ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DISEÑO DE LA RED CONVERGENTE DE LA UNIDAD EDUCATIVA FERNÁNDEZ SALVADOR VILLAVICENCIO PONCE "FESVIP"

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE INFORMACIÓN

LUIS ANDRÉS PERUGACHI MORENO

DIRECTOR: MSc. PABLO WILIAN HIDALGO LASCANO

Quito, marzo 2022

AVAL

Certifico que el presente trabajo fue desarrollado por Luis Andrés Perugachi Moreno, bajo mi supervisión.

MSc. Pablo Wilian Hidalgo Lascano

DIRECTOR DEL TRABAJO DE TITULACIÓN

DECLARACIÓN DE AUTORÍA

Yo Luis Andrés Perugachi Moreno declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración dejo constancia de que la Escuela Politécnica Nacional podrá hacer uso del presente trabajo según los términos estipulados en la Ley, Reglamentos y Normas vigentes.

Luis Andrés Perugachi Moreno

DEDICATORIA

Dedicado a Gloria y Aníbal, Mis Padres, el mejor ejemplo de trabajo duro, perseverancia, dedicación y constancia que la vida me pudo dar.

AGRADECIMIENTO

En primer lugar, agradezco a Dios por todas las oportunidades que me ha brindado a lo largo de esta vida y por permitirme mantener la fe aún en los momentos más oscuros.

A mis padres, Gloria y Aníbal por ser el mejor ejemplo que he tenido, sin ellos nada de esto fuera posible.

A mis hermanos: Pauli, Paty, Caro, Dany y David por aguantarme y quererme en todo momento. A Chris apoyo siempre de la familia, A mis sobrinas Naara y Lucy la alegría de la casa. A Amel por la amistad generada en tan corto tiempo.

A Geovanna y Nico por permitirme formar una familia y ser siempre incondicionales, ante todo.

Al Ing. Pablo, por aceptar ser mi tutor y más que todo por estar siempre dispuesto a ayudar para concluir este trabajo.

A la Sub-30 (Renato, Christian y Mauro) los hermanos que la vida me dio y a todos los panas y amigos que fueron parte de ese largo camino en la EPN (a los panas de la vida).

A la empresa Akros Cía. Ltda., en especial a Marcos y Mauricio por el apoyo para poder desarrollar este trabajo de titulación.

A la Unidad Educativa Fernández Salvador Villavicencio Ponce “FESVIP” y en especial a sus principales autoridades por todo el apoyo para el desarrollo de este trabajo de titulación.

“Cuando estés a punto de renunciar, recuerda por qué empezaste. Nada, absolutamente nada que valga la pena resultará sencillo”

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

Este Trabajo de Titulación propone como objetivo el diseño de la red convergente para la UNIDAD EDUCATIVA FERNÁNDEZ SALVADOR VILLAVICENCIO PONCE “FESVIP”, Institución ubicada al sur de la ciudad de Quito, la cual desde hace algunos años tiene varias necesidades a nivel tecnológico que se han ido incrementado y han generado malestar en su personal. En el primer capítulo se presentan los fundamentos teóricos ajustables a las nuevas tecnologías de redes, así como toda la información necesaria para el desarrollo de este trabajo.

En el segundo capítulo se detalla el estado actual de la infraestructura tecnológica, recopilando información de los problemas que presenta la Institución y en base a reuniones mantenidas con las autoridades se determinan las necesidades y nuevos requerimientos, para luego presentar una propuesta de diseño con ingeniería de detalle, acorde a las nuevas tendencias a nivel de tecnología, inclusive a nivel de cableado estructurado considerándose para ello estándares internacionales; como parte del diseño se presentan costos referenciales del mercado actual para validar la mejor alternativa. Adicionalmente se realiza una simulación para presentar las funcionalidades principales de este diseño, se la realiza en el aplicativo EVE-NG y VMware.

En el capítulo tres se realizan las pruebas de funcionamiento, validando así los resultados del diseño y la simulación.

Finalmente, en el capítulo cuatro se presentan las conclusiones y recomendaciones obtenidas de este trabajo de titulación.

Tomar en cuenta que se adjuntan en la parte final de este documento, los anexos obtenidos en la realización de este trabajo de titulación.

PALABRAS CLAVE: Redes, Diseño, Convergente, FESVIP, Simulación, EVE-NG, VMware.

ABSTRACT

This Degree Project proposes as an objective the design of the convergent network for the FERNÁNDEZ SALVADOR VILLAVICENCIO PONCE "FESVIP" HIGH SCHOOL, an institution located at the south of the city of Quito, which for some years has various needs at the technological level that they have been increasing and have generated discomfort in its personnel. The first chapter presents the theoretical foundations adjustable to the new network technologies, as well as all the information necessary for the development of this work.

In the second chapter, the current state of the technological infrastructure is detailed, collecting information on the problems that the Institution presents and based on meetings held with the authorities, the needs and new requirements are determined, and then presenting a design proposal with engineering of detail, according to new trends at the level of technology, including at the level of structured cabling, considering international standards; reference costs of the current market are presented as part of the design to validate the best alternative. Additionally, a simulation is carried out to present the main functionalities of this design, it is carried out in the EVE-NG and VMware applications.

In chapter three makes functional tests, thus validating the design and simulation results.

Finally, in chapter four the conclusions and recommendations obtained from this degree work are presented.

Consider that the annexes obtained in the completion of this degree work are attached at the end of this document.

KEY WORDS: Networks, Design, Converged, FESVIP, Simulation, EVE-NG, VMware.

1. INTRODUCCIÓN

Desde la aparición de las redes de datos, las comunicaciones se han extendido a nivel mundial, facilitando la interacción humana. El avance tecnológico en este campo ha permitido seguir desarrollando estas redes; incluso en esta época tan difícil de pandemia por el COVID-19, ha dejado continuar con la enseñanza en las instituciones educativas. Por esta razón es de vital importancia fortalecer las redes de datos institucionales y educativas, ya que con esto se garantizará una educación adecuada para los estudiantes.

La Unidad Educativa Fernández Salvador Villavicencio Ponce "FESVIP", situada en el sector de la Villaflora, sur de Quito, consta de una amplia infraestructura física utilizada por el personal administrativo, docente, de apoyo y estudiantes.

En los últimos años esta Unidad Educativa ha tenido varios problemas a nivel tecnológico, siendo uno de los principales, el no contar con la infraestructura necesaria; el cableado estructurado para datos en varias áreas se ha realizado sin cumplir con normas y estándares por lo que es deficiente, no posee un diseño de su red (lógico-físico), cuenta con equipos de comunicaciones en mal estado, la red inalámbrica no tiene cobertura en todas las áreas, el acceso a Internet es limitado, no dispone de un repositorio compartido donde el personal pueda manejar la información de gestión docente, administrativa y de apoyo, no existe correo institucional, la telefonía y servicios de comunicación son analógicos y antiguos, no cuenta con un sistema de administración de usuarios y equipos, no dispone de personal técnico capacitado para el soporte y administración tecnológica, entre otros. Estos problemas han generado malestar a la comunidad educativa, ya que no ha permitido desarrollar adecuadamente sus actividades académicas.

Este trabajo se presenta como una solución que permita solventar las necesidades tecnológicas de la institución, a través del diseño de una red convergente, el diseño del cableado estructurado acorde a estándares internacionales y el diseño de los principales servicios que la unidad educativa necesita.

La idea es mejorar la eficiencia de sus usuarios, la facilidad para comunicarse, mejorar los procesos de enseñanza aprendizaje y los servicios educativos. Dentro del diseño se genera un presupuesto referencial en base a las diferentes opciones del mercado actual y para concluir se realiza una simulación, donde se muestran algunas de las principales funcionalidades del diseño.

Este diseño cuenta con el aval de las autoridades de la Unidad Educativa, las cuales han brindado todas las facilidades del caso para que este proyecto culmine de la mejor manera y sea beneficioso para todos.

1.1 OBJETIVOS

1.1.1 OBJETIVO GENERAL

Diseñar la red convergente de la Unidad Educativa Fernández Salvador Villavicencio Ponce “FESVIP”.

1.1.2 OBJETIVOS ESPECÍFICOS

- Analizar la información técnica/teórica asociada al diseño de redes.
- Diseñar la red con ingeniería de detalle en base a los requerimientos de la Unidad Educativa “FESVIP”
- Simular la red diseñada para mostrar las principales funcionalidades y características.
- Analizar los resultados obtenidos de la simulación de red.

1.2 ALCANCE

En este trabajo de titulación inicialmente se hace una revisión de todos los fundamentos teóricos relacionados con el diseño de redes, cableado estructurado, arquitecturas de red, así como de los conceptos relacionados a redes convergentes, los cuales permiten tener el conocimiento teórico para realizar el presente diseño.

Como parte del levantamiento de información, se realiza un análisis detallado de la situación actual, para tomarlo como punto de partida en el diseño. Para la toma de requerimientos se coordinan visitas técnicas y reuniones las cuales se efectúan con las principales autoridades de la Unidad Educativa. Con el levantamiento de información y los requerimientos se obtiene la información necesaria para realizar el diseño con ingeniería de detalle.

El diseño del cableado estructurado está basado en normas y estándares ANSI/TIA (*American National Standard Institute/Telecommunications Industry Association*) y considera los diferentes subsistemas que lo conforman, siendo capaz de soportar todo el tráfico generado por el personal de “FESVIP”. Se establece el número de puntos de

red necesario en la Institución para el cableado horizontal, espacio en *rack*, número de puertos y reflejos; se incluye el diseño del equipamiento del cuarto de equipos.

Dentro del diseño de cableado se toma en cuenta el sistema de video vigilancia con el cual actualmente cuenta la Institución, se proponen puntos específicos para el uso de las cámaras.

Las comunicaciones a nivel de red que incluyen datos, voz y video son vitales para la Unidad Educativa entre sus diferentes edificaciones, por lo que se realiza un diseño adecuado de la red activa donde se toma en cuenta la creación de VLAN (*Virtual Local Area Network*) para el acceso a los servicios de red y aplicaciones, segmentando el tráfico que se genera por parte de cada una de las unidades.

Cada departamento de "FESVIP" cumple un rol específico, por esta razón se analizan sus necesidades de conexión y comunicaciones, de tal manera que se puedan determinar los servicios a ser ofrecidos y calcular el tráfico de red por departamento y a nivel institucional.

Se dimensionan y determinan los componentes necesarios a nivel de *hardware* y *software* para el uso de la red diseñada, como por ejemplo *switches* y puntos de acceso inalámbricos en cada piso para garantizar el servicio; adicionalmente se realiza un *site survey* predictivo para validar conectividad a todos los usuarios.

A nivel de servicios se diseña el servidor de Directorio Activo (AD), para centralizar la administración de usuarios y equipos dentro de un dominio, se incluyen los servicios de DHCP (*Dynamic Host Configuration Protocol*) por cada subred creada, DNS (*Domain Name System*), FTP (*File Transfer Protocol*). Se considera un servidor de correo electrónico, ya que actualmente la Unidad Educativa no cuenta con este servicio [10], [11].

Se diseñan los servicios de telefonía IP e integración con la PSTN (*Public Switched Telephone Network*) [12]; este incluye el directorio telefónico para cada área y la utilización de *softphones* de ser necesario. Como un *plus* adicional se propone el uso de salas de colaboración web que permiten generar videoconferencias e incluso servir como solución para clases virtuales en situaciones extremas como el caso de la pandemia COVID 19.

Para la seguridad en la red y permisos de navegación, se incluye dentro del diseño un *firewall*, el cual actúa como dispositivo intermedio entre la red interna y la Internet, para permitir o denegar el tráfico de entrada y salida.

Dentro del diseño se presenta un presupuesto referencial, en base a las proformas obtenidas de diferentes propuestas en el mercado actual; se escoge y recomienda la mejor alternativa para dar solución a la problemática de la Institución.

Para finalizar, se realiza una simulación que se presenta con el programa EVE-NG (*Emulated Virtual Environment - Next Generation*) y VMware, donde se puede observar cómo funciona la red activa, se valida conectividad entre todos sus elementos de red. Adicionalmente se simula un servidor que actúa como AD, DHCP, DNS, otro servidor de correo electrónico y una central telefónica para mostrar las funcionalidades principales de esta; la simulación es creada y configurada con licencias demo que se pueden obtener de los diferentes fabricantes. No se realiza la simulación del cableado estructurado.

En la Figura 1.1, se presenta el diagrama a nivel lógico.

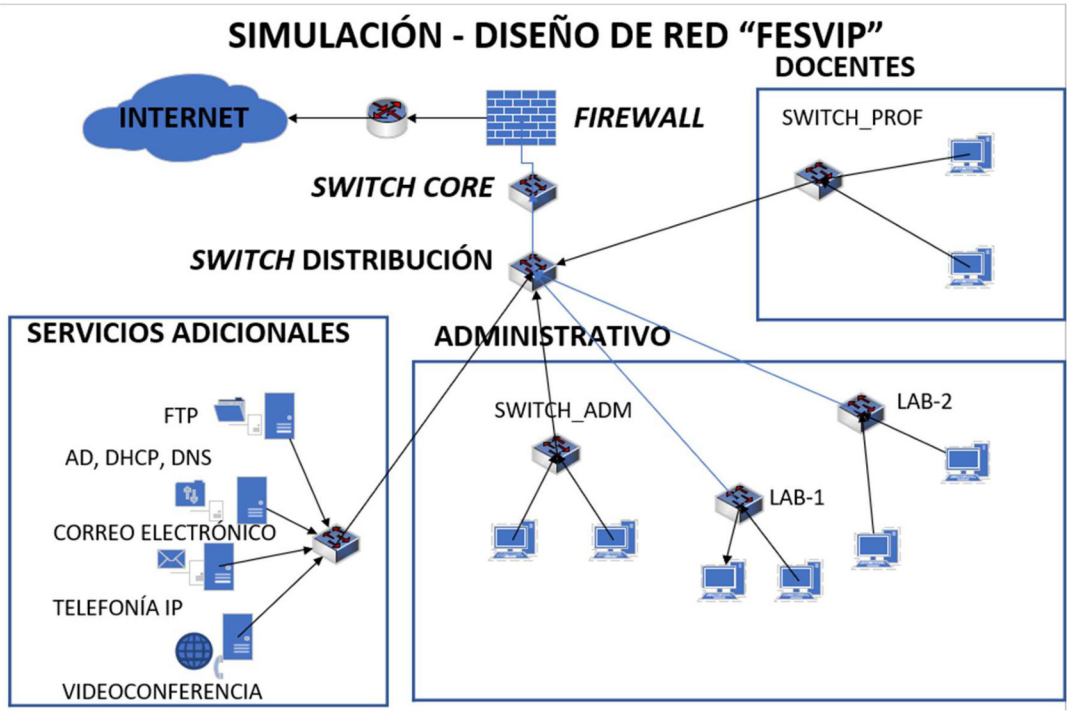


Figura 1.1 Diagrama de la red por diseñar y simular en la UE-FESVIP

Una vez generada la simulación se muestra el análisis de resultados y las funcionalidades descritas anteriormente; se realiza una retroalimentación para de ser necesario mejorar características en el diseño. Finalmente se presentan las respectivas conclusiones y recomendaciones generadas en la realización del proyecto.

Este Trabajo de Titulación tiene un producto final demostrable.

1.3 MARCO TEÓRICO

1.3.1 REDES DE DATOS

Las redes de datos son infraestructuras conformadas de equipos, medios físicos y lógicos que permiten transmitir información a través del intercambio de datos entre diferentes usuarios a cualquier distancia. [2]

En 1977 la Organización Internacional de Normalización (ISO, por sus siglas en inglés) desarrolló una estructura a base de normas comunes, como un marco de referencia para la definición de arquitecturas aplicable a todo tipo de sistemas de red, conocida como el modelo de referencia OSI *(Open System Interconnection)* [15]; así mismo se definió la arquitectura TCP/IP (*Transmission Control Protocol/Internet Protocol*) basada en un modelo conceptual con menos capas que OSI, que permite la configuración de redes básicas.[12]

Existen varios tipos de redes definidas por características únicas.

1.3.1.1 Redes de área local

Las LAN (por sus siglas en inglés) permiten conectar varios dispositivos de red tales como computadoras e impresoras dentro de un mismo entorno. La importancia de esta red es la interconectividad y el poder compartir recursos e información de forma eficiente en un entorno pequeño de red [3], (ver Figura 1.2).

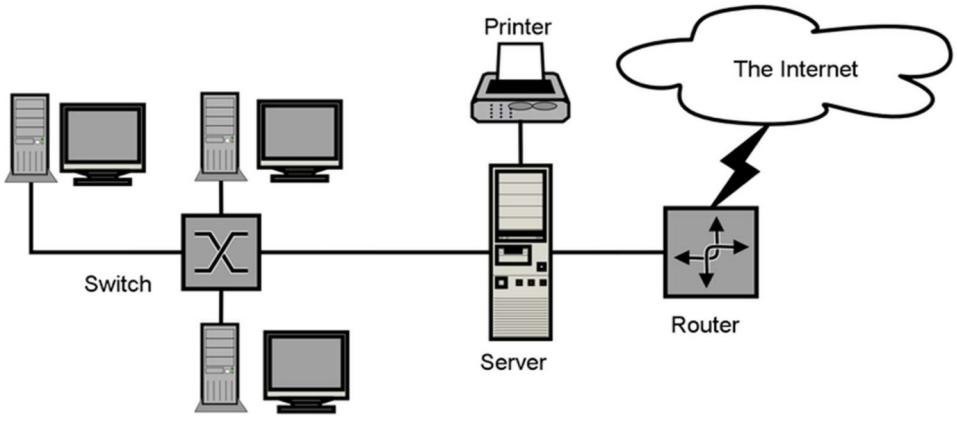


Figura 1.2 Red de área local [5]

Las LAN se encuentran definidas de acuerdo con varios parámetros entre los cuales se pueden mencionar, la velocidad de transmisión, el medio de transmisión, la topología de red, entre otros; la topología más utilizada es la jerárquica o en árbol (ver Figura 1.3) que tiene similitud con la topología en estrella extendida, debido a que a más de conectar

hosts, suele emplearse para conectar los concentradores o distribuidores entre sí; partiendo de un punto raíz, se va ramificando para llegar finalmente a los equipos de la red. Se encuentra más orientada a grandes entornos [11].

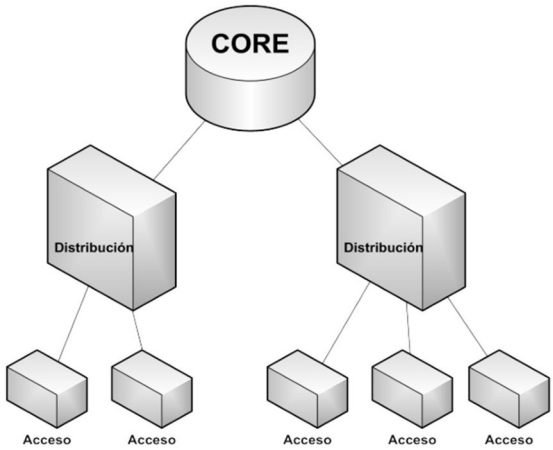


Figura 1.3 Topología jerárquica [11]

Las LAN basan su tecnología en el standard 802.3 de IEEE (*Institute of Electrical and Electronics Engineers*) conocido como *Ethernet,* el cual ha ido evolucionando a lo largo de los años, como se puede observar en la Figura 1.4.

The Evolution of Ethernet Standards to Meet Higher Speeds

Date	IEEE Std.	Name	Data Rate	Type of Cabling
1990	802.3i	10BASE-T	10 Mb/s	Category 3 cabling
1995	802.3u	100BASE-TX	100 Mb/s*	Category 5 cabling
1998	802.3z	1000BASE-SX	1 Gb/s	Multimode fiber
	802.3z	1000BASE-LX/EX		Single mode fiber
1999	802.3ab	1000BASE-T	1 Gb/s*	Category 5e or higher Category
2003	802.3ae	10GBASE-SR	10 Gb/s	Laser-Optimized MMF
	802.3ae	10GBASE-LR/ER		Single mode fiber
2006	802.3an	10GBASE-T	10 Gb/s*	Category 6A cabling
2015	802.3bq	40GBASE-T	40 Gb/s*	Category 8 (Class I & II) Cabling
2010	802.3ba	40GBASE-SR4/LR4	40 Gb/s	Laser-Optimized MMF or SMF
	802.3ba	100GBASE-SR10/LR4/ER4	100 Gb/s	Laser-Optimized MMF or SMF

Figura 1.4 Evolución de las tecnologías ethernet [71]

1.3.1.2 Redes de área local inalámbrica

Los estándares de la WLAN (por sus siglas en inglés) se encuentran determinados por la familia de normas IEEE 802.11. Las redes locales inalámbricas (ver Figura 1.5) brindan la posibilidad de integrar terminales cómodamente en una red doméstica o empresarial y son compatibles con las LAN ethernet, aunque el rendimiento es, en este caso, algo menor que el de una conexión ethernet. [5]

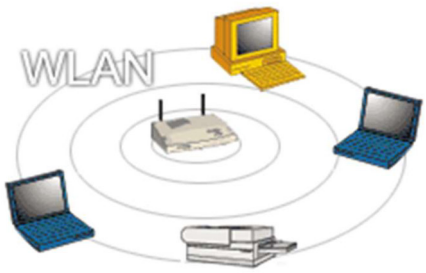


Figura 1.5 Red WLAN [10]

1.3.2 REDES CONVERGENTES

La evolución de las redes en los últimos años ha generado nuevos conceptos, entre ellos las llamadas redes convergentes o multiservicio. Como su nombre lo indica, en este tipo de redes se hace referencia a la integración de varios servicios como, por ejemplo: datos, voz y video, todos basados en IP (*Internet Protocol*) como protocolo de red, es decir, se transportan varios servicios por una misma red y se evita el esquema tradicional en el que anteriormente se ejecutaban los servicios por separado, por lo que se tenían varias redes, tal como se observa en la Figura 1.6.

La integración de servicios beneficia en gran medida a la administración de estos, tomando en consideración el aumento de la productividad, ahorros a nivel de costos y de tiempo a quienes decidan optar por este nuevo concepto. Al ofrecer estos servicios las redes convergentes utilizan tecnología LAN de alta velocidad para de esta manera lograr una transmisión adecuada [9].

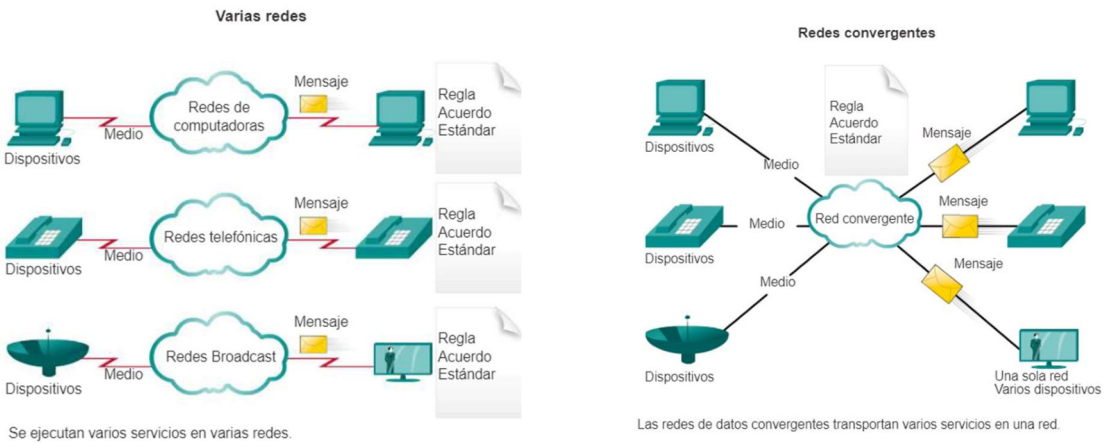


Figura 1.6 Redes independientes vs. Redes Convergentes [13]

1.3.3 CABLEADO ESTRUCTURADO

Cuando se habla de cableado estructurado es necesario mencionar que es un sistema que consta de varios elementos, entre ellos: conectores, cables, canalizaciones, dispositivos, que forman parte de una infraestructura de red dentro de una edificación y que en conjunto permiten transportar las señales (datos) desde uno o varios emisores hasta uno o varios puntos receptores [17].

Sus subsistemas están basados en normas y estándares internacionales que fueron desarrollados en conjunto con varias organizaciones donde se incluyeron usuarios finales, fabricantes, consultores, expertos entre otros [12]. En la Figura 1.7 se muestran los principales sistemas y subsistemas.

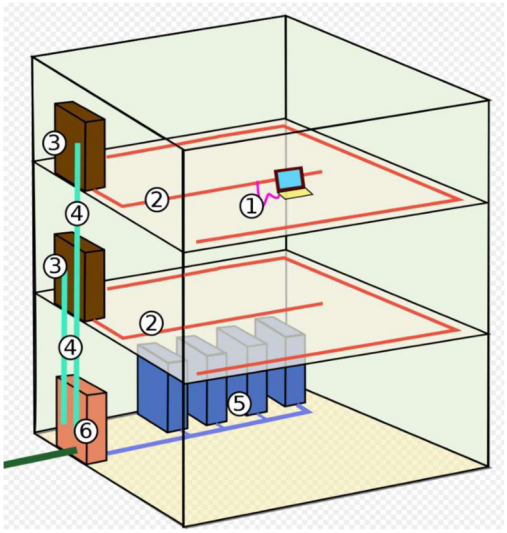


Figura 1.7 Elementos o subsistemas de cableado estructurado [12]

1. **Área de trabajo:** consta de conectores de telecomunicaciones y cables de conexión (“*patch-cords”),* que permiten el acceso a la red de equipos tales como: computadores, teléfonos, impresoras, entre otros. Se debe tomar en cuenta que los equipos activos que se instalen no forman parte del sistema de cableado estructurado [18].

2. **Cableado horizontal:** es la porción del sistema de cableado de telecomunicaciones que específicamente va del conector/salida de telecomunicaciones del área de trabajo a la conexión cruzada horizontal en el armario de telecomunicaciones [19].

3. **Armario de cableado:** conocido también como *rack* de telecomunicaciones de piso, es un estante de metal que sirve como lugar de almacenamiento de los equipos informáticos, el equipamiento electrónico y el de comunicaciones. Es donde se ubican todos los elementos de centralización del sistema de cableado y donde están ubicados los equipos activos de red y otros elementos como el soporte eléctrico, guía y latiguillos [20].

4. **Cableado vertical:** conocido también como *backbone***,** es el que proporciona interconexiones entre cuartos de entrada de servicios de edificio, cuartos de equipo y cuartos de telecomunicaciones [22]. Cubre la comunicación vertical entre pisos en edificios e incluye medios de transmisión (cables), puntos principales e intermedios de conexión cruzada y terminaciones mecánicas. Este sistema realiza la interconexión entre los diferentes gabinetes de telecomunicaciones y entre estos y el cuarto de equipos [21].

5. **Centro de cómputo (centro de datos, cuarto de equipos):** es el cuarto de equipos principal donde se alojan todos los *racks* necesarios y el punto de partida para la distribución de la red activa.

6. **Infraestructura de entrada (acometida):** es el lugar en el que ingresan los servicios de telecomunicaciones, la ubicación donde llega la empresa suministradora/proveedora de un servicio o donde llegan las canalizaciones de interconexión entre edificios. La infraestructura de entrada puede contener dispositivos de interfaz con redes públicas prestadoras de servicios y equipos de telecomunicaciones. Las interfaces pueden incluir borneras (telefónicas) y equipos activos [23].

1.3.3.1 Estándares de cableado estructurado

Los estándares de cableado estructurado definen varios tipos de conexiones y configuraciones que se pueden utilizar a la hora de realizar una implementación de un sistema; esto incluye por ejemplo cómo instalar el cableado, los componentes que deben ser utilizados, normas de recorridos y espacios de telecomunicaciones, en fin, son los requisitos básicos que se deben cumplir para que una implementación esté garantizada [25].

Los principales organismos implicados en la elaboración de estas normas, mayoritariamente utilizadas en el país, actualmente son: [29]

ANSI: *American National Standards Institute*, es una organización creada en el año de 1918, sin fines de lucro que se encarga de supervisar el desarrollo de estándares entre ellos para productos y servicios de telecomunicaciones.

TIA: *Telecommunications Industry Association*, es una asociación de EE. UU. que se encarga de generar estándares y documentos técnicos, basados en las guías establecidas por ANSI, ya que forma parte de esta.

Existen varias normas y estándares, pero de ellas las más utilizadas en el ámbito del cableado estructurado son las que se describen a continuación.

1.3.3.1.1 Estándares ANSI/TIA generales

- ANSI/TIA-568.0-D en general
- ANSI/TIA-569-D caminos, rutas y espacios
- ANSI/TIA-606-B administración
- ANSI/TIA-862-B estándar de infraestructura de cableado estructurado para edificios inteligentes [29].

1.3.3.1.2 Estándares ANSI/TIA locales

- ANSI/TIA-568.1-D cableado para edificios comerciales.
- ANSI/TIA-570-C estándar de infraestructura de telecomunicaciones residencial.
- ANSI/TIA-942-A estándar de infraestructura de telecomunicaciones para *data center*.
- ANSI/TIA-1005-A estándar de infraestructura de telecomunicaciones industrial.
- ANSI/TIA-4966 infraestructura de telecomunicaciones para instalaciones educativas [29].

1.3.3.1.3 Estándares ANSI/TIA de componentes

- ANSI/TIA-568.2-D componentes y cableado de telecomunicaciones de par trenzado.
- ANSI/TIA-568.3-D componentes de cableado de fibra óptica.

1.3.4 COMUNICACIONES UNIFICADAS (UC)

Las comunicaciones unificadas se refieren a diferentes formas de herramientas de comunicación que permiten la interacción y colaboración digital en las empresas, que,

al permitir unificar las llamadas telefónicas, conferencias web, SMS (*Short Message Service*) y correo electrónico (ver Figura 1.8), posibilita que los usuarios sean capaces de compartir y acceder a la información en tiempo real. La solución de comunicaciones unificadas correcta puede llevar a mejorar los procesos empresariales y llevarlos al siguiente nivel, aumentando la productividad, mejorando la colaboración y la movilidad [30].

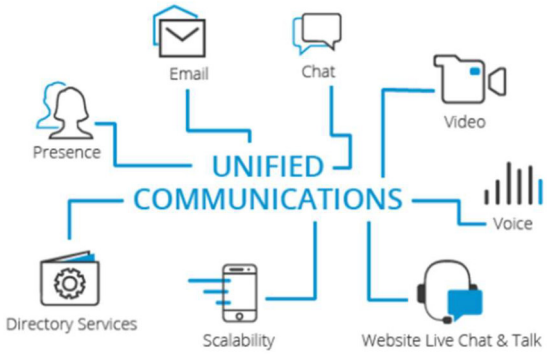


Figura 1.8 Canales de comunicación para usuarios en tecnología [30].

1.3.4.1 Telefonía IP

Es una tecnología que permite la integración de comunicaciones de voz en una misma red de datos, basada en el protocolo IP (*Internet Protocol*). En muchos casos se utiliza el término red convergente o convergencia IP, que se refiere a un concepto un poco más amplio relacionado a la integración de voz, datos y video [31].

La transmisión del tráfico de voz (Voz sobre IP - VoIP) se basa en un conjunto de recursos que hacen posible que la señal de voz viaje a través de Internet utilizando el protocolo IP, esto es digitalizando la señal, en lugar de usar las redes telefónicas tradicionales PSTN (Red Telefónica Pública Conmutada) donde la voz se envía de forma analógica. La PSTN trabaja a través de líneas telefónicas físicas, sistemas de cableado y redes que permiten a los usuarios realizar llamadas de teléfono fijo. La Telefonía IP es mucho más versátil permitiendo la transmisión de voz, datos y video a una variedad de dispositivos como *smartphones*, computadoras personales, tabletas y teléfonos IP a un menor costo [31], (ver Figura 1.9).

1.3.4.1.1 Componentes y funcionamiento de VoIP

- **Decodificador:** reconvierte la voz en el destino. Se realiza la traducción de un mensaje para que el receptor pueda entender [32].

- **Gateway VoIP:** dispositivo que permite convertir el tráfico de telefonía tradicional a llamadas de VoIP [32].
- **Teléfonos IP:** elementos que permiten hacer llamadas de VoIP, está basado en software (*softphone*) o un teléfono de escritorio (hardware).
- **La red IP:** provee conectividad entre todos los terminales IP.
- **Servidor:** puede ser un servidor físico o en la nube, solo se necesitará una conexión a Internet. Efectúa operaciones de validación, recolección, distribución, enrutamiento, administración general del servicio [32].

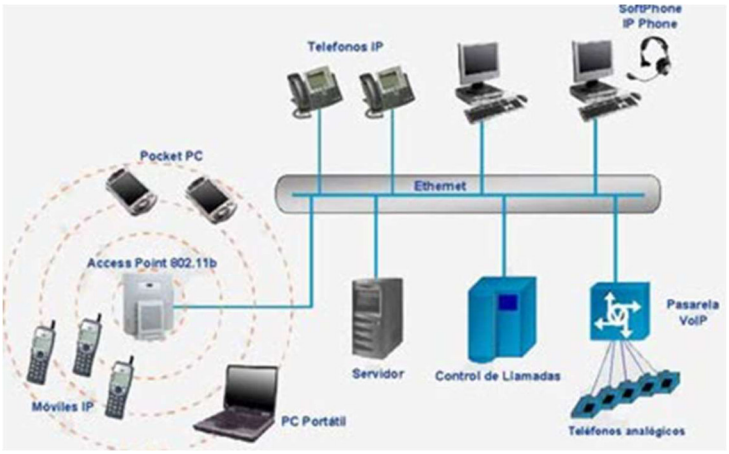


Figura 1.9 Componentes y funciones VoIP [32].

1.3.4.1.2 Protocolos de señalización

Estos son lenguajes utilizados en varios dispositivos de VoIP para establecer, controlar y finalizar llamadas, en teléfonos, servidores de gestión de llamadas, red telefónica pública conmutada, y los sistemas PBX (*Private Branch eXchange*). En el mercado se han encontrado varios protocolos de señalización para la VoIP [33].

- **H.323:** este protocolo suministra sesiones de comunicación sobre paquetes. (ver Figura 1.10) Se basa en estándares existentes como H.320, RTP (*Real Time Transport Protocol*) y Q.931, que son mecanismos para el transporte de aplicaciones multimedia en las redes de área local, las cuales han evolucionado rápidamente para cumplir con las necesidades de las redes de VoIP. [34]

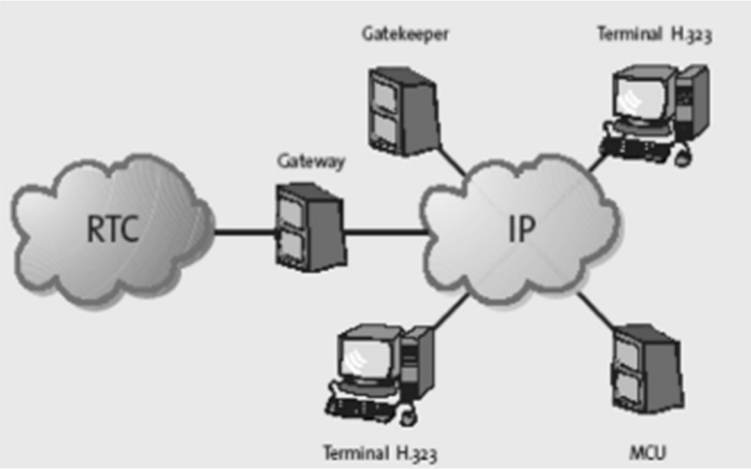


Figura 1.10 Protocolo de señalización H.323 [35]

- **SIP:** *Session Initiation Protocol*, protocolo de señalización que permite establecer, modificar y finalizar una sesión interactiva entre dos o más usuarios (ver Figura 1.11), en la que intervienen elementos como: voz, video, mensajería instantánea, entre otros.

  Está integrado con las aplicaciones y servicios de Internet, ya que posee mayor flexibilidad para incorporar nuevas funciones y su implementación es mucho más sencilla que H.323, incluso es parecido a los protocolos HTTP (*Hypertext Transfer Protocol*) y SMTP (*Simple Mail Transfer Protocol*) [36].

  El protocolo SIP se utiliza frecuentemente en telefonía IP y en los últimos años se ha consolidado como el protocolo preferido en las comunicaciones multimedia [36].

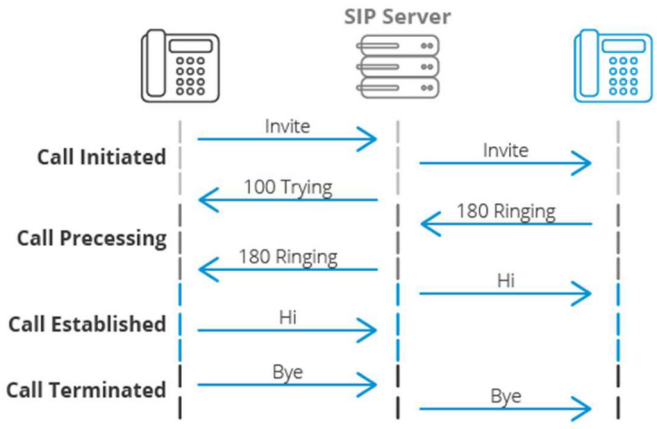


Figura 1.11 Protocolo de señalización SIP [36]

- **IAX:** *Inter-Asterisk eXchange Protocol*, es utilizado para manejar conexiones VoIP entre servidores asterisk y entre servidores y clientes que utilizan este protocolo (ver Figura 1.12). El protocolo original ha quedado obsoleto en favor de IAX2 que es la segunda versión, la cual permite manejar una gran cantidad de *códecs* y puede ser utilizado para transportar virtualmente cualquier tipo de dato. Esta capacidad lo hace muy útil para realizar videoconferencias o realizar presentaciones remotas [37].

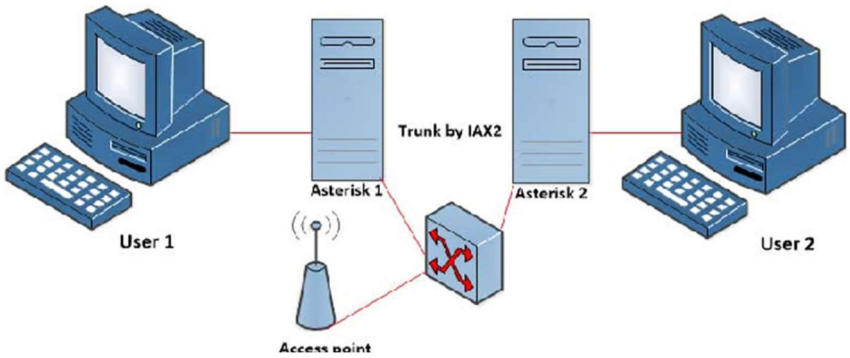


Figura 1.12 Protocolo de señalización IAX [37]

- **SCCP:** *Skinny Client Control Protocol,* es propiedad de Cisco y fue diseñado con el propósito de enviar mensajes entre un cliente ligero y el *Call Manager* de Cisco (ver Figura 1.13), y así facilitar el transporte de mensajes orientados a conexión [35].

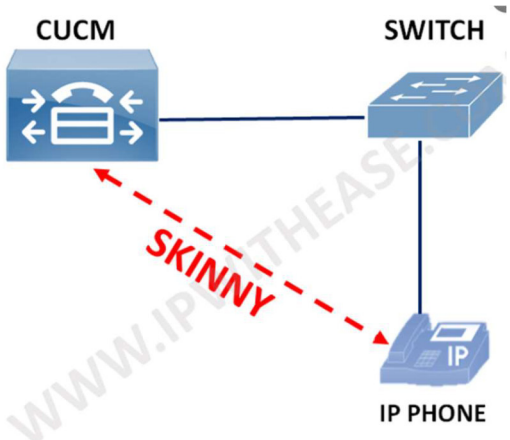


Figura 1.13 Protocolo de señalización SCCP [35]

1.3.4.1.3 Soluciones de telefonía IP

La telefonía IP se ha convertido en el sistema con mayor aceptación a nivel mundial, siendo una herramienta importante en el desarrollo de la sociedad. Las diferentes marcas que se encuentran en el mercado permiten establecer comunicación dentro de una empresa mostrando un servicio de voz y datos de calidad en una red controlada [48].

A continuación, se presentan algunas marcas que tienen soluciones de telefonía IP

- **Grandstream:** la marca Grandstream (ver Figura 1.14) ha sido utilizada desde el 2002 con soluciones SIP que permiten que las instituciones o empresas sean más productivas, ya que ofrece características de voz, video, datos y movilidad de vanguardia [49]. Entre las funciones más destacadas se tienen:
    - Pantalla gráfica
    - Cuenta SIP
    - Desde dos llamadas simultáneas
    - Agenda telefónica hasta 500 contactos e historial de llamadas
    - Puertos de red duales auto sensitivos de 10/100 Mbps, PoE integrado.

Figura 1.14 Productos Grandstream [49]

- **CISCO:** la telefonía IP Cisco (ver Figura 1.15) es muy importante en el mercado de las redes y tecnologías de la información; ofrece una central completa con todas sus funcionalidades como: llamadas, videollamadas integradas, conferencias, entre otras. Las funcionalidades antes mencionadas están preparadas para trabajar en remoto y usarlas a través de aplicaciones, siendo

compatibles con teléfonos IP populares y troncales SIP [50]. La principal ventaja de los sistemas de comunicaciones de Cisco es la unificación de servicios, ya que tienen equipos que integran medios de comunicación como texto, video y voz. Funciona en redes fijas o inalámbricas, permitiendo así, que no se requiera una gran infraestructura y sea accesible en el mercado.

Figura 1.15 Telefonía IP CISCO [50]

- **Asterisk:** es uno de los líderes mundiales en telefonía (ver Figura 1.16) de código abierto (bajo licencia GPL – *General Public License*). Puede convertir un ordenador en un servidor de comunicaciones VoIP; además es un sistema utilizado por empresas para mejorar su comunicación [51].

  La ventaja más destacada es su escalabilidad, debido a que responde a las necesidades de las empresas; permite también gestionar la centralita mediante una configuración web o interfaz gráfica [51].

  Se enlistan a continuación algunas ventajas de Asterisk VoIP:

  - Conferencia
  - Gestiona colas de llamadas
  - Contestador automático
  - Operadora automática, IVR (*Interactive Voice Response*)
  - Distribución de llamadas entrantes y salientes
  - Escalabilidad total de líneas y extensiones

Figura 1.16 Centralita telefónica Asterisk [51]

1.3.4.2 Videoconferencia

Es un sistema multimedia, que permite a múltiples usuarios mantener la interacción virtual a través de la transmisión en tiempo real de video, sonido y texto a través de una red de área local e inclusive desde Internet.

Estos sistemas están diseñados para llevar a cabo reuniones de trabajo, demostraciones de productos, entrenamiento, soporte, atención a clientes, *marketing* de productos. La videoconferencia interactiva permite la interacción permanente y no requiere conocimientos técnicos para su manipulación y su costo es asequible. [40]

Los sistemas de videoconferencia están compuestos por: monitores, cámaras, micrófonos, altavoces y el más importante que es el códec [40].

1.3.4.2.1 Modelos de entrega de videoconferencia

En la actualidad existen dos modelos de entrega de videoconferencia bien marcados en el mercado [59]:

- **Video local:** consta de uno o varios servidores locales y es un modelo muy popular en las empresas que empezaron implementando este tipo de soluciones que tienen el control y administración de este, bajo su equipo de TI (Tecnología de la Información) [59].

- **Videoconferencia como servicio en la nube:** en la actualidad varias marcas ofrecen los servicios de videoconferencia en la nube a través de redes IP e Internet, es una solución que no necesita recursos locales y el proveedor es responsable del mantenimiento y monitoreo del sistema; se tiene un ahorro en la implementación, pero al ser un servicio bajo suscripción los costos asociados podrían incrementar. La nube proporciona escalabilidad por lo que se ha convertido en una opción para las organizaciones que tienen sobretodo varias

sucursales en diferentes ubicaciones geográficas [59]. Como ejemplos de soluciones de videoconferencia en la nube se tienen: Cisco Webex, Avaya Spaces, Microsoft Teams.

1.3.4.2.2 Protocolos y códecs de videoconferencia

Existen protocolos estándar para la transferencia de datos en las videoconferencias entre sistemas de *software* y como puntos finales los *hardware* de los fabricantes; entre los mencionados a nivel de telefonía IP como son SIP y H.323, también se tienen a otros muy comunes:

- **H.320:** protocolo de redes de conmutación de circuitos el cual permite que los mecanismos de señalización y la forma de transmisión de la voz, video y cargas sean a través de la interfaz de la RDSI (Red Digital de Servicios Integrados) [47].
- **H.264:** estándar introducido en el 2004 para la codificación/decodificación de video, proporciona alto nivel de compresión al tiempo que conserva la calidad [47].
- **SVC:** codificación de video escalable, es una nueva forma de compresión, es un anexo al códec H.264; ajusta dinámicamente la frecuencia de fotogramas de la resolución en función de las condiciones de la red [47].
- **H.265:** estándar que presenta mejoras en los algoritmos de codificación, mayor resistencia a pérdida de paquetes durante la transferencia de datos y soporta los formatos ultra HD, 4K y 8K [47].
- **RTV:** *Real Time Video*, es un códec propiedad de Microsoft utilizado para todos los productos de Office como *Skype For Business* [47].

1.3.4.2.3 Códecs de audio para telefonía IP y videoconferencia

- **G.711**: estándar para la codificación de audio que ofrece un flujo de datos de 64 kbits/s; se utiliza generalmente para telefonía, tiene dos variantes geográficas: *u-law* utilizado en EE. UU. - Japón y *A-law* para Europa y resto del mundo [47].
- **G.729:** es un algoritmo de compresión de audio que se usa en gran medida en VoIP ya que requiere un mínimo de ancho de banda y opera a una tasa de 8 kbits/s, pero existen extensiones que trabajan a menores tasas.
- **G.722:** es un códec evolucionado de G.711 que funciona a 48, 56 y 64 Kbits/s, proporciona mejoras a nivel de transmisión de voz

1.3.5 SEGURIDAD EN LA RED

Es un campo específico dentro de las redes de datos, que permite proteger los recursos informáticos de fallos y ataques a la integridad, confidencialidad y disponibilidad de esta; además, es uno de los puntos más importantes que se debe considerar en una red. [41].

1.3.5.1 Seguridad perimetral

Mecanismo de control de acceso, prevención, detección, autorización y denegación de acceso. La seguridad perimetral de red es donde se protegen las redes privadas de una entidad con el mundo exterior [52]. Actualmente, los perímetros de una red son más difíciles de especificar, pero se siguen utilizando las mismas tecnologías con nuevas funcionalidades que abarcan más controles a nivel de seguridad.

Las funciones principales se basan en filtrar y bloquear, permitiendo solo a quien sea necesario aislar y segmentar los servicios en función de su exposición a ataques, resistir a ataques externos, e identificar los ataques sufridos y alertar.

1.3.5.1.1 Firewall de red

Conocido comúnmente como cortafuegos, es un elemento informático que bloquea a usuarios no autorizados el acceso a una red privada conectada a Internet. Por tanto, se centra en examinar cada uno de los mensajes que entran y salen de la red para obstaculizar los que no cumplen con ciertos criterios de seguridad; así mismo da vía libre a las comunicaciones que sí están reglamentadas en la política de seguridad [41].

Las nuevas generaciones de *firewall* en el mercado presentan funcionalidades adicionales a las de un *firewall* tradicional, como: filtrado web, control de aplicaciones, detección de intrusos, *antivirus, antibotnets, antispam*, entre otras.

Se detallan a continuación las marcas en el mercado que ofrecen soluciones de *firewall* de nueva generación.

- **Checkpoint Software: Next Generation *Firewall***

Checkpoint es uno de los pioneros en seguridad con *firewall* brindando protección superior contra todo tipo de amenazas, reduciendo así la complejidad de seguridad y costo. Son líderes en la prevención de amenazas, protegiendo de ataques cibernéticos como *malware*, *spam*, entre otros. Tiene un panel centralizado para la administración de toda la seguridad y puede ser instalado en un servidor físico o en la nube; sus principales módulos de seguridad son: VPN (*Virtual Private Network*), IPS (*Intrusion Prevention Service*), *Application Control* y Web *Filtering* [53].

- **Fortinet: Fortigate Next Generation *Firewall* (NGFW)**

Dispositivo de seguridad de nueva generación, en la solución *on premise* se puede tener una consola de administración simple y centralizada, en donde se puede crear redes seguras y protección automatizada contra amenazas emergentes. Cuenta con características como: control de aplicaciones, prevención de intrusos, inspección SSL *(Secure Sockets Layer), Sandboxing*, filtrado de URL (*Uniform Resource Locator*). También cuenta con soluciones, con las mismas características, virtualizadas y en la nube [54].

- **Sophos: XG *Firewall***

Sophos XG f*irewall* es un dispositivo de seguridad de red el cual provee no solo seguridad a nivel LAN, sino que incluso a WLAN; es fácil de implementar y escalable. Trabaja de la mano con Sophos *central* e *Intercept X* en tiempo real para mantener la seguridad dentro de la red. Tiene funcionalidades adicionales y también puede proteger redes híbridas o públicas.

Puede ser desplegado de cuatro formas: dispositivo *hardware (XG devic*e), *software* compatible con diferente *hardware*, dispositivo virtual en los hipervisores más comunes (VMware, Citrix, Hyper-V, KVM) y XG *firewall* desplegado en la nube de Azure y AWS (*Amazon* Web *Services*) [55].

1.3.6 SERVICIOS ADICIONALES

En la actualidad toda institución como mínimo debe contar con servicios que le permitan gestionar de mejor manera toda su infraestructura tecnológica, a continuación, se detallan los principales.

Active Directory, también llamado AD, es una herramienta que pertenece a la empresa Microsoft la cual proporciona servicios de directorio normalmente en una LAN; es decir, permite administrar los componentes internos de una red tales como usuarios, equipos, gestionar políticas, entre otros [42].

Dynamic Host Configuration Protocol (DHCP), fue desarrollado como solución para redes de gran extensión, computadores portátiles y por ello complementa a BOOTP. Asigna automáticamente direcciones de red que son reutilizables. En un servidor Windows se puede activar la funcionalidad de DHCP y generar varios *pools* de direcciones que van a ser utilizadas dentro de una red privada [42].

Domain Name System (DNS), es un sistema de dominio de nombres que permite comunicarse más fácilmente, siendo este un sistema de bases de datos que se encuentra distribuido en la red y su función principal es traducir la solicitud de ciertos nombres de *host* a direcciones IP que las computadoras entiendan, esto en una red local o en una WAN, inclusive en Internet [43].

File Transfer Protocol (FTP), protocolo de transferencia de archivos, es aquel que permite la transferencia de archivos entre sistemas interconectados o enlazados y se encuentra basado en la arquitectura cliente-servidor. Por tal motivo, su función es permitir el intercambio de datos entre diferentes servidores/computadores, facilitando el acceso a información en una organización [43].

1.3.7 CORREO ELECTRÓNICO

Llamado también *e-mail*, es un servicio de red que permite enviar y recibir mensajes a múltiples destinatarios o receptores que se encuentren en cualquier parte del mundo. Para utilizar este servicio es necesario cualquiera de los programas de correo electrónico que ofrece la red Internet mediante sus *hostings* públicos e incluso configurar un servidor *on premise* que cumpla esta funcionalidad. En un correo electrónico se puede adjuntar archivos como documentos, imágenes, música, archivos de video [44].

Todos los sistemas que gestionan correo electrónico utilizan tres protocolos:

- **SMTP:** *Simple Mail Transfer Protocol*, utilizado para la tarea de entrega de correo electrónico, es decir, gestionar el correo saliente de una cuenta. Generalmente trabaja por el puerto 25.
- **IMAP:** *Internet Message Access Protocol*, utilizado para la recepción de correo electrónico; su característica principal es que no descarga el correo en el computador, sin cifrado utiliza por defecto el puerto 143.
- **POP3:** *Postal Office Protocol* versión 3, al igual que IMAP es utilizado para la recepción de mensajes, con la diferencia que POP3 descarga los mensajes en el computador, donde se almacenará; su puerto por defecto es el 110 para conexiones sin cifrar.

Actualmente los servicios en la nube ofrecen paquetes bajo suscripción para el uso de este servicio y tal ha sido su acogida que la gran mayoría de empresas está pasando a utilizar este servicio, el ejemplo más poderoso es Office365.

1.3.8 SERVICIOS EN LA NUBE

Son aquellos servicios que se utilizan a través de Internet y no están físicamente instalados en el computador, debido a que son programas que se alojan en un servidor accesible desde cualquier dispositivo conectado y que se encuentra en cualquier parte del mundo. Existen varios tipos de nubes: [45].

Nubes privadas. - entorno diseñado dentro de una infraestructura organizacional interna, a la cual tienen acceso los usuarios y se encuentra alojado localmente.

Nubes públicas. - entornos creados a partir de recursos ajenos del usuario y se redistribuyen a otros usuarios. Está diseñado dentro de una infraestructura externa.

Nubes híbridas. – Conjunto de nubes públicas y privadas que interactúan entre sí [56].

1.3.8.1 Proveedores y Tipos de servicios en la nube

En la actualidad existen varios servicios que se ofrecen en la nube; algunas de las empresas posicionadas en el mercado que ofrecen este tipo de servicio son:

- Microsoft Azure
- Alibaba Cloud
- Amazon Web Services (AWS)
- Google Cloud

Considerando la tendencia de crecimiento en este campo, a continuación, se detallan tres grandes bloques de servicios en la nube:

- ***Infraestructure as a Service (IaaS)***

Es aquel que ofrece todos los recursos informáticos (almacenamiento, memoria, procesador, red, entre otros). Este servicio es el que le da mayor control al cliente por lo que genera mayor complejidad de uso [45].

- ***Plataform as a Service (PaaS)***

En este servicio los usuarios tienen una plataforma en la cual ejecutan sus aplicaciones, el proveedor se encarga del mantenimiento y gestión, es decir, ofrece todo lo necesario al cliente. El cliente no tiene control sobre los recursos informáticos [45].

- ***Software as a Service (SaaS)***

En este servicio el cliente solamente puede acceder al *software* alojado en servidores del proveedor. Es el más usado; el soporte y disponibilidad están a cargo del proveedor [56].

1.3.9 SOFTWARE DE SIMULACIÓN

Tiene como objetivo fundamental automatizar el proceso de modelar un fenómeno del mundo real mediante el uso de fórmulas matemáticas a través de la programación. Por esta razón, se trata de un programa que permite al usuario ver que pasará al realizar varias operaciones sin la necesidad de tener que hacerla en el mundo real [46].

Existen varios *softwares* que permiten simular diferentes ambientes, a nivel de red uno de los más utilizados es EVE-NG, el cual se detalla a continuación.

1.3.9.1 Emulated Virtual Environment Next Generation (EVE-NG)

Es un *software* de simulación y emulación de redes, que trabaja con imágenes de sistemas operativos reales de equipos. Es rápido, fácil de implementar, permite simular y emular ambientes reales o arquitecturas que en un futuro se vayan a implementar.

EVE NG se implementa en el sistema Ubuntu basado en Linux, por lo que es importante tener conocimientos básicos de comandos y uso de librerías. Una vez instalado trabaja mediante acceso Web a la interfaz de administración y creación de laboratorios; es compatible con imágenes de varias marcas de dispositivos como Cisco, Aruba, Juniper, entre otros.

La particularidad de EVE NG es el uso de HTML5 (*Hyper Text Markup Language 5*) con lo que se elimina el cliente de conexión, aun así, se puede administrar y configurar los dispositivos de *software* de terminales como: PuTTY y Wireshark.

Existen distintas versiones entre ellas se tienen la PRO y *Community* la cual trabaja con diferentes características de equipamiento. [46]

Al utilizar la versión *Community* de EVE NG se tienen las siguientes ventajas:

- No tiene costo y es más que suficiente para realizar las simulaciones que se desee.
- Se tiene múltiples tipos de conexión.
- No hay sobrecarga de recursos de sistema.
- No usa clientes, lo que facilita su uso y administración.

1.3.10 SOFTWARE DE VIRTUALIZACIÓN

La virtualización en términos simples es crear un ambiente simulado dentro de un *hardware* con las condiciones necesarias. Mediante este proceso se crean diversas instancias comúnmente conocidas como máquinas virtuales que poseen sus propias características como: recursos informáticos, sistemas operativos, repositorios de almacenamiento, entre otros.

Una de las principales características de la virtualización es la optimización de los recursos, reducir el consumo de energía y a mediano plazo generar un ahorro económico donde sea esta aplicable [60] [61].

En el mercado existen varios *softwares* que permiten la virtualización y cada vez es más común que las entidades las ejecuten. Una de las principales empresas que proporciona virtualización es VMware, su *software* permite virtualizar tanto equipos de escritorio como servidores.

1.3.10.1 Software de Virtualización VMWARE - VSPHERE

VMware Vsphere es una línea de productos que permite a los usuarios ejecutar máquinas virtuales, proporcionando un ambiente de ejecución similar a un computador físico. Este sistema permite simular varios computadores y/o servidores de manera simultánea dentro de un mismo *hardware*. Dichos productos utilizan funciones especiales y la capa de visualización asigna recursos de *hardware* físicos a los recursos de la máquina virtual [57].

Las principales ventajas de utilizar VMware para virtualizar servidores son:

- Reducción de la inversión y gastos operativos a mediano plazo.
- Optimizar el uso de recursos de hardware.
- Aumentar la productividad y la capacidad de respuesta del área de TI.
- Hacer una distribución equitativa y rápida de recursos y aplicaciones.
- Mejorar la continuidad del negocio y tener la capacidad de recuperación ante desastres.
- Tener una administración, gestión simplificada y fácil manejo del Centro de Datos.

2 METODOLOGÍA

2.1 ANÁLISIS DE LA SITUACIÓN ACTUAL

En el presente capítulo se detalla brevemente la situación actual de la Unidad Educativa "FESVIP"; se describe la infraestructura física, el estado de todos los elementos o subsistemas de cableado, la cantidad de usuarios, el estado actual de su red activa, los servicios con los que actualmente cuenta la institución. Se hace un resumen de las falencias encontradas y se complementa con el levantamiento de requerimientos institucionales para lograr el diseño de red propuesto.

2.1.1 DESCRIPCIÓN DEL CONTEXTO DE LA UNIDAD EDUCATIVA "FESVIP"

La Unidad Educativa Particular Fernández Salvador Villavicencio Ponce "FESVIP", según reuniones mantenidas con las autoridades, acoge alrededor de 936 estudiantes y en relación con el personal que labora en la institución, este se encuentra conformado por 42 docentes, 14 personas como administrativo, 3 autoridades y 5 como personal de apoyo, (ver Tabla 2.1).

Para tener una idea clara de los objetivos que tiene la institución se presenta a continuación la misión, visión e ideario.

2.1.1.1 Misión

"Somos una Institución Educativa Particular Católica Arquidiocesana de Quito que brinda educación formal y escolarizada en los niveles de Inicial II, Preparatoria, Educación General Básica y Bachillerato General Unificado. Educamos a niños, niñas y jóvenes hacia el humanismo solidario, para que vivan, piensen y actúen como seres humanos responsables, comprometidos con el desarrollo de sus capacidades y el cambio social para la búsqueda del bien común. Proponemos una educación con un enfoque Inter estructurante y biocentrista con profesionales idóneos que buscan la excelencia académica mediante técnicas metodológicas constructivistas y la promoción de la identidad católica cristiana, con el fortalecimiento del sentido de iglesia y el buen vivir, considerando a Cristo como ejemplo de hermano, amigo y maestro" [70].

2.1.1.2 Visión

Para el 2024 la Unidad Educativa FESVIP será reconocida como una institución educativa de excelencia en el marco de los estándares de calidad del Ministerio de Educación con estudiantes y docentes que lideren y ejecuten proyectos educativos

innovadores, que promuevan el pensamiento crítico, participación y conciencia social, respetando los principios del Buen Vivir acorde a las razones del humanismo solidario [70].

2.1.1.3 Ideario

La Unidad Educativa Fernández Salvador Villavicencio Ponce, se suscribe al ideario de la REDA-Q como soporte esencial del ser institucional y elemento orientador de la praxis educativa, en el que se expresa claramente las políticas, los principios y valores del compromiso por una educación de calidad, calidez y excelencia, que lleve al desarrollo integral de las personas y al cambio social en la línea del Evangelio. En este orden de ideas, el ideario es una construcción colectiva y participativa de todas y cada una de las instituciones educativas que, desde la perspectiva del Evangelio, la experiencia educativa de la Iglesia y de los principios y fines planteados por la Ley Orgánica de Educación Intercultural (LOEI) [70].

2.1.2 INFORMACIÓN GENERAL DE LA INSTITUCIÓN

Tabla 2.1 Cantidad de población “FESVIP"

POBLACIÓN	NÚMERO TOTAL
Autoridades	3
Personal Administrativo	14
Personal Docente	42
Personal de Apoyo	5
Estudiantes	936
TOTAL	**1000**

2.1.3 ESTRUCTURA ORGANIZACIONAL

El personal se encuentra organizado de la siguiente manera:

- Personal Administrativo:
    - Autoridades

    - Rector
    - Vicerrector
    - Inspector General
    - Secretaria General y auxiliar
    - Colecturía
    - Recepción
    - Enfermería
    - Departamento de Consejería estudiantil
    - Inspectores de Nivel
- Personal de Apoyo
- Personal docente:
    - Coordinadores de área
    - Coordinadores de Junta académica
    - Tutores
    - Pastoral
- Estudiantes

La clasificación se realiza mediante las funciones que desempeñan en la institución. También se toma en cuenta como personal administrativo a las autoridades, inspectores y a coordinadores de departamentos que a su vez fungen funciones docentes.

Los organismos existentes en la institución son los siguientes:

- Consejo Ejecutivo
- Departamento de Pastoral
- Departamento Financiero
- Departamento de Talento Humano
- Consejo Estudiantil
- Comité Central de Padres de Familia
- Departamento de Consejería estudiantil
- Departamento de Enfermería
- Junta académica
- Departamento de inspección

Se debe considerar que la administración tecnológica de la Unidad Educativa “FESVIP” se encuentra a cargo de un docente con conocimientos básicos en sistemas informáticos. La institución no cuenta con personal técnico capacitado, el cual se encargue entre otras cosas de la administración y mantenimiento de la red activa y pasiva, así como del manejo de servicios, aplicaciones y desarrollo de *software*.

2.1.4 DESCRIPCIÓN DE LA INFRAESTRUCTURA “FESVIP”

La Unidad Educativa “FESVIP” tiene la extensión de área útil 8961,12 m^2, con una superficie total de 9261,19 m^2, está ubicada en el sector de la Villa Flora, Av. Maldonado S8-268 y Av. Rodrigo de Chávez. La distribución física de sus instalaciones se detalla en la Figura 2.1 y la ubicación en la Figura 2.2.

La distribución completa de cada uno de los edificios de la Unidad Educativa “FESVIP” se encuentra en el **ANEXO A**.

Figura 2.1 Distribución física de las instalaciones de la UE-FESVIP

Figura 2.2 Ubicación de la UE-FESVIP a través de Google Earth.

2.1.5 ESTRUCTURA TECNOLÓGICA DE LA UNIDAD EDUCATIVA "FESVIP"

2.1.5.1 Sistema de comunicaciones

La Unidad Educativa "FESVIP" cuenta al momento de realizar la inspección con un sistema de comunicaciones muy básico, el cual ha sido implementado en base a la necesidad de la institución de contar con puntos de red para que su personal pueda trabajar y tenga acceso a Internet. (ver Figura 2.3) Este sistema no permite obtener todas las bondades de una red convergente.

Figura 2.3 Switch de red - sala de profesores escuela

Adicionalmente se observan redes inalámbricas creadas sin ninguna planeación, en la que solamente se han ido incrementando equipos *routers* repetidores (ver Figura 2.4). No se tienen VLAN, lo cual genera problemas de conexión.

Figura 2.4 Router repetidor TP-LINK

2.1.5.2 Topología de red

No existe una topología de red diseñada ni definida en la Institución. El proveedor de Internet se conecta directamente a través de un *router* a 4 *switches* en cascada y de ellos se desprenden cables de red para las estaciones de trabajo y puntos de acceso inalámbrico, tal como se puede evidenciar en la Figura 2.5 Rack – área administrativa.

Figura 2.5 Rack – área administrativa

De las inspecciones realizadas se verificó que las aulas de los pisos superiores del edificio principal (piso 1, piso 2 y piso 3), aulas prefabricadas y aulas de inicial, no poseen ningún tipo de red, sea cableada o inalámbrica.

En la Figura 2.6, se presenta el diagrama lógico de red de la Unidad Educativa “FESVIP”.

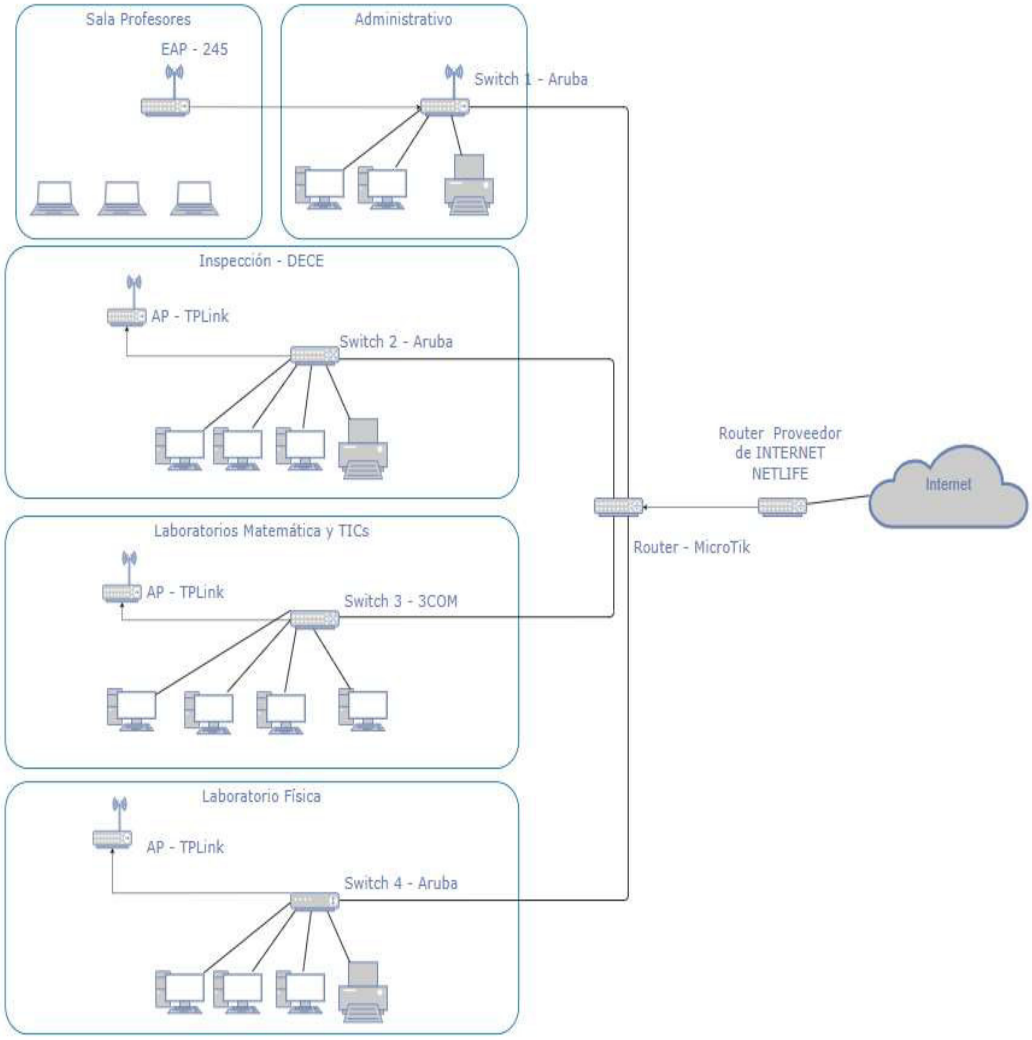


Figura 2.6 Diagrama lógico de red de la UE - FESVIP

2.1.5.3 Descripción del sistema de voz

La red de telefonía de la Unidad Educativa "FESVIP" está constituida por una central telefónica de marca PANASONIC (ver Figura 2.7), modelo *Advanced Hybrid System* KX-YA616, la cual brinda comunicación entre las diferentes áreas y es el punto de conexión para realizar y recibir llamadas hacia la PSTN.

Figura 2.7 Central telefónica PANASONIC

La central telefónica dispone de un total de 25 extensiones, las cuales se integran para brindar comunicación interna y llamadas externas, pero no todas las extensiones están en uso, como se puede evidenciar en la Tabla 2.2.

Tabla 2.2 Extensiones en uso de la Unidad Educativa “FESVIP”

EXTENSIÓN	DEPARTAMENTO	RESPONSABLE
101	Recepción	Jenny Andrade
102	Secretaría General	Cecilia Andrade
103	Auxiliar Secretaría	Johanna Tello
104	Contabilidad	Ing. César Serrano
105	Rectorado	M.Sc. Edison Ponce
106	DECE	Psi. Paola Muñoz
107	Colecturía	Ing. César Serrano
108	Administración	Padre Mario Serrano
110	Inspección General	Ing. Geovanna Guevara
111	Vicerrectorado	Lic. Gabriela Quintero
112	DECE	Psi. Erika Hurtado
113	Subinspección	Lic. Hernán Jami
120	Consejería	Sr. Francisco Guamán
124	BAR	Sra. Narcisa de Naranjo

Las líneas externas que son provistas por el proveedor de servicios telefónicos CNT (Corporación Nacional de Telecomunicaciones) son las indicadas en la Tabla 2.3.

Tabla 2.3 Servicios telefónicos CNT

PROVEEDOR	NÚMERO	PERMISOS
CNT	02-2653478	L, N, C
CNT	02-2653881	L, N, C

Esta central telefónica tiene varios inconvenientes entre los cuales se pueden mencionar: los años de vida útil cumplidos, funcionalidades básicas y descontinuadas con la realidad actual, cableado en malas condiciones, instalación sin mantenimiento, por lo que se considera un sistema de comunicaciones prácticamente obsoleto.

2.1.5.4 Descripción del sistema de video vigilancia

El sistema de video vigilancia de la Unidad Educativa “FESVIP” es de marca DAHUA, que consta de 31 cámaras instaladas las cuales utilizan su propio cableado (ver Figura 2.8).

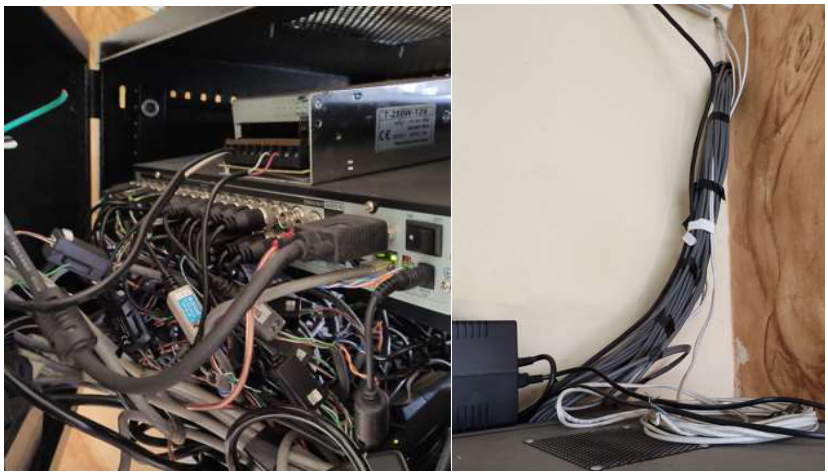


Figura 2.8 Sistema de video vigilancia DAHUA

Este sistema permite vigilar y monitorear toda la Institución, pero se encuentran falencias a nivel de cableado estructurado y ductos hacia donde se hallan ubicadas las cámaras.

2.1.5.5 Descripción del sistema de cableado estructurado

El principal problema que se pudo observar dentro de las instalaciones de la Unidad Educativa “FESVIP” es su cableado estructurado. Se constató la instalación de cables de red de forma artesanal y conectados directamente desde un *switch* hasta las estaciones de trabajo.

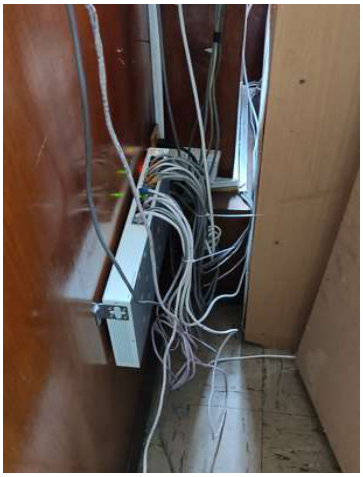


Figura 2.9 Switch en áreas de trabajo del personal

En la Figura 2.9 se observa claramente que se están incumpliendo las normas correspondientes de cableado estructurado.

Dentro de los laboratorios se encontraron mini *racks* conectados con cables de red directamente a las estaciones de trabajo (ver Figura 2.10), incumpliendo igualmente las normas de cableado estructurado.

Figura 2.10 Mini Racks en laboratorios de computación e instalaciones de red.

2.1.5.6 Sistema eléctrico y UPS

De las entrevistas a las autoridades de la Unidad Educativa, se pudo determinar que el sistema eléctrico se instaló hace más de 40 años, por lo que se encuentra totalmente deteriorado.

Los ductos que existen en el edificio principal son utilizados y adaptados para el sistema eléctrico, pero adicionalmente existen canaletas y manguera corrugada que es visible a simple vista y que no está acorde a la fachada de la edificación.

Actualmente existen 400 tomas eléctricas y 448 lámparas tal y como se detalla en la Tabla 2.4 Resumen de lámparas y tomas eléctricas “FESVIP”, que necesitan ser remodeladas para garantizar el correcto funcionamiento del sistema eléctrico y de iluminación.

Tabla 2.4 Resumen de lámparas y tomas eléctricas “FESVIP”

ZONAS	LÁMPARAS	TOMACORRIENTES
BLOQUE 1	267	216
BLOQUE 2	26	19
BLOQUE 3	37	29
BLOQUE 4	118	136
TOTAL	448	400

A nivel de UPS y reguladores de voltaje, solamente se encontraron 2, uno que protege a los equipos principales de comunicación, sobre el *rack* principal en el edificio administrativo y otro que protege el sistema de cámaras. El detalle de estos dispositivos se muestra en la Tabla 2.5.

Tabla 2.5 UPS en video vigilancia y equipos de comunicación

MARCA	MODELO	N° DE SERIE	UBICACIÓN
CDP (*Chicago Digital Power*) Power B-UPR505 500VA/300V	MEREGU008	N/A	Video vigilancia
EMERSON /VERTIV	Liebert GXT5	N/A	Equipos de Comunicación

2.1.5.7 Características de los equipos que integran la red activa “FESVIP”

Las necesidades de comunicación que han ido creciendo en los últimos años, han determinado que la Unidad Educativa “FESVIP” adquiera equipamiento que de cierta manera brinde conectividad, acceso a Internet y continuidad de trabajo en el día a día. En la Tabla 2.6 Equipos de red "FESVIP" se presenta un resumen de los equipos de red que dispone la Institución.

Desde el año 2016 “FESVIP” dispone de un servicio de Internet proporcionado por el proveedor NETLIFE a través de un *router* (ver Figura 2.11) con una capacidad actual de 100 Mbps.

Tabla 2.6 Equipos de red "FESVIP"

TIPO	MARCA	MODELO	PUERTOS	OBSERVACIONES
Router	Huawei	EchoLife HS8245W	4 puertos	Proveedor de Internet
Router	*MikroTik*	*RouterBoard 1100 AHx4*	13 puertos	Área Administrativa
Switch	*Aruba*	*2930F JL259A*	24 puertos Gb, 4 puertos SFP	
Controller	*TPLink*	*Omada OC200*	2 puertos	
Switch	Aruba	InstantON 1930 JL682A	24 puertos Gb, 4 puertos SFP	Sala de Profesores
Switch	3COM	4500 26-Port	26 puertos Gb	Laboratorios
Switch	Aruba	InstantON 1930 JL682A	24 puertos Gb, 4 puertos SFP	

Figura 2.11 Router HUAWEI proveedor de Internet

En el mini *rack* principal que se encuentra en el área administrativa, se ubican equipos que están actuando como *switches* de *Core* y de acceso como se muestra en la Figura 2.12.

Figura 2.12 Equipos mini *rack* área administrativa

En el área de inspección general y sala de profesores escuela, existe un equipo que está interconectado en cascada con el equipo de *Core* (ver Figura 2.13).

Figura 2.13 Switch de inspección y sala de profesores

En los laboratorios de computación, física y TIC, en un mini *rack* empotrado en la pared, se encuentran equipos en cascada con una conexión mediante cable UTP al equipo de *Core*. Estos equipos se han ido incrementando con el fin de aumentar puntos de red para los laboratorios, tal como muestra la Figura 2.14.

Figura 2.14 Mini *rack* – equipos de red laboratorios

En la visita técnica realizada a la Institución se evidenció que existen varios equipos *Access Point* que están actuando como equipos de acceso inalámbrico, conectados a los *switches* de acceso, trabajando como repetidores, y "facilitando" el acceso a la red vía inalámbrica. En la Tabla 2.7 se detallan los equipos inalámbricos, así como sus principales características.

Tabla 2.7 Equipos AP

ÁREA	TIPO	MARCA	MODELO	OBSERVACIONES
Laboratorio TIC	AP	TPLINK	TL-WR840N	1 puerto 10/100 Mbps WAN y 4 puertos 10/100 Mbps LAN
Laboratorio Física	AP	TPLINK	TL-WR840N	1 puerto 10/100 Mbps WAN y 4 puertos 10/100 Mbps LAN
Capilla	AP	TPLINK	TL-WR840N	1 puerto 10/100 Mbps WAN y 4 puertos 10/100 Mbps LAN
Administrativo	AP	TPLINK	TL-WR841N	1 puerto 10/100 Mbps WAN y 4 puertos 10/100 Mbps LAN
Sala de Profesores	AP	TPLINK	EAP245	2 puertos 10/100 Mbps LAN
Inspección de nivel - Piso 1	AP	NEXXT	NEBULA 300 ARN02304U4	4 puertos 10/100 Mbps LAN

Todos estos equipos (ver Figura 2.15) se han incorporado a la red sin ninguna planificación, por lo que presentan varios problemas, entre ellos la cobertura y acceso a Internet de los usuarios, causando malestar y descontento.

Figura 2.15 AP dispuestos en el área administrativa

2.1.5.8 Servidores y aplicaciones

La Unidad Educativa “FESVIP” no posee ningún servicio y/o aplicación alojada en servidores propios de la institución; únicamente posee una página web (**http://fesvip.edu.ec/)** alojada en un *hosting* público y administrada por personal externo a la institución.

2.1.5.9 Estaciones de trabajo

Dentro de la Unidad Educativa “FEVIP” las estaciones de trabajo asignadas al personal que labora en las diferentes áreas de la Unidad Educativa “FESVIP”, así como los equipos que se encuentran en las oficinas tienen las características mostradas en la Tabla 2.8.

Tabla 2.8 Equipos de computación “FESVIP” área administrativa

ÁREAS	EQUIPOS	CARACTERÍSTICAS
Rectorado	1	RAM 4 - AMD Ryzen 5 3500U - 2.1 GHz
Secretaría	2	RAM 4 - AMD Ryzen 5 3500U - 2.1 GHz
		RAM 4 - CORE I3 -1,8 GHz
Inspección General	4	RAM 4 - AMD Ryzen 5 3500U - 2.1 GHz
		RAM 4 - CORE I3 -1,8 GHz
Inspección de Nivel	2	RAM 4 - CORE I3 -1,8 GHz
Vicerrectorado	2	RAM 4 - AMD Ryzen 5 3500U - 2.1 GHz
		RAM 4 - CORE I3 -1,8 GHz
Departamento de Investigación	1	RAM 4 - AMD Ryzen 5 3500U - 2.1 GHz
Sub-coordinación del departamento de investigación	1	RAM 4 - AMD Ryzen 5 3500U - 2.1 GHz
Colecturía	9	RAM 4 - AMD Ryzen 5 3500U - 2.1 GHz
DECE escuela	1	RAM 4 - CORE I3 -1,8 GHz
DECE básica superior	1	RAM 4 - CORE I3 -1,8 GHz
DECE Bachillerato	2	RAM 4 - CORE I3 -1,8 GHz
Pastoral	1	RAM 4 - AMD Ryzen 5 3500U - 2.1 GHz
Enfermería	1	RAM 4 - CORE I3 -1,8 GHz
TOTAL	**28**	

En la Tabla 2.10 se detallan las cantidades de estaciones de trabajo en toda la Institución, incluidos los laboratorios (Tabla 2.9), siendo importante indicar que al momento la gran mayoría de equipos se encuentran almacenados (ver Figura 2.16).

Figura 2.16 Equipos de computación área educativa laboratorios

Tabla 2.9 Equipos laboratorio de computación

AREAS EDUCATIVAS	EQUIPOS	CARACTERÍSTICAS
Laboratorio de computación escuela	24	RAM 4 - CORE I3 -1,8 GHz
	1	8 RAM - CORE I3 -1,2 GHz-10°generación
Laboratorio de computación colegio	24	RAM 4 - CORE I3 -1,8 GHz
	1	8 RAM - CORE I3 -1,2 GHz-10°generación
Laboratorio de Física	3	RAM 4 - CORE I3 -1,8 GHz
	1	8 RAM - CORE I3 -1,2 GHz-10°generación
Laboratorio de Química	1	8 RAM - CORE I3 -1,2 GHz -10°generación
TOTAL	**55**	

Tabla 2.10 Total de estaciones de trabajo “FESVIP”

ÁREA	EQUIPOS
ADMINISTRATIVA	28
EDUCATIVA	55
TOTAL	**83**

2.1.5.10 Seguridad en la red

A nivel de seguridad, la Unidad Educativa “FESVIP” no ha realizado ninguna inversión, siendo actualmente uno de los principales puntos de falla dentro de su infraestructura tecnológica, ya que se encuentran expuestos ante cualquier tipo de ataque cibernético.

A nivel de seguridad perimetral no se cuenta con un dispositivo *firewall* que permita controlar, filtrar, examinar toda la información que circula desde la red interna hacia el Internet, por lo que toda su red está en peligro inminente, incluidos los equipos que actualmente posee como equipos de comunicaciones.

2.1.6 RESUMEN DEL ANÁLISIS Y DE LOS PRINCIPALES PROBLEMAS DE COMUNICACIÓN “FESVIP”

En base a la situación actual de la Unidad Educativa “FESVIP” descrita, se puede concluir que se tienen muchas falencias a nivel tecnológico. En la red pasiva se observa que la Institución no posee un sistema de cableado estructurado; la instalación artesanal de cables de red y conexiones directas a los equipos provocan inestabilidad en la red de datos y no se considera como un sistema. Así mismo al no disponer de todos los subsistemas se generan en muchos de los casos una mala interoperabilidad de los elementos de red actuales; igualmente al no considerar estándares y especificaciones técnicas, las condiciones del cableado son lamentables. Es importante indicar que existen áreas donde no existe conectividad a nivel de LAN cableada, como por ejemplo los pisos 1, 2 y 3 del edificio principal y las zonas de las aulas prefabricadas que están aisladas de los edificios principales.

La renovación del cableado eléctrico es fundamental para continuar con la operatividad de todos los servicios, es primordial renovar todo el sistema.

Sobre la red activa, se puede decir que se tienen equipos relativamente nuevos a nivel de conectividad de red, pero que no están siendo usados de manera correcta. El no tener un diseño y una topología de red definidos provoca una red deficiente y con un rendimiento que a percepción de todos los usuarios es pésimo; en muchas ocasiones incluso no se tiene servicio ya que se han tenido “caídas” totales de la red. Del mismo modo en las redes inalámbricas creadas con cada *Access Point* instalado, se presenta mucha inestabilidad a la hora de la conexión; existe un desorden en el despliegue que genera una señal deficiente en ciertos puntos de la Unidad Educativa “FESVIP” e incluso hay lugares sin conectividad inalámbrica para el personal administrativo, autoridades y profesores.

Los servicios telefónicos en la Unidad Educativa “FESVIP” son antiguos, analógicos, prácticamente obsoletos por lo que es inevitable renovar e implementar un sistema de comunicaciones unificadas que facilite el trabajo de todos.

En lo que a servicios se refiere, es indispensable contar con las aplicaciones mínimas que requiere una Unidad Educativa para su operación, considerando el crecimiento tecnológico y las diferentes necesidades que se presentan en el día a día; el no contar con estas herramientas retrasará las labores diarias de todo el personal.

En cuanto a equipamiento para personal administrativo y laboratorios, es necesario actualizar los mismos, mejorar las características para que estén acordes a la realidad actual y puedan brindar un servicio de calidad a todos; de no poder actualizar los mismos se debe considerar repotenciarlos (aumento de disco, de memoria, cambio de procesador) e instalar software acorde a las necesidades, tomando como punto de partida un antivirus más que necesario para salvaguardar la información de los usuarios.

El principal problema más allá de todo lo mencionado anteriormente, es que la Unidad Educativa no cuenta con un sistema de seguridad perimetral, por lo que la exposición a ataques no solo a las estaciones de trabajo sino también a los equipos de conectividad es muy grande; es fundamental la instalación de un equipo que pueda brindar la seguridad que amerita la institución y además que pueda controlar y regular el tráfico hacia Internet.

2.1.7 REQUERIMIENTOS EN LA UNIDAD EDUCATIVA "FESVIP"

Los requerimientos de la Unidad Educativa se han obtenido en base a reuniones generadas con autoridades, personal administrativo y personal docente. Estas entrevistas han permitido recabar información acerca de las falencias y necesidades de servicios de red para dar continuidad a sus labores diarias.

A nivel de red se ha observado la necesidad de generar una estructura jerárquica de red, dotar de equipamiento para cubrir todas las áreas de la Institución, adecuar correctamente los equipos, dar facilidades al usuario para la conexión ya sea por cable de red o *Wifi (Wireless Fidelity)*, tener una gestión de administración controlada para que la red funcione sin problemas y se pueda garantizar su servicio.

Es necesario realizar una correcta organización a nivel de segmentación de red, es decir, generar subredes para los diferentes servicios y/o áreas de la Institución; con una segmentación correcta se podrá generar las VLAN necesarias para que la red funciones de manera óptima.

Actualmente la Unidad Educativa cuenta con una red inalámbrica instalada sin planificación, como se mencionó solo se han ido agregando dispositivos de acceso que han generado un sinnúmero de redes inalámbricas que causan conflicto y malestar en la conexión de los usuarios. Es necesario realizar un *Site survey* predictivo para planificar la cantidad de puntos de acceso necesarios en la Institución, además de los modelos a utilizar.

A nivel de telefonía IP es necesario el cambio de central telefónica ya que actualmente la central PANASONIC, de tecnología antigua, está descontinuada en el mercado. Por ello se propone un sistema de telefonía VoIP acorde a los estándares y tecnologías actuales, que además permite funcionalidades de comunicaciones unificadas y que puede integrarse con líneas de la PSTN.

Actualmente la Institución no cuenta con un sistema de videoconferencia por lo que es de vital importancia proveer de un sistema que permita el uso de estas nuevas tecnologías para continuar con el proceso de enseñanza-aprendizaje en la Institución en el contexto actual de pandemia COVID-19.

El sistema de cableado estructurado que posee actualmente la institución como se ha podido observar no cumple con ningún estándar, por lo que es sumamente necesario la reestructuración de todos los sistemas y subsistemas de cableado estructurado.

La Unidad Educativa “FESVIP” no cuenta con aplicaciones propias para varios servicios fundamentales propios de una Entidad Educativa a nivel tecnológico como: *Active Directory*, DNS, DHCP, FTP, correo electrónico. Por lo que se requiere disponer de estos servicios para que la Institución pueda utilizarlos y mejorar sustancialmente los procesos internos y el desempeño del personal.

La seguridad en la red actualmente es el arma más poderosa para contrarrestar amenazas y ataques que se vienen generando y dar protección a la infraestructura de red y a los usuarios. En la institución es necesario un equipo de seguridad perimetral que actúe como *firewall* y además tenga características como filtrado web, control de aplicaciones, detección de intrusos, control de accesos y que permita tener una administración centralizada y generación de reportes para los análisis correspondientes.

2.2 DISEÑO DE LA RED CONVERGENTE PARA “FESVIP”

Con lo detallado en el apartado anterior se puede deducir que la Unidad Educativa “FESVIP” presenta carencias en su infraestructura de red física y lógica. Por tal motivo se presenta su diseño con el propósito de dar soluciones a dichos problemas, tomando en cuenta también las necesidades institucionales, las cuales se incluirán en el presente diseño, para permitir una adecuada solución técnica y económica.

2.2.1 TECNOLOGÍA Y TOPOLOGÍA DE RED

Se debe considerar que la topología de red dentro del diseño es uno de los conceptos más importantes y es fundamental definir y conocer la mejor alternativa partiendo de la teoría base disponible.

Para el presente diseño se propone el esquema de interconexión jerárquico redundante de *switches*, (ver Figura 2.17) con capas definidas en base al modelo de diseño jerárquico de CISCO.

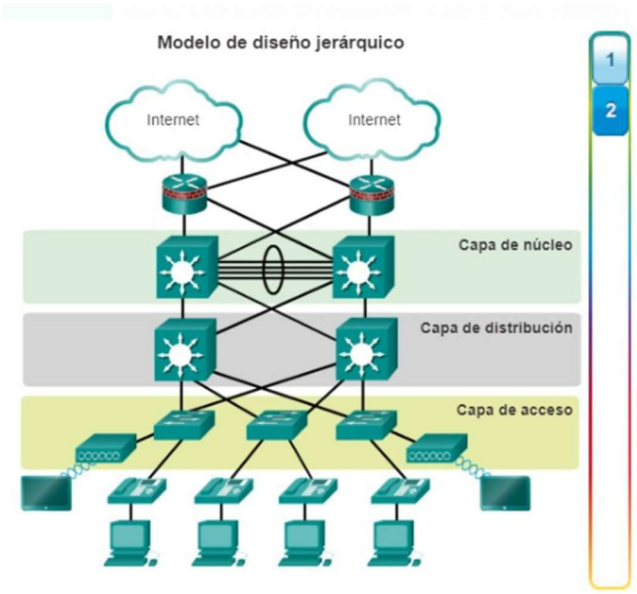


Figura 2.17 Modelo jerárquico CISCO [72]

En este diseño, la tecnología de red que se va a utilizar es Gigabit Ethernet e incluso 10GBaseT, debido a que la demanda de tráfico de las aplicaciones a utilizar, la cantidad de usuarios y las mejoras presentadas en este diseño así lo requieren.

2.2.2 DISEÑO LÓGICO DE RED

Las redes de datos se encuentran basadas principalmente en diseños jerárquicos por la eficiencia que deben presentar; este diseño proporciona una fácil administración y operatividad de las redes convergentes. Al diseñar las redes de manera jerárquica (dividiendo en capas), cada una de las capas realiza una tarea específica obteniendo un diseño modular, el cual mejora la eficiencia y rendimiento en la red. A continuación, se describen las capas a diseñar dentro de este modelo.

2.2.2.1 Core

La Capa núcleo o *Core* se encarga de interconectar dispositivos de la capa de distribución y el *router* del proveedor de Internet; en este diseño se considera manejar un solo equipo *switch* de *Core* por el costo asociado del mismo.

2.2.2.2 Distribución

La capa de distribución es el punto intermedio entre la capa *Core* y la capa de acceso a la red y sus servicios. En el diseño de la Unidad Educativa "FESVIP" se propone dos *switches* de distribución interconectados con el *Core* a través de enlaces de fibra. Estos *switches* de distribución permitirán acceso a la red a través de la interconexión con la capa de acceso en todas las áreas de la institución, especialmente a las aulas prefabricadas que se encuentran distantes al edificio principal y administrativo. En estos dispositivos se realizan configuraciones de red tales como VLAN, ruteo y protocolos que faciliten la interconexión.

2.2.2.3 Acceso

La capa acceso permite interconectar a la red, dispositivos finales como CPU (*Central Processing Unit*), *laptops*, impresoras, teléfonos IP, cañones de proyección, entre otros. Su función principal es aportar una técnica o medio de conexión, así como controlar la comunicación de los dispositivos a la red. La distribución de los *switches* en la red de la Institución se muestra en la Figura 2.18.

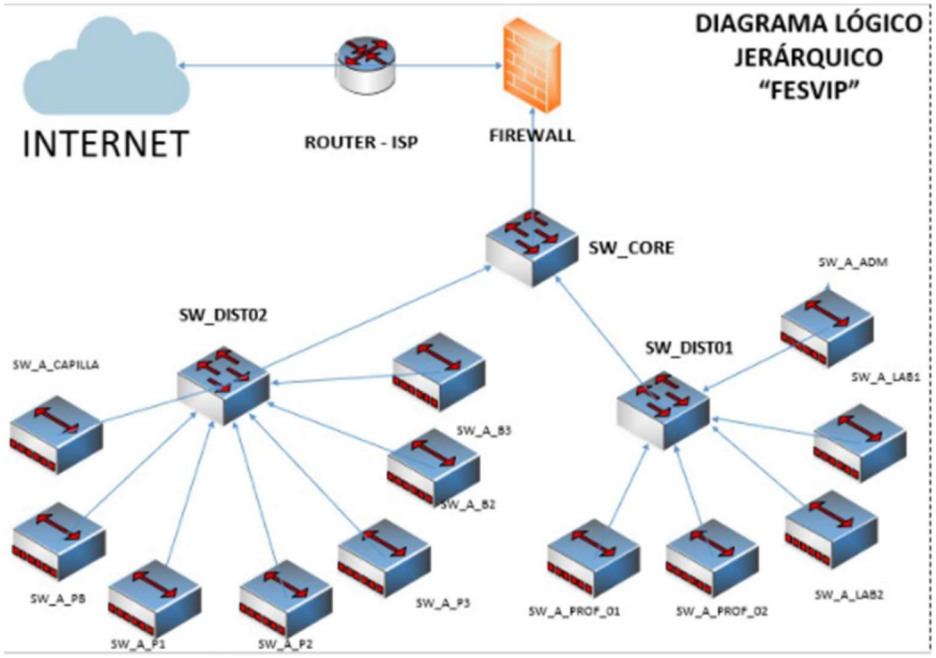


Figura 2.18 Diseño de la red

2.2.3 DISEÑO DE LA RED PASIVA

El presente diseño se encuentra conformado por la estructura física de la red, que consta de los elementos que son necesarios para interconectar los enlaces de datos en la Unidad Educativa “FESVIP”.

2.2.3.1 Sistema de cableado estructurado

El sistema de cableado estructurado (SCE), es el soporte físico que dará servicio a toda la infraestructura de equipos activos brindando protección y evitando pérdida de datos.

La Unidad Educativa “FESVIP” como se indica en la situación actual, posee un SCE que no cumple con las normas, por lo que se planteará un SCE estandarizado.

2.2.3.1.1 Distribución de puntos de red

Para el diseño y la distribución de los puntos de red se considera el estándar ANSI/TIA 568.0-D, que especifica la distancia para todos los subsistemas de cableado estructurado a nivel horizontal, mencionando una longitud de cable máxima de 100 m.

En el **ANEXO B**, se encuentra el detalle de los puntos de red, ubicación y funcionalidad dentro de todas las áreas de la Unidad Educativa “FESVIP”. En la Tabla 2.11. se muestra la cantidad de puntos total para el diseño del SCE.

Tabla 2.11 Puntos de red en la UE - FESVIP

ÁREAS PRINCIPALES DE LA UNIDAD EDUCATIVA "FESVIP"	PUNTOS DE RED
EDIFICIO PRINCIPAL	132
AULAS PREFABRICADAS INICIAL Y PREPARATORIA	12
AULAS PREFABRICADAS - PATIO PRINCIPAL	20
EDIFICIO ADMINISTRATIVO	128
TOTAL	**292**

Se debe considerar un porcentaje de crecimiento de número de puertos para un cableado futuro en un período aproximado de 10 años.

2.2.3.2 Subsistema de cableado vertical

El subsistema de cableado vertical de la Unidad Educativa “FESVIP” es aquel que provee la interconexión entre las distintas áreas de la institución, tal y como se describen en el apartado anterior.

Por la distancia que existe entre el cuarto de equipos y el edificio principal, así como de las aulas prefabricadas, se ha optado el uso de fibra óptica multimodo 62.5/125 µm TIA 492AAAA(OM1), la cual soporta una longitud máxima de 2000 metros, de acuerdo con las recomendaciones establecidas por el “estándar de componentes de cableado de fibra óptica” EIA/TIA 568C-3. Se ha tomado en cuenta este medio de transmisión por sus características como flexibilidad y ancho de banda.

2.2.3.2.1 Rutas

En la Tabla 2.12 se detallan las distancias para interconectar el cuarto de comunicaciones con los *racks* de piso de las diferentes áreas y en la Tabla 2.13 se resume la longitud total en cada bloque con la holgura recomendada para la Unidad Educativa “FESVIP”

Tabla 2.12 Longitud de fibra óptica entre los cuartos de telecomunicaciones

EDIFICIO PRINCIPAL		
ÁREA 1	**ÁREA 2**	**DISTANCIA (metros)**
Subsuelo (capilla)	Planta Baja	20
Subsuelo (capilla)	Primer Piso	40
Subsuelo (capilla)	Segundo Piso	60
Subsuelo (capilla)	Tercer Piso	80
Cuarto de equipos	Capilla	77,4
Subsuelo (capilla)	Aulas Prefabricadas Inicial y Preparatoria	60
Subsuelo (capilla)	Aulas Prefabricadas Patio Principal	70
Cuarto de equipos	Sala de profesores escuela	40
Cuarto de equipos	Subsuelo – Laboratorios	60
TOTAL (metros)		507,4

Tabla 2.13 Longitud de fibra óptica con margen de holgura del 10 %

CABLE FIBRA ÓPTICA			
ZONA	LONGITUD (metros)	HOLGURA 10%	LONGITUD TOTAL (metros)
BLOQUE 1	277,4	27,74	305,14
BLOQUE 2	60	6	66
BLOQUE 3	70	7	77
BLOQUE 4	100	10	110
TOTAL (metros)			558,14

2.2.3.2.2 Accesorios

El diseño que se ha establecido para la Institución en el edificio principal, se lo realiza mediante interconexiones entre las plantas de forma interna, evitando que el cableado se encuentre fuera (uso de escalerillas y canaletas) y que tenga problemas por agentes externos. Adicionalmente se ha considerado la interconexión desde el cuarto de equipos al *switch* de distribución (subsuelo capilla), que por la distancia se lo realiza con cableado subterráneo, cumpliendo las normas.

2.2.3.3 Subsistema de cableado horizontal

El subsistema de cableado horizontal es aquel que se extiende desde la salida/conector del equipo de telecomunicaciones en las áreas de trabajo de la Institución hasta el *rack* el cual se encuentra ubicado en el cuarto de comunicaciones. Como se ha mencionado, la topología de red es en estrella, con cada salida que estará conectada al *rack*, incluyendo la salida del cable horizontal. El *rack* para el diseño se ubicará en el cuarto de comunicaciones en el edificio administrativo primer piso.

En el diseño se considera también la conexión de los puntos de red, mediante *patch cords* RJ45 – Norma TIA/EIA 568.0-D y cables UTP de 100 Ω, categoría 6A, apegados a la norma T568B. Por tal motivo los *patch cords* deben ser certificados y elaborados en fábrica.

En cada área de trabajo se encuentra una computadora, la cual estará conectada a un punto de red, por lo que se deberá instalar *faceplate*s dobles, los cuales estarán ubicados a 50 cm del nivel del piso.

Para el cableado horizontal se utilizará en el *rack patch panels* de 24 puertos para la conexión de las estaciones de trabajo.

2.2.3.3.1 Rutas

En el **ANEXO C**, se detallan las distancias para el cableado horizontal en todas las áreas de la Unidad Educativa "FESVIP". En la Tabla 2.14. se muestra la longitud total del cable, sin tomar en cuenta el margen de holgura del 10%, así como los puntos de red.

Tabla 2.14 Longitud total cable

TOTAL	DISTANCIA (metros)	PUNTOS DE RED
	8532 m	292

En la Tabla 2.15 se detalla la longitud de cable UTP por zonas tomando en cuenta el margen de holgura del 10 % con un total de 8933,1 metros, por lo que es necesario para el cableado horizontal **31 rollos** de cable UTP, ya que cada rollo contiene 305 metros aproximadamente.

Tabla 2.15 Longitud total de UTP con margen de holgura del 10%

BLOQUE	LONGITUD (metros)	HOLGURA 10%	LONGITUD TOTAL (metros)
1	4298	429,8	4727,8
2	218	21,8	239,8
3	448	44,8	492,8
4	3157	315,7	3472,7
		TOTAL (metros)	**8933,1**

Tomando en cuenta la ubicación de los *access point*, se considera la longitud de cable UTP Cat 6A que se utilizará con un margen de holgura del 10%. (ver Tabla 2.16)

Tabla 2.16 Longitud cable UTP para AP

CABLE UTP 6A ACCESS POINT			
ZONA	LONGITUD	HOLGURA 10%	LONGITUD TOTAL
BLOQUE 1	451	45,1	496,1
BLOQUE 2	38	3,8	41,8
BLOQUE 3	108	10,8	118,8
BLOQUE 4	227	22,7	249,7
TOTAL			906,4

Para el sistema de video vigilancia se ha considerado el cálculo de cable UTP que se utilizará para integrar las cámaras a los *switches* de acceso en el diseño propuesto.

Tabla 2.17 Longitud de cable UTP para video vigilancia

CABLE UTP 6A VIDEO VIGILANCIA			
ZONA	LONGITUD (metros)	HOLGURA 10%	LONGITUD TOTAL (metros)
BLOQUE 1	705	70,5	775,5
BLOQUE 2	26	2,6	28,6
BLOQUE 3	35	3,5	38,5
BLOQUE 4	189	18,9	207,9
TOTAL (metros)			1050,5

En las Tabla 2.16 y Tabla 2.17 se ha calculado la longitud de cable UTP para la ubicación de los *Access Point* y las cámaras del sistema de video vigilancia con un total de 1956,9 metros con un margen de holgura de 10%, siendo necesario **7 rollos** de cable UTP.

Para el enrutamiento del cable UTP se seguirá la norma TIA/EIA 569-A la cual exige instalación de una tendido Conduit desde ductos o escalerillas para cableados hasta las áreas de trabajo.

Se mencionan las alternativas para enrutamiento que pueden ser en sistemas de piso removible, ductos y canaletas, cielo falso como bandejas y tubos metálicos o PVC. En el diseño de la red se propone el uso de canaletas, tubo conduit y sistemas de cielo falso tomando en cuenta la norma antes mencionada. La ocupación será del 20 al 40 % en conductos eléctricos perimetrales, depende del radio del cable y la flexión; con esta consideración se conoce cuántos cables van a pasar por la canaleta, por lo que se adquirirán canaletas de longitud 2 metros con un área de 60x40mm (2400mm^2); con las especificaciones de ocupación se deberá utilizar el 60% del área de la canaleta es decir 1440 mm^2. Para el cálculo se debe conocer que el diámetro del cable UTP categoría 6A es de 9 mm.

$$UTP\ X\ CANALETA\ (60X40) = \frac{60\%\ X\ 2400\ mm^2}{área\ cable\ UTP} = \frac{1440\ mm^2}{81\ mm^2} = 17\ cables\ /canaleta \qquad (2.1)$$

De acuerdo con la ecuación 2.1 para el cálculo de cable UTP por canaleta se podrá determinar el número de cables y el material necesario considerando las canaletas PVC disponibles en el mercado, como son:

- Canaleta 60 x 60 mm = 26 cables UTP
- Canaleta 60 x 40 mm = 17 cables UTP
- Canaleta 40 x 40 mm = 11 cables UTP

- Canaleta 40 x 22 mm = 6 cables UTP
- Canaleta 32 x 12 mm = 2 cables UTP

Las áreas como Capilla, aulas de tercer piso, prefabricadas patio principal y prefabricadas inicial-preparatoria tienen techo de cielo falso lo que facilitará la canalización de cable UTP.

2.2.3.3.2 Accesorios

De acuerdo con los puntos de cada área de trabajo, se procede a realizar un análisis y se detalla la lista de elementos necesarios para el diseño de este subsistema en cada piso, considerando un margen de error del 10%, ver Tabla 2.18.

Tabla 2.18 Elementos para el cableado horizontal por área

DESCRIPCIÓN	CANTIDAD			
	BLOQUE 1	BLOQUE 2	BLOQUE 3	BLOQUE 4
Canaleta PVC 60X60mm	0	0	0	29
Canaleta PVC 60X40mm	40	0	0	0
Canaleta PVC 40X40mm	0	0	0	45
Canaleta PVC 40X22mm	18	0	0	63
Canaleta PVC 32X12mm	792	56	131	309
Ángulo interno 60x60 mm	0	0	0	0
Ángulo interno 60x40 mm	0	0	0	3
Ángulo interno 40x40 mm	0	0	0	3
Ángulo interno 40x22 mm	1	0	0	2
Ángulo interno 32x12 mm	36	6	9	30
Derivación T 60x 60 mm	0	0	0	31
Derivación T 60x 40 mm	13	0	0	0
Derivación T 40x 40 mm	0	0	0	10
Derivación T 40x 22 mm	3	0	0	4
Derivación T 32x 12 mm	2	0	0	2
Patchcore Cat 6A 3 ft	110	12	15	155
faceplate doble	54	6	6	68
faceplate simple	4	0	3	19
Jack categoría 6A	110	12	15	155

2.2.3.4 Subsistema cuarto de telecomunicaciones

El subsistema cuarto de telecomunicaciones es un espacio exclusivo para los equipos de telecomunicaciones, ya que desde aquí se realizará la interconexión del cableado

horizontal y vertical en todas la áreas educativas y administrativas. Para el diseño de la red se debe tomar en cuenta la norma TIA/EIA-569-A que menciona las rutas y espacios de telecomunicaciones y establece que el cuarto de equipos debe estar ubicado lo más lejos de interferencia electromagnética y su tamaño debe ser de acuerdo con las dimensiones de los equipos instalados. Así también se considera la implementación de los cuartos de telecomunicaciones donde estos nos deben exceder los 100 m de interconexión con las áreas de trabajo cumpliendo la normativa EIA/TIA 569.

Los armarios son de tipo *rack* mural de 19" donde se ubicarán los *switches* y *patch panels*; estos serán instalados en sitios específicos donde exista facilidad de acceso y seguridad.

En el **ANEXO D**, se encuentra detallada la ubicación de cada uno de los *racks* que serán considerados para el diseño en los diferentes sectores de la Unidad Educativa "FESVIP", así como su respectivo dimensionamiento.

El cuarto de comunicaciones principal se ubica en el bloque 4 del edificio administrativo, siendo esta un área que cumple con la normativa EIA/TIA 569, y en la cual ya existe la acometida de Internet y otros servicios como las líneas de la PSTN que permitirán administrar la red eficientemente. Los elementos y equipos que se dispondrán son:

- Bandeja Modem-router
- *Switch* de distribución 16 puertos
- *Switch* de acceso 48 puertos
- *Patch panels*
- 1 *switch* de *Core* de 24 puertos
- 2 organizadores horizontales
- Tomas horizontales
- Servidor de red
- *Gateway* de telefonía
- Sistema de Videoconferencia
- UPS

2.2.3.4.1 Rack

De acuerdo con lo especificado en el **ANEXO D**, en el cuarto de equipos se ubica un armario *rack* de 19" de 22 UR (Unidades de *Rack*), tomando en cuenta que la altura elegida debe ser la suma de los paneles de cableado dejando un espacio libre del 25% para futuro crecimiento o ampliaciones (ver Figura 2.19).

Figura 2.19 Altura armario rack 19" [58].

Adicionalmente se ha tomado en cuenta que en las áreas educativas y administrativas se colocará un *rack* mural de 19" de 6, 12,17 y 22 UR.

Para seguridad de los *racks* se dispone de llaves que reposarán en la inspección general con el fin de evitar que exista una manipulación inadecuada por los miembros de la comunidad educativa como estudiantes, docentes y personal de apoyo.

2.2.3.5 Administración del sistema de cableado estructurado

La administración del SCE se encuentra estandarizada por EIA/TIA 606-A (*Administration Standard for Commercial Telecommunications Infraestructure*). Esta normativa tiene como objetivo dar lineamientos para la administración del sistema de cableado estructurado, la cual es indispensable para obtener una certificación y garantizar el funcionamiento de dicho sistema [17].

2.2.3.5.1 Etiquetas

El etiquetado será básicamente realizado con material adhesivo cumpliendo la normativa EIA/TIA 606-A, que proporciona directrices uniformes para el registro de sistemas de telecomunicaciones.

En el diseño se procederá a etiquetar los puntos de red considerando los aspectos indicados en la Tabla 2.19 y en la Tabla 2.20, como ejemplo se puede ver la Figura 2.20.

Tabla 2.19 Nomenclatura para las diferentes zonas

ZONA	NOMENCLATURA
BLOQUE 1	A
BLOQUE 2	B
BLOQUE 3	C
BLOQUE 4	D

Tabla 2.20 Nomenclatura para las diferentes áreas

ÁREA	NOMENCLATURA
SUBSUELO	S
PLANTA BAJA	B
PRIMER PISO	1
SEGUNDO PISO	2
TERCER PISO	3

Figura 2.20 Ejemplo de etiquetado de la UE - FESVIP

Donde se tiene:

- R1: Lugar de cuarto de equipos de telecomunicaciones
- PP1: *Patch panel*
- A: Zona
- S: Área
- D01: Servicio de datos

2.2.4 DISEÑO DE LA RED ACTIVA

Para la estructura del diseño de la red activa de la Unidad Educativa “FESVIP” se debe considerar los servicios que se ofrecerán para que los equipos activos mantengan un funcionamiento eficiente.

El presente diseño se basa en un modelo jerárquico de tres capas; la primera corresponde al núcleo de la red que permite la interconexión con los dispositivos de distribución y salida desde/hacia Internet, la segunda capa es de distribución y la tercera de acceso, donde están las conexiones de las estaciones de trabajo, cámaras de video vigilancia, teléfonos IP y equipos terminales.

2.2.4.1 Switches

2.2.4.1.1 Switch de núcleo

En el análisis del capítulo anterior se determinó colocar un *switch* de núcleo, el mismo que se ubicará en el cuarto de equipos del edificio administrativo, bloque 4. Esta capa permitirá la interconexión con los *switches* de distribución mediante fibra óptica, con los servidores y hacia Internet a través del *router* proporcionado por el proveedor.

El ancho de banda de transmisión para soportar la comunicación o *backplane* del *switch* de *Core* se calcula en la ecuación 2.2.

$$C_{backpla-cor} = N° \; de \; puertos \; X \; 2 \; X \; 1000 \; Mbps + puertos \; de \; fibra \; x \; 2 \; x \; 1000 Mbps \qquad (2.2)$$

$$C_{backpla-cor} = 12 \; X \; 2 \; X \; 1000 \; Mbps + 4x \; 2 \; x \; 1000 \; Mbps$$

$$C_{backpla-cor} = 32000 \; Mbps$$

$$C_{backpla-co} = 32 \; Gbps$$

En la Tabla 2.21 se presentan los mínimos requerimientos para el *switch* de *Core*.

Tabla 2.21 Requerimientos necesarios para el switch de *Core*

SWITCH DE NÚCLEO	
PARÁMETROS	**CARACTERÍSTICAS MÍNIMAS**
Backplane	32 Gbps
Estándares	IEEE 802.1w
	IEEE 802.1q
	IEEE 802.1d
	IEEE 802.1x
	IEEE 802.1p

	IEEE 802.3d
	IEEE 802.3u
	IEEE 802.3af
	IEEE 802.3x
Puertos	12 puertos 100/1000/10000 Mbps
	IP
	OSPF
	RIPv2
	IGM
	BGP
	DHCP
Throughput	50 Mpps

En el diseño se han considerado equipos de conectividad de las marcas Cisco y Aruba debido a su alta confiabilidad y disponibilidad, siendo estas marcas líderes en el cuadrante mágico de Gartner en los últimos años.

Para la marca Cisco y de acuerdo con el *stock* de equipos a nivel nacional por parte de mayoristas en el mercado local, se ha escogido el modelo SX550X-24 24-Port 10GBase-T *Stackable Managed Switch* (ver Figura 2.21) con sus características mostradas en la Tabla 2.22.

Figura 2.21 Switches administrados apilables Cisco de la serie 550X [73]

Tabla 2.22 Características de switch de Core Cisco [73]

Cisco SX550X-24 24-Port 10GBase-T	
CISCO –CORE	
PARÁMETROS	**DESCRIPCIÓN**
Puertos	24 x 10/100/1000
Capacidad de Conmutación	Capa 2 y 3
Enrutamiento	Capa 3
VLAN	Admite un máximo de 4094 VLAN activas simultáneas; VLAN basadas en puerto, en etiquetas 802.1Q.
Autenticación	basada en la Web / IEEE 802.1X

Principales Estándares	IEEE 802.3 10BASE-T Ethernet, IEEE 802.3u 100BASE-TX Fast Ethernet, IEEE 802.3ab 1000BASE-T Gigabit Ethernet, IEEE 802.3ad Link Aggregation Control Protocol, IEEE 802.3z Gigabit Ethernet, IEEE 802.3ae 10 Gbit / s Ethernet sobre fibra para LAN, IEEE 802.3an 10GBase-T 10 Gbit / s Ethernet sobre cable de par trenzado de cobre, IEEE 802.3x Flow Control, IEEE 802.1Q / p VLAN, IEEE 802.1w Rapid STP, IEEE 802.1s Multiple STP, IEEE 802.1X Port Access Authentication, IEEE 802.3af, IEEE 802.3at, IEEE 802.1AB Link Layer Discovery Protocol, IEEE 802.3az Energy Efficient Ethernet.
IPv6	Modo de host IPv6 sobre Ethernet pila doble IPv6 / IPv4 Descubrimiento de enrutadores y vecinos (ND) IPv6, configuración automática de direcciones IPv6, Cliente con estado DHCPv6

Para la marca Aruba se ha escogido el modelo 3810m 24g 1-slot switch (Figura 2.22) cuyas características principales se pueden ver en la Tabla 2.23.

Figura 2.22 Switch Aruba 3810m 24g 1-slot [74]

Tabla 2.23 Características switch de *Core* Aruba [74]

Aruba 3810m 24g 1-slot switch		
ARUBA –CORE		
PARÁMETROS	**DESCRIPCIÓN**	
Puertos	24 x 10/100/1000 Ethernet	
Capa	Capa 3	
Puertos SFP	No	
Puerto POE	No	
Apilable	Si	
Administrable	Si	ClearPass Policy Manager, Airwave y Soporte central
Familia	3810M	
Velocidad	10 GbE y 40 GbE	

2.2.4.1.2 Switch de distribución

En el modelo jerárquico se propone el uso de dos *switches* de distribución con interconexión al *switch* de núcleo y a los *switches* de acceso. Deberán soportar la configuración de VLAN ya que realizará la diferenciación del tráfico de datos con el de voz, con el fin de tener manejo eficiente del tráfico de la red (ver Tabla 2.24)

Para el cálculo de *backplane* del *switch* de distribución se considera que tendrá 16 puertos de cobre y 2 puertos de fibra (ver ecuación 2.3).

$$C_{backplane-distrib.=} N° \, de \, puertos \, X \, 2 \, X \, 1000 \, Mbps + puertos \, de \, fibra \;\; x \, 2 \, x \, 1000 Mbps \qquad (2.3)$$

$$C_{backplane-distrib\,=} \, 16 \, X \, 2 \, X \, 1000 Mbps + 2 \, x \, 2 \, x \, 1000 Mbps$$

$$C_{backplane-distrib\,=} \, 16 \, X \, 2 \, X \, 1000 Mbps + 2 \, x \, 2 \, x \, 1000 Mbps = 36000 \, Mbps$$

$$C_{backplane-distrib\,=} \, 36 \, Gbps$$

Tabla 2.24 Requerimientos necesarios para el switch de distribución

SWITCH DE DISTRIBUCIÓN	
PARÁMETROS	**CARACTERÍSTICAS MÍNIMAS**
Backplane	36 Gbps
Estándares	IEEE 802.1w
	IEEE 802.1q
	IEEE 802.1d
	IEEE 802.1x
	IEEE 802.1p
	IEEE 802.3d
	IEEE 802.3u
	IEEE 802.3af
	IEEE 802.3x
Puertos	16 puertos 10/100/1000 Mbps
Protocolos	IP
	IPv6
	OSPF
	RIPv2
	IGM
	BGP
	DHCP
Throughput	6 Mpps
Rendimiento	Alta capacidad de conmutación

En el diseño se han considerado las marcas Cisco y Aruba debido a su alta confiabilidad y disponibilidad, siendo estas marcas líderes en el cuadrante mágico de Gartner.

Para la marca Cisco se ha escogido el modelo SX550X-24F 24-Port 10G SFP+ *Stackable Managed Switch* (ver Figura 2.23) con las características de la Tabla 2.25.

Figura 2.23 Cisco SX550X-24F 24-Port 10G SFP [73]

Tabla 2.25 Características switch de distribución marca Cisco [73]

Cisco SX550X-24F 24-Port 10G SFP+ Stackable Managed Switch	
CISCO –DISTRIBUCIÓN	
PARÁMETROS	**DESCRIPCIÓN**
Puertos	24 x 10/100/1000
Capacidad de Conmutación	Capa 2 y 3
Enrutamiento	Capa 3
VLAN	Admite un máximo de 4094 VLAN activas simultáneas; VLAN basadas en puerto, en etiquetas 802.1Q y en MAC. VLAN de administración.
Autenticación	basada en la Web / IEEE 802.1X
Principales Estándares	IEEE 802.3 10BASE-T Ethernet, IEEE 802.3u 100BASE-TX Fast Ethernet, IEEE 802.3ab 1000BASE-T Gigabit Ethernet, IEEE 802.3ad Link Aggregation Control Protocol, IEEE 802.3z Gigabit Ethernet, IEEE 802.3ae 10 Gbit / s Ethernet sobre fibra para LAN, IEEE 802.3an 10GBase-T 10 Gbit / s Ethernet sobre cable de par trenzado de cobre, IEEE 802.3x Flow Control, IEEE 802.1Q / p VLAN, IEEE 802.1w Rapid STP, IEEE 802.1s Multiple STP, IEEE 802.1X Port Access Authentication, IEEE 802.3af, IEEE 802.3at, IEEE 802.1AB Link Layer Discovery Protocol, IEEE 802.3az Energy Efficient Ethernet.
IPv6	Modo de host IPv6 sobre Ethernet pila doble IPv6 / IPv4 Descubrimiento de enrutadores y vecinos (ND) IPv6, configuración automática de direcciones IPv6, Cliente con estado DHCPv6

Para la marca Aruba se ha escogido el modelo: Aruba 3810M 16SFP+ 2-slot (ver Figura 2.24) con características básicas detalladas en la Tabla 2.26.

Figura 2.24 Switch Aruba 3810M 16SFP+ 2-slot [74]

Tabla 2.26 Características switch de distribución marca Aruba [74]

Aruba 3810M 16SFP+ 2-slot		
ARUBA –DISTRIBUCIÓN		
PARÁMETROS	**DESCRIPCIÓN**	
Puertos	16 x 10/100/1000 Ethernet	
Capa	Capa 3	
Puertos SFP	SFP	
Puerto POE	No	
Apilable	Si	
Administrable	Si	ClearPass Policy Manager, AirWave y Soporte central
Familia	3810M	
Velocidad	10 GbE y 40 GbE	

La cantidad de *switches* de distribución necesarios en la Unidad Educativa se detallan en la Tabla 2.27 Switches de distribución.

Tabla 2.27 Switches de distribución

UBICACIÓN	CANTIDAD
BLOQUE 1	1
BLOQUE 2	0
BLOQUE 3	0
BLOQUE 4	1
TOTAL	**2**

2.2.4.1.3 Switch de acceso

En el diseño se ha determinado un total de 292 puntos de red que serán distribuidos en los 4 bloques de la Institución.

Los *switches* de acceso deberán soportar una capacidad de *backplane* considerando los números de puertos que serán utilizados. A continuación, se indica su cálculo, considerando una simultaneidad de 22 puertos de los 24 disponibles, ecuación 2.4.

$$C_{backplane} = N° \ de \ puertos \ X \ 100 \ Mbps \ x \ 2 \quad (2.4)$$

$$C_{backplane} = \{(22x100 \ Mbps) + (1 * 1000)\} \ x \ 2 = 6400 \ Mbps$$

$$= 6{,}4 \ Gbps$$

Tabla 2.28 Características de los *switches* de acceso

SWITCH DE ACCESO	
PARÁMETROS	**CARACTERÍSTICAS MÍNIMAS**
Backplane	6,4 Gbps
Estándares	IEEE 802.1w
	IEEE 802.1q
	IEEE 802.1d
	IEEE 802.1x
	IEEE 802.1p
	IEEE 802.3d
	IEEE 802.3u
	IEEE 802.3af
	IEEE 802.3x
Puertos	24/48 puertos 10/100/1000 Mbps
Capa OSI	3
Protocolos	RMON
	Telnet
	SNMP v1
	SNMP v2
	SNMP v3
Throughput	6 Mpps
Rendimiento	Alta capacidad de conmutación

En el diseño se han considerado las marcas Cisco y Aruba debido a su alta confiabilidad y disponibilidad.

Para la marca Cisco se han escogido los modelos CBS250 Smart de 48 puertos GE y CBS250 Smart de 24 puertos GE; sus características se muestran en la Tabla 2.29 y Tabla 2.30. (ver Figura 2.25 y Figura 2.26)

- **CBS250 Smart 48-port GE, PoE, 4x10G SFP+**

Figura 2.25 CBS250 Smart 48-port GE, PoE, 4x10G SFP+ [75]

Tabla 2.29 Características de switch de acceso CBS250 Smart 48-port GE, PoE, 4x10G SFP+ [75]

CBS250 Smart 48-port GE, PoE, 4x10G SFP+	
CISCO –ACCESO	
PARÁMETROS	**DESCRIPCIÓN**
Puertos	48 x 10/100/1000
Capacidad de Conmutación	Capa 2
Enrutamiento	Capa 3
VLAN	255 VLAN simultáneamente
Autenticación	IEEE 802.1X
Estándares	IEEE 802.3 10BASE-T Ethernet, IEEE 802.3u 100BASE-TX Fast Ethernet, IEEE 802.3ab 1000BASE-T Gigabit Ethernet, IEEE 802.3ad Link Aggregation Control Protocol, IEEE 802.3z Gigabit Ethernet, IEEE 802.3x Flow Control, IEEE 802.3 ad LACP, IEEE 802.1D (STP), IEEE 802.1Q / p VLAN, IEEE 802.1w RSTP, IEEE 802.1s STP múltiple, Autenticación de acceso al puerto IEEE 802.1X, IEEE 802.3af, IEEE 802.3at,
IPv6	Modo de host IPv6 IPv6 sobre Ethernet Pila doble de IPv6 / IPv4 Descubrimiento de vecinos IPv6 (ND) Configuración automática de direcciones sin estado IPv6 Descubrimiento de la unidad de transmisión máxima de ruta (MTU) Detección de direcciones duplicadas (DAD) Protocolo de mensajes de control de Internet (ICMP) versión 6 IPv6 sobre red IPv4 con compatibilidad con el protocolo de direccionamiento automático de túnel dentro del sitio (ISATAP) Certificación USGv6 e IPv6 Gold Logo

- **CBS250 Smart 24-port GE, PoE, 4x10G SFP**

Figura 2.26 CBS250 Smart 24-port GE, PoE, 4x10G SFP [75]

Tabla 2.30 Características de switch de acceso CBS250 Smart 24-port GE, PoE, 4x10G SFP [75]

CBS250 Smart 24-port GE, PoE, 4x10G SFP	
CISCO –ACCESO	
PARÁMETROS	**DESCRIPCIÓN**
Puertos	24 x 10/100/1000
Capacidad de Conmutación	Capa 2
Enrutamiento	Capa 3
VLAN	255 VLAN simultáneamente
Autenticación	IEEE 802.1X
Estándares	IEEE 802.3 10BASE-T Ethernet, IEEE 802.3u 100BASE-TX Fast Ethernet, IEEE 802.3ab 1000BASE-T Gigabit Ethernet, IEEE 802.3ad Link Aggregation Control Protocol, IEEE 802.3z Gigabit Ethernet, IEEE 802.3x Flow Control, IEEE 802.3 ad LACP, IEEE 802.1D (STP), IEEE 802.1Q / p VLAN, IEEE 802.1w RSTP, IEEE 802.1s STP múltiple, Autenticación de acceso al puerto IEEE 802.1X, IEEE 802.3af, IEEE 802.3at.
IPv6	Modo de host IPv6 IPv6 sobre Ethernet Pila doble de IPv6 / IPv4 Descubrimiento de vecinos IPv6 (ND) Configuración automática de direcciones sin estado IPv6 Descubrimiento de la unidad de transmisión máxima de ruta (MTU) Detección de direcciones duplicadas (DAD) Protocolo de mensajes de control de Internet (ICMP) versión 6 IPv6 sobre red IPv4 con compatibilidad con el protocolo de direccionamiento automático de túnel dentro del sitio (ISATAP) Certificación USGv6 e IPv6 Gold Logo

Para la marca Aruba se ha escogido los modelos Aruba Instant On 1930 48G y Aruba Instant On 1930 24G; sus características se muestran en las Tablas 2.31 y 2.32 respectivamente. (Ver Figura 2.27 y Figura 2.28).

- **Aruba Instant On 1930 48G 4SFP+ 370W**

Figura 2.27 Aruba Instant On 48-port [77]

Tabla 2.31 Características de switch de acceso Aruba Instant On 1930 48G 4SFP+ 370W [77]

Aruba Instant On 1930 48G 4SFP+ 370W		
ARUBA -ACCESO		
PARÁMETROS	**DESCRIPCIÓN**	
Puertos	48 x 10/100/1000 Ethernet	
Capa	Capa 2	
Puertos SFP	SFP	
Puerto POE	PoE	
Apilable	No	
Administrable	Si	IEEE 802.1X – VLAN
Familia	1930	

- **Aruba Instant On 1930 24G 4SFP+ 370W**

Figura 2.28 Switch Aruba Instant On 1930 24G 4SFP+ 370W [76]

Tabla 2.32 Características de switch de acceso Aruba Instant On 1930 24G 4SFP+ 370W [76]

Aruba Instant On 1930 24G 4SFP+ 370W		
ARUBA -ACCESO		
PARÁMETROS	DESCRIPCIÓN	
Puertos	24 x 10/100/1000 Ethernet	
Capa	Capa 2	
Puertos SFP	SFP	
Puerto POE	PoE	
Apilable	No	
Administrable	Si	IEEE 802.1X – VLAN
Familia	1930	

La cantidad de *switches* de Acceso, necesarios en cada uno de los bloques, se presenta en la Tabla 2.33.

Tabla 2.33 Switches en bloques administrativos y educativos

UBICACIÓN	CANTIDAD	N° DE USUARIOS
BLOQUE 1	5	110
BLOQUE 2	1	12
BLOQUE 3	1	15
BLOQUE 4	5	155
TOTAL	**12**	**292**

Tabla 2.34 Puertos utilizados y libres en *switches* de acceso

UBICACIÓN	N° DE PUERTOS	N° DE USUARIOS	N° PUERTOS DISPONIBLES
BLOQUE 1	240	110	130
BLOQUE 2	24	12	12
BLOQUE 3	48	15	33
BLOQUE 4	240	155	85
TOTAL	**552**	**292**	**260**

En la Tabla 2.34 se detallan los puertos a utilizar en los *switches* de acceso y aquellos que se encontrarán disponibles para una posible expansión.

2.2.4.2 Red Inalámbrica

Como se pudo observar en el apartado de la situación actual, en la Unidad Educativa "FESVIP", no se ha considerado una red diseñada a nivel LAN, mucho menos a nivel WLAN. Por ello es necesario realizar como mínimo un *site survey* predictivo, para que, en base a este, se puedan ubicar y determinar los *Access Point* necesarios.

Se toma en consideración también que se crearán SSID para servicios y que se tendrá a un *Access Point* para administrar centralizadamente todos los equipos.

2.2.4.2.1 Site Survey Predictivo

Para el diseño se realizó un s*ite survey* predictivo de todas las áreas de la institución, el cual permitió determinar la cantidad de *Access Point* necesarios según el área de cobertura. Para el análisis se utilizó el portal de administración de Aruba Networks, con una cuenta de *partner* dentro del portal (ver Figura 2.29) para poder generar el *site survey* predictivo de una manera fácil y rápida en base a los planos de la institución, esto se lo realizó área por área en toda la Unidad Educativa. (ver Figura 2.30)

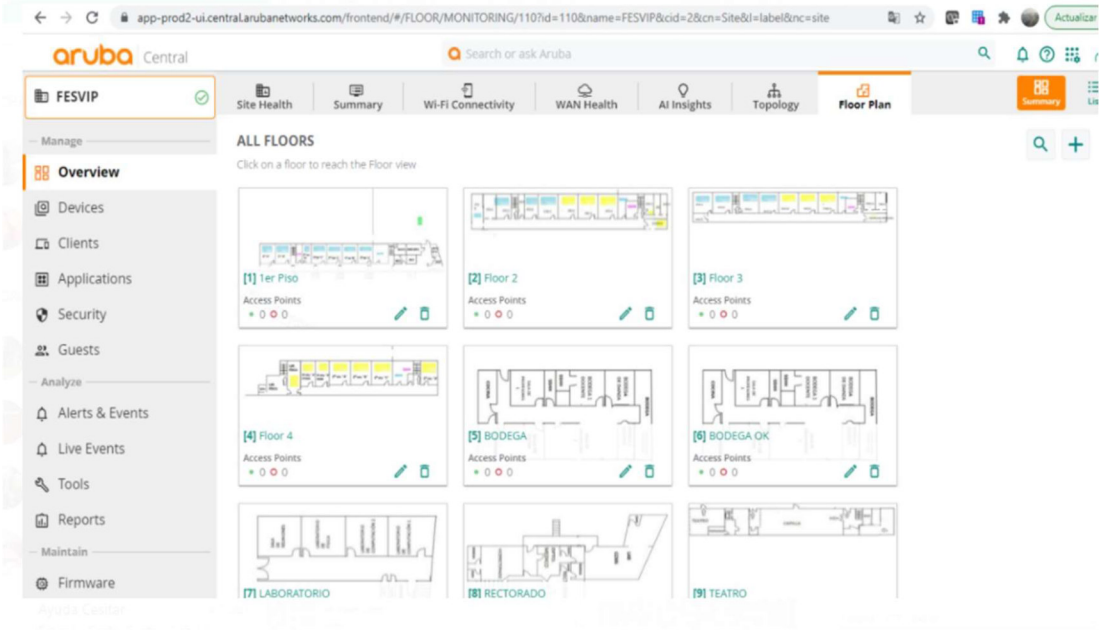


Figura 2.29 Portal Aruba Networks

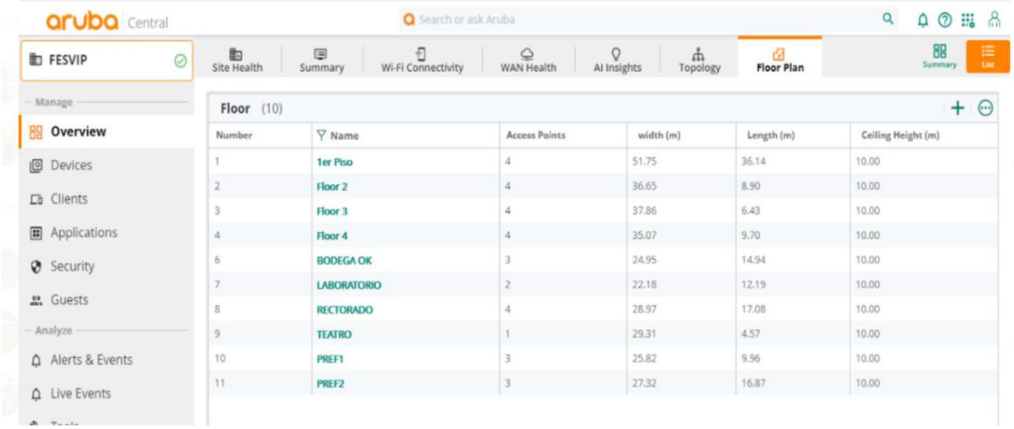


Figura 2.30 Site survey por áreas

En el diseño se debe tomar en cuenta que no exista interferencia entre las redes inalámbricas. Por tal motivo en la Tabla 2.35. se muestran los lugares donde se ubicarán los *Access Point* y el área a cubrir en base al *site survey* realizado.

Tabla 2.35 Distribución de AP

CANTIDAD	DESCRIPCIÓN	UBICACIÓN	LUGAR	ÁREA QUE CUBRIR
4	AP-FEB01-1	BLOQUE 1	Planta baja	Aulas y oficinas
4	AP-FEB01-2		Primer piso	Aulas y oficinas
4	AP-FEB01-3		Segundo piso	Aulas y oficinas
4	AP-FEB01-4		Tercer piso	Aulas y oficinas
1	AP-FEB01-5		Teatro	Teatro
2	AP-FEB02-1	BLOQUE 2	Aula Prefabricada Inicial	Aulas inicial y preparatoria
1	AP-FEB03-1	BLOQUE 3	Bodega	Bodega materiales y EEFF
1	AP-FEB03-2		Aulas Prefabricadas 1	Aulas Bachillerato
1	AP-FEB03-3		Aulas Prefabricadas 4	Aulas Bachillerato
1	AP-FEB03-4		Bar	Bar estudiantil
1	AP-FEB12	BLOQUE 4	Laboratorio de Química	Laboratorio y Coordinación
1	AP-FEB13		Rectorado	Rectorado y Colecturía
1	AP-FEB14		Secretaría	Secretaría
1	AP-FEB15		Vicerrectorado	Vicerrectorado y recepción
1	AP-FEB16		Sala de Profesores colegio	Sala de profesores y de planificación
1	AP-FEB17		Comedor	Comedor y cocina
1	AP-FEB18		Bodegas	Bodega de materiales e insumos
2	AP-FEB18		Laboratorios	Laboratorio de Computación y Física

TOTAL, AP FESVIP	32

2.2.4.2.2 Áreas de cobertura

En base a los diagramas de construcción de la Unidad Educativa “FESVIP” y mediante *site survey* predictivo se pudo determinar la cantidad de *Access Point* a utilizar.

En el **ANEXO E** se muestran todos los mapas de calor generados por área; en la Figura 2.31 se puede observar un ejemplo de lo realizado.

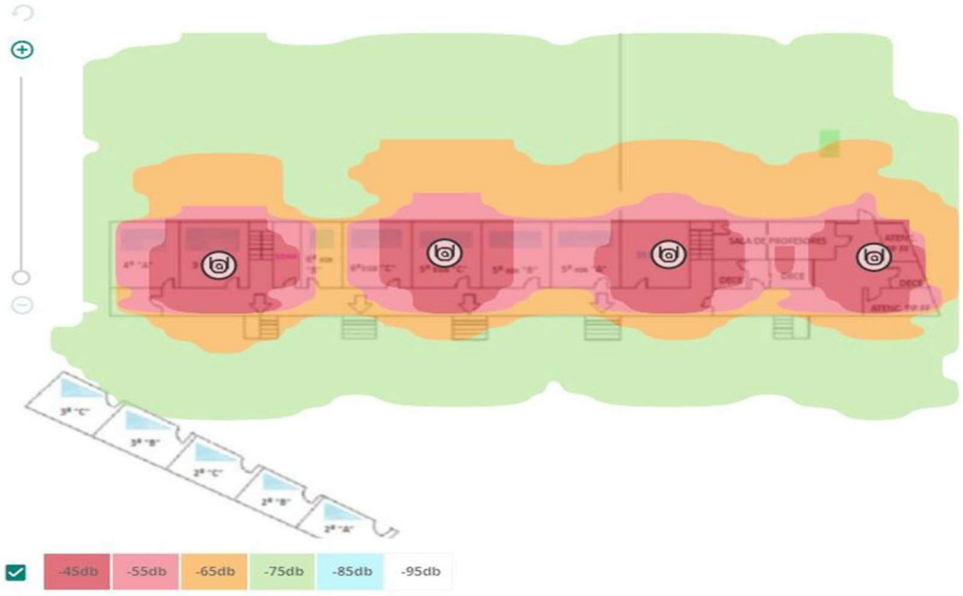


Figura 2.31 *Access Point* planta baja del bloque 1

2.2.4.2.3 Integración con la LAN cableada

Los *Access Point* deben estar conectados directamente a puntos exclusivos de red, los cuales estarán dimensionados en el *switch* de acceso.

La alimentación eléctrica empleada a los equipos no será considerada, debido a que es recomendable el uso de equipos que admiten energía a través de Ethernet PoE *(Power over Ethernet*), estándar 802.3af.

Tabla 2.36 SSID para los AP

SSID	DESCRIPCIÓN
W_ADM	Conexión de personal administrativo
W_DOC	Conexión de personal docente
W_EST	Conexión de estudiantes
W_INV	Conexión de invitados

2.2.4.2.4 SSID (Service Set Identifier)

SSID o identificadores de red inalámbrica permitirán reconocer de manera sencilla los AP dentro de la Institución, por lo que se planea emplear cuatro SSID de acceso a la red inalámbrica en base a su estructura organizacional institucional. Se establecerá una red acorde a las necesidades y de fácil acceso para la conexión de dispositivos portátiles y móviles.

En los diferentes puntos de acceso se colocarán los SSID descritos en la Tabla 2.36 SSID para los , de acuerdo con lo mencionado anteriormente.

2.2.4.2.5 Seguridad en la red inalámbrica

La seguridad en los puntos de acceso es muy importante, debido a que, al transmitir la información de forma inalámbrica, esta se vuelve más vulnerable y fácil de ser interceptada por usuarios maliciosos; es por ello, que se sugiere protegerlos a través de contraseñas sugeridas por organismos internacionales de seguridad.

Las claves de acceso a la red y a la configuración de los dispositivos deben ser diferentes, para que solo el personal encargado de la administración pueda realizar configuraciones. Estas contraseñas deben cumplir con ciertos parámetros como letras mayúsculas, minúsculas, números; esta misma estructura deberán poseer las claves de acceso a la red inalámbrica.

Existen diferentes métodos de seguridad basados en el esquema WPA2 (*Wi-Fi Protected Access 2*) que corrige las deficiencias de estándar 802.11i, evita el acceso no autorizado a la red inalámbrica y permite el cifrado de los datos enviados a través de la red. Funciona con clave compartida y algoritmos TKIP basados en AES (*Advanced Encription Standard*).

2.2.4.2.6 Selección de access point

Para el diseño de la red se establecen características principales de los *Access Point*, las cuales están descritas en la Tabla 2.37.

Tabla 2.37 Características mínimas de los AP

ACCESS POINT	
PARÁMETROS	**CARACTERÍSTICAS MÍNIMAS**
Estándares y protocolos	IEEE 802.11 a, b, g, n
	IEEE 802.11x
	IEEE 802.11n
	IEEE 802.1p
	IEEE 802.1q
	IEEE 802.3af
	IEEE 802.3u
Administración	GUI; SNMP; HTTP
Mecanismos de Encriptación	WPA, WPA2, TKIP
Interfaces	Ethernet RJ45

Velocidad de transmisión	54 Mbps

En el diseño se ha considerado para los *Access Point* dos tipos de marcas, Cisco y Aruba, debido a su alta confiabilidad y disponibilidad.

Para la marca Cisco se ha escogido el modelo Cisco Aironet Mobility Express 2800 series (ver Figura 2.32), cuyas características se describen en la Tabla 2.38.

Tabla 2.38 Características *access point* Cisco [78]

Cisco Aironet Mobility Express 2800 series	
CISCO - ACCESS POINT	
PARÁMETROS	**DESCRIPCIÓN**
Puertos	2x detección automática 100/1000 BASE-T (RJ-45)
Estándar	IEEE 802.11a / b / g, 802.11n, 802.11h, 802.11d, IEEE 802.11ac
Seguridad	802.11i, acceso protegido Wi-Fi 3 (WPA3), WPA2, WPA,802.1X
Compatibilidad con 802.11ac Wave 2	Tasa de conexión teórica de hasta 2.6 Gbps por radio, aproximadamente el doble de las tasas que ofrecen los puntos de acceso 802.11ac de alta gama de hoy en día.
Software	Versión de software de red inalámbrica unificada de Cisco 8.2.111.0 o posterior
	Cisco IOS ® XE Software Release 16.3

Figura 2.32 AP Cisco [78]

Para la marca Aruba se ha escogido el modelo Aruba AP-515 (RW) Unified AP (ver Figura 2.33), con características indicadas en la Tabla 2.39 Características access point Aruba.

Tabla 2.39 Características *access point* Aruba [79]

Aruba AP-515 (RW) Unified AP	
ARUBA- ACCESS POINT	
PARÁMETROS	**DESCRIPCIÓN**
Puertos	100/1000/2500BASE-T y MDI/MDX
Estándar	801.11ax
Seguridad	WPA, WPA2 y WPA3
Tipos de modulación compatibles	802.11b: - 802.11a/g/n: - 802.11ac - 802.11ax
Software	ArubaOS y Aruba InstantOS 8.4.0.0

Figura 2.33 AP Aruba [79]

2.2.5 SEGURIDAD PERIMETRAL

2.2.5.1 *Firewall*

Los *firewalls* son de tipo *hardware* o *software* que examinan y protegen la información que va o viene a través del Internet. En el diseño se ha tomado en cuenta un *firewall* físico cuya función será proteger y prevenir a la red de la Unidad Educativa de intrusiones o ataques.

Para este proyecto se han considerado dos marcas líderes en el mercado Checkpoint (ver Figura 2.34) y Fortinet (ver Figura 2.35). En la Tabla 2.40 y en la Tabla 2.41, se detallan las características de cada uno de estos *firewalls*.

2.2.5.1.1 Checkpoint

Figura 2.34 Checkpoint Quantum 6600 [80]

Tabla 2.40 Características Checkpoint Quantum 6600 [80]

PARÁMETROS	DESCRIPCIÓN
Prevención de amenazas Gbps	3.7
NGFW Gbps	6.2
IPS Gbps	10.14
Firewall Gbps	18
Conexiones/segundo Gbps	116
Conexiones concurrentes Gbps	2/4/8M
Seguridad de contenido	Se integra con Microsoft AD, LDAP, RADIUS, Cisco pxGrid, Terminal Server y con terceros a través de una API Web
	Cumple una política coherente para los usuarios locales y remotos en Windows, Plataformas macOS, Linux, Android y Apple iOS.
IPv6	NAT66, NAT64, NAT46
	CorelXL, SecureXL, HA con VRRPv3
Enrutamiento	OSPFv2 y V3 BGP, RIP
	Rutas estáticas y multidifusión
	Enrutamiento basado en políticas

2.2.5.1.2 Fortinet

Figura 2.35 Fortigate 900D [81]

Tabla 2.41 Características Fortigate 900 D [81]

PARÁMETROS	DESCRIPCIÓN
Prevención de amenazas Gbps	3
NGFW Gbps	4
IPS Gbps	4.2
Firewall políticas	10.000
Interfaces de red	Multiple GE RJ45, GE SFP y 10 GE SFP+slots
Sesiones concurrentes TCP	11 millones
Nuevas sesiones/segundos TCP	280.000
IPsec VPN Gbps	25
Gateway a Gateway IPsec VPN	2.000
Client a Gateway IPsec VPN	50.000
SSL-VPN Throughput Gbps	3.6
Virtual/domains (default/maximun)	10/10
Número máximo de FortiSwitches	64
Número máximo de FortiAP	1042/512

2.2.6 SERVICIOS ADICIONALES

2.2.6.1 Servicio de directorio activo (AD)

El servicio de directorio activo es una estructura jerárquica que permite almacenar, organizar y administrar de manera centralizada el acceso a objetos como recursos, permisos, servicios y usuarios en la red. Además, administra los inicios de sesión de los equipos enlazados mediante autenticación, así como el acceso a recursos e información mediante políticas aplicadas a las cuentas de usuario o grupos en las que se definen sus restricciones, atribuciones o permisos.

En la unidad Educativa “FESVIP” es de vital importancia, sobre todo para el personal administrativo y docente, el poder tener un servicio de directorio activo, que permitirá el control de usuarios y equipos conectados a la red de la Institución, evitando puntos de vulnerabilidad ya sea por instalación de aplicaciones no necesarias o vulnerabilidad a nivel de sistema operativo. Se estandarizarán las aplicaciones base del personal y se enviarán políticas de restricción y/o configuración acordes a la institución.

Las unidades organizativas, OU por sus siglas en inglés, estarán establecidas en base al organigrama institucional, es decir, dentro del dominio “FESVIP” existirán OU con los nombres de los usuarios en base a lo anteriormente mencionado; así mismo los equipos y servidores tendrán su respectiva OU para poder ser almacenados de mejor manera y

tener claridad del equipo que pertenece a cada persona para un mejor control de los activos TIC.

2.2.6.2 Servicio DNS

El Sistema de Nombres de Dominio (DNS) es el encargado de estructurar de manera jerárquica a los dispositivos dentro de un dominio asignándoles un nombre; si se tiene un AD es necesario tener un servicio de DNS.

El servicio DNS es capaz de traducir nombres dentro de la red a direcciones IP y viceversa, lo cual permitirá identificar de manera sencilla el nombre del equipo; en este caso la Unidad Educativa “FESVIP” debería utilizar un dominio acorde a su categoría, es decir, con terminación edu.ec. Actualmente la institución mantiene el dominio fesvip.edu.ec, debido a que posee una página Web, pero no se tiene control del dominio público, por lo que es necesario recuperar los accesos para que ese dominio no se pierda; a nivel interno con el servidor DNS se podrán crear registros de cualquier tipo, y se tendrá una administración detallada.

Este servicio puede “correr” en el mismo servidor que un directorio activo, por lo que en el diseño se lo considera de esa manera, para el cálculo de los recursos necesarios.

2.2.6.3 Servicio DHCP

El servicio de Protocolo de Configuración Dinámica de Host permite asignar direcciones IP de manera dinámica, a los dispositivos conectados a la red cableada e inalámbrica; con esto se podrá:

- Evitar conflictos de direcciones IP duplicadas y llevar un orden acertado en la asignación de estas.
- Reutilizar direcciones que ya no estén siendo utilizadas, pero serán asignadas a dispositivos que no pertenecen a la red habitual o que no requieren de una dirección de forma constante.
- Se podrán reservar direcciones IP para diferentes elementos o dispositivos que por alguna razón necesiten tener una dirección IP asociada a su dirección MAC.

En la Unidad Educativa “FESVIP” el servicio de DHCP será diseñado en el mismo servidor que el AD y DNS, considerando los recursos necesarios para que estos servicios coexistan.

Se pretende diseñar los *pools* de direccionamiento IP necesario para todos los segmentos que utilicen asignación dinámica de dirección IP, como por ejemplo para las redes de administrativo, docente, estudiantes, entre otras y se considerará un tiempo de reserva de IP de 8 días.

2.2.6.4 Servicio FTP

El servidor de transferencia de archivos en la Unidad Educativa "FESVIP" contará con el servicio que permita a sus miembros (estudiantes, profesores, personal administrativo) descargar, almacenar y compartir información dentro de su red interna.

Permitirá tener información almacenada como formularios, solicitudes, circulares, oficios, informes, entre otra información valiosa para los miembros de la institución y que al momento se las tiene en diferentes repositorios e incluso desordenados. El servicio de FTP permitirá tener una organización adecuada de toda la documentación de la institución, sin olvidarse de las seguridades que deberá tener cada carpeta.

Para el diseño de estos servicios adicionales se deberá tomar en cuenta las características necesarias para soportar esta funcionalidad. Los servicios de AD, DNS y DHCP se alojarán en un mismo servidor; en la actualidad los más utilizados y fáciles de implementar son los que corren en el sistema operativo Windows server. De igual manera el servicio de FTP, por su funcionalidad será implementado en otro servidor Windows.

Por facilidad de administración se considerará un ambiente virtual, donde se instalarán estos servicios en los diferentes servidores virtuales.

En la Tabla 2.42 se pueden observar las características mínimas de un servidor *windows* que permite alojar estos servicios.

Tabla 2.42 Características mínimas de un servidor *windows* y sus servicios adicionales

SERVIDOR	PROCESADOR	MEMORIA RAM	STORAGE
Windows Server 2019	Mínimo 2vCPU	2 GB Desktop Experience	32GB
Active Directory	Mínimo 4vCPU	Mínimo 8 GB	100 GB
DNS and DC	Mínimo 4vCPU	Mínimo 4 GB	60 GB
DHCP	Mínimo 4vCPU	Mínimo 4 GB	60 GB
FTP	Mínimo 4vCPU	Mínimo 8 GB	200 GB

Para alojar los servicios AD, DNS y DHCP en el diseño se presenta en la Tabla 2.43. los requerimientos recomendables.

Tabla 2.43 Características recomendables del servidor donde se alojarán los servicios AD, DNS y DHCP

SERVIDOR	PROCESADOR	MEMORIA RAM	STORAGE
Windows Server 2019	Mínimo 8vCPU - Recomendable 16 vCPU	Recomendable 16 GB	Recomendable >150 GB

Las características recomendables del servidor virtual para alojar los servicios FTP en el diseño se muestran en la Tabla 2.44.

Tabla 2.44 Características recomendables del servidor donde se alojarán los servicios FTP

SERVIDOR	PROCESADOR	MEMORIA RAM	STORAGE
Windows Server 2019	Recomendado 8vCPU	Recomendable 8 GB	Recomendable 250 GB

Se debe considerar que se plantea el diseño sobre un ambiente virtualizado, por lo que se necesita para estos servicios únicamente licenciamiento *windows*.

Posteriormente se realizará el dimensionamiento del servidor físico que alojará todos estos servicios virtualizados; para esto se han considerado dos marcas que se detallan con las características físicas necesarias en la Tabla 2.45 para un servidor de marca Dell y en la Tabla 2.46 para un servidor de marca HPE

Tabla 2.45 Servidor rack DELL PowerEdge

DELL SERVIDOR RACK PowerEdge R640:
CARACTERÍSTICAS
- 1 x Procesador Intel Xeon-Silver 4210R 10-Core (2.40GHz)
- 4 x Módulos de memoria 32GB 2Rx4 PC4-2933Y-R Smart Kit
- 8 Bahías para discos Hot Plug 2.5in Small Form Factor
- 3 x discos 960GB SATA MU SFF SC MV SSD
- 1 x Controladora de discos Smart Array P408i-a SR Gen10 SAS
- 1 x Tarjeta de red Ethernet 1Gb 4-port 366FLR
- 2 x Fuente de poder 500W Flex Slot Platinum Hot Plug Low Halogen
- HPE 3Y TC Ess DL360 Gen10 SVC
- VMw vSphere Std 1P 3yr E-LTU

Tabla 2.46 Servidor rack HPE DL360

SERVIDOR HPE DL360 Gen10 8SFF
CARACTERÍSTICAS
- 1 x Procesador Intel Xeon-Silver 4210R 10-Core (2.40GHz)
- 4 x Módulos de memoria 32GB 2Rx4 PC4-2933Y-R Smart Kit
- 8 Bahías para discos Hot Plug 2.5in Small Form Factor
- 3 x discos 960GB SATA MU SFF SC MV SSD
- 1 x Controladora de discos Smart Array P408i-a SR Gen10 SAS
- 1 x Tarjeta de red Ethernet 1Gb 4-port 366FLR
- 2 x Fuente de poder 500W Flex Slot Platinum Hot Plug Low Halogen
- HPE 3Y TC Ess DL360 Gen10 SVC
- VMw vSphere Std 1P 3yr E-LTU

Se debe considerar adicionalmente en los servidores el licenciamiento VMware ya que se realizarán ambientes virtualizados. Por tal motivo en el estudio de costos se incluirá el costo de esta licencia.

2.2.7 SERVIDOR DE CORREO ELECTRÓNICO

El servidor de correo electrónico será el encargado de manejar los mensajes de correo internos y externos de la Unidad Educativa “FESVIP” utilizando software especializado con características que permitan utilizar esta funcionalidad dentro de la institución. Sus características más importantes son:

- Protocolo SMTP (*Simple Mail Transfer Protocol*), transmisión de correo electrónico de manera plana o encriptada sobre TSL (*Transport Layer Security*) o SSL (*Secure Socket Layer*), IMAP o POP3 para la recepción
- Seguridad: certificado SSL, asegura la información encriptada que va del equipo al servidor de correo.
- Soporte para clientes
- Configuración en dispositivos móviles
- Cooperación: Calendario, contactos, tareas, compartir documentos en la nube y comunicación
- Capacidad suficiente: depende del flujo y cantidad de correos electrónicos, existen servidores que ofrecen desde 5 a 50 GB de almacenamiento.

- Alta disponibilidad: el servicio de correo debe estar disponible 24/7/365 garantizando una actividad del 99.9%.
- Mantenimiento y respaldos: los respaldos se deben realizar una vez al día y depende de las necesidades institucionales.

La institución necesitará un correo electrónico con el dominio fesvip.edu.ec para cada uno de los miembros que conforma la institución, es decir, para el personal administrativo, docente, apoyo y estudiantes (ver Tabla 2.47).

Tabla 2.47 Número de correos electrónicos para la comunidad FESVIP

POBLACIÓN	N° TOTAL DE CORREOS ELECTRÓNICOS
Autoridades	3
Personal Administrativo	14
Personal Docente	42
Personal de Apoyo	5
Estudiantes	936
TOTAL	**1000**

Para el diseño se propone utilizar un servidor de correo electrónico tomando sus características y costos de servicio e implementación. Se han tomado en cuenta los servidores comúnmente utilizados como son: Zimbra, Exchange Server de Microsoft y Office 365, cabe mencionar que para Microsoft 365 existe un plan llamado Microsoft 365 Educación el cual brinda a los educadores la mejor experiencia para promover su trabajo; cuando se adquiere este tipo de solución se obtienen accesos sin costo adicional para los estudiantes. Existen varios planes de Microsoft 365 educación que pueden ser implementados [62], en la Tabla 2.48 se muestra el detalle.

Tabla 2.48 Planes Microsoft Office 365 Educación [62]

MICROSOFT 365	CARACTERÍSTICAS
A1	Versión gratuita en línea Simple de implementar y permite trabajar con aplicaciones de escritorio como: Word, Excel Power point, Microsoft Teams, entre otros
A3	Acceso a las aplicaciones de escritorio de Office. Características adicionales reservas y eventos en vivo. Análisis, seguridad y administración avanzados.
A5	Todas las aplicaciones de Office en el escritorio. Funciones de enseñanza y aprendizaje 365 A3. Administración, movilidad y seguridad Microsoft defender.

Zimbra es un servidor de correo electrónico que utiliza lenguaje AJAX (JavaScript + XML, al igual que Gmail. Es una versión libre, incluye una versión comercial que es Zimbra Network en la cual se añaden funcionalidades, servicios con enfoque profesional y ofrece una arquitectura abierta y estándar [63]. Entre las ventajas de implementar Zimbra se tienen:

- Bajo costo de gestión
- Sistema de almacenamiento nativo
- Soporte multidominio con administración desde un único nodo.
- Solución de alta disponibilidad integrada
- Compatible con antivirus/antispam.
- Interfaz de administración basado en AJAX

Microsoft Exchange Server es una cuenta de correo electrónico a nivel profesional o educativa, trabaja con IMAP, POP3, SMTP. Tiene funcionalidades como: acceso al correo electrónico desde un computador, teléfono o T*ablet*, permite que bandeja de entrada, elementos enviados y eliminados se sincronicen entre el dispositivo y el servidor [64].

Se consideran estas tres opciones de servidor las cuales pueden ser implementadas en la institución ya que cumplen con las funciones necesarias para realizar los procesos institucionales. En el presupuesto referencial se verificará cada una de estas opciones para la toma de decisión.

2.2.8 TELEFONÍA IP

La telefonía IP dentro de la Unidad Educativa se encargará de brindar servicios como: llamadas internas y externas, monitoreo, grabaciones, identificación de usuarios y generar extensiones internas. Para el cumplimiento de estas funciones principales el servidor de telefonía deberá tener las siguientes características:

- Calidad de servicio QoS: asignando prioridades a paquetes transmitidos por la red IP.
- Integración: con servicios de telecomunicaciones como datos, voz, video e Internet.
- Compatibilidad: con hardware de distintos fabricantes.

- Seguridad: autenticación, autorización y protección de datos.

La Unidad Educativa necesita que su personal administrativo y docente tenga una extensión, por lo que se asignará una extensión a cada uno de los usuarios, que tendrá cuatro dígitos empezado por el 1. A manera de ejemplo en Tabla 2.49 se indica la asignación de extensiones para las autoridades de la institución.

Tabla 2.49 Ejemplo de asignación de extensiones a las autoridades de "FESVIP"

NOMBRE Y APELLIDO	DEPARTAMENTO	EXTENSIÓN
Edison Ponce	Rectorado	1001
Gabriela Quintero	Vicerrectorado	1002
Geovanna Guevara	Inspección General	1003

El número de extensiones que se deberán generar en la institución para todo el personal es de 65 con un crecimiento de hasta 100 licencias. Adicionalmente la central telefónica deberá tener como mínimo 2 puertos FXO (*Foreign Exchange Office*) para la conexión de líneas analógicas de la PSTN.

En telefonía IP existen varias marcas en el mercado que cumplen con las características requeridas por la Unidad Educativa. Se detallan dos marcas que cumplen con las funcionalidades requeridas.

Se ha considerado la central telefónica IP Grandstream UCM6304 (ver Figura 2.36), cuyas principales características se detallan en la Tabla 2.50.

Figura 2.36 Central telefónica IP Grandstream

Tabla 2.50 Central telefónica IP Grandstream [65]

CARACTERÍSTICAS	UCM6304	
Puertos FXS para Teléfono Analógico	4 RJ11	
Puertos FXO para Línea PSTN	4 RJ11	
Interfaces de Red	Tres puertos Gigabit auto adaptativos (conmutados, enrutados o en modo de tarjeta dual) con PoE+	
Sistema Operativo de Telefonía	Basado en Asterisk versión 16	
Fuente de Alimentación Universal	Entrada: 100 ~ 240VAC, 50/60Hz; Salida: DC 12V, 1.5A	2 Conectores de alimentación DC 12V
		Entrada: 100 ~ 240VAC, 50/60Hz; Salida: DC 12V, 2A
Montaje	Montaje en rack y escritorio	
Identificador de Llamadas	Bellcore/Telcordia, ETSI-FSK, ETSI-DTMF, SIN 227 – BT, NTT	
Call Center	Múltiples colas de llamadas configurables, distribución automática de llamadas (ACD) basada en las habilidades, la disponibilidad y la carga de trabajo de los agentes, anuncio de espera	
Asistente Automático Personalizable	Hasta 5 capas de IVR (*Interactive Voice Response*) en múltiples idiomas	
Capacidad Máxima de Llamadas	Usuarios: 2000	
	Llamadas simultáneas (G.711): 300	
	Cantidad máxima de llamadas SRTP simultáneas (G.711): 200	
Cantidad Máxima de Asistentes de Puentes de Conferencia	4 salas de videoconferencia y hasta 40 participantes con 1080p, asumiendo 4 secuencias de video + 1 pantalla compartida (H.264 y G.711)	
	Conferencia de voz: Hasta 200 participantes	
Aplicación Wave	Permite a los usuarios de Android y iOS unirse a reuniones organizadas por UCM y comunicarse con otros usuarios	
	Soluciones registradas en la serie UCM6300	

Para la central telefónica IP también se ha considerado en este diseño la Cisco Unified Communications Manager (CUCM) en su versión 12.5, considerada una de las mejores en el mercado.

En la Tabla 2.51 se detallan las principales características.

Tabla 2.51 Central telefónica IP Cisco [66].

CARACTERÍSTICAS	VERSION 12.5 UCM
Actualización simple	Comprobaciones automáticas previas para la actualización 10x, 11x, 12x a 12.5
Gestión de archivos de configuración Jabber	Administración de forma centralizada
Licencia inteligente: modo BE6000	Licencias del paquete de inicio modo UCL, UWL
Adición rápida de dispositivos y mejora de la plantilla de dispositivo unificado	Permite la creación de un dispositivo no vinculado a un usuario (teléfono de sala de conferencias)
CMR para llamadas de troncales SIP	Escritura de métricas de calidad de voz en CUCM Call Management Records (CMR) para llamadas troncales SIP que terminan en Cisco Unified Border Element (CUBE) o Cisco IOS Gateways.
Nube conectada	Ofrecen un modelo de suscripción flexible, alojado y operado por Cisco en América del Norte, Europa, la región de Asia Pacífico y Japón. Soluciones de voz, video, mensajería, reuniones y movilidad con las características y beneficios de los teléfonos IP, dispositivos móviles y clientes de escritorio de Cisco.

2.2.9 VIDEOCONFERENCIA

Como se evidencia en la situación actual la Unidad Educativa “FESVP” no cuenta con un sistema de videoconferencia. Por esta razón es necesario considerar en su diseño un sistema que de esta funcionalidad; en el mercado existen un sinnúmero de soluciones, pero se han escogido tres de las más importantes.

2.2.9.1 Microsoft Teams - Office 365

Es una plataforma colaborativa que se encuentra en la nube de Microsoft que cuenta con diferentes aplicaciones y servicios; permite desde generar documentos y compartirlos en OneDrive, hasta modificarlos de formar colaborativa.

El uso de esta plataforma no es complicado y se puede acceder desde una PC o dispositivo móvil, se debe también crear una cuenta Microsoft (Outlook /Hotmail). Tras el inicio de sesión en la plataforma se pueden crear salas de *chat* y videoconferencia; permite también adicionar a más personas al entorno [67].

Esta plataforma tiene ventajas como:

- Vincula cuenta de usuario con varios dispositivos

- Videoconferencias y llamadas de voz.
- Añade aplicaciones de terceros a su plataforma como: Twitter, Trello, Yammer y RSS.

En el diseño de correo electrónico se ha propuesto trabajar con Office 365 que se encuentra vinculado con Microsoft Teams, por lo que al adquirir este licenciamiento será posible trabajar con esta plataforma de Videoconferencia.

2.2.9.2 Webex Cisco

Es una herramienta de videoconferencia bajo suscripción, que permite reuniones desde cualquier lugar y en tiempo real, ofreciendo capacidad integrada al compartir video, audio y contenido.

Webex se encuentra en la nube de Cisco y es utilizado para reuniones virtuales interactivas, soporte técnico y accesos remotos, brindando una experiencia de colaboración segura y confiable [68].

Existe una versión gratuita de 90 días para que los clientes puedan conocer su funcionamiento y aplicativos. Una vez terminado el tiempo de prueba se deberá cancelar mensualmente para acceder al licenciamiento de esta herramienta [69].

2.2.9.3 Cisco Meeting Server (CMS)

CMS, por sus siglas en inglés, es una herramienta de comunicación Web, audio y video; permite a sus usuarios trabajar en ambientes colaborativos, agradables y de fácil manejo. Se detalla a continuación las principales características. [82]

- Experiencias de usuario intuitiva y sencilla
- Facilita colaboración en las empresas
- Se puede invitar a unirse a una reunión a cualquier usuario externo utilizando un punto final de colaboración Cisco.
- Escalabilidad: implementaciones pequeñas o grandes.
- Opción de licencias multipartidaria que admite concesión de licencias por reunión.

Dentro de las Plataformas se tiene a Cisco Meeting Server 1000 (servidor Cisco UCS x86 admite hasta 120 llamadas de videoconferencia HD simultáneas) y 2000 (servidor Cisco UCS x86 admite hasta 875 llamadas de videoconferencia HD simultáneas.)

La Unidad Educativa al no contar con este servicio requiere que al menos su personal administrativo y docente cuente con el licenciamiento para realizar videoconferencias. Durante la emergencia sanitaria, el área administrativa y educativa se ha visto en la necesidad de realizar reuniones constantes con docentes, estudiantes y padres de familia. Por tal motivo, es necesario contar con una herramienta que facilite esta comunicación con los miembros de la comunidad educativa. Así mismo, el personal docente imparte sus clases mediante entornos virtuales por lo que es necesario contar con una plataforma colaborativa estudiante - docente para lograr un mejor aprendizaje.[82]

2.2.10 VIDEO VIGILANCIA

El sistema de video vigilancia que la Institución posee ha estado trabajando sin problemas desde su implementación, por lo que no es necesario realizar un rediseño de este. Lo que se recomienda en este proyecto es solamente realizar un mantenimiento a los sistemas de video vigilancia y sus cámaras.

En reuniones mantenidas con las autoridades no se ha considerado la reubicación o adquisición de nuevas cámaras, por lo que en el diseño se ha considerado solamente la integración con la red propuesta a través de una nueva VLAN de videoconferencia, para que estas se conecten a los equipos de red más cercanos.

En la Tabla 2.17 se encuentra el cálculo de cable UTP para la integración con los *switches* de Acceso propuestos en el diseño.

2.2.11 PLANEAMIENTO IP Y VLAN

En el planeamiento IP de la Unidad Educativa “FESVIP”, se asignarán direcciones IP a cada uno de los equipos de usuarios de la red cableada e inalámbrica, tomando en cuenta que la institución contará con 292 puntos de datos físicos y acceso vía inalámbrica. Por tal motivo, se utilizará el esquema VLSM (Máscaras de subred de longitud variable), que permite crear una red lógica jerárquica, en la que el direccionamiento se establecerá mediante una dirección 192.168.0.0.

En la Tabla 2.52. se detallan las subredes, áreas y número de puntos considerados en el diseño. Para este cálculo se utilizó la calculadora FLSM & VLSM [70].

Tabla 2.52 Direcciones IP para servicios de red

VLAN	VLAN ID	SUBRED	MASCARA	IP INICIAL	IP FINAL	IP DE BROADCAST	N° DE HOST
Servidores	10	192.168.8.128/27	255.255.255.224	192.168.8.129	192.168.8.158	192.168.8.159	30
Administración de red	20	192.168.8.160/27	255.255.255.224	192.168.8.161	192.168.8.190	192.168.8.191	30
Access point	30	192.168.7.128/26	255.255.255.192	192.168.7.129	192.168.7.190	192.168.7.191	62
Laboratorios	40	192.168.7.192/26	255.255.255.192	192.168.7.193	192.168.7.254	192.168.7.255	62
Aulas y Salas	50	192.168.4.0/24	255.255.255.0	192.168.4.1	192.168.4.254	192.168.4.255	254
Administrativo	60	192.168.5.0/24	255.255.255.0	192.168.5.1	192.168.5.254	192.168.5.255	254
Docentes	70	192.168.6.0/24	255.255.255.0	192.168.6.1	192.168.6.254	192.168.6.255	254
Estudiantes	80	192.168.0.0 /22	255.255.252.0	192.168.0.1	192.168.3.254	192.168.3.255	1022
Autoridades	90	192.168.8.192/28	255.255.255.240	192.168.8.193	192.168.8.206	192.168.8.207	14
Invitados	100	192.168.7.192/26	255.255.255.192	192.168.8.1	192.168.8.62	192.168.8.63	62
Video vigilancia	110	192.168.7.192/26	255.255.255.192	192.168.8.65	192.168.8.126	192.168.8.127	62
VoIP	120	192.168.7.0/25	255.255.255.128	192.168.7.1	192.168.7.126	192.168.7.127	126
TOTAL							2232

En el diseño, se han creado VLAN (LAN virtuales) para cada una de las áreas que conforman la Institución, con el fin de brindar seguridad, flexibilidad y calidad en la red. Además, permite que en cada una de las áreas pueda existir el intercambio de información y el acceso sea de acuerdo con el personal autorizado en cada VLAN.

Las VLAN creadas en el diseño, se enlistan a continuación:

- VLAN Servidores
- VLAN Administración de red
- VLAN Access point
- VLAN Aulas y salas
- VLAN Laboratorios
- VLAN Administrativo
- VLAN Estudiantes
- VLAN Autoridades
- VLAN Invitados
- VLAN Video vigilancia
- VLAN VoIP

2.2.12 DIMENSIONAMIENTO DEL TRÁFICO

En el siguiente apartado se realiza el dimensionamiento de red de la Unidad Educativa "FESVIP", ya que como se había mencionado esta no cuenta con una red diseñada para los procesos de comunicación. En el diseño se considerarán los servicios de red, correo electrónico, VoIP, acceso a la web y descarga de archivos; es importante indicar que en este dimensionamiento el ancho de banda se referirá a la capacidad de transmisión. Adicionalmente se tomará en cuenta los tiempos en que existe mayor demanda o exigencia por parte de los usuarios de la Institución.

2.2.12.1 Cálculo del ancho de banda para correo electrónico

La finalidad de realizar el cálculo del ancho de banda para correo electrónico es para que toda la comunidad educativa autoridades, administrativos, docentes, estudiantes y personal de apoyo cuente con este servicio y sea un medio de comunicación formal; este servicio permitirá la entrega de informes, oficios y circulares importantes. En este proceso se deberá tomar en cuenta que en general un *mail* tiene un tamaño aproximado de 10 Kbytes; considerando que se adjuntan documentos de programas como Word, Excel, PowerPoint y PDF, se asume que el tamaño relativo de dicho correo en promedio es de 300 KBytes.

Para el siguiente cálculo se considera el tamaño promedio del correo y el tiempo de descarga de 30 segundos:

$$Capacidad_{C.electrónico} = \frac{300KBytes}{1\ Correo} * \frac{8\ bits}{1\ Byte} * \frac{1\ correo}{30\ segundos} = 80\ Kbps \qquad (2.5)$$

2.2.12.2 Cálculo del tráfico de navegación web

La Unidad Educativa "FESVIP", cuenta con su propia página web: www.fesvip.edu.ec que es utilizada por padres de familia, personal docente, administrativo y estudiantes.

Para realizar el cálculo de la capacidad de página web se deberá considerar el tamaño promedio de 1977 Kbytes y el tiempo de carga de 30 segundos aproximadamente; se deberá tomar en cuenta que en el área administrativa existen páginas que serán utilizadas con mayor frecuencia como: IDUKAY, IESS, Ministerio de Educación, entre otras; mientras que el personal docente y estudiantes ingresarán a páginas educativas e informativas. En este diseño el acceso a sitios web será controlado y limitado.

$$Capacidad_{página\ web} = \frac{1977KBytes}{Página\ web} * \frac{8\ bits}{1\ Byte} * \frac{Página\ web}{30\ segundos} = 527{,}2\ Kbps \qquad (2.6)$$

2.2.12.3 Descarga de archivos

Para realizar el cálculo de la capacidad de descarga de archivos se debe considerar el tamaño promedio de un archivo de 3 MBytes (audio, video, documentos, etc.). Adicionalmente se considera que el tiempo de descarga de un archivo es de 60 segundos.

$$Capacidad_{Descarga\ de\ archivos} = \frac{3000KBytes}{archivo} * \frac{8\ bits}{1\ Byte} * \frac{1\ archivo}{60\ segundos} = 400\ Kbps \qquad (2.7)$$

2.2.12.4 Consideraciones para conexión a Internet

Una vez que se ha calculado la capacidad de tráfico en correo electrónico, descargas y página web; se estima que todas estas aplicaciones van a ser utilizadas de manera simultánea, por lo que se procede a considerar un valor aproximado para el intercambio de información.

- Descarga de archivos 30%
- Tráfico en la Web 40%
- Correo electrónico 30%

Se ha determinado estos porcentajes debido al uso de la red de los usuarios, un 30% en descarga de archivos recibidos por el área administrativa y estudiantes, 40% tráfico en la Web y un 30% en revisión de correo electrónico.

En la Tabla 2.53 se presenta el número de usuarios de acuerdo con los puntos a implementarse en la Unidad Educativa “FESVIP” y considerando un 30% de uso concurrente, estos datos fueron obtenidos en base a entrevistas y análisis con el personal de la Institución.

Tabla 2.53 Número de usuarios finales en la UE - FESVIP

ÁREA	N° DE PUNTOS DE RED	N° DE USUARIOS POTENCIALES (30%)
BLOQUE 1	110	33
BLOQUE 2	12	4
BLOQUE 3	15	5
BLOQUE 4	155	47
TOTAL	**292**	**89**

2.2.14.5 Cálculo de ancho de banda para la VoIP

Para realizar el cálculo de ancho de banda total de la red, se debe tomar en cuenta el tráfico de la VoIP. En este caso, las cabeceras de sobrecarga para el transporte de la voz corresponden a la de los protocolos de IP, UDP, RTP. También se deberá considerar que este tráfico de voz en la LAN se encapsulará en ethernet; también debe tomarse en cuenta el códec empleado en la digitalización de la voz.

La trama ethernet de una LAN que transporta VoIP se observa en la Figura 2.37. En esta trama se debe considerar que:

- La suma de las cabeceras IP, UDP y RTP es de 40 bytes, a esto se debe añadir 18 bytes de la trama Ethernet, dado un resultado de *overhead* de 58 bytes.

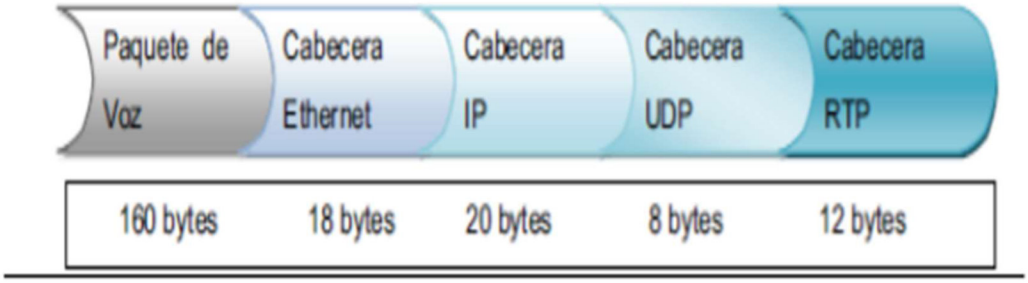


Figura 2.37 Trama ethernet de VoIP

Para el cálculo de ancho de banda se tiene la ecuación 2.8, en la que se considera un códec G.711 que trabaja con una velocidad de digitalización de 64 Kbps, siendo este el más adecuado para optimizar los recursos de transmisión de voz.

$$A.Banda = Ancho\ de\ banda\ códec * \frac{Tamaño\ overhead + Tamaño\ paquete\ de\ voz}{Tamaño\ paquete\ de\ voz} \qquad (2.8)$$

$$A.Banda = 64\ Kbps * \frac{58\ bytes + 160\ bytes}{160\ bytes} = 87{,}2\ Kbps$$

Se considera que de los 292 puntos de red existirá una estimado de 89 usuarios que consumirán un ancho de banda de 7760 Kbps con un grado de simultaneidad del 30%.

$$AB\ total = 87{,}2\ Kbps * 89\ usuarios = 7760\ Kbps \qquad (2.9)$$

$$AB\ total\_sim = 87{,}2\ Kbps * (89\ usuarios)30\% = 2328{,}24\ Kbps$$

2.2.14.6 Cálculo para WLAN

Para realizar el cálculo de WLAN se deberá considerar el servicio más utilizado tomando en cuenta principalmente los servicios de VoIP. Se han utilizado los valores anteriormente calculados, y de ese valor se estima que un 50% corresponde al tráfico WLAN en comparación al tráfico de red cableada.

$$C_{WLAN=} 50\% \left(C.c.electrónico + C\ pweb + C.descargas + C.ancho\ de\ banda\ VoIP \right) \qquad (2.10)$$

$$C_{WLAN=} 50\% \left(80 + 527{,}2 + 400 + 87{,}2 \right) = 547{,}2\ Kbps$$

2.2.14.7 Capacidad de canales requeridos para datos

En el cálculo de ancho de banda se considera el número de usuarios estimados y la simultaneidad de uso. En la Tabla 2.54 se muestra el cálculo de ancho de banda total, tomando en cuenta el número de usuarios que simultáneamente se encuentran utilizando cada una de las aplicaciones, que se han considerado en la Institución.

Tabla 2.54 Ancho de banda por aplicación

APLICACIÓN	ÁREA	AB promedio por usuario [Kbps]	[%] Simultaneidad	Usuarios estimados	AB [Kbps]
Correo electrónico	BLOQUE 1	80	30%	33	792
	BLOQUE 2			4	96
	BLOQUE 3			5	120
	BLOQUE 4			47	1128
Total, ancho de banda				89	2136
Página Web	BLOQUE 1	527,2	40%	33	6959,04
	BLOQUE 2			4	64
	BLOQUE 3			5	80
	BLOQUE 4			47	752
Total, ancho de banda				89	7855,04
Descargas	BLOQUE 1	400	30%	33	2640
	BLOQUE 2			4	320
	BLOQUE 3			5	400
	BLOQUE 4			47	3760
Total, ancho de banda				89	7120
WLAN	BLOQUE 1	547,2	50%	33	9028,8
	BLOQUE 2			4	1094,4
	BLOQUE 3			5	1368
	BLOQUE 4			47	12859,2
Total, ancho de banda				89	24350,4
TOTAL					41461,44

2.2.14.8 Ancho de banda de la conexión a Internet

Se ha considerado el tráfico de VoIP solamente de uso interno, por lo que en la Tabla 2.55 se muestran los valores correspondientes al cálculo de ancho de banda por aplicación que se generarán en la intranet.

Tabla 2.55 Ancho de banda de todas las áreas para la Intranet

APLICACIÓN	ANCHO DE BANDA [Kbps]
Correo electrónico	2136
Página Web	7855,04
Descargas	7120
WLAN	24350,4

A continuación, se consideran las descargas que se realizan desde el Internet, página web y correo electrónico.

$$Capacidad\ ISP = Capacidad\ mail + Capacidad\ web + Capacidad\ descargas + Capacidad\ WLAN \quad (2.11)$$

$$Capacidad\ ISP = 2{,}136 + 7{,}855 + 7{,}120 + 24{,}350 = 41{,}461\ Mbps$$

Con la ecuación 2.11 **¡Error! No se encuentra el origen de la referencia.**se determina la capacidad de canal que demandarán las aplicaciones, llegándose a obtener un canal de 41,461 Mbps, por lo que se recomienda tener un enlace mínimo de 50 Mbps.

2.2.14.9 Cálculo para el servicio de video vigilancia

Para realizar el cálculo del tráfico del servicio de video vigilancia IP se deben considerar varios parámetros como:

- Compresión del códec: varía entre (70:1) para imágenes con movimiento y a 200:1 para imágenes estáticas, se escoge el valor intermedio de 130:1 (130 bits a 1 bit)
- Resolución de la cámara (pixeles): de 640 x 480 (alto y ancho)
- Velocidad de cuadro por segundo (fps): valor de 15
- Profundidad de color (bits x píxel): 24 bits, permiten una apreciación en buen tamaño.

Con los valores anteriormente mencionados se puede calcular la capacidad para transmitir por cada una de las cámaras IP.

$$Capacidad_{Videovigilancia\ IP} = \frac{\frac{640x480\ pixeles}{cuadro} * \frac{24\ bits}{pixel} * \frac{15\ cuadros}{segundo}}{130} = 850{,}70\ Kbps \qquad (2.12)$$

La capacidad de este servicio estará en funcionamiento en las 31 cámaras de forma ininterrumpida. Se obtiene un valor de simultaneidad de 26371,7 Kbps lo cual es un valor manejable en una LAN.

$$\boldsymbol{CV} = 850{,}70\ Kbps\ x\ 31 = 26371{,}7\ Kbps \qquad (2.13)$$

2.3 CÁLCULO DEL PRESUPUESTO REFERENCIAL

Para el cálculo del presupuesto referencial se han determinado las características para el diseño de la red convergente de la Unidad Educativa "FESVIP", la cual ha permitido realizar una determinación de costos de los equipos y accesorios necesarios para la implementación. Las proformas han sido solicitadas a empresas de tecnología que se encuentran posicionadas en el mercado durante ya varios años, las cuales han facilitado los costos de diferentes marcas disponibles en el mercado nacional.

Durante este proceso se han tomado en cuenta los equipos y elementos que cumplen los requerimientos técnicos, normativas y estándares. Se detallan a continuación los costos referenciales de red pasiva, activa, operación y mantenimiento.

2.3.1 COSTOS REFERENCIALES DE LA RED PASIVA

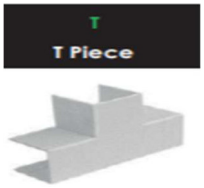
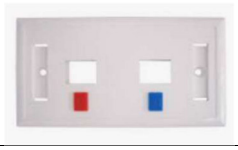
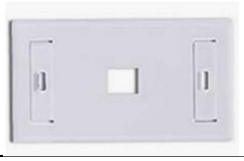
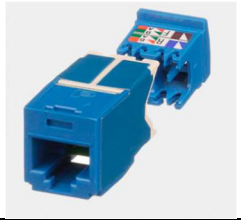
Para poder determinar los costos de la red pasiva es indispensable reconocer la importancia de esta, ya que es la encargada de que los datos se propaguen en toda la Unidad Educativa. Los elementos que conforman la red pasiva son:

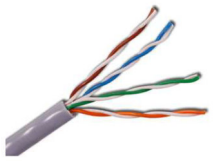
Sistema de cableado estructurado: *patch cords*, *faceplates*, cables UTP, canaletas, escalerillas, tubo conduit, conectores, Jack Cat 6A, entre otros.

***Racks* – Gabinetes:** Pie y Mural

En la Tabla 2.56, se detallan los materiales necesarios para el diseño de la red pasiva de todas las zonas de la Institución.

Tabla 2.56 Elementos para la red pasiva

DESCRIPCIÓN	CARACTERÍSTICAS			FORMA
	MEDIDA	UNIDAD	COLOR	
Canaleta /Cable Trunking	60 x 60 mm	2 m	RAL 9010	
	60 x 40 mm	2 m	RAL 9010	
	40 x 22 mm	2 m	RAL 9010	
	32 x 12 mm	2 m	RAL 9010	
Ángulo, pliegue de 90	60 x 60 mm	N/A	RAL 9010	
	60 x 40 mm		RAL 9010	
	40 x 22 mm		RAL 9010	
	32 x 12 mm		RAL 9010	
Derivación T	60 x 60 mm	N/A	RAL 9010	
	60 x 40 mm		RAL 9010	
	40 x 22 mm		RAL 9010	
	32 x 12 mm		RAL 9010	
Faceplate doble	2 UR	N/A	BLANCO	
Faceplate simple	N/A	N/A	BLANCO	
Patch cords Cat 6A	3 y 7 pies	N/A	EcuRed	
Jack Cat 6A	N/A	N/A		

Cable UTP 6A	305 m	1 rollo	Blanco	
Tubo Conduit PVC	3 m	N/A	Blanco	
Rack de Pie	19"	22 UR	Negro	
Gabinetes de pared	19"	12, 6, 17, 22 UR	Negro	
Conector MPTL modular RJ-45 Cat6A Blindad	N/A	N/A	N/A	
Módulos de fibra Cisco SFP Multimodo	N/A	N/A	N/A	

2.3.2 COSTOS TOTALES DE LA RED PASIVA

Los costos de equipos y elementos de la red pasiva de los cuatro bloques en los que se divide la Institución se detallan de acuerdo con las proformas solicitadas a empresas de tecnología y principales distribuidores de cableado estructurado a nivel nacional. El detalle se encuentra en el **ANEXO F.**

En la Tabla 2.57. se presenta un resumen de los costos de los equipos y elementos a utilizar de la red pasiva para la implementación de la red diseñada en la Unidad Educativa.

Tabla 2.57 Costos finales de la red pasiva

ZONA	COSTO ($)
BLOQUE 1	20521,15
BLOQUE 2	2501,03
BLOQUE 3	3296,61
BLOQUE 4	20981,97
TOTAL, SIN IVA	47300,76

2.3.3 COSTOS REFERENCIALES DE LA RED ACTIVA

La red activa consta de elementos como *switches* y *access point*. En el presente diseño se realiza la comparación de las características de dos marcas que se tienen actualmente en el mercado Nacional e Internacional.

2.3.3.1 Equipos de conectividad

2.3.3.1.1 Switches

Se han considerado en equipos de conectividad las marcas Cisco y Aruba debido a su alta confiabilidad y disponibilidad en el mercado.

Las cotizaciones han sido facilitadas por una empresa líder en telecomunicaciones en el Ecuador como los es Akros Soluciones Tecnológicas. Estas cotizaciones se presentan en el **ANEXO H**.

En la Tabla 2.58 se detallan los costos referenciales de las marcas mencionadas en este diseño.

Tabla 2.58 Costo total de equipos de conectividad

DESCRIPCIÓN	CANTIDAD	C/U CISCO ($)	TOTAL, CISCO ($)	C/U ARUBA ($)	TOTAL, ARUBA ($)
CORE	1	9441,12	9441,12	9367,59	9367,59
DISTRIBUCIÓN	2	13953,77	27907,54	27210,91	54421,82
ACCESO - 48P	11	2101,84	23120,24	2071,76	22789,36
ACCESO - 24P	1	1568,53	1568,53	1629,26	1629,26
TOTAL, SIN IVA			**62037,43**		**88208,03**

Una vez establecidos los costos de las dos marcas líderes en el mercado, se ha tomado como una alternativa conveniente y que cumple con todas las funcionalidades necesarias para el diseño la marca Cisco, que a su vez mantiene costos más bajos en los *switches* de distribución y acceso de 24 puertos.

2.3.3.1.2 Access Point

En la Unidad Educativa se propone para la red inalámbrica dos marcas de equipos como Aruba y Cisco que cumplen con las características funcionales para la implementación de la red, brindando a los usuarios fácil manejo y configuración de sus equipos.

Se detallan en la Tabla 2.59 los costos referenciales de las marcas mencionadas.

Tabla 2.59 Costos AP

DESCRIPCIÓN	CANTIDAD	C/U CISCO ($)	TOTAL, CISCO ($)	C/U ARUBA ($)	TOTAL, ARUBA ($)
Access Point	32	1804,92	**57757,44**	1235,4	**39532,8**

Tomando en cuenta el costo para la implementación de *access point* en todas las áreas de la Unidad Educativa, se ha considerado la marca Aruba que cumple con todas las funcionalidades necesarias y adicionalmente refieren un costo menor que la marca Cisco.

2.3.3.2 *Firewall*

A partir de las especificaciones técnicas necesarias mencionadas en el diseño para la Unidad Educativa “FESVIP” se han seleccionado dos marcas de equipos de seguridad perimetral que actúan como *firewalls* de última generación, en la Tabla 2.60 y Tabla 2.61 se pueden observar los costos referenciales tanto para Checkpoint y Fortinet, respectivamente.

Tabla 2.60 Costos Checkpoint

CANTIDAD	EQUIPO	COSTO UNITARIO ($)	VALOR TOTAL SIN IVA ($)
1	6600 Appliance- Plus package with SNBT service package for 1 year	45.000	45.000
1	Collaborative Enterprise Support - Premium Add-on for Products	6750	6750
TOTAL, SIN IVA			51.750

Tabla 2.61 Costos FortiGate

CANTIDAD	EQUIPO	COSTO UNITARIO ($)	VALOR TOTAL SIN IVA ($)
1	FortiGate-900D Hardware plus 3 Year 8×5 FortiCare and FortiGuard UTM Protection	32.220	32.220

Una vez analizados los costos de las dos marcas líderes en el mercado, se considera el equipo de marca Fortinet, que cumple con las funcionalidades requeridas y adicionalmente sus costos de implementación son más bajos que Checkpoint.

2.3.3.3 Servidores para alojar los nuevos servicios

Como se menciona en el diseño para los servicios adicionales AD, DNS y DHCP se utilizará un servidor con sistema operativo *Windows Server* 2019 estándar; y de la misma manera para el servicio FTP se utilizará un servidor con sistema operativo *Windows Server* 2019 estándar, por lo que en la Tabla 2.62 se detallan los costos de licenciamiento asociado, se debe tomar en consideración que estos costos son exclusivos para el segmento de Educación en el mercado y deben ser aclarados en el momento de la cotización, caso contrario no se aplicará al beneficio del segmento con el fabricante Microsoft.

Tabla 2.62 Costos de licenciamiento *Windows Server*

SERVICIOS			
CANTIDAD	SERVIDOR	COSTO UNITARIO ($)	VALOR TOTAL ($)
2	WinSvrSTDCore 2019 SNGL OLP 16Lic NL Acdmc CoreLic	287	574

Para todos los servicios adicionales se ha considerado la adquisición de un servidor físico con licenciamiento VMware que permitirá virtualizarlos. En la Tabla 2.63 y en la Tabla 2.64 se encuentra la descripción de costos de las dos marcas de servidores propuestas en el diseño.

Tabla 2.63 Costos de servidor DELL y licencia VMware

SERVIDOR RACK PowerEdge R640			
CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO ($)	PRECIO TOTAL ($)
1	SERVIDOR RACK PowerEdge R640	3170,00	3170,00
4	Dell Memory Upgrade - 32GB - 2Rx4 DDR4 RDIMM 3200MHz	543,75	2175,00
3	960GB SSD SATA Mixed Use 6Gbps 512e 2.5in Hot Plug Drive, S4610, CK	872,50	2617,50
1	PowerEdge R640: Upgrade from 3Yr ProSupport NBD On-Site to 3Yr ProSupport MC 4H On-Site	625,00	625,00
1	VMware vSphere 7 Standard for 1 processor	1099,74	1099,74
1	Basic Support/Subscription for VMware vSphere 7 Standard for 1 processor for 3 years	896,16	896,16
VALOR TOTAL SIN IVA			10583,40

Tabla 2.64 Costos de servidos HPE y licencia VMware

SERVIDOR HPE DL360 Gen10 8SFF			
CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO ($)	PRECIO TOTAL ($)
1	HPE DL360 Gen10 4210R 1P 16G NC 8SFF Svr	2905,00	2905,00
4	HPE 32GB 2Rx4 PC4-2933Y-R Smart Kit	742,50	2970,00
3	HPE 960GB SATA MU SFF SC MV SSD	713,75	2141,25
1	HPE 500W FS Plat Ht Plg LH Pwr Sply Kit	176,25	176,25
1	HPE 3Y TC Ess DL360 Gen10 SVC	626,25	626,25
1	VMw vSphere Std 1P 3yr E-LTU	1775,00	1775,00
VALOR TOTAL SIN IVA			10593,75

Al analizar los costos de los dos servidores mencionados se ha podido determinar que no existe una variación considerable en cuanto al valor indicado y características, pero por experiencia en el mercado y facilidad en casos de soporte y/o garantía se escoge la marca DELL para este diseño.

2.3.3.4 Telefonía IP

Una vez que se han determinado las centrales telefónicas IP que cumplen con los requerimientos de la Unidad Educativa, se procede a establecer los costos de las dos marcas seleccionadas.

Los costos en la marca Grandstream es de una central telefónica *on premise* (se puede observar en la Tabla 2.65), mientras que en la de Cisco se ha considerado el despliegue de esta en un ambiente virtual por lo que se ha cotizado licenciamiento para su funcionamiento, además de un *Gateway* que permitirá la interconexión con la PSTN (ver Tabla 2.66).

Tabla 2.65 Costos Grandstream

CANTIDAD	DESCRIPCIÓN	COSTO UNITARIO ($)	VALOR TOTAL ($)
1	Grandstream UCM6304	1130	1130
5	Teléfonos Grandstream GRP2602	45,5	227,50
VALOR TOTAL SIN IVA			1357,50

Para el diseño de la red de voz de acuerdo con la Tabla 2.65, se ha considerado adicionalmente la adquisición de 5 teléfonos IP para el área administrativa los cuales serán distribuidos de la siguiente manera: Rectorado, recepción, Vicerrectorado, Inspección general y Secretaría. Los demás usuarios utilizarán *softphones* en cada uno de sus equipos de computación.

En la Tabla 2.66 se muestran los costos del Sistema de Telefonía correspondiente a la marca Cisco, en la que igualmente se han incluido 5 teléfonos IP para las áreas administrativas anteriormente indicadas.

En el contexto postpandemia donde la institución ha sido afectada económicamente, se ha tomado como la opción más viable a la central Grandstream, ya que permitirá cumplir con los requerimientos básicos de la institución a nivel de Telefonía IP.

Tabla 2.66 Costos Cisco CUCM versión 12.5

CANTIDAD	DESCRIPCIÓN	COSTO UNITARIO ($)	VALOR TOTAL SIN IVA ($)
1	Gateway de Voz ISR4321 (Conexión PSTN) - 1 interfaces WAN RJ45 (conexión a la troncal SIP) - 4 Interfaces 1G RJ45 (Conexión LAN o crecimiento de Troncales SIP) - PVDM 64 Canales - Módulo de 4 interfaces FXO, Cantidad 1 - Garantía 24x7 3 años	9140,7	9140,7
1	Suscripción Licencias Central Telefónica - Licencias Enhanced (Cantidad 100) - Incluye Webex Teams para un dispositivo Suscripción 3 años	15800,4	15800,4
5	Teléfono IP Básico 7821 (Teléfono 2 líneas) - 2 Interfaces de red 10/100 - Incluye Patchcord de red - Garantía 8x5xNBD 3 años	201,63	1008,15
1	SERVICIOS - Configuración de servidor BE6K-M - Integración de servicios - Escalamiento de soporte con fabricante - Transferencia de conocimientos 24 horas	6666,67	6666,67
TOTAL, SIN IVA			32615,92

2.3.3.5 Videoconferencia

Tomando en consideración las plataformas de videoconferencia que existen en el mercado se ha optado por Microsoft Teams, Webex Cisco y Cisco Meeting Server 1000, que cumplen las características técnicas necesarias para las actividades administrativas y educativas de la institución.

En la Tabla 2.67 se presenta el valor referencial de licenciamiento de Microsoft Teams que se encuentra vinculado con Office 365.

Tabla 2.67 Costos de licenciamiento Office 365 - Microsoft Teams

CANTIDAD	PLATAFORMA	VALOR ANUAL ($)	VALOR TOTAL ANUAL ($)
65	Office 365 A3 for faculty - Microsoft Teams	39,67	2578,55

En la Tabla 2.68 se muestra el valor referencial del licenciamiento Webex Cisco.

Tabla 2.68 Costos Webex Cisco

CANTIDAD	PLATAFORMA	VALOR 3 AÑOS + TELEFONÍA CISCO ($)	VALOR TOTAL 3 AÑOS ($)
100	Webex Cisco	15800,4	15800,4

La Tabla 2.69 indica el valor de licenciamiento para el servicio Cisco Meeting Server.

Tabla 2.69 Costo CMS 1000

CANTIDAD	PLATAFORMA	VALOR TOTAL ($)
1	Cisco Meeting Server 1000	23869,00

En el servicio de videoconferencia, dadas las diferentes propuestas tanto en la nube como *on premise,* la mejor solución que podría adoptar la Unidad Educativa, considerando el costo – beneficio a largo plazo, es el de implementar el servicio de Office 365 que incluye licencias de MS Teams, por su crecimiento, versatilidad e incluso facilidad de administración es la mejor opción.

2.3.4 COSTOS TOTALES DE LA RED ACTIVA

En la Tabla 2.70. se resumen los costos de la red activa los cuales deberán ser tomados en cuenta por el administrador de la Unidad Educativa “FESVIP” para la implementación de la red activa.

Tabla 2.70 Costo total de la red activa

DESCRIPCIÓN	COSTO ($)
Equipos de Conectividad	60037,43
Access Point	39532,8
Firewall	32220,0
Licenciamiento Servidores	574
Servidores	10583,4
Telefonía IP	1357,5
Videoconferencia	23869
TOTAL, SIN IVA	168174,13

2.3.5 COSTOS REFERENCIALES DE OPERACIÓN Y MANTENIMIENTO

Los costos referenciales de instalación, configuración y puesta en marcha se han realizado en base al mercado actual, al costo/hora del especialista encargado de realizar este trabajo e incluyen un año de soporte y garantía de fábrica (ver Tabla 2.71).

Tabla 2.71 Costos de instalación, configuración y puesta en marcha

DESCRIPCIÓN	COSTO DE INSTALACIÓN, CONFIGURACIÓN, PUESTA EN MARCHA Y MANTENIMIENTO POR UN AÑO ($)
Equipos de Conectividad	2200
Access Point	1280
Firewall	1280
Servidores	1200
Telefonía IP	1200
Videoconferencia	1200
TOTAL, SIN IVA	8360

2.3.6 COSTO TOTAL DEL DISEÑO DE RED

Se consideran los valores de la red pasiva y activa para conocer la inversión que deberá realizar la Unidad Educativa “FESVIP”. La Tabla 2.72. presenta los valores totales referenciales del diseño de la red.

Tabla 2.72 Costo de inversión para el diseño de la red

DESCRIPCIÓN	COSTO ($)
Costos referenciales red pasiva	47300,76
Costos referenciales red activa	168174,3
Costo de Instalación, Configuración, Puesta en Marcha y Mantenimiento por un año	8360
Subtotal	223835,06
12% IVA	26860,21
TOTAL	**250695,27**

2.4 SIMULACIÓN

Para el presente proyecto, dentro del alcance se ha considerado un producto demostrable, es decir, una simulación/emulación con las principales características de este diseño, lo que permitirá validar el diseño.

2.4.1 CONSIDERACIONES INICIALES

Las consideraciones iniciales que se han tomado en cuenta son los medios necesarios para la realización del producto demostrable, *hardware* y *software* utilizado.

A nivel de *hardware* como elemento principal se utilizó un servidor línea blanca que soporte el ambiente virtual que se desea obtener (ver Figura 2.38), donde se alojan todos los servicios simulados. En la Tabla 2.73 se indican las características principales de este servidor.

Tabla 2.73 Características servidor línea blanca

SERVIDOR	
Marca	N/A
Modelo	N/A
Procesador	AMD Ryzen 9 3950X 16-Core
Memoria RAM	128 GB
Almacenamiento	1.24 TB

Adicionalmente, se utilizaron equipos *laptops* para la conexión y configuración de los diferentes ambientes. A nivel de *software*, para las diferentes aplicaciones y servicios, se consideran los que se detallan a continuación.

Como hipervisor principal (monitor de máquinas virtuales) en el servidor físico se ha instalado VMware ESXi, 7.0.2, el cual permite la creación de las diferentes máquinas virtuales que actúan como servidores y equipos dentro del ambiente de simulación.

Figura 2.38 Servidor línea blanca

Para la simulación de la red se utilizó EVE-NG versión 2.0.3-112 el cual permite la simulación de las capas jerárquicas de red. Se usó *software* para la implementación de los diferentes servicios, los cuales se mencionan en la instalación de cada uno de ellos.

2.4.2 DIRECCIONAMIENTO IP PARA SIMULACIÓN

Como parte de la simulación se consideró la creación de subredes y VLAN que permitan mostrar la red diseñada; por facilidad no estarán basadas en un esquema de VLSM. Los segmentos utilizados para la simulación se indican en la Tabla 2.74.

Tabla 2.74 Direccionamiento IP simulación

DESCRIPCIÓN	RED	ID, VLAN	OBSERVACIÓN
Red Principal	192.168.100.0/24	N/A	Red doméstica, donde se instalan servidores principales como: VMware y *firewall* de red y es la red que permite la salida a Internet
Red Secundaria	192.168.200.0/30	VLAN 200	Red de interconexión entre *CORE* y *FIREWALL* de red
Red Servidores	192.168.10.0/24	VLAN 10	Red de servidores (SRV)
Red Administrativo	192.168.20.0/24	VLAN 20	Red Equipos Administrativos
Red Docentes	192.168.30.0/24	VLAN 30	Red Equipos Docentes

Red Estudiantes	192.168.40.0/24	VLAN 40	Red Equipos Estudiantes
Red Laboratorio 01	192.168.50.0/24	VLAN 50	Red Equipos Laboratorio 01
Red Laboratorio 02	192.168.60.0/24	VLAN 60	Red Equipos Laboratorio 02

2.4.3 INSTALACIÓN DE SOFTWARE DE SIMULACIÓN

Para la instalación y configuración del *software* de simulación y virtualización se obtuvieron los instaladores en los portales respectivos de cada uno de los elementos.

El proceso de instalación y configuración se encuentra detallado en el **ANEXO G**.

2.4.4 DIAGRAMA LÓGICO DE LA SIMULACIÓN

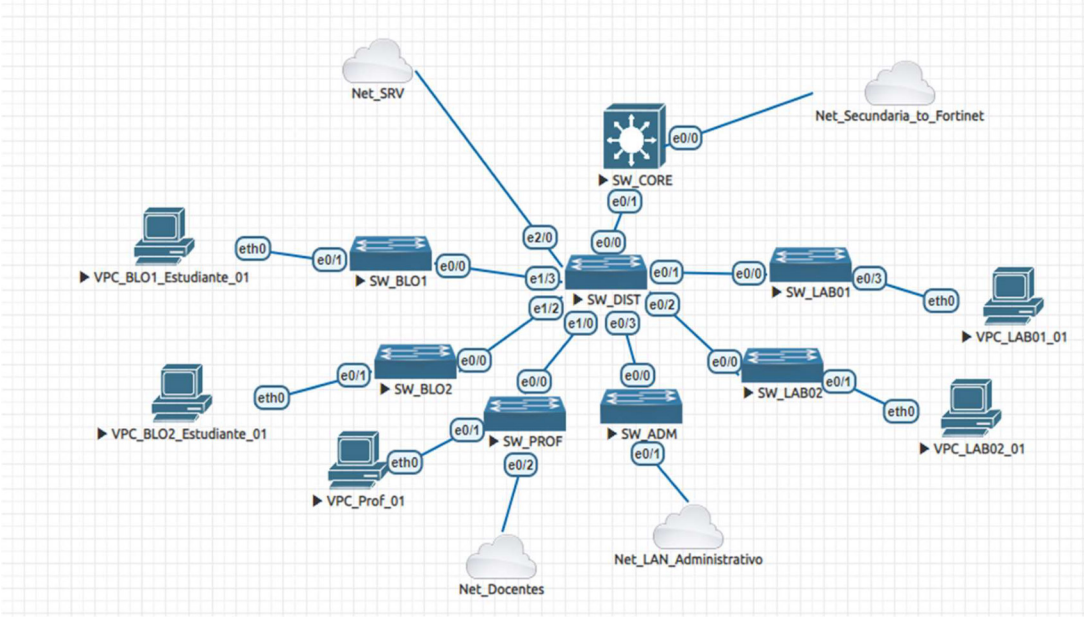


Figura 2.39 Diagrama lógico de red simulada en EVE-NG

2.4.5 SIMULACIÓN DE EQUIPOS DE CONECTIVIDAD

Como se mencionó, el *software* para simular los equipos de conectividad es EVE-NG; para empezar con la simulación se presenta en la Figura 2.40 el diagrama lógico de la red a simular.

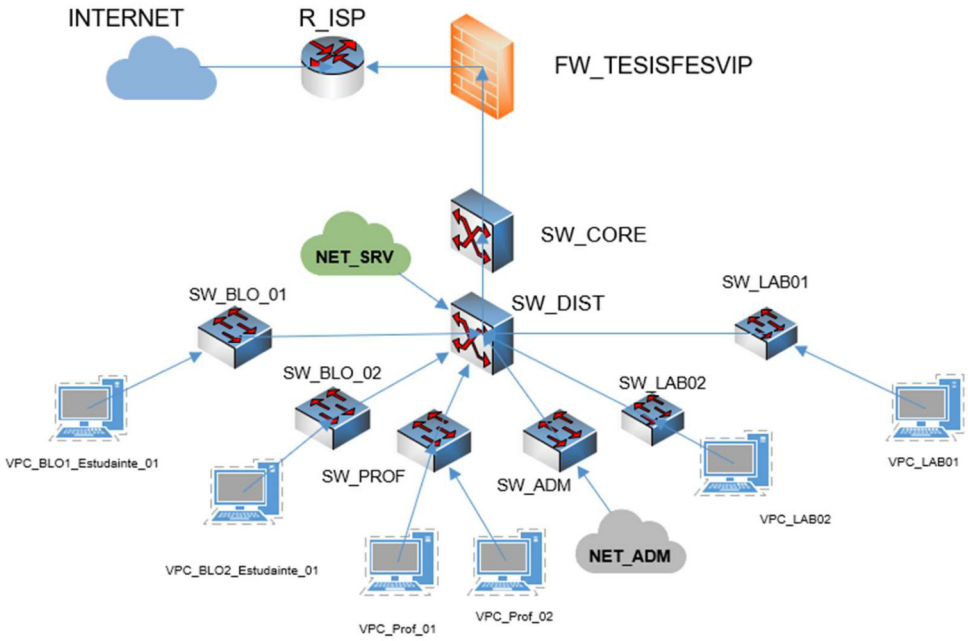


Figura 2.40 Diseño de red por simular

2.4.5.1 Configuración de equipos de red

Para la configuración de los equipos de conectividad dentro de EVE-NG, es necesario acceder a la consola de administración, esto se lo realiza dando doble clic al equipo dentro del simulador (ver Figura 2.41), o si el equipo tiene una dirección IP de administración se lo puede acceder desde un aplicativo de acceso del tipo SSH o TELNET.

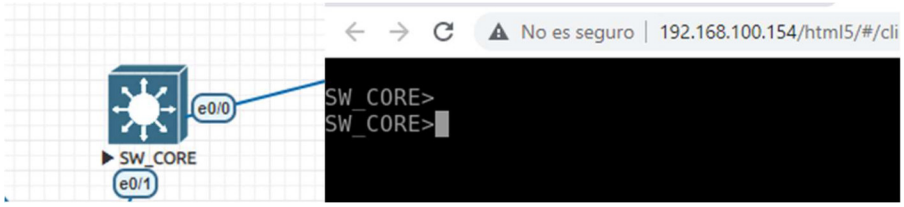


Figura 2.41 Configuración de equipos de red

Una vez estructuradas las capas de los equipos en la simulación, en cada uno de ellos se realizan configuraciones básicas donde se puede observar y aplicar los principales comandos.

2.4.5.1.1 Configuración básica de equipos switches de core

Para la configuración básica del equipo de *Core* o núcleo, se aplican varios comandos necesarios para el correcto funcionamiento; a continuación, se muestran algunos de ellos, para la demostración en la simulación:

- Nombre del equipo, comando: *hostname* SW_CORE
- Contraseña de acceso, comando: *enable secret* fesvip123
- Contraseña de acceso por consola, comandos: *line console* 0
    - *password* fesvip123
    - *login*
- Cantidad de conexiones, comando: *line vty* 0 15
    - *password* fesvip123
    - l*ogin*
- Grabar configuración, comando: wr
- Visualizar la configuración del equipo, comando: *show running-config*

En el *switch* de *Core*, al ser el equipo que trabaja en capa 3, se realizan las configuraciones de enrutamiento y adicionalmente se configuran las subinterfaces con los diferentes segmentos de red, para luego configurar las VLAN en el *switch* de distribución.

Configuración de la interfaz de conexión hacia el equipo *firewall*:

- interface Ethernet0/0
- ip address 192.168.200.2 255.255.255.252

Configuración de la interfaz y subinterfaces para la interconexión con el equipo *switch* de distribución.

- interface Ethernet0/1
- no ip address
- interface Ethernet0/1.10
- description NET_SERVIDORES
- encapsulation dot1Q 10
- ip address 192.168.10.254 255.255.255.0
- interface Ethernet0/1.20
- description NET_ADMINISTRATIVO
- encapsulation dot1Q 20
- ip address 192.168.20.254 255.255.255.0
- ip helper-address 192.168.10.10

- interface Ethernet0/1.30
- description NET_PROFESORES
- encapsulation dot1Q 30
- ip address 192.168.30.254 255.255.255.0
- ip helper-address 192.168.10.10
- interface Ethernet0/1.40
- description NET_ESTUDIANTES
- encapsulation dot1Q 40
- ip address 192.168.40.254 255.255.255.0
- ip helper-address 192.168.10.10
- interface Ethernet0/1.50
- description NET_LAB01
- encapsulation dot1Q 50
- ip address 192.168.50.254 255.255.255.0
- ip helper-address 192.168.10.10
- interface Ethernet0/1.60
- description NET_LAB02
- encapsulation dot1Q 60
- ip address 192.168.60.254 255.255.255.0
- ip helper-address 192.168.10.10

Al realizar el comando: *show ip interface brief* se pueden validar las interfaces y subinterfaces en el equipo *switch* de *Core* y el estado de cada una de ellas (Figura 2.42).

```
SW_CORE#sh ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                192.168.200.2   YES NVRAM  up                    up
Ethernet0/1                unassigned      YES NVRAM  up                    up
Ethernet0/1.10             192.168.10.254  YES NVRAM  up                    up
Ethernet0/1.20             192.168.20.254  YES NVRAM  up                    up
Ethernet0/1.30             192.168.30.254  YES manual up                    up
Ethernet0/1.40             192.168.40.254  YES manual up                    up
Ethernet0/1.50             192.168.50.254  YES manual up                    up
Ethernet0/1.60             192.168.60.254  YES manual up                    up
```

Figura 2.42 Configuración interfaces SW_CORE

2.4.5.1.2 Configuración básica del equipo switch de distribución

Además de las configuraciones básicas, como el nombre del equipo o permisos de seguridad, destaca en la configuración del *switch* de distribución, la creación de VLAN y la configuración de las interfaces en modo acceso o modo troncal para los diferentes servicios, que se interconectan a través de un puerto con el *Switch* de *Core* y sus subinterfaces.

- interface Ethernet0/0
- description CONEXION_CORE
- switchport trunk encapsulation dot1q
- switchport mode trunk
- interface Ethernet0/1
- description CONEXION_SW_LAB01
- switchport access vlan 50
- switchport mode Access
- interface Ethernet0/2
- description CONEXION_SW_LAB02
- switchport access vlan 60
- switchport mode Access
- interface Ethernet0/3
- description CONEXION_SW_ADMIN
- switchport access vlan 20
- switchport mode Access
- interface Ethernet1/0
- description CONEXION_SW_PROF
- switchport access vlan 30
- switchport mode Access
- interface Ethernet1/1
- interface Ethernet1/2
- description CONEXION_SW_BLO2
- switchport access vlan 40
- switchport mode Access

- interface Ethernet1/3
- description CONEXION_SW_BLO1
- switchport access vlan 40
- switchport mode Access
- interface Ethernet2/0
- description CONEXION_SRV
- switchport access vlan 10
- switchport mode access
- Configuración de las VLAN en el switch de distribución:
- interface Vlan10
- no ip address
- interface Vlan20
- no ip address
- interface Vlan30
- no ip address
- interface Vlan40
- no ip address
- interface Vlan50
- no ip address
- interface Vlan60
- no ip address

2.4.5.1.3 Configuración básica del equipo switch de acceso

La configuración de los equipos de acceso es muy similar a los otros equipos; se configura además del nombre del equipo y seguridad de acceso, los puertos en modo acceso en la VLAN que se requiera. Por motivos de simulación como se observa en el *switch* de *core* se han generado las VLAN mencionadas y en la simulación se configuran puertos de acceso con las diferentes VLAN.

2.4.5.1.4 Diagrama de red simulada en EVE-NG

En la Figura 2.39 se puede observar el diagrama lógico y en la Figura 2.43., se muestran los nodos creados para la simulación en el laboratorio.

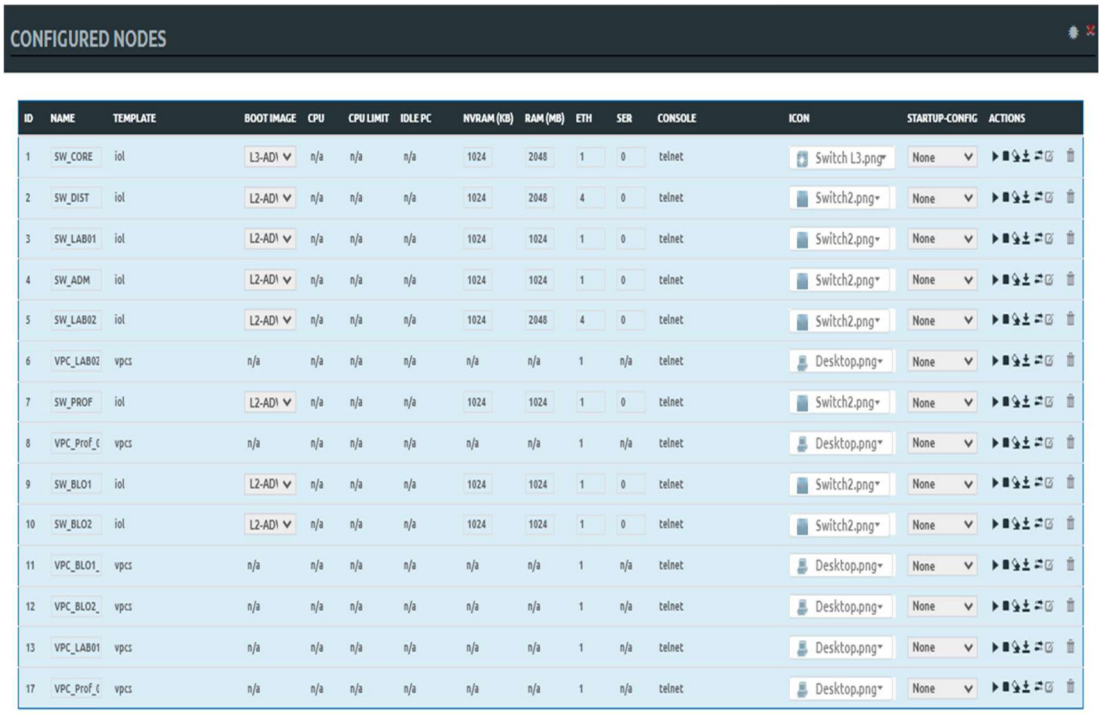


Figura 2.43 Nodos configurados EVE-NG

2.4.6 SIMULACIÓN DE SERVICIOS ADICIONALES

Para la simulación de servicios adicionales, se han generado las diferentes máquinas virtuales en VMware, y la conexión hacia la red simulada mediante interfaces virtuales entre VMware y EVE-NG; a continuación, se detalla el proceso de instalación y configuración de estas.

2.4.6.1 Instalación y configuración de AD, DHCP, DNS

Para la instalación de los servicios de AD, DHCP y DNS se utilizó un servidor virtual *Windows Server 2019 Standard*, se obtuvo la imagen y se desplegó la máquina virtual en el ambiente VMware, con las características presentadas en la Tabla 2.75.

Tabla 2.75 Características *Windows Server 2019*

CARACTERÍSTICAS	ESPECIFICACIONES
Procesador	8 vCPU
Memoria RAM	16 GB
Disco Duro	200 GB
Adaptadores de Red	1 adaptador de red

Este servidor virtual está conectado a la red de servidores (192.168.10.0/24) a través de la interfaz virtual de VMware y EVE-NG (ver Figura 2.44).

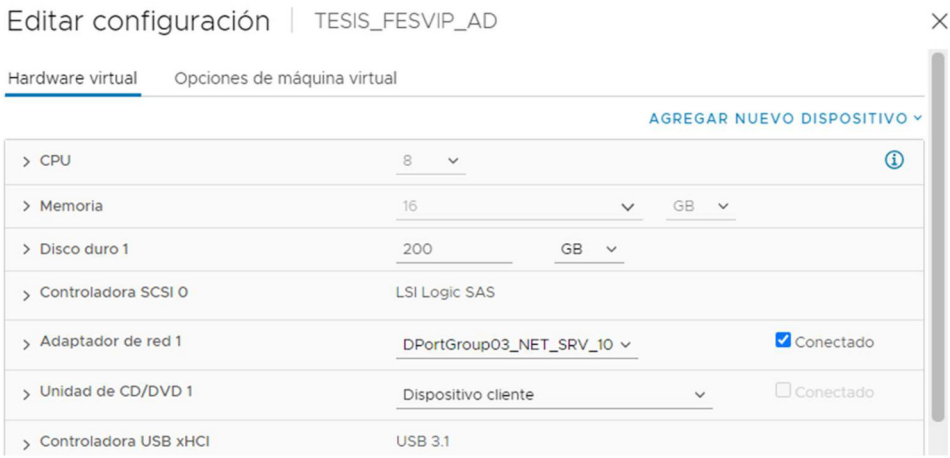


Figura 2.44 Configuración MV AD-DNS-DHCP

Una vez instalado el sistema operativo base y realizadas las configuraciones de direccionamiento IP básicas, con los datos de la Tabla 2.76, se procede a activar los diferentes roles en el servidor (AD, DNS, DHCP).

Tabla 2.76 Características servidor AD-DNS-DHCP

CARACTERÍSTICAS	ESPECIFICACIONES
Hostname	SRVAD01
IP	192.168.10.10
Máscara	255.255.255.0
Gateway	192.168.10.254
Dominio	tesisfesvip.com
Usuario Local	Administrator
Contraseña	Admin001*$

Una vez completo el *wizard* de activación de roles y funcionalidades en el servidor, se realiza un reinicio de este para aplicar todos los cambios.

Es importante antes de reiniciar la máquina virtual cambiar el nombre para que se agregue como AD principal y con su respectivo *hostname* dentro de la configuración;

una vez culminado el proceso y reiniciada la máquina virtual, todos los roles son habilitados y validados dentro del servidor como se puede observar en la Figura 2.45.

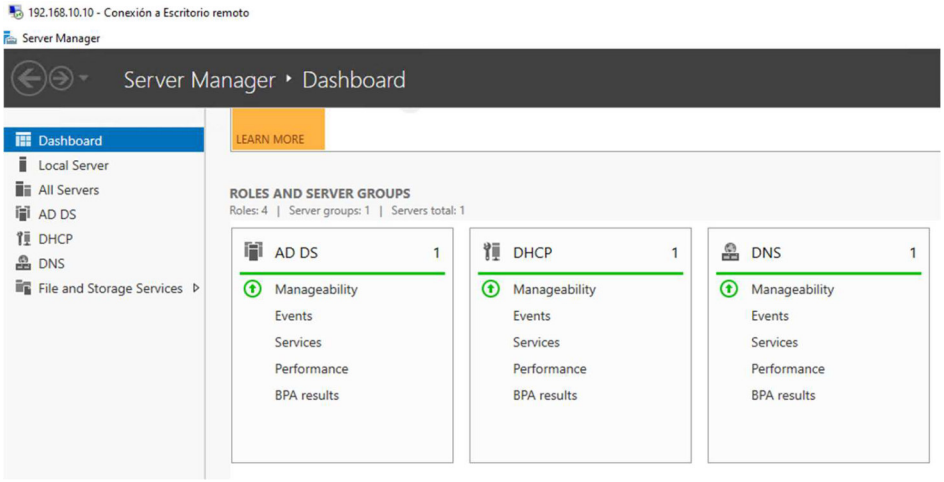


Figura 2.45 Roles activados en servidor (AD, DNS, DHCP)

Una vez activados los roles, se procede a configurar cada uno de ellos, empezando por la organización de usuarios y equipos dentro del Directorio Activo. En el dominio principal *tesisfesvip.com*, se crea la Unidad Organizativa principal (OU, por sus siglas en inglés) llamada FESVIP y dentro de ella otras Unidades Organizativas para establecer de mejor manera a Equipos, Usuarios y servidores. (ver Figura 2.46)

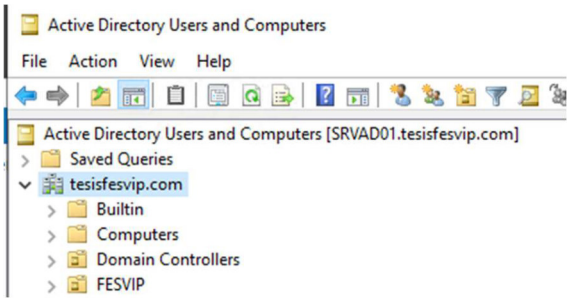


Figura 2.46 Directorio activo

Dentro de Usuarios se crean adicionalmente las Unidades Organizativas en base a la estructura organizacional de la Unidad Educativa “FESVIP” para un mejor entendimiento y estructura de usuarios, por lo que cada vez que se genere un usuario nuevo dentro del Directorio Activo, este será organizado en base a su departamento y con todas las propiedades que deba tener. (ver Figura 2.47)

Así mismo, cada vez que un nuevo equipo, estación de trabajo y servidores se agreguen al dominio, se tienen que mover a sus respectivas unidades organizativas; esto facilita

además de una buena organización, el despliegue de políticas de administración grupal dentro del directorio activo.

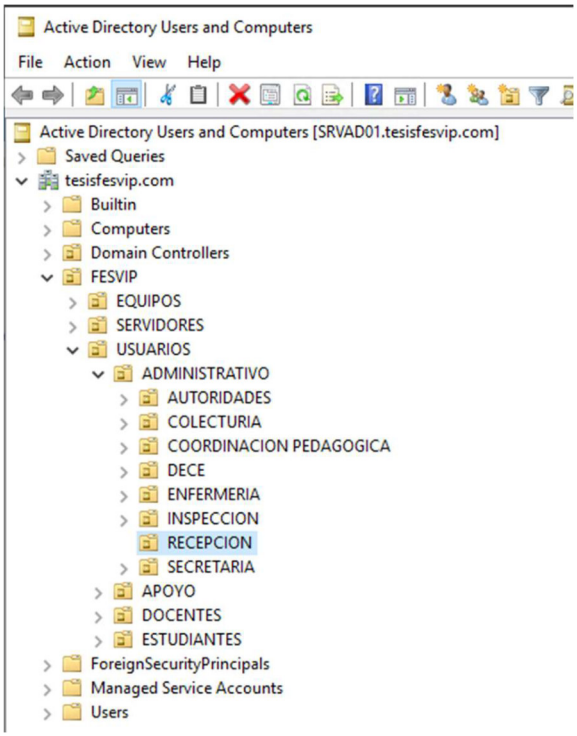


Figura 2.47 Unidades organizativas

Los usuarios que se crean para las pruebas de simulación son las autoridades (3 usuarios) de la Institución y 2 profesores al azar tal como se observa en la Figura 2.48.

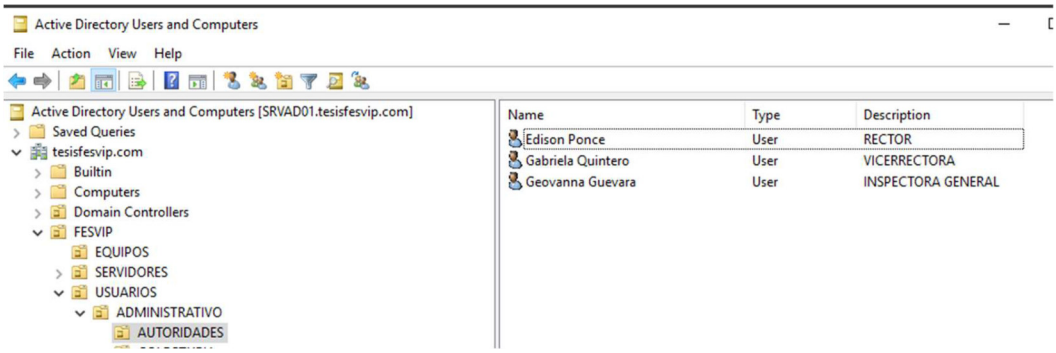


Figura 2.48 Usuarios - autoridades

Para validar el servidor de DHCP se crean varios *pools* en base a los segmentos de red utilizados en la simulación, a excepción de la red de servidores en la que no se configura para asignación dinámica de direcciones IP. Lo mencionado se observa en la Figura 2.49.

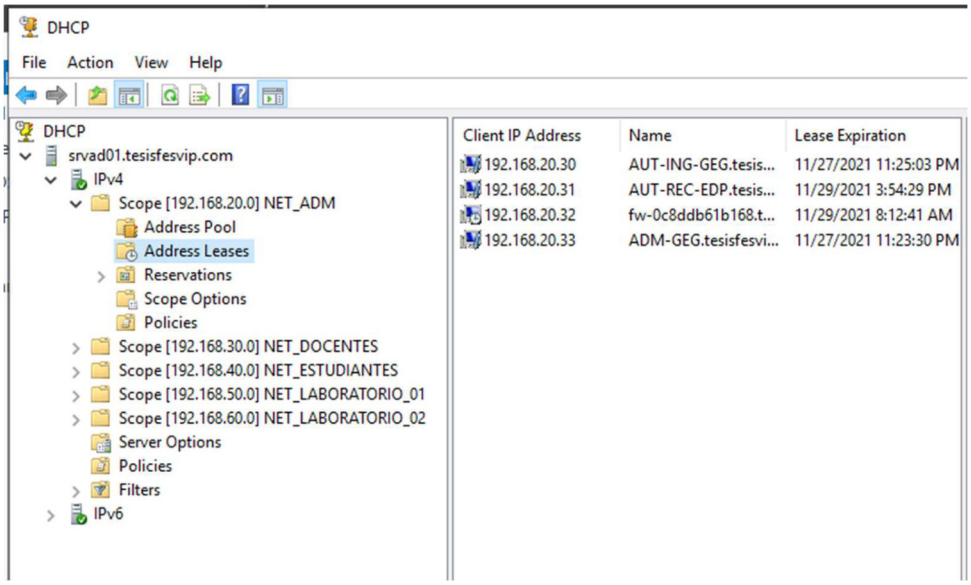


Figura 2.49 Administración DHCP

Para finalizar, en el *DNS Manager* se crean varios registros para la resolución de nombres en la red interna, tal como se muestra en la Figura 2.50.

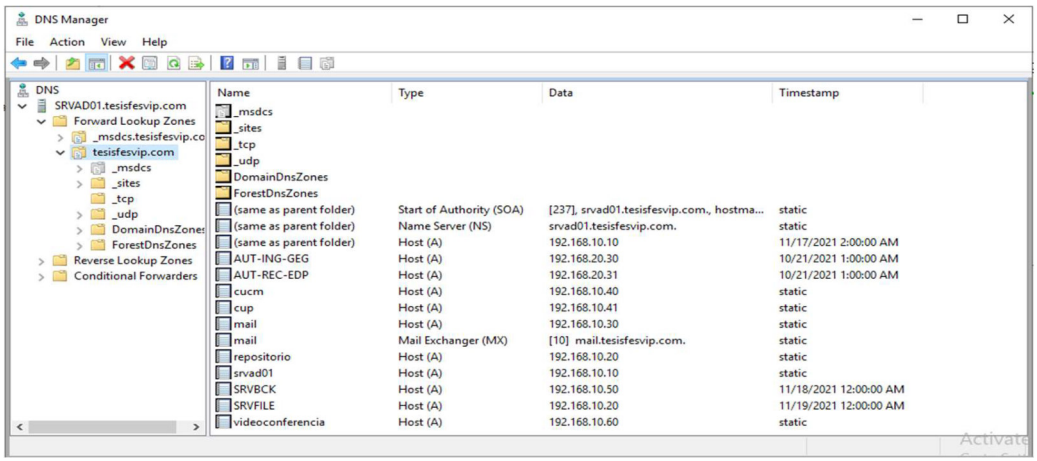


Figura 2.50 DNS Manager

2.4.6.2 Instalación y configuración de FTP

Para la instalación y configuración del servicio de FTP conocido en *windows* como *File and Storage Services*, se utiliza un servidor virtual *Windows Server 2019 Standard* en el ambiente VMware, con características que permitan desplegar la funcionalidad con los requerimientos necesarios, que se muestran en la Tabla 2.77. se procede a crear la máquina virtual con sus características básicas (ver Figura 2.51), se despliega el sistema operativo, se agrega el servidor al dominio con su respectivo *hostname* y direccionamiento IP.

Tabla 2.77 Características MV - FTP

CARACTERÍSTICAS	ESPECIFICACIONES
Procesador	8 vCPU
Memoria RAM	8 GB
Disco Duro 1	250 GB
Disco Duro 2	150 GB
Adaptadores de Red	1 adaptador de red
Sistema Operativo	Windows Server 2019 Standard
Hostname	SRVFILE
IP de Administración	192.168.10.20
Máscara	255.255.255.0
Gateway	192.168.10.254
Dominio	tesisfesvip.com
Usuario Local	Administrator
Contraseña	Admin001*$

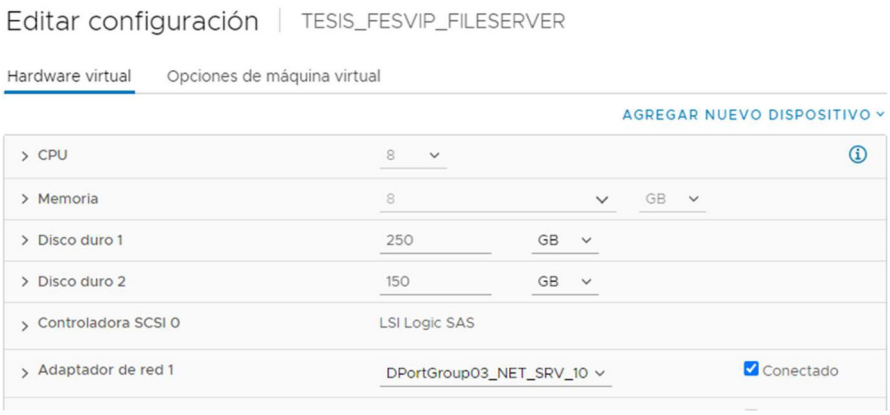


Figura 2.51 Características configuradas MV - FTP

Para finalizar se habilita el rol necesario que emule un servidor de archivos, como se muestra en la Figura 2.52, creando una carpeta compartida con el nombre UE_FESVIP (ver Figura 2.53) y sus respectivas subcarpetas (ver Figura 2.54) las cuales tienen permisos de acceso en base a la estructura organizacional de la Institución.

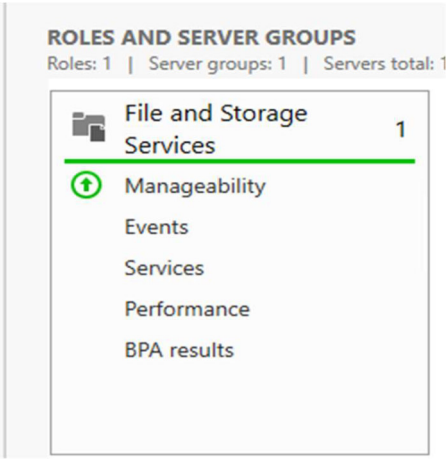


Figura 2.52 File and Storage Services

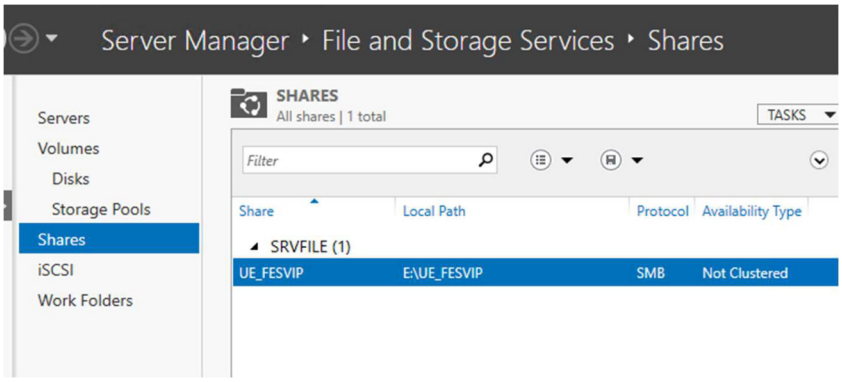


Figura 2.53 Carpeta principal

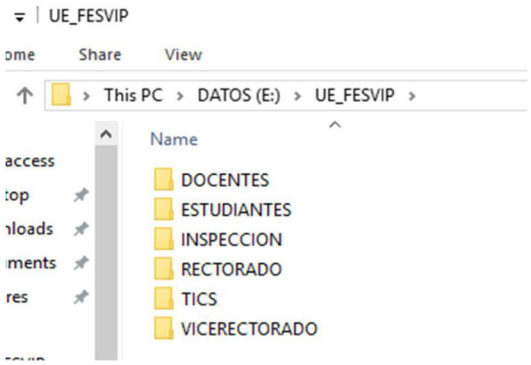


Figura 2.54 Subcarpetas

2.4.7 SIMULACIÓN DE SERVICIO DE CORREO

Para la simulación del servicio de correo electrónico, se escogió la opción de *software* libre Zimbra *Collaboration*, la cual trabaja sobre sistemas operativos Linux; para el despliegue en la simulación se utilizó Ubuntu en su versión 18.04.06. Se procede a crear

la máquina virtual en VMware (ver Figura 2.55), con las características mostradas en la Tabla 2.78.

Tabla 2.78 Características VM - ZIMBRA

CARACTERÍSTICAS	ESPECIFICACIONES
Procesador	8 vCPU
Memoria RAM	12 GB
Disco Duro 1	100 GB
Adaptadores de Red	1 adaptador de red
Sistema Operativo	Ubuntu 18.04.06

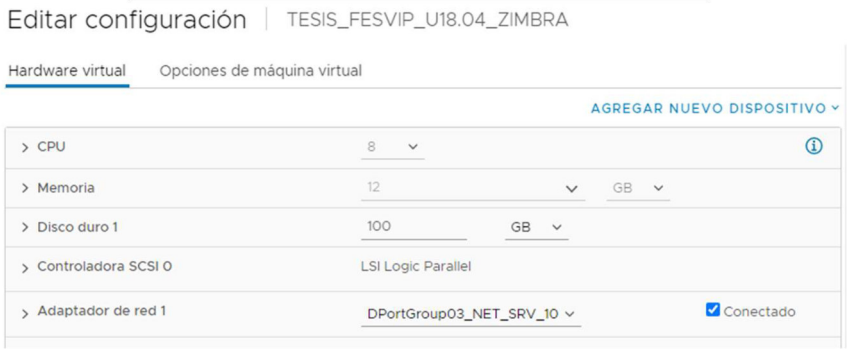


Figura 2.55 Características configuradas MV - ZIMBRA

Una vez creada la máquina virtual, se enciende y se ejecuta la instalación del sistema operativo base Ubuntu (ver Figura 2.56) y se ejecuta la instalación del servicio Zimbra.

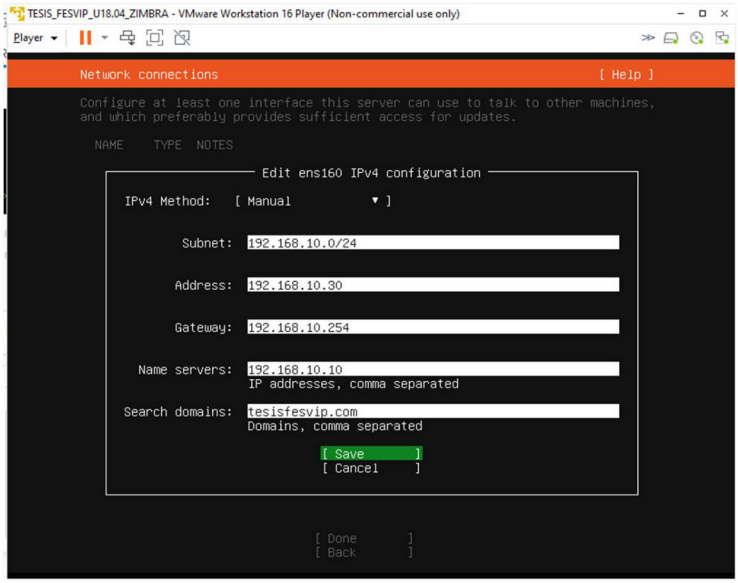


Figura 2.56 Instalación Ubuntu 18.04

Como recomendación en sistemas Linux se deben ejecutar los siguientes comandos para instalar las actualizaciones necesarias de la plataforma:

- apt-get update
- apt-get upgrade

2.4.7.1 Instalación y Configuración de Servidor de Correo Zimbra

Para desplegar el servicio de correo electrónico Zimbra, fue necesario preparar el servidor con ciertos requisitos previos antes de descargar y ejecutar el instalador. A continuación, se detallan los principales archivos que se modificaron:

- **etc/hostname** con el nombre: mail.tesisfesvip.com (ver Figura 2.57)

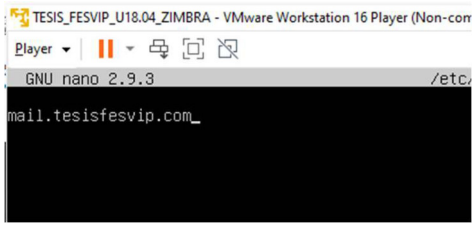


Figura 2.57 Archivo etc/hostname

- **etc/hosts** agregando el registro para: 192.168.10.30 mail.tesisfesvip.com mail (ver Figura 2.58)

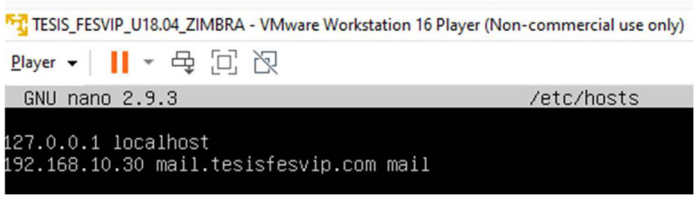


Figura 2.58 Archivo etc/hosts

- **etc/resolv.conf** agregando: nameserver 192.168.10.10 como DNS local. (ver Figura 2.59)

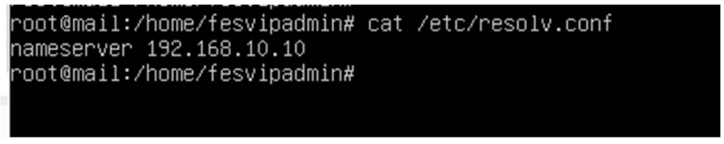


Figura 2.59 Archivo etc/resolv.conf

- **etc/dnsmasq.conf** agregando los siguientes parámetros (ver Figura 2.60):
    - Dirección IP de servidor

- Dominio
- Registro MX
- Dirección de *loopback*

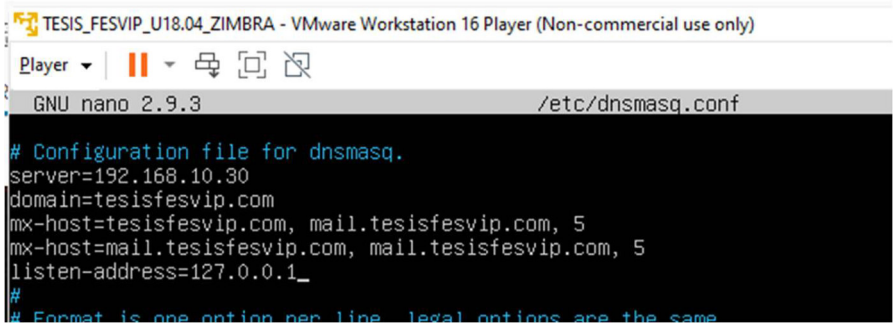


Figura 2.60 Archivo etc/dnsmasq.conf

Una vez configurados los requisitos previos, se ejecutan los comandos para descargar el instalador de Zimbra, con el comando **wget**, tal como se muestra en la Figura 2.61.

Figura 2.61 Descarga comando wget

Se descomprime el archivo y se instala la solución ejecutando el archivo **./install.sh** con privilegios *root* en la carpeta de Zimbra. (ver Figura 2.62).

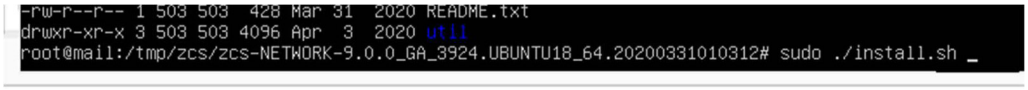


Figura 2.62 Comando ./install.sh

Una vez ejecutado el comando, se inicia la instalación de Zimbra con todos sus componentes. (Ver Figura 2.63)

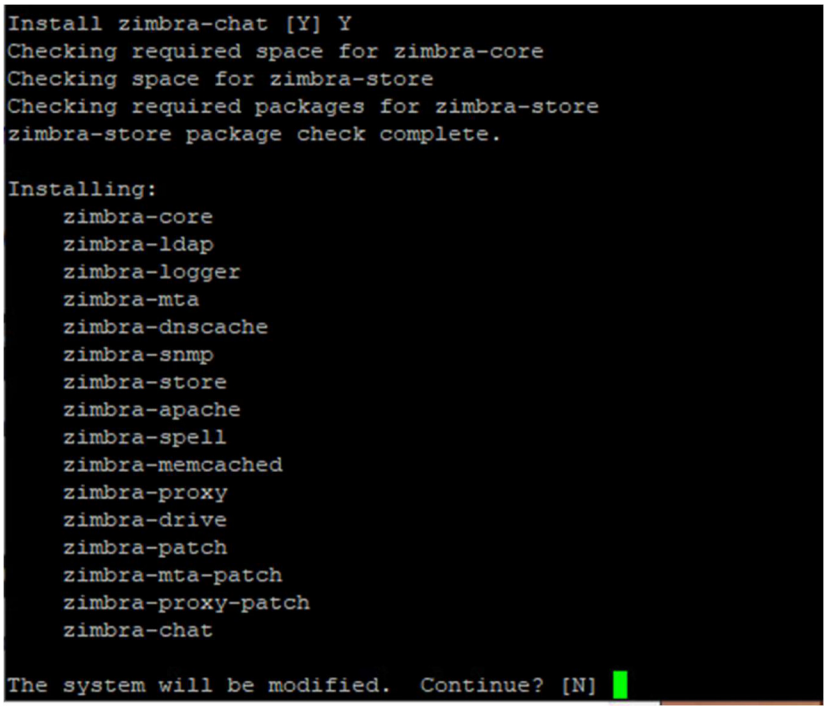


Figura 2.63 Proceso de instalación Zimbra

Terminado el proceso de instalación se validan los accesos al portal de administración: https://192.168.10.30:7071 (ver Figura 2.64).

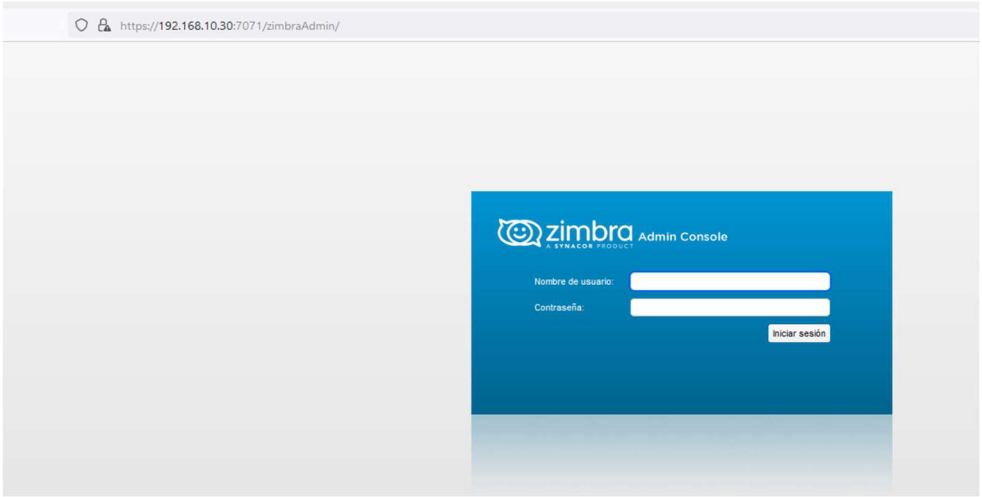


Figura 2.64 Página de administración Zimbra

Se adjunta un cuadro resumen de la instalación de Zimbra, en la Tabla 2.79, y en la Figura 2.65 se pueden observar todos los servicios activos una vez finalizada la instalación.

Tabla 2.79 Características Zimbra

CARACTERÍSTICAS	ESPECIFICACIONES
FQDN	mail.tesisfesvip.com
IP de Administración	192.168.10.30
Máscara	255.255.255.0
Gateway	192.168.10.254
Dominio	tesisfesvip.com
Usuario Local Ubuntu	Fesvipadmin
Contraseña	fesvip123
Usuario administrador Zimbra	admin@mail.tesisfesvip.com
Contraseña	fesvip123

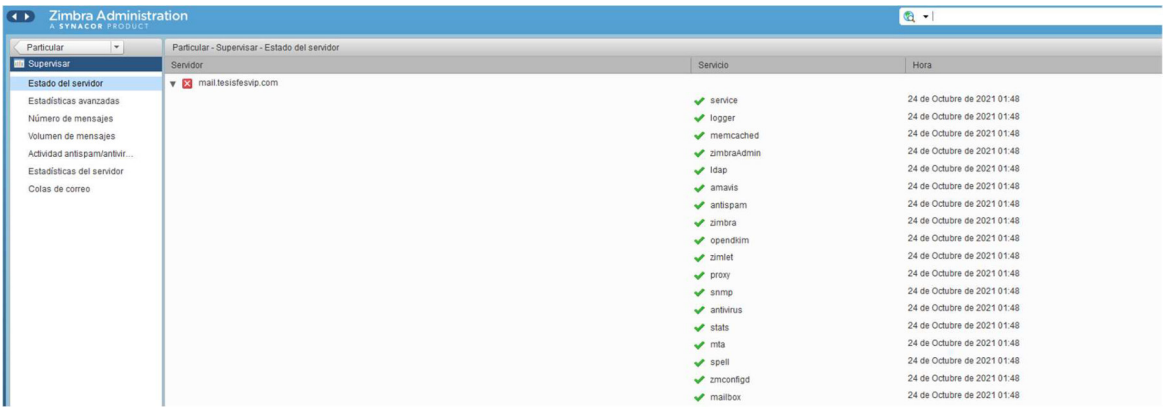


Figura 2.65 Servicios activos de Zimbra

2.4.7.2 Creación y configuración de cuentas correo en Zimbra

Una vez listo el servicio de Zimbra se procede a crear las cuentas de usuario de correo, indicadas en Figura 2.66, para la demostración de envío y recepción.

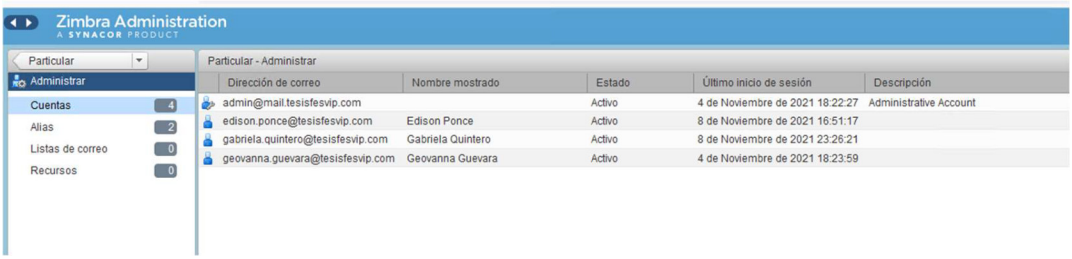


Figura 2.66 Cuentas de correo creadas en Zimbra

Para la simulación se crea otro dominio dentro de la administración de Zimbra para utilizar las cuentas con el dominio @tesisfesvip.com (ver Figura 2.67) tal como en el dominio local.

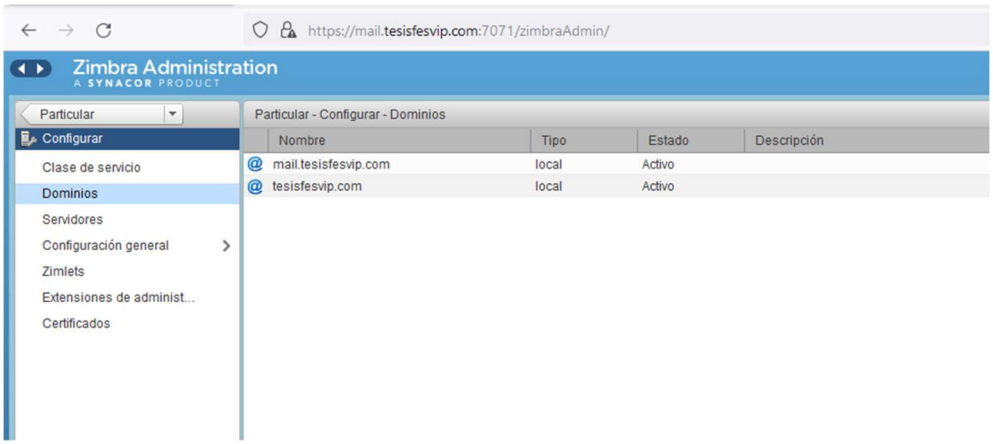


Figura 2.67 Creación de dominio en Zimbra

Adicionalmente, en la Figura 2.68 se puede visualizar la integración con el Directorio Activo para la autenticación del usuario, es decir, para que utilice las mismas credenciales para su inicio de sesión.

Figura 2.68 Configuración de autenticación

2.4.8 SIMULACIÓN DE TELEFONÍA IP

Para la simulación del sistema de Telefonía IP se consiguieron licencias demo de la plataforma Cisco; se instalaron en el ambiente VMware los servidores virtuales de Cisco *Unified Communications Manager, Call Manager (CUCM) y Cisco Unified Communications Manager IM and Presence (CUP)*.

Estas licencias demo permiten el uso por 90 días a partir de la instalación y posibilitan observar las funcionalidades principales de esta plataforma.

Para la instalación, se crean máquinas virtuales a través de un archivo de configuración OVA, que básicamente es una plantilla de instalación, conseguida desde el portal del fabricante con credenciales de Partner. Este archivo es ejecutado en VMware. (ver Figura 2.69 y Figura 2.70).

2.4.8.1 Para el CUCM

Figura 2.69 Creación máquina virtual CUCM

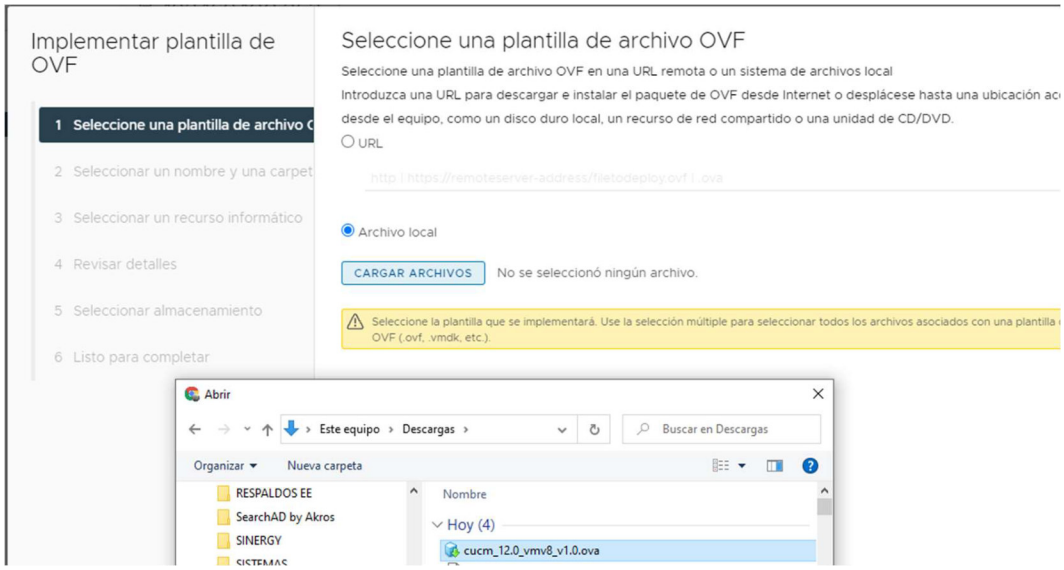


Figura 2.70 Archivo OVF CUMC

Al ejecutarse este archivo cucm_12.0_vmv8_v1.0.ova se genera la máquina virtual con las características que se presentan en la Tabla 2.80.

Tabla 2.80 Características de la máquina virtual

CARACTERÍSTICAS	ESPECIFICACIONES
Procesador	2 vCPU
Memoria RAM	6 GB
Disco Duro 1	80 GB
Adaptadores de Red	1 adaptador de red
Sistema Operativo	Centos 4/5/6 (64 bits)

Una vez creada la máquina virtual, se enciende y se despliega la instalación y configuración, tal como se muestra en la Figura 2.71.

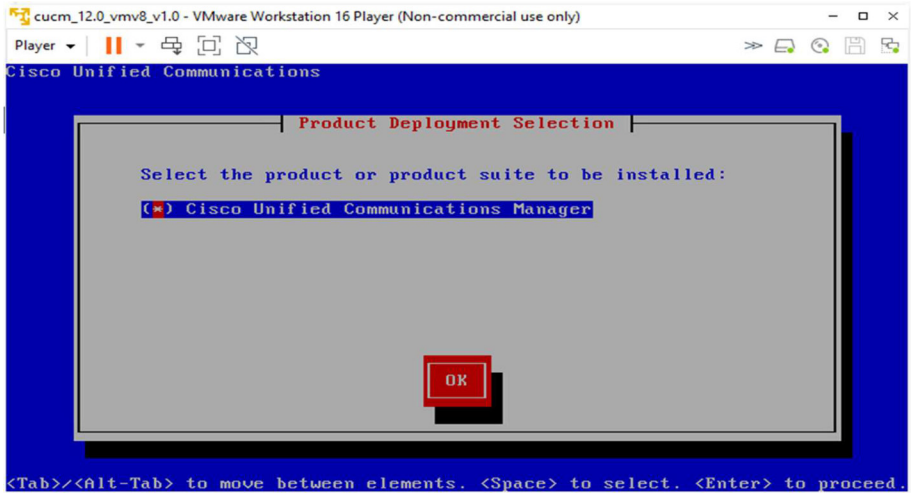


Figura 2.71 Instalación y configuración CUCM

En el proceso de instalación, se solicitan varios datos que se detallan en la Tabla 2.81.

Tabla 2.81 Características para el proceso de instalación CUCM

CARACTERÍSTICAS	ESPECIFICACIONES
FQDN	cucm.tesisfesvip.com
IP de Administración	192.168.10.40
Máscara	255.255.255.0
Gateway	192.168.10.254
NTP Server	192.168.10.254
Dominio	tesisfesvip.com
Usuario Local	Admin
Contraseña	f3svip2021
Usuario de Seguridad	Admin
Contraseña de seguridad	f3svip2021

Para finalizar, se dan de alta todos los servicios en el servidor virtual del CUCM, tal como se indica en la Figura 2.72.

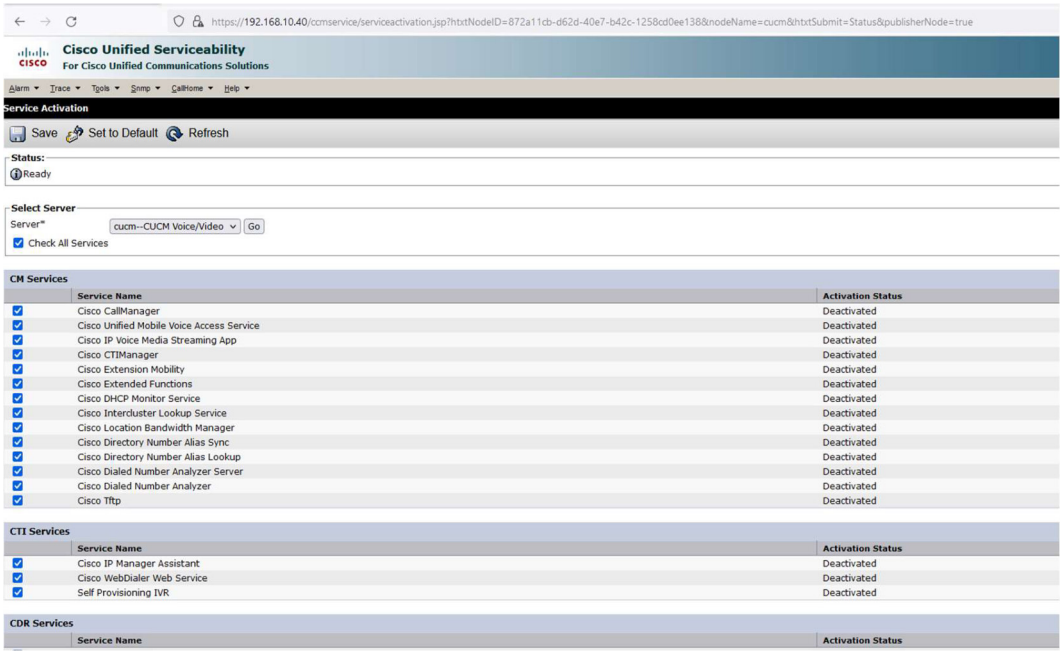


Figura 2.72 Servicios activos en CUCM

2.4.8.2 Para el CUP

De la misma manera que el despliegue de CUCM, para CUP se crea una máquina virtual en el ambiente VMware (ver Figura 2.73) y se despliega mediante el archivo cucm_im_p_12.0_vmv8_v1.4.ova, con las características básicas presentadas en la Tabla 2.82.

Tabla 2.82 Características máquina virtual CUP

CARACTERÍSTICAS	ESPECIFICACIONES
Procesador	1 VCPU
Memoria RAM	4 GB
Disco Duro 1	80 GB
Adaptadores de Red	1 adaptador de red
Sistema Operativo	Centos 4/5/6 (64 bits)

Una vez creada la máquina virtual, se enciende y se realiza la configuración respectiva para su utilización, como se muestra en la Figura 2.74.

Figura 2.73 Configuración características máquina virtual CUP

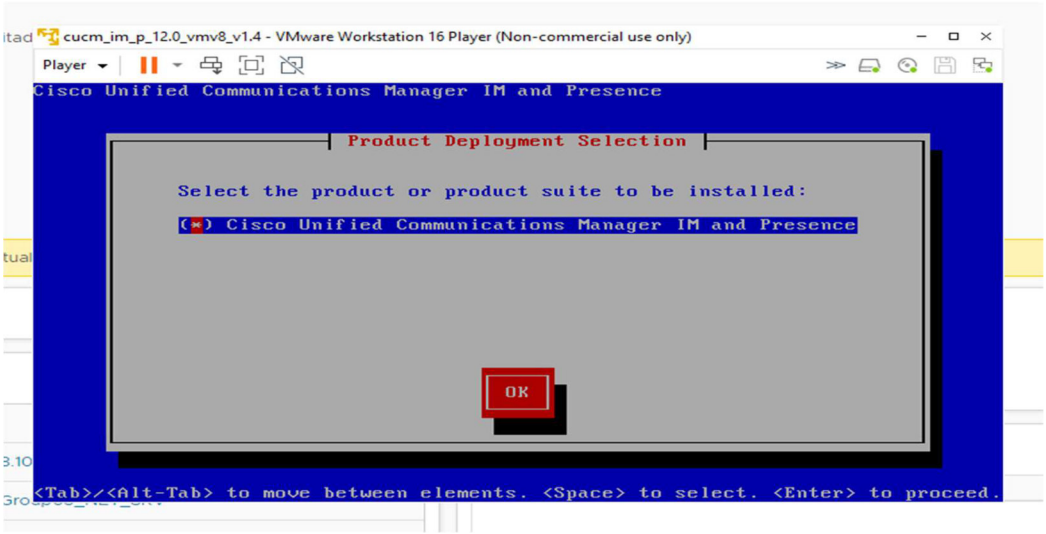


Figura 2.74 Configuración CUP

La información para completar la configuración se encuentra en la Tabla 2.83.

Tabla 2.83 Características de configuración CUP

CARACTERÍSTICAS	ESPECIFICACIONES
FQDN	cup.tesisfesvip.com
IP de Administración	192.168.10.41
Máscara	255.255.255.0
Gateway	192.168.10.254
NTP Server	192.168.10.254
Dominio	tesisfesvip.com
Usuario Local	Admin
Contraseña	f3svip2021
Usuario de Seguridad	Admin
Contraseña de seguridad	f3svip2021

Una vez completa la configuración se reinician los servicios y se validan que se encuentren operativos, tal como se puede observar en la Figura 2.75.

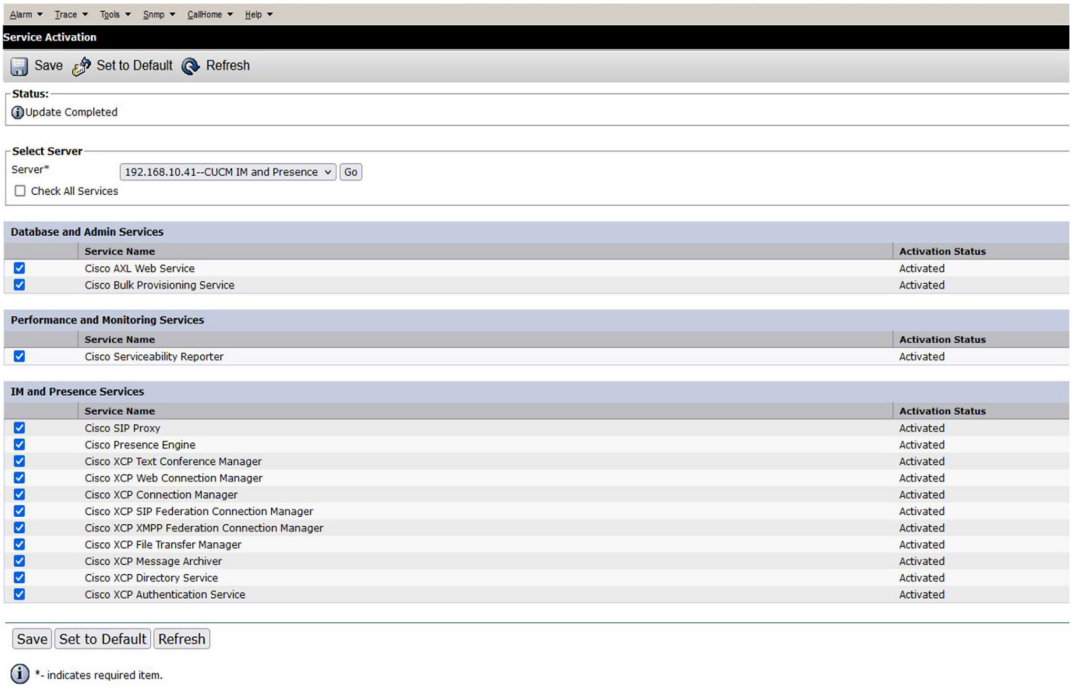


Figura 2.75 Validación de servicios CUP

2.4.8.3 Configuración de servidores de Telefonía IP

Previo a la creación de usuarios fue necesario realizar las configuraciones básicas en el CUCM para el correcto funcionamiento del servicio, pero antes de empezar en el servidor DNS se crean los registros respectivos para los servicios de telefonía, registros del tipo A y del tipo SRV (ver Figura 2.76).

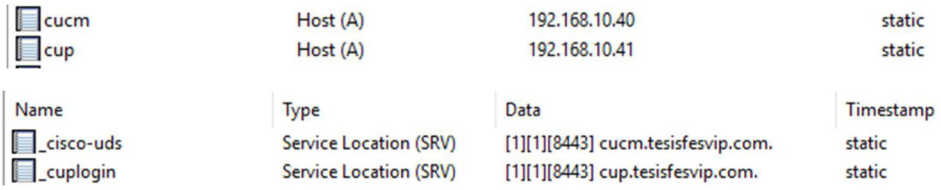


Figura 2.76 Registros DNS servicios telefonía IP

Para empezar, se realiza la integración con el servidor CUP, como se visualiza en la Figura 2.77.

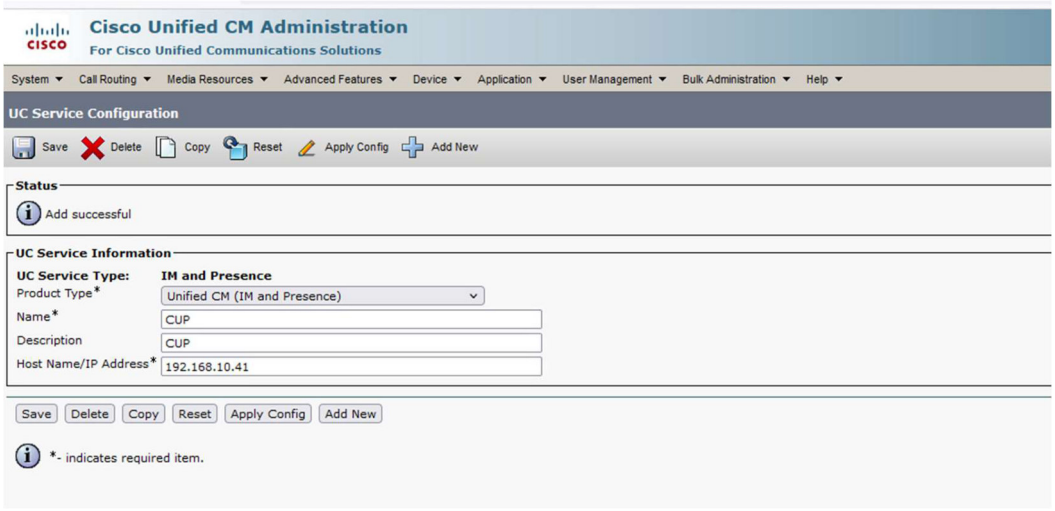


Figura 2.77 Integración con servidor CUP

Otra configuración necesaria fue la de la creación de los permisos de llamada, en el CUCM, lo cual se lo conoce como *Calling Search Space* (CSS); con esto se pudieron crear los perfiles de usuario con el permiso para llamadas internas, es decir entre extensiones, tal como se evidencia en la Figura 2.78.

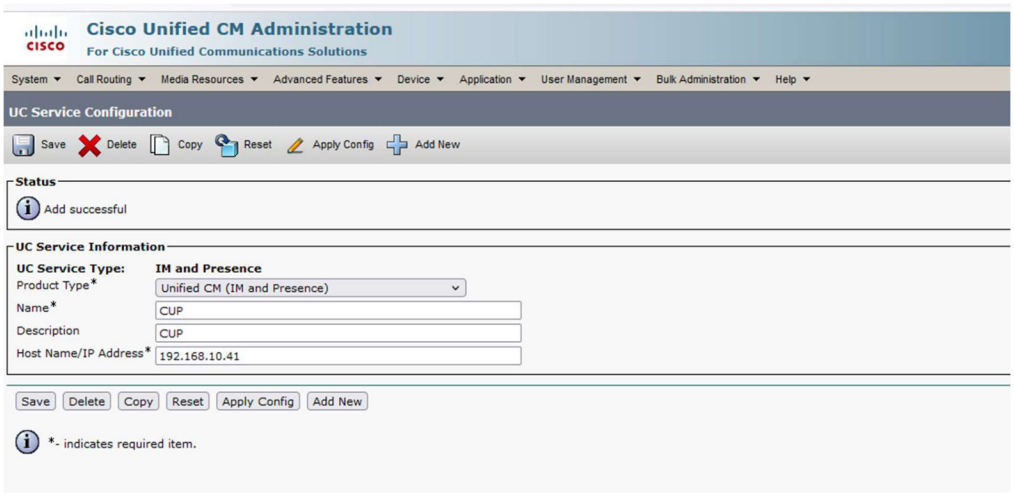


Figura 2.78 Integración CUCM y CUP

Para la autenticación y creación de usuarios en el CUCM, se realiza la integración con el Directorio Activo (ver Figura 2.79), esto a través del protocolo LDAP (*Lightweight Directory Access Protocol*); con esta configuración todos los usuarios que se encuentren en el Directorio Activo son creados en el CUCM y se programa una sincronización para que esté validando nuevos usuarios.

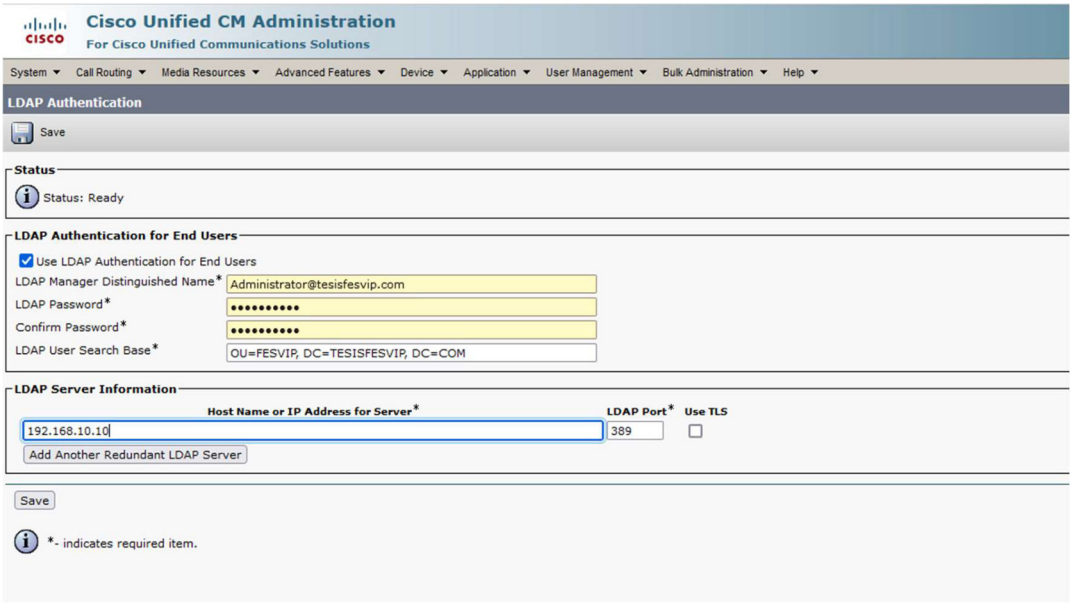


Figura 2.79 Integración con AD

2.4.8.4 Configuración de perfiles de usuario

Para la creación de perfiles en el CUCM, se deben considerar los diferentes escenarios que se podrían presentar para la creación de una extensión asociada a un usuario, ya que se puede tener: un teléfono IP físico, en un computador con un *softphone*, aplicativos en dispositivos móviles (Android y IOS).

Para esto Cisco en su CUCM ha desarrollado la creación de perfiles de dispositivos con la siguiente nomenclatura:

- ***Cisco Unified Client Services Framework* (CSF):** Creación de perfil de dispositivo para equipos que usan *softphones* en equipos Windows.
- ***Cisco Dual Mode for Android* (BOT):** Creación de perfil de dispositivo para equipos que usan dispositivos Android.
- ***Cisco Dual Mode for IOS* (TCT):** Creación de perfil de dispositivo para equipos que usan dispositivos IOS.
- **SEPXXXX:** Creación de perfil de dispositivo para un teléfono físico, en base a su número de serie (XXXX)

Cabe mencionar que el *softphone* o aplicativo preferido para trabajar con el CUCM es Jabber de propiedad de Cisco, pero también existe una integración con Webex.

Para la simulación de los servicios telefónicos en este proyecto se crean perfiles de dispositivos del tipo CSF para instalar el aplicativo en dispositivos Windows. Los perfiles creados se muestran en la Figura 2.80.

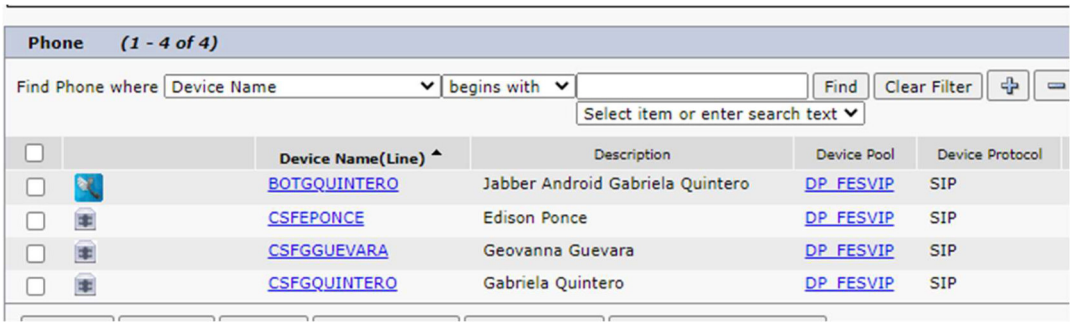


Figura 2.80 Perfiles creados

2.4.9 SIMULACIÓN DE VIDEOCONFERENCIA

Para la validación de servicios de videoconferencia, se logró obtener una prueba en el portal de Cisco Webex, la cual permitió generar un espacio en la nube de Webex para "FESVIP". Este licenciamiento además posibilitó evaluar todas las funcionalidades de la plataforma que básicamente ofrece su servicio como un SaaS.

Al tener acceso al portal de administración, se creó la prueba, tal como se indica en la Figura 2.81.

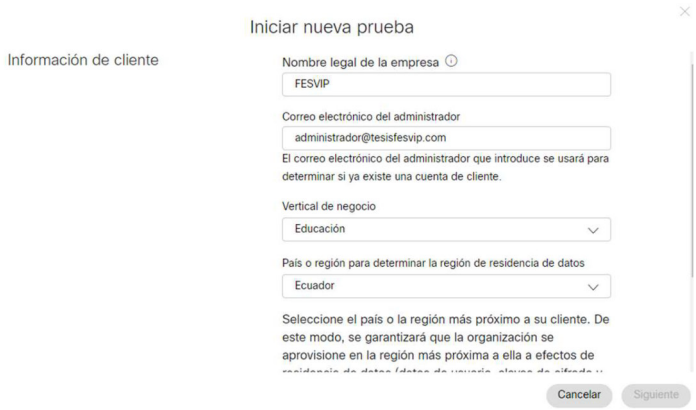


Figura 2.81 Configuración prueba Webex

La vertical de negocio es importante dentro del fabricante, ya que en base a esta se generan funcionalidades adicionales; por ejemplo, en la vertical de educación se crea la opción automática de generar subgrupos dentro de una videoconferencia, función muy útil en el sector educativo.

Los principales servicios que se habilitaron en la prueba fueron (ver Figura 2.82):

- Mensajería
- Reuniones avanzadas
- Webex Meeting

Figura 2.82 Servicios de Webex

Todas estas funcionalidades fueron habilitadas para 100 usuarios dentro del espacio de Webex para “FESVIP”, tal como se muestra en la Figura 2.83.

Figura 2.83 Número de licencias

El espacio creado por Webex para “FESVIP” tiene la siguiente URL de acceso: *https://fesvip.webex.com* (ver Figura 2.84).

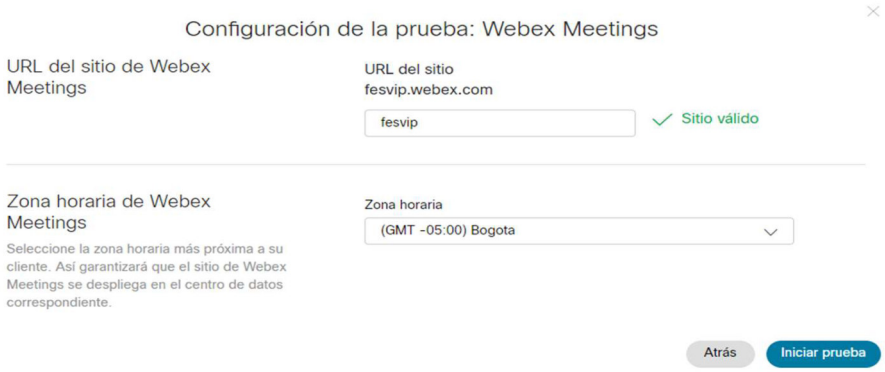


Figura 2.84 URL de sitio Webex creado

Una vez creado el espacio de Webex, se crean 2 usuarios (ver Figura 2.85), con los cuales se realizan varias pruebas de los servicios ofrecidos por Webex.

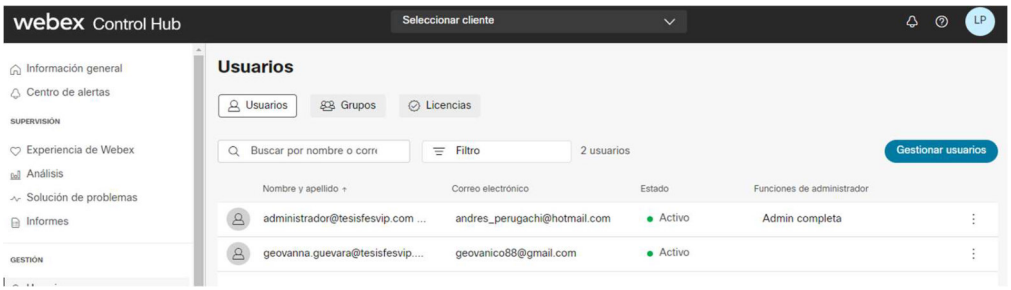


Figura 2.85 Usuarios creados Webex

2.4.10 SIMULACIÓN DE LA SEGURIDAD PERIMETRAL

Para la simulación de la seguridad perimetral se considera la marca FORTINET, al ser una marca líder en el cuadrante de Gartner en el año 2021 y al tener la disponibilidad de usar su software para ser implementado en un ambiente virtual.

La limitante que se tiene para la simulación es que la licencia demo que se genera para implementar el ambiente virtual dura solamente 15 días, por lo que de ser necesario se generarán varios despliegues y cargas de *Backups* de configuración en la simulación.

Una vez obtenidos los archivos de configuración para desplegar un FortiGate en un ambiente virtual, se procede con el despliegue en el ambiente VMware; la versión de fortiIOS obtenida fue la 7.0 y los archivos necesarios fueron:

- FortiGate-VM64.hw07_vmxnet3.ovf
- datadrive.vmdk
- fortios.vmdk

Se crea la máquina virtual en base a esta plantilla y a sus respectivos discos virtuales, tal como se observa en la Figura 2.86 (estos archivos fueron obtenidos directamente de la página del fabricante y son los necesarios para el despliegue en un ambiente virtual).

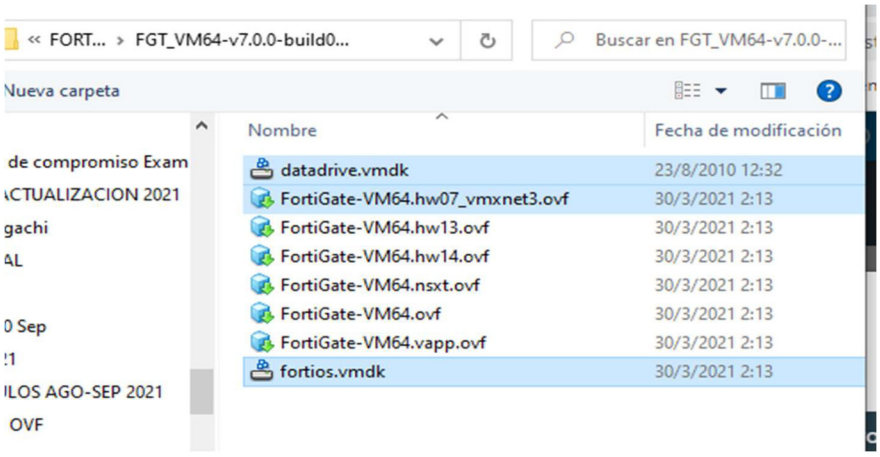


Figura 2.86 Creación máquina virtual *firewall*

Generada la máquina virtual, se enciende para ejecutar y configurar algunas de las características mostradas en la Tabla 2.84 y en la Figura 2.87.

Tabla 2.84 Características de la máquina virtual

CARACTERÍSTICAS	ESPECIFICACIONES
Procesador	1 VCPU
Memoria RAM	2 GB
Disco Duro 1	30 GB
Adaptadores de Red	2 adaptadores de red
Sistema Operativo	Other 3.x Linux (64-bit)
FQDN	FW-TESISFESVIP
IP puerto1 - SALIDA INT	192.168.100.221
Máscara	255.255.255.0
Gateway	192.168.100.1
IP puerto2 - RED 200	192.168.200.1
Máscara	255.255.255.252
Gateway	192.168.200.2
Dominio	tesisfesvip.com
Usuario Local	Admin
Contraseña	fesvip123
Accesos Permitidos para la administración	SSH, http, https

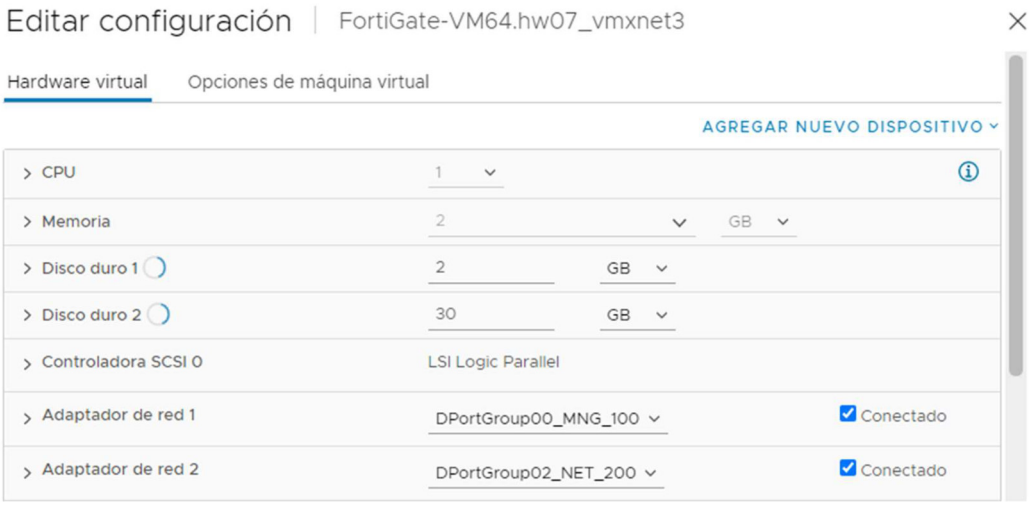


Figura 2.87 Configuración máquina virtual *firewall*

Una vez configurados los parámetros principales, se accede a la consola de administración Web para las demás configuraciones (ver Figura 2.88).

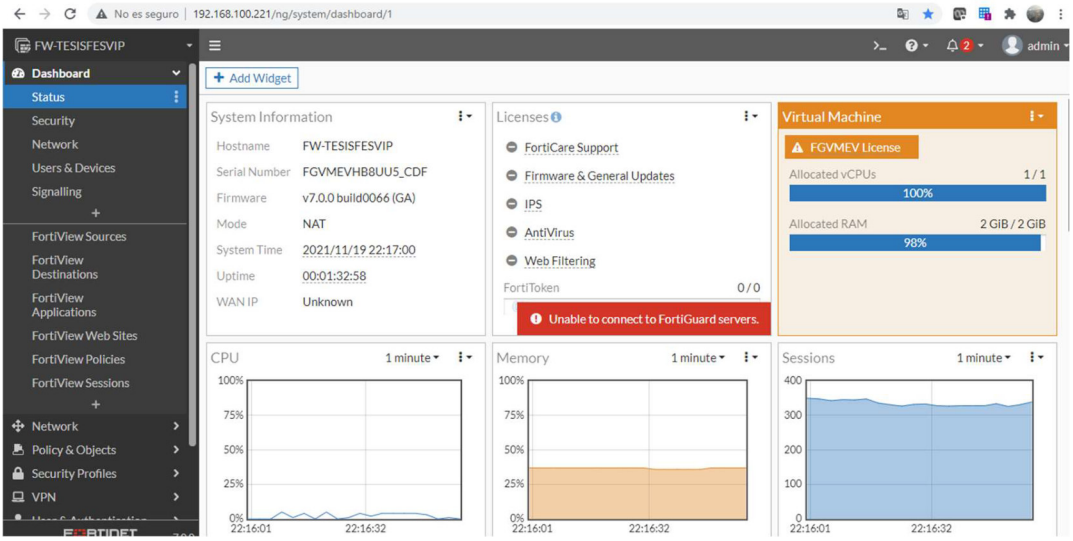


Figura 2.88 Panel de administración *firewall*

2.4.10.1 Configuración de *firewall*

Además de las configuraciones realizadas a nivel de consola para el acceso al *firewall* virtual, se consideran los siguientes puntos para la simulación y validación de permisos de navegación a través de la consola de administración web:

- **Interfaces de red virtuales**: fueron configuradas de acuerdo con el diagrama de conectividad planteado para la simulación (ver Figura 2.89).

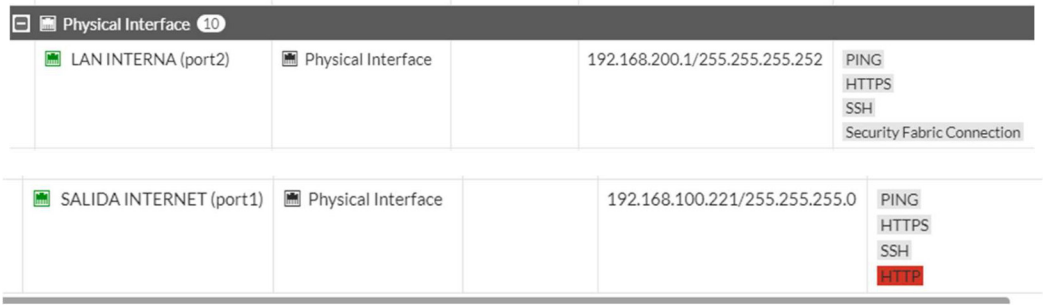


Figura 2.89 Interfaces de *firewall*

- **Rutas estáticas**: se crean para las diferentes subredes en la simulación mostrada, incluida la ruta por defecto, como se puede observar en la Figura 2.90.

Destination	Gateway IP	Interface	Status	Comments
IPv4 7				
0.0.0.0/0	192.168.100.1	SALIDA INTERNET (port1)	Enabled	RUTA POR DEFECTO
192.168.10.0/24	192.168.200.2	LAN INTERNA (port2)	Enabled	NET_SERVIDORES
192.168.20.0/24	192.168.200.2	LAN INTERNA (port2)	Enabled	NET_ADM
192.168.30.0/24	192.168.200.2	LAN INTERNA (port2)	Enabled	NET_DOCENTES
192.168.40.0/24	192.168.200.2	LAN INTERNA (port2)	Enabled	NET_ESTUDIANTES
192.168.50.0/24	192.168.200.2	LAN INTERNA (port2)	Enabled	NET_LAB01
192.168.60.0/24	192.168.200.2	LAN INTERNA (port2)	Enabled	NET_LAB02

Figura 2.90 Rutas estáticas

- **Perfiles de Seguridad:** Se crean para validar los servicios adicionales del *firewall* Fortinet. Cabe mencionar que estos perfiles no funcionan si no se cuenta con una licencia válida. Dentro de los perfiles de seguridad se tiene en todas las opciones perfiles por defecto, por ejemplo, para Antivirus, Web *Filter*, *Application Control*, *Video Filter*, IPS (ver Figura 2.91), *SSL Inspection*, entre otros.

Name	Comments
IPS all_default	All predefined signatures with default setting.
IPS all_default_pass	All predefined signatures with PASS action.
IPS default	Prevent critical attacks.
IPS high_security	Blocks all Critical/High/Medium and some Low severity vulnerabilities
IPS protect_client	Protect against client-side vulnerabilities.
IPS protect_email_server	Protect against email server-side vulnerabilities.
IPS protect_http_server	Protect against HTTP server-side vulnerabilities.
IPS wifi-default	Default configuration for offloading WiFi traffic.

Figura 2.91 Configuración de perfil IPS

- **Políticas de navegación:** Se crean con el fin de permitir o denegar el tráfico de las diferentes redes configuradas como objetos dentro del *firewall* virtual. En las políticas de seguridad también es donde se aplican los diferentes perfiles de seguridad.

  Para la simulación se crean políticas de navegación en base a los segmentos de red generados (ver Figura 2.92).

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log
LAN INTERNA (port2) → SALIDA INTERNET (port1) 6								
POL_CUCM_CUP	SRV_CUCM SRV_CUP SRV_CMS	NET_MNG	always	ALL	ACCEPT	Disabled	AV default IPS default SSL no-inspection	All
POL_SRV	SRV_AD SRV FILESERVER SRV ZIMBRA SRV VEEAM BACKUP	all	always	ALL	ACCEPT	Disabled	AV default IPS default SSL no-inspection	All
POL_NET_ADM	NET_ADM	all	always	ALL	ACCEPT	Disabled	AV default WEB default SSL no-inspection	All
POL_NET_DOCENTES	NET_DOCENTES	all	always	ALL	ACCEPT	Disabled	AV default WEB monitor-all SSL no-inspection	All
POL_NET_ESTUDIANTES	NET_ESTUDIANTES	all	SCHEDULE_ESTUDIANTES	ALL	ACCEPT	Disabled	AV default WEB WF_ESTUDIANTES APP AC_ESTUDIANTES SSL certificate-inspection FF default	All
POL_NET_LABS	NET_LAB01 NET_LAB02	all	always	ALL	ACCEPT	Disabled	AV default WEB default SSL no-inspection	All

Figura 2.92 Políticas de navegación

2.4.11 SIMULACIÓN DE ESTACIONES DE TRABAJO POR ÁREA

Para la simulación de estaciones de trabajo en las diferentes áreas, se crean VM en el ambiente VMware, con el sistema operativo w*indows* 10 pro (ver Figura 2.93).

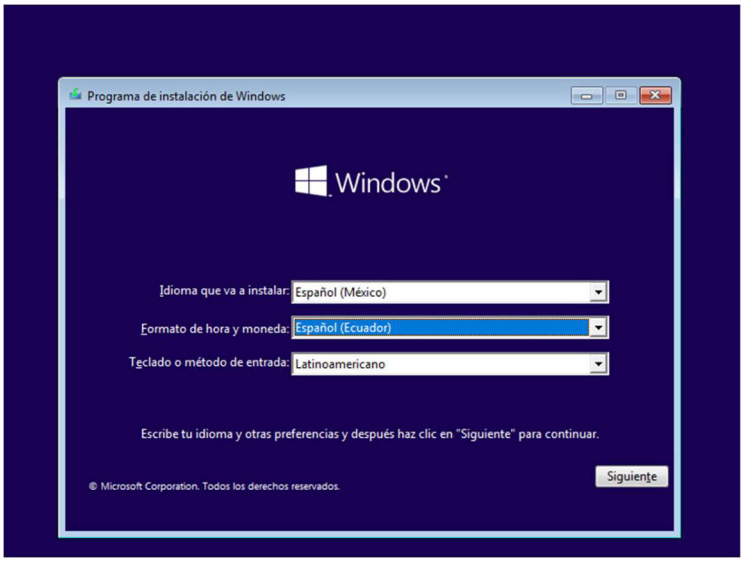


Figura 2.93 Instalación sistema operativo *windows* 10

Se crean 6 máquinas virtuales, que se indican en la Figura 2.94, con características mínimas (ver Tabla 2.85), donde se validan los servicios instalados.

Figura 2.94 Máquinas virtuales simuladas

Tabla 2.85 Características de máquinas virtuales simuladas

CARACTERÍSTICAS	ESPECIFICACIONES
Procesador	4 vCPU
Memoria RAM	8 GB
Disco Duro 1	50 GB
Adaptadores de Red	1 adaptador de red
Sistema Operativo	Windows 10

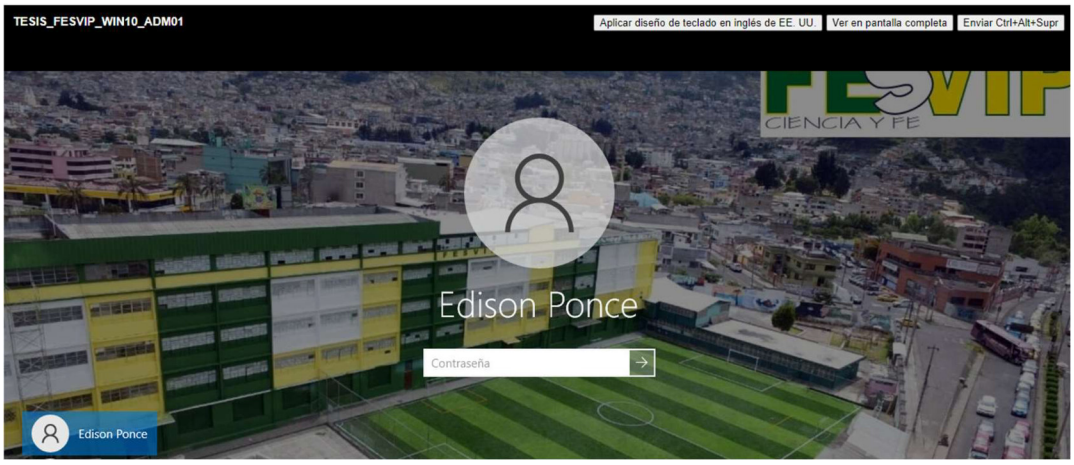


Figura 2.95 Estación de trabajo de usuario

3 RESULTADOS Y DISCUSIÓN

3.1 PRUEBAS DE FUNCIONAMIENTO

En las pruebas de funcionamiento se evalúa el desempeño de la simulación, a nivel de la red, así como de los servicios simulados.

3.1.1 CONECTIVIDAD DE RED

Para validar la conectividad y funcionamiento de la red, básicamente se utilizan los comandos *ping* y *tracert/traceroute* desde los servidores y equipos de trabajo, así como desde los equipos de conectividad (*switches)*, tal como se muestra en la Figura 3.2.

Se validan conexiones desde una máquina virtual conectada en la VLAN 20 (ver Figura 3.1), que es la VLAN para personal administrativo en la simulación, se valida el DHCP *server* y conectividad con otros segmentos de red y salida hacia Internet, de acuerdo con lo que se indica en la Figura 3.3.

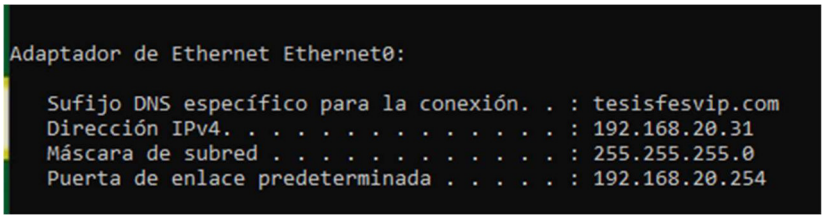


Figura 3.1 Direccionamiento IP VLAN20

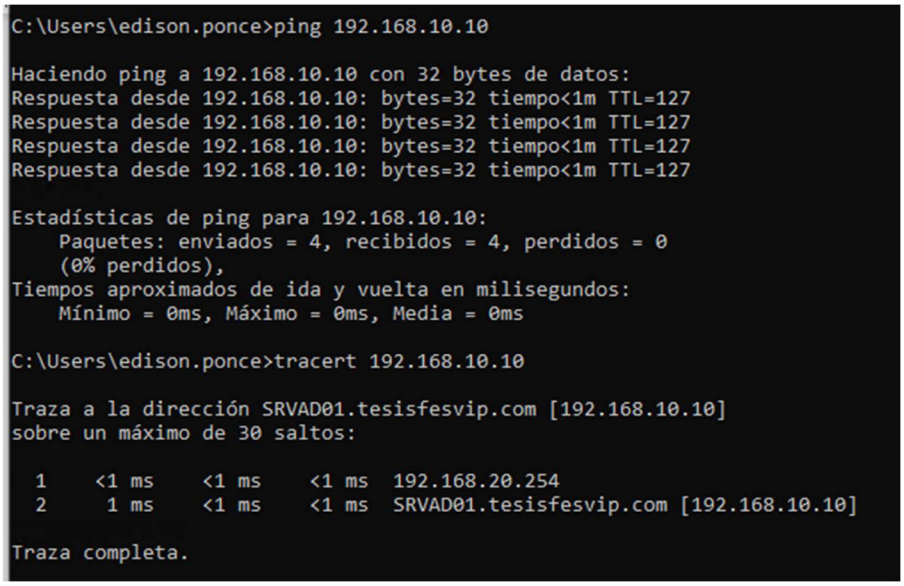


Figura 3.2 Ping y tracert hacia red de servidores

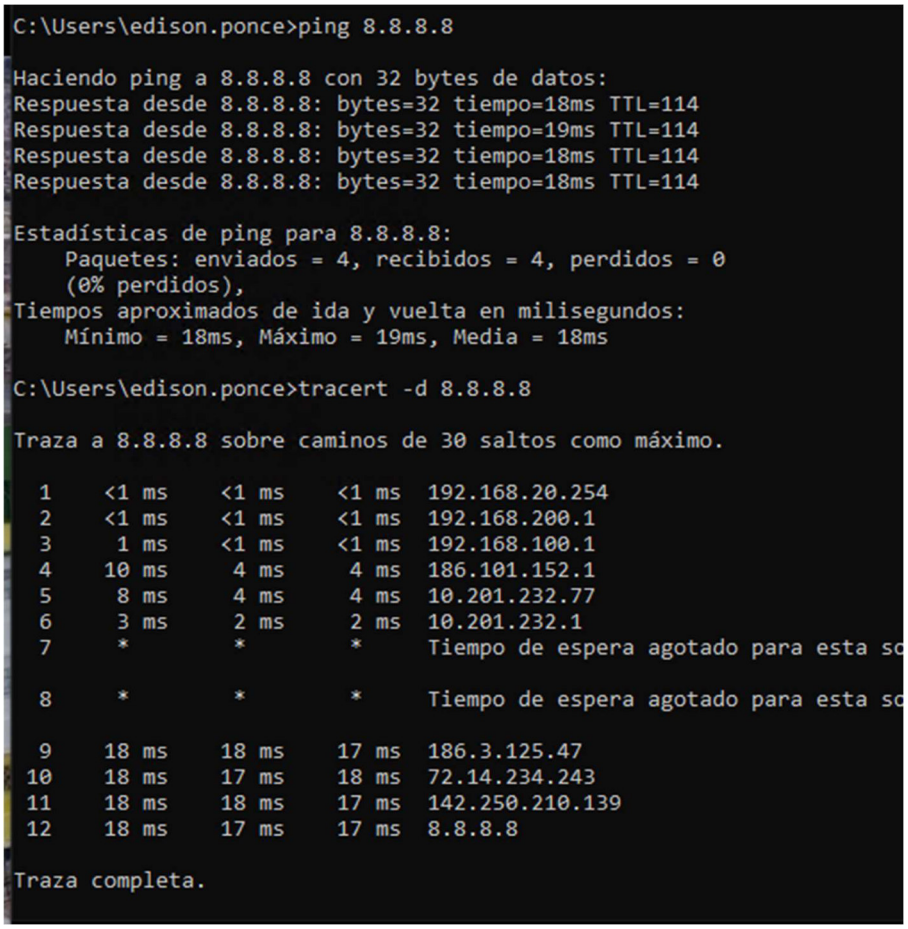


Figura 3.3 Ping y tracert hacia Internet

Desde la VLAN de servidores con ID de VLAN 10 (ver Figura 3.4) y el servidor que actúa como AD, DNS y DHCP se valida también la conexión hacia otras redes e Internet, de acuerdo con lo que se muestra en la Figura 3.5 y en la Figura 3.6.

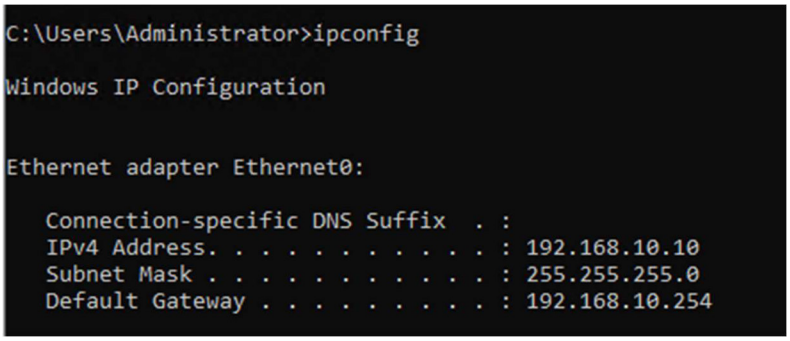


Figura 3.4 Direccionamiento IP servidor AD

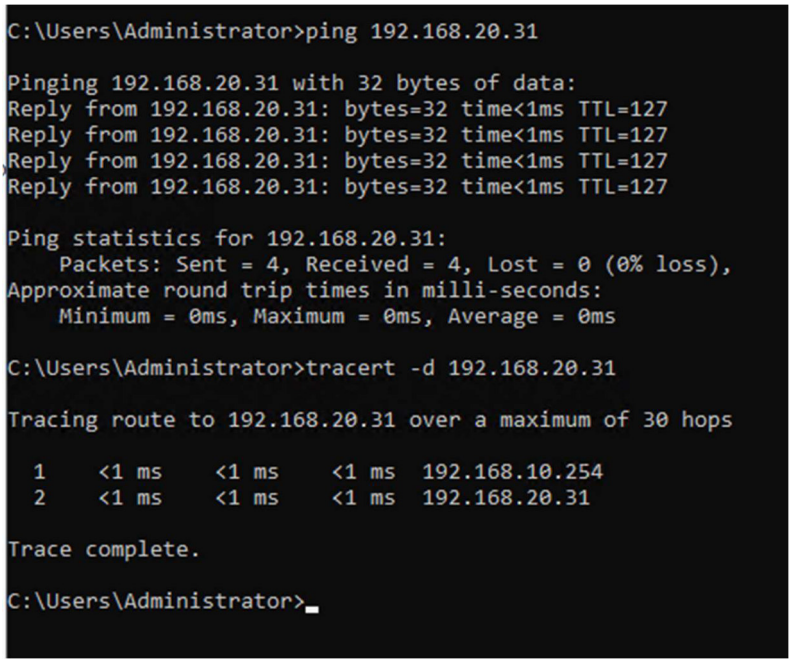


Figura 3.5 Ping y tracert hacia servidor VLAN20

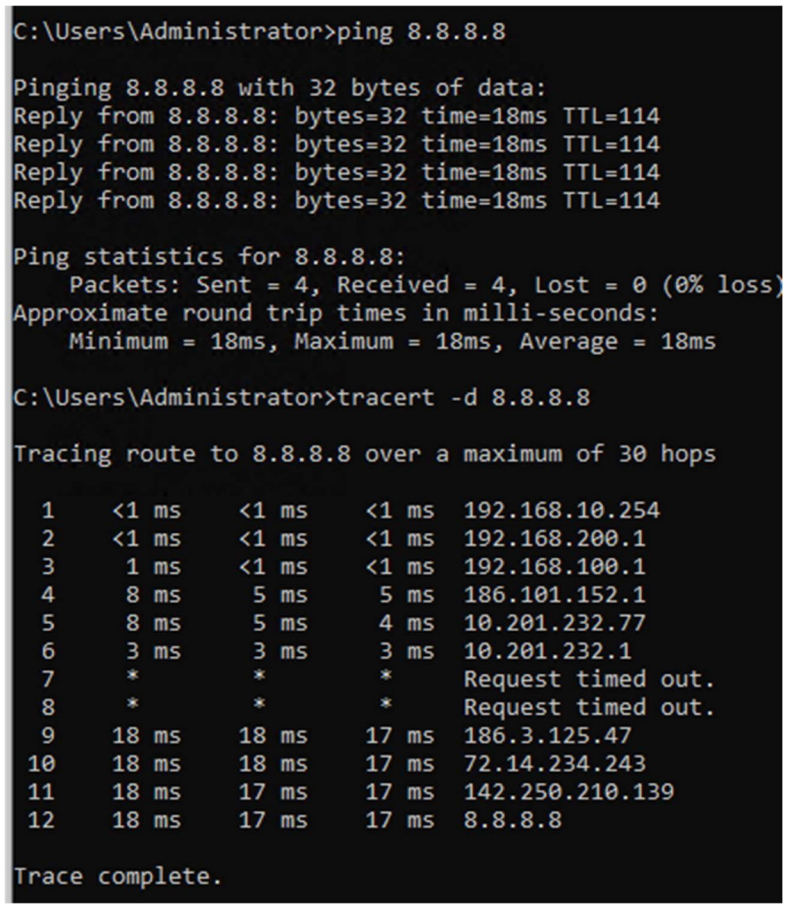


Figura 3.6 Ping y tracert hacia Internet

Adicionalmente, se realizan pruebas de conectividad desde el *switch* de *Core* (ver Figura 3.7) hacia algunas direcciones IP de equipos ubicados en diferentes segmentos y creados en la simulación.

```
SW_CORE#ping 192.168.10.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
SW_CORE#ping 192.168.20.31
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.31, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
SW_CORE#ping 192.168.50.31
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.31, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
SW_CORE#
```

Figura 3.7 Ping desde el *switch* de *core*

3.1.2 AD, DNS, DHCP

Para la validación de los servicios de AD, DNS y DHCP se realizan las acciones que se describen a continuación.

3.1.2.1 Creación de usuarios e ingreso de equipos al dominio

Se crean varios usuarios en las diferentes unidades organizativas, en el ejemplo se observa el usuario correspondiente al M.Sc. Edison Ponce, Rector de la Unidad Educativa “FESVIP”, Figura 3.8.

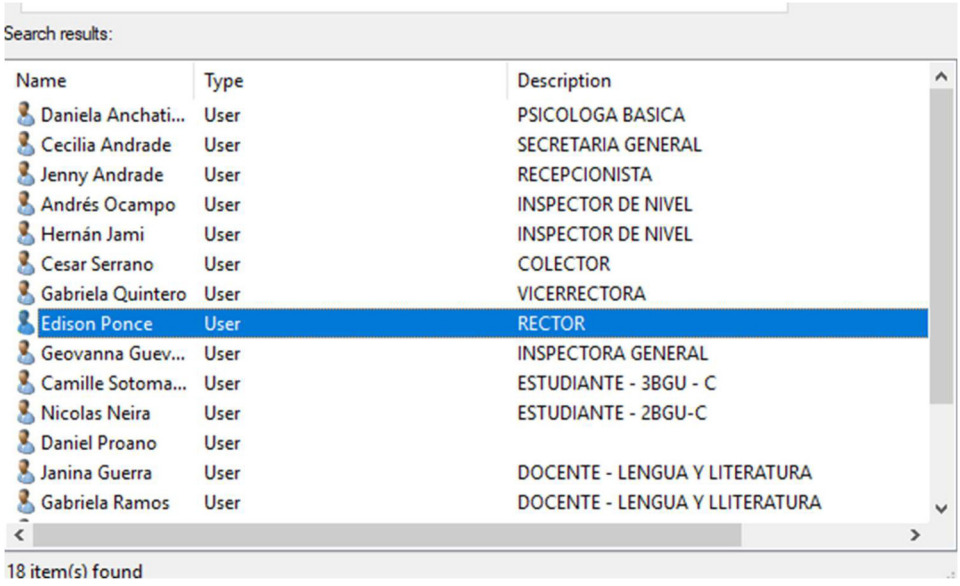


Figura 3.8 Usuarios creados dentro de AD

Una vez creados estos usuarios en el directorio activo, se procede a ingresar equipos al dominio para validar el acceso con su cuenta de usuario, donde adicionalmente se pueden observar los equipos ingresados, con la siguiente nomenclatura:

AUT-REC-EDP, ver Figura 3.9 (AUT: Unidad Organizativa - Autoridades, REC: Cargo - Rector, EDP: Nombre de la persona que usa el equipo - Edison Ponce)

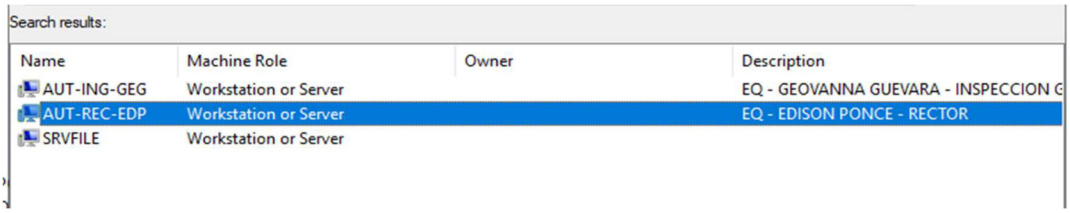


Figura 3.9 Estación de trabajo en dominio

Se valida el acceso de una máquina virtual creada e ingresada al dominio tesisfevip.com, con una cuenta de usuario (ver Figura 3.10 y Figura 3.11).

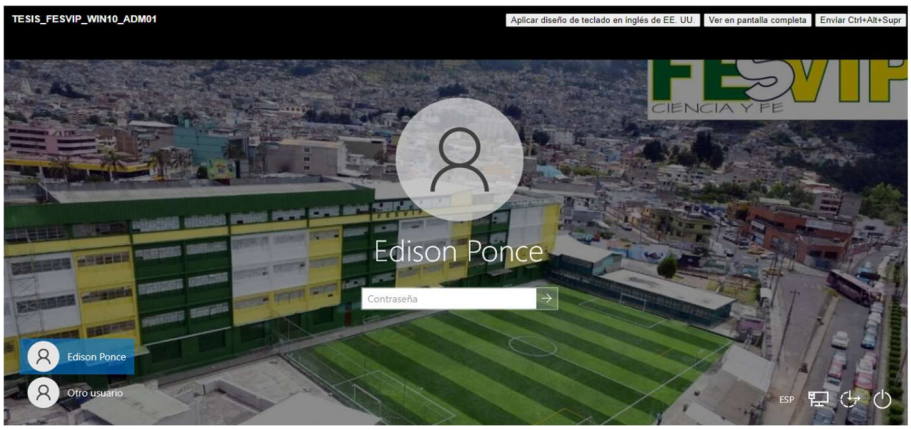


Figura 3.10 Máquina virtual con usuario de dominio

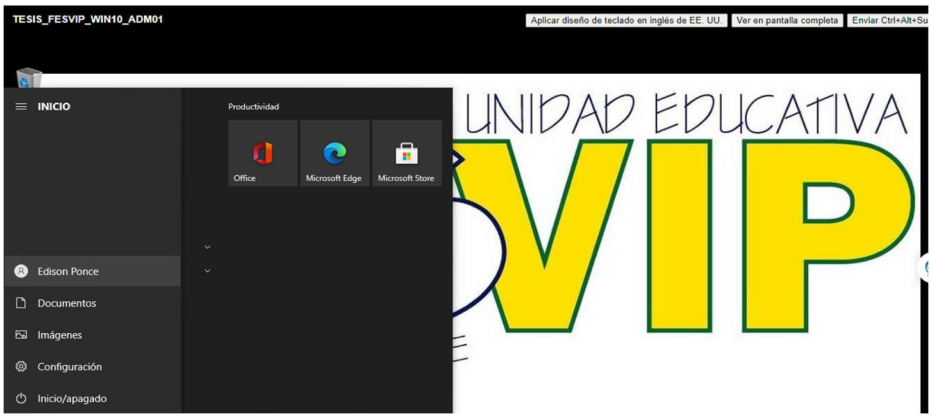


Figura 3.11 Escritorio de equipo virtual

Adicionalmente se puede validar la aplicación de una política de grupo a través del AD, donde se personaliza el fondo de escritorio y el protector de pantalla con imágenes de la Institución. Esto se configura para aplicar a todos los equipos que ingresen el dominio tesisfesvip.com.

Para la validación de DHCP, una vez agregado el equipo al dominio se configura en la interfaz VLAN del *switch* de *Core* el *ip helper-address* apuntando al servidor DHCP para que asigne una dirección IP del segmento deseado (ver Figura 3.12). En el ejemplo, se asigna una dirección IP del segmento de personal Administrativo al equipo configurado para el usuario Edison Ponce, como se puede observar en las Figura 3.13 y Figura 3.14 se ha asignado la IP 192.168.20.31 al equipo AUT-REC-EDP.

```
interface Ethernet0/1.20
 description NET_ADMINISTRATIVO
 encapsulation dot1Q 20
 ip address 192.168.20.254 255.255.255.0
 ip helper-address 192.168.10.10
```

Figura 3.12 Configuración VLAN20

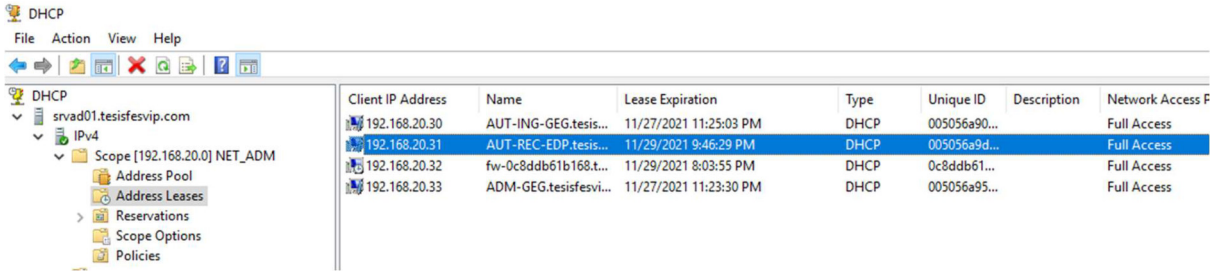


Figura 3.13 DCHP VLAN20

```
C:\Users\edison.ponce>ipconfig

Configuración IP de Windows


Adaptador de Ethernet Ethernet0:

   Sufijo DNS específico para la conexión. . : tesisfesvip.com
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.20.31
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 192.168.20.254

C:\Users\edison.ponce>_
```

Figura 3.14 Direccionamiento de equipo VLAN20

3.1.3 FTP

Para la verificación del servicio FTP o transferencia de archivos se crea una carpeta en el servidor por cada una de las áreas, con los permisos exclusivos de acceso al personal que pertenece a esa área. Para el ejemplo se crea una carpeta Rectorado donde solo tiene acceso de lectura y escritura el Rector y accesos de solamente lectura Vicerrectorado e Inspección General (ver Figura 3.15 y Figura 3.16).

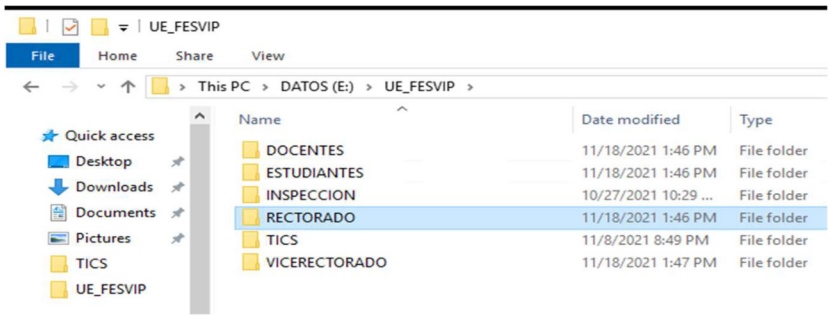


Figura 3.15 Subcarpetas creadas en servidor FTP

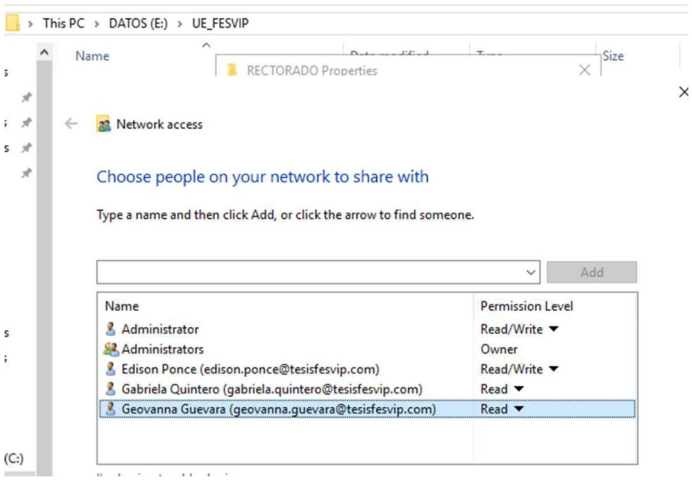


Figura 3.16 Permisos de acceso en una carpeta de FTP

3.1.4 CORREO ELECTRÓNICO

Para la validación de correo electrónico, como se mencionó, se crearon 3 cuentas, con las cuales se realizaron las diferentes pruebas de envío de correo.

- edison.ponce@tesisfesvip.com
- gabriela.quintero@tesisfesvip.com
- geovanna.guevara@tesisfesvip.com

A cada usuario se asignó una máquina virtual donde está configurada su cuenta. Se accede al portal de usuario de Zimbra vía Web, para el envío y recepción de correo (Ver Figura 3.17 y Figura 3.18).

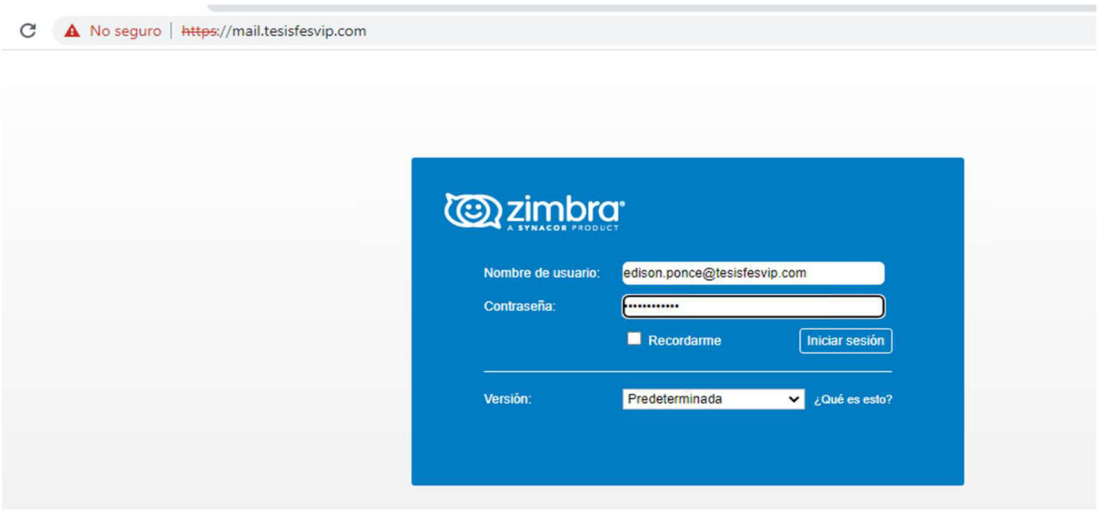


Figura 3.17 Portal de acceso a cuenta de usuario

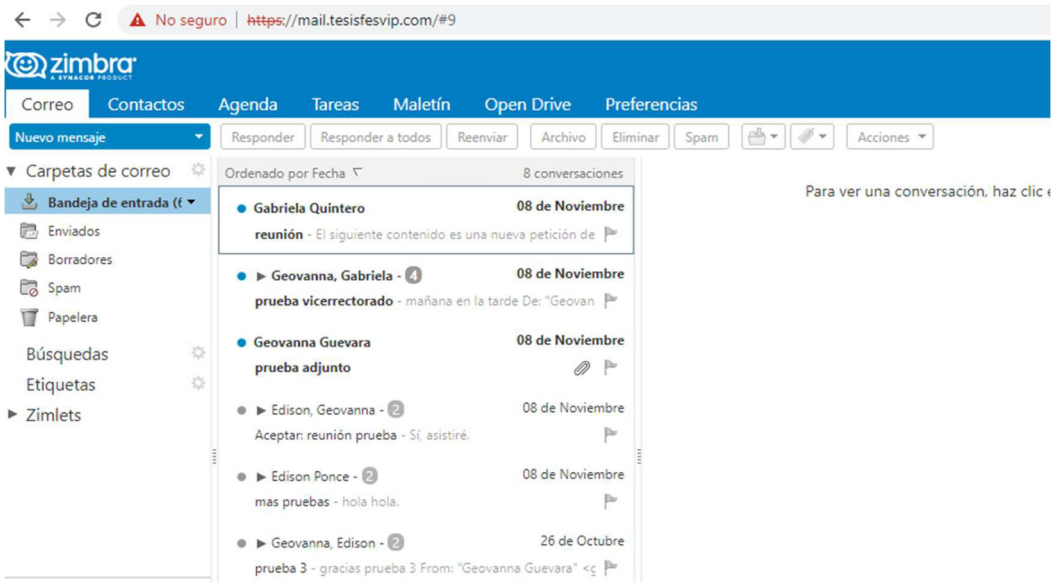


Figura 3.18 Bandeja de entrada del correo de un usuario

3.1.5 TELEFONÍA IP

Se verifica el funcionamiento del servicio de telefonía, generando 2 usuarios para el uso de este servicio; a la par se instala el software Jabber dentro de las máquinas virtuales de los usuarios, en primer lugar, se valida el inicio de sesión de los usuarios, tal como se muestra en las Figura 3.19 y Figura 3.20.

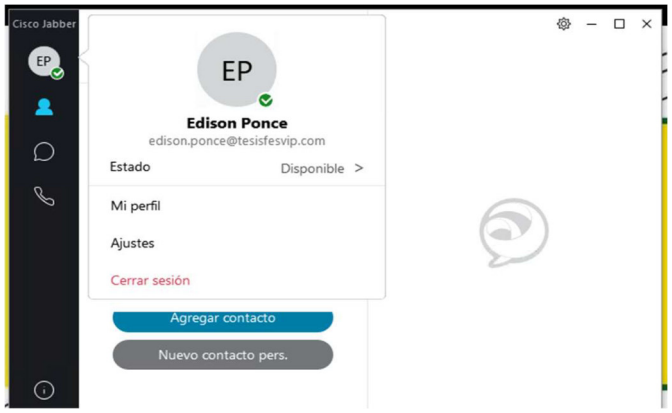


Figura 3.19 Aplicativo Jabber con perfil de Edison Ponce

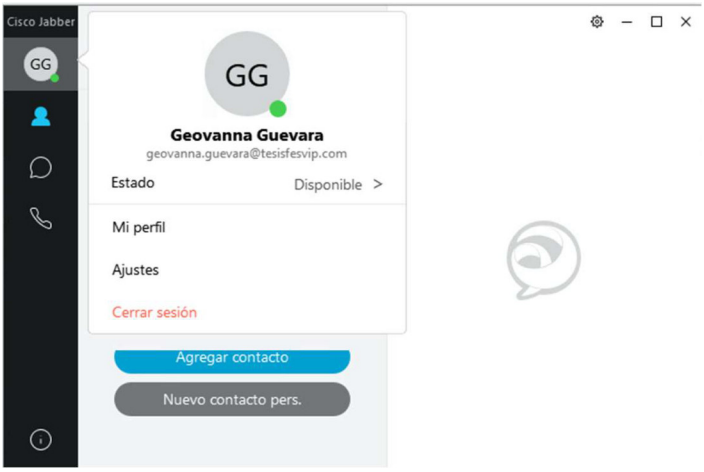


Figura 3.20 Aplicativo Jabber con perfil Geovanna Guevara

Posteriormente se verifica la llamada y el *chat* entre los usuarios Edison Ponce y Geovanna Guevara, tal como se muestra en la Figura 3.21.

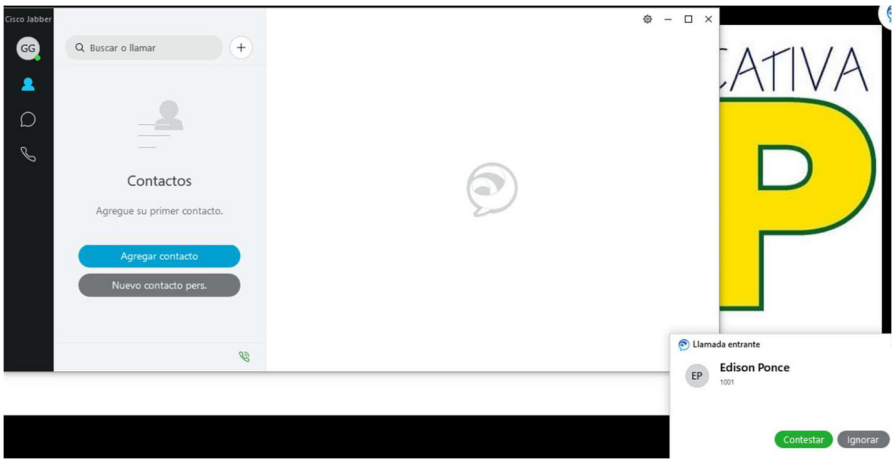


Figura 3.21 Validación de llamadas entre usuarios

3.1.6 VIDEOCONFERENCIA

Uno de los servicios ofrecidos por Webex, es mensajería instantánea, esto vía Web o a través de la aplicación Webex de Cisco, en la que se validan los servicios de *chat* entre los usuarios creados en la plataforma (ver Figura 3.22). Incluso se podrían agregar usuarios externos a la plataforma para interactuar.

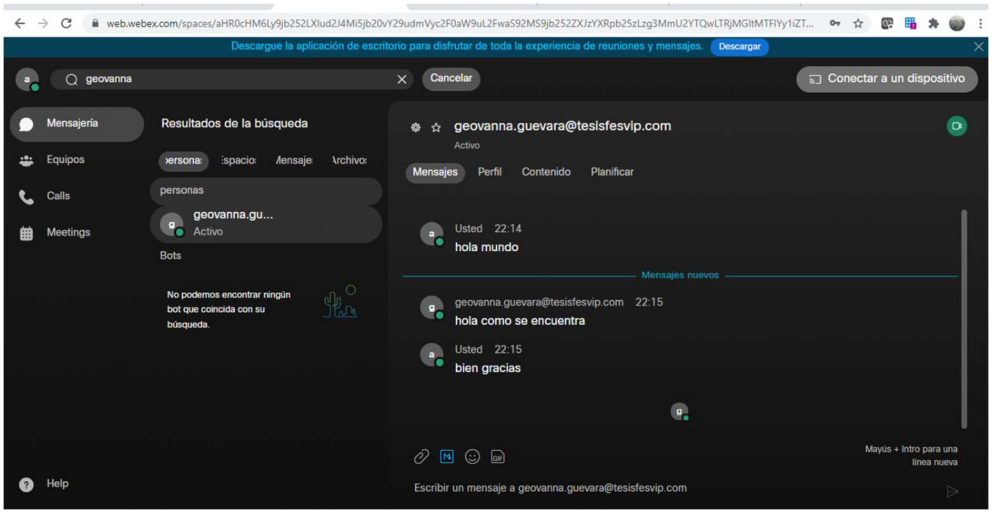


Figura 3.22 Chat en aplicación web

Desde la misma aplicación Webex, se realizan las validaciones de videollamadas (ver Figura 3.23); también se pueden comprobar funcionalidades como compartir pantalla, agregar invitados y los muy necesarios controles de audio y video.

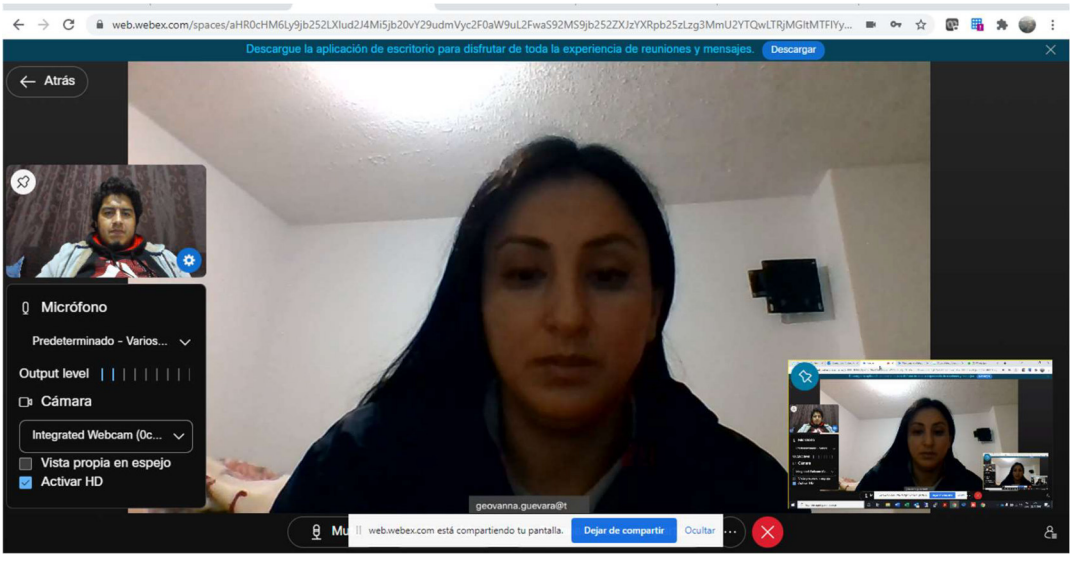


Figura 3.23 Videollamada desde aplicación web

La funcionalidad de la sala virtual personal es un sello de Cisco Webex Meeting y se incluye en la licencia de esta prueba; todos los usuarios que tengan esta licencia pueden acceder a su sala virtual personal para generar videoconferencias de hasta 1000 participantes (ver Figura 3.24).

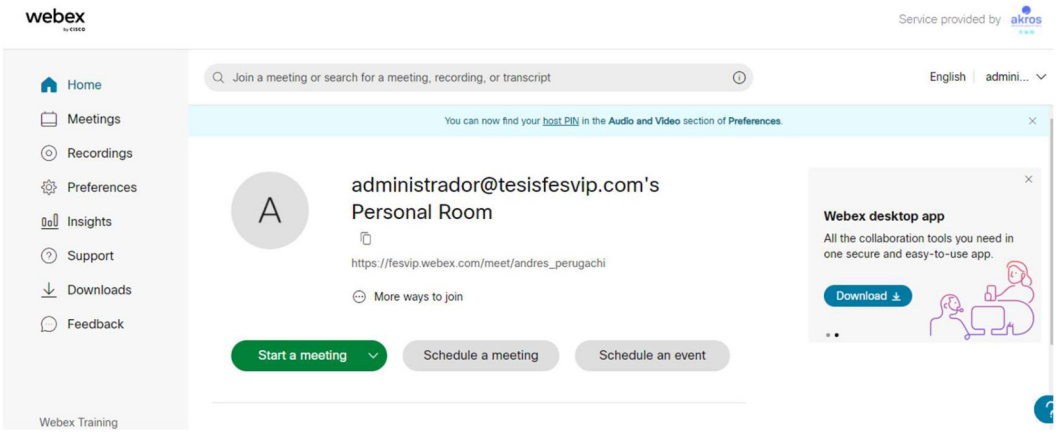


Figura 3.24 Sala virtual personal Webex

Se realiza una prueba con varios participantes en diferentes ubicaciones y dispositivos, los cuales pudieron acceder sin problemas a la sala virtual y tener una videoconferencia con todas las funcionalidades necesarias (ver Figura 3.25); entre estas se tienen:

- Creación de subsalas.
- Grabación de reuniones en la nube.
- Compartir contenido, incluso con audio del computador.

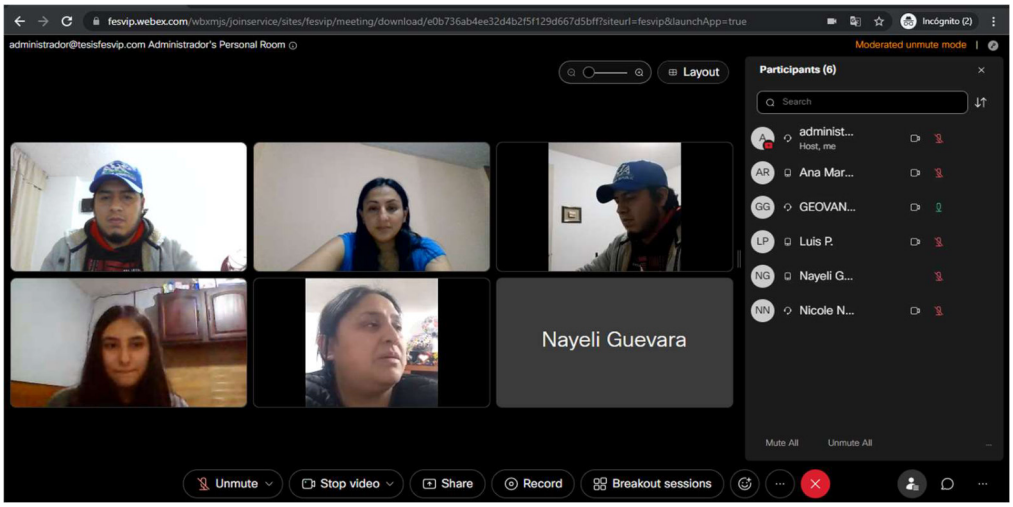
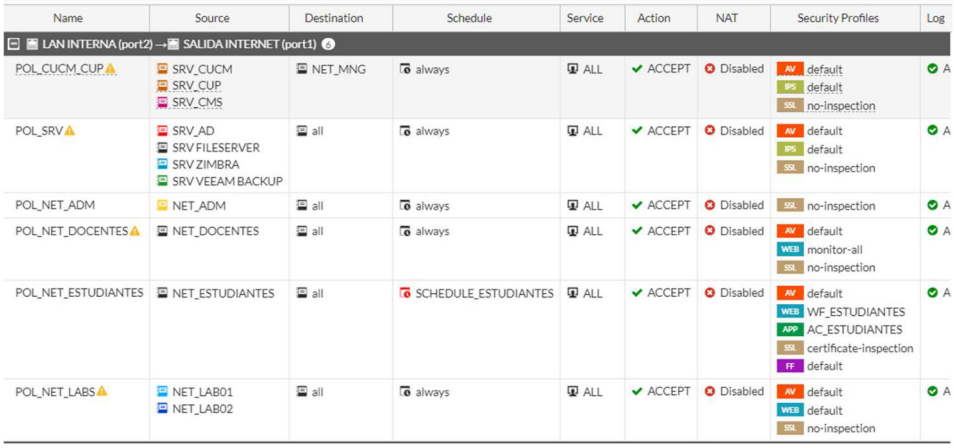


Figura 3.25 Reunión en sala virtual personal Webex

3.1.7 SEGURIDAD PERIMETRAL

Para la validación de la seguridad perimetral, se han generado varias políticas en base a las redes que se crearon para la simulación.

Como se puede observar en la configuración del equipo de seguridad perimetral *firewall* FortiGate, una vez generadas las políticas se revisan los *logs* para verificar que el tráfico está siendo monitoreado y aceptado o denegado según la configuración de la política (ver Figura 3.26).



Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log
LAN INTERNA (port2) → SALIDA INTERNET (port1) 6								
POL_CUCM_CUP	SRV_CUCM SRV_CUP SRV_CMS	NET_MNG	always	ALL	ACCEPT	Disabled	AV default IPS default SSL no-inspection	A
POL_SRV	SRV_AD SRV FILESERVER SRV ZIMBRA SRV VEEAM BACKUP	all	always	ALL	ACCEPT	Disabled	AV default IPS default SSL no-inspection	A
POL_NET_ADM	NET_ADM	all	always	ALL	ACCEPT	Disabled	SSL no-inspection	A
POL_NET_DOCENTES	NET_DOCENTES	all	always	ALL	ACCEPT	Disabled	AV default WEB monitor-all SSL no-inspection	A
POL_NET_ESTUDIANTES	NET_ESTUDIANTES	all	SCHEDULE_ESTUDIANTES	ALL	ACCEPT	Disabled	AV default WEB WF_ESTUDIANTES APP AC_ESTUDIANTES SSL certificate-inspection FF default	A
POL_NET_LABS	NET_LAB01 NET_LAB02	all	always	ALL	ACCEPT	Disabled	AV default WEB default SSL no-inspection	A

Figura 3.26 Políticas de *firewall*

Se puede observar en la Figura 3.27 como el tráfico de un equipo con dirección IP: 192.168.20.31 (VLAN 20 de personal Administrativo) está cayendo en la política POL_NET_ADM según lo configurado en el *firewall*, al hacer un filtro en los logs por dirección IP origen.

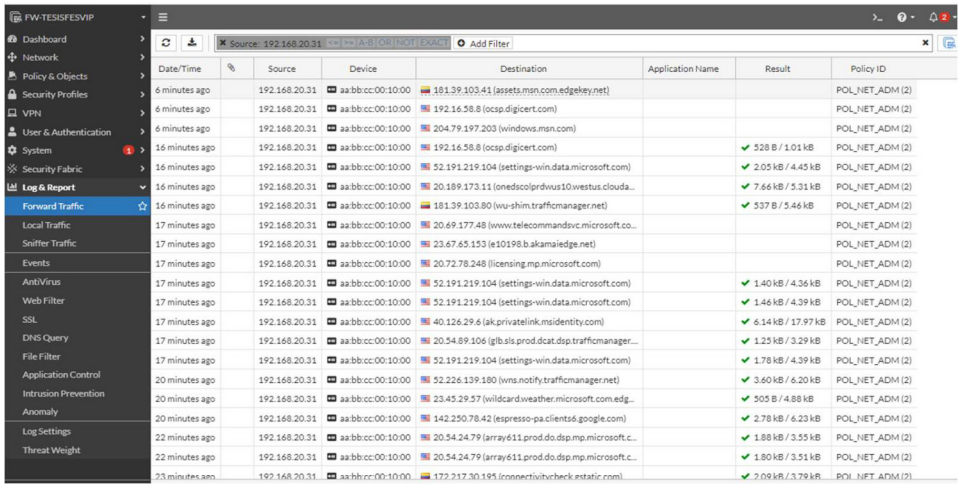


Figura 3.27 Logs de tráfico en *firewall* VLAN20

De igual manera se pudo verificar el tráfico que se origina en el servidor de AD hacia Internet y la política en la que cayó en el *firewall* (ver Figura 3.28).

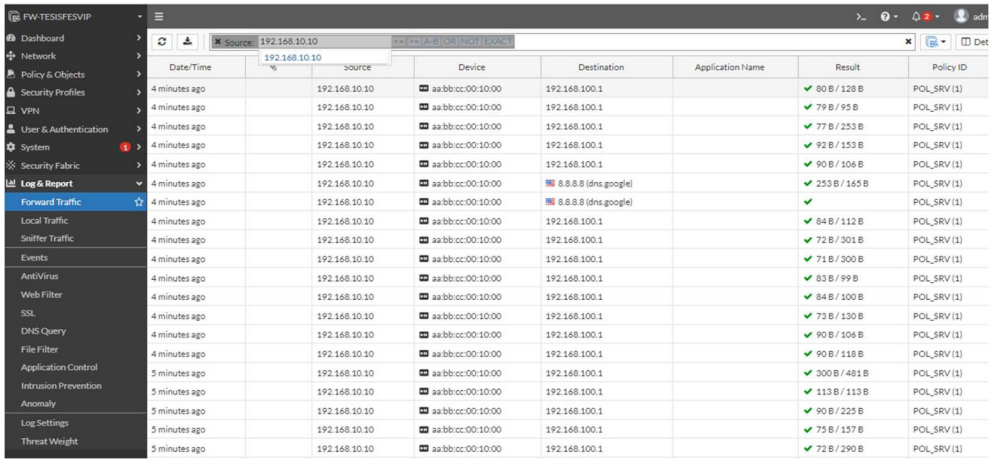


Figura 3.28 Logs de tráfico en *firewall* VLAN servidores

3.2 ANÁLISIS DE RESULTADOS

Una vez realizadas todas las pruebas de funcionamiento de cada uno de los componentes simulados en este proyecto, se debe realizar un análisis para determinar si la simulación se apega al diseño y si satisface las necesidades de la Unidad Educativa “FESVIP” por lo que a continuación se detalla lo encontrado.

Empezando por la simulación de la red, si bien es cierto que EVE-NG es un *software* robusto y permite a personal de TIC (Tecnologías de Información y Comunicaciones) realizar todo tipo de diseños, es importante mencionar que en la versión *Community*, existen limitaciones; una de las principales es que no todas las imágenes de dispositivos son accesibles y desplegables en el *software*, por lo que limita la simulación en ambientes más complejos y con otro tipo de dispositivos, por ejemplo, no se pudo encontrar y cargar una imagen de un dispositivo de red que soporte configuraciones de capa 2 y capa 3 (como los equipos físicos actuales), por lo que solamente se pudo configurar equipos bien en capa 2 (creación de VLAN) o bien en capa 3 (enrutamiento por configuración de interfaces). Por lo que en la simulación realizada en el SW_CORE que actúa como capa 3, se tuvo que configurar subinterfaces para simular las diferentes redes con sus respectivos ID de VLAN.

Adicionalmente en la versión *Community* de EVE-NG se puede configurar y simular hasta 9 interfaces físicas para las diferentes conexiones a otras redes, que, para el caso de este trabajo de titulación, fueron utilizadas para interconectar al *firewall* y hacia las distintas máquinas virtuales creadas en el ambiente VMware.

Por todo lo demás se pudo comprobar las principales funcionalidades del diseño, como: diseño jerárquico, creación de VLAN, ruteo e interconexión.

A nivel de simulación de los servicios adicionales que la Institución necesita, y que se evidenciaron en su levantamiento de requerimientos, se puede mencionar que, si no se contaba con un servidor con recursos suficientes para implementar un ambiente VMware y sobre él, las máquinas virtuales, no hubiese sido posible asemejar la simulación al diseño, ya que los recursos a nivel de *hardware* no hubiesen sido suficientes en un PC o *laptop*.

También es necesario mencionar que el trabajar en una empresa de prestación de servicios de tecnología ha facilitado en gran medida la obtención de las diferentes sistemas operativos, aplicaciones necesarias y licencias demo para la finalización exitosa de este proyecto, ya que para la gran mayoría de licencias y *software* propietario es necesario tener una cuenta de *partner* en cada uno de los portales del fabricante.

Una vez implementados los diferentes servicios con sus respectivas licencias demo, la configuración realizada es la necesaria para validar los servicios mencionados en el diseño, ya que, si se quieren explotar todas las funcionalidades de un servicio, llevaría varios meses el configurar y demostrar todos sus componentes y elementos.

Con lo descrito al momento, realizando una revisión de la simulación práctica y lo detallado en las pruebas de funcionamiento, se puede decir que la simulación ha logrado su objetivo de demostrar las principales funciones y características de cada uno de los servicios y que si la Unidad Educativa “FESVIP” en algún momento desea implementar este diseño podrá proveer de todos los servicios mencionados.

4 CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

- Del análisis de la situación actual en la Unidad Educativa “FESVIP”, se pudo determinar las fortalezas y debilidades a nivel tecnológico que esta presenta; se logró tener un panorama más amplio y con ello se levantó la línea base de requerimientos para diseñar una red convergente, servicios adicionales necesarios (AD, DHCP, DNS, FTP, Correo Electrónico, entre otros), cumpliendo con el objetivo principal de este trabajo, con el que se podrá alcanzar un adecuado proceso administrativo – educativo si es implementado en un futuro.

- Así mismo, el análisis de las necesidades actuales de comunicación a nivel de cableado estructurado permitió en el diseño, ubicar puntos de red tomando en cuenta la necesidad Institucional, el crecimiento de espacios de trabajo (aulas, departamentos, salas) y la cantidad de usuarios que podría haber a largo plazo, estimando un periodo de 10 años.

- Del análisis de la situación actual de y su posterior diseño, también se determinó que los materiales y equipos con los que cuenta actualmente la Unidad Educativa no presentan las condiciones necesarias para ser reutilizados a posteriori, tal es el caso del cableado estructurado y *switches*; la excepción es el sistema de video vigilancia en donde se reutilizarán las cámaras que la Institución posee, y se realizará solamente una reubicación e integración con la red convergente mediante una VLAN de video vigilancia.

- En el diseño de la red convergente se han evaluado los elementos que podrán ser utilizados en toda la Institución, tomando en cuenta que cumplan con una tecnología estándar, permitan escalabilidad, mantengan las características técnicas necesarias, proveyendo conectividad en toda la Institución, de tal manera que conociendo los costos referenciales y la disponibilidad en el mercado actual ya dependerá de las autoridades de la Institución y la situación en la que se encuentre, el poder implementar la solución planteada en este trabajo de titulación.

- Del diseño realizado, se concluye que es indispensable implementar la red convergente en la Unidad Educativa “FESVIP”, con el fin de mejorar procesos de comunicación, conectividad, así mismo en el área educativa permitirá dar un

paso más allá de una pizarra, al permitir trabajar con recursos digitales tal y como lo demanda la actualidad.

- El diseño propuesto para telefonía IP y videoconferencia en la Unidad Educativa, además de ser de última tecnología, mejorará la comunicación Institucional, ampliará los medios de contacto entre el personal, facilitará en gran medida el trabajo colaborativo y brindará flexibilidad laboral; por lo que es fundamental considerar implementar estas soluciones, que además no tienen ni punto de comparación con el sistema analógico y obsoleto que actualmente posee la Institución.

- Para los equipos de conectividad se solicitaron proformas con sus respectivas características, de las soluciones líderes en el mercado actual de acuerdo con el cuadrante mágico de Gartner 2021, estas fueron de los fabricantes CISCO y ARUBA y se determinó que ambas cumplen con los requerimientos tecnológicos mínimos para este diseño, diferenciándose únicamente por su precio, por lo que la toma de decisión para el trabajo radicó en el costo que implicaría para la Unidad Educativa la adquisición de estas soluciones.

- En este diseño no se contempla redundancia de *switches* de *Core,* por consideraciones netamente económicas una vez validadas las cotizaciones solicitadas, ya que el costo de implementación sería muy alto para la Institución, considerando el costo – beneficio, según conversaciones mantenidas con las autoridades.

- Aplicando el modelo jerárquico a nivel de distribución se estimaron dos *switches* que permitirán interconectar los *switches* de Acceso con el *Core* en los puntos más lejanos, realizando una correcta distribución que no impacte en el rendimiento de estos y manteniendo todos los beneficios del diseño como la facilidad de escalabilidad. Cabe mencionar que, en ciertos diseños, hablando prácticamente, no se considera la capa de Distribución con el propósito de minimizar los costos, generando así un modelo de dos capas en donde se tendrá una capa con las funciones de *Core* y Distribución conocido como "*Core* colapsado" que es aplicado generalmente a redes pequeñas.

- El *site survey* predictivo realizado en este diseño utilizando el portal de Aruba Networks, permitió definir la cantidad de *Access Point* por área en relación con un estimado de la intensidad de señal que estos emiten, basado en estándares

de la marca; con esto se garantizó la cobertura en todas las zonas definidas por las autoridades de la Institución. Cabe mencionar que este tipo de *site survey* predictivo es aplicable en cualquier diseño, considerando que los resultados son estimados.

- Si bien es cierto que la simulación permitió evaluar el diseño que se está realizando con sus principales funcionalidades, al aplicar y ejecutar un proyecto de esta magnitud con equipos físicos, los datos, características y modelos pueden variar lo que refleja que es un método válido, pero no exacto.

- Al utilizar la versión *Community* de EVE-NG se tuvieron limitantes que dificultaron de cierta manera el trabajo realizado, una de ellas fue la complejidad de cargar imágenes de diferentes equipos y marcas como por ejemplo la de Cisco *Catalyst,* para desarrollar de mejor manera la simulación a nivel de capa de Acceso; además de que a pesar de tener una interfaz gráfica para la creación de laboratorios, al ser un *software* basado en Linux es indispensable tener conocimientos básicos en comandos para poder utilizarlo y explotarlo adecuadamente.

4.2 RECOMENDACIONES

- La principal recomendación para la Unidad Educativa “FESVIP” una vez concluido el trabajo es la de considerar la implementación de este diseño que beneficiará en gran medida a toda la Institución y personal que necesita de todas estas mejoras para su labor diaria.

- De ser considerada la implementación de este diseño, se recomienda capacitar al personal para el uso de los nuevos servicios en la Institución y así puedan ser explotados de la mejor manera.

- La Unidad Educativa debe contar con personal que cumpla las funciones de administrador y operador de toda su infraestructura tecnológica, más aún si este diseño es implementando. Esto con el fin de realizar un manejo responsable, tomando en cuenta que existirán procesos los cuales no podrán ser manejados por cualquier empleado; incluso se puede considerar la contratación de servicios a terceros para los niveles más altos de soporte.

- La Institución necesita contar con una política de seguridad de la información en base a normas y estándares internacionales, la cual deberá ser desarrollada por

expertos en el tema y ser plasmada en un documento que a su vez deba ser implementada y socializada a los miembros de la comunidad educativa, para evitar de esta manera todos los riesgos, intrusiones y vulnerabilidades existentes en la actualidad.

- Se recomienda a la Institución adquirir un equipo de seguridad perimetral (*firewall*) lo más pronto posible, incluso si no se implementa este diseño, ya que al momento su infraestructura de red y sus usuarios se encuentran expuestos a los diferentes ataques existentes en la Internet.

- Si se implementa este diseño, en un futuro incluso se podrían implementar nuevos aplicativos en esta infraestructura, como por ejemplo el sistema de asistencia y notas de los estudiantes o la página Web de la institución que al momento se encuentra en un *hosting* externo.

- Si se implementa este diseño a nivel de red inalámbrica es recomendable realizar un *site survey* activo antes de la implementación, este nos brindará datos reales y exactos para la correcta ubicación de los *Access Point* y la cantidad necesaria requerida, además se podría considerar todo el campus de la Institución incluyendo las áreas de patios y cancha sintética de ser el caso.

- Para la administración y gestión inalámbrica es importante y se recomienda dotar de herramientas que permitan realizar este trabajo de manera centralizada, en el diseño por rapidez y facilidad se propuso instalar *Access Points* y configurar el principal como *manager,* pero ya existen plataformas incluso en la nube que permiten de manera rápida realizar esta actividad, por un costo adicional, por lo que, si se implementa este diseño, se recomienda en un futuro tomar en consideración lo mencionado.

5 REFERENCIAS BIBLIOGRÁFICAS

[1] EUATM, «REDES,» [En línea]. Available: http://www.edificacion.upm.es/informatica/documentos/redes.pdf. [Último acceso: octubre 2021].

[2] Universidad Internacional de Valencia, «Redes de datos, todo lo que hay que saber sobre ellas,» 09 octubre 2018. [En línea]. Available: https://www.universidadviu.com/ec/actualidad/nuestros-expertos/redes-de-datos-todo-lo-que-hay-que-saber-sobre-ellas.

[3] Digital Guide IONOS, «LAN — Red de área local: la tecnología de un vistazo,» Digital Guide IONOS, 02 marzo 2020. [En línea]. Available: https://www.ionos.es/digitalguide/servidores/know-how/lan/. [Último acceso: 2021].

[4] D. Hwang, «Red de área local o LAN,» ComputerWeekly, abril 2021. [En línea]. Available: https://www.computerweekly.com/es/definicion/Red-de-area-local-o-LAN. [Último acceso: 2021].

[5] Digital Guide IONOS, «Un aperçu des différents réseaux informatiques,» Digital Guide IONOS, 06 septiembre 2019. [En línea]. Available: https://www.ionos.fr/digitalguide/serveur/know-how/les-types-de-reseaux-informatiques-a-connaitre/. [Último acceso: 2021].

[6] L. Molero, «REDES DE AREA LOCAL,» Universidad Rafael Belloso Chacín, [En línea]. Available: https://www.urbe.edu/info-consultas/Web-profesor/12697883/archivos/Redes%20de%20Area%20Local%20y%20Metropolitana-cd2/Contenido/RedesdeDatos.pdf. [Último acceso: 2021].

[7] GPC, «Redes informáticas LAN, MAN, WAN: ¿Cuál es la diferencia entre ellas?,» GPC, 26 abril 2019. [En línea]. Available: https://gpcinc.mx/blog/redes-lan-man-wan/. [Último acceso: 2021].

[8] X. Hesselbach Serra y J. Altés Bosch, «Análisis de redes y sistemas de comunicación,» 2002. [En línea]. Available: https://books.google.com.ec/books?id=11DSMYYKvL0C&pg=PA26&dq=tipos+de+redes&hl=es-

419&sa=X&ved=2ahUKEwit9M7t9ZnyAhXeKDQIHbbcDWAQ6AEwAHoECAUQAg#v=onepage&q&f=false. [Último acceso: 2021].

[9] J. A. Ramón Bedoya, «DISEÑO Y SIMULACIÓN DE UNA RED INTEGRADADE VOZ Y DATOS PARA LA UNIDAD EDUCATIVA TEMPORAL “JAIME ROLDÓS AGUILERA”,» noviembre 2014. [En línea]. Available: https://1library.co/document/qmjrwowq-diseno-simulacion-integrada-unidad-educativa-temporal-roldos-aguilera.html. [Último acceso: 2021].

[10] S. Criollo , «Redes WLAN 2 parte,» 19 marzo 2012. [En línea]. Available: https://es.slideshare.net/santiagocriollo10119/redes-wlan-2-parte.

[11] etitudela, «Topologías de redes,» [En línea]. Available: http://www.etitudela.com/fpm/comind/downloads/topologiadered.pdf. [Último acceso: 2021].

[12] H. G. Colula Márquez y J. Lama Gervacio, «“Administración de Puertos TCP/IP como prevención de ataques”,» 25 enero 2012. [En línea]. Available: https://1library.co/document/1y9573jz-administracion-de-puertos-tcp-ip-como-prevencion-ataques.html.

[13] H. Lizarraga, «Redes convergentes,» 01 mayo 2015. [En línea]. Available: https://sites.google.com/site/cursoenlineaccna1/unidad-1-la/1-3-la-red-como-plataforma/1-3-3-redes-convergentes.

[14] cloudfare, «¿Qué es el modelo OSI?,» cloudfare, [En línea]. Available: https://www.cloudflare.com/es-es/learning/ddos/glossary/open-systems-interconnection-model-osi/. [Último acceso: 2021].

[15] M. d. C. Romero Ternero, «El Modelo de referencia OSI (ISO 7498),» 2004-2005. [En línea]. Available: https://www.dte.us.es/personal/mcromero/docs/arc1/tema2-arc1.pdf.

[16] Universidad Internacional de Valencia, «Explicando la arquitectura de protocolos TCP/IP,» Universidad Internacional de Valencia, 17 agosto 2016. [En línea]. Available: 16. https://www.universidadviu.com/es/actualidad/nuestros-expertos/explicando-la-arquitectura-de-protocolos-tcpip.

[17] A. Barrera, «CABLEADO ESTRUCTURADO: ¿QUÉ ES Y CUÁLES SON SUS ELEMENTOS?,» next_u, [En línea]. Available: https://www.nextu.com/blog/cableado-estructurado-que-es-y-cuales-son-sus-elementos/. [Último acceso: 2021].

[18] BIRTLH, «Subsistemas de cableado estructurado.,» BIRTLH, [En línea]. Available: https://ikastaroak.ulhi.net/edu/es/IEA/ICTV/ICTV10/es_IEA_ICTV10_Contenidos/Website_212_subsistemas_de_cableado_estructurado.html.

[19] A. Salguero, «Redes de áreas locales,» Blogger, 19 agosto 2011. [En línea]. Available: https://angello-salguero.blogspot.com/2011/08/cableado-horizontal.html.

[20] Montegar, «INSTALACIONES DE TELECOMUNICACIONES: ¿CUÁLES SON LOS ELEMENTOS QUE COMPONEN UN RACK?,» Montegar, 12 agosto 2020. [En línea]. Available: https://montegar.es/instalaciones-de-telecomunicaciones-cuales-son-los-elementos-que-componen-un-rack/.

[21] Djhiper, «Cableado estructurado,» 22 octubre 2017. [En línea]. Available: https://www.slideshare.net/djhiper/cableado-estructurado-81074759.

[22] TICS STEFFY, «CABLEADO,» TICS STEFFY, [En línea]. Available: https://steffyvicious.wordpress.com/redes/cableado/.

[23] G. Moreno, «Cableado estructurado,» 23 julio 2018. [En línea]. Available: https://www.slideshare.net/GIOVANNIMORENO3/cableado-estructurado-1. [Último acceso: 2021].

[24] S. D. Aspina Perdomo, «Medios de Transmisión,» 02 octubre 2011. [En línea]. Available: https://sites.google.com/site/redesatualcance/contact-us. [Último acceso: 2021].

[25] M. Fernández Barcell, «Medios de transmisión,» [En línea]. Available: https://rodin.uca.es/xmlui/bitstream/handle/10498/16867/tema05_medios.pdf. [Último acceso: 2021].

[26] Ismael, «Como funciona el cable par trenzado,» COMO FUNCIONA, 30 noviembre 2016. [En línea]. Available: https://comofunciona.co.com/el-cable-par-trenzado/.

[27] J. A. Castillo, «Fibra óptica: qué es, para qué se usa y cómo funciona,» Profesional Review, 19 febrero 2019. [En línea]. Available: https://www.profesionalreview.com/2019/02/15/fibra-optica-que-es/.

[28] Comunicandonos, «MEDIOS DE TRANSMISIÓN NO GUIADOS,» Comunicandonos, 2017. [En línea]. Available: https://comunicandonos2017.wordpress.com/medios-de-transmision-no-guiados/. [Último acceso: 2021].

[29] J. Joskowicz, «CABLEADO ESTRUCTURADO,» septiembre 2006. [En línea]. Available: https://bibdigital.epn.edu.ec/bitstream/15000/10009/1/Cableado%20Estructurado.pdf. [Último acceso: 2021].

[30] A. Sánchez, «¿Qué son Comunicaciones Unificadas?,» 3CX, 6 febrero 2018. [En línea]. Available: https://www.3cx.es/voip-sip/comunicaciones-unificadas/.

[31] A. Sánchez, «¿Qué es voz sobre IP(VoIP)?,» 3CX, 2018. [En línea]. Available: https://www.3cx.es/voip-sip/voz-sobre-ip/.

[32] J. A. Sánchez González, «Componentes y funciones VOIP,» Universidad Veracruzana, 29 febrero 2016. [En línea]. Available: https://www.uv.mx/universo/general/componentes-y-funciones-voip/. [Último acceso: 2021].

[33] P. Turmero, «Protocolos de Señalización y transmisión de Flujo Multimedia,» monografias.com, 24 marzo 2016. [En línea]. Available: https://www.monografias.com/trabajos107/protocolos-senalizacion-y-transmision-flujo-multimedia/protocolos-senalizacion-y-transmision-flujo-multimedia.shtml. [Último acceso: 2021].

[34] F. Matango, «Protocolos VoIp “ Señalización”,» SERVER VoIP, 19 agosto 2016. [En línea]. Available: http://www.servervoip.com/blog/protocolos-voip-senalizacion/. [Último acceso: 2021].

[35] J. Villalón, «VoIP: Protocolos de señalización,» SECURITY ART WORK, 20 febrero 2008. [En línea]. Available: https://www.securityartwork.es/2008/02/20/voip-protocolos-de-senalizacion/. [Último acceso: 2021].

[36] F. Matango , «Protocolos de Señalización de la VoIP,» SERVER VoIP, 26 septiembre 2016. [En línea]. Available: http://www.servervoip.com/blog/protocolos-de-senalizacion-de-la-voip/.

[37] Á. U. Munguía Vega, «Telemática,» [En línea]. Available: https://www.coursehero.com/file/81313092/KSG2-U1-A3-ANMVpdf/. [Último acceso: 2021].

[38] F. Matango, «Requisitos de tráfico en redes VoIP,» SERVER VoIP, 26 agosto 2016. [En línea]. Available: http://www.servervoip.com/blog/tag/calidad-servicio/.

[39] T. Chacin, «¿Qué es la conexión PSTN?,» Enlaces del caribe, 23 febrero 2018. [En línea]. Available: https://www.enlacesdelcaribe.com/la-conexion-pstn/. [Último acceso: 2021].

[40] A. Chacón Medina, «LA VIDEOCONFERENCIA: CONCEPTUALIZACIÓN, ELEMENTOS Y USO EDUCATIVO,» diciembre 2011. [En línea]. Available: https://www.ugr.es/~sevimeco/revistaeticanet/Numero2/Articulos/La%20videoconferencia.pdf. [Último acceso: 2021].

[41] CISCO, «¿Qué es la seguridad de red?,» CISCO, [En línea]. Available: https://www.cisco.com/c/es_mx/products/security/what-is-network-security.html. [Último acceso: 2021].

[42] «¿Qué es Active Directory? Conozca qué es AD y cómo funciona,» Quest, [En línea]. Available: https://www.quest.com/mx-es/solutions/active-directory/what-is-active-directory.aspx. [Último acceso: 2021].

[43] J. Diaz, «¿Que es DNS y como funciona?,» EXTASSIS NETwork, 11 junio 2019. [En línea]. Available: https://extassisnetwork.com/tutoriales/dns/. [Último acceso: 2021].

[44] M. Pérez , «Correo Electrónico,» Concepto Definición, 23 julio 2021. [En línea]. Available: https://conceptodefinicion.de/correo-electronico/. [Último acceso: 2021].

[45] F. Llordachs Marqués, «¿Qué son los servicios en la nube? Tipos y ejemplos,» Clinic Cloud, 2021. [En línea]. Available: https://clinic-cloud.com/blog/servicios-en-la-nube-tipos-ejemplos/. [Último acceso: 2021].

[46] namecheap, «Software para todo,» namecheap, [En línea]. Available: http://softwareparatodo.com/?ts=fERvbmF1X0R8fGExNjQ0fGJ1Y2tldDA5M3x8fHx8fDYxNzJiNzg3YmU2MmJ8fHwxNjM0OTA4MDM5Ljc5Njd8ZmIxMmYwODM0MWE5NDJiMzM2Y2JjODM0NGE1Y2M4MmQ3YWZiMTg4NHx8fHx8MXx8MHwwfHx8fDF8fHx8fDB8MHx8fHx8fHwwfDF8fDB8MHx8MHwwfGV5SnpkSGxzWlVsa0lqb2l. [Último acceso: 2021].

[47] TrueConf, «Protocolos de videoconferencia y desafíos comunes,» TrueConf, [En línea]. Available: https://trueconf.com/es/arquitectura-de-videoconferencia.html. [Último acceso: 2021].

[48] Telalca, «Grandstream,» Telalca, [En línea]. Available: https://www.telalca.com/grandstream/. [Último acceso: 2021].

[49] A. Sánchez , «Central Telefónica 3CX. Voz, Video y Chat,» 3CX, 2021. [En línea]. Available: https://www.3cx.es/centralita-telefonica/central/?src=centraltelefonicalatamads&gclid=CjwKCAjwn8SLBhAyEiwAHNTJbVx06Vy_F_OiGDKXkvPy-q4y2De1r8_Ac26LbLOTxiiwiMQVoxpHORoCozUQAvD_BwE.

[50] QUAREA, «¿Que es Asterisk?: Centralita telefónica IP,» QUAREA, [En línea]. Available: https://quarea.com/es/que-es-asterisk-centralita-telefonica-ip/. [Último acceso: 2021].

[51] UNIR, «Seguridad perimetral informática: objetivos y plataformas recomendables,» 30 julio 2020. [En línea]. Available: https://www.unir.net/ingenieria/revista/seguridad-perimetral-informatica/.

[52] GMS seguridad, «Seguridad de la información,» GMS seguridad, [En línea]. Available: https://gmsseguridad.com/partners/check-point/. [Último acceso: 2021].

[53] FortiGate, «Conociendo el *Firewall*,» QUANTI, 11 febrero 2021. [En línea]. Available: https://quanti.com.mx/articulos/conociendo-el-*Firewall*-fortigate/. [Último acceso: 2021].

[54] SOPHOS, «Sophos Anti-Virus para NetApp Storage,» marzo 2010. [En línea]. Available: https://www.sophos.com/es-es/medialibrary/PDFs/documentation/netapp_sen.pdf. [Último acceso: 2021].

[55] CLOUD COMPUTING, «¿Qué son los servicios de nube?,» Red Hat, [En línea]. Available: https://www.redhat.com/es/topics/cloud-computing/what-are-cloud-services. [Último acceso: 2021].

[56] vmware, «¿Qué es VMware Workstation?,» vmware, [En línea]. Available: https://www.vmware.com/mx/products/workstation-pro/faq.html. [Último acceso: 2021].

[57] RackOnline, «¿Cómo elegir un armario rack?,» RackOnline, [En línea]. Available: https://www.rackonline.es/content/como-elegir-un-armario-rack. [Último acceso: 2021].

[58] DINECOM, «Cuáles Son Los Componentes Clave De Una Videoconferencia,» DINECOM, 28 noviembre 2019. [En línea]. Available: https://dinecom.cl/blog/cuales-son-los-componentes-clave-de-una-videoconferencia/.

[59] SIAG CONSULTING, «Los 5 software de virtualización más utilizados,» SIAG CONSULTING, 31 mayo 2018. [En línea]. Available: https://siagconsulting.es/5-software-virtualizacion/.

[60] AYUDALEY, «Software de virtualización. Los 11 mejores,» AYUDALEY, 17 mayo 2021. [En línea]. Available: https://ayudaleyprotecciondatos.es/2021/05/17/software-de-virtualizacion/.

[61] Microsoft 365, «Microsoft 365 Educación,» Microsoft 365, [En línea]. Available: https://www.microsoft.com/en-us/education/buy-license/microsoft365.

[62] HOSTINGNET, «¿Qué es Zimbra?,» HOSTINGNET, 12 junio 2018. [En línea]. Available: https://hostingnet.cl/blog/que-es-zimbra/.

[63] Microsoft, «Servicios de correo empresarial,» Microsoft 365, [En línea]. Available: https://www.microsoft.com/es-ww/microsoft-365/exchange/email.

[64] GRANDSTREAM, «Características de Comunicaciones Unificadas Optimizadas para PyMEs,» GRANDSTREAM, [En línea]. Available: https://www.grandstream.com/hubfs/Product_Documentation/datasheet_ucm6200_series_spanish.pdf?hsLang=en.

[65] CISCO, «Hoja de datos de Cisco Unified Communications Manager versión 12.5,» CISCO, 19 diciembre 2020. [En línea]. Available: https://www.cisco.com/c/en/us/products/collateral/unified-communications/unified-communications-manager-callmanager/datasheet-c78-741428.html.

[66] mundocuentas, «Microsoft Teams: qué es, cómo funciona y cuáles son sus ventajas,» mundocuentas, [En línea]. Available: https://www.mundocuentas.com/microsoft/teams/.

[67] e-GATIC, «Webex, una herramienta de video para el trabajo colaborativo,» e-GATIC, 02 julio 2009. [En línea]. Available: https://www.icesi.edu.co/blogs/egatic/2009/07/02/Webex-una-herramienta-video-para-el-trabajo-colaborativo/.

[68] Capterra, «Software para call center / WebEx,» Capterra, [En línea]. Available: https://www.capterra.ec/software/733/Webex.

[69] arcadio, «SUBREDES VLSM,» 21 noviembre 2021. [En línea]. Available: https://arcadio.gq/php/reporte/reporte_VLSM_172.10.0.0_211121212546.pdf.

[70] FESVIP, «UNIDAD EDUCATIVA FERNANDEZ SALVADOR VILLAVICENCIO PONCE» [En línea]. Available: https://fesvip.edu.ec/.

[71] Cuadros, FR (2019, 15 de marzo). Estándares multigigabit (803.3bz 2.5 y 5 Gigas): Así funcionan Cloud Center Andalucía. https://www.cloudcenterandalucia.es/blog/estandares-multigigabit-803-3bz-2-5-y-5-gigas-asi-funcionan/

[72] Walton, A. (2018, 13 de enero). Implementación de un Diseño de Red . CCNA desde Cero. https://ccnadesdecero.es/implementacion-diseno-de-red/

[73] Hoja de datos de switches administrados apilables de la serie Cisco 550X . (2021, 22 de febrero). Cisco. https://www.cisco.com/c/en/us/products/collateral/switches/550x-series-stackable-managed-switches/datasheet-c78-735874.html

[74] SERIE DE INTERRUPTORES ARUBA 3810 . (Dakota del Norte). Arubanetworks.Com. Obtenido el 27 de diciembre de 2021 de https://www.arubanetworks.com/assets/ds/DS_3810SwitchSeries.pdf

[75] Hoja de datos de los conmutadores inteligentes Cisco Business 250 Series . (2021, 13 de diciembre). Cisco. https://www.cisco.com/c/en/us/products/collateral/switches/business-250-series-smart-switches/nb-06-bus250-smart-switch-ds-cte-en.html

[76] Switch Aruba Instant On 1930 24G Class 4 PoE 4SFP/SFP+ 370W (JL684A). (n.d.). Datacenter360.net. Retrieved December 27, 2021, from https://datacenter360.net/catalogo/aruba/switch-aruba-instant-on-1930-24g-class-4-poe-4sfp-sfp-370w-jl684a/

[77] Switch Aruba Instant On 1930 48G Class 4 PoE 4SFP/SFP+ 370W (JL686A). (n.d.). Datacenter360.net. Retrieved December 27, 2021, from https://datacenter360.net/catalogo/aruba/switch-aruba-instant-on-1930-48g-class-4-poe-4sfp-sfp-370w-jl686a/

[78] Sgt-wireless. (2019, November 25). Sgtnetworks.Com. https://sgtnetworks.com/accesspointinalambricoincluyensoporte.html

[79] (N.d.). Arubanetworks.Com. Retrieved December 27, 2021, from https://www.arubanetworks.com/assets/_es/ds/DS_AP510Series.pdf.

[80] Ghonaimy, M. A. (2009). Quantum network security. 2009 International Conference on Computer Engineering & Systems.

[81] FortiGate ® 900D. (n.d.). Fortinet.Com. Retrieved December 27, 2021, from https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_900D.pdf

[82] Versión de funciones de Cisco Meeting Server 2.7 . (2019, 3 de octubre). Bienvenido al Centro de videoconferencias. https://blog.Webex.com/es/videoconferencias/cisco-meeting-server-2-7-caracteristicas-de-la-ultima-version-actualizada/

ANEXOS

ANEXO A. Distribución de los edificios de la Unidad Educativa “FESVIP”.

ANEXO B: Puntos de red por área en la Unidad Educativa “FESVIP”.

ANEXO C: Distancias de Cableado Horizontal de la Unidad Educativa “FESVIP”.

ANEXO D: Dimensionamiento *racks* “FESVIP”.

ANEXO E: Mapas de calor Unidad Educativa “FESVIP”, *site survey* predictivo.

ANEXO F: Elementos y costos red pasiva.

ANEXO G: Instalación y Configuración de software de simulación y virtualización.

ANEXO H: Cotizaciones.

ANEXO I: Planos de la Unidad Educativa “FESVIP” proporcionados por las autoridades.

ORDEN DE EMPASTADO