Universidad Católica Andrés Bello

Facultad de Ingeniería

Escuela de Telecomunicaciones

# DISEÑO DE UNA RED PARA LA EMPRESA ARABITO CON SOLUCIÓN EN LA NUBE EN SU SEDE PRINCIPAL INTERCONECTANDO SUS SUCURSALES MEDIANTE VPN MPLS.

**TRABAJO ESPECIAL DE GRADO**

Presentado ante la

**UNIVERSIDAD CATÓLICA ANDRÉS BELLO**

Como parte de los requisitos para optar al título de

**INGENIERO EN TELECOMUNICACIONES**

**REALIZADO POR:** Br. Cabrera Albornoz, Omar Alejandro

Br. Cordero Hernández, Richard Eduardo

**TUTOR:** Ing. Castro Borges, Alexander José

Caracas, Agosto del 2021

**Diseño de una red para la empresa Arabito con solución en la nube en su sede principal interconectando sus sucursales mediante VPN MPLS.**

Universidad Católica Andrés Bello

Facultad de Ingeniería

Escuela de Telecomunicaciones

# DISEÑO DE UNA RED PARA LA EMPRESA ARABITO CON SOLUCIÓN EN LA NUBE EN SU SEDE PRINCIPAL INTERCONECTANDO SUS SUCURSALES MEDIANTE VPN MPLS.

**TRABAJO ESPECIAL DE GRADO**

Presentado ante la

**UNIVERSIDAD CATÓLICA ANDRÉS BELLO**

Como parte de los requisitos para optar al título de

**INGENIERO EN TELECOMUNICACIONES**

**REALIZADO POR:** Br. Cabrera Albornoz, Omar Alejandro

Br. Cordero Hernández, Richard Eduardo

**TUTOR:** Ing. Castro Borges, Alexander José

Caracas, Agosto del 2021

**Diseño de una red para la empresa Arabito con solución en la nube en su sede principal interconectando sus sucursales mediante VPN MPLS.**

Universidad Católica Andrés Bello

Facultad de Ingeniería

Escuela de Telecomunicaciones

# DISEÑO DE UNA RED PARA LA EMPRESA ARABITO CON SOLUCIÓN EN LA NUBE EN SU SEDE PRINCIPAL INTERCONECTANDO SUS SUCURSALES MEDIANTE VPN MPLS.

**Este Jurado; una vez realizado el examen del presente trabajo ha evaluado el contenido con el resultado:**

---

J U R A D O  E X A M I N A D O R:

Firma: Firma: Firma:

Nombre:_____ Nombre:_____ Nombre:_____

**REALIZADO POR:** Br. Cabrera Albornoz, Omar Alejandro

Br. Cordero Hernández, Richard Eduardo

**TUTOR:** Ing. Castro Borges, Alexander José

## RESUMEN


### DISEÑO DE UNA RED PARA LA EMPRESA ARABITO CON SOLUCIÓN EN LA NUBE EN SU SEDE PRINCIPAL INTERCONECTANDO SUS SUCURSALES MEDIANTE VPN MPLS.



**Cabrera Albornoz, Omar Alejandro.** Correo: cabreraomarr13@gmail.com

**Cordero Hernández, Richard Eduardo.** Correo: richardcordero2006@gmail.com



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 prestarían 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.

## DEDICATORIA

*"Un sueño no se hace realidad por arte de magia, necesita sudor, determinación y trabajo duro" - Colin Powell*

*Desde la creación del ser humano, el mismo siempre busca plantearse metas y busca logarlas/cumplirlas a lo largo de su vida, claro está que no todas son sencillas y que además se presentan ciertas dificultades al momento de su ejecución, pero con apoyo y trabajo duro el final siempre será exitoso.*

*Las grandes batallas se luchan poco a poco, y se logran conquistar con cualidades como la fé, la humildad, la honestidad, la perseverancia, el respeto, la paciencia, entre otros, pero además también es necesario el apoyo y la motivación de todas aquellas personas que de alguna manera u otra juegan papeles importantes en el proceso. A todas ellas dedico este Trabajo Especial de Grado:*

*Principalmente a mi padre, que está en el cielo, y a mi madre por todo el esfuerzo, apoyo, confianza, motivación e inspiración que permitieron realizar mis estudios, por enseñarme todos aquellos valores e ideales que hoy en día me forman como persona y como profesional.*

*A mis dos hermanas, Andrea e Isabella, que siempre han estado a mi lado, ayudándome a mejorar y brindándome su apoyo incondicional. Además, poder demostrarles que con orden y perseverancia se puede lograr cada meta planteada.*

*A mis tíos, primos y abuelos por brindarme sus enseñanzas y sus consejos a lo largo de mi vida, mostrar que determinación podemos conseguir todo lo propuesto.*

*Y para finalizar, a mi grupo de amigos, Elite, que a pesar de la distancia estuvieron presente en todo momento para impulsarme a seguir adelante e inspirándome a continuar y a concluir mis estudios de manera exitosa. Cada uno de ustedes son fundamentales en mi crecimiento.*

*"Estudia, Aprende y Vive"*

*Omar Alejandro Cabrera Albornoz*

## DEDICATORIA

*"Todos los triunfos nacen cuando nos atrevemos a comenzar" – Eugene Ware*

*La voluntad continuada en la determinación de hacer una cosa hasta alcanzarla nos caracteriza como seres humanos, pero es la curiosidad la que nos permite aspirar o buscar cosas más allá de los límites establecidos, el proceso no es nada fácil, precisamente la dificultad da valor al cometido, es por esto que el apoyo de la gente que nos rodea es tan importante en el camino.*

*La influencia en nuestras vidas dada por todas aquellas personas que constantemente formaron parte del proceso, es esencial en lo que somos y aspiramos, queriendo dedicar a las mismas este Trabajo Especial de Grado.*

*Primeramente a mi padre, hasta el cielo, al cual tengo como ejemplo de cómo ser un buen hombre, gracias por enseñarme tantos valores, este sueño cumplido es por y para ti, espero estés orgulloso de en quien me convertí y me acompañes siempre. De igual forma a mi madre, gracias por ser mi pilar fundamental, por tus consejos, paciencia y amor incondicional, son todo para mí, los amo con mi vida.*

*A mis familiares, por su persistente preocupación, motivación y ayuda, en especial a mi abuela, hermana, mamá Yacke y papa Gregorio, gracias por demostrarme que podemos conseguir todo lo que nos proponemos con disciplina y constancia.*

*Por último, a mis amigos y compañeros presentes en cada etapa del trayecto, son fuente de admiración para mí, agradezco haber coincidido con cada uno de ustedes, y espero seguir aprendiendo juntos.*

*Todos ustedes, sin excepción, forman parte de mi desarrollo como persona, y espero se mantengan presentes en mi vida.*

*"La determinación siempre será el primer paso en cada logro"*

*Richard Eduardo Cordero Hernández*

## AGRADECIMIENTOS

*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!*

# ÍNDICE GENERAL

## ÍNDICE DE FIGURAS

# ÍNDICE DE TABLAS

# INTRODUCCIÓN

A continuación se presenta el Trabajo Especial de Grado que consiste en diseñar una nueva 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, 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.

En el Capítulo I se presenta el planteamiento del proyecto y la justificación del mismo, también se encuentran los objetivos que se buscan alcanzar durante el diseño de la red, y por último las limitaciones y alcances del trabajo. Luego, el Capítulo II contiene la investigación de conceptos teóricos que hacen referencia a: *Multi-Protocol Label Switching* (MPLS), *Virtual Private Network* (VPN), *IP security* (IPsec) y sus algoritmos de seguridad, *Tunneling* y además VPN-MPLS y sus tipos.

El Capítulo III comprende la metodología y el desarrollo del proyecto, en el mismo se explica cada una de las seis (6) fases y las actividades realizadas para alcanzar los objetivos planteados. Posteriormente en el Capítulo IV se encuentran los resultados obtenidos en cada una de las actividades ejecutadas, estas se encuentran formadas por: la recopilación de información técnica de las tecnologías, los datos importantes acerca de la red actual de la empresa y de los

dispositivos de redes a utilizar, además se encuentra el diseño físico, lógico e inalámbrico de cada sede de la empresa en donde se incluye el direccionamiento IP, diseño de las VLANs la selección de los equipos físicos, el contacto con los proveedores para determinar el tipo de servicio y el precio del mismo, el esquema general de la nueva red de la empresa y su simulación a través del software de simulación *GNS3* y por último se encuentran las recomendaciones para realizar una migración óptima de la red actual a la diseñada en este trabajo.

Seguidamente, en el Capítulo V se presentan las conclusiones y recomendaciones realizadas, que son producto de la elaboración y ejecución del Trabajo Especial de Grado, es importante destacar que toda información mostrada en este documento está sustentada en las fuentes bibliográficas presentadas.

## GLOSARIO

***Active Directory (AD)***. Es una base de datos y un conjunto de servicios que contiene información crítica sobre su entorno, incluidos los usuarios y las computadoras que hay y quién puede hacer qué (Quest, s.f).

***File Server.*** Es una instancia de servidor central de una red de ordenadores que permite a los clientes conectados acceder a sus propios recursos de almacenamiento (Ionos, 2019).

***MPLS.*** *Multi-Protocol Label Switching.*

***SAP.*** *Systems, Applications, Products in Data Processing*. Es uno de los principales productores mundiales de software para gestión de procesos de negocio, y desarrolla soluciones que facilitan el procesamiento eficaz de datos y el flujo de información entre las organizaciones (SAP, s.f).

***Stellar.*** Empresa que brinda servidores en la nube.

***VPN.*** *Virtual Private Network.*

# CAPÍTULO I

# PLANTEAMIENTO DEL PROYECTO

En este capítulo se expone toda la descripción y desarrollo de la necesidad de diseño de una nueva red de datos en la empresa *Arabito* que pueda interconectar todas sus sedes en el Distrito Capital mediante la utilización de la tecnología ***VPN MPLS***, considerando soluciones en la nube en la sede principal incluyendo: *SAP* y *Office/Microsoft 365*. Cabe destacar que además se exponen los objetivos planteados, la justificación de los mismos, los alcances y las limitaciones que se encuentran relacionados con la ejecución del proyecto.

## I.1 PLANTEAMIENTO DEL PROBLEMA

Venezuela actualmente se encuentra atravesando una situación socio-económica que afecta en gran medida el crecimiento de las empresas, este escenario se ha vuelto más complicado con el pasar de los años. Cada una de las mismas está expuesta a muchas circunstancias las cuales obligan a buscar alternativas para lograr su desarrollo y evolución, enfrentándose a un sin número de vicisitudes dentro de un mercado cambiante, producto de factores tales como inseguridad, transporte, baja calidad de los servicios básicos, los altos costos de los productos, escenario político; agudizados en este año por la pandemia ocasionada por el COVID-19, aspectos que obligan a encaminar sus operaciones hacia el teletrabajo.

Una de estas empresas es *Arabito*, Restaurante/Panadería/Bodegón, reconocido 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.

Para lograr la implementación de una plataforma tecnológica en la nube segura, se debe corregir uno de los mayores problemas que presenta esta organización, su arquitectura de red de datos, esto debido a que, si una red de datos LAN no es bien diseñada y administrada, puede ser objeto de alteración o de extracción de información, ataques cibernéticos, bajo performance de las operativas diarias, causando así una cantidad importante de pérdidas para la empresa. 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.

Los nuevos sistemas operativos y aplicaciones de nueva generación obligan a utilizar 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. Sumado a esto, se debe otorgar 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 realizar teletrabajo en pro de la empresa.

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.

## I.2 OBJETIVOS

### I.2.1 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.

### I.2.2 OBJETIVOS ESPECÍFICOS

I. Realizar el levantamiento de información de la infraestructura tecnológica actual en la sede principal *Arabito* y sus sucursales.

II. 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*.

III. 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.

IV. 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.

V. Realizar pruebas de rendimiento y seguridad de la arquitectura de red propuesta en un ambiente controlado.

VI. Establecer los procedimientos para las fases de migración hacia la nueva plataforma tecnológica.

## I.3 ALCANCES Y LIMITACIONES

La puesta en acción definitiva del prototipo de la red diseñada, se realizó en un ambiente de operación con distintas variables controladas tomadas en consideración en los proyectos de redes y puesta en producción de todos los productos y servicios que pueda brindar la empresa *Arabito*. Las variables mencionadas incluyen:

- Los recursos y el tiempo disponible brindados por la empresa (ya sean técnicos y/o humanos).
- El acceso a la información técnica de los equipos ya usados.
- Aprobación otorgada por las unidades que se encargan de la operación y de la continuidad de los servicios y las redes.

Dicho esto, se definieron de la siguiente manera los alcances y las limitaciones que incluye este Trabajo de Grado:

**Alcances:** Este trabajo de grado incluye los siguientes alcances:

- Se elaboró un plan que contiene una plataforma de servidores *core* y *Microsoft 365* en la nube mediante la interconexión de sus sedes con de tecnología MPLS.

- Diseño de la arquitectura de la red que permite interactuar entre las sedes bajo la combinación de red LAN, MPLS y nube privada.
- Evaluación del diseño propuesto de la red elaborada, controlado y verificado bajo un ambiente pre-productivo donde se realizaron todas las pruebas de certificación con los equipos de comunicación necesarios para el proyecto, tales como *routers*, *switches*, entre otros.

**Limitaciones:**

- Este trabajo de grado sólo abarcó las sedes ubicadas en Catia, Sabana Grande y San Martín. Para este trabajo de tesis no se contempló la segunda fase de expiación donde se tiene proyectado la apertura de nuevas localidades en Las Mercedes y La Trinidad.
- Este trabajo de grado abarcó hasta simulaciones y un prototipo de la solución más no la implementación en físico del mismo, debido a las complicaciones que generalmente conlleva el montaje de una red de esta magnitud ocasionando que algunos objetivos puedan no ser cumplidos para los tiempos y el alcance del trabajo.

## I.4 JUSTIFICACIÓN

Con la realización de este proyecto, se busca alcanzar una propuesta de diseño de red óptima que mediante la utilización de la tecnología VPN MPLS, permita una mejora en el desempeño y funcionamiento tecnológico de la empresa, considerando

esenciales las soluciones en la nube en la sede principal, en la cual confluye gran cantidad de información importante, para ser distribuida en la totalidad de las sedes.

El presente trabajo busca obtener un grado razonable en la precisión del estudio de las tecnologías VPN MPLS, sus beneficios y aplicaciones, brindando de esta manera un enfoque coherente en la caracterización del diseño.

# CAPÍTULO II

# MARCO TEÓRICO

En el presente capítulo del trabajo especial de grado se describen los conceptos teóricos fundamentales, descripciones de procedimientos, desglose de los tipos de estructuras características que definen y forman parte de las tecnologías MPLS y VPN, y además, ciertos tipos de encriptación de datos y otros puntos que guardan total relación con el trabajo de grado realizado.

## II.1 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 (Conmutación Multi-Protocolo mediante Etiquetas) usando una VPN (Red Privada Virtual). 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 (Penalojas, 2020).

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 (Penalojas, 2020).

MPLS exige un marco de trabajo orientado a conexión en un ambiente de internet basado en IP facilitando el uso de los contratos de tráfico de *QoS* exigentes.

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 (Penalojas, 2020). 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 (Penalojas, 2020).

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 (por esta razón se establece que MPLS está orientada a conexión) (Castro, 2015).

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* (Castro, 2015).

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 (Castro, 2015).


***Figura 1:*** *Funcionamiento MPLS. Extraído de: (Penalojas, 2020)*

### II.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 (como lo pueden ser ATM, *Frame Relay* y Ethernet), envía este tráfico a través de la red MPLS después de haber establecido un LSP (caminos conmutados mediante etiquetas) 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 (Orozco, 2014).
- **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. Además de esto, los *routers* LSR en MPLS se clasifican en base a la dirección del flujo de los datos, como *routers* ascendentes

(*upstream*, origen) o descendentes (*downstream*, destino). 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) (Orozco, 2014).

- **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 (Orozco, 2014).
- **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 (Orozco, 2014).

- **Dominio MPLS:** es la parte de la red donde los diversos procedimientos de enrutamiento y de envío están acorde con el protocolo MPLS (Orozco, 2014).
- **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 específico 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 (Orozco, 2014).

### II.1.3 BENEFICIOS DE MPLS

- El eje troncal o *backbone* tiene permitido expandirse de modo de transferencia asíncrona (ATM) y *Frame Relay* (FE) de capa 2, ambas sobre las capacidades

de la ingeniería de tráfico, la misma es esencial para los ejes troncales de proveedores de servicio los cuales están obligados a soportar un uso elevado de transmisión **(**Menéndez, 2012.).

- Las capacidades de ingeniería de tráfico mediante la utilización de **MPLS** son incorporadas a la capa 3 del modelo OSI, esta acción genera la mejora del ruteo del tráfico reconociendo la labor de las pautas establecidas por la topología aunado a las capacidades de la troncal (Morales, 2006.)**.**
- En el momento de enrutamiento del flujo de tráfico, la ingeniería de tráfico de **MPLS** se basa fielmente en los recursos que el mismo flujo requiere además de los disponibles en la totalidad de la red (Morales, 2006.)**.**
- Tomando en cuenta distintos requisitos tales como ancho de banda, de medios y prioridad sobre otros flujos MPLS usa la ruta más corta que cumpla con dichos requisitos del flujo de tráfico (Menéndez, 2012.).
- Al estar basado en etiquetas y no en direcciones IP de destino la conmutación de paquetes es más rápida (Morales, 2006.).
- Total independencia de las redes de clientes (**VPN-MPLS**) **(**Menéndez, 2012.).
- Es Multi-Protocolo (Morales, 2006.)**.**
- Uso del ancho de banda en acceso eficiente (full-mesh virtual) (Morales, 2006.).

## II.2 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 (Menéndez, 2012).

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 (Menéndez, 2012). 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 (Cisco, 2008).

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 (Cisco, 2008).

### II.2.1 VENTAJAS DE LAS VPN

- Otorga mejores niveles de seguridad a las conexiones, con algoritmos de cifrado y autenticación avanzados.
- Ayudan a evitar los bloqueos geográficos en las redes.
- Gracias a los niveles de seguridad que tiene, garantiza un ambiente de trabajo seguro en un entorno corporativo.
- Reducción de costos en procesos de conectividad remota.

### II.2.2 DESVENTAJAS DE LAS VPN

- Pueden llegar a disminuir la velocidad de conexión a una red.

- Así como son útiles para saltar bloqueos regionales, también pueden generar nuevos bloqueos.
- Muchas veces los usuarios de estas, no tienen la certeza de la calidad de los procesos de cifrado.
- Los buenos servicios de VPN suelen ser costosos, existen servicios gratis pero estos pueden no tener buenos niveles de seguridad.

### II.2.3 REQUISITOS PARA UNA VPN

Para una red VPN se poseen ciertos requisitos que se pueden agrupar en cuatro áreas principales las cuales son:

- **Compatibilidad:** principalmente para que una VPN pueda utilizar Internet, esta debe tener compatibilidad con el Protocolo de Internet (IP). Se puede considerar obvia esta consideración con el fin de poder asignar y utilizar ciertos conjuntos de direcciones IP. Sin embargo, la mayoría de las VPN utilizan direcciones IP privadas, ocasionando que únicamente unas pocas puedan ser empleadas para poder interactuar con Internet. La razón por la que sucede esto es debido a que la obtención de un bloque de direcciones IP oficiales que sea suficientemente grandes para realizar un *subnetting* es casi imposible. Las subredes simplifican la administración de direcciones, así como la operabilidad de los enrutadores y switches, pero lo malo es que malgasten direcciones IP preciadas. Actualmente existen diversas técnicas que permiten obtener cierta compatibilidad entre las VPN e internet, técnicas como por ejemplo NAT (*Network Address Translation*) y el empleo de

*Tunneling*. En la técnica NAT, las direcciones IP oficiales van a coexistir con redes IP privadas en la parte interna de la red organizacional. Ocasionando que, de este modo, un usuario con una IP privada pueda acceder al exterior de la red mediante un servidor de direcciones IP públicas sin necesidad de emplear ningún tipo de acción especial (Peña, 2016).

- **Seguridad:** al utilizar Internet, debe de considerarse seriamente este aspecto de seguridad, ya que las comunicaciones que se van a realizar no van a estar confinadas a circuitos privados, sino que van a ser capaces de navegar a través de internet, una red muy pública para poder realizar cualquier tipo de comunicación privada. Cuando la información se encuentra encriptada, se deben de requerir algunas claves para poder cifrar y descifrar, y cada uno de los usuarios que se encuentran a los extremos deben poseer la clave adecuada. Si se configura una conexión con una sede es relativamente sencillo administrar el uso e intercambio de dichas claves, sin embargo, si un usuario remoto accede a la red privada, se necesita con urgencia un modo de poder verificar en primer lugar quién es y luego encontrar un modo de poder intercambiar las claves de encriptación. Las claves públicas que están basadas en PKI y certificados digitales, son las más utilizadas (Peña, 2016).
- **Disponibilidad:** este aspecto viene motivado principalmente por dos variables: una accesibilidad plena e independiente del momento y del lugar, y un rendimiento óptimo que vaya a garantizar la calidad de servicio que es ofrecida al usuario final. La cualidad de servicio (o *QoS: Quality of Service*) puede venir dada como una cierta cantidad de ancho de banda o un retraso que

no debe sobrepasarse (o una combinación de ambas). No obstante, en un futuro, Internet será capaz de sustituir esta carencia ya que ofrecerá un soporte para la *QoS* a través de distintos protocolos, pero por ahora, los proveedores de internet solo proporcionan la cualidad del servicio de las VPN haciendo uso del CIR (*Committed Information Rate*) en *Frame Relay* u otras técnicas conocidas como por ejemplo lo es MPLS (Peña, 2016).

- **Interoperabilidad:** los diversos estándares sobre el *tunneling*, autenticación, encriptación y modos de operaciones que ya han sido mencionados anteriormente son de nuevo conocimiento o bien se encuentran en un proceso de desarrollo avanzado. Es por esta razón que, antes de la adquisición de una tecnología VPN, se debe estar atento a una interoperabilidad de extremo a extremo. Esta responsabilidad puede caer tanto en el usuario final como en el proveedor de internet de la red, esto depende de la implementación que se desee realizar. Una manera de poder asegurar una correcta interoperabilidad radica en la elección de una solución que sea completa y que sea ofrecida por un mismo fabricante, en el caso de que dicho fabricante no sea capaz de satisfacer todos los requisitos, los aspectos inter operacionales deben ser limitados a un subconjunto que vaya a englobar todos aquellos que sean esenciales, además de utilizar únicamente aquel equipamiento que haya sido sometido a pruebas o probados en un laboratorio (Peña, 2016).

## II.3 PROTOCOLO IPSEC

Según (Trujillo, 2006) IPSec en realidad es un conjunto de estándares para integrar en IP, funciones de seguridad basadas en criptografía.

Las tecnologías de clave pública como RSA, algoritmos de cifrado (tales como DES, 3DES, IDEA, *Blowfish*), los algoritmos de hash (MD5, SHA-1) y certificados digitales *X509v3*, son combinados en la búsqueda de proporcionar confidencialidad, integridad y autenticidad de datagramas IP (Trujillo, 2006).

La concepción y diseño del protocolo IPSec ha sido en su totalidad de forma modular, de esta manera se evita afectar partes de la implementación que no están relacionados con la selección del conjunto de algoritmos deseados. Para asegurar la interoperabilidad es necesario que se definan distintos algoritmos encargados de soportar las implementaciones en el mundo global de Internet. Dichos algoritmos de referencia son DES y 3DES, para cifrado, así como MD5 y SHA-1, como funciones de HASH. El uso de estos algoritmos no limitará la implementación de otros ya que pueden existir algunos que el usuario considere más seguros o más adecuados en su uso para un entorno específico. (Trujillo, 2006).

### II.3.1 COMPONENTES DE IPSEC

**Protocolos de Seguridad:** encargados de suministrar los mecanismos de seguridad necesarios para la protección del tráfico IP (Trujillo 2006).

- IP *Authentication Header* (AH)
- IP *Encapsulating Security Payload* (ESP)

**Protocolo de Gestión de Clave:** posibilita la negociación de las claves a dos nodos en conjunto de todos los parámetros necesarios para establecer una conexión AH o ESP (Trujillo 2006).

- *Internet Key Exchange* (IKE)

### II.3.1.1 PROTOCOLO AH

Es el protocolo previsto que se encargará de la integridad y autenticación de los datagramas IP, al receptor de los paquetes IP se le proporciona un medio para la autenticación del origen de los datos, como también verificar que los datos no hayan sufrido una alteración en su tránsito. Este protocolo no proporciona garantías de confiabilidad, debido a que terceros pueden ver los datos transmitidos. Esta cabecera de autenticación es insertada en la cabecera IP estándar y los datos transportados, que pueden ser un mensaje TCP, UDP o ICMP, o incluso un datagrama IP completo (Trujillo 2006).

Su funcionamiento está basado en un código de autenticación de mensajes, conocido como HMA, el mismo consiste en aplicar una función HASH a la combinación de unos datos de entrada y una clave, la salida es una pequeña cadena de caracteres denominados “extractos”. La salida tendrá el papel de asociar los datos con los de la persona que los generó, el emisor copiará en uno de los campos de la cabecera AH un extracto del mensaje que él mismo calcula. El nuevo paquete es enviado a la red hasta llegar al receptor donde el proceso de cálculo se repite para la comparación del extracto (Trujillo 2006).

Se podrá confirmar si el paquete IP procede del origen esperado y no ha sido alterado o modificado en el tránsito si la comparación arroja los mismos resultados, la seguridad del protocolo consiste en que, sin el conocimiento de la clave, el cálculo del extracto no podrá lograrse, obteniendo resultados diferentes en la comparación, la clave solo la conocen el receptor y emisor (Trujillo 2006).

#### II.3.1.2 PROTOCOLO ESP

El objetivo principal del protocolo ESP se basa en proporcionar confidencialidad, para esto ESP específica el modo de cifrado de datos que se desea enviar, y cómo este contenido que se encuentra cifrado se incluye en un datagrama IP. Además de esto, puede ofrecer diversos servicios de integridad y autenticación del origen de los datos incorporando un mecanismo que es muy similar al de AH (Trujillo 2006).

Ya que ESP proporciona más funciones que el protocolo AH, el formato de la cabecera es mucho más complejo; este formato consta de la cabecera y una cola que rodean los datos transportados. Estos datos pueden ser cualquier protocolo IP (dando como ejemplo a TCP, UDP, ICMP, o incluso un paquete IP completo) (Trujillo 2006).

Dentro del mensaje ESP se indica la naturaleza de todos sus datos, ya que este campo (al igual que el *payload*) se encuentra cifrado, un supuesto infiltrado que intercepte el paquete no podrá saber si el contenido del mismo es TCP o UDP (Trujillo 2006).

La función de cifrado dentro del protocolo ESP se desempeña mediante un algoritmo de cifrado de clave/llave simétrica. Generalmente se utilizan algoritmos de cifrado de bloque, de modo que la longitud de los datos a cifrar debe ser un múltiplo del tamaño del bloque (es decir 8 o 16 *bytes*, en la mayoría de los casos). Debido a esto existe un campo de relleno el cual posee una función adicional, la misma se basa en la posibilidad de añadir caracteres de relleno al campo de datos para así poder ocultar su longitud real y, por lo tanto, las características del tráfico. Un atacante podría deducir fácilmente cierta información a partir del análisis de algunos parámetros de las comunicaciones (aunque se encuentren cifradas), tales como el retardo que existe entre los paquetes y su longitud. Esta función de relleno es analizada para poder dificultar estos posibles ataques. En el proceso de tránsito hasta su destino, si el paquete es interceptado por un agente externo sólo obtendrá ciertos bits que son ininteligibles; y en el destino, el receptor aplicará de nuevo el algoritmo de cifrado con la misma clave, recuperando así todos los datos originales (Trujillo, 2006).

La seguridad de este protocolo recae en la robustez del algoritmo de cifrado, es decir que, un atacante no puede descifrar los datos sin conocer la clave, así como en que la misma solamente es conocida por el emisor y el receptor (Trujillo 2006).

De la misma manera, es fundamental que el emisor y el receptor se encuentren de acuerdo tanto en el algoritmo de cifrado (o de HASH) como en el resto de los parámetros comunes. Esta labor que se encarga de realizar un contacto y una negociación es ejecutada por el protocolo IKE (Trujillo 2006).

### II.3.1.3 PROTOCOLO IKE

Uno de los conceptos más importantes, hablando de IPsec, es el de la Asociación de Seguridad (SA), debido a que este es un canal de comunicación en una sola dirección que conecta dos nodos, a través del cual fluyen los datagramas que son protegidos mediante distintos mecanismos criptográficos que fueron acordados previamente. Como únicamente se identifica un canal unidireccional, una conexión que utiliza IPsec se debe componer de dos SA, una para cada sentido de la comunicación (Trujillo, 2006).

Hasta el momento, se ha supuesto que los dos extremos de una SA deben tener conocimiento de las claves, así como también del resto de la información que necesitan para así poder enviar y recibir datagramas AH o ESP. Esta operación se puede realizar mediante configuraciones manuales o mediante algunos protocolos de control que se encargan de negociar de manera automática los parámetros necesarios; esta operación tiene el nombre de *negociación de SA* (Trujillo 2006).

El IETF (*Internet Engineering Task Force*) ha definido el protocolo IKE para que pueda realizar funciones tanto de gestión automática de claves como de establecimiento de SA correspondientes. Una característica importante de este protocolo es que su utilidad no se limita a IPsec, sino que es un protocolo estándar que gestiona claves que podría ser útil en otros protocolos como, por ejemplo, OSPF (Trujillo, 2006).

El principal objetivo que posee el protocolo IKE consiste en establecer una conexión cifrada y autenticada entre dos entidades/localidades, a través de la cual se

negocian diversos parámetros que son necesarios para poder establecer una SA IPsec. Esta negociación es llevada a cabo en dos fases:

#### II.3.1.3.1 PRIMERA FASE IKE

La fase común a cualquier aplicación, en la que los dos nodos establecen un canal que sea seguro y autenticado. Este canal se puede conseguir mediante el uso de un algoritmo de cifrado simétrico y un algoritmo HMAC. Las clases que sean necesarias se obtienen de una clave maestra que se obtiene mediante el algoritmo de intercambio de claves llamado *Diffie-Hellman*. Este procedimiento no va a garantizar la identidad de los nodos, para esto es necesario un paso adicional de autenticación (Trujillo 2006).

Existen distintos métodos para autenticar, entre los dos más comunes se tiene: El primer método se basa en el análisis de un secreto compartido que es una cadena de caracteres que solamente conocen ambos extremos que van a establecer una comunicación IPsec. Mediante la utilización de funciones de HASH, cada extremo le demuestra al otro que conoce el secreto sin revelar el valor del mismo y así los dos se autentican mutuamente. Para que no se debilite la seguridad de este mecanismo, se debe configurar un secreto distinto para cada par de nodos, por lo que el número de secretos crecen de manera muy rápida cuando aumenta el número de nodos. Es debido a esto que en entornos en los que se quiere interconectar muchos nodos IPsec, la gestión de las claves es muy complicada. Para este caso no se recomienda el uso de autenticación mediante secreto compartido, sino otro tipo de autenticación que se basa en certificados digitales (Trujillo 2006).

#### II. 3.1.3.2 SEGUNDA FASE IKE

Es en esta fase donde el canal seguro es usado para las negociaciones de los parámetros de seguridad como las características de la conexión ESP o AH y todos los parámetros necesarios que estén asociados a un protocolo determinado, siendo el caso a tratar IPsec (Trujillo 2006).

Las posibles opciones que tenga configuradas en su política de seguridad y con la prioridad que se hayan configurado serán proporcionadas por el equipo que ha iniciado la comunicación, a la vez que el sistema receptor admite las que coincida con los parámetros de seguridad establecidos en su configuración (Trujillo 2006).

## II.4 PROTOCOLO DE INTERCAMBIO DE LLAVES DIFFIE-HELLMAN

El protocolo criptográfico *Diffie-Hellman* (desarrollado en 1976) es empleado para intercambiar claves entre los diversos usuarios que intervienen en la comunicación de grupo, esto se realiza a través de un lugar inseguro. Comúnmente es utilizado con la finalidad para poder establecer una clave común, la cual será empleada para el cifrado durante un período de tiempo específico. El problema de este algoritmo es que no proporciona autenticación (Islas, 2013).

*Diffie-Hellman* utiliza la función de exponenciación modular a través de canales que son inseguros. En este protocolo se utilizan claves públicas, las cuales pueden llegar a ser conocidas por todos, y también utiliza claves privadas donde éstas solamente son conocidas por el propietario. Utilizando las claves públicas y privadas se generan claves secretas comunes para ser empleadas como claves privadas de criptosistemas simétricos (Islas, 2013).

## II.5 TUNNELING

El *tunneling* es el método que es utilizado en la encapsulación de los datos de los usuarios, datos conocidos como paquetes, dentro de otros que serán enviados mediante la tecnología de red por la que viaja. Las ventajas que esto ofrece son abundantes, debido a que permite el transporte de protocolos que posean diferentes esquemas de direccionamiento y debido a esto no sean compatibles con una red que utiliza otros protocolos de direccionamiento dentro de paquetes que sí reconoce la red (González, 2006).

### II.5.1 FUNCIONAMIENTO DEL TUNNELING

Para que un paquete incompatible con una red pueda ser transportado, el mismo es encapsulado dentro de un paquete que sí lo sea, el proceso como tal está basado en agregar un encabezado adicional al mismo (González, 2006).

Posteriormente el paquete encapsulado es enviado atravesando una ruta lógica ya establecida que es denominada “túnel”, la misma suele ser transparente, pero los elementos como *routers, switches,* servidores *proxy* u otras puertas de enlace de seguridad son desconocidos para los usuarios (González, 2006).

El uso de un túnel involucra todo lo relacionado al proceso de encapsulación, enrutamiento y desencapsulación. En la encapsulación el túnel es el encargado de envolver el paquete original dentro de uno nuevo, pudiendo contener la información del direccionamiento y enrutamiento, permitiendo su viaje a través de la red, en este punto es posible contar con la confidencialidad de datos si la misma es deseada, la información como el origen y destino están ocultas a quienes observen el tráfico de

red, al llegar al destino se desencapsula el paquete y el encabezado original del paquete es utilizado para enrutar el mismo a su destino final (Trujillo, 2006).

### II.5.2 TUNNELING Y VPN

El *tunneling* puede utilizarse para proporcionar servicios de VPN cuando el mismo es combinado con el cifrado de datos, ofreciendo el transporte de datos de forma segura mediante tres tareas principales siendo estas: la encapsulación, la protección de las direcciones privadas y por último la integridad y confidencialidad impuesta en los datos (González, 2006).

Para que el *tunneling* pueda ser llevado a cabo correctamente, existen algunos protocolos (Protocolos de Túnel) que se encargan de encapsular y desencapsular todos los datos que se encuentran viajando dentro de una VPN. Los protocolos de túnel que son comúnmente los más usados por las VPN como PPTP y L2TP son utilizados para encapsular las tramas de la capa de enlace de datos (PPP). Otros protocolos como IPsec en modo túnel son utilizados para poder encapsular los paquetes de la capa de red (González, 2006).

Es posible que se coloque un paquete que utiliza una dirección IP privada dentro de una paquete que usa una dirección IP global individual para que así se pueda ampliar una red privada sobre una red pública como lo es Internet, ya que los contenidos que se encuentran en el paquete que fue entunelado sólo se pueden interpretar por las interfaces de túnel, las direcciones IP privadas se pueden ocultar completamente dentro de las redes IP públicas (Trujillo, 2006).

Para el *tunneling*, existen mecanismos de integridad y confidencialidad que garantizan que ningún usuario que no esté autorizado pueda alterar de alguna forma los paquetes que se encuentran en el túnel durante una transmisión sin que el ataque pueda ser detectado. Agregando que, el *tunneling* de manera opcional puede asegurar la integridad de la cabecera de los paquetes IP externos, utilizando diversas técnicas de autenticación. Si se toma un ejemplo, si se utiliza IPsec, los protocolos AH y ESP pueden proporcionar autenticación de paquetes transmitidos (González, 2006).

Existen tres protocolos de *tunneling* que son los más utilizados para poder implementar una VPN, estos son:

- Protocolo de Túnel punto a punto (PPTP)
- Protocolo de Túnel de Capa 2 (L2TP)
- Protocolo de Seguridad IP (IPsec)

Los primeros dos mencionados se enfocan principalmente a las redes privadas de acceso remoto, mientras que el tercer protocolo es utilizado para redes privadas de sitio a sitio.

### II.5.3 TIPOS DE TÚNELES

Según (González, 2006), Los túneles que se implementan se pueden clasificar de acuerdo a cómo se establece la conexión entre dos usuarios. En base a esto, existen dos tipos de túneles:

- Túnel Voluntario
- Túnel Obligatorio

#### II.5.3.1 TUNEL VOLUNTARIO

Un túnel voluntario puede ser creado y configurado, mediante una petición VPN que emita un equipo usuario o cliente, sirviendo estos como un extremo del túnel, este túnel es producido en el momento en que un *router* o una estación de trabajo utilizan el software de cliente del túnel para la creación de una conexión VPN con el servidor de túnel de destino. Es necesaria la instalación del protocolo de túnel correspondiente en el equipo cliente, el túnel voluntario puede ser creado mediante una conexión *dial-up* tanto como con una LAN. (González, 2006).

Con el primer método el usuario deberá hacer una llamada a su proveedor de servicios de internet para lograr la conexión, posteriormente podrá ser creado el túnel, dejando en claro que la conexión a Internet es un paso preliminar para la creación, mas no forma parte de su proceso. En cambio, si la creación es realizada mediante la conexión LAN, el cliente ya tendrá en su disposición la conexión a la red, por lo tanto, cualquier servidor túnel deseado estará disponible para el proceso, siendo este el caso de un usuario de una LAN que crea un túnel para acceder a otra LAN (González, 2006).

#### II.5.3.2 TUNEL OBLIGATORIO

Un túnel obligatorio es la creación de un túnel seguro por parte de otro equipo u otro dispositivo de la red en nombre del equipo cliente. Estos son configurados y se crean de manera automática para los usuarios sin que éstos intervengan ni posean conocimiento de los mismos. Si se posee un túnel obligatorio, el equipo del usuario no es un extremo del túnel, sino que es otro dispositivo entre el equipo del usuario y el servidor de túnel que actuará como cliente (Trujillo, 2006).

Este tipo de configuración se llama túnel obligatorio ya que el cliente se encuentra obligado a utilizar el túnel que fue creado por el dispositivo que lo proporcionó. Una vez que se realiza la primera conexión, todo el tráfico que se realiza en la red y hacia el cliente, se envía de manera automática a través del túnel (González, 2006).

A diferencia de los túneles por separado, que son creados para cada cliente, un túnel entre el dispositivo que lo brinda y el servidor puede ser utilizado por varios clientes. Cuando un segundo cliente se encuentra conectado al dispositivo fuente para alcanzar un destino para el cual ya existe un túnel, no hay necesidad de crear uno nuevo entre el dispositivo que lo proporciona y el servidor. El tráfico de datos para este nuevo cliente se transporta sobre el mismo túnel, debido a que puede haber varios clientes en un túnel único, y el mismo no se termina hasta que el último usuario se desconecte (Trujillo, 2006).

Una compañía tiene la disponibilidad de contratar a un Proveedor de Servicios de Internet que se encargue de la implementación de un conjunto de dispositivos capaces de proporcionar túneles en los territorios donde existan LANs pertenecientes a la compañía. Dichos dispositivos establecen los túneles hasta un servidor VPN utilizando el internet como medio, el servidor VPN ha de estar conectado a la red privada de la organización, consiguiendo una integración de redes dispersas establecidas en zonas geográficas diferentes a una sola conexión a Internet en la red de la organización (González, 2006).

## II.6 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 (Orozco, 2014).

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 (Matías & Millán, 2009):

- 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 (Orozco, 2014).

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 (Matías & Millán, 2009).

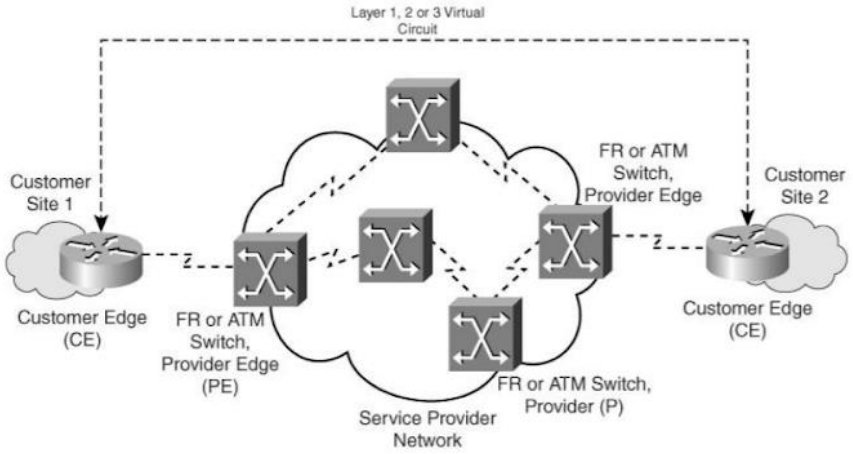


***Figura 2:*** *Ejemplo del modelo de Capa Superpuesta. Extraído de (Orozco, 2014).*

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 (Orozco, 2014).

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 o CPE (*Customer Premises Equipment*) o CE (*Customer Equipment*) ahora ha de conectarse con el *router* del proveedor de servicios, o PE (*Provider Equipment*) 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 (Matías & Millán, 2009).

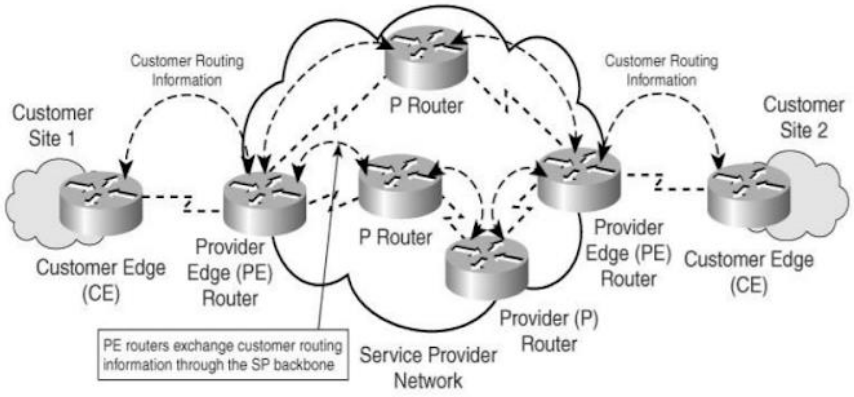


***Figura 3:*** *Ejemplo del modelo de Igual-Igual. Extraído de (Orozco, 2014).*

### II.6.1 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 (Matías & Millán, 2009).
- 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 (Matías & Millán, 2009).

### II.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 (Orozco, 2014).

Según (Orozco, 2014), 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.

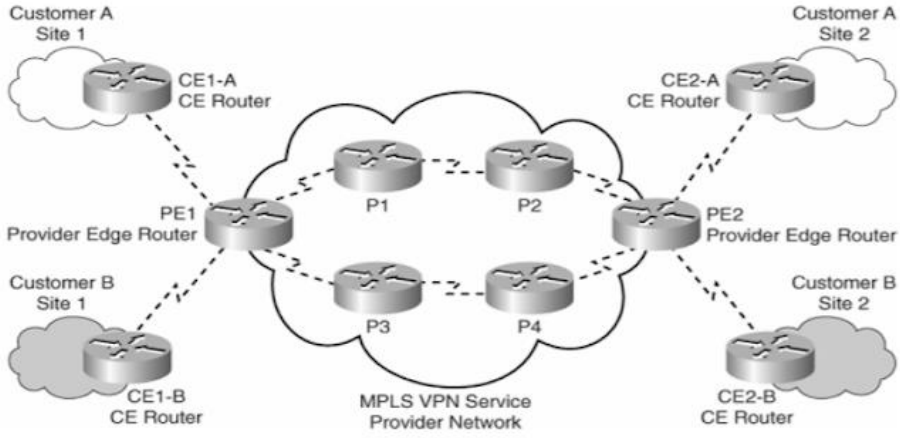


***Figura 4:*** *Ejemplo de una arquitectura VPN MPLS. Extraído de (Orozco, 2014).*

### II.6.3 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 (Orozco, 2014).

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 (Orozco, 2014).

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 (Orozco, 2014).

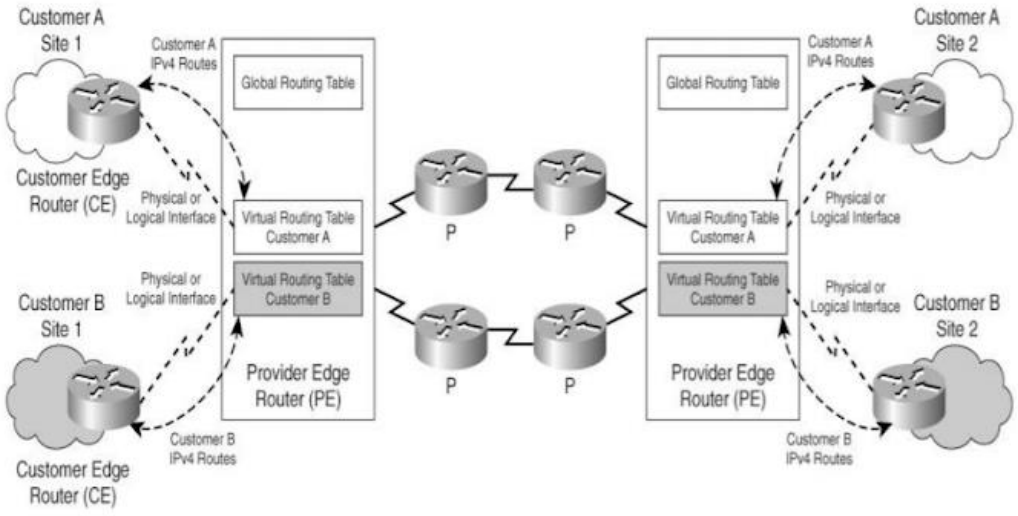


***Figura 5:*** *Explicativa de un enrutamiento VPN MPLS. Extraído de (Orozco, 2014).*

### II.6.4 PREPARACIÓN DEL ÚLTIMO PASO

Este tipo de acción ocurre en las redes MPLS donde el *router upstream* al E-LSR de la topología se encarga de remover la etiqueta tope de la pila de etiquetas y envía únicamente el paquete resultante para un FEC particular, este proceso es indicado por el *router* E-LSR *downstream* durante la distribución de etiquetas con LDP. El *router* E-LSR *downstream* se encarga de distribuir una *implicit-null* (POP) *label* hacia el *router upstream* indicando que se debe de remover la etiqueta tope y enviar el paquete resultante, por consiguiente, cuando el paquete se recibe en el *router* E-LSR no se realiza una consulta en LIB, si el paquete que llega es un paquete IP. Y es por eso que en el penúltimo salto se evita el proceso de consulta al E-LSR (Orozco, 2014).

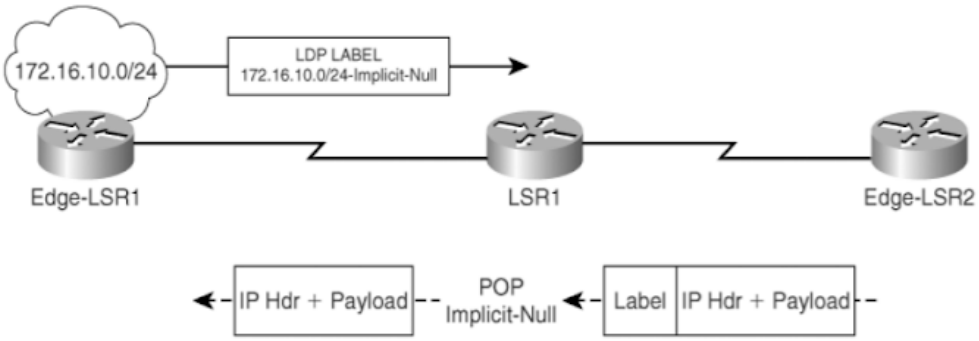


***Figura 6:*** *Penúltimo salto en redes MPLS. Extraído de (Orozco, 2014).*

# CAPÍTULO III

# 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.

## III.1 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 (Hurtado, 2012).

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 (Hurtado de Barrera, 2010).

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 (Hernández y Mendoza, 2018).

## III.2 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 cuáles sirvieron como base de estudio del proyecto.

## III.3 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:

### III.3.1 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.

### III.3.2 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.

### III.3.3 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 y servicios 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.

### III.3.4 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.

### III.3.5 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.

### III.3.6 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.

# CAPÍTULO IV

# 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:

## IV.1 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.

## IV.2 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. Los resultados arrojados por la encuesta en cada caso se muestran a continuación:

### IV.2.1 ENCUESTA: SAN MARTÍN

1. **Sede (Ubicación):** San Martín (Próxima sede principal).
2. **Encargado/Entrevistado:**
    a. Iván Martínez (Coordinador de sistemas).
    b. Jorge Baroudi (Encargado).
3. **Rubro/Dedicación de la Sede:** Distribución de materia prima a todas las tiendas (Próximamente se busca producción de productos).
4. **Tamaño de la sede ($m^2$):** 5000$m^2$ (aproximadamente).
5. **Tiempo de Operatividad:** 3 meses (Anteriormente a esto, la sede tenía un año y medio de planificación).
6. **Personal (estimado):** Actualmente se encuentran 60 trabajadores y se estima un total de 100-120 en un futuro cercano al ser próxima sede principal.
    a. **Departamentos de la sede (proyectado):**
        1. Administración (Requiere Conexión).
        2. Ventas (Requiere Conexión).
        3. Compras (Requiere Conexión).
        4. Tecnología (Requiere Conexión).

b. **¿Necesitan de teletrabajo?:** Sí, es necesario el teletrabajo.

1. **De necesitar teletrabajo, ¿Actualmente utilizan herramientas para el mismo? ¿Cuáles?:** Actualmente se encuentra en proceso de implementar una VPN.
2. **Si la respuesta es VPN, ¿Qué tipo de VPN se plantea?:** IPsec Site-to-Site.

7. **Red Actual:**
   a. **Equipos (marcas):** Únicamente Fortinet.
   b. **Seguridad:**
      1. **¿Posee información que necesite respaldo?:** Sí.
      2. **¿Posee una base de datos?:** Sí, actualmente se encuentra en la sede ubicada en Casanova.
      3. **¿Qué proveedor de servicios posee?:** Totalcom.
      4. **Estado de los servidores actuales:** Posee servidores operativos.
      5. **¿Posee servicio de Office 365 en esta sede?:** No.
      6. **¿Poseen conectividad con alguna otra sede?:** Actualmente no.
8. **SAP:** Se desea implementar (se estableció que únicamente en esta sede).

### IV.2.2 ENCUESTA: CASANOVA

1. **Sede:** Casanova (sede principal actual).

2. **Encargado/Entrevistado:**
    a. Iván Martínez (Coordinador de Sistemas).
    b. Jessica Jaime (Encargada de la Sede).
3. **Rubro/Dedicación de la sede:** Administración, Panificadora, Bodegón, Restaurante.
4. **Tamaño de la sede ($m^2$):** 520$m^2$ (aproximadamente).
5. **Tiempo de Operatividad:** 40 años aproximadamente.
6. **Personal:** 95 trabajadores.
    a. **Departamentos de la sede:**
        1. Local de ventas alimenticias.
        2. Cocina, Panificadora.
        3. Administración (Requiere Conexión).
        4. Ventas (Requiere Conexión).
        5. Base de Datos (Requiere Conexión).
        6. Bodegón (Requiere Conexión).
        7. Producción.
        8. Delivery.
        9. Mantenimiento.
    b. **¿Necesitan de teletrabajo?:** Sí, es necesario (debido a Inventarios, actualización de costos y otras actividades).
    c. **De necesitar teletrabajo, ¿Actualmente utilizan herramientas para el teletrabajo? ¿Cuáles?:** Actualmente se encuentra en proceso de implementar una VPN.

d. **Si la respuesta es VPN, ¿Qué tipo de VPN se plantea?:** IPsec Site-to-Site.

7. **Red Actual:**
    a. **Equipos (marcas):** Mikrotik, SuperStak
        1. Switch: 2 de 24 puertos, 1 de 28 puertos (SuperStak).
        2. 2 Routers (Mikrotik).
    b. **Seguridad:**
        1. **¿Posee información que necesite respaldo?:** Sí.
        2. **¿Posee una base de datos?:** Operativa (se encuentra en la sede), utiliza SQL como manejador.
        3. **¿Qué proveedor de servicios posee?:**

i. **Principal:** TotalCom.

ii. **BackUp:** Cantv.

4. **Estado de los servidores actuales:** Operativos, se encuentran en la sede.
5. **¿Posee servicio de Office 365 en esta sede?:** No, pero necesitan de este servicio.
6. **¿Poseen conectividad con alguna otra sede?:** actualmente no.

8. **SAP:** Ambiente en prueba (se utilizará en la próxima sede principal: San Martín).

### IV.2.3 ENCUESTA: CATIA

1. **Sede:** Catia.
2. **Encargado/Entrevistado:**
    a. Arturo Ramírez (Encargado de Redes).
    b. José Marcano (Encargado de la sede).
3. **Rubro/Dedicación de la sede:** Bodegón, Panificadora y Burgo (Producción) y Despacho.
4. **Tamaño de la sede ($m^2$):** 1000 $m^2$ (Aproximadamente).
5. **Tiempo de Operatividad:** 12 años (aproximadamente).
6. **Personal:** 62 trabajadores.
    a. **Departamentos de la sede:**
        1. Facturación (Requiere de conexión).
        2. Producción.
            i. Pan.
            ii. Trigo.
        3. Mantenimiento.
        4. Higiene y Desinfección.
        5. Ventas (Requiere de conexión).
        6. Bodegón (Requiere de conexión).
        7. Administración (Requiere de conexión).
    b. **¿Necesitan Teletrabajo?:** No necesariamente.
    c. **De necesitar teletrabajo, ¿Actualmente utilizan herramientas para el teletrabajo? ¿Cuáles?:** -.

d. **Si la respuesta es VPN, ¿Qué tipo de VPN se plantea?:** -.

7. **Red Actual:**

   a. **Equipos (marcas):** HP, TP Link y FortiNet.

      1. 2 Switch (HP y TP Link).
      2. 1 Router/Firewall FortiNet.
      3. Antenas.

   b. **Seguridad:**

      1. **¿Posee información que necesite respaldo?:** Sí.
      2. **¿Posee una base de datos?:** Casanova.
      3. **¿Qué proveedor de servicios posee?:**
         ii. **Principal:** Movistar.
         iii. **BackUp:** Cantv.
      4. **Estado de los servidores actuales:** Activos, en la sede.
      5. **¿Posee servicio de Office 365 en esta sede?:** No se maneja.
      6. **¿Poseen conectividad con alguna otra sede?:** Actualmente no.

8. **SAP:** no es necesario en la sede.

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.

## IV.3 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 (Vélez, 2018).

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

### IV.3.1 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 (Gallardo, 2019).

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 (Gallardo, 2019) los aspectos presentes en el Cuadrante de Gartner se definen de la siguiente manera:

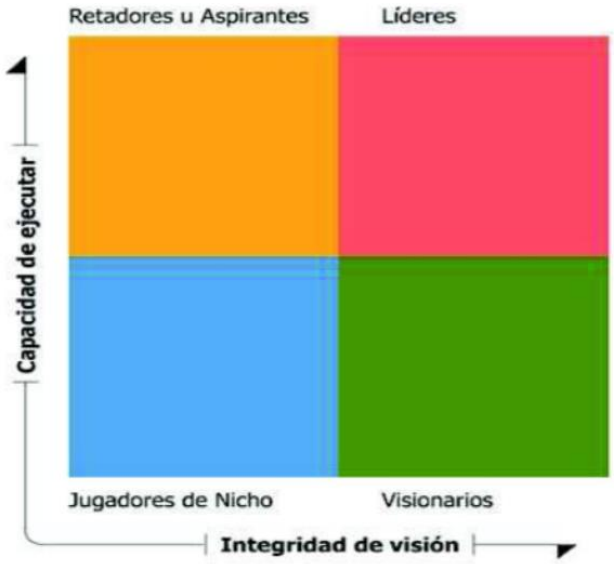


***Figura 7:*** *Representación del Cuadrante de Gartner. Extraído de: (Gallardo, 2019).*

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:


***Figura 8:*** *Cuadrante de Gartner, Wired and Wireless LAN (2020). Extraído desde: https://www.juniper.net/us/en/forms/juniper-a-leader-in-gartners-2020-magic-quadrant.html#:~:text=Gartner%20nombra%20a%20Juniper%20como,engendradas%20en%20la%20nube%20moderna.*

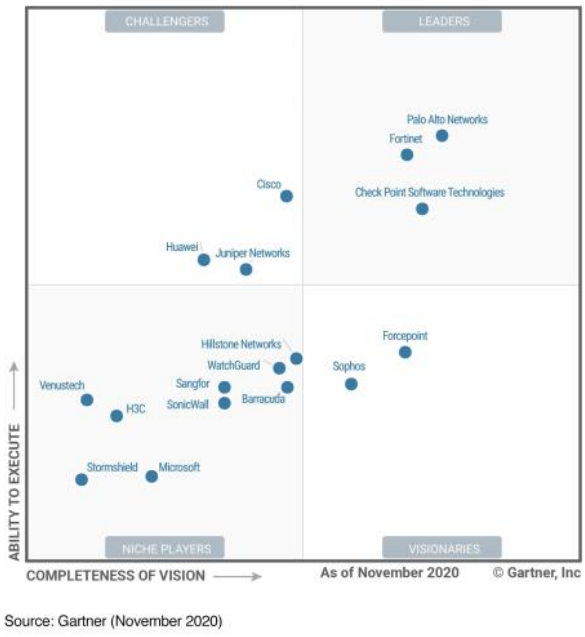


***Figura 9:*** *Cuadrante de Gartner, Firewalls 2020. Extraído de: www.google.com.*

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. **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 |

***Tabla 1:*** *Comparativa de Equipos Preseleccionados (Firewalls)*

**Especificaciones destacables según (JMTelcom, 2021):**

**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 | Interfaces |
|---|---|---|---|---|
| 10 Gbps | 1.4 Gbps | 1 Gbps | 900 Mbps | Multiple GE RJ45 \| Variants with internal storage and LAN Bypass |

***Figura 10:*** *Especificaciones Firewall FortiGate-80F. Extraído de: (Fortinet, 2021).*

### FortiGate-60F / 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

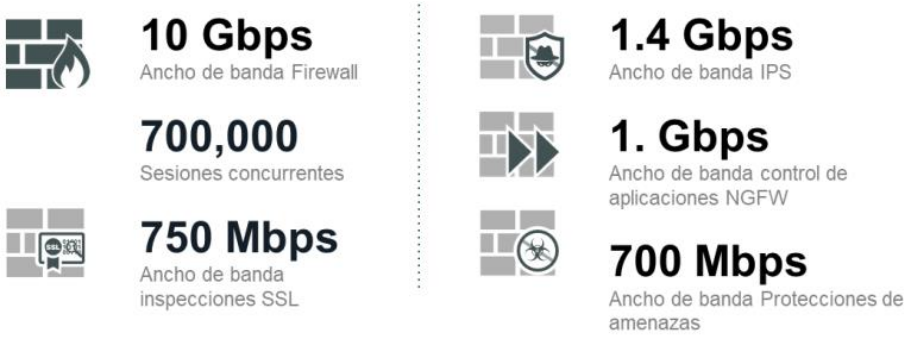


***Figura 11:*** *Especificaciones Firewall FortiGate-60F. Extraído de: (JMTelecom, 2021).*

### 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


***Figura 12:*** *Especificaciones Firewall FortiGate 50E. Extraído de: (JMTelcom, 2021)*

**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

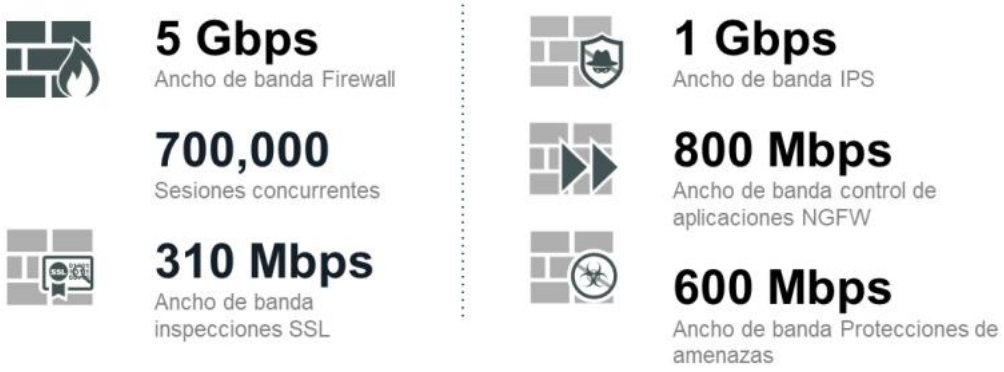

***Figura 13:*** *Especificaciones Firewall FortiGate 40F. Extraído de: (JMTelcom, 2021)*

2. **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 |

***Tabla 2:*** *Comparativa de Equipos Preseleccionados (Switches)*

**Especificaciones destacables según (Intercompras, 2021):**

**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

**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

3. **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 |

***Tabla 3:*** *Comparativa de Equipos Preseleccionados (Red Inalámbrica)*

**Especificaciones destacables:**

**Según (WNI, 2021), Ubiquiti Unifi AP-AC:**

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

**Según (TP-Link Colombia, 2021), 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:

**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:

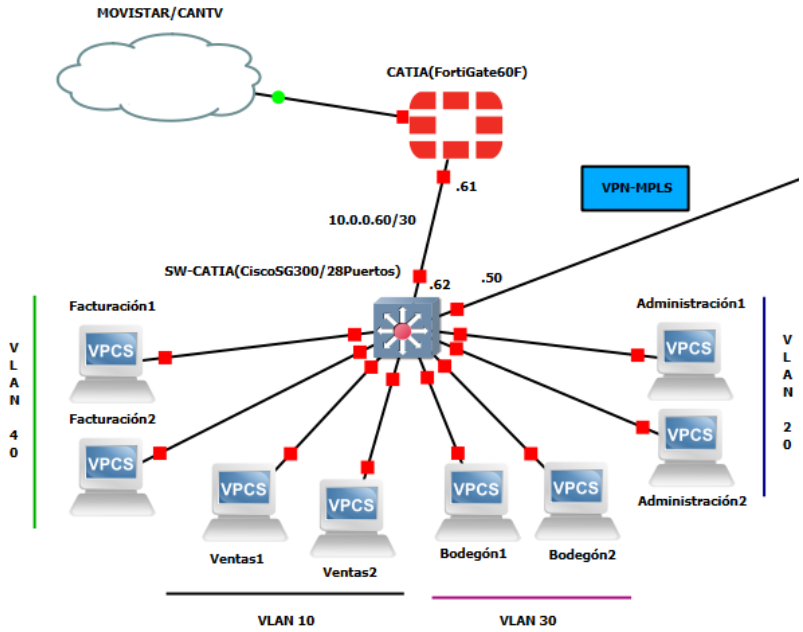


***Figura 14:*** *Diseño de la topología de red física: Sede Catia (Realizado en GNS3)*

**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:

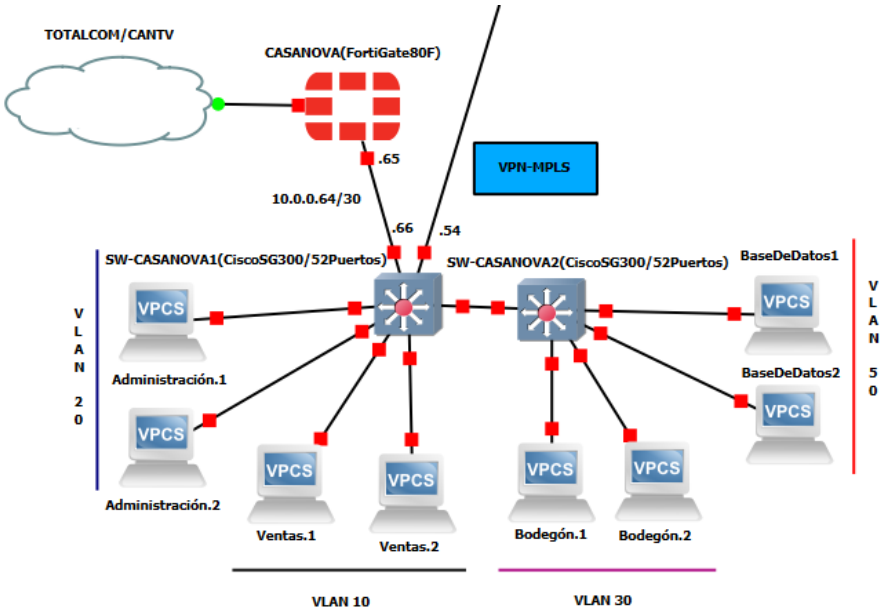


***Figura 15:*** *Diseño de la topología de red física: Sede Casanova (Realizado en GNS3)*

**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 Catia se muestra a continuación:

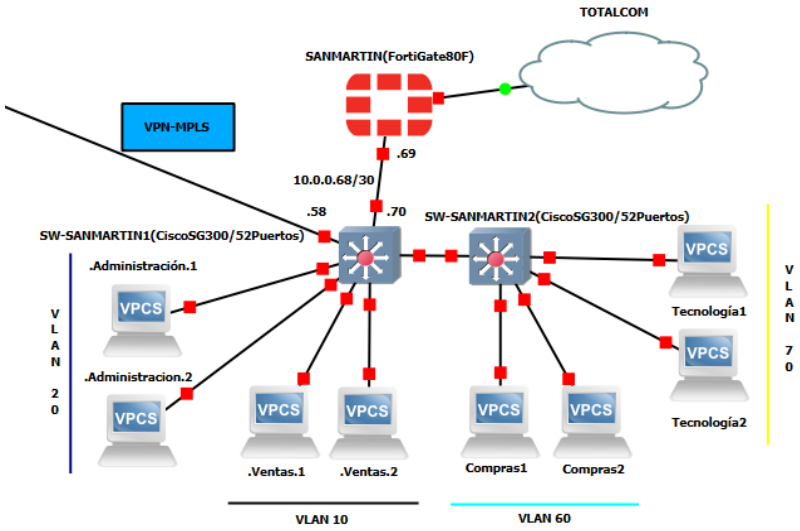


***Figura 16:*** *Diseño de la topología de red física: Sede San Martín (Realizado en GNS3)*

## 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 planteó un diagrama que permita representar la arquitectura de la red propuesta, el mismo se muestra a continuación.

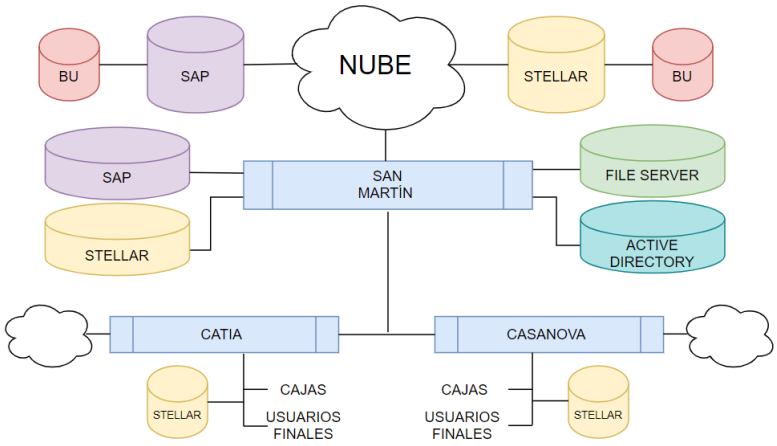


***Figura 17:*** *Diagrama de Red incluyendo servicios en la nube.*

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.

## IV.3.2 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**

| 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 |

***Tabla 4:*** *Direcciones de Red Privadas*

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

| 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 |

***Tabla 5:*** *Direccionamiento Sede Catia*

**Sede Casanova:** Dirección de Red – 172.16.2.0/24

| 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 |

***Tabla 6:*** *Direccionamiento Sede Casanova*

**Sede San Martín:** Dirección de Red – 172.16.1.0/24

| 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 |

***Tabla 7:*** *Direccionamiento Sede San Martín*

- **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

## IV.4 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:

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

***Tabla 8:*** *Precios Servicio VPN-MPLS por proveedor*

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 Mbits** de datos, entonces:

- 50$ x 6 MB = **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.

## IV.5 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:

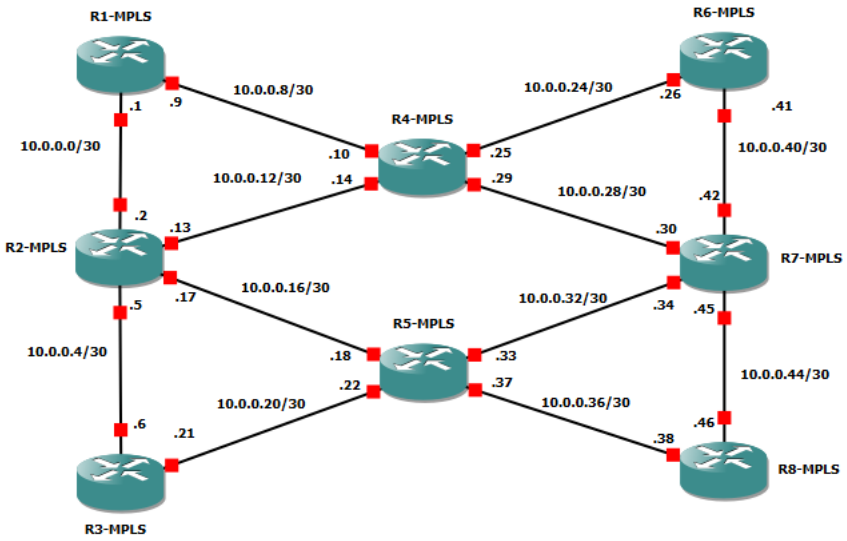


***Figura 18:*** *Core MPLS (Realizado en GNS3)*

| 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 |

***Tabla 9:*** *Esquema Lógico Core MPLS*

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.

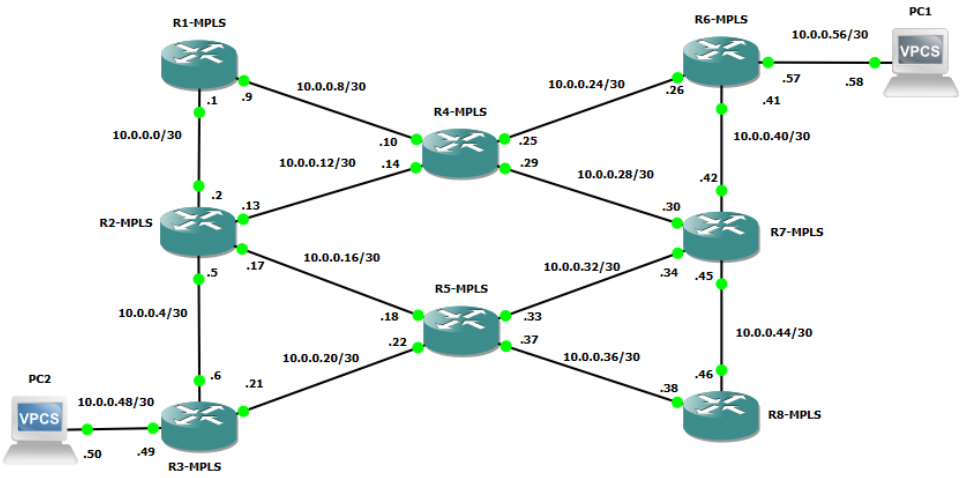


***Figura 19:*** *Verificación del funcionamiento del Core MPLS*

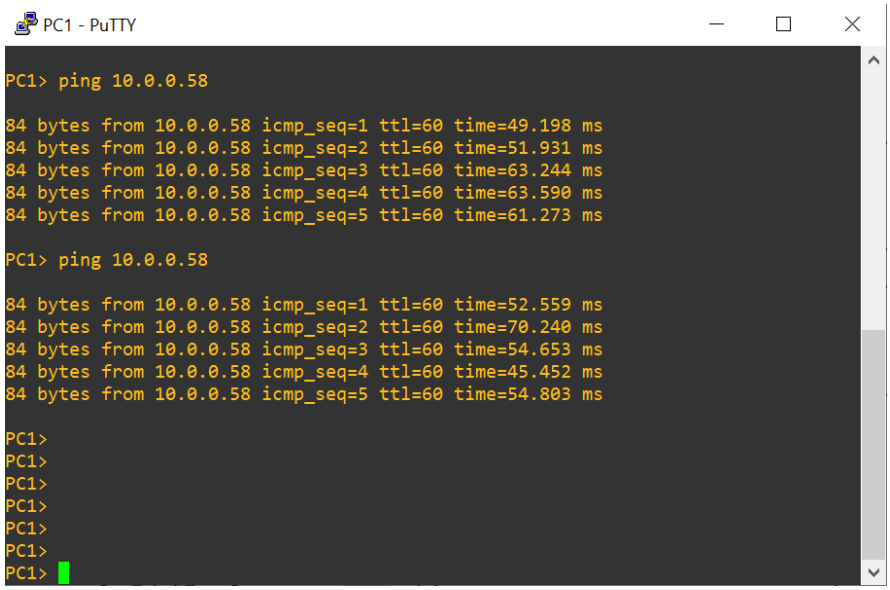


***Figura 20:*** *Comunicación de la PC1 con PC2 utilizando el comando "ping"*

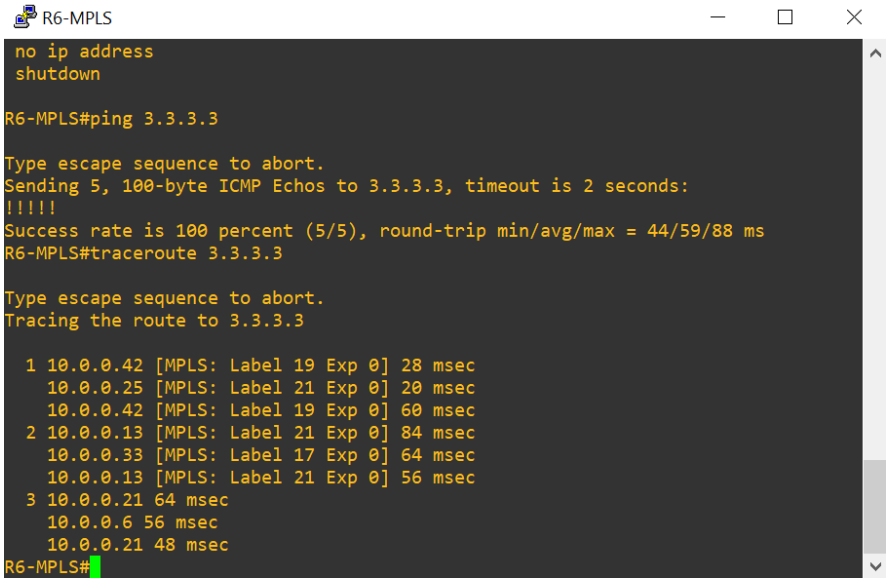


***Figura 21:*** *Proceso MPLS desde R6-MPLS a R3-MPLS*

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, 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.

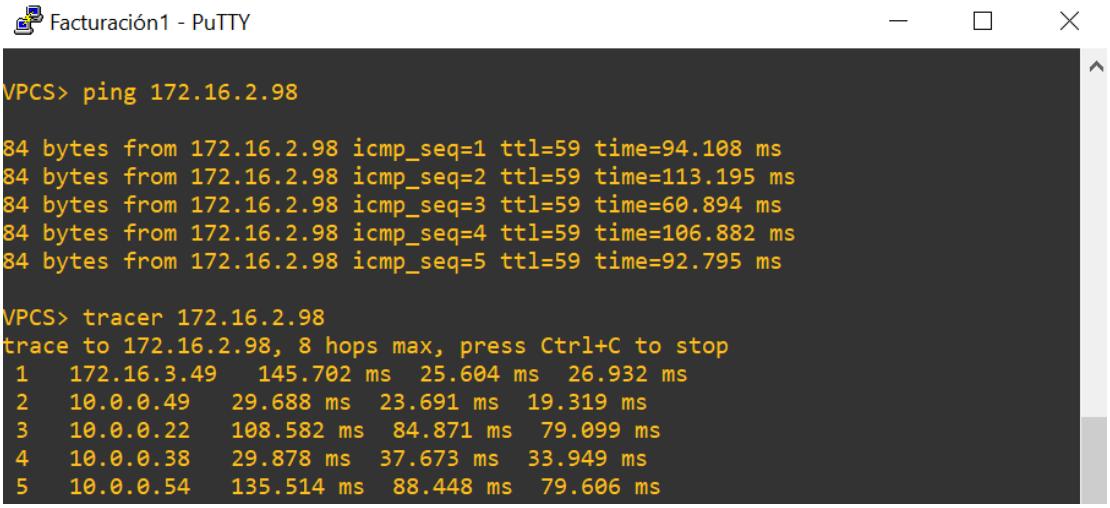


***Figura 22:*** *Conectividad de Facturación1 (CATIA) a BaseDeDatos1 (CASANOVA) - Caso MPLS.*

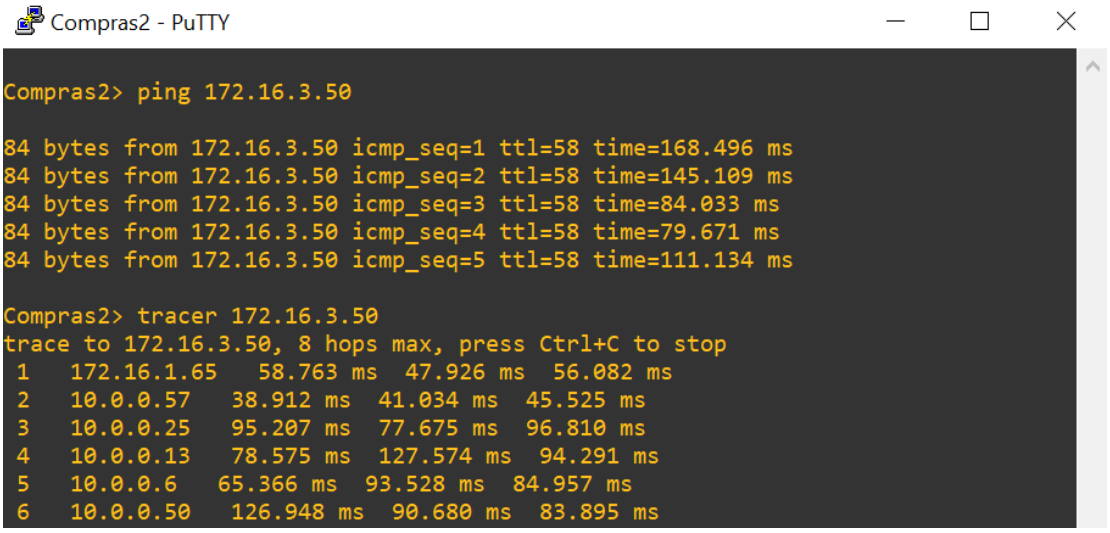


***Figura 23:*** *Conectividad de Compras2 (SAN MARTIN) a Facturación1 (CATIA) - Caso MPLS.*

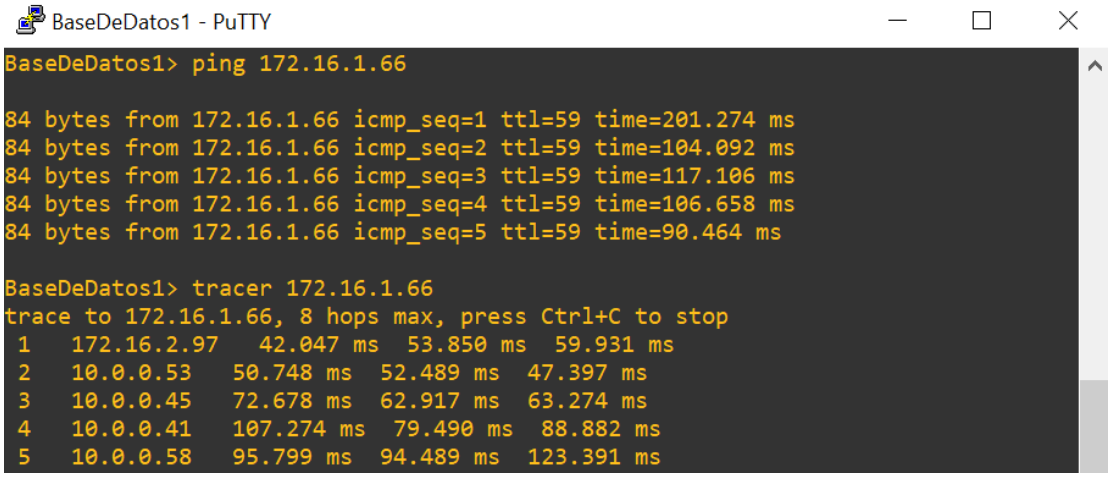


***Figura 24:*** *Conectividad de BaseDeDatos1 (CASANOVA) a Compras2 (SAN MARTIN) - Caso MPLS.*

Cuando la arquitectura de red simulada se encuentra en total convergencia, el transporte de los paquetes ocurre mediante el core MPLS diseñado, cada sede se encuentra interconectada entre si y utiliza dicho modelo de transmisión para el transporte de datos y su enlace interno con el ISP para su conexión a internet. En las figuras previamente mostradas se evidencia la conectividad que existe entre distintos hosts de cada una de las sedes con respecto a similares en una sede distinta.

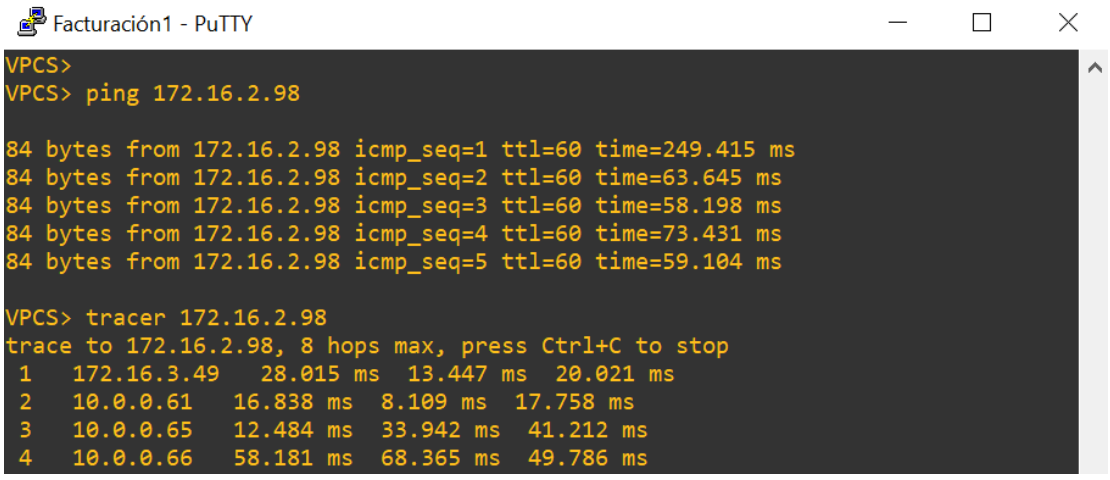


***Figura 25:*** *Conectividad de Facturación1 (CATIA) a BaseDeDatos1 (CASANOVA) - Caso IPsec.*

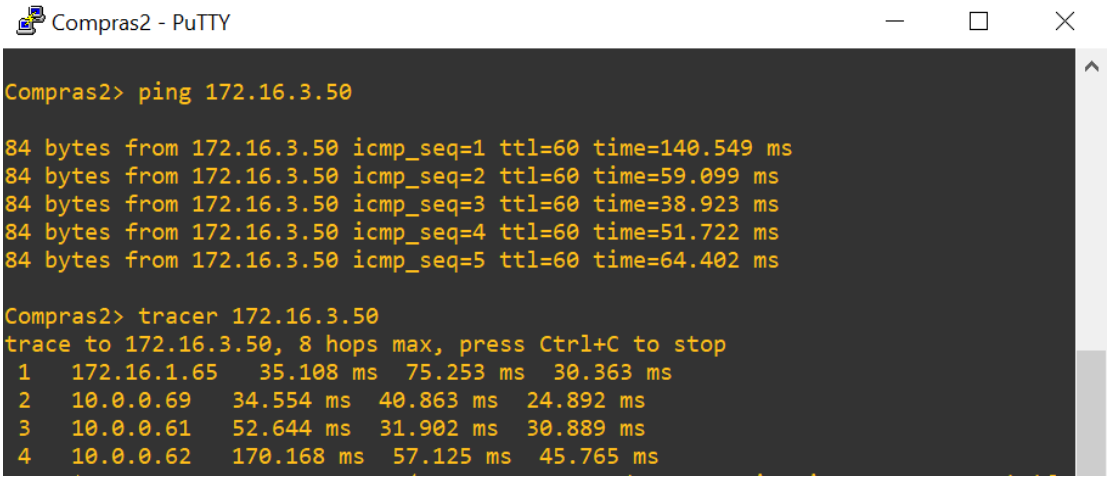


***Figura 26:*** *Conectividad de Compras2 (SAN MARTIN) a Facturación1 (CATIA) - Caso IPsec.*

En el momento que ocurre una falla en el enlace entre el Switch de capa 3 de cada sede y el servicio VPN-MPLS, el transporte de datos cambia de ruta, utilizando específicamente el túnel VPN de tipo IPSec creado por los dispositivos Fortigate de cada sede, de esta manera se garantiza una alta operatividad y disponibilidad de la red. De igual forma en las figuras previamente mostradas se evidencia la conectividad que existe entre distintos hosts de cada una de las sedes con respecto a similares en una sede distinta.

Facturación1 - PuTTY

```
VPCS> ping 172.16.2.98 -t

84 bytes from 172.16.2.98 icmp_seq=1 ttl=59 time=88.633 ms
84 bytes from 172.16.2.98 icmp_seq=2 ttl=59 time=102.621 ms
84 bytes from 172.16.2.98 icmp_seq=3 ttl=59 time=106.814 ms
84 bytes from 172.16.2.98 icmp_seq=4 ttl=59 time=127.812 ms
84 bytes from 172.16.2.98 icmp_seq=5 ttl=59 time=76.240 ms
84 bytes from 172.16.2.98 icmp_seq=6 ttl=59 time=119.422 ms
84 bytes from 172.16.2.98 icmp_seq=7 ttl=59 time=89.558 ms
84 bytes from 172.16.2.98 icmp_seq=8 ttl=59 time=66.382 ms
84 bytes from 172.16.2.98 icmp_seq=9 ttl=59 time=116.226 ms
172.16.2.98 icmp_seq=10 timeout
172.16.2.98 icmp_seq=11 timeout
172.16.2.98 icmp_seq=12 timeout
172.16.2.98 icmp_seq=13 timeout
172.16.2.98 icmp_seq=14 timeout
172.16.2.98 icmp_seq=15 timeout
172.16.2.98 icmp_seq=16 timeout
172.16.2.98 icmp_seq=17 timeout
172.16.2.98 icmp_seq=18 timeout
172.16.2.98 icmp_seq=19 timeout
172.16.2.98 icmp_seq=20 timeout
172.16.2.98 icmp_seq=21 timeout
172.16.2.98 icmp_seq=22 timeout
172.16.2.98 icmp_seq=23 timeout
172.16.2.98 icmp_seq=24 timeout
172.16.2.98 icmp_seq=25 timeout
172.16.2.98 icmp_seq=26 timeout
172.16.2.98 icmp_seq=27 timeout
172.16.2.98 icmp_seq=28 timeout
172.16.2.98 icmp_seq=29 timeout
172.16.2.98 icmp_seq=30 timeout
84 bytes from 172.16.2.98 icmp_seq=31 ttl=60 time=108.664 ms
84 bytes from 172.16.2.98 icmp_seq=32 ttl=60 time=79.849 ms
84 bytes from 172.16.2.98 icmp_seq=33 ttl=60 time=97.174 ms
84 bytes from 172.16.2.98 icmp_seq=34 ttl=60 time=62.484 ms
84 bytes from 172.16.2.98 icmp_seq=35 ttl=60 time=43.325 ms
84 bytes from 172.16.2.98 icmp_seq=36 ttl=60 time=59.242 ms
^C
```

***Figura 27:*** *Conectividad de Facturación1 (CATIA) a BaseDeDatos1 (CASANOVA) - Switch over.*

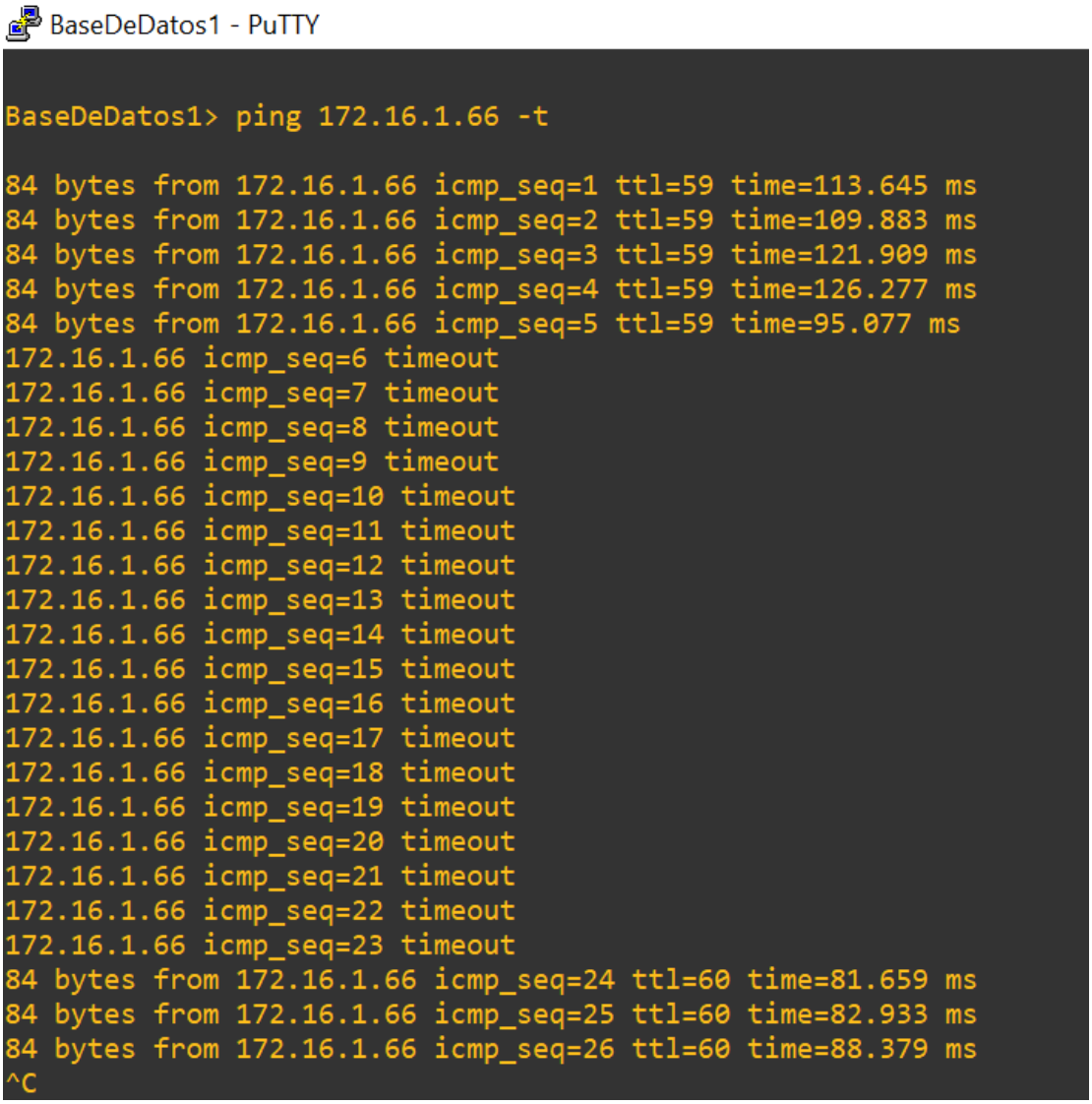


***Figura 28:*** *Conectividad de BaseDeDatos1 (CASANOVA) a Compras2 (SAN MARTIN) - Switch over.*

De ocurrir una caída del servicio VPN-MPLS, el Switch de capa 3 realiza un *switch over* de la ruta de transporte de datos desde el core MPLS hacia la VPN IPSec sin necesidad de hacer configuraciones en el sistema o restablecer el mismo, el *switch over* se ve evidenciado en las figuras presentadas anteriormente, hay un período de transición relativamente corto manteniendo alta disponibilidad de la red. En el

momento que el servicio VPN-MPLS vuelve a sus condiciones normales, ocurre de nuevo un *switch over* hacia el mismo siendo este la ruta principal.

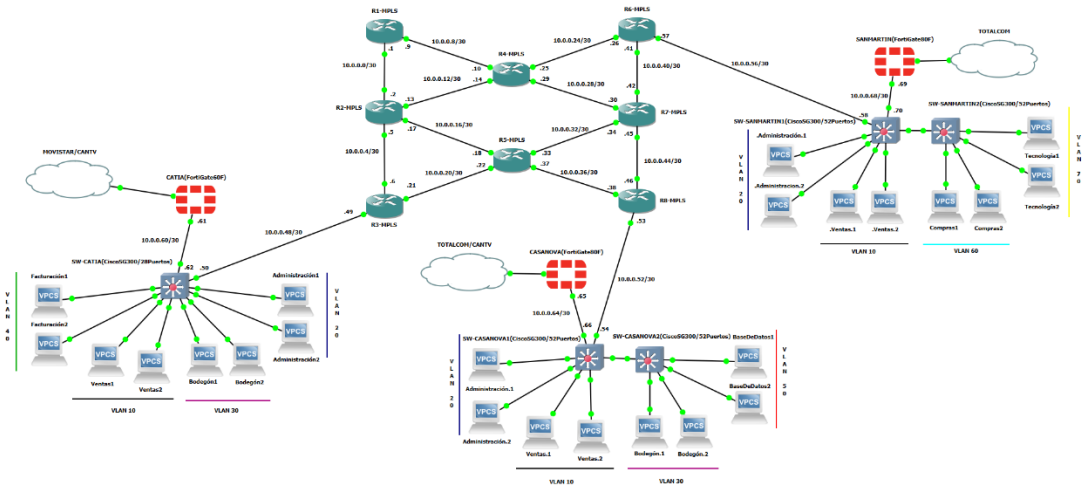


***Figura 29:*** *Red Telemática de Arabito en total convergencia.*

## IV.6 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 encentran 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. Dicho documento se encuentra reflejada como Anexo C del presente trabajo.

# CAPÍTULO V

# CONCLUSIONES Y RECOMENDACIONES

## V.1 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.

## V.2 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.

a) 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.

b) 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.

c) 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.

d) 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.

e) 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.

f) 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.

g) 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.

## REFERENCIAS BIBLIOGRÁFICAS CONSULTADAS

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

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.

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.

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

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.

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

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.

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

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

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

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

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

Ionos Digital Guide. (2019). *File Server: definición y aspectos básicos*. Recuperado el 14 de julio del 2021. Extraído desde: https://www.ionos.es/digitalguide/servidores/know-how/file-server/

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.

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

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

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

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

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.

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

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

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.

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*

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.

Quest. (s.f). *¿Qué es Active Directory? ¿Cómo funciona?*. Recuperado el 14 de julio del 2021. Extraído desde: https://www.quest.com/mx-es/solutions/active-directory/what-is-active-directory.aspx

SAP. (s.f). *¿Qué es SAP?*. Recuperado el 14 de julio del 2021. Extraído desde: https://www.sap.com/latinamerica/about/company/what-is-sap.html

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/

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

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.

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

# ANEXO A: ENCUESTA REALIZADA A LOS ENCARGADOS DE CADA SUCURSAL.

Universidad Católica Andrés Bello

Facultad de Ingeniería

Escuela de Telecomunicaciones

## ENCUESTA A SEDES: ARABITO

Datos de Relleno:

1. **Sede (Ubicación):**
2. **Encargado/Entrevistado:**
3. **Rubro/Dedicación de la Sede:**
4. **Tamaño de la sede ($m^2$):**
5. **Tiempo de Operatividad:**
6. **Personal (estimado):**
    a. **Departamentos de la sede que requieren de conexión (proyectado):**
    b. **¿Necesitan de teletrabajo?:**
    c. **De necesitar teletrabajo, ¿Actualmente utilizan herramientas para el mismo? ¿Cuáles?:**
    d. **Si la respuesta es VPN, ¿Qué tipo de VPN posee?:**
7. **Red Actual:**
    a. **Equipos (marcas):**
    b. **Seguridad:**
        i. **¿Posee información que necesite respaldo?:**

ii. **¿Posee una base de datos?:**

c. **¿Qué proveedor de servicios posee?:**

d. **Estado de los servidores actuales:**

e. **¿Posee servicio de Office 365 en esta sede?:**

f. **¿Poseen conectividad con alguna otra sede?:**

g. **SAP:**

# ANEXO B: CONFIGURACIONES DE LOS EQUIPOS

Universidad Católica Andrés Bello.

Facultad de Ingeniería

Escuela de Telecomunicaciones

## PLANTILLA DE CONFIGURACIÓN INICIAL: EQUIPOS ARABITO

**Switches Capa 3:**

```
enable
configure terminal
hostname (Nombre)
enable secret arabito
ip domain name arabito.com
crypto key generate rsa
ip ssh version 2
line console 0
        login local
        exit
line vty 0 15
        login local
        transport input ssh
        exit
username Arabito privilege 15 secret arabito
service password-encryption
no ip domain-lookup
```

banner motd " This is a secure system. Authorized Access Only. Este es un sistema de seguridad. Unicamente Acceso Autorizado "

interface (ID de la interfaz)

spanning-tree portfast

spanning-tree bpduguard enable

exit

exit

wr

**FortiGate (60F y 80F):** se realizó mediante la interfaz gráfica de los mismos dispositivos.

## PLANTILLA DE CONFIGURACIÓN: EQUIPOS CORE MPLS

**PASO 1: OSPF**

- R-MPLS(X)

router ID: X.X.X.X (loopback-mpls)

hostname R-MPLSX

interface (ID de la Interfaz)

ip address (dirección IP) (máscara)

no shutdown

ex

router ospf 1

router-id X.X.X.X

network (dirección IP) (*wildcard*) area 0

ex

**PASO 2: HABILITAR IP CEF (*CISCO EXPRESS FORWARDING*)**

mpls ip

ip cef (Habilitar tecnología de conmutación de capa 3, mejora el rendimiento)

**PASO 3: HABILITAR LDP PARA EL INTERCARMBIO DE ETIQUETAS**

mpls label protocol ldp

**PASO 4: UTILIZAR UNA INTERFACE LOOPBACK COMO ROUTER-ID PARA LDP Y ANUNCIARLA**

- R-MPLS(X)

interface loopback 0

ip address X.X.X.X 255.255.255.255

ex

mpls ldp router-id loopback 0

router ospf 1

network X.X.X.X 0.0.0.0 area 0

ex

**PASO 5: HABILITAR MPLS PARA CADA INTERFAZ**

router ospf 1

mpls ldp autoconfig area 0

ex

---

**COMANDOS DE VERIFICACIÓN**

do show mpls interface (verificar si los puertos poseen MPLS).

do show mpls ldp neighbor (verificar los vecinos MPLS).

do show mpls ldp bindings (muestra la tabla LIB, donde se guardan todas las etiquetas que se pasan los vecinos).

do show mpls forwarding-table (tabla que asocia las etiquetas con los destinos o rutas de capa 3 y la interaz de salida del *router*).

# ANEXO C: FASES DE MIGRACIÓN

Universidad Católica Andrés Bello

Facultad de Ingeniería

Escuela de Telecomunicaciones

## DOCUMENTO DE MIGRACIÓN DE DATOS

Actualmente existen diversas razones por las que un proyecto de migración de datos se puede llevar a cabo. En esta ocasión, la empresa *Arabito* deberá ejecutar el proyecto de migración debido a la actualización del diseño de su red telemática y de los equipos que se utilizarán en el mismo, este documento se basa en la recomendación por parte de los realizadores del proyecto para poder lograr una transferencia de datos óptima de la red actual a la diseñada en el trabajo, ya que pensar en la posibilidad de perder la base de datos de los clientes, el historial de las ventas o el inventario de los productos causaría terribles consecuencias para la empresa en cuestión.

Es importante recalcar que el proceso de migrar datos de una red a otra puede ser un proceso engorroso ya que no se trata de un simple proceso de copia o sincronización de datos, se trata de un proyecto que requiere de planificación y tiempo, es decir que, es un trabajo crítico que consta de ciertas fases, además de tener que hacer pruebas de validación de los datos antes y después de la transferencia de los mismos para verificar que puedan migrar correctamente. Claro está que, dependiendo del tipo de iniciativa es necesario un planteamiento específico y para realizar una buena toma de decisiones hay que tomar en consideración ciertos factores como, por ejemplo:

- Tiempo que tardará el proceso de migración (tiempo del proyecto).

- Cantidad de tiempo de inactividad de la empresa durante la transferencia de datos.
- Analizar todos aquellos posibles riesgos para la empresa que vengan desglosados por algunos problemas técnicos, extracción o pérdida indeseada de datos, bajo rendimiento de los dispositivos/softwares, entre otros.

Ahora, luego de haber considerado los factores mencionados y los posibles riesgos que se pueden generar en el proceso, es de suma importancia entender qué tipo de datos se están transfiriendo y qué función realizan dentro de la red empresarial ya que esto determinarán las políticas de migración a implementar para poder garantizar el orden necesario a lo largo de todo el proyecto. Además, es recomendable que antes de comenzar la migración se utilicen procesos ETL (*Extract, Transform and Load*) para poder conocer y concentrar los datos en un único repositorio y así se realicen de manera más sencilla las pruebas y validaciones de los datos a migrar, es decir que se asegure que los datos reúnen todos los parámetros de calidad.

Resumiendo lo mencionado anteriormente, se puede establecer que las ***FASES DE MIGRACIÓN DE DATOS*** que se deben llevar a cabo en el proceso son las siguientes:

1. *Planificación*. Aquel momento en el que se establece la estrategia y se definen los alcances del proyecto.
2. *Análisis*. Tener en cuenta las características y la calidad de los datos (como por ejemplo la integridad, la exactitud, entre otros) y de las bases de datos de origen y de destino.

3. *Proceso de Pruebas*. Llevar a cabo un ciclo de pruebas a los dispositivos o softwares que se utilizarán en el proceso.
4. *Migración*. Luego de haber asegurado el proceso, realizar la transferencia de información.
5. *Evaluación*. Medir, analizar e implementar los ajustes finales del proceso.

## ALGUNOS DESAFÍOS DE LA MIGRACIÓN DE DATOS

Ahora, tocando el tema de una manera más específica, el éxito de este proceso va a depender del nivel de comprensión y de planificación que se le dé al mismo. Tomando en cuenta los dispositivos telemáticos que posee la empresa *Arabito*, el proceso de transferencia de datos se realizará haciendo uso de sus *bases de datos*, y conocer los retos que implica esta iniciativa es de suma importancia.

La migración utilizando *bases de datos* es uno de los procesos menos complicados al momento de realizar un movimiento de datos, de igual forma, a pesar de la simplicidad del proceso, se pueden conseguir ciertos contratiempos como en cualquier proyecto, como por ejemplo que existan datos no coincidentes en ciertos parámetros como la fecha, el número, entre otros, o que también se encuentren diferentes conjuntos de caracteres en una misma tabla. En cualquiera de las dos situaciones habría que revisar a fondo y con total calma los softwares y las características de las bases de datos.

Como se mencionó anteriormente, las herramientas ETL son muy recomendadas para poder ejecutar un proyecto con estos requerimientos, además que

su uso es muy utilizado en migraciones donde existan pocas conexiones entre el origen (red actual) y el destino (nueva red).

Si la base de datos de la empresa *Arabito*, además de almacenar datos, contiene la lógica empresarial en forma de procedimientos almacenados, se debe realizar un estudio mucho más profundo de la viabilidad de la migración hacia una nueva red, esta podría ser la acción más indicada si la nueva red contiene mejoras en sus equipos y en su seguridad cibernética.

## MEJORES PRÁCTICAS EN LA MIGRACIÓN DE DATOS

Las implicaciones del proceso de migración llevan a la necesidad de conocer mejores prácticas aplicables, como las recomendadas:

- **Análisis situacional actualizado:** antes de emplear un proceso de migración de datos, establecer un mapeo de la relación de cada uno de los servidores con el almacenamiento, haciendo énfasis en su funcionalidad y asignaciones, de esta manera poder replicar las mismas en el nuevo entorno y prevenir problemas relacionados con el reinicio tras la migración.
- **Recopilar métricas:** se deben tener claras las necesidades de ancho de banda de la red, programando esta tarea de forma previa a la migración, tomando en cuenta cuánto debe ser asignado y cuánto estará disponible.
- **Reducir presión sobre el proyecto:** en búsqueda de una mayor consistencia en los datos, es recomendado planificar y establecer la iniciativa de migración fuera de las horas de producción habituales, dentro de un periodo de inactividad, es posible llevarla a cabo sin causar interrupciones en horario laboral pero no suele ser lo habitual.

- **Monitoreo de seguridad de la información:** los diferentes permisos, aplicaciones, sistemas, proveedores y configuraciones, incrementan las probabilidades de que una brecha de seguridad esté presente en el momento de la migración haciéndola vulnerable, es debido a esto que se recomienda establecer una hoja de ruta de las actividades a realizar con su respectivo monitoreo y prevención, garantizando la protección de los datos.
- **Revisión del software:** los detalles en el software son importantes, conocer e informarse de las versiones y parches de los mismos es de suma relevancia, pasar por alto esta información podría ocasionar incompatibilidad o fallos en la red.
- **Minimizar la incertidumbre:** La preparación forma parte crucial del proceso, es debido a esto que se recomienda al equipo, tomarse el tiempo necesario y requerido para informarse sobre lo que implica la migración de datos y de qué forma se abordará el proceso en pro de la reducción de riesgos para una alta fiabilidad y seguridad.

**RECOMENDACIONES**

La aplicación de las mejoras prácticas descritas anteriormente, unificadas a la conciencia de los desafíos que se presentarán, influyen en las expectativas planteadas inicialmente, por esto se debe tener presente que los ***procesos automatizados son tomados como prioridad***, es de suma importancia contar con herramientas de migración que permitan minimizar la intervención humana a la par de aumentar la capacidad de traslado, tanto en rapidez como en calidad de los datos.

A la vez, existen varios requisitos de almacenamiento con respecto al entorno en una migración de datos que deben tomarse en cuenta:

- **Cambio de proveedor.** Puede estar presente un cambio de proveedor en la migración, siendo necesario disponer de herramientas heterogéneas como por ejemplo la variación de las marcas/modelos de los dispositivos telemáticos.
- **Optimización.** Al momento de un traslado hacia un entorno mayor y mejorado, se requerirá de una planificación más cuidada, de más tiempo y un uso de herramientas más complejas.

Ha habido muchos avances en el campo, en especial en lo que concierne a la automatización del descubrimiento. Para aprovechar las ventajas que brindan al proyecto hay que orientar su elección hacia:

- La búsqueda de herramientas que ayuden a aumentar la flexibilidad, desde un nivel de servidor hasta el almacenamiento.
- La herramienta competente para la iniciativa, que no tiene porqué ser ni la más novedosa, ni la más cara.

# ANEXO D: PRESUPUESTO ESTIMADO

**Servicios Mensuales:**

| Descripción del servicio | Cantidad | Ancho de Banda | Tarifa Unitaria ($/mes) | Total |
|---|---|---|---|---|
| Servicio MPLS | - | 6 Mb | 300 | 300 |
| Servicio de Internet Dedicado | - | 12 MB | 299 | 299 |
| Servicio Microsoft Office 365 | 180 usuarios (Aproximadamente) | - | 5 | 900 |
| Servicio SAP (San Martin) | 5 usuarios *Professional* - 15 usuarios *Limited* | - | 110 *Professional* - 80 *Limited* | 1750 |
| Servidores SAP (Nube) | - | - | 300 | 300 |
| Servicio Stellar (Catia y Casanova) | 10 cajas | - | 60 | 600 |
| Servidores Stellar (Nube) | - | - | 200 | 200 |
| TOTAL | | | | 4349 |

**Inversión Inicial (Dispositivos)**

| Equipo | Cantidad | Tarifa Unitaria ($) | Total |
|---|---|---|---|
| FortiGate 80F | 2 | 1200 | 2400 |
| FortiGate 60F | 1 | 850 | 850 |
| Switch Cisco SG300 52 Puertos | 4 | 900 | 3600 |
| Switch Cisco SG300 28 Puertos | 1 | 500 | 500 |
| TOTAL | | | 7350 |