Diseño de una Red para la Empresa Arabito con Solución en la Nube en su Sede Principal Interconectando sus Sucursales mediante VPN MPLS.

Cabrera Omar, Cordero Richard

Escuela de Ingeniería en Telecomunicaciones, Universidad Católica Andrés Bello, Venezuela

cabreraomar13@gmail.com

richardcordero2006@gmail.com

Resumen - Este trabajo se encuentra enfocado en dos tecnologías vanguardistas en la administración y diseño de redes como lo son VPN y MPLS, el valor de las mismas radica en la escalabilidad, integridad e interoperabilidad con la que operan, lo que las vuelven herramientas indispensables en el desarrollo tecnológico al satisfacer las expectativas de la disponibilidad de acceso a los servidores, para que el enlace de comunicación no se vea colapsado por la cantidad de concurrencias por el aumento de usuarios manteniendo la seguridad y calidad de la conexión. Siendo coherente con estas tecnologías, se diseñó una red telemática para la empresa Arabito que permitiera interconectar sus sucursales haciendo uso de VPN-MPLS. Dentro de las tareas propuestas en la metodología del proyecto se realizó una investigación profunda de las tecnologías y de los dispositivos físicos a implementar en la red, una búsqueda de conceptos teóricos y prácticos, posteriormente se definieron los servicios y los proveedores que prestarán los mismos y luego se realizó el diseño de la red para después comprobar su correcto funcionamiento mediante el software de simulación GNS3. Los logros obtenidos se reflejan en el diseño de una red telemática que garantice una comunicación segura y de alta velocidad entre todas las sucursales de la empresa, y que en su sede principal contenga soluciones en la nube que permita aumentar el desempeño de la empresa, además se encuentra prevenida para un futuro crecimiento de la empresa.

Palabras claves: VPN-MPLS, Diseño, Arabito, GNS3.

Abstract - This project is focused on two state-of-the-art technologies in network management and design such as VPN and MPLS, the value of these technologies lies in the scalability, integrity and interoperability with which they operate, which make them indispensable tools in technological development by meeting the expectations of availability of access to the servers, so that the communication link is not collapsed by the Consistent with these technologies, a telematic network was designed for the Arabito company to enable its branches to be interconnected using VPN-MPLS. Within the tasks proposed within the methodology, an in-depth investigation of the technologies and physical devices was carried out, in order to be implemented in the network, a search for theoretical and practical concepts, then defined the services and the suppliers that will be provided and then the design of the network was carried out to then verify its proper functioning using the simulation software GNS3. the achievements are reflected in the design of a telematics network that ensures secure and high-speed communication between all branches of the company, and that at its headquarters contains solutions in the cloud to increase the performance of the company, and is also prevented for the future growth of the company.

Key Words: VPN-MPLS, Design, Arabito, GNS3.

I. INTRODUCCIÓN

Se presenta el artículo del Trabajo Especial de Grado que consiste en el diseño de una red de datos para la empresa Arabito que pueda ofrecer servicios de acuerdo a la calidad de sus productos, interconectando todas sus sedes en el Distrito Capital mediante la utilización de la tecnología VPN-MPLS.

II. PLANTEAMIENTO DEL PROYECTO

La empresa Arabito, Restaurante/Panadería/Bodegón, es reconocida por ofrecer servicios de comida y productos árabes - libanesa. Actualmente cuenta con 3 sedes en el territorio nacional, específicamente en el Distrito Capital, ubicadas en: Sabana Grande (siendo esta su sede principal actual), Catia y San Martín (próxima sede principal), que sumado a un proyecto de expansión y modernización de todas sus tiendas se presenta como una de las compañías con mayor inversión en el pasado 2020 en Venezuela. Todo este proceso de modernización no solo es a nivel físico, ya que la misma apunta a convertirse en una de las empresas del sector alimenticio venezolano con una infraestructura tecnológica moderna, con soluciones basadas en la nube, que les garantice no solo continuidad comercial, sino, además, le permita entrar en el ritmo de la gestión operativa necesaria desde la modalidad de teletrabajo. Sin embargo, en la actualidad se encuentra muy alejado de esta visión debido que todas estas sedes no cuentan con ninguna arquitectura de red que garantice interconexión con todas sus sucursales, funcionando de manera independiente con estructuras de red desactualizadas, no acordes a las tendencias actuales y con

grandes debilidades en su diseño que las colocan muy expuestas para ataques cibernéticos.

Es por esta razón, que la empresa Arabito requiere un diseño de red de datos que garantice no solo continuidad operativa, sino también los accesos a las aplicaciones y sistemas que estarán en plataforma *cloud*, permitiendo almacenar y acceder a los datos y programas a través de internet (en lugar de unidades de almacenamiento convencionales), para así mejorar las diversas características que dicha red va a poseer. La sede ubicada en San Martín (próxima sede principal) de dicha empresa, no cuenta con ninguna red debido a que está en fase de construcción, siendo un punto importante de esa sede la implementación de la misma analizando las necesidades e identificando la capacidad de cada área y los niveles de conexión que se desean alcanzar. Es por ello que surge la necesidad de diseñar una nueva red de datos en la empresa Arabito para poder ofrecer servicios de acuerdo a la calidad de sus productos, interconectando todas sus sedes en el Distrito Capital mediante la utilización de la tecnología VPN MPLS, asimismo se consideran esenciales las soluciones en la nube en esta sede principal, las mismas incluyen un sistema de planificación de recursos empresariales (SAP) para el core del negocio, además de utilizar Office/Microsoft 365 que contiene todas sus aplicaciones y servicios de correo electrónico, todo esto con la finalidad de traer a esta red beneficios importantes para la empresa, incluyendo reducción de costos, menos gastos en infraestructura, y logrando proporcionar mayor seguridad y rendimiento de la misma, trayendo como resultado la solución de las problemáticas mencionadas anteriormente.

A. Objetivos

1) Objetivo General

- Diseñar una red privada para la empresa Arabito con soluciones en la nube en su sede principal interconectando sus sucursales mediante VPN MPLS.

2) Objetivos Específicos

- Realizar el levantamiento de información de la infraestructura tecnológica actual en la sede principal Arabito y sus sucursales.
- Analizar la infraestructura tecnológica actual de las tres sedes para el establecimiento de componentes esenciales para la red, incluyendo los servicios de SAP y Microsoft 365.
- Diseñar una nueva arquitectura de red que permita llevar a la nube elementos importantes de la infraestructura tecnológica, como el ERP y el software de ofimática mediante la interconexión de las sedes con red VPN MPLS.
- Evaluar los niveles de seguridad que se establecerán en la nueva arquitectura de red, aplicando niveles de autenticación, segmentación de red, calidad de servicios y alta disponibilidad.
- Realizar pruebas de rendimiento y seguridad de la arquitectura de red propuesta en un ambiente controlado.
- Establecer los procedimientos para las fases de migración hacia la nueva plataforma tecnológica.

III. MARCO TEÓRICO

A. Multi-Protocol Label Switching (MPLS)

Actualmente surgen nuevas tecnologías que trabajan eficazmente en asegurar la disponibilidad de la información en todo momento de primera mano, las mismas basadas en el diseño de una infraestructura con tecnología MPLS usando una VPN. El crecimiento en el uso de MPLS se volvió necesario, de igual manera que su adaptación y adopción, siendo actualmente el estándar principal de la mayoría de los proveedores de servicio. Debido a los avances en la ingeniería de hardware, la diferencia en el desempeño entre un reenvío de datos basados en Labels o IP es inexistente, el valor de la misma se encuentra en la utilización de MPLS gracias a su escalabilidad e interoperabilidad, sumado a servicios o infraestructuras que tienen la posibilidad de correr encima, lo que lo vuelve una herramienta indispensable en el desarrollo tecnológico al satisfacer las expectativas de la disponibilidad de acceso a los servidores, para que el enlace de comunicación no se vea colapsado por la cantidad de concurrencias por el aumento de usuarios [1].

Es un método de conmutación que tiene como utilidad reenviar los paquetes a través de una red mediante la información que se encuentra en las etiquetas que son añadidas a los paquetes IP, en lugar de realizar un lookup basado en la dirección IP de destino. Dicho método tiene la finalidad de crear redes adaptables y escalables para así aumentar el desempeño y la estabilidad de la misma.

De forma general, MPLS funciona de igual manera que los marcadores que se encuentran en los navegadores, el mismo le ordena a los routers donde deben buscar exactamente en la tabla de enrutamiento mediante un prefijo específico, es decir que, cuando un router corre este método, asigna un número único a cada uno de los prefijos que se encuentran en su tabla de enrutamiento [1]. Dicho número será determinante para la rapidez de la comunicación, esto debido a que identifica cada prefijo de manera individual, y una vez ya asignados, los mismos son comunicados a sus vecinos.

Específicamente una red MPLS consiste en un grupo de routers de conmutación de etiquetas (LSR) que poseen la capacidad de realizar conmutación y enrutación de paquetes en base a una etiqueta que fue añadida a cada uno de los paquetes. Cada etiqueta colocada va a definir una cantidad de paquetes entre dos puntos de conexión. Cada flujo es distinto al otro y se llama Clase de Equivalencia de Reenvío (FEC), y también cada uno de los flujos posee caminos distintos a través de los LSR de la red [2].

Cada FEC, además de contener la ruta por donde los paquetes se van a transportar, posee una serie de caracteres que van a definir los requerimientos de QoS [2].

Cabe destacar que esta es una de las ventajas más importantes que poseen los routers MPLS sobre los routers IP, ya que el proceso de reenvío de los paquetes es más complejo. En un router IP, cada vez que se recibe un paquete, este analiza su encabezado IP para así poder compararlo directamente con la tabla de enrutamiento y así determinar el siguiente salto que dará el paquete, y por ese simple hecho de examinar cada paquete en los distintos puntos por donde transita el mismo para poder llegar a su destino, significa un mayor tiempo de procesamiento para el router en cada uno de los nodos de la red y por lo tanto, la duración del recorrido es mucho mayor [2].

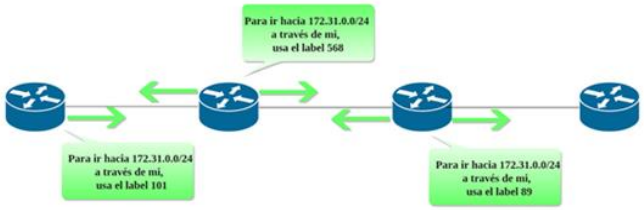

Fig. 1: Funcionamiento MPLS [1].

1) Componentes de una red MPLS

Los distintos componentes que posee una red MPLS se encuentran conformados por los siguientes elementos:

- LER (Label Edge Router o Enrutadores de Etiquetas de Borde): es aquel elemento que inicia o finaliza el túnel de comunicación, dichos elementos son dispositivos que operan en los límites de la red de acceso y la red MPLS, este se encarga de colocar las etiquetas en base a la información de enrutamiento. Un LER soporta múltiples puertos que se encuentran conectados a redes distintas, envía este tráfico a través de la red MPLS después de haber establecido un LSP utilizando un protocolo de distribución de etiquetas. Este también tiene la responsabilidad de quitar las etiquetas y distribuir el tráfico a las distintas redes de salida [3].
- LSR (Label Switching Router - Enrutadores Conmutadores de Etiquetas): se trata de un router de gran velocidad que se encuentra ubicado en el centro o corazón de la red MPLS, el cual debe soportar todos los protocolos de enrutamiento IP y debe participar en el establecimiento de las distintas trayectorias de intercambio de etiquetas utilizando el protocolo de señalización de etiquetas que sea más adecuado. El LSR permite la conmutación de tráfico de datos a alta velocidad y está basado en las trayectorias que son establecidas, en otras palabras, es un conmutador. Cada LSR también posee la función de construir una tabla la cual especifica cómo será enviado cada paquete; esta tabla lleva el nombre de "Base de Información de etiqueta" (LIB) [3].
- LSP (Label Switched Path - Caminos Conmutados Mediante Etiquetas): es un nombre genérico que se le otorga a un camino MPLS para cierto tipo de tráfico o FEC, es decir del túnel de comunicación MPLS que es establecido entre los puntos extremos. Es completamente parecido a un canal virtual y este puede ser punto a punto, punto a multipunto, multipunto a punto o multipunto a multipunto [3].
- LDP (Label Distribution Protocol - Protocolo de Distribución de Etiquetas): es un protocolo encargado de la distribución de las etiquetas, cada LSR creará una unión local por cada prefijo IGP IP existente en la tabla de enrutamiento IP, esto quiere decir que una etiqueta se enlaza al prefijo IPv4. El LSR es el encargado de posteriormente distribuir esta unión a todos los vecinos LDP presentes, convirtiéndose en enlaces recibidos remotos. Los LDP almacenan los enlaces recibidos remotos y locales en una tabla especial, la base de información de la etiqueta (LIB). Por cada LSR solo existe una unión local por prefijo, esto ocurre cuando el espacio de la etiqueta es por plataforma, en cambio cuando el espacio es por interfaz puede existir un sello local de unión relacionado a prefijo por interfaz. Es debido a esto que se puede tener una etiqueta por prefijo o una etiqueta por prefijo por interfaz, pero al LSR por lo general por tener más de un LSR adyacente, obtiene más de un control remoto de unión [3].
- Dominio MPLS: Es la parte de la red donde los diversos procedimientos de enrutamiento y de envío están acorde con el protocolo MPLS [3].
- FEC (Forwarding Equivalence Class - Clase Equivalente de Envío): Es una representación de un grupo de paquetes que comparten los mismos requerimientos para su transporte. El trato es el mismo para todos los paquetes en un grupo determinado, siguiendo una misma ruta hacia su destino. En contraparte del envío empleado convencionalmente por IP, en MPLS la asignación de un FEC particular a un paquete en particular es realizado sólo una vez, cuando el paquete ingresa a la red. Están basados en los requerimientos de servicio que tienen un conjunto de paquetes dados, simplemente para un prefijo de dirección [3].

B. Virtual Private Network (VPN)

Es una estructura de red que simula un tipo de red privada que se aplica en una base ya existente, y el mismo aporta comunicación en los niveles de capa 2 y 3 del modelo OSI.

Este tipo de redes virtuales permite la interconexión de distintas localidades o sedes mediante el aporte de un proveedor de servicios, esto es posible debido a que la tecnología utilizada por VPN permite la creación de un túnel con encriptación entre las localidades a través de internet u otra red pública existente, brindando así seguridad, privacidad y funciones que redes privadas no poseen [4].

Realizar una red VPN trae distintos beneficios tanto para la empresa como para la misma red, ya que brinda una mayor reducción de costos debido a menos uso de dispositivos y por sus diversas funciones, existe una mayor seguridad en la información que se transmite por la misma, su escalabilidad es mayor ya que utiliza servicios de internet, permite ahorrar direcciones IP de versión 4, genera una mayor productividad debido a que brinda un amplio nivel de acceso durante un tiempo mayor, además de que es compatible con tecnologías de banda ancha [4]. Los 2 tipos de VPN más comunes son los siguientes:

- VPN Remote Access (Acceso Remoto)
- VPN Site-to-Site (Sitio-a-Sitio)

El tipo de VPN de acceso remoto se basa en una conexión de usuario a red LAN que es utilizada por una empresa y que posee diversos empleados que necesitan la conexión a la red privada desde distintas ubicaciones. Generalmente, cualquier empresa que desee configurar este tipo de VPN, debe proporcionar algún tipo de cuenta telefónica de internet a los usuarios mediante un proveedor de servicios (o ISP). Las VPN de acceso remoto permiten conexiones seguras y totalmente cifradas entre la red LAN de la empresa y los

usuarios remotos a través de un proveedor de servicios de terceros [5].

Las VPN de sitio-a- sitio mediante el uso de distintos equipos y con un cifrado a gran escala, permite la conexión de varios sitios fijos de una empresa a través de una red pública como lo es internet. Cada localidad de la empresa necesita únicamente de una conexión local a internet, lo cual permite un uso menor de capital en extensas líneas arrendadas privadas. Es importante destacar que este tipo de VPN se puede clasificar en *intranets* o *extranets*, una se diferencia de la otra debido a que la VPN intranet es desarrollada entre oficinas de la misma empresa, en cambio la VPN extranet conecta la empresa con su *partner* o cliente [5].

C. VPN – MPLS

En MPLS una de las aplicaciones más utilizadas es la creación de redes privadas virtuales, mejor conocidas como VPN. En lo que concierne a los proveedores de servicios de internet, MPLS ha reducido de gran forma la programación y el montaje de soluciones VPN para sus usuarios. Además, MPLS también se encarga de facilitar la interconexión de distintos usuarios, cuando los mismos lo deseen. Originalmente, las VPN fueron introducidas para permitir a los proveedores de servicios el uso de infraestructuras físicas comunes para así implementar la simulación de enlaces punto a punto. En las redes comunes que son basadas en routers, diferentes puntos de clientes realizan conexiones unos con otros mediante el montaje de enlaces dedicados, el costo de este depende del número de clientes que se encuentran conectados a la red, además de la participación del proveedor de servicios en el proceso de enrutamiento al cliente [3].

Actualmente, se encuentran diversas opciones para repartir las responsabilidades del manejo de todas las políticas, una de las mismas es dejar esta responsabilidad al proveedor de servicios, otra posibilidad es que sea el usuario quien se encargue de manejarlas y por última opción sería distribuir todo el trabajo entre la empresa y el cliente, para que de esta manera se pueda realizar una división del estudio de las VPN en dos tipos de modelos [6]:

- Modelo de capa superpuesta (Overlay Model)
- Modelo de igual-igual (Peer to Peer Model)

Las VPN de modelo de capa superpuesta (Overlay Model) fueron implementadas originalmente por los proveedores de servicio para poder establecer una conectividad de capa 1 o una conexión de capa 2 de transporte entre las distintas ubicaciones donde se encuentre el cliente. En cuanto a la implementación de capa 1, el proveedor se encargaría de establecer la conectividad de la capa física entre los sitios donde se ubique el cliente y el mismo se haría responsable de las capas restantes. Con respecto al montaje de la capa 2 (enlace de datos), el proveedor de servicios se encargaría de las tramas entre los sitios del cliente, la red generalmente era transparente al cliente y el protocolo de enrutamiento corría directamente entre los enrutadores de los clientes [3].

Resumiendo, se puede establecer que las tareas para el proveedor de servicios y el cliente se encuentran definidas. El proveedor de servicios se va a encargar de brindar el servicio de los circuitos virtuales, mientras que el cliente establece la comunicación entre los enrutadores y la información se intercambia por los equipos del mismo [6].

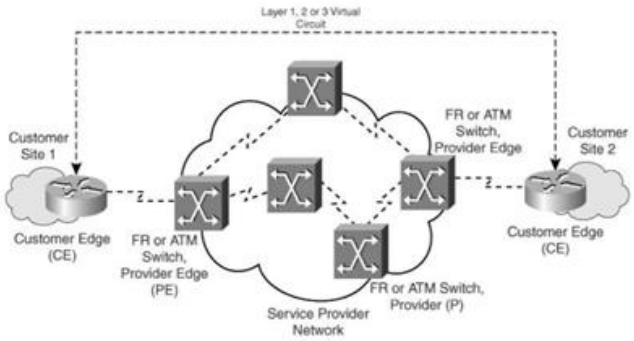

Fig. 2: Ejemplo del modelo de Capa Superpuesta [3].

El modelo igual-igual fue creado para poder superar todas aquellas desventajas que el modelo de la capa superpuesta posee y además para proveer a los clientes una vía eficiente de transporte a través del backbone del proveedor de servicios, por lo tanto, este puede participar de forma activa en el proceso de enrutamiento. En este modelo, la información de enrutamiento es canjeada entre los routers del cliente y los routers de los proveedores de servicios, por tal motivo los datos del cliente son enviados a lo largo del proveedor de manera óptima [3].

En el modelo de igual-igual se facilitan ciertas funcionalidades como la escalabilidad y la posibilidad de habilitar calidad de servicio (QoS) en la capa de red (capa 3), la diferencia cae principalmente en que el router del cliente ahora ha de conectarse con el router del proveedor de servicios, y no directamente con otro CE. La razón para nombrar a este modelo "Igual-Igual" radica en que desde el punto de vista del enrutamiento de la red del proveedor de servicios, este actúa como un par con la red del cliente desde el momento en el que los CE se conectan directamente con los PE [6].

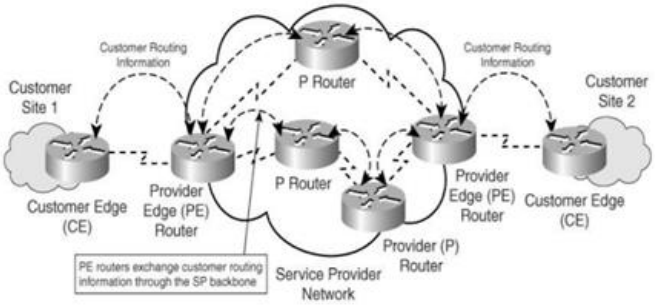

Fig. 3: Ejemplo del modelo de Igual-Igual [3].

1) Ventajas del modelo PEER TO PEER

- El intercambio de información de enrutamiento entre los routers que posee el cliente y los que tiene el proveedor de servicios va a permitir que se obtenga gran escalabilidad ya que el número de ubicaciones se pueden aumentar sin tener que incrementar la tabla de enrutamiento [6].
- Con el aumento de los usuarios del cliente no se van a producir cambios en la red, solamente entre el CE y el PE al cual se conecte el mismo. Mientras que en el modelo de capas superpuestas se requiere de la creación de VC (Circuitos Virtuales) hacia los distintos sitios de la red [6].

2) Arquitectura y terminología de VPN-MPLS

Al igual que la VPN común, el dominio que posee la VPN MPLS consiste principalmente en una red cliente y una red del proveedor, este modelo es muy semejante al modelo aplicado de un router PE en un montaje punto a punto, pero en lugar de implementar un router PE dedicado por un cliente, el tráfico del cliente es asignado sobre el mismo router PE que se encarga de establecer la conectividad con la red del proveedor de servicios [3].

Según [3], una arquitectura VPN MPLS posee los siguientes componentes esenciales:

- Red Cliente (CN): tradicionalmente esta se basa en el dominio del cliente que se encuentra conformado por distintos dispositivos o routers que cubren múltiples ubicaciones que pertenecen todas al cliente.
- Router CE: son todos aquellos routers que se encuentran en la red del cliente y que además se conectan con la red del proveedor.
- Red del Proveedor: se puede definir como el dominio del proveedor de servicios, este se encuentra conformado por los routers de extremo "PE" y de los routers de backbone que se encargan de conectar las ubicaciones que pertenecen al cliente, formando un tipo de infraestructura compartida. Cabe destacar que el proveedor de la red es el que controla todo el enrutamiento del tráfico entre los sitios donde se ubique el cliente.
- Routers PE: son aquellos routers que se encuentran en la red del proveedor de servicios que se van a conectar a los routers de extremo del cliente.
- Routers P: son todos los routers que se encuentran en el núcleo de la red del proveedor, estos se conectan con los otros routers del mismo núcleo o con los routers extremos PE.

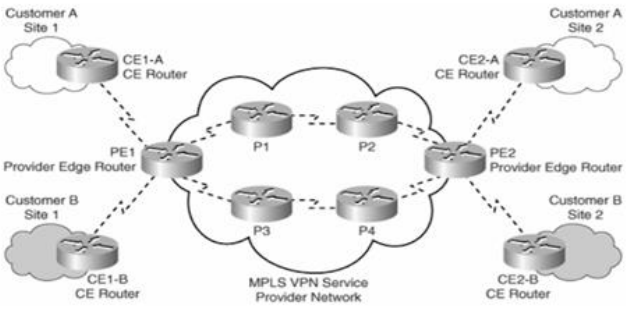

Fig. 4: Ejemplo de una arquitectura VPN MPLS [3].

3) Modelo de enrutamiento VPN MPLS

El montaje de una VPN MPLS es muy parecido al modelo punto a punto desde la perspectiva de un router cliente (CE), ya que los datos son enviados desde el mismo hasta el router PE. Los routers CE no van a requerir de una configuración en específico para poder ser parte de un dominio VPN MPLS, el único requerimiento que debe tener el router del cliente es poseer un protocolo de enrutamiento que permita el intercambio de información de ruta con el router PE del proveedor de servicios [3].

En este tipo de implementación de VPN, el router PE posee múltiples tareas, en primer lugar este debe ser capaz de poder aislar el tráfico de un usuario, claro está que esto lo debe realizar si más de un solo cliente se encuentra conectado al mismo router PE. Cada uno de los clientes por lo menos debe tener asignado una tabla de enrutamiento que sea totalmente independiente, mientras que el enrutamiento que se realiza a través de la red del proveedor de servicios es llevado a cabo utilizando un proceso de ruta en la tabla de enrutamiento global [3].

Los routers P van a permitir la comunicación de etiquetas entre los routers extremos del proveedor de servicios, mientras que los routers que se encuentran en la red del cliente no es consciente de los routers P del proveedor de servicios, indicando que la topología de la red del mismo proveedor de servicios es totalmente transparente al cliente. Entonces, los routers P son únicamente responsables de la conmutación de etiquetas de los paquetes y no llevan rutas VPN y además no participan en el enrutamiento de la red VPN MPLS. Los routers PE intercambian rutas IPv4 que se encuentran conectadas a los routers CE utilizando protocolos de enrutamiento [3].

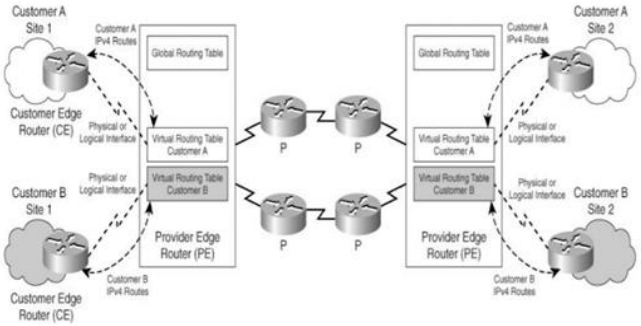

Fig. 5: Explicativa de un enrutamiento VPN MPLS [3].

IV. METODOLOGÍA Y DESARROLLO

En el siguiente capítulo se exhiben todos los procesos llevados a cabo para el desarrollo del Trabajo Especial de Grado, incluyendo las actividades definidas y procedimientos necesarios para el óptimo desenvolvimiento y progreso dentro de la investigación del proyecto.

A. Tipo de investigación.

La investigación por la que se ve enmarcada este estudio es de tipo Proyectiva.

La Investigación Proyectiva es aquella que propone soluciones a una situación determinada a partir de un proceso de indagación a un problema o necesidad de tipo práctico. Implica explorar, describir, explicar y proponer diversas alternativas de cambio, más no necesariamente ejecutar la propuesta que se realice [7].

La identificación de un evento a modificar, y el diagnóstico descriptivo en el cual se inicia la investigación, se hace con base en ese evento, de implicar la ejecución de la propuesta, la misma pasaría a ser investigación interactiva [8].

Se plantea la utilización del enfoque cuantitativo basado en la recolección de datos, mediciones numéricas y el análisis estadístico, estableciendo pautas al comportamiento y prueba de teorías. A su vez que alcance descriptivo, especificando las propiedades y características de la situación estudiada [9].

B. Período de Desarrollo del Proyecto

La ejecución del presente Trabajo Especial de Grado fue realizada entre los meses de noviembre de 2020 y agosto de 2021. A lo largo del desarrollo estuvieron involucradas las locaciones físicas de las distintas sedes de la empresa Arabito, las cuales sirvieron como base de estudio del proyecto.

C. Descripción de Actividades

En esta sección se muestran los pasos que se llevaron a cabo para la ejecución del presente trabajo. La implementación de la red se basará en la metodología de "Network Design" dividiendo el proyecto en las siguientes fases:

1) Fase I: Estudio Teórico y Técnico de las Tecnologías VPN y MPLS.

Mediante el estudio teórico y técnico de las tecnologías VPN y MPLS, se logró obtener la cantidad de información necesaria para ampliar el conocimiento relacionado a estas tecnologías y poder ser desarrolladas para el trabajo. Es de gran importancia destacar que, dentro de la investigación se abarcaron aspectos como conceptos teóricos, descripciones de procedimientos, desglose de los tipos de estas tecnologías, además de ciertos tipos de encriptación de datos y otros puntos que guardan total relación con las tecnologías MPLS y VPN, junto con la investigación teórica de los distintos términos estudiados en la red en la que se desarrolló el proyecto como lo es Arabito.

Es importante destacar que dentro de las fuentes bibliográficas que fueron consultadas para esta fase del trabajo se encuentran distintos trabajos de grado (nacionales e internacionales), libros técnicos, documentos de páginas web; pero teniendo en cuenta que la principal fuente de información fue internet, a través de los distintos tipos de buscadores de publicaciones académicas y científicas.

Debido a los resultados que fueron extraídos en esta fase del proyecto, se dieron a conocer distintas posibilidades y opciones acerca de la transmisión de datos, los dispositivos y los medios físicos necesarios para la red a diseñar. Claro está que gracias a este estudio exhaustivo de las tecnologías a utilizar se obtuvo el conocimiento necesario para realizar una buena toma de decisiones en los aspectos del diseño de la red en fases posteriores.

2) Fase II: visita y levantamiento de las sedes de la empresa Arabito.

Para un adecuado análisis de los objetivos y necesidades de la empresa se logró identificar la infraestructura tecnológica y las restricciones técnicas tanto de la empresa como las necesidades del servicio que se requerían.

En esta sección se contó con diversas actividades que se realizaron para obtener todo tipo de información acerca de la red existente en la empresa y los requisitos necesarios para la nueva red a diseñar, estas tareas incluyeron:

- La planificación y visita de cada sede involucrada en el proyecto (ubicadas en San Martín, Sabana Grande y Catia), para esta actividad se realizaron reuniones y llamadas con los encargados de cada una de las sucursales para realizar la visita y el estudio de las mismas en el día indicado.
- Realización de una encuesta que fue aplicada a los encargados de cada sede de la empresa Arabito con el fin de realizar un análisis sobre los datos arrojados por la misma y obtener todo tipo de información necesaria de la red de la empresa y los requerimientos de la futura. La encuesta desarrollada en cada una de las sucursales de la empresa se encuentra ubicada en la sección de anexos del presente trabajo.

También se tomaron en cuenta las características físicas y organizacionales de la infraestructura de cada sede individualmente, de esta forma se obtuvo una serie de datos sistemáticos y una visualización clara de las siguientes fases y sus respectivas actividades.

3) Fase III: Diseño de la topología.

En primer lugar, para esta fase del trabajo se realizó la descarga y el estudio de la herramienta de simulación de redes telemáticas GNS3, la cual permitió representar el diseño de la red de una manera gráfica y esquematizada facilitando su comprensión y entendimiento. Es importante resaltar que la misma herramienta fue utilizada en fases posteriores para simulación y aprobación de la red diseñada.

Posterior a eso se realizó el diseño físico de la topología de la red, donde se ejecutaron actividades como: la investigación, el análisis y la comparativa de los equipos potencialmente recomendados para cada una de las sucursales, todo basado en el estudio realizado en fases anteriores gracias a los resultados de la encuesta ejecutada y los requerimientos de la empresa. Además, se realizó el esquema físico de la totalidad de la red utilizando la herramienta de simulación de redes GNS3.

Al momento de finalizar con el diseño físico, el siguiente paso fue el diseño lógico e inalámbrico de la topología, donde se decidió y se realizó el direccionamiento de la red tomando en cuenta: cantidad de VLANs a utilizar, cantidad de dispositivos de routing y switching (es decir Routers y Switches), cantidad de usuarios finales de la LAN, (como por ejemplo los servidores, computadores e impresoras) y la cantidad de usuarios finales de la red inalámbrica (usuarios que utilizarán los Access Point), entre otros.

4) Fase IV: Proceso de interconexión de las sedes.

Para esta fase del trabajo se planificaron y ejecutaron diversas actividades para poder aplicar los distintos niveles de seguridad en la arquitectura de red que fue diseñada en fases anteriores. La primera actividad se basó en escoger a los proveedores que prestarían el servicio VPN-MPLS para la interconexión de las sedes de la empresa, seguido de esto se estableció la comunicación con los mismos para conocer el costo del servicio a utilizar, luego se realizó el estudio de las opciones para tener una buena toma de decisión con respecto al beneficio de la empresa.

También se realizaron reuniones con el fin de planificar y decidir otros aspectos importantes de seguridad para la red: tipo de VPN para utilizar como "back up", el tipo de enrutamiento que sería utilizado para conectar cada una de las sedes con los proveedores de internet y el proveedor del servicio VPN MPLS, la verificación de la segmentación de la red, entre otras.

5) *Fase V: Simulación y verificación de la red en un ambiente controlado.*

Luego de tener todos los aspectos decididos acerca de la nueva red telemática, se realizó el proceso de simulación de la misma en un ambiente totalmente controlado, es importante recalcar que para esta parte del proyecto se utilizó el software GNS3 que facilitó la ejecución y verificación del correcto funcionamiento de la red planificada.

La red a simular es el resultado del diseño planteado en fases anteriores, cabe destacar que aunque en la realidad se plantea que el servicio de MPLS sea brindado por un proveedor de servicios en específico, en este caso se simuló un bosquejo sencillo de tal mecanismo de transporte de datos que permita observar de forma más clara los beneficios que ofrece esta arquitectura a la red empresarial deseada.

6) *Fase VI: Fases de migración hacia la nueva red.*

Para la última fase del proyecto se realizaron estudios y reuniones para poder planificar todos los procedimientos, estrategias y fases de la migración de la red antigua hacia la nueva arquitectura tecnológica diseñada en este proyecto.

Se estableció una guía de pasos necesarios que la empresa pueda seguir de tal forma que su desenvolvimiento y actividades se vean afectadas en la menor medida posible durante la transición y que de esta manera la misma sea óptima.

V. RESULTADOS

En este capítulo se presentan de manera específica todos y cada uno de los resultados obtenidos al ejecutar la metodología planteada en el capítulo anterior:

A. Fase I: Estudio Teórico y Técnico de las Tecnologías VPN y MPLS.

Mediante la investigación y el estudio teórico y técnico de las tecnologías VPN, MPLS, encriptación, además de otros puntos importantes, se pudo ampliar el conocimiento acerca del funcionamiento y el comportamiento de las mismas. Importante destacar que dicha información fue la base teórica para el desarrollo de las siguientes fases del trabajo.

La investigación realizada en esta fase culminó con un documento escrito, en donde se plasmaron todos los conocimientos que se consideraron pertinentes (acerca de las tecnologías anteriormente mencionadas) para ser utilizados en este trabajo. Es importante resaltar que todos los métodos, parámetros y premisas involucradas en la delimitación teórica de la investigación, se encuentran en el capítulo II del presente trabajo.

B. Fase II: Visita y levantamiento de las sedes de la empresa Arabito.

Las sucursales de la empresa Arabito, ubicadas en San Martín, Casanova y Catia, fueron los sitios físicos estudiados para la aplicación de este proyecto. En esta fase se realizaron diversas actividades para obtener todo tipo de información acerca de la red existente en la empresa y los requisitos necesarios para la nueva. Entre ellas se planificó la visita de cada una de las sedes mencionadas mediante llamadas y reuniones y posteriormente, durante el encuentro, fue aplicada una encuesta a cada encargado de las sucursales

Es importante destacar que de esta forma se obtuvo una serie de datos sistemáticos y una visualización clara de los dispositivos y los servicios que actualmente posee dicha empresa.

C. Fase III: Diseño de la topología.

Antes de poder comenzar con la elaboración del esquema de la red, fue necesario la descarga y el estudio teórico y técnico del software GNS3, con el fin de permitir una mejor esquematización de las distintas topologías.

GNS3 es un software de simulación que permite el diseño de todo tipo de topologías de red avanzadas y que a su vez posibilita la prueba de su correcto funcionamiento, antes de una futura implementación. Se puede establecer que es una herramienta bastante útil y que es amigable para el usuario al momento de simular las distintas soluciones y montar los escenarios de prueba [10].

Luego de realizar un análisis completo de dicha herramienta, se procedió con el diseño topológico de la nueva red, específicamente se esquematizan la topología física, lógica e inalámbrica.

1) *Diseño de la topología física*

En este apartado del diseño se realizó una búsqueda y un estudio profundo de los nuevos dispositivos que se utilizarían en la nueva red. Además, se identificaron todas aquellas conexiones físicas entre dispositivos LAN (routers, switches, dispositivos finales, puntos de acceso, etc.), de cada una de las sedes.

Para una correcta toma de decisiones con respecto a los dispositivos a utilizar en la nueva red, se tomó como referencia los datos arrojados por el "Cuadrante de Gartner".

Gartner, Inc. es una compañía que trabaja en base a la investigación, información de tecnología y además es el líder en consultoría a nivel mundial. Todos los días se encarga de entregar una visión que se encuentre relacionada con la tecnología necesaria para que sus clientes realicen una correcta toma de decisiones al momento de adquirir una determinada solución de seguridad [11].

Al momento de presentar sus distintas investigaciones, la empresa Gartner utiliza lo que denomina como "Cuadrantes Mágicos", estos consisten en la clasificación de los proveedores de equipos de seguridad de acuerdo a ciertas categorías, las mismas

son: líderes, retadores o aspirantes, visionarios y jugadores de nicho. Según [11] los aspectos presentes en el Cuadrante de Gartner se definen de la siguiente manera:

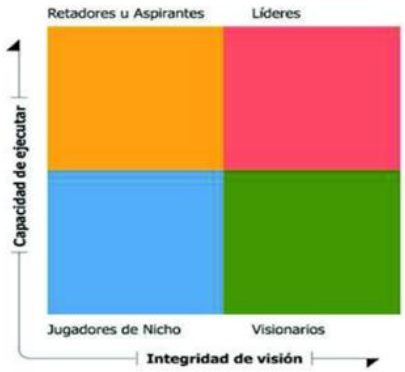

Fig. 7: Representación del Cuadrante de Gartner [11].

Es importante destacar que, se utilizó el "Cuadrante de Gartner" únicamente para tomar referencia de los equipos firewall y los equipos LAN cableados e inalámbricos. Luego de realizar una investigación y obtener las referencias más actualizadas al momento, los datos arrojados por Gartner para los equipos mencionados fueron los siguientes:

Fig. 8: Cuadrante de Gartner, Wired and Wireless LAN (2020).

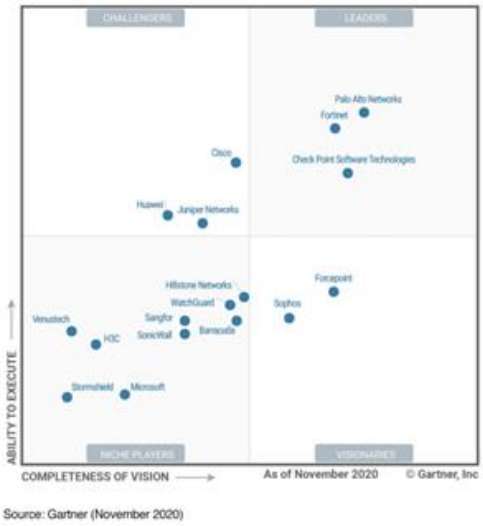

Fig 9: Cuadrante de Gartner, Firewalls 2020.

En base a esto, se efectuaron investigaciones y estudios de distintos dispositivos y distribuidores de los mismos, tomando en cuenta: sus precios, las características necesarias que debía poseer cada equipo para su función en la red y las recomendaciones brindadas por la misma empresa (Arabito). Se realizaron diversas tablas comparativas donde se colocaron las opciones más viables para la inclusión de los mismos en la topología. A continuación, se presentan las tablas y las especificaciones de cada uno de los dispositivos

1.2) Firewalls

TABLA I

Comparativa de Equipos Preseleccionados (Firewalls)

EQUIPO	CAPACIDAD	PRECIO UNIDAD	DISTRIBUIDOR
FortiGate-80F	200 Usuarios	890 - 1200 $	AMAZON
		950 - 1300 $	SECUREBYTE SOLUTIONS C.A.
FortiGate-60F / FG-60F	100 Usuarios	440 - 850 $	AMAZON
		515 - 1000 $	ALIBABA
Fortigate 50E	40 Usuarios	490 $	AMAZON
		550 $	ALIBABA
FortiGate 40F	30 Usuarios	300 - 500 $	AMAZON
		400 - 800 $	ALIBABA

Especificaciones destacables:

FortiGate 80F

- 1 Puerto USB
- 1 Puerto de Consola
- 2 Puertos GE RJ45 WAN
- 2 Puertos GE RJ45/SFP
- 6 Puertos GE RJ45
- 2 Puertos GE RJ45 FortiLink

- WiFi: 1,300Mbps, MIMO 3x3 Wave 2

Firewall	IPS	NGFW	Threat Protection
10 Gbps	1.4 Gbps	1 Gbps	900 Mbps

Fig. 10: Especificaciones Firewall FortiGate-80F [12].

Especificaciones destacables según [13]:

FortiGate-60 F / FG-60F

- 1 Puerto USB
- 1 Puerto de Consola
- 2 Puertos RJ45 WAN 10/100/1000Mbps
- 1 Puerto RJ45 DMZ 10/100/1000Mbps
- 2 Puertos RJ45 Forti Link 10/100/1000Mbps
- 5 Puertos RJ45 LAN 10/100/1000Mbps
- WiFi: 1,300Mbps, MIMO 3x3 Wave 2

Fig. 11: Especificaciones Firewall FortiGate-60F [13].

Especificaciones destacables según [14]:

FortiGate 50E

- Puerto USB
- Puerto de Consola
- 2 Puertos RJ45 WAN 10/100/1000Mbps
- 5 Puertos RJ45 Ethernet 10/100/1000Mbps
- WiFi: 300Mbps, MIMO 2x2

Fig. 12: Especificaciones Firewall FortiGate 50E [14].

Especificaciones destacables según [15]:

FortiGate 40F

- 1 Puerto USB
- 1 Puerto de Consola
- 1 Puerto RJ45 WAN 10/100/1000Mbps
- 1 Puerto RJ45 LAN 10/100/1000Mbps Fortilink
- 3 Puertos RJ45 LAN 10/100/1000Mbps
- WiFi: 1,300Mbps, MIMO 3x3 Wave 2

Fig. 13: Especificaciones Firewall FortiGate 40F [15].

1.3) Switches

TABLA II

Comparativa de Equipos Preseleccionados (Switches)

EQUIPO	PRECIO UNIDAD	DISTRIBUIDOR
Switch Cisco SG300-52P-K9-NA 52 puertos	600 - 900 $	AMAZON
	800 - 1000 $	MERCADO LIBRE
Switch Cisco SG300 – 28P-K9-NA 28 Puertos	210 - 500 $	AMAZON
	450 $	MERCADO LIBRE

Especificaciones destacables según [16]:

Switch Cisco SG300 52 Puertos

- Administrable
- 52 puertos Giga Ethernet (10/100/1000)
- Capa 2-3
- Tabla de Direcciones MAC: 16384 entradas
- Número de VLANs: 4096
- Capacidad de conmutación: 104 Gbps

Especificaciones destacables según [17]:

Switch Cisco SG300 28 Puertos

- Administrable
- 26 puertos Giga Ethernet (10/100/1000)
- Capa 2-3
- Tabla de Direcciones MAC: 16384 entradas
- Número de VLANs: 4096
- Capacidad de conmutación: 56 Gbit/s

1.4) Red Inalámbrica

TABLA III

Comparativa de Equipos Preseleccionados (Red Inalámbrica)

EQUIPO	PRECIO UNIDAD	DISTRIBUIDOR
Ubiquiti Unifi AP-AC	100 - 150 $	AMAZON
	100 - 120 $	ALIBABA
TP-Link TL-WR941HP	90 - 110 $	AMAZON
	95 - 115 $	MERCADO LIBRE

Especificaciones destacables:

Según [18], Ubiquiti Unifi AP-AC:

- 175 x 43.2 mm
- Indoor
- 450 Mbps
- 10/ 100/1000 Ethernet
- Capacidad para 100 personas o más

Según [19], TP-Link TL-WR941HP:

- 227.5 × 190 × 48.3mm
- Indoor
- 450 Mbps
- 1× 10/100 Mbps WAN Port - 4× 10/100 Mbps LAN Ports

Al momento de obtener todas las especificaciones de los dispositivos anteriormente mostrados, se comenzó con el proceso de selección de los artefactos que estarían presente en la nueva red y posteriormente se identificaron los puertos y las conexiones entre los dispositivos, es importante mencionar que, con respecto a los dispositivos de la red inalámbrica, no se escogió algún dispositivo específico debido a que la empresa Arabito puede hacer uso de ambas opciones ya que poseen especificaciones similares:

1.5) Sede: Catia

Para la sede de Catia se realizó el proceso de elección de los siguientes equipos con los siguientes motivos:

- **FortiGate 60F:** además de las grandes características de velocidad y seguridad que posee un dispositivo FortiGate, la razón por la que se escogió este equipo para la sucursal de Catia se debe a que la misma cuenta con un número reducido de personas con requerimientos de conexión a la red, a pesar de esto, la serie "E" de estos equipos no soporta una cantidad de usuarios que cumpla con la exigencia del diseño, se debe tomar en cuenta que en fases futuras se trabajará con el diseño de la red inalámbrica y los Access Points necesarios, esto ocasionará un aumento en los usuarios concurrentes por lo que se optó por el modelo Fortigate 60F el cual soporta 100 usuarios. Además de lo mencionado, con la elección del equipo se obtiene 4 veces más la capacidad de ancho de banda de firewall que la serie "E" y el doble que el modelo 40F llegando a 10Gbps. El uso de FortiGate como seguridad perimetral es reconocido como una de las mejores alternativas con un manejo sencillo e intuitivo por parte de los técnicos, siendo ideal para su implementación en dicha sede.
- **Switch Cisco SG300 – 28 Puertos:** el número de personas que necesitarán conexión LAN directa es limitada en la sede debido a la cantidad de trabajadores que se encuentran en los departamentos de producción y panificadora, por lo tanto, se tomó como un factor principal en la elección del equipo adecuado. Sumado a esto, el alcance de la red puede verse potenciado con el uso de Access Points.

Los dispositivos escogidos para esta sede estarían colocados en el cuarto de tecnología (totalmente acondicionado), ubicado físicamente en el primer piso de la planta, aledaño al departamento de administración:

Rack 1:

- FortiGate 60F: Posición 1
- Switch Cisco SG300 - 28 Puertos: Posición 2

Conexiones:

FortiGate 60F

- 1er Puerto RJ45 WAN FortiGate 60F - ISP (Movistar)
- 1er Puerto RJ45 Ethernet FortiGate 60F - ISP (CANTV)
- 2do Puerto RJ45 Ethernet FortiGate 60F - Puerto 1 Switch Cisco SG300-28P

Switch Cisco SG300 – 28 Puertos

- Puerto 1 Switch Cisco SG300-28P - 2do Puerto RJ45 Ethernet FortiGate 60F
- Puerto 2 Switch Cisco SG300-28P – Servicio VPN-MPLS
- Rango de puertos (3-7) Switch Cisco SG300-28P - Hosts Administración
- Rango de puertos (8-12) Switch Cisco SG300-28P - Hosts Facturación
- Rango de puertos (13-17) Switch Cisco SG300-28P - Hosts Bodegón
- Rango de puertos (18-22) Switch Cisco SG300-28P - Hosts Ventas
- Rango de puertos (23-25) Ubiquiti Unifi AP-AC/ TP-Link TL-WR941HP (Red Inalámbrica).
- Rango de puertos libre (26-28) – Puertos libres en caso de un futuro crecimiento en la empresa.

Tomando en cuenta el estudio realizado y los dispositivos escogidos, el esquema de la red LAN para la sede de Catia se muestra a continuación:

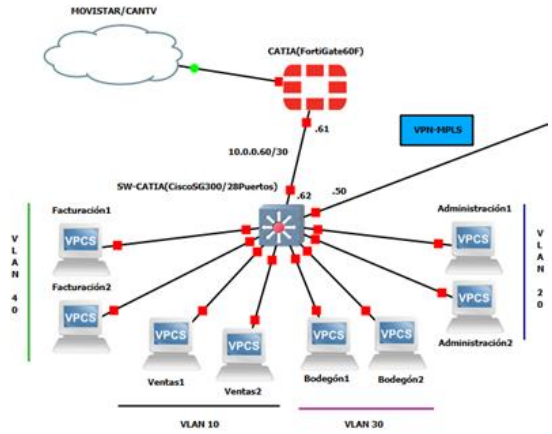

Fig. 14: Diseño de la topología de red física: Sede Catia (Realizado en GNS3)

1.6) Sede: Casanova

Para la sede de Casanova se realizó el proceso de elección de los siguientes equipos con los siguientes motivos:

- **FortiGate 80F:** En aspectos técnicos la elección de un equipo FortiGate como Firewall en seguridad perimetral cumple con las mismas consideraciones que en el caso de la sede de Catia, pero a diferencia de la ya mencionada, la sucursal de Casanova cuenta con un número mayor de personas que poseen requerimientos de conexión a la red, por lo tanto, es por esto que se optó por el modelo Fortigate 80F el cual soporta 200 usuarios. Además de lo mencionado, con la elección del equipo se obtienen 200 Mbps adicionales de ancho de banda para la protección contra amenazas en comparación al modelo "60F".
- **Switch Cisco SG300 – 52 Puertos:** como en la sede de Casanova existe una mayor cantidad de personal con respecto a la sede de Catia, el equipo seleccionado para red LAN es el Switch Cisco SF300 de 52 puertos, cabe acotar que por la misma razón nació la necesidad de utilizar 2 dispositivos que cubran el total de hosts finales.

Los dispositivos escogidos para esta sede estarían colocados en el cuarto de tecnología (totalmente acondicionado), ubicado físicamente aledaño al departamento de administración:

Rack 1:

- FortiGate 80F: Rack 1 - Posición 1
- SW-1 Cisco SG300 - 52 Puertos: Rack 1 - Posición 2
- SW-2 Cisco SG300 - 52 Puertos: Rack 1 - Posición 3

Conexiones:

FortiGate 80F

- 1er Puerto RJ45 WAN FortiGate 80F - ISP (Totalcom)
- 1er Puerto RJ45 Ethernet FortiGate 80F - ISP (CANTV)
- 2do Puerto RJ45 Ethernet FortiGate 80F - Puerto 1 SW-1 Cisco SG300-52P

Switch Cisco SG300 – 52 Puertos (1)

- Puerto 1 SW-1 Cisco SG300-52P - 2do Puerto RJ45 Ethernet FortiGate 80F
- Puerto 2 SW-1 Cisco SG300-52P - Puerto 1 SW-2 Cisco SG300-52P
- Puerto 3 SW-1 Cisco SG300-52P – Servicio VPN-MPLS
- Rango de puertos (4-23) SW-1 Cisco SG300-52P - Hosts Administración
- Rango de puertos (24-43) SW-1 Cisco SG300-52P - Hosts Ventas
- Rango de puertos (44-47) Ubiquiti Unifi AP-AC/ TP-Link TL-WR941HP (Red Inalámbrica).
- Rango de puertos libre (48-52) – Puertos libres en caso de un futuro crecimiento en la empresa.

Switch Cisco SG300 – 52 Puertos (2)

- Puerto 1 SW-2 Cisco SG300-52P - Puerto 2 SW-1 Cisco SG300-52P
- Rango de puertos (2-21) SW-2 Cisco SG300-52P - Hosts Bodegón
- Rango de puertos (22-41) SW-2 Cisco SG300-52P - Hosts Base de Datos
- Rango de puertos (42-45) Ubiquiti Unifi AP-AC/ TP-Link TL-WR941HP (Red Inalámbrica).
- Rango de puertos libre (46-52) – Puertos libres en caso de un futuro crecimiento en la empresa.

Tomando en cuenta el estudio realizado y los dispositivos escogidos, el esquema de la red LAN para la sede de Catia se muestra a continuación:

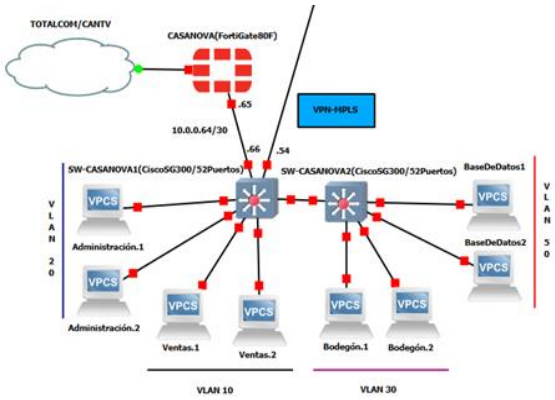

Fig. 15: Diseño de la topología de red física: Sede Casanova (Realizado en GNS3)

1.7) Sede: San Martín

Para la sede de San Martín se realizó el proceso de elección de los siguientes equipos con los siguientes motivos:

- **FortiGate 80F:** Se tomaron las mismas consideraciones que en la sede de Casanova, se optó por el modelo FortiGate 80F el cual soporta 200 usuarios.
- **Switch Cisco SG300 – 52 Puertos:** como futura sede principal, San Martín tendrá la mayor cantidad de personal con respecto a las otras 2 sucursales de la empresa, y es por eso que se utilizan 2 equipos Switch Cisco SG300 de 52 puertos para así poder cubrir la totalidad de usuarios necesarios.

Los dispositivos escogidos para esta sede estarían colocados en el cuarto de tecnología (totalmente acondicionado), ubicado físicamente en el primer piso de la sede, aledaño al departamento de administración:

Rack 1:

- FortiGate 80F: Rack 1 - Posición 1
- SW-1 SG300 - 52 Puertos: Rack 1 - Posición 2
- SW-2 Cisco SG300 - 52 Puertos: Rack 1 - Posición 3

Conexiones:

FortiGate 80F

- 1er Puerto RJ45 WAN Fortigate 80F - ISP (Totalcom)
- 1er Puerto RJ45 Ethernet Fortigate 80F - Puerto 1 SW-1 Cisco SG300-52P

Switch Cisco SG300 – 52 Puertos (1):

- Puerto 1 SW-1 Cisco SG300-52P - 1er Puerto RJ45 Ethernet FortiGate 80F
- Puerto 2 SW-1 Cisco SG300-52P - Puerto 1 SW-2 Cisco SG300-52P
- Puerto 3 SW-1 Cisco SG300-52P – Servicio VPN-MPLS
- Rango de puertos (4-23) SW-1 Cisco SG300-52P - Hosts Administración
- Rango de puertos (24-43) SW-1 Cisco SG300-52P - Hosts Ventas
- Rango de puertos (44-47) Ubiquiti Unifi AP-AC/ TP-Link TL-WR941HP (Red Inalámbrica).
- Rango de puertos libre (48-52) – Puertos libres en caso de un futuro crecimiento en la empresa.

Switch Cisco SG300 – 52 Puertos (2):

- Puerto 1 SW-2 Cisco SG300-52P - Puerto 2 SW-1 Cisco SG300-52P
- Rango de puertos (2-21) SW-2 Cisco SG300-52P - Hosts Bodegón
- Rango de puertos (22-41) SW-2 Cisco SG300-52P - Hosts Base de Datos
- Rango de puertos (42-45) Ubiquiti Unifi AP-AC/ TP-Link TL-WR941HP (Red Inalámbrica).
- Rango de puertos libre (46-52) – Puertos libres en caso de un futuro crecimiento en la empresa.

Tomando en cuenta el estudio realizado y los dispositivos escogidos, el esquema de la red LAN para la sede de San Martín se muestra a continuación:

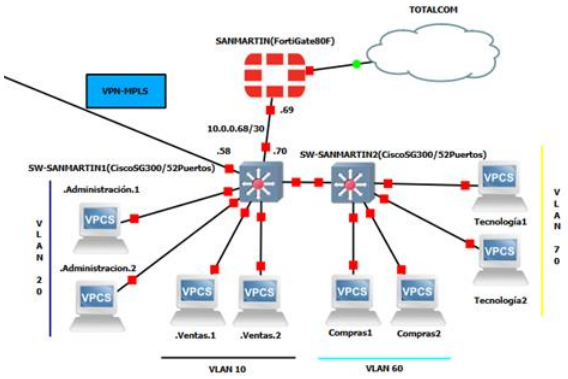

Fig. 16: Diseño de la topología de red física: Sede San Martín (Realizado en GNS3)

Diagrama de Red (Incluyendo los Servicios en la Nube).

Mediante un análisis de los requerimientos de la red y los servicios a prestar, se diseñó y planteo un diagrama que permita representar la arquitectura de la red propuesta, el mismo se muestra a continuación.

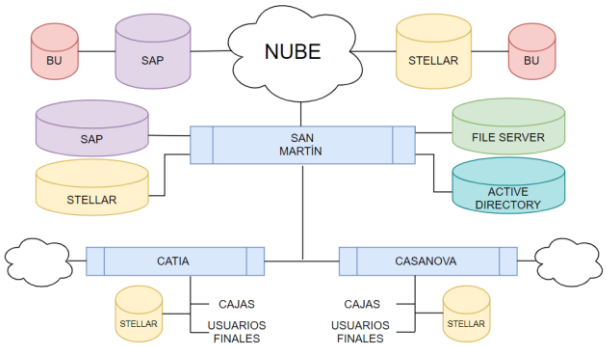

Fig. 17: Diagrama de Red incluyendo servicios en la nube.

Cuenta con servidores alojados en la nube y de forma local, los mismos serán parte fundamental de los procesos y actividades empresariales, en conjunto con el diseño de las redes locales de cada sede.

Se puede observar en el diagrama que las sedes de Catia y Casanova sólo cuentan con servidores Stellar, a diferencia de la sede Principal San Martin donde sumado a este, están presente el servidor *SAP*, el *Active Directory* y el *File Server*. A su vez se evidencia la presencia de los servidores principales SAP y Stellar ubicados en la nube, con su respectivo respaldo.

Este diseño se encuentra sustentado bajo la premisa de que al tener servidores locales y en la nube, si físicamente se presentara inconvenientes con respecto a la conectividad entre empresas con el servicio MPLS, se pueda mantener la operatividad de la empresa debido a la presencia de los servidores principales en la nube. De igual forma, si ocurre un corte de conexión con el proveedor de internet (es decir, ocurre una falla en la comunicación con la nube), la presencia de los servidores locales en cada una de las sucursales permite la continuidad de las actividades de la empresa debido a su comunicación MPLS.

Es importante mencionar que el servicio de *Microsoft Office 365* se obtiene únicamente haciendo el contacto con el proveedor que lo brinda, manteniendo total conocimiento de sus términos y condiciones de uso.

2) Diseño de la topología lógica e inalámbrica

Para esta parte del diseño se realizó el direccionamiento de la red y la asignación de VLANs para los diferentes departamentos y redes inalámbricas de cada sucursal. Se debe destacar que para ambos aspectos (direccionamiento y VLANs) se tomaron en cuenta los servidores existentes de la empresa y la creación de 3 subredes inalámbricas: Empleados, Gerencia y Cortesía.

Direccionamiento Privado

TABLA IV

Direcciones de Red Privadas

Sedes	San Martín	Casanova	Catia
N° de Hosts	254	254	126
IP de Red	172.16.1.0/24	172.16.2.0/24	172.16.3.0/25
Máscara	255.255.255.0	255.255.255.0	255.255.255.128
Primer Host	172.16.1.1	172.16.2.1	172.16.3.1
Último Host	172.16.1.254	172.16.2.254	172.16.3.126
Broadcast	172.16.1.255	172.16.2.255	172.16.3.127

A pesar de conocer la cantidad específica de usuarios finales (cantidad observada en los datos arrojados por la encuesta realizada), se decidió asignarle a cada sede un número mayor de direcciones IP privadas para prever un futuro crecimiento de la empresa.

Sede Catia: Dirección de red – 172.16.3.0/25

TABLA V

Direccionamiento Sede Catia

Subredes	Ventas	Admin.	Bodegón	Factura.	Emple.	Gerencia	Cortesía (por fuera)	Server	Enlace Forti-Switch
N° de Hosts	14	14	14	14	2	2	2	2	2
IP de Red	172.16.3.0/28	172.16.3.16/28	172.16.3.32/28	172.16.3.48/28	172.16.3.64/30	172.16.3.68/30	172.16.3.72/30	172.16.3.76/30	10.0.0.60/30
Máscara	.240	.240	.240	.240	.252	.252	.252	.252	.252
Primer Host	.1	.17	.33	.49	.65	.69	.73	.77	.61
Último Host	.14	.30	.46	.62	.66	.70	.74	.78	.62
Broadcast	.15	.31	.47	.63	.67	.71	.75	.79	.63

Sede Casanova: Dirección de Red – 172.16.2.0/24

TABLA VI

Direccionamiento Sede Casanova

Subredes	Ventas	Admin.	Bodegón	Base de Datos	Emple.	Gerencia	Cortesía (por fuera)	Server 1	Server 2	Enlace Forti-Switch
N° de Hosts	30	30	30	30	6	6	6	2	2	2
IP de Red	172.16.2.0/27	172.16.2.32/27	172.16.2.64/27	172.16.2.96/27	172.16.2.128/29	172.16.2.136/29	172.16.2.144/29	172.16.2.152/30	172.16.2.156/30	10.0.0.64/30
Máscara	.224	.224	.224	.224	.248	.248	.248	.252	.252	.252
Primer Host	.1	.33	.65	.97	.129	.137	.145	.153	.157	.65
Último Host	.30	.62	.94	.126	.134	.142	.150	.154	.158	.66
Broadcast	.31	.63	.95	.127	.135	.143	.151	.155	.159	.67

Sede San Martín: Dirección de Red – 172.16.1.0/24

TABLA VII

Direccionamiento Sede San Martín

Subredes	Ventas	Admin.	Compras	Tecno.	Emple.	Gerencia	Cortesía (por fuera)	Enlace Forti-Switch
N° de Hosts	30	30	30	30	6	6	6	2
IP de Red	172.16.1.0/27	172.16.1.32/27	172.16.1.64/27	172.16.1.96/27	172.16.1.128/29	172.16.1.136/29	172.16.1.144/29	10.0.0.68/30
Máscara	.224	.224	.224	.224	.248	.248	.248	.252
Primer Host	.1	.33	.65	.97	.129	.137	.145	.69
Último Host	.30	.62	.94	.126	.134	.142	.150	.70
Broadcast	.31	.63	.95	.127	.135	.143	.151	.71

Asignación de las VLANs

Para asignar cada una de las VLANs se tomaron en cuenta cada uno de los departamentos en cada sede, y además las redes inalámbricas creadas:

- VLAN 10: Ventas
- VLAN 20: Administración
- VLAN 30: Bodegón
- VLAN 40: Facturación
- VLAN 50: Base de Datos
- VLAN 60: Compras
- VLAN 70: Tecnología
- VLAN 80: Empleados
- VLAN 90: Gerencia
- VLAN 100: Cortesía

D. Fase IV: Proceso de interconexión de las sedes.

Para poder interconectar cada una de las sucursales de la empresa Arabito con el servicio de VPN-MPLS se tuvo que contactar con proveedores que pudieran brindar dicho beneficio. Los proveedores contactados para obtener información acerca de las especificaciones del servicio fueron: Movistar y Digitel ya que los mismos son los principales prestadores a nivel nacional.

Es importante mencionar que el tipo de servicio VPN-MPLS a utilizar es el peer-to-peer (igual-igual), debido a que este modelo permite utilizar el backbone del proveedor para poder

transmitir los datos de la empresa de una manera más rápida y segura. Al momento de contactar a los proveedores mencionados, se obtuvieron los siguientes precios para el servicio VPN-MPLS:

TABLA VIII

Precios Servicio VPN-MPLS por proveedor

	Movistar (Mensual)	Digitel (Mensual)
Datos	50$ por Mega	50$ por Mega
Internet	40$ por Mega	50$ por Mega

El servicio de VPN-MPLS se utilizará únicamente para transmitir datos entre las sedes, y según los requerimientos de la empresa Arabito, entre sucursales se debe de circular un total de 6 MB de datos, entonces:

- 50$ x 6 Mbits = 300$ mensuales (con cualquiera de los proveedores).

Posterior a esto, se decidieron otros dos aspectos importantes para la conexión de las sucursales de la empresa:

- El protocolo de enrutamiento a utilizar para conectar la empresa con el proveedor de la VPN-MPLS: OSPF (Open Shortest Path First).
- VPN de BackUp (respaldo): IPsec.

E. Fase V: Simulación y verificación de la red en un ambiente controlado.

Luego de decidir todos los aspectos necesarios para la red diseñada, se procedió a simular dicha red en un ambiente controlado. Para ejecutar esta parte del proyecto se utilizó la herramienta de simulación de redes GNS3, software que permitió verificar el óptimo funcionamiento de la red planificada.

Es importante mencionar que, aunque se plantea que el servicio de MPLS sea brindado por un proveedor de servicios en específico, para poder simular la red en su totalidad, se realizó un diseño sencillo del mecanismo de transporte de datos MPLS para así poder visualizar de una manera más clara los beneficios que dicho servicio ofrece a esta arquitectura de red empresarial. El esquema realizado para el core MPLS, tanto físico como lógico se muestra a continuación:

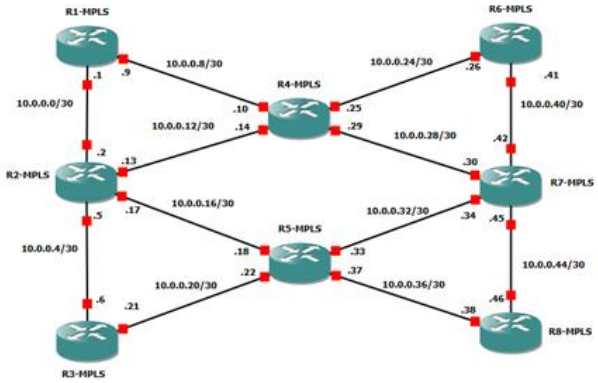

Fig. 18: Core MPLS (Realizado en GNS3)

TABLA IX

Esquema Lógico Core MPLS

Subred	N° de Hosts	IP de red	Máscara	Primer Host	Último Host	Broadcast
1	2	10.0.0.0/30	.252	.1	.2	.3
2	2	10.0.0.4/30	.252	.5	.6	.7
3	2	10.0.0.8/30	.252	.9	.10	.11
4	2	10.0.0.12/30	.252	.13	.14	.15
5	2	10.0.0.16/30	.252	.17	.18	.19
6	2	10.0.0.20/30	.252	.21	.22	.23
7	2	10.0.0.24/30	.252	.25	.26	.27
8	2	10.0.0.28/30	.252	.29	.30	.31
9	2	10.0.0.32/30	.252	.33	.34	.35
10	2	10.0.0.36/30	.252	.37	.38	.39
11	2	10.0.0.40/30	.252	.41	.42	.43
12	2	10.0.0.44/30	.252	.45	.46	.47
13	2	10.0.0.48/30	.252	.49	.50	.51
14	2	10.0.0.52/30	.252	.53	.54	.55
15	2	10.0.0.56/30	.252	.57	.58	.59

Para verificar el correcto funcionamiento del mismo, se conectaron 2 VPCS, identificadas como PC1 y PC2, en ambos extremos del core y se utilizó el comando “ping” para verificar la comunicación entre ambas.

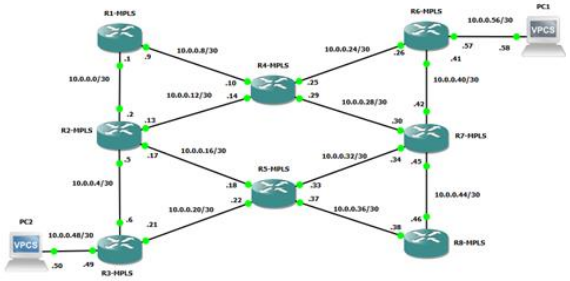

Fig. 19: Verificación del funcionamiento del Core MPLS

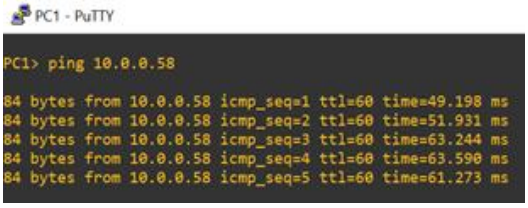

Fig. 20: Comunicación de la PC1 y PC2 utilizando el comando "ping"

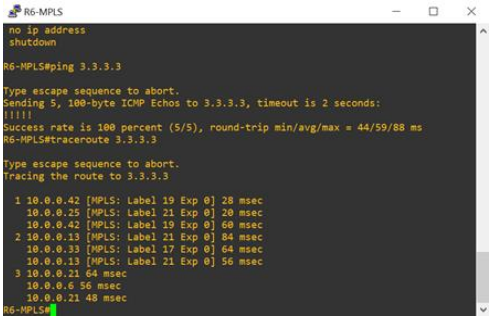

Fig. 21: Proceso MPLS desde R6-MPLS a R3-MPLS

Posterior a la verificación del funcionamiento del core MPLS, se procedió a realizar las configuraciones necesarias a los dispositivos LAN (switches, routers y firewalls) de las redes de cada una de las sucursales para la convergencia total de la red, dentro de dichas configuraciones se destacan: direcciones IP (DHCP), VLANs, enrutamiento estático y dinámico (OSPF), VPN IPsec, listas de acceso, entre otros.

Luego de confirmar la convergencia total de la red, se ejecutaron las líneas de comando que dieran seguridad a los equipos de la red, como por ejemplo claves de consola, claves de acceso, protocolo SSH (Secure Shell), banner motd, entre otros.

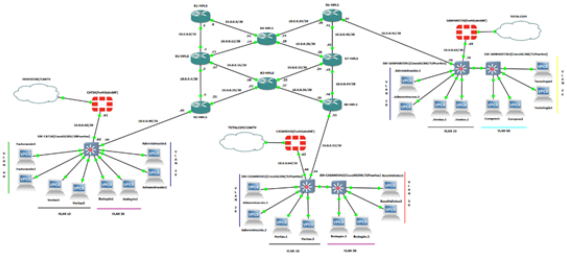

Fig. 22: Red Telemática de Arabito en total convergencia.

F. Fase VI: Fases de migración hacia la nueva red.

Luego de haber diseñado, verificado y aprobado la totalidad de la nueva red, se planificó y se redactó un documento escrito en donde se reflejara un planteamiento de migración desde la red que existe actualmente en la empresa a la diseñada en este proyecto, en este se encuentran procedimientos, estrategias y fases para que la empresa las pueda seguir de tal forma que su desenvolvimiento y sus actividades se vean afectadas en la menor medida posible durante la transición y así lograr con éxito este proceso.

VI. CONCLUSIONES Y RECOMENDACIONES

A. Conclusiones

En la actualidad es común presenciar un aumento de los parámetros básicos que comprometen el funcionamiento eficiente de las redes de datos empresariales, el número de usuarios que acceden a las mismas influyen en la manera que se desempeña, tomando en cuenta las solicitudes de servicios y requerimientos de los mismos. Con la aparición de los nuevos sistemas operativos y aplicaciones de nueva generación, es de vital importancia como empresa ofrecer total disponibilidad y operatividad de la red, utilizando nuevas infraestructuras de telecomunicaciones y de redes que puedan optimizar la resolución de las exigencias y demandas de una conectividad continua de los usuarios, dado el crecimiento y la variedad de los dispositivos de comunicaciones existentes, otorgando la posibilidad de que, al estar la totalidad de la red empresarial en la nube con un nivel de seguridad óptimo, los empleados sean capaces de conectarse y resolver problemas en cualquier momento.

Para el diseño de red de telecomunicaciones propuesto fue necesario recopilar información relevante acerca de las características físicas del proyecto, es decir de cada sede estudiada de forma independiente. Seguidamente, a través de la investigación previa, se procedió a seleccionar y definir los servicios que forman parte del sistema y diseño, comprobando los mismos mediante una simulación realizada a través del software GNS3. En base a todo lo mencionado anteriormente se llevó a cabo la elección de los equipos.

El uso de MPLS se sustenta puesto que hoy en día representa una tecnología que se caracteriza por entregar servicios con alta seguridad y velocidad, basados en el protocolo IP. Además, MPLS sustituirá con el tiempo las configuraciones basadas sólo en el enrutamiento tradicional, gracias a la alta velocidad de enrutamiento y a los beneficios que ofrece para la configuración del ancho de banda de la red.

GNS3 permitió la verificación de varios aspectos del diseño planteado: el funcionamiento de la red, el protocolo de enrutamiento seleccionado (OSPF), el direccionamiento y las configuraciones de las VLANs, además de la simulación del core MPLS y VPNs Site to Site.

En conclusión, el desarrollo de este Trabajo Especial de Grado permitió llevar a la práctica los conocimientos teóricos obtenidos, siendo la base para la toma de decisiones con un criterio técnico de las alternativas presentes en el mercado tecnológico, dando como resultado la red diseñada.

B. Recomendaciones

A partir del escenario planteado y el desarrollo del trabajo especial de grado, se exponen las siguientes recomendaciones con el propósito de aportar aspectos que ayuden a investigaciones y proyectos futuros relacionados al tópico, las mismas se encuentran en búsqueda de un trabajo eficiente y productivo.

1) En la etapa inicial del proyecto es de suma importancia reconocer e identificar los puntos críticos y necesidades de cada sede involucrada, se recomienda realizar un estudio en base a los obstáculos que estén presentes en la

estructura y organización, como también establecer las posibles repercusiones de la propuesta tomando en cuenta las características para el futuro diseño.

2) Con respecto al dimensionamiento de la red, se recomienda establecer estrategias en base a la predicción, de esta manera el crecimiento exponencial de la empresa es tomado en cuenta, optimizando las decisiones económicas, organizacionales y de implementación de la red, llegando a cubrir las necesidades a nivel del desempeño y rendimiento de la misma, características esenciales para la integración de todos los servicios empresariales, sirviendo como punto de partida para la expansión prevista en nuevas localidades como Las Mercedes y La Trinidad.
3) Se recomienda el estudio previo del software de simulación de redes GNS3, ya que el mismo permite la combinación de dispositivos tanto reales como virtuales de distintos proveedores, de esta manera se facilitará el proceso de la simulación del diseño de red propuesto, no obstante, se puede hacer uso de otro software y no limitarse única y exclusivamente a GNS3.
4) Se recomienda contar con un equipo adecuado para la simulación, ya que la misma exige una gran cantidad de recursos para un correcto funcionamiento, los requerimientos que se pueden prever como mínimos son los siguientes: un sistema operativo Windows 7 (64 bit) o superior, un procesador de 2 o más núcleos lógicos, extensiones de virtualización, espacio en disco disponible de 1GB, memoria RAM de 8GB o mayor y posiblemente almacenamiento adicional para las imágenes de los equipos.
5) De hacer uso de un firewall perimetral, se recomienda aplicar a los mismos, sistemas de políticas de ingreso y de egreso, a su vez de aprovechar sus funcionalidades de monitoreo, tomando en cuenta la labor de los especialistas y su aporte a la seguridad y desempeño de la red.
6) Es de suma importancia hacer un seguimiento de la red y de los cambios en la escalabilidad y necesidades de los usuarios, de esta manera se debe estar atento a futuras mejoras o reestructuraciones del proyecto, sugiriendo evaluaciones a mediano y largo plazo comprobando el estado de la misma, tomando en cuenta la modernización de la red y nuevos servicios que se presenten.
7) Se recomienda realizar un diseño de esta arquitectura de red utilizando una tecnología SD-WAN en lugar de utilizar tecnología MPLS, debido a que SD-WAN es un tipo de red que permite simplificar y consolidar mejores resultados en la topología de una red, además de que la misma se proyecta para suplantar a MPLS como servicio principal en conexiones telemáticas.

Todo lo planteado busca mejorar la toma de decisiones y optimizar la metodología de implementación de red actual en búsqueda de un manejo eficiente de los recursos y disponibilidades de la empresa en la que se desarrolla el proyecto

RECONOCIMIENTOS

A nuestros padres por ser ejemplo, inspiración, por tanto apoyo, paciencia, motivación, sostén y fuerza en cada momento de nuestras vidas.

A nuestros hermanos y familiares, por siempre ser siempre un punto de apoyo, fuente de consejos y de fuerza para continuar.

A nuestro Señor Dios, aquel que guía nuestros caminos y bendice nuestras vidas en todo momento.

A nuestra casa de estudio, la Universidad Católica Andrés Bello, y a los profesores de la Facultad y de la Escuela en Telecomunicaciones por acogernos y brindarnos todos sus conocimientos durante estos años.

A nuestro tutor, el Ingeniero Alexander Castro, por su aporte, paciencia, conocimientos, motivación, enseñanzas y su buena disposición a lo largo de todo el proyecto.

Al Ingeniero y amigo Arturo Ramírez por brindarnos sus enseñanzas, su ayuda y su apoyo incondicional desde el inicio del proyecto.

A todo el personal de Arabito y Seguros Pirámide por abrirnos sus puertas y colaborar con nuestro Trabajo Especial de Grado.

A nuestros amigos y compañeros, por siempre brindarnos su motivación y su apoyo incondicional en todo momento.

A todos y cada uno de ustedes, ¡INFINITAS GRACIAS!

REFERENCIAS BIBLIOGRÁFICAS

[1] Penalojas, D., 2020. Introducción a MPLS. Recuperado el 4 de enero de 2021. Disponible en: https://community.cisco.com/t5/documentos-routing-y switching/introducci%C3%B3n-a-mpls/ta-p/3407436

[2] Castro Ullauri, E. (2015). Diseño y Simulación de una red MPLS para interconectar estaciones remotas utilizando el simulador GNS3 (Licenciatura). Universidad Politécnica Salesiana sede Guayaquil.

[3] Orozco Lara., F. (2014). Diseño de una red privada virtual con tecnología MPLS para la Carrera de Ingeniería de Networking de la Universidad de Guayaquil (Master). Universidad Católica de Santiago Guayaquil.

[4] Menéndez Avila, R. (2012). Estudio Del Desempeño e Implementación De Una Solución MPLS-VPN Sobre Múltiples Sistemas Autónomos (Licenciatura). Pontificia Universidad Católica Del Perú.

[5] Cisco, 2008. Cómo funcionan las redes privadas virtuales. Recuperado el 17 de diciembre de 2020. Disponible en: https://www.cisco.com/c/es_mx/support/docs/security-vpn/ipsec-negotiation-ikeprotocols/14106-how-vpn-works.html

[6] Matías, L., & Millán, M. (2009). Estudio de la factibilidad de un BACKBONE MPLS para brindar servicio de VPN, para acceder a un FILE SERVER desde un punto remoto (Pregrado). Universidad Católica de Santiago de Guayaquil.

[7] Hurtado, J. (2012). *El proyecto de investigación*. Caracas, Venezuela: Quirón Ediciones.

[8] Hurtado de Barrera, J. (2010). Metodología de la investigación. Caracas, Venezuela: Quirón Ediciones.

[9] Hernández-Sampieri, R., & Mendoza Torres, C. (2018). *Metodología de la investigación*. Ciudad de México: McGraw-Hill Interamericana.

[10] Vélez, D., 2018. Diseño y Simulación en GNS3 de una Red Multiservicios MPLS para Medianas empresas en el Ecuador. Magister. Universidad Católica de Santiago de Guayaquil.

[11] Gallardo, J., 2019. Análisis de las características técnicas mínimas de los equipos de seguridad, para empresas de mediana escala, enfocados a amenazas externas a la intranet. Pregrado. Escuela Politécnica Nacional de Quito.

[12] Fortinet. (2021). Fortinet Asset. Recuperado el 12 de marzo 2021, Disponible en: https://www.fortinet.com/resources-content/fortinet/assets/data-sheets/file/fortigate-fortiwifi-80f-series

[13] JMTelcom. (2021). Firewall Fortigate 60F. Recuperado el 12 de marzo 2021, Disponible en: https://www.jmtelcom.com/product/firewall-fortigate-60f/

[14] JMTelcom. (2021). Firewall Fortigate 50E. Recuperado el 12 de marzo 2021, Disponible en: https://www.jmtelcom.com/product/fortigate-fortiwifi-50e51e/

[15] JMTelcom. (2021). Firewall Fortigate 40F. Recuperado el 12 de marzo 2021, Disponible en: https://www.jmtelcom.com/product/firewall-fortigate-40f/

[16] Intercompras. (2021). Switch Cisco SG300-52P-K9-NA 52 Puertos Gigabit PoE. Recuperado el 12 de marzo 2021, Disponible en: https://intercompras.com/p/switch-cisco-sg300-52p-puertos-gigabit-poe-administrable-68216

[17] Intercompras. (2021). Switch Cisco SG300-28PP-K9-NA 28 Puertos Gigabit. Recuperado el 12 de marzo 2021, Disponible en: https://intercompras.com/p/switch-cisco-sg300-puertos-gigabit-poe-87564

[18] WNI. (2021). UniFi AC Lite. Punto de Acceso 802.11ac de Banda-Dual, MIMO.Recuperado el 12 de marzo 2021, Disponible en: https://wni.mx/index.php?page=shop.product_details&category_id=40&flypage=flypage_new.tpl&product_id=696&option=com_virtuemart&Itemid=48

[19] TP-Link Colombia. (2021). TL-WR941HP | Router de Alta Potencia de hasta 450Mbps. Recuperado el 12 de marzo 2021, Disponible en: https://www.tp-link.com/co/home-networking/high-power-router/tl-wr941hp/

[20] Aguilar G, K. (2008). Desarrollo de procesos para el producto Redes Virtuales Privadas IP/MPLS en Capa 3 (Licenciatura). Universidad Católica Andrés Bello.

[21] Atouguia Dos Santos, J. (2008). Redes Privadas Virtuales (VPN) y calidad de servicio (QOS) en redes de conmutación de paquetes (IPV4) basados en el protocolo de conmutación de etiquetas (MPLS). (Licenciatura). Universidad Católica Andrés Bello.

[22] Camacho R, M., & Carrillo C, M. (2013). Diseño de una VPN para la conexión y sincronización entre los servidores para las aplicaciones en Tele salud ubicado en los grupos de Física Médica (UCV) y Telemedicina (UCAB) (Licenciatura). Universidad Católica Andrés Bello.

[23] González Morales, A. (2006). Redes Privadas Virtuales (Licenciatura). Universidad Autónoma del Estado de Hidalgo.

[24] Islas Mendoza, E. (2013). Protocolo Diffie Hellman utilizando los criptosistemas ElGamal y AES (Maestría). Instituto Politécnico Nacional Centro de Innovación y Desarrollo Tecnológico en Cómputo.

[25] Kaur, R., Hils, A., D´Hoinne, J. and Watts, J., 2019. Magic Quadrant for Network Firewalls. 1st ed.

[26] Morales, L., 2006. Investigación De Redes VPN Con Tecnología MPLS. Licenciatura. Universidad de las Américas Puebla.

[27] Peña, D. (2016). Diseño e Implementación de una Red Privada Virtual (VPN-SSL) utilizando el método de autenticación LDAP en una empresa privada (Postgrado). Universidad Central de Venezuela.

[28] Trujillo Machado, E. (2006). Diseño e implementación de una VPN en una empresa comercializadora utilizando IPSEC (Licenciatura). Escuela Politécnica Nacional.