edificio	2
MultiGE0/0/11	AP29	Outdoor	Edificio Riñón	Riñón fachado de edificio	2

**Tabla 30: Distribución de puntos de Acceso Wifi 6 para Medicina 1/ Nivel.**

Switch Nombre: MEDICINA 1					
Interfaz para APs	Nombre	Tipo	Ubicación	Descripción de la ubicación o referencia	Nivel
MultiGE0/0/1	AP01	Indoor	Facultad de Medicina	Edif. de Medicina 1 Pasillo	1
MultiGE0/0/2	AP02	Indoor	Facultad de Medicina	Edif. de Medicina 1 Aula 39	1
MultiGE0/0/3	AP03	Indoor	Facultad de Medicina	Edif. de Medicina 1 Aula 40	1
MultiGE0/0/4	AP04	Indoor	Facultad de Medicina	Edif. de Medicina 1 Pasillo	1
MultiGE0/0/5	AP05	Indoor	Facultad de Medicina	Edif. de Medicina 1 Aula 38	1

MultiGE0/0/6	AP06	Indoor	Facultad de Medicina	Edif. de Medicina 1 Aula 41	1
MultiGE0/0/7	AP07	Indoor	Facultad de Medicina	Edif. de Medicina 1 Aula 34	1
MultiGE0/0/8	AP08	Indoor	Facultad de Medicina	Edif. de Medicina 1 Aula 35	1
MultiGE0/0/9	AP09	Indoor	Facultad de Medicina	Edif. de Medicina 1 Aula 36	1
MultiGE0/0/10	AP10	Indoor	Facultad de Medicina	Edif. de Medicina 1 Aula 37	1
MultiGE0/0/11	AP11	Outdoor	Facultad de Medicina	Edif. de Medicina 1 poste	1
MultiGE0/0/12	AP12	Outdoor	Facultad de Medicina	Edificio de Medicina 1 poste	1
MultiGE0/0/13	AP13	Outdoor	Facultad de Medicina	Edif. de Medicina 1 Pared Externa	1
MultiGE0/0/14	AP14	Outdoor	Facultad de Medicina	Edif. de Medicina 1 Pared	1
MultiGE0/0/15	AP15	Outdoor	Facultad de Medicina	Edif. de Medicina 1 Pared	1

*Tabla 31: Distribución de puntos de Acceso Wifi 6 para Medicina 1 / Nivel 2.*

Switch Nombre: MEDICINA 1 NIVEL 2					
Interfaz para APs	Nombre	Tipo	Ubicación	Descripción de la ubicación o referencia	Nivel
MultiGE0/0/1	AP01	Indoor	Facultad de Medicina	Edificio de Medicina 1 Cubículos de docentes	2
MultiGE0/0/2	AP02	Indoor	Facultad de Medicina	Edificio de Medicina 1 Pasillo	2
MultiGE0/0/3	AP03	Indoor	Facultad de Medicina	Edificio de Medicina 1 Cubículos de docentes	2
MultiGE0/0/4	AP04	Indoor	Facultad de Medicina	Edificio de Medicina 1 Proceso de grado	2

MultiGE0/0/5	AP05	Indoor	Facultad de Medicina	Edificio de Medicina 1 pasillo	2
MultiGE0/0/6	AP06	Indoor	Facultad de Medicina	Edificio de Medicina 1 Auditorium	2
MultiGE0/0/7	AP07	Indoor	Facultad de Medicina	Edificio de Medicina 1 Auditorium	2
MultiGE0/0/8	AP08	Indoor	Facultad de Medicina	Edificio de Medicina 1 Auditorium	2
MultiGE0/0/9	AP09	Indoor	Facultad de Medicina	Edificio de Medicina 1 Auditorium	2
MultiGE0/0/10	AP10	Indoor	Facultad de Medicina	Edificio de Medicina 1 Pasillo	2
MultiGE0/0/11	AP11	Outdoor	Facultad de Medicina	Edificio de Medicina 1 Pared Externa	2

**Tabla 32: Distribución de puntos de Acceso Wifi 6 para Medicina 2 / Nivel 2.**

<b>Switch Nombre: MEDICINA 2 / NIVEL 1</b>					
<b>Interfaz para APs</b>	<b>Nombre</b>	<b>Tipo</b>	<b>Ubicación</b>	<b>Descripción de la ubicación o referencia</b>	<b>Nivel</b>
MultiGE0/0/1	AP01	Indoor	Facultad de Medicina	Edificio de Medicina 2 Pasillo por entrada	1
MultiGE0/0/2	AP02	Indoor	Facultad de Medicina	Edificio de Medicina 2 Lab. De Microanatomía	1
MultiGE0/0/3	AP03	Indoor	Facultad de Medicina	Edificio de Medicina 2 Aula de Autopsias	1
MultiGE0/0/4	AP04	Indoor	Facultad de Medicina	Edificio de Medicina 2 Pasillo por baños	1
MultiGE0/0/5	AP05	Indoor	Facultad de Medicina	Edificio de Medicina 2 enfermería	1
MultiGE0/0/6	AP06	Indoor	Facultad de Medicina	Edificio de Medicina 2 Lab. De Fisiología	1
MultiGE0/0/7	AP07	Outdoor	Facultad de Medicina	Edificio de Medicina 2 Poste	1
MultiGE0/0/8	AP08	Outdoor	Facultad de Medicina	Edificio de Medicina 2 Poste	1
MultiGE0/0/9	AP09	Outdoor	Facultad de Medicina	Edificio de Medicina 2 Fachada	1
MultiGE0/0/10	AP10	Outdoor	Facultad de	Edificio de Medicina 2 exterior	1

			Medicina	de clínica	
MultiGE0/0/11	AP11	Outdoor	Facultad de Medicina	Edificio de Medicina 2 Fachada	1

**Tabla 33: Distribución de puntos de Acceso Wifi 6 para Medicina 2 / Nivel 2.**

Switich Nombre: MEDICINA 2 / NIVEL 2					
Interfaz para APs	Nombre	Tipo	Ubicación	Descripción de la ubicación o referencia	Nivel
MultiGE0/0/1	AP01	Indoor	Facultad de Medicina	Edificio de Medicina 2 Lab. De química Clínica	2
MultiGE0/0/2	AP02	Indoor	Facultad de Medicina	Edificio de Medicina 2 Lab. De Bioquímica	2
MultiGE0/0/3	AP03	Indoor	Facultad de Medicina	Edificio de Medicina 2 Pasillo por baños	2
MultiGE0/0/4	AP04	Indoor	Facultad de Medicina	Edificio de Medicina 2 Lab. De fisiología y farmacia	2
MultiGE0/0/5	AP05	Indoor	Facultad de Medicina	Edificio de Medicina 2 Pasillo	2
MultiGE0/0/6	AP06	Indoor	Facultad de Medicina	Edificio de Medicina 2 Lab. De Microbiología	2
MultiGE0/0/7	AP07	Outdoor	Facultad de Medicina	Edificio de Medicina 2 Pared Externa	2

**Tabla 34: Distribución de puntos de acceso Wifi 6 para aulas de Agronomía.**

<b>Switch Nombre: AGRONOMÍA AULAS</b>				
<b>Interfaz para-APs</b>	<b>Nombre</b>	<b>Tipo</b>	<b>Ubicación</b>	<b>Descripción de la ubicación o referencia</b>
MultiGE0/0/1	AP02	Indoor	Facultad de Agronomía Aula 3	Aula CCAA 3
MultiGE0/0/2	AP03	Indoor	Facultad de Agronomía Aula 3	Pasillo fuera de Aula CCAA 3
MultiGE0/0/3	AP04	Indoor	Facultad de Agronomía Aula 3	Aula CCAA 4
MultiGE0/0/4	AP05	Indoor	Facultad de Agronomía Aula 3	Aula 4
MultiGE0/0/5	AP06	Indoor	Facultad de Agronomía Aula 3	Aula 5
MultiGE0/0/6	AP07	Outdoor	Facultad de Agronomía Aula 3	Zona verde en poste por Aulas
MultiGE0/0/7	AP08	Indoor	Facultad de Agronomía Aula 3	Aula
MultiGE0/0/8	AP09	Indoor	Facultad de Agronomía Aula 3	Pasillo
MultiGE0/0/9	AP10	Indoor	Facultad de Agronomía Aula 3	Aula 01
MultiGE0/0/10	AP11	Indoor	Facultad de Agronomía Aula 3	Aula 01

**Tabla 35: Distribución de puntos de Acceso Wifi 6 para Agronomía Oficinas.**

<b>Switch Nombre: AGRONOMÍA OFICINAS</b>				
<b>Interfaz para-APs</b>	<b>Nombre</b>	<b>Tipo</b>	<b>Ubicación</b>	<b>Descripción de la ubicación o referencia</b>
MultiGE0/0/22	AP01	Indoor	Facultad de Agronomía Oficina	Oficina administrativa
MultiGE0/0/23	AP02	Indoor	Facultad de Agronomía Oficina	Oficina administrativa
MultiGE0/0/24	AP03	Indoor	Facultad de Agronomía Oficina	Oficina administrativa Pasillo exterior
MultiGE0/0/25	AP04	Outdoor	Facultad de Agronomía Oficina	Zona verde en poste

**Tabla 36: Distribución de puntos de Acceso Wifi 6 para Aulas de Economía.**

<b>Switch Nombre: AULAS DE ECONOMÍA</b>				
<b>Interfaz para-APs</b>	<b>Nombre</b>	<b>Tipo</b>	<b>Ubicación</b>	<b>Descripción de la ubicación o referencia</b>
MultiGE0/0/1	AP04	Indoor	Facultad de Economía	Edificio de Aulas Aula 29
MultiGE0/0/2	AP05	Indoor	Facultad de Economía	Edificio de Aulas Aula 27
MultiGE0/0/3	AP06	Indoor	Facultad de Economía	Edificio de Aulas Aula 27
MultiGE0/0/4	AP08	Indoor	Facultad de	Edificio de Aulas Aula 28

			Economía	
MultiGE0/0/5	AP09	Indoor	Facultad de Economía	Edificio de Aulas Aula 28
MultiGE0/0/6	AP10	Indoor	Facultad de Economía	Edificio de Aulas Aula 30
MultiGE0/0/7	LIBRE	LIBRE	LIBRE	LIBRE
MultiGE0/0/8	AP11	Indoor	Facultad de Economía	Edificio de Aulas Aula 30
MultiGE0/0/9	AP12	Outdoor	Facultad de Economía	En pared entrada principal
MultiGE0/0/10	AP13	Outdoor	Facultad de Economía	En pared entrada principal
MultiGE0/0/11	AP14	Outdoor	Facultad de Economía	Poste en Jardín

*Tabla 37: Distribución de puntos de Acceso Wifi 6 para Aulas de Inglés.*

<b>Switch Nombre: AULAS DE INGLÉS</b>				
<b>Interfaz para-APs</b>	<b>Nombre</b>	<b>Tipo</b>	<b>Ubicación</b>	<b>Descripción de la ubicación o referencia</b>
MultiGE0/0/1	AP02	Indoor	Facultad de Idiomas	Aula de Inglés
MultiGE0/0/2	AP03	Indoor	Facultad de Idiomas	Aula de Inglés
MultiGE0/0/3	AP04	Indoor	Facultad de Idiomas	Aula de Inglés
MultiGE0/0/4	AP05	Outdoor	Facultad de Idiomas	Aulas de Inglés poste 1

MultiGE0/0/5	AP06	Outdoor	Facultad de Idiomas	Aulas de Inglés poste 2
MultiGE0/0/6	AP07	Outdoor	Facultad de Idiomas	Pared externa de Aula de Inglés
MultiGE0/0/7	AP08	Outdoor	Facultad de Idiomas	Pared externa de Aula de Inglés

**Tabla 38: Distribución de puntos de Acceso Wifi 6 para Aulas de Ingeniería y Arquitectura.**

<b>Switch Nombre: INGENIERÍA Y ARQUITECTURA</b>				
<b>Interfaz para APs</b>	<b>Nombre</b>	<b>Tipo</b>	<b>Ubicación</b>	<b>Descripción de la ubicación o referencia</b>
MultiGE0/0/1	AP01	Indoor	Facultad de Ing. y Arquitectura	Oficina Ing. y Arquitectura
MultiGE0/0/2	AP02	Indoor	Facultad de Ing. y Arquitectura	Oficina Ing. y Arquitectura
MultiGE0/0/3	AP03	Outdoor	Facultad de Ing. y Arquitectura	Poste de parqueo de postgrado

**Tabla 39: Distribución de puntos de Acceso Wifi 6 para Aulas de Ingeniería y Arquitectura.**

<b>Switch Nombre: AULAS DE INGENIERIA Y ARQUITECTURA</b>				
<b>Interfaz para-APs</b>	<b>Nombre</b>	<b>Tipo</b>	<b>Ubicación</b>	<b>Descripción de la Ubicación o Referencia</b>
MultiGE0/0/1	AP03	Indoor	Facultad de Ingeniería	Aulas de Ingeniería Aula 18
MultiGE0/0/2	AP04	Indoor	Facultad de Ingeniería	Aulas de Ingeniería Aula 18

MultiGE0/0/3	AP05	Indoor	Facultad de Ingeniería	Aulas de Ingeniería Aula 19
MultiGE0/0/4	AP06	Indoor	Facultad de Ingeniería	Aulas de Ingeniería Aula 20
MultiGE0/0/5	AP07	Indoor	Facultad de Ingeniería	Aulas de Ingeniería Aula 20
MultiGE0/0/6	AP08	Outdoor	Facultad de Ingeniería	Aulas de Ingeniería poste 1
MultiGE0/0/7	AP09	Outdoor	Facultad de Ingeniería	Aulas de Ingeniería poste 2

La infraestructura de red actual de la Universidad de El Salvador, Facultad Multidisciplinaria Oriental, funciona 24/7 para brindar servicios académicos y administrativos. Sin embargo, evidencia limitaciones técnicas que afectan su rendimiento, seguridad y disponibilidad.

La red está basada en un modelo jerárquico, pero no es un modelo consistente, porque carece de cierta redundancia, además presenta ciertas deficiencias en la segmentación lógica y en las distribuciones de las direcciones IP. La distribución de VLANs no está diseñada de acuerdo con las necesidades reales de cada área a nuestro parecer, lo que provoca que algunas subredes quedan con rangos de direcciones sin utilizar, mientras que otras podrían saturarse fácilmente. Esta falta de equilibrio y planificación limita la eficiencia del direccionamiento y dificulta la gestión del tráfico dentro de la red, generando dependencia directa entre los diferentes edificios y zonas del campus; cuando un enlace o equipo de distribución falla varios sectores pierden conexión al mismo tiempo. Los enlaces hacia los switches de distribución se manejan de forma individual, sin rutas alternativas automáticas; haciendo que cuando algo falla la recuperación sea más lenta y cause interrupciones en la red.

Desde el punto de vista de seguridad perimetral, el firewall principal Huawei USG6610E realiza filtrado básico, pero carece de las suficientes políticas avanzadas de control, y la segmentación por roles presenta limitaciones, debido a que dispone de una cantidad reducida de roles para la asignación de permisos y roles. Además, no hay redundancia en el firewall ni en los routers, lo que hace a la red más vulnerable ante fallos y ataques.

Finalmente, el sistema de cableado estructurado combina segmentos de cobre y fibra óptica, aunque la cobertura de fibra óptica no está completa en todos los edificios limitando el potencial de ancho de banda y la expansión futura de servicios digitales.

La infraestructura de la Universidad de El Salvador, Facultad Multidisciplinaria Oriental, cuenta con limitaciones en seguridad, respaldo, segmentación y monitoreo, mostrando que necesita una revisión completa. La propuesta es reorganizar la red en un modelo jerárquico de 3 capas; se debe incluir enlaces de respaldo, VLANs bien definidas. Estas medidas garantizarán mayor rendimiento y escalabilidad para la institución educativa.

## 5. PROPUESTA DE MEJORA Y DISEÑO DE RED

### 5.1. Planteamiento de la propuesta

La infraestructura de red actual de la Universidad de El Salvador, Facultad Multidisciplinaria Oriental, permite que estudiantes, docentes, visitantes y personal administrativo accedan a los servicios de la institución. Sin embargo, aunque cumple con su función básica de conectividad, presenta diversas limitaciones que evidencian la necesidad de un rediseño integral orientado a la mejora en rendimiento, seguridad y disponibilidad.

Uno de los principales problemas es la falta de redundancia en sus enlaces y equipos. Esta limitación provoca que diversos departamentos dependan de un solo punto de conexión, lo que convierte a la red en vulnerable ante cualquier fallo. La falta de redundancia puede provocar interrupciones críticas en el servicio, afectando el acceso a recursos académicos y administrativos en amplias áreas del campus. En término técnico, esto se traduce en un punto único de falla que limita la continuidad y confiabilidad de la red. Se evidencia la falta de documentación actualizada de la infraestructura de red de la Universidad de El Salvador, Facultad Multidisciplinaria Oriental, lo que dificulta las labores de mantenimiento, diagnóstico y planificación de futuras mejoras, al no contar con información precisa sobre la configuración y el estado actual de los equipos y enlaces.

En cuanto a la segmentación lógica, actualmente coexisten dos esquemas:

- Una segmentación más reciente, implementada para la red Wifi 6 con nuevos puntos de acceso.
- Una segmentación anterior, que aún se utiliza en varias áreas de la facultad.

Además, se identifican las siguientes deficiencias en la infraestructura actual:

- La ausencia de sistemas de redundancia eléctrica provoca que, cuando ocurre un corte de energía, varios equipos de red quedan fuera de servicio, interrumpiendo completamente la conectividad.
- En algunos segmentos se han reservado más direcciones de las necesarias, lo que genera un uso ineficiente del direccionamiento y complica la administración
- La coexistencia de dos tablas de segmentación distintas incrementa la complejidad administrativa y puede generar ambigüedad en la gestión de la red.
- Aunque muchos switches y equipos de acceso se encuentran en funcionamiento, varios están cerca del final de su vida útil o carecen de capacidades necesarias, como un mayor procesamiento, soporte de velocidades elevadas, funciones de seguridad avanzadas y tolerancias a fallo

En términos de seguridad, la red también presenta vulnerabilidad, dificultades para aplicar controles de acceso específicos, riesgos de suplantación de identidad y acceso no autorizado y vulnerabilidad ante fallas de hardware sin redundancia ni protección eléctrica.

De esta manera, aunque la red actual cumple con la función de conectar a la comunidad universitaria, lo hace con deficiencia en redundancia, segmentación y seguridad, lo que limita su eficiencia confiabilidad y capacidad de crecimiento. Por ello se vuelve necesario un rediseño de la infraestructura que incluya enlaces de redundancia, respaldo energético, segmentación más eficiente, actualización tecnológica y mecanismos de seguridad que permita garantizarla continuidad y confiabilidad de los servicios de la institución.

#### 5.1.1. Soluciones propuestas según el diagnóstico

1. Se propone rediseñar la red bajo un modelo jerárquico de 3 capas, permitiendo una gestión modular, facilitando la escalabilidad y mejorando la disponibilidad del servicio. Los switches de núcleo concentran el tráfico principal, los de distribución manejan la segmentación por edificios y los de acceso conectan directamente a los usuarios finales.
2. Se plantea la implementación de enlace redundante entre los switches principales mediante los protocolos VRRP, LAC o STP, garantizando la continuidad operativa ante fallas. Cada edificio contará con doble enlace de fibra óptica monomodo hacia el switch de distribución más cercano, reduciendo el impacto de caída por daños físicos o cortes eléctricos.

3. Se propone unificar la segmentación lógica de la red mediante la creación de VLANs estructurada por áreas funcionales, administración, aulas, laboratorio, servidores, VoIP, cámaras, invitados, etc. Esto permite un mejor control de tráfico, priorizando mayor seguridad interna, evitando conflictos entre tablas antiguas.
4. Se recomienda la adquisición de equipo Huawei S5736- 24UM4XC con soportes para múltiples velocidades (1GB/ 2.5GB/ 5GB/10GB), administración inteligente VLANs, PoE+ y funciones de capa 3. Estos equipos garantizan mayor rendimiento, soporte para Wifi 6 y escalabilidad a futuro.
5. La facultad ya tiene implementados cortafuegos de seguridad, por lo que se propone optimizar la configuración del firewall integrando filtrado avanzado, inspección profunda de paquetes (DPI), lista de control de acceso (ACL) y segmentación por roles o departamentos, con el fin de garantizar que solo usuarios y dispositivos autorizados accedan a la red y que cada servicio opere bajo políticas de seguridad específica.

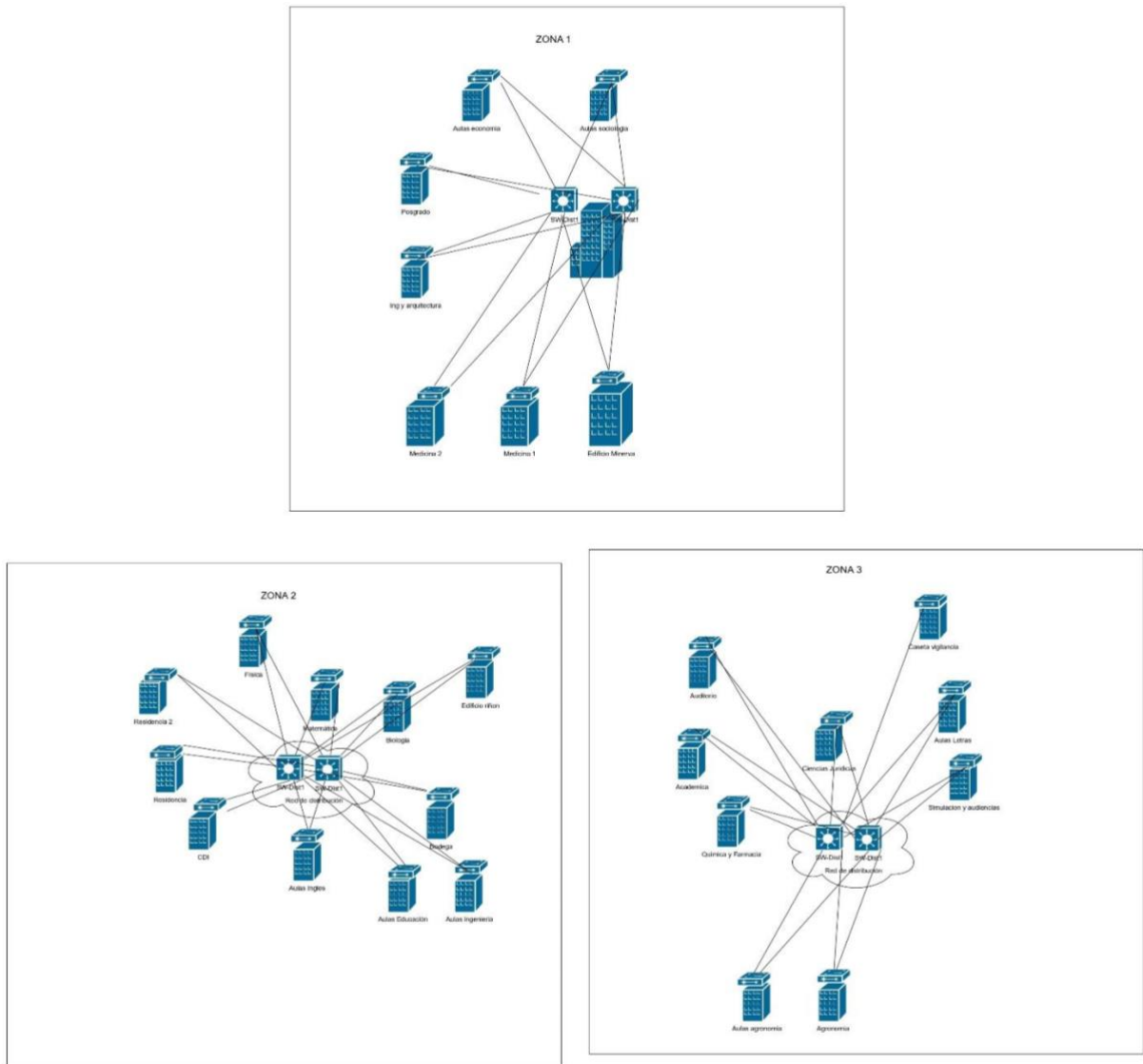
### **5.1.2. Beneficios de las soluciones propuestas**

Estas soluciones fortalecen la infraestructura tecnológica de la facultad, garantizando un entorno de comunicación más seguro, estable y escalable que optimiza los recursos existentes, reduce los tiempos de inactividad y permite la integración de nuevas tecnologías sin comprometer el rendimiento. Este nuevo diseño asegura una red moderna, eficiente compatible con las demandas tecnológicas actuales y futuras, permitiendo el crecimiento institucional y académico.

### **5.2. Topología de Red**

La topología de la red propuesta representa la estructura general del nuevo diseño de conectividad para la Universidad de El Salvador, Facultad Multidisciplinaria Oriental. Su función es mostrar cómo se interconectan los diferentes edificios, zonas y equipos de red dentro de la universidad, tanto en el nivel físico como nivel lógico. Estos diseños se crearon basados en el modelo jerárquico de tres capas, con el objetivo de mejorar la eficiencia, la escalabilidad y la tolerancia a fallos. La propuesta de la topología de red busca mejorar el rendimiento de la red, garantizando la disponibilidad del servicio y evitar caídas totales por medio de enlaces redundantes.

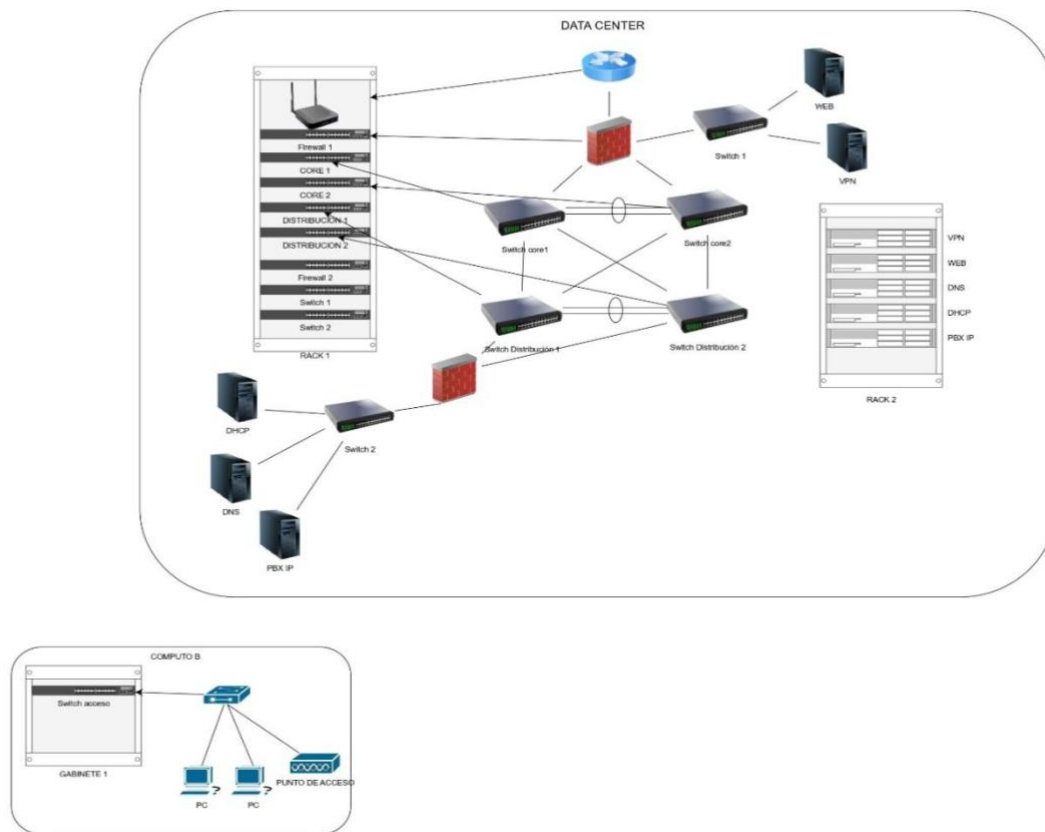
### 5.2.1. Topología Física por Zona



**Figura 21: Topología de Red Por Zonas.**

El diagrama muestra una topología física por zonas, es decir, cómo están organizados los equipos de red y los enlaces físicos que conectan los distintos edificios del campus. Se muestran dos switches de distribución ubicados en el edificio de biblioteca, se puede observar que cada edificio cuenta con dos enlaces, uno hacia cada switch de distribución.

## 5.2.2. Topología Física Biblioteca



*Figura 22: Topología Física Biblioteca.*

La topología física biblioteca representa la estructura propuesta de la red, mostrando la disposición de los equipos y cómo se interconectan mediante switches, firewalls y puntos de acceso.

En esta red de la biblioteca se observa una arquitectura jerárquica de tres capas: núcleo (Core), distribución, acceso.

### Capa de núcleo

Está compuesta por dos switches principales (Core1 y Core2) ubicados en RACK 1. Estos equipos son el punto central de conexión entre las capas de distribución, los firewalls y el Datacenter. Se conectan directamente a los firewalls y a los switches de distribución.

### Capa de distribución

Hay dos switches de distribución (Distribución 1 y Distribución 2), se encargan de concentrar las conexiones de las distintas áreas (por ejemplo, laboratorios, oficinas o salas de cómputo).

### Capa de acceso



La topología lógica muestra cómo se organiza el tráfico de red y cómo se comunican los distintos segmentos o subredes dentro de la infraestructura de la biblioteca. En este diagrama se muestra cómo fluyen los datos y cómo están segmentadas las redes mediante direcciones IP, routers y firewalls.

En el diagrama se pueden observar las siguientes áreas:

### **Zona perimetral**

Flujo: Internet – Firewall – Zona DMZ. En la DMZ se encuentra el servidor web, que es accesible desde el exterior, pero está aislado del resto de la red interna. El firewall controla qué tráfico puede entrar y salir de esta zona para proteger los sistemas internos.

### **Capa de núcleo**

Es el centro de la red, interconecta las diferentes áreas (Distribución, DMZ, Datacenter). A través del núcleo se enrutan las redes internas (por ejemplo, 10.10.0.0, 10.20.0.0, 10.30.0.0, etc.).

### **Capa de distribución**

Se encarga de dividir la red por áreas funcionales (Biblioteca, Decanato, Cómputo A/B, Laboratorio de Idiomas, Financiera, etc.). Cada segmento o VLAN tiene su propia red IP (por ejemplo, 10.10.0.0, 10.20.0.0...).

Capa de acceso (Usuarios y equipos finales)

### **Cada área tiene sus propios dispositivos conectados:**

- Computo A/B – Redes 10.101.0.0 y 10.103.0.0
- Biblioteca – Red 10.104.0.0 y 10.85.0.0
- Financiera y Decanato – Red 10.30.0.0
- Laboratorio de idiomas – Red 10.20.0.0
- Todos los segmentos cuentan con puntos de acceso Wi-Fi, PCs, e impresoras.

### **Datacenter o Servidores internos**

- Servidor DHCP: asigna direcciones IP a los clientes.
- Servidor DNS: resuelve nombres dentro de la red interna.
- PBX IP: maneja la telefonía interna.
- Servidores internos: aplicaciones o sistemas internos no accesibles desde Internet.
- Esta zona utiliza la red 10.60.0.0/26.

### 5.3. Segmentación Lógica

La segmentación de la propuesta de la nueva infraestructura se basó en el Subneteo de la IP 10.0.0.0/8.

**Tabla 40: Segmentación Lógica.**

Ubicación	VLAN ID	VLAN nombre	Subred	DHCP Rango	Función
Toda la universidad	99	Gestión	10.99.0.0/29	10.99.0.1 - 10.99.0.6	Administración de equipos
Toda la universidad	10	Administración	10.10.0.0/24	10.0.0.1- 10.0.0.254	Personal administrativo
Toda la universidad	20	VoIP	10.20.0.0/24	10.20.0.1 - 10.20.0.254	Telefonía IP
Toda la universidad	30	Impresoras	10.30.0.0/26	10.30.0.1 - 10.30.0.62	Impresoras
Toda la universidad	40	Pantallas	10.40.0.0/24	10.40.0.1 - 10.40.1.254	Pantallas interactivas
Toda la universidad	50	Cámaras	10.50.0.0/26	10.50.0.1 - 10.50.0.62	Red para videovigilancia
Datacenter	60	Servidores	10.60.0.0/28	10.60.0.1 - 10.60.0.14	Servidores internos
Datacenter	61	Servidores externos	10.61.0.0/29	10.61.0.1 - 10.61.0.6	Servidores externos
Toda la universidad	70	Invitados	10.70.0.0/23	10.70.0.1 - 10.70.1.254	Red Wifi sin contraseña para invitados
Toda la universidad	80	Docentes	10.80.0.0/23	10.80.0.1 - 10.80.1.254	Red cableada para docentes
Toda la universidad	81	Docentes Wifi	10.81.0.0/23	10.81.0.1 - 10.82.1.254	Red inalámbrica para docentes
Biblioteca	100	Estudiante-Biblioteca	10.100.0.0/23	10.100.0.1 - 10.100.1.254	Red inalámbrica para estudiantes
Biblioteca	101	Cómputo A	10.101.0.0/26	10.101.0.1 -	Red cableada

				10.101.0.62	cómputo A
Biblioteca	102	Cómputo B	10.102.0.0/26	10.101.0.1 - 10.101.0.62	Red cableada computo B
Biblioteca	103	UESED	10.103.0.0/25	10.103.0.1 - 10.103.0.126	Red cableada UESED
Biblioteca	104	Lab. Idiomas	10.104.0.0/26	10.104.0.1 - 10.104.0.62	Red cableada lab. Idiomas
Posgrado	105	Estudiante_postgrado	10.105.0.0/24	10.105.0.1 - 10.105.0.254	Red inalámbrica posgrado
Aulas economía	106	Estudiante_economia	10.106.0.0/24	10.106.0.1 - 10.106.0.254	Red inalámbrica
Aulas Sociología	107	Estudiante_sociologia	10.107.0.0/24	10.107.0.1 - 10.107.0.254	Red inalámbrica
Edificio riñón	108	Estudiante_riñón	10.108.0.0/24	10.108.0.1 - 10.108.0.254	Red inalámbrica
Administración académica	109	Estudiante_académica	10.109.0.0/24	10.109.0.1 - 10.109.0.254	Red inalámbrica
Edificio Minerva	110	Estudiante_minerva	10.110.0.0/23	10.110.0.1 - 10.110.1.254	Red inalámbrica
Medicina 1	111	Estudiante_medicina1	10.111.0.0/23	10.111.0.1 - 10.111.1.254	Red inalámbrica
Medicina 2	112	Estudiante_medicina2	10.112.0.0/23	10.112.0.1 - 10.112.1.254	Red inalámbrica
Matemática	113	Estudiante_matemática	10.113.0.0/24	10.113.0.1 - 10.113.0.254	Red inalámbrica
Física	114	Estudiante_fisica	10.114.0.0/24	10.114.0.1 - 10.114.0.254	Red inalámbrica
Biología	115	Estudiante_biología	10.115.0.0/24	10.115.0.1 - 10.115.0.254	Red inalámbrica
Química y	116	Estudiante_química_farmacia	10.116.0.0/24	10.116.0.1 -	Red inalámbrica

farmacia				10.116.0.254	
Ciencias Jurídicas	117	Estudiantes_jurídicas	10.117.0.0/24	10.117.0.1 - 10.117.0.254	Red inalámbrica
Agronomía	118	Estudiante_agronomía	10.118.0.0/24	10.118.0.1 - 10.118.0.254	Red inalámbrica
Aulas agronomía	119	Estudiante_agronomia_aulas	10.119.0.0/24	10.119.0.1 - 10.119.0.254	Red inalámbrica
Auditorio	120	Estudiante_auditorio	10.120.0.0/23	10.120.0.1 - 10.120.1.254	Red inalámbrica
Aulas letras	121	Estudiante_letras	10.121.0.0/24	10.121.0.1 - 10.121.0.254	Red inalámbrica
Aulas ingeniería	122	Estudiante_ingeniería	10.122.0.0/24	10.122.0.1 - 10.122.0.254	Red inalámbrica
Aulas educación	123	Estudiante_educación	10.123.0.0/24	10.123.0.1 - 10.123.0.254	Red inalámbrica
Aulas ingles	124	Estudiante_inglés	10.124.0.0/24	10.124.0.1 - 10.124.0.254	Red inalámbrica
CDI	125	Estudiante_CDI	10.125.0.0/25	10.125.0.1 - 10.125.0.126	Red inalámbrica
Residencia 1	126	Estudiante_residencia1	10.126.0.0/26	10.126.0.1 - 10.126.0.62	Red inalámbrica
Residencia 2	127	Estudiante_residencia2	10.127.0.0/26	10.127.0.1 - 10.127.0.62	Red inalámbrica
Simulación y audiencias	128	Estudiante_audiencias	10.127.0.0/24	10.127.0.1 - 10.127.0.254	Red inalámbrica
Bodega	129	Estudiante_bodega	10.129.0.0/24	10.129.0.1 - 10.129.0.254	Red inalámbrica
Caseta de vigilancia	130	Estudiante_vigilancia	10.130.0.0/25	10.130.0.1 - 10.130.0.126	Red inalámbrica
Ing. Y arquitectura	131	Estudiante_Ing_arquitectura	10.131.0.0/24	10.131.0.1 - 10.131.0.254	Red inalámbrica

**Nota:** En la tabla se muestran las direcciones IP asignadas a cada dispositivo que conforma la topología.

La segmentación lógica de la red se diseñó utilizando la dirección 10.0.0.0/8 y aplicamos el método de Subneteo. Lo principal fue dividir la red en diferentes VLANs según el tipo de usuario, servicio o área dentro de la universidad. Esto permite organizar mejor el tráfico, dar seguridad y evitar que todo quede en una sola red que pueda colapsar.

Para la segmentación lógica de la red se implementaron diferentes VLANs con el objetivo de organizar el tráfico, dar seguridad y facilitar la administración. Se tomó la red 10.0.0.0/8 y se fue dividiendo en subredes más pequeñas, asignadas a cada área y servicio de la universidad.

Para la gestión de equipos se creó la VLAN 99 con la subred 10.99.0.0/29, la cual solo dispone de 6 direcciones IP, suficientes para el control administrativo de la red. El personal administrativo se encuentra en la VLAN 10 con la subred 10.10.0.0/24, que ofrece 254 direcciones IP, mientras que la red de telefonía IP está en la VLAN 20 con la subred 10.20.0.0/24.

También, se reservó VLANs para servicios específicos, como impresoras (VLAN 30 con 10.30.0.0/26), pantallas interactivas (VLAN 40 con 10.40.0.0/24) y videovigilancia (VLAN 50 con 10.50.0.0/26). En el caso del DataCenter, se separaron los servidores internos en la VLAN 60 con la subred 10.60.0.0/28 y los servidores externos en la VLAN 61 con la subred 10.61.0.0/29.

Además, se pensó en los diferentes usuarios. Los invitados cuentan con su propia red WiFi en la VLAN 70 (10.70.0.0/23), mientras que los docentes tienen dos segmentos: uno cableado (VLAN 80 con 10.80.0.0/23) y otro inalámbrico (VLAN 81 con 10.81.0.0/23).

En cuanto a los estudiantes, se creó una segmentación más detallada: cada facultad, edificio o laboratorio tiene su propia VLAN y subred. Por ejemplo, en la biblioteca se encuentran la VLAN 100 para el WiFi, la 101 y 102 para los laboratorios de cómputo A y B, la 103 para UESED y la 104 para el laboratorio de idiomas. En posgrado, aulas de economía, sociología, medicina, matemáticas, letras, ingeniería, educación y otras áreas, cada grupo tiene su propia VLAN con subredes como 10.106.0.0/24, 10.111.0.0/23 o 10.121.0.0/24. También se incluyeron lugares específicos como el auditorio (VLAN 120), las residencias (126 y 127), el CDI (125), la caseta de vigilancia (130) y la facultad de ingeniería y arquitectura (131).

**Tabla 41: Direcciones IP utilizadas en switches L3 para capa de núcleo.**

Dispositivo	Puerto	Host	IP	Máscara	Barra
Switch-core-1	G0/3	10.0.0.0	10.0.0.3	255.255.255.252	/30
Switch-core-1	G0/4	10.0.0.8	10.0.0.9	255.255.255.252	/30
Switch-core-1	G01 y G02 (LACP)	10.0.0.16	10.0.0.17	255.255.255.252	/30
Switch-core-1	G0/5	10.0.0.20	10.0.0.21	255.255.255.252	/30
Switch-core-2	G0/1 y g0/2 (LACP)	10.0.0.18	10.0.0.16	255.255.255.252	/30
Switch-core-2	G0/3	10.0.0.4	10.0.0.12	255.255.255.252	/30
Switch-core-2	G0/4	10.0.0.12	10.0.0.13	255.255.255.252	/30
Switch-core-2	G0/5	10.0.0.24	10.0.0.25	255.255.255.252	/30

Switch-distribución-1	G0/1	10.0.0.0	10.0.0.2	255.255.255.252	/30
Switch-distribución-1	G0/2	10.0.0.4	10.0.0.6	255.255.255.252	/30
Switch-distribución-1	G0/7	10.0.0.28	10.0.0.29	255.255.255.252	/30
Switch-distribución-1	VRRP	10.10.0.0	10.10.0.1	255.255.255.0	/24
Switch-distribución-1	VRRP	10.20.0.0	10.20.0.1	255.255.255.0	/24
Switch-distribución-1	VRRP	10.80.0.0	10.80.0.1	255.255.254.0	/23
Switch-distribución-1	VRRP	10.100.0.0	10.100.0.1	255.255.254.0	/23
Switch-distribución-1	VRRP	10.101.0.0	10.101.0.1	255.255.255.192	/26
Switch-distribución-2	G0/1	10.0.0.8	10.0.0.10	255.255.255.252	/30
Switch-distribución-2	G0/2	10.0.0.12	10.0.0.14	255.255.255.252	/30
Switch-distribución-2	G0/7	10.0.0.32	10.0.0.33	255.255.255.252	/30
Switch-distribución-2	VRRP	10.10.0.0	10.10.0.1	255.255.255.0	/24
Switch-distribución-2	VRRP	10.20.0.0	10.20.0.1	255.255.255.0	/24
Switch-distribución-2	VRRP	10.80.0.0	10.80.0.1	255.255.254.0	/23
Switch-distribución-2	VRRP	10.100.0.0	10.100.0.1	255.255.254.0	/23
Switch-distribución-2	VRRP	10.101.0.0	10.101.0.1	255.255.255.192	/26

La Tabla muestra la asignación de direcciones IP en los switches de núcleo y distribución. Se observa un esquema con enlaces punto a punto (/30) para las interconexiones, lo cual permite un uso eficiente del direccionamiento y facilita la identificación de fallas. Además, se implementa VRRP en las VLANs principales, lo que proporciona redundancia y alta disponibilidad en los Gateways virtuales.

**Tabla 42: Dirección de VLANs en switches.**

Dispositivo	VLAN	Host	IP	Máscara	Barra
Switch-distribución-1	10	10.10.0.0	10.10.0.2	255.255.255.0	/24
Switch-distribución-1	20	10.20.0.0	10.20.0.2	255.255.255.0	/24
Switch-distribución-1	80	10.80.0.0	10.80.0.2	255.255.254.0	/23
Switch-distribución-1	100	10.100.0.0	10.100.0.2	255.255.254.0	/23
Switch-distribución-1	101	10.101.0.0	10.101.0.2	255.255.255.192	/26
Switch-distribución-1	99	10.99.0.0	10.99.0.3	255.255.255.240	/28
Switch-distribución-2	10	10.10.0.0	10.10.0.3	255.255.255.0	/24
Switch-distribución-2	20	10.20.0.0	10.20.0.3	255.255.255.0	/24
Switch-distribución-2	80	10.80.0.0	10.80.0.3	255.255.254.0	/23
Switch-distribución-2	100	10.100.0.0	10.100.0.3	255.255.254.0	/23
Switch-distribución-2	101	10.101.0.0	10.101.0.3	255.255.255.192	/26
Switch-distribución-2	99	10.99.0.0	10.99.0.4	255.255.255.240	/28

La Tabla presenta la asignación de direcciones IP a las VLANs de los switches de distribución. Se aprecia que las VLANs se encuentran bien diferenciadas para distintos propósitos (usuarios, administrativos, servidores, gestión), con máscaras que varían entre /24, /23 y /26 según la densidad esperada de dispositivos.

**Tabla 43: Direcciones IP en servidores.**

Dispositivo	Puerto	Host	IP	Máscara	Barra
DHCP	enp0s3	10.60.0.0	10.60.0.2	255.255.255.240	/28
IP PBX	enp0s3	10.60.0.0	10.60.0.3	255.255.255.240	/28
DNS	enp0s3	10.60.0.0	10.60.0.4	255.255.255.240	/28

Servidor web	enp0s3	10.61.0.0	10.61.0.2	255.255.255.248	/29
Servidor VPN	enp0s3	10.61.0.0	10.61.0.3	255.255.255.248	/29

La Tabla muestra las direcciones asignadas a los servidores principales (DHCP, IP PBX, DNS, web y VPN). Se muestra que los servidores se encuentran distribuidos en subredes pequeñas (/28 y /29), lo cual es adecuado ya que limita el tamaño del dominio de broadcast y mejora la seguridad. Además, la separación por funciones críticas (telefonía IP, DNS, web, VPN) favorece la segmentación de servicios y facilita la aplicación de políticas de firewall más específicas.

**Tabla 44: Direcciones IP firewall.**

Dispositivo	Puerto	Host	IP	Máscara	Barra
Firewall 1	em2	10.0.0.20	10.0.0.22	255.255.255.252	/30
Firewall 1	em3	10.0.0.24	10.0.0.26	255.255.255.252	/30
Firewall 1	em4	10.61.0.0	10.61.0.1	255.255.255.248	/29
Firewall 2	em2	10.0.0.28	10.0.0.30	255.255.255.252	/30
Firewall 2	em3	10.0.0.32	10.0.0.34	255.255.255.252	/30
Firewall 2	em4	10.60.0.1	10.60.0.0	255.255.255.240	/28

La Tabla muestra la configuración de interfaces en los firewalls redundantes. Se observa el uso de enlaces punto a punto (/30) hacia el núcleo y distribución, junto con subredes más pequeñas (/28 y /29) para la interconexión con servidores y servicios críticos. Este esquema permite un control granular del tráfico y mejora la seguridad perimetral.

## **6. JUSTIFICACIÓN TÉCNICA Y ECONÓMICA.**

### **6.1. Justificación Técnica**

La Universidad de El Salvador, Facultad Multidisciplinaria Oriental, cuenta con una infraestructura de red que constituye una base sólida para el funcionamiento de los servicios académicos, administrativos y tecnológicos. Dicha infraestructura está compuesta por equipos de alto rendimiento de marcas reconocidas como Huawei y Cisco, instalados en el DataCenter y distribuidos estratégicamente en distintos puntos del Campus. Esta plataforma tecnológica ofrece las condiciones necesarias para llevar a cabo una actualización integral de la red, aprovechando los recursos existentes y garantizando una administración más eficiente de los sistemas de comunicación institucionales.

La propuesta de mejora responde a la necesidad de optimizar el rendimiento de la infraestructura mediante la implementación de mecanismos que incrementen la eficiencia operativa, la disponibilidad del servicio y la capacidad de adaptación a futuras demandas tecnológicas. Entre las acciones planteadas se incluye la segmentación lógica mediante VLAN, la cual permite un control más eficaz del tráfico de datos, reduciendo la congestión y los conflictos de transmisión. Asimismo, la automatización en la asignación de direcciones IP a través del protocolo DHCP elimina procesos manuales y acelera la configuración de dispositivos, garantizando acceso inmediato y confiable a los recursos de red para estudiantes, docentes y personal administrativo.

El diseño propuesto incorpora alta disponibilidad y redundancia como principios fundamentales, de modo que ante cualquier eventualidad se disponga de rutas y enlaces alternos que aseguren la continuidad de los servicios críticos. Esta característica permite mantener en funcionamiento los sistemas administrativos, plataformas virtuales y demás recursos institucionales, minimizando el tiempo de inactividad y aumentando la resiliencia de la red.

En el ámbito de recursos humanos, la Facultad cuenta con personal técnico capacitado en administración y mantenimiento de redes, así como con estudiantes y egresados de Ingeniería de Sistemas Informáticos que poseen las competencias necesarias para participar en proyectos de mejora tecnológica. Este capital humano representa una ventaja significativa para la implementación y sostenibilidad de la propuesta, al combinar conocimientos teóricos con experiencia práctica. No obstante, se recomienda fortalecer las capacidades existentes mediante programas de capacitación continua en áreas como seguridad informática, virtualización, monitoreo y gestión avanzada de redes, con el fin de mantener actualizado al personal frente a las tendencias tecnológicas.

Estos elementos técnicos, humanos y estructurales en su totalidad justifican la viabilidad de la propuesta y demuestran que la Facultad Multidisciplinaria Oriental posee las condiciones necesarias para consolidar una red moderna, segura, escalable y alineada con los objetivos estratégicos de la Universidad de El Salvador.

## 6.2. Justificación Económica

La propuesta presentada cumple con criterios técnicos económicos, y es viable ya que la Universidad dispone de tecnología existente que puede aprovecharse para la administración y modernización de la red. Sin embargo, se requiere realizar ajustes y proponemos solventar algunos ajustes de falla en los equipos actualmente instalados e implementar un nuevo tendido de fibra óptica que cubra la totalidad del campus, con el fin de mejorar la conectividad, velocidad y el rendimiento general de la infraestructura de red. Aunque la Universidad cuenta con personal técnico capacitado en administración y mantenimiento de redes, este recurso no resulta suficiente para una implementación de gran magnitud; por ello se sugiere involucrar a estudiantes de ingeniería de sistemas informáticos como apoyo en labores técnicas y de instalación, reduciendo así los costos de ejecución. Esta propuesta es factible porque la Universidad posee la capacidad técnica y económica.


Para esta propuesta se sugiere cambiar algunos equipos, a continuación, se muestran los equipos que se plantean cambiar.


Para la propuesta de mejora se realizó una cotización para 9,020 metros aproximadamente de fibra óptica, y se propone adquirir 10 km de materiales, ya que durante la instalación pueden ocurrir daños en tramos pequeños, dejando márgenes por empalmes o cortes. Esta cantidad se determinó en base a que la red se diseñó con un esquema de redundancia, lo que implica la instalación de un doble tendido de fibra óptica hacia cada switch de acceso para que esté conectado con switch de distribución. De esta forma, desde el Datacenter se desplegarán enlaces independientes hacia cada uno de los switches de acceso ubicados en los distintos edificios de la Universidad de El Salvador, Facultad Multidisciplinaria oriental, garantizando así la disponibilidad, tolerancia, fiabilidad ante fallos y continuidad del servicio.

Los equipos propuestos, HUAWEI S5736-S24UM4XC, Conmutadores multi-GE serie S5736-S de Huawei CloudEngine S5736-S24UM4XC: 24 puertos Ethernet de 100 M/1G/2,5G/5G/10G Base-T, 4 puertos SFP+ de 10 GE. Este modelo de switches será ubicado en las siguientes zonas: Cómputo redes 3, Cómputo de redes 1 y 2. También se hará el cambio de D'LINK DE-1210 que está ubicado en oficina UESED.

Para el desarrollo de la propuesta se tiene un estimado de una inversión de unos \$17,417.52 dólares que sería para la compra de equipos y materiales necesarios para la mejora de la red.

**Tabla 45: Equipos Propuestos.**

Cantidad	Nuevo equipo	Imagen	Precio Unitario	Precio Total
4	<p>HUAWEI S5736-S24UM4XC</p> <p>Conmutadores multi-GE serie S5736-S de Huawei CloudEngine S5736-S24UM4XC: 24 puertos Ethernet de 100 M/1G/2,5G/5G/10G Base-T, 4 puertos SFP+ de 10 GE</p> <p>Enlace de compra:  <a href="https://www.grupososa.com.ve/">https://www.grupososa.com.ve/</a></p>		\$5,092.76	\$20,371.04

2 bobinas (5 KM c/u)	Fibra Óptica Monomodo  Fibra Optica ADSS24H 150 SPAN.  Enlace de compra <a href="https://fointer.com/product/fibra-optica-adss-2/">https://fointer.com/product/fibra-optica-adss-2/</a>		\$3,616.00	\$7,232.00
<b>Total</b>				\$17,417.52

*Tabla 46: Medidas de Fibra Óptica.*

Nº	Origen	Destino	Distancia (m)
1	Biblioteca	Edificio Minerva	130 m
2	Biblioteca	Depto. Ingeniería y Arquitectura	85 m
3	Biblioteca	Riñón	150
4	Biblioteca	Medicina 1	180
5	Biblioteca	Medicina 2	210
6	Biblioteca	Residencia 1	230
7	Biblioteca	Residencia 2	265
8	Biblioteca	CDI	270
9	Biblioteca	Física	140
10	Biblioteca	Matemática	160
11	Biblioteca	Aulas de ingeniería y Arq.	210
12	Biblioteca	Aulas de inglés	200

13	Biblioteca	Aulas de educación	210
14	Biblioteca	Biología	145
15	Biblioteca	Agronomía	360
16	Biblioteca	Académica	170
17	Biblioteca	CCJJ	210
18	Biblioteca	Simulación	220
19	Biblioteca	Aulas de letras	210
20	Biblioteca	Vigilancias	235
21	Biblioteca	Auditorio	135
22	Biblioteca	Aulas de sociología	60
23	Biblioteca	Postgrado	60
24	Biblioteca	Aula de economía	70
25	Biblioteca	Química y farmacia	195
Total			4,510 m

## 7. METODOLOGÍA DE TRABAJO

Para este proyecto, se utilizó un enfoque de metodología mixta, con un propósito descriptivo, analítico y propositivo, porque buscaba entender cómo está la red actualmente, analizar sus problemas y proponer soluciones. Es descriptiva porque se documentó cómo está organizada la red de la Universidad de El Salvador, Facultad Multidisciplinaria Oriental; es analítica porque se identificaron los principales problemas, como la falta de redundancia, mal uso de direcciones IP; y es propositiva porque, con esa información, se diseñó una red más segura, estable y eficiente.

Primero, en el enfoque descriptivo, se documentó la situación actual de la red usando la información proporcionada por la universidad, incluyendo la topología, las direcciones IP y la distribución de los equipos. Además, se nos permitió hacer una visita guiada al DataCenter en un día, lo que facilitó observar directamente la infraestructura, el funcionamiento de los switches, routers y servidores, y el estado físico de las conexiones.

Con toda la información recopilada, se analizaron los problemas de la red. Se encontró que le falta redundancia en la infraestructura, ya que la topología actual solo tiene un enlace hacia cada switch de distribución; si ese enlace se corta, se perdería la conectividad en esa área. La ingeniera encargada explicó que los switches de distribución están apilados (stackeados) para contar con un respaldo, pero el cambio se realiza de forma manual. En nuestra propuesta, este proceso se implementa de manera automática, garantizando continuidad del servicio sin intervención humana.

Con toda la información recopilada, se analizaron los problemas de la red. Se encontró que le falta redundancia en la infraestructura. También, la segmentación mediante VLAN existente puede mejorarse para optimizar el tráfico y aumentar la seguridad entre departamentos. Este análisis ayuda a entender las causas de las fallas y los riesgos futuros.

A partir del diagnóstico, se propuso un diseño de red en jerarquía, basado en el modelo de tres capas (acceso, distribución y núcleo). Incluye enlaces redundantes para evitar caídas del servicio, mejoras en la segmentación mediante VLANs para subir la eficiencia y la seguridad. Se crearon diagramas lógicos y jerárquicos de la propuesta, y se probaron diferentes escenarios para asegurar que el diseño soporte interrupciones sin dejar sin servicio.

Esta metodología asegura que el proyecto se base no solo en teoría, sino también en evidencia concreta, a través de observaciones. Combina el análisis con soluciones prácticas para una mejor implementación.

## 8. CONCLUSIÓN Y RECOMENDACIONES

En conclusión, el desarrollo de la propuesta de la nueva infraestructura de la red del campus de la Universidad de El Salvador, Facultad Multidisciplinaria Oriental, permite establecer una estructura robusta diseñado en arquitectura jerárquica de 3 capas, lo que facilita la administración centralizada, switches gestionables, enlaces troncales, enrutamientos por VLANs, redundancia y alto rendimiento.

La propuesta desarrollada facilita la administración y el control del tráfico, además proporciona mayor estabilidad y escalabilidad para el soporte de crecimiento y la incorporación de nuevos servicios. La integración de VLANs, firewall, switches L2 y switches L3, garantizan una segmentación adecuada, mayor seguridad y disponibilidad de los recursos. Además, incorpora políticas de seguridad, monitoreo constante y mecanismos de alta disponibilidad, asegura que la infraestructura no solo es moderna sino también confiable frente a las amenazas y exigencia del entorno digital actual.

Esta propuesta no solo mejora el rendimiento operativo de la red universitaria, sino que garantiza la continuidad de confiabilidad y redundancia en un entorno académico donde la alta disponibilidad de la red es esencial. la infraestructura de red escalable permitirá a la institución afrontar con solidez los futuros desafíos tecnológicos.

### Recomendaciones

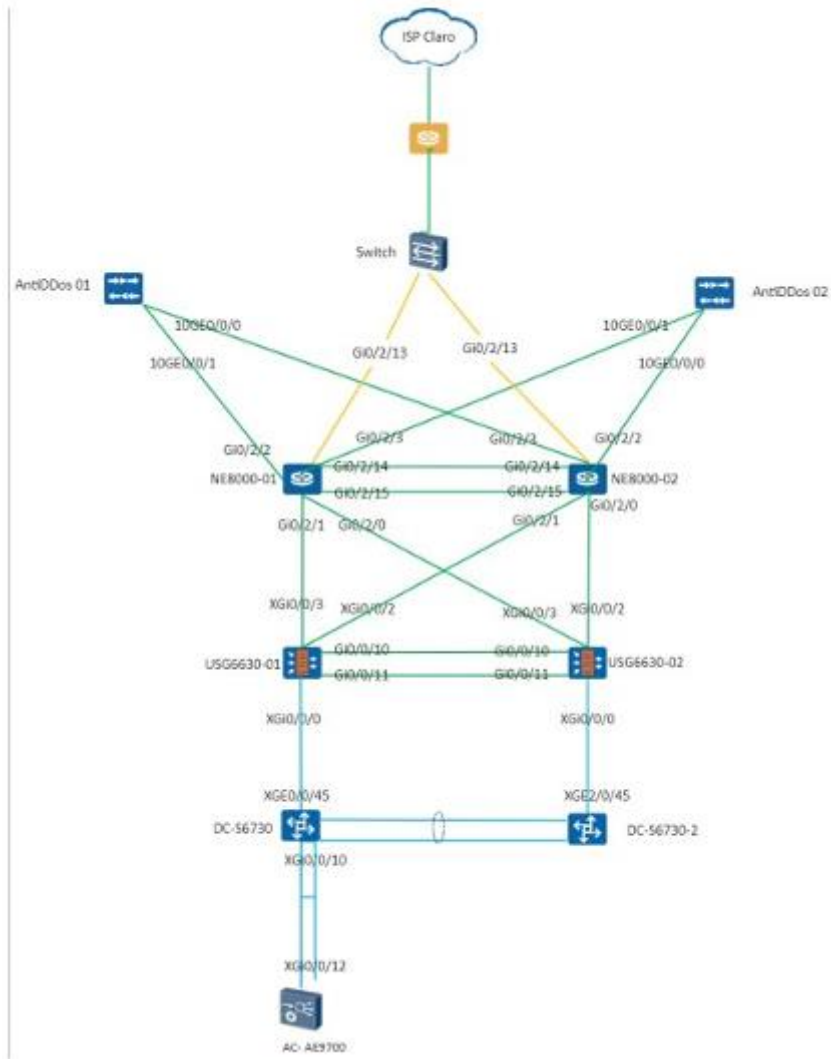
1. Implementar enlaces redundantes entre cada edificio y ambos switches de distribución. Cada switch de acceso debe tener al menos 2 uplinks físicos para distribución (o LACP hacia un par de puertos agregados).
2. Configurar agregación de enlaces (LACP) en uplinks críticos y en interconexiones entre distribución y núcleo para aumentar ancho de banda y resiliencia.
3. Implementar Gateway virtuales redundantes con VRRP en las VLANs de usuario críticas (administración, servidores, voz). Configurar prioridades y tiempos adecuados para failover rápido.
4. Evitar subredes /20 salvo que se justifique por gran densidad. Preferir bloques /24 o /26 según necesidad
5. Reasignar las subredes grandes actuales (/20) a bloques más pequeños para reducir broadcast Domains y mejorar control. Crear un inventario de APs y mapear dispositivos antes del recorte.
6. Inventario y CMDB: registrar todos los dispositivos, firmware y configuración.
7. Habilitar autenticación 802.1X para puertos críticos y Wi-Fi empresarial con RADIUS (FreeRADIUS / Windows NPS) para distinguir usuarios y aplicar políticas

## REFERENCIAS

- [1] J. E. BARAJAS MARISCAL, «Redes de Computadoras,» de *Redes de Computadoras*, México, 2018. Available: [REDES DE COMPUTADORAS.pdf](#)
- [2] D. J. W. Andrew S. Tanenbaum, *Redes de Computadoras* 5a. edición, México: Pearson, 2011.
- [3] F. O. Arciniega Martínez, «¿Qué son las Topologías de Red?,» 2023. Available: <https://fernandoarciniega.com/que-son-las-topologias-de-red/>
- [4] Red Hat y sus Partners, «Infraestructura de red con Red Hat y sus Partners,» Red Ht, Available: <https://www.redhat.com/es/partners/network-infrastructure>
- [5] Cloudflare, Inc, «"¿Qué es una red de área de campus (CAN)?",» 2025. Available: <https://www.cloudflare.com/es-es/learning/network-layer/what-is-a-campus-area-network/>
- [6] Systems, Cisco, «Resumen de Diseño de la Red LAN inalámbrica de Campus,» 1 Abril 2014. Available [https://www.cisco.com/c/dam/r/es/la/internet-of-everything-ioe/assets/pdfs/en-05\\_campus-wireless\\_wp\\_cte\\_es-xl\\_42333.pdf](https://www.cisco.com/c/dam/r/es/la/internet-of-everything-ioe/assets/pdfs/en-05_campus-wireless_wp_cte_es-xl_42333.pdf)
- [7] Redesinformaticas.org, «Redes CAN: ¿Qué son? Características, ventajas y desventajas,» 2023. Available: [https://redesinformaticas.org/red-can/?utm\\_source](https://redesinformaticas.org/red-can/?utm_source)
- [8] M. H. Cervantes, «Administración de la red,» CUAED-UNAM, 2017. Available: [https://programas.cuaed.unam.mx/repositorio/moodle/pluginfile.php/931/mod\\_resource/content/4/contenido/index.html](https://programas.cuaed.unam.mx/repositorio/moodle/pluginfile.php/931/mod_resource/content/4/contenido/index.html)
- [9] «Anexo Planificación Redes y subredes,» de *práctica/laboratorio: Redes de Computadores. Laboratorio. Práctica 2. Planificación de redes y subredes*, 2018.
- [10] Unknown, «Principales elementos de una RED,» 28 Octubre 2012. Available: <https://elementosderedadpq.blogspot.com/2012/10/principales-componentes-de-una-red.html>
- [11] A. S. TANENBAUM, "Redes de Computadoras", 4ta ed., México: Pearson, 2003.

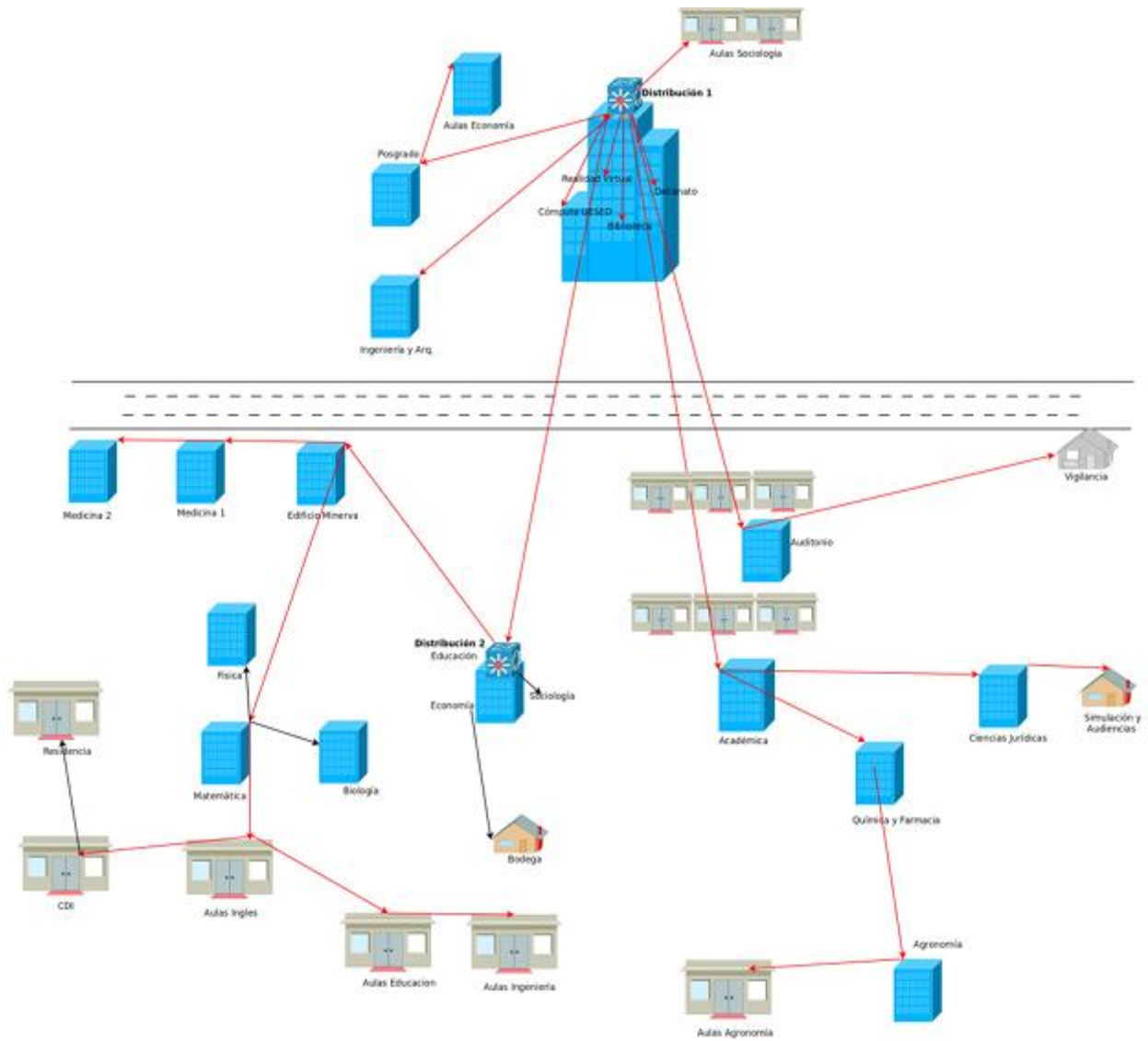
ANEXOS Y DIAGRAMAS

Topología de la Situación Actual FMO-UES



Anexo 1: Topología de Enlace Principal

## Topología Física Actual UES-FMO



*Anexo 2: Topología Física Actual.*



*Anexo 3: Enlaces Principales Ubicados en El Datacenter.*

## **CONFIGURACIÓN DE EQUIPOS DE LA NUEVA PROPUESTA**

### **Configuración en Switches de Acceso.**

# Crear bridge con VLAN filtering y RSTP por defecto

/Interface bridge

add name=bridge-access VLANs-filtering=yes

### **# Asignar puertos troncales al bridge**

/Interface bridge port

add bridge=bridge-access interface=ether1

add bridge=bridge-access interface=ether2

### **Configuración en switches de distribución**

# Crear bridge con VLAN filtering

/Interface bridge

add name=bridge-dist vlan-filtering=yes

### **#Configuración de troncales a switches de acceso**

/Interface bridge port

add bridge=bridge-dist interface=ether3

add bridge=bridge-dist interface=ether4

add bridge=bridge-dist interface=ether5

add bridge=bridge-dist interface=ether6

/Ip address

add address=10.10.0.2/24 interface= Vlan10-dist1

add address=10.20.0.2/24 interface= Vlan20 -dist1

add address=10.80.0.2/23 interface=Vlan80-dist1

add address=10.101.0.2/23 interface=Vlan100-dist1

add address=10.101.0.2/24interface=Vlan101-dist1

### **# Configurar VRRP para VLAN 10**

```
/interface vrrp  
add name=vrrp10 interface= Vlan10-dist1 vrid=10 priority=110  
  
# Dirección virtual  
  
/Ip address  
add address=10.10.0.1/24 interface=vrrp10
```

### **# Configurar VRRP para VLAN 20**

```
/interface vrrp  
add name=vrrp20 interface=vlan20-dist1 vrid=20 priority=110  
  
/ip address  
add address=10.20.0.1/24 interface=vrrp20
```

### **# Configurar VRRP para VLAN 80**

```
/interface vrrp  
add name=vrrp80 interface=vlan80-dist1 vrid=80 priority=110  
  
/ip address  
add address=10.80.0.1/23 interface=vrrp80
```

### **# Configurar VRRP para VLAN 100**

```
/interface vrrp  
add name=vrrp100 interface=vlan100-dist1 vrid=100 priority=110  
  
/ip address  
add address=10.100.0.1/23 interface=vrrp100  
add address=10.101.0.1/26 interface=vrrp101
```

### **# Configurar VRRP para VLAN 101**

```
/interface vrrp
```

```
add name=vrrp101 interface=vlan101-dist1 vrid=101 priority=110
```

```
/ip address
```

## **Configuración de OSPF**

### **# Instancia OSPF**

```
/routing ospf instance
```

```
add name=ospf-dist router-id=3.3.3.3
```

### **# Área backbone**

```
/routing ospf area
```

```
add name=backbone area-id=0.0.0.0 instance=ospf1
```

### **# Plantillas de Interfaz**

```
/routing ospf interface-template
```

### **# Enlace hacia core**

```
add area=backbone interfaces=ether1
```

```
add area=backbone interfaces=ether2
```

### **# VLANs**

```
add area=backbone interfaces=vlan10-dist1
```

```
add area=backbone interfaces=vlan20-dist1
```

```
add area=backbone interfaces=vlan80-dist1
```

```
add area=backbone interfaces=vlan100-dist1
```

```
add area=backbone interfaces=vlan101-dist1
```

## **Configuración de Switch core 1**

### **Configuración de OSPF**

### # Instancia principal

```
/routing ospf instance
```

```
add name=ospf-core router-id=1.1.1.1
```

### # Área backbone

```
/routing ospf area
```

```
add name=backbone area-id=0.0.0.0 instance=ospf1
```

### # Plantillas de interfaz OSPF

```
/routing ospf interface-template
```

### # Enlaces hacia distribución

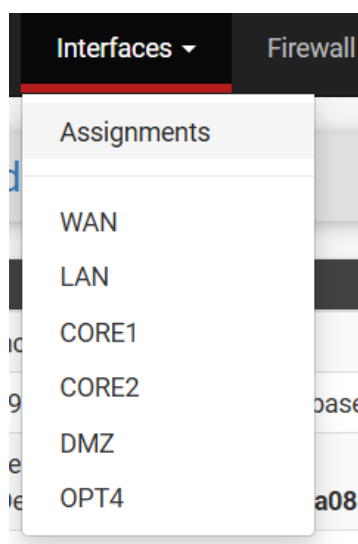
```
add area=backbone interfaces=ether3 Dist1
```

```
add area=backbone interfaces=ether4 Dist2
```

### Configuración de firewall (PfSense)

Para configurar pfSense se accede a la interfaz web a través de una ip

Primero configuramos las interfaces



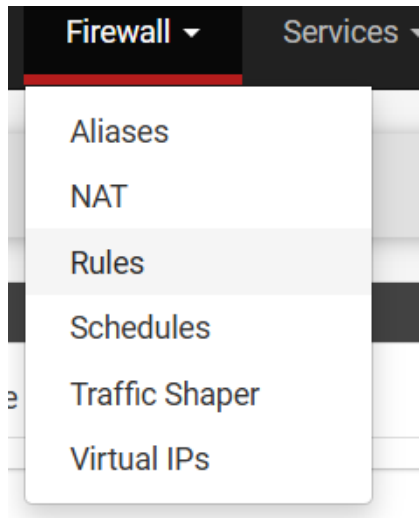
Damos clic en la interfaz que queremos configurar por ejemplo core1(interfaz conectada a switch core 1)

Se mostrará el siguiente menú:

<b>Enable</b>	<input checked="" type="checkbox"/> Enable interface
<b>Description</b>	<input type="text" value="CORE1"/> Enter a description (name) for the interface here.
<b>IPv4 Configuration Type</b>	<input type="text" value="Static IPv4"/>
<b>IPv6 Configuration Type</b>	<input type="text" value="None"/>
<b>MAC Address</b>	<input type="text" value="XXXXXXXXXXXX"/> This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.
<b>MTU</b>	<input type="text"/> If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
<b>MSS</b>	<input type="text"/> If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.
<b>Speed and Duplex</b>	<input type="text" value="Default (no preference, typically autoselect)"/> Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.
<b>Static IPv4 Configuration</b>	
<b>IPv4 Address</b>	<input type="text" value="10.0.10.22"/> / <input type="text" value="30"/>
<b>IPv4 Upstream gateway</b>	<input type="text" value="None"/> <input type="button" value="+ Add a new gateway"/> If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button. On local area network interfaces the upstream gateway should be "none". Selecting an upstream gateway causes the firewall to treat this interface as a <b>WAN type interface</b> .

Seleccionamos tipo de configuración "IPv4 Configuration Type" y seleccionamos "Static IPv4" y en "IPv4 Address" ingresamos la Ip, luego guardamos la configuración dando clic en botón "Save" que aparece al final del menú.

**Para asignar reglas vamos a firewall > rules**



Y asignamos las reglas

Para permitir el tráfico de la LAN

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/0 B	IPv4 UDP	*	*	*	*	none			
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	*	*	*	*	none			

Reglas para permitir el acceso a los servicios internos

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/0 B	IPv4 UDP	*	*	*	67 - 68	none			
<input type="checkbox"/>	✓	0/0 B	IPv4 UDP	*	*	10.60.0.0/28	53 (DNS)	none			
<input type="checkbox"/>	✓	0/0 B	IPv4 UDP	10.20.0.0/23	*	10.60.0.3	*	none			

## Configuración de Servidor DHCP

Primero se actualizan los repositorios y se descarga el paquete isc-dhcp-server

```
apt update-y
```

```
apt-get install isc-dhcp-server -y
```

Luego se accede al archivo de configuración isc-dhcp-server para agregar la interfaz por donde va a escuchar las peticiones de DHCP.

```
sudo nano /etc/default/isc-dhcp-server
```

```
INTERFACESv4="enp0s3"
```

Luego accedemos al archivo de configuración del servidor.

```
sudo nano /etc/dhcp/dhcpd.conf
```

### **se agrega la configuración para VLANs**

# Configuración global

default-lease-time 600;

max-lease-time 7200;

authoritative;

#### **# VLAN 10 - 10.10.0.0/24**

subnet 10.10.0.0 netmask 255.255.255.0 {

  range 10.10.0.4 10.10.0.200;

  option routers 10.10.0.1;

  option domain-name-servers 10.60.0.4;

}

#### **# VLAN 20 - 10.20.0.0/24**

subnet 10.20.0.0 netmask 255.255.255.0 {

  range 10.20.0.4 10.20.0.200;

  option routers 10.20.0.1;

  option domain-name-servers 10.60.0.4;

}

#### **# VLAN 80 - 10.80.0.0/23**

subnet 10.80.0.0 netmask 255.255.254.0 {

  range 10.80.0.4 10.80.1.200;

  option routers 10.80.0.1;

  option domain-name-servers 10.60.0.4;

}

#### **# VLAN 100 - 10.100.0.0/23**

subnet 10.100.0.0 netmask 255.255.254.0 {

```
range 10.100.0.4 10.100.1.200;

option routers 10.100.0.1;

option domain-name-servers 10.60.0.4;

}
```

#### **# VLAN 101 - 10.101.0.0/24**

```
subnet 10.101.0.0 netmask 255.255.255.0 {

    range 10.101.0.50 10.101.0.200;

    option routers 10.101.0.1;

    option domain-name-servers 10.60.0.4;

}
```

Por último, iniciamos el servicio

```
sudo systemctl start isc-dhcp-server
```

### **Configuración de servidor DNS**

#### **Primero actualiza los repositorios y se instala el paquete bind9**

```
sudo apt update
```

```
sudo apt install bind9 bind9-utils bind9-doc -y
```

#### **Luego accedemos al siguiente archivo**

```
sudo nano /etc/bind/named.conf.options
```

#### **Agregamos las siguientes configuraciones**

```
options {

    directory "/var/cache/bind";

    recursión yes;          # Permite consultas recursivas (LAN)

    allow-query { any; };  # Permitir consultas desde cualquier cliente interno
```

```

allow-recursion {127.0.0.1; 10.60.0.0/26; 10.20.0.0/24; 10.80.0.0/23;};

allow-query-cache {127.0.0.1; 10.60.0.0/26, 10.20.0.0/24; 10.80.0.0/23;};

forwarders {

    8.8.8.8;

    8.8.4.4;

};

dnssec-validation no;

listen-on-v6 { none; };

listen-on { 127.0.0.1; 10.60.0.4; };

};

```

### **Luego configuramos el archivo de zona local**

#### **Primero accedemos al archivo para declarar el archivo de zona**

```
sudo nano /etc/bind/named.conf.local
```

#### **se agrega la siguiente configuración**

```

zone "universidadfmo.edu.sv" {

    type master;

    file "/etc/bind/db.universidadfmo.edu.sv";

};

```

#### **Luego creamos y accedemos al archivo de zona**

```
sudo nano /etc/bind/db.universidadfmo.edu.sv
```

#### **Agregamos las siguientes configuraciones al archivo de zona local**

```

$TTL 604800

@ IN SOA ns.universidadfmo.edu.sv. admin.universidadfmo.edu.sv. (
    2025093001 ; Serial
    604800 ; Refresh
    86400 ; Retry

```

2419200 ; Expire

604800 ) ; Negative Cache TTL

; Servidor DNS

@ IN NS ns.universidadfmo.edu.sv.

ns IN A 10.61.0.2

www IN A 10.61.0.3

dhcp IN A 10.60.0.2

### **Por último, habilitamos e iniciamos el servicio**

```
sudo systemctl restart bind9
```

```
sudo systemctl enable bind9
```

### **Configuración de servidor IP PBX**

#### **Primero actualizamos los repositorios e instalamos Asterisk**

```
sudo apt update
```

```
sudo apt install asterisk -y
```

#### **luego accedemos**

```
sudo nano /etc/asterisk/pjsip.conf
```

#### **y agregamos la configuración para los usuarios**

```
; ===== CONFIGURACIÓN GLOBAL =====
```

```
[transport-udp]
```

```
type=transport
```

```
protocol=udp
```

```
bind=0.0.0.0
```

; ===== Usuario 1001 =====

[1001]

type=endpoint

context=internos

disallow=all

allow=ulaw

auth=auth1001

aors=1001

[auth1001]

type=auth

auth\_type=userpass

username=1001

password=clave 1001

[1001]

type=aor

max\_contacts=1

; ===== Usuario 1002 =====

[1002]

type=endpoint

context=internos

disallow=all

allow=ulaw

auth=auth1002

aors=1002

```
[auth1002]
type=auth
auth_type=userpass
username=1002
password=clave1002
```

```
[1002]
type=aor
max_contacts=1
```

**luego accedemos al archivo extensión.conf y agregamos la siguiente configuración**

```
sudo /etc/asterisk/extension.conf
```

```
[general]
```

```
static = yes
```

```
writeprotect = no
```

```
[internos]
```

```
exten => 1001,1,Dial(PJSIP/1001,20)
```

```
same => n Hangup()
```

```
exten => 1002,1,Dial(PJSIP/1002,20)
```

```
same => n Hangup()
```

Por último reiniciamos el servicio asterisk

```
sudo systemctl restart asterisk
```

### **Configuración de servidor web**

Primero actualizamos los repositorios, usaremos el stack LAMP (Linux, Apache, MySQL/MariaDB y PHP) ejecutamos el siguiente comando para instalar las herramientas necesarias.

```
sudo apt update
```

```
sudo apt install apache2 mariadb-server php libapache2-mod-php php-mysql git unzip -y
```

### **Habilitamos apache**

```
sudo systemctl enable apache2
```

```
sudo systemctl start apache2
```

### **Accedemos al cliente MySQL**

```
sudo mysql -u root
```

### **Creamos base de datos y usuario para el proyecto**

```
CREATE DATABASE proyectodb;
```

```
CREATE USER 'proyecto'@'localhost' IDENTIFIED BY 'clave123';
```

```
GRANT ALL PRIVILEGES ON proyectodb.* TO 'proyecto'@'localhost';
```

```
FLUSH PRIVILEGES;
```

```
EXIT;
```

### **Navegamos a la carpeta html y descargamos un proyecto que use SQL y PHP que tengamos en github**

```
cd /var/www/html/
```

```
sudo rm index.html
```

```
sudo git clone [enlace al repositorio donde esté el proyecto]
```

### **Damos los permisos necesarios al proyecto**

```
sudo chown -R www-data:www-data /var/www/html/proyecto
```

```
sudo chmod -R 755 /var/www/html/proyecto
```

### **Importamos base de datos del proyecto (Opcional)**

```
mysql -u proyecto -p proyectodb < /var/www/html/proyecto/database.sql
```

## **Configuración de server vpn**

### **Actualizamos los repositorios e instalamos openvpn**

```
sudo apt update
```

```
sudo apt install openvpn easy-rsa -y
```

### **configuramos la infraestructura de claves pki**

```
make-cadir ~/openvpn-ca
```

```
cd ~/openvpn-ca
```

### **Se crea entidad certificadora y claves para servidor**

```
./easyrsa init-pki
```

```
./easyrsa build-ca nopass
```

```
./easyrsa gen-req server1 nopass
```

```
./easyrsa sign-req server server1
```

```
./easyrsa gen-dh
```

```
openvpn --genkey --secret ta.key
```

### **Se crean claves para clientes**

```
./easyrsa gen-req cliente1 nopass
```

```
./easyrsa sign-req client cliente1
```

### **Se crea un a carpeta para el servidor dentro de /etc/openvpn/**

```
mkdir servidor
```

### **se mueven los siguientes archivos a la carpeta creada anteriormente**

- ca.crt
- server1.crt
- server1.key
- dh.pem
- ta.key

### **Creamos el archivo /etc/openvpn/server/server.conf y agregamos la configuración para el servidor**

port 1194

proto udp

dev tun

ca ca.crt

cert server1.crt

key server1.key

dh dh.pem

tls-auth ta.key 0

server 10.8.0.0 255.255.255.0

ifconfig-pool-persist ipp.txt

keepalive 10 120

cipher AES-256-CBC

user nobody

group nogroup

persist-key

persist-tun

status openvpn-status.log

verb 3

**Se habilita el reenvío de ip y se aplica cambios**

net.ipv4.ip\_forward=1

sudo sysctl -p

**Creamos el archivo para el cliente**

client  
dev tun  
proto udp  
remote TU\_IP\_PUBLICA 1194  
resolv-retry infinite  
nobind  
persist-key  
persist-tun  
remote-cert-tls server  
tls-auth ta.key 1  
cipher AES-256-CBC  
verb 3

<ca>

-----BEGIN CERTIFICATE-----

(Contenido de ca.crt)

-----END CERTIFICATE-----

</ca>

<cert>

-----BEGIN CERTIFICATE-----

(Contenido de cliente1.crt)

-----END CERTIFICATE-----

</cert>

<key>

-----BEGIN PRIVATE KEY-----

(Contenido de cliente1.key)

-----END PRIVATE KEY-----

</key>