Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Mecánica Eléctrica

DISEÑO DE INVESTIGACIÓN DE UNA PLANTILLA HOMOLOGADA PARA LA SOLUCIÓN SD-WAN DE ENLACES DE DATOS PARA CLIENTES CORPORATIVOS EN UNA RED MPLS REGIONAL

Ana Silvia Marroquín Morales
Asesorado por el MSc. Ing. Freddy Manolo Guzmán Orellana

Guatemala, abril de 2022

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

DISEÑO DE INVESTIGACIÓN DE UNA PLANTILLA HOMOLOGADA PARA LA SOLUCIÓN SD-WAN DE ENLACES DE DATOS PARA CLIENTES CORPORATIVOS EN UNA RED MPLS REGIONAL

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

ANA SILVIA MARROQUÍN MORALES
ASESORADO POR EL MSC. ING. FREDDY MANOLO GUZMÁN ORELLANA

AL CONFERÍRSELE EL TÍTULO DE

INGENIERA EN ELECTRÓNICA

GUATEMALA, ABRIL DE 2022

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANA	Inga. Aurelia Anabela Cordova Estrada
VOCAL I	Ing. José Francisco Gómez Rivera
VOCAL II	Ing. Mario Renato Escobedo Martínez
VOCAL III	Ing. José Milton de León Bran
VOCAL IV	Br. Kevin Vladimir Armando Cruz Lorente
VOCAL V	Br. Fernando José de Paz González
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Pedro Antonio Aguilar Polanco
EXAMINADOR	Ing. Guillermo Antonio Puente Romero
EXAMINADOR	Ing. Byron Odilio Arrivillaga Méndez
EXAMINADOR	Ing. Carlos Eduardo Guzmán Salazar
SECRETARIA	Inga. Lesbia Magalí Herrera López

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

DISEÑO DE INVESTIGACIÓN DE UNA PLANTILLA HOMOLOGADA PARA LA SOLUCIÓN SD-WAN DE ENLACES DE DATOS PARA CLIENTES CORPORATIVOS EN UNA RED MPLS REGIONAL

Tema que me fuera asignado por la Dirección de Escuela de Estudios de Postgrado con fecha 19 de febrero de 2019.

Ana Silvia Marroquín Morales

ESCUELA DE ESTUDIOS DE
POSTGRADO
FACULTAD DE INGENIERÍA

EEPFI-PP-0178-2022
Guatemala, 12 de enero de 2022

Director
Armando Alonso Rivera Carrillo
Escuela De Ingenieria Mecanica Electrica
Presente.

Estimado Ing. Rivera

Reciba un cordial saludo de la Escuela de Estudios de Postgrado de la Facultad de Ingeniería.

El propósito de la presente es para informarle que se ha revisado y aprobado el Diseño de Investigación titulado: **DISEÑO DE UNA PLANTILLA HOMOLOGADA PARA LA SOLUCIÓN SD WAN DE ENLACES DE DATOS PARA CLIENTES CORPORATIVOS EN UNA RED MPLS REGIONAL**, el cual se enmarca en la línea de investigación: **Telecomunicaciones - Telecomunicaciones**, presentado por la estudiante **Ana Silvia Marroquín Morales** carné número **201020708**, quien optó por la modalidad del "PROCESO DE GRADUACIÓN DE LOS ESTUDIANTES DE LA FACULTAD DE INGENIERÍA OPCIÓN ESTUDIOS DE POSTGRADO". Previo a culminar sus estudios en la Maestría en ARTES en Ingeniería Para La Industria Con Especialidad En Telecomunicaciones.

Y habiendo cumplido y aprobado con los requisitos establecidos en el normativo de este Proceso de Graduación en el Punto 6.2, aprobado por la Junta Directiva de la Facultad de Ingeniería en el Punto Décimo, Inciso 10.2 del Acta 28-2011 de fecha 19 de septiembre de 2011, firmo y sello la presente para el trámite correspondiente de graduación de Pregrado.

Atentamente,

"Id y Enseñad a Todos"

Freddy Manolo Guzmán Orellana
INGENIERO ELECTRÓNICO
Colegiado No. 10,172

Mtro. Freddy Manolo Guzman Orellana
Asesor(a)

UNIVERSIDAD DE SAN CARLOS
ESCUELA DE POSTGRADO
FACULTAD DE INGENIERIA
DE GUATEMALA

Mtro. Mario Renato Escobedo Martinez
Coordinador(a) de Maestría

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE INGENIERIA
DIRECCIÓN
ESCUELA DE POSTGRADO

Mtro. Edgar Dario Alvaréz Cotí
Director
Escuela de Estudios de Postgrado
Facultad de Ingeniería

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÍA

EEP-EIME-0178-2022

El Director de la Escuela De Ingenieria Mecanica Electrica de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del Asesor, el visto bueno del Coordinador y Director de la Escuela de Estudios de Postgrado, del Diseño de Investigación en la modalidad Estudios de Pregrado y Postgrado titulado: **DISEÑO DE UNA PLANTILLA HOMOLOGADA PARA LA SOLUCIÓN SD WAN DE ENLACES DE DATOS PARA CLIENTES CORPORATIVOS EN UNA RED MPLS REGIONAL**, presentado por el estudiante universitario **Ana Silvia Marroquin Morales**, procedo con el Aval del mismo, ya que cumple con los requisitos normados por la Facultad de Ingeniería en esta modalidad.

ID Y ENSEÑAD A TODOS

Ing. Armando Alonso Rivera Carrillo
Director
Escuela De Ingenieria Mecanica Electrica

Guatemala, enero de 2022

Decanato
Facultad de Ingeniería
24189101- 24189102
secretariadecanato@ingenieria.usac.edu.gt

LNG.DECANATO.OI.272.2022

La Decana de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Mecánica Eléctrica, al Trabajo de Graduación titulado: **DISEÑO DE INVESTIGACIÓN DE UNA PLANTILLA HOMOLOGADA PARA LA SOLUCIÓN SD-WAN DE ENLACES DE DATOS PARA CLIENTES CORPORATIVOS EN UNA RED MPLS REGIONAL,** presentado por: **Ana Silvia Marroquín Morales ,** después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, autoriza la impresión del mismo.

IMPRÍMASE:

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANA
FACULTAD DE INGENIERÍA

Inga. Aurelia Anabela Cordova Estrada
Decana

Guatemala, abril de 2022

AACE/gaoc

ACTO QUE DEDICO A:

Dios	Por siempre estar a mi lado y darme la fe y fuerzas para realizar una más de mis metas.
Mis padres	Por ser mi ejemplo, por su apoyo y amor incondicional brindado a lo largo de mi vida, por enseñarme a no darme por vencida y por todo el esfuerzo que han hecho para hacer realidad este sueño.
Mis hermanos	Mercedes, Javier y Alejandra Marroquín Morales, por llenar mi vida de alegría y brindarme su apoyo en todo momento.
Mis abuelos	Por sus enseñanzas y consejos durante toda mi vida.
Mis amigos	Por siempre brindarme su cariño y apoyo sincero.

AGRADECIMIENTOS A:

Universidad de San Carlos de Guatemala	Por ser la casa de estudios que me permitió formarme como profesional.
Facultad de Ingeniería	Por ser el lugar donde pude expandir y alcanzar muchos objetivos personales.
Mis amigos y compañeros de carrera	Por todas las convivencias, apoyo y motivaciones para cumplir nuestra meta en común.
Mi asesor	MSc. Ing. Freddy Manolo Guzmán, por haberme guiado durante el trabajo de graduación.
Mis compañeros de trabajo	Por compartir sus conocimientos y experiencias. Por acompañarme durante este proceso.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

LISTA DE SÍMBOLOS

Símbolo	Significado
$	Dólar estadounidense
Z	Nivel de Confianza
p	Página
P	Población
%	Porcentaje
c	Precisión
n	Tamaño de la muestra

GLOSARIO

Alta disponibilidad (**HA)** Es la capacidad de un sistema para operar continuamente sin fallar durante un período de tiempo designado. HA trabaja para garantizar que un sistema cumpla con un nivel de rendimiento operativo acordado.

Ancho de banda Es la máxima cantidad de datos transmitidos a través de una conexión a Internet en cierta cantidad de tiempo.

AS *Autonomous System.*

Automatización Aplicación de máquinas o de procedimientos automáticos en la realización de un proceso o en una industria.

Cloud computing La computación en la nube (c*loud computing*) es una tecnología que permite acceso remoto a softwares, almacenamiento de archivos y procesamiento de datos por medio de Internet, siendo así, una alternativa a la ejecución en una computadora personal o servidor local. En el modelo de nube, no hay necesidad de instalar aplicaciones localmente en la computadora.

Conectividad	Se denomina conectividad a la capacidad de establecer una conexión: una comunicación, un vínculo. El concepto suele aludir a la disponibilidad que tiene un dispositivo para ser conectado a otro o a una red.
Corporativo	Se entiende por corporativo como relativo, concerniente y perteneciente a la corporación como una entidad con o sin ánimo de lucro, asociación u organismo, pero de manera independiente a una administración estatal y que agrupa a varias personas que ejercen la misma actividad.
DHCP	*Dynamic Host Configuration Protocol*.
Equipo de última milla	La última milla es definida en las telecomunicaciones como el tramo final de una línea de comunicación, ya sea telefónica o un cable óptico, que llega al usuario final. El equipo de última milla es el que se entrega al final de este tramo.
Host	El término host o anfitrión se usa en informática para referirse a las computadoras u otros dispositivos (tabletas, móviles, portátiles) conectados a una red que proveen y utilizan servicios de ella.
Implementar	Poner en funcionamiento o aplicar métodos, medidas, entre otros. Para llevar a cabo una entrega de un servicio.

LAN	*Local Area Network*.
Metro Ethernet	Es una arquitectura tecnológica destinada a suministrar servicios de conectividad de datos en una Red de área metropolitana (MAN) de capa 2 en el modelo OSI, a través de interfaces (UNIs) Ethernet.
MP-BGP	Extensiones multiprotocolo para BGP (MBGP o MP-BGP), a veces denominadas *Multiprotocol* BGP o *Multicast* BGP y definidas en IETF RFC 4760, es una extensión del *Border Gateway Protocol* (BGP) que permite diferentes tipos de direcciones (conocidas como familias de direcciones) que se distribuirán en paralelo. Mientras que BGP estándar sólo admite direcciones de unidifusión IPv4, *Multiprotocol* BGP admite direcciones IPv4 e IPv6 y admite variantes de unidifusión y multidifusión de cada una.
MPLS	*Multiprotocol label switching*.
Nube	Aplicaban los conceptos de la virtualización del centro de datos en las funciones de la red. Con la llegada de la tecnología 5G, comenzaron a incorporar tecnologías modernas como los contenedores, los microservicios y las arquitecturas de nube híbrida. Durante esta transición, los contenedores y los microservicios deberán coexistir con las antiguas funciones de red virtualizadas (VNF) que se ejecutan en la actualidad.

On-premise	Equipo de telecomunicaciones que se instala y/o se ejecuta en computadoras en las instalaciones de la persona u organización que usa el software, en lugar de en una instalación remota como un granja de servidores o nube.
Overlay	Una red superpuesta (*overlay*) es una red de computadoras que se construye sobre otra red. Se puede pensar que los nodos en la red de superposición están conectados por enlaces lógicos o virtuales, cada uno de los cuales corresponde a una ruta, tal vez a través de muchos enlaces físicos, en la red subyacente.
Postventa	Período posterior a la venta de un producto, en el que el vendedor o el fabricante garantizan ciertos servicios, especialmente la reparación.
Protocolo de configuración dinámica de host (DHCP)	*Dynamic Host Configuration Protocol*, también conocido por sus siglas de DHCP) es un protocolo de red de tipo cliente/servidor mediante el cual un servidor DHCP asigna dinámicamente una dirección IP y otros parámetros de configuración de red a cada dispositivo en una red para que puedan comunicarse con otras redes IP.
Proveedor de Servicio	Un proveedor de servicios es una entidad que presta servicios a otras entidades. Por lo general, esto se

	refiere a un negocio que ofrece la suscripción o servicio web a otras empresas o particulares.
QoS	*Quality of Service*.
Red de transmisión	Es un conjunto de medios, tecnologías, protocolos y facilidades en general, necesarios para el intercambio de información y archivos entre los usuarios de una red.
Red	Una red de telecomunicación es un conjunto de medios, tecnologías, protocolos y facilidades en general, necesarios para el intercambio de información y archivos entre los usuarios de una red.
Redes sociales	Son sitios y aplicaciones que operan en niveles diversos – como el profesional, de relación, entre otros – pero siempre permitiendo el intercambio de información entre personas o empresas.
Región	Cada una de las divisiones territoriales de un país que tiene las mismas características geográficas e históricas o culturales, pero no administrativas; se puede dividir a su vez en provincias, departamentos, entre otros.
***Route* reflector**	Un *route* reflector es un *router* configurado para reenviar actualizaciones a sus vecinos o *peers* a través del mismo AS.

***Router* (enrutador)**	Es un dispositivo que permite interconectar computadoras que funcionan en el marco de una red. Su función es la de establecer la ruta que destinará a cada paquete de datos dentro de una red informática.
SDN	*Software-Defined Network*.
SD-WAN	*Software-Defined Wide Area Network*.
Servicio	Un servicio es todo acto o actividad que se ofrece para satisfacer una necesidad.
Solución	Elementos y conjuntos de elementos que nos permiten acceder a las redes de transmisión de información, sean éstas de carácter corporativo o personal.
Streaming	Tecnología que permite ver y oír contenidos que se transmiten desde internet u otra red sin tener que descargar previamente los datos al dispositivo desde el que se visualiza y oye el archivo.
Switch	Un *switch* o conmutador es un dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local (LAN) y cuyas especificaciones técnicas siguen el estándar conocido como Ethernet.

Traducción de direcciones de red (NAT)	La traducción de direcciones de red, también llamado enmascaramiento de IP o NAT (del inglés *Network address translation*), es un mecanismo utilizado por *routers IP* para cambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles. Consiste en convertir, en tiempo real, las direcciones utilizadas en los paquetes transportados. También es necesario editar los paquetes para permitir la operación de protocolos que incluyen información de direcciones dentro de la conversación del protocolo.
Transport-Domain	Se trata de redes de transporte distintas, cada una con accesibilidad, capacidades y comportamientos de SLA diferentes.
Underlay	Una red de transporte que ofrece tipos de conexión o transporte, como conmutación de etiquetas multiprotocolo (MPLS), internet, internet dedicado, fibra y banda ancha inalámbrica. Y sobre esta se configura de forma lógica otra red que tendrá el transporte de información mientras que ésta brinda únicamente el transporte de señalización.
VNF	*Virtualized Network Function.*
VPN	*Virtual Private Network.*
VPN-MPLS	*Virtual Private Network - Multiprotocol Label Switching.*

WAN *Wide Area Network.*

RESUMEN

El presente trabajo plantea el diseño de una plantilla homologada para la entrega de servicios de la solución SD-WAN para clientes corporativos utilizando como medio de transporte una red MPLS regional que se encuentra desplegada en la región centroamericana.

Para abordar el problema se trabaja en fases las cuales son: revisión documental de entregas y plantillas existentes, análisis de configuraciones comunes y configuraciones atípicas del producto, establecer el catálogo de servicios que se puede ofrecer para el producto, propuesta de configuraciones especiales de la solución (seguridad y QoS), diseño de la plantilla homologada para la solución y por último el diseño del plan de capacitación.

Con esta propuesta de diseño lo que se quiere lograr es una mejora en las características técnicas entregadas, simplificará los procesos de implementación, soporte y mantenimiento de los enlaces, brindando una mejor experiencia de usuario; teniendo una definición en común de entrega en las diferentes operaciones donde se aprovisionan los servicios.

1. INTRODUCCIÓN

En las redes de telecomunicaciones corporativas una de las formas en las que podemos validar la calidad de su servicio es a través del medio de transporte que da conectividad a sus usuarios. Las empresas están contando con la habilidad de poder operar aplicaciones críticas por medio de sus enlaces por lo que es importante contar con una red que brinde un gran ancho de banda y baja latencia. Las *Software-Define Wide Area Network* (SD-WAN) proporcionan varios beneficios para las empresas como lo son: simplificación de WAN, menores costos de infraestructura, eficiencia de ancho de banda y un medio de acceso sin problemas a la nube con un rendimiento de aplicaciones significativo, especialmente para aplicaciones críticas sin sacrificar la seguridad y la privacidad de los datos.

Las *Software-Define Wide Area Network* (SD-WAN) permiten a las empresas aprovechar cualquier combinación de red de transporte para conectar de forma segura a los usuarios a las aplicaciones, por medio de una función de control centralizada para dirigir el tráfico de forma segura e inteligente a través de la WAN. Esto ofrece una experiencia de usuario de alta calidad, lo que se traduce en una mayor productividad empresarial, agilidad y reducción de los costos.

Una solución SD-WAN dirige el tráfico de acuerdo con reglas predefinidas, generalmente programadas a través de plantillas. Una plantilla SD-WAN implementada de forma correcta ofrece un rendimiento óptimo del servicio. A través del monitoreo continuo y el autoaprendizaje, una SD-WAN se adapta continuamente a los cambios en la red, seleccionando tareas automáticamente

en tiempo real ante cualquier cambio que pueda afectar el rendimiento de la aplicación, incluida la congestión de la red, las caídas de tensión y las condiciones de desconexión de equipos, lo que permite a los usuarios conectarse siempre a la aplicación sin la intervención manual.

SD-WAN, es una alternativa rentable a las redes tradicionales de conmutación de etiquetas multiprotocolo (MPLS), que proporciona conectividad para ubicaciones geográficamente dispersas de una manera escalable y segura. SD-WAN se basa en la metodología de separar el plano de control del plano de datos para hacer que la red sea más inteligente. Arquitectónicamente cuenta con los siguientes aspectos: Gestión u orquestación centralizada (el plano de control), función de reenvío de datos distribuidos (el plano de datos) y políticas de enrutamiento de tráfico impulsadas por aplicaciones.

SD-WAN es una nueva solución que vino a cubrir los campos que otras tecnologías no podían satisfacer debido a los requerimientos de los clientes para cumplir con el correcto funcionamiento de sus aplicaciones. Pero como toda nueva tecnología esta se debe de estandarizar para que su entrega sea ágil y de fácil diagnóstico cuando se tenga una falla en la misma.

Se trata este tema de investigación por la importancia que tiene la homologación de nuevas tecnologías que salen al mercado. La homologación nos permite mejorar los tiempos de entrega de servicios y sobre todo tiene la función de poder satisfacer las necesidades de los clientes. Los proveedores cumplen un rol muy importante en el mercado, si ellos fallan al brindar un servicio que no cumple con las especificaciones técnicas, la calidad, el tiempo de entrega y capacidades de entrega requeridas, ocasionaron inconvenientes con sus clientes provocando pérdidas de dinero por no tener el dimensionamiento adecuado y perdiendo el sentido de flexibilidad que tiene SD-WAN.

Para lograr una homologación es muy importante que los proveedores desarrollen un reconocimiento de la situación actual y aceptación de las mejores prácticas a aplicar. Al lograr homologar las plantillas con las que se implementan los servicios SD-WAN, se logrará una mejora en las características técnicas entregadas, simplificará los procesos postventa y mantenimiento de los enlaces, pero lo más importante: brindará una mejor experiencia de usuario a los clientes corporativos que contraten el servicio.

La investigación se trabajará con un método de investigación mixto ya que permite comparar factores y resultados involucrados en el proceso; enriqueciendo la investigación, promoviendo una mayor amplitud, profundidad, diversidad y sentido de comprensión de lo que se está analizando. Con el método mixto se estudia más a fondo la situación de las entregas actuales de la tecnología SD-WAN para llegar a comprender y analizar la realidad que se tiene en cada operación, y así estructurar la transformación de la entrega por medio de la homologación del servicio a través de la región de Centro América. Además de planificar la capacitación y seguimiento que se debe tener con el personal que estará implementado los enlaces.

2. ANTECEDENTES

Los cambios de tecnología que han presentado las redes de telecomunicaciones en los últimos años se ven orientados a brindar servicios de mayor capacidad y pensando en la operación del cliente que lo contrata más que solo dar un canal de comunicación común entre dos puntos. Los análisis en tiempo real y la automatización del aprovisionamiento son factores que llegan a tener relevancia al momento de contratar una nueva solución.

> El nacimiento de aplicaciones en tiempo real, el video *streaming;* la masificación de las redes sociales, la introducción al *cloud computing* y muchos otros servicios, han dado como resultado el crecimiento exponencial del tráfico que circula por la red. A pesar de ello se continúan utilizando las mismas tecnologías que hace cincuenta años y los avances en cuanto a nuevas formas de comunicación y tratamiento de la información son casi inexistentes. (Intriago, 2017, p. 2)

Como indica Nazareno (2019) en su estudio, el utilizar tecnologías basadas en *Software Define Network* (SDN) brindaría un cambio importante en el desarrollo de proyectos de redes y telecomunicaciones generando un ahorro de dinero en implementaciones tecnológicas.

> SD-WAN, es una tecnología que tiene el potencial de revolucionar el sector de las redes de área extendida y viene dada como reemplazo de los servicios de optimización WAN, VPN-MPLS, automatización y administración de redes. Además, SD-WAN se puede entender como un enfoque único que permite a las organizaciones enrutar el tráfico a

> ubicaciones remotas, a través de medios de transporte más apropiados y proporcionar capacidades mejoradas para monitorear y administrar el tráfico de la red en tiempo real. (López, 2020, p. 14)

Pero contar con una nueva tecnología no es el único enfoque con el que se debe de trabajar, la nueva tecnología nos puede brindar las herramientas para la mejora de la red, pero su buen funcionamiento se encuentra también de la mano de una buena implementación y del diseño que se proponga para la solución de un cliente, sobre todo al tratarse de uno corporativo cuyo manejo de tráfico es crítico para su operación.

Como indica Delgado y Rubiano (2018) en su investigación, la tecnología SD-WAN es actualmente una de las tecnologías de auge por muchos proveedores de servicio y por fabricantes en la lucha por optimizar el tráfico de datos, pero un factor importante a tomar en cuenta es el análisis, planeación, coordinación, tiempos y puesta en marcha al momento de migrar a esta tecnología a un cliente ya en producción para poder mantener el buen nombre de la empresa encargada de realizar el cambio tecnológico.

A pesar de que las redes SDN nos permiten automatizar y manejar redes altamente escalables y flexibles que se adaptan rápidamente a los requerimientos de un cliente; se llegó también a la conclusión que una ejecución adecuada por parte del proveedor del servicio hace que la experiencia de cliente sea satisfactoria y tenga mayor aceptación en el mercado actual cuyas exigencias por el manejo de tráfico que se tiene es bastante alto y no permite que se tenga un mal manejo de tiempo y recursos.

3. PLANTEAMIENTO DEL PROBLEMA

Las soluciones de telecomunicaciones corporativas son aquellas con las que las empresas trabajan día a día para llevar a cabo sus actividades. Estas soluciones se encuentran orientadas a sus negocios y a la calidad del servicio que brindan; determinando aspectos importantes como su relación con el mercado, sus colaboraciones y su organización interna.

Los avances en telecomunicaciones y las necesidades de las personas que utilizan los servicios hicieron que las redes evolucionarán a medida que se requería un aumento de conectividad y seguridad. Las redes *Software Design Network* (SDN) son la apuesta como la solución más conveniente para Data Centers y redes de próxima generación por la flexibilidad y beneficios que brindan cuando el software asume tareas antes realizadas por hardware; pero a pesar de los beneficios que SDN brinda existen diferentes factores por lo que las empresas y proveedores de servicios aún no se encuentran listos para brindar este servicio.

Software define Wide Area Network (SD-WAN) es un tipo de SDN que tiene como objetivo disminuir los costos e incrementar uso de recursos de despliegue de equipos en múltiples ubicaciones geográficas para un mismo cliente en sus puntos remotos. Los administradores de red serán capaces de utilizar los anchos de banda contratados de forma más eficiente y así garantizar el rendimiento de aplicaciones críticas sin tener que sacrificar la seguridad de la información transmitida.

Una red SD-WAN maneja el tráfico tomando diferentes factores como: la prioridad y la calidad de servicio; además, aplica los requisitos de seguridad de

acuerdo con las necesidades que la empresa que está contratando el servicio requiera. Una de las principales ventajas de utilizar SD-WAN, aparte de mejorar el rendimiento de las aplicaciones, es que permite administrar de mejor manera el ancho de banda, adaptándolo a las necesidades y prioridades del cliente de forma personalizada. Todo ese control y gestión se realiza desde una única plataforma centralizada.

Para un proveedor de servicio el vender este tipo de soluciones a clientes corporativos como un producto definido es una tarea difícil, ya que parte de los beneficios que tiene SD-WAN es la flexibilidad de adaptarse a las necesidades de quien desee utilizar la solución. Uno de los principales problemas que se ha identificado en estas situaciones es que múltiples diseños pueden solucionar el mismo requerimiento de un cliente; teniendo como resultado diferentes topologías para una misma solicitud, ya que cada una depende de la persona que estructura la arquitectura y de quien la implemente. Si se tratará de una única operación local entregando un diseño no sería un inconveniente, pero estas son soluciones pensadas en despliegues en múltiples ubicaciones geográficas. Esta diferencia de topologías crea que se tenga problemas de diagnóstico de fallas y un deficiente servicio postventa; ya que al momento de analizar el enlace se tiene que entender lo que cada persona que implementó la solución llegó a proponer como topología.

Otro factor a tomar en cuenta en la implementación de los servicios SD-WAN son las políticas de cada una de las operaciones de los distintos proveedores en sus diferentes ubicaciones geográficas. Cada operación de cada país trabaja con diferentes definiciones para la entrega de servicios corporativos, estas son elegidas dependiendo los criterios de trabajo definidos según sus necesidades. Al momento de integrar todas las operaciones para la entrega de servicios de un cliente SD-WAN que tiene presencia en los países donde operan,

esas diferentes definiciones de entrega afectan; ya que se crea inconsistencia en los servicios implementados, teniendo variantes como costos, tiempo de implementación, rendimiento del enlace y calidad. Además, implica que la imagen del proveedor puede ser dañada al no tener conocimiento exacto de lo que se está configurando en cada ubicación, dando como percepción un producto de baja calidad o que no se cuenta con el personal adecuado para atender a los requerimientos.

Para esta investigación lo que se plantea es la creación de una plantilla para la entrega de productos SD-WAN que tenga como medio de transporte una red MPLS en la región centroamericana que incluye los países de Guatemala, Honduras, El Salvador, Nicaragua, Costa Rica y Panamá. Esto lleva a plantear la pregunta principal de estudio: ¿Cuál es la manera de optimizar con respecto a las entregas actuales la integración de servicios para trabajar de forma homologada en diferentes países de la región la entrega de las soluciones SD-WAN? Para responder a esta interrogante se deberán contestar las siguientes preguntas auxiliares.

- ¿Cuáles son los servicios de datos que se pueden entregar en una solución SD-WAN?

- ¿Qué características de seguridad se implementan para los enlaces de datos de clientes corporativos?

- ¿Cómo se establece la calidad de servicio en los enlaces de datos corporativos entregados en una solución SD-WAN?

- ¿Cuál es el conocimiento necesario para implementar un servicio SD-WAN corporativo para la entrega de enlaces de datos?

4. JUSTIFICACIÓN

La realización de la presente investigación se justifica en la línea de investigación de método mixto, ya que este método es la combinación de la perspectiva cuantitativa y la cualitativa en un mismo estudio. Se realizó de esta manera ya que las preguntas de la investigación son complejas y nos permite ampliar los temas y las teorías para profundizar en los procesos de enseñanza y aprendizaje para la entrega de los servicios corporativos en la solución de SD-WAN.

Los aportes que se esperan de este trabajo de investigación es un entendimiento unificado sobre las soluciones SD-WAN que se ofrecen a los diferentes clientes corporativos utilizando como medio de transmisión una red MPLS, mejorando la calidad del producto a ofrecer y sobre todo tener solo una única solución optimizada para cada requerimiento que se tenga.

Los productos que se obtendrán dentro de esta investigación es un catálogo de servicios donde se podrán analizar las limitantes y las características que se podrían ofrecer para la implementación de la solución SD-WAN en los diferentes países; así como un estándar para la calidad de servicio y seguridad que se puede ofrecer para la transmisión de datos.

El beneficio será tanto para los clientes como para el proveedor de servicio que implemente, esto es porque se brindará un producto definido y al ser una solución homologada la entrega será ágil y contará con los requisitos necesarios para que la experiencia del cliente sea satisfactoria. Adicionalmente el mantenimiento y el soporte de los servicios se simplificará, teniendo también un

mejor servicio postventa y disminuyendo la curva de aprendizaje necesaria para que las áreas involucradas tengan la capacitación necesaria para implementar y soportar los servicios entregados.

La importancia de la homologación de los servicios para una nueva tecnología es encontrar las respectivas especificaciones técnicas que se consideran para las diferentes soluciones de software que ofrece SD-WAN. Así mismo, la pruebas a realizar con cada uno de los escenarios que se ofrecerían a los clientes corporativos. Es así como se detalla el procedimiento técnico a seguir para la implementación de cada uno de estos servicios. Las conclusiones y recomendaciones permiten reconocer los conceptos importantes que se deben tener en cuenta para lograr una homologación exitosa, la cual se debe reflejar en la gran aceptación del producto en el mercado competitivo.

5. OBJETIVOS

5.1. General

Diseñar una plantilla homologada para la entrega de servicios corporativos SD-WAN a nivel regional utilizando enlaces de datos dedicados configurados sobre una red MPLS.

5.2. Específicos

- Definir el catálogo de servicios a implementar para una solución SD-WAN para los clientes corporativos.

- Establecer las configuraciones de seguridad necesarias para un servicio corporativo entregado por SD-WAN.

- Plantear las características de QoS para la priorización de transmisión de datos en la entrega de los servicios SD-WAN para clientes corporativos.

- Diseñar un plan de capacitación para la implementación de servicios corporativos.

6. NECESIDADES POR CUBRIR Y ESQUEMA DE SOLUCIÓN

La necesidad de realizar este trabajo de investigación es para lograr la homologación de SD-WAN como producto para la mejora de los procesos de entrega y de soporte. La homologación permitirá garantizar el funcionamiento de la solución bajo los mismos parámetros para todos los clientes que deseen contratarla sin importar el país en donde se esté implementando. También permitirá fijar indicadores para la mejora continua del producto y de las actividades.

El no contar con una plantilla homologada para la entrega de servicios da lugar a que las topologías propuestas a los clientes no puedan ser implementadas de forma adecuada, hace que al momento de ocurrir una falla el soporte sea más difícil de brindar porque no se conoce con exactitud las variantes que se pudieron configurar ya que SD-WAN tiene mucha flexibilidad como solución, pero esta se debe de limitar en sus alcances para poder ofrecer como producto.

Un diseño unificado beneficia tanto a proveedor como a cliente simplificando tareas como el mantenimiento y las solicitudes de cambio que se tengan por crecimiento o reestructuración de la topología, haciendo que estas tareas sean más sencillas de ejecutar al contar en todos los países con una configuración estandarizada y con la gestión centralizada de SD-WAN. Los cambios son fácilmente replicables por lo que, si aprovisionar antes era una tarea de meses, ésta se puede realizar en minutos sin enviar personal técnico a cada punto remoto.

Para lograr diseñar la plantilla lo primero que debemos delimitar son los servicios que se brindarán en SD-WAN, como se espera que su uso sea para clientes corporativos se plantea un catálogo de servicios en donde se pueden brindar los siguientes servicios: Transporte de datos, redistribución de internet, DHCP, NAT, integración de sus equipos *on-premise* con la solución SD-WAN, configuraciones de alta disponibilidad (HA), calidad de servicio (QoS) y políticas de seguridad. Teniendo ya los servicios a entregar, en el orquestador de SD-WAN se crea la plantilla general de servicio en donde se especificarán las configuraciones de WAN, LAN, *Transport–Domains*, anchos de banda y alta disponibilidad (HA).

Para realizar las configuraciones específicas para cada cliente se trabajará por medio de plantillas de servicio. El director u orquestador de SD-WAN nos permite cargar las plantillas de servicio a una plantilla general sin que esté borrar o sobrescribir información y así hacer modular las configuraciones que se desean realizar; para poder brindar la granularidad del servicio que cada cliente solicite y que es parte de los beneficios que brinda SD-WAN.

Al establecer los alcances y limitantes del producto por medio de la homologación se logrará el entendimiento del producto SD-WAN como solo uno a través de la región, garantizando de esta manera que se trabaje bajo un mismo catálogo, bajo las mismas topologías y con las mismas capacidades técnicas a través de los distintos países. El alcance a nivel de plantilla es sólo para configuraciones iniciales de entrega, los cambios postventa o reingenierías sobre la topología diseñada se deberán trabajar con otro tipo de plantillas, pero se trabajará sobre el mismo catálogo de servicios establecido.

6.1. Esquema de la solución

El esquema de la solución del problema que se aborda en esta investigación contará de 6 fases las cuales son: revisión documental de entregas y plantillas existentes, análisis de configuraciones comunes y configuraciones atípicas del producto, establecer el catálogo de servicios que se puede ofrecer para el producto, propuesta de configuraciones especiales de la solución (seguridad y QoS), diseño de la plantilla homologada para la solución y por último el diseño del plan de capacitación para la mejora de las entregas.

La primera fase es la revisión documental de entregas y plantillas de servicios existentes; con esto se quiere llevar el histórico de las topologías diseñadas y servicios configurados para poder establecer un repositorio de información histórica de la solución SD-WAN.

La segunda fase es el análisis de configuraciones comunes y casos atípicos de configuración; con esto se espera establecer el alcance técnico del producto en cuanto a las configuraciones comunes para crear una oferta estándar. Con los casos atípicos se establecerán las soluciones y plantillas de servicios adicionales que se pueden ofrecer como complementos a la solución y que se encuentren homologadas entre el catálogo a ofrecer.

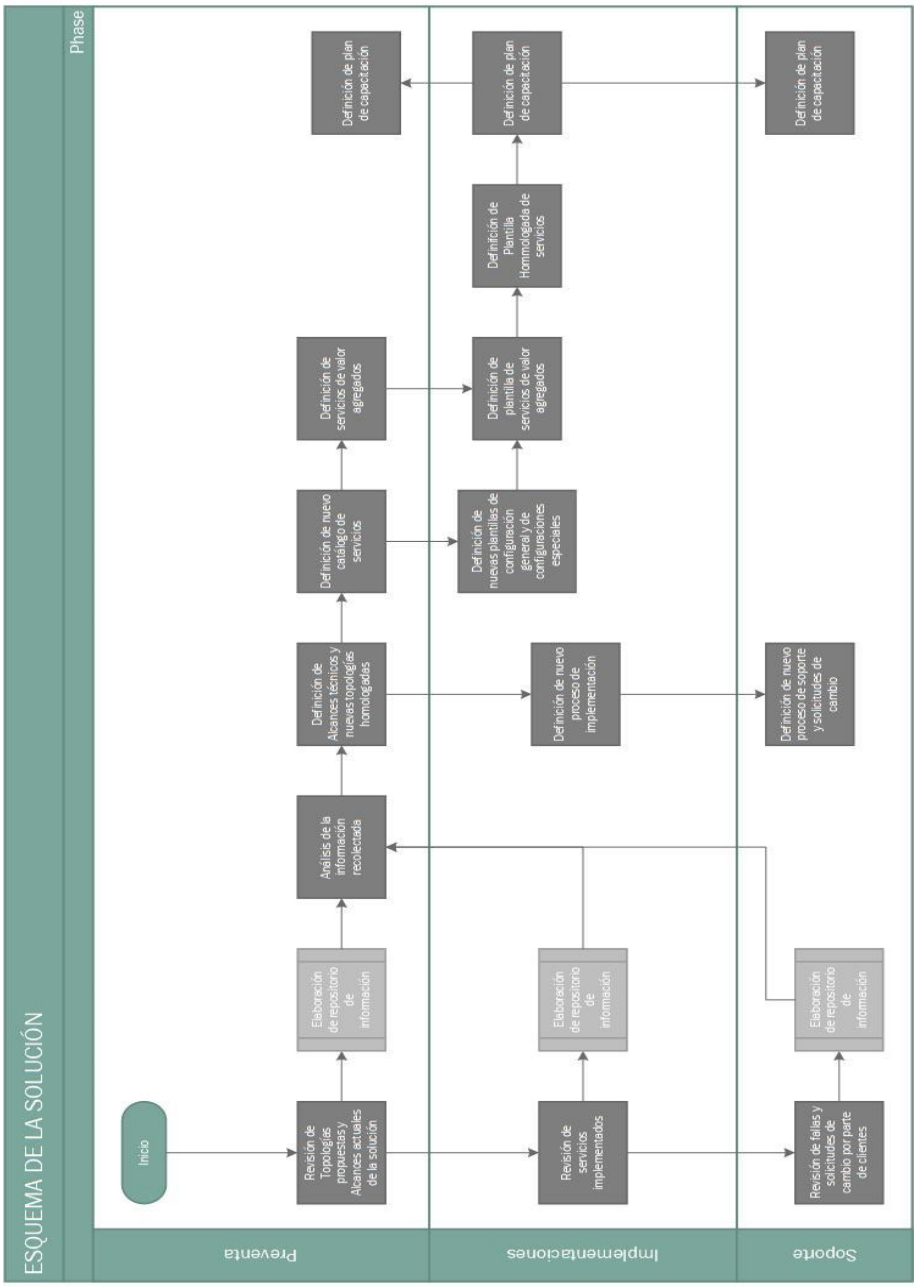
La tercera fase es la creación del catálogo del servicio; ya teniendo los alcances técnicos y comerciales del producto en la nueva versión homologada se creará un catálogo de servicios para poder ofrecer estos a los clientes y también poder capacitar a las distintas áreas que se involucran por parte del proveedor para el conocimiento de este.

La cuarta fase es la propuesta de configuraciones de la solución, cuando ya se tiene el producto establecido en el catálogo con sus posibles variantes atípicas; se plantea de forma adicional el estandarizar el uso del QoS y características de seguridad adicionales como un servicio de valor agregado para SD-WAN.

La quinta fase es ya proponer las plantillas generales de SD-WAN y las plantillas de servicios que incluirían las configuraciones atípicas, las configuraciones de QoS y las configuraciones de seguridad.

La sexta y última fase es planificar el plan de capacitación para todas las áreas involucradas: preventa, implementaciones y soporte. Con este plan se tendrán expertos en los servicios definidos en el catálogo y en los servicios de valor agregado que se tenga para la solución de SD-WAN.

Figura 1. **Esquema de la solución**

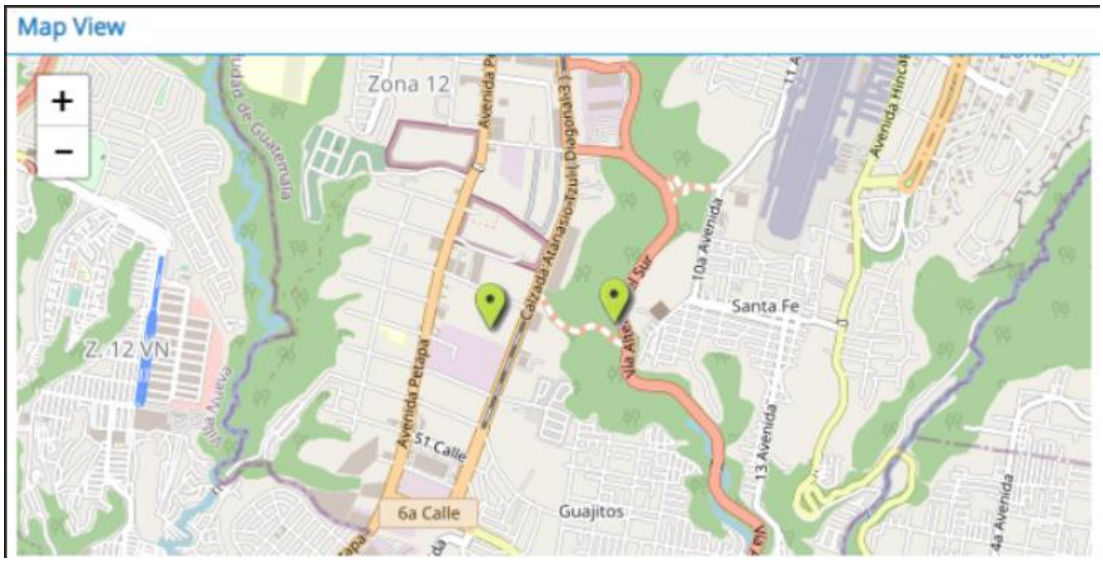


Fuente: elaboración propia, empleando Microsoft Visio 2019.

6.2. Ubicación geográfica de la solución

El orquestador o director del SD-WAN, así como los controladores y la analítica se encuentran virtualizados en un Data Center en la zona 12 de la ciudad de Guatemala. Estos son los que brindan el servicio de SD-WAN a la región centroamericana, conociéndose a nivel de *underlay* con *transport-domain* de datos y de internet.

Figura 2. **Ubicación *Headend***



Fuente: Google Earth (2021). Consultado el 12 de agosto de 2021. Recuperado de Lansat/Copernicus 2020 INEGI.

Los equipos cuentan con las siguientes características.

Figura 3. **Servicios *Headend***

Fuente: Versa Networks. (2021). *Arquitectura de una solución SD-WAN.* Consultado el 13 de septiembre de 2021. Recuperado de https://docs.versa-networks.com/Reference/Architecture/02_SD-WAN_Solution_Architecture.

7. MARCO TEÓRICO

Esta sección está dirigida a presentar la base teórica para dar a conocer el fundamento del conocimiento en materia de la entrega de servicios corporativos, los fundamentos de MPLS y los servicios SD-WAN.

7.1. Servicios de telecomunicaciones corporativos

Un servicio de telecomunicaciones se puede definir como:

> Conjuntos de facilidades y medios (físicos y lógicos) operados y/o gestionados por un proveedor de servicio que éste pone a disposición de los usuarios, con unas normas de acceso y utilización, para satisfacer las necesidades de telecomunicaciones de los clientes. (Figueiras, 2002, p. 99)

Los servicios de telecomunicaciones son aquellos servicios que ofrece una empresa de comunicaciones dentro de un área de cobertura. La forma más común de servicio de telecomunicaciones es el servicio telefónico, que puede ser entregado cableado o inalámbrico. Otros servicios que se pueden brindar son Internet, televisión y redes de datos para empresas y hogares. Es posible que estos servicios no estén disponibles en todas las áreas o en todas las empresas; y sus precios pueden ser diferentes variando ampliamente si son brindados a residencias o negocios.

Los elementos básicos para brindar un servicio de telecomunicaciones son: los equipos físicos, el medio de transporte, las configuraciones lógicas y el tipo de información que por medio de este servicio se brinda. Un proveedor de

servicio puede ser contratado por uno o por múltiples usuarios y puede trabajar ya sea con medio propio o servir de intermediario subarrendando medios para poder brindar el servicio a un cliente a través de terceros.

Los servicios de telecomunicaciones se pueden clasificar de diferentes maneras, por sus atributos, características, tecnologías de transporte, mercado objetivo, entre otros. Los servicios de telecomunicaciones corporativos es una de estas clasificaciones y nos referimos a este tipo de servicio como aquellos que se utilizan en las empresas para llevar a cabo sus actividades laborales. Su principal diferenciador es el nivel de calidad ya que esto determinará aspectos importantes como su productividad, seguridad y colaboración en la organización. Los clientes corporativos se preocupan principalmente por la calidad y confiabilidad de sus enlaces para la entrega de datos u otros servicios.

Un servicio corporativo brinda una conexión dedicada obteniendo el cliente un servicio simétrico, seguro, rápido y estable; permitiendo de esta manera garantizar la calidad de los enlaces del usuario. Los servicios corporativos pueden brindar enlaces de datos o de internet según lo que el usuario desee contratar.

Los servicios corporativos de datos tienen la capacidad de interconectar dos o más puntos de manera privada y segura, extendiendo la red corporativa permitiendo usar este medio para el transporte de voz, video y datos en múltiples puntos en tiempo real. Son enlaces con menor latencia, optimizando los tiempos de respuesta en una conexión segura ya que el tráfico nunca sale a internet; permitiendo conectar diferentes sucursales en un amplio territorio geográfico.

7.2. Homologación

Una homologación la podemos definir como una aprobación oficial de cumplimiento de requerimientos de un producto o servicio. La tecnología es uno de los campos donde los servicios homologados tienen mayor relevancia ya que esto garantiza su correcto funcionamiento, aumentando los niveles de confianza al proveedor y manteniendo la fidelidad de los clientes.

Las homologaciones son llevadas a cabo por medio de ensayos, pruebas y calibraciones. Por medio de la homologación se comprueban las características y especificaciones de un producto o servicio acorde a un conjunto de normas. Esta aprobación es realizada por una autoridad en el campo dando validez al resultado.

En la actualidad muchas empresas solicitan las homologaciones a sus proveedores de servicios para contrataciones nuevas o renovaciones de contrato, esto para garantizar que el servicio o producto contratado cumpla con los requerimientos para la necesidad que se desea cubrir, de acuerdo con su forma de trabajar y a las políticas de la empresa.

Los campos que abarca una homologación son varios y dependen del servicio o producto a homologar. En cuanto a tecnología podemos mencionar que los principales factores que se evalúan son: Calidad, seguridad, estabilidad, alta disponibilidad, entre otros. Con esta evaluación se tendrá la validación de que el proveedor contratado cuenta con las capacidades y recursos para brindar el servicio esperado en el tiempo contratado.

7.2.1. Métodos de homologación

Los procedimientos con los cuales se puede realizar la homologación de un servicio o producto brindado por una empresa que brinda servicios a usuarios pueden ser:

- Auditorías: es uno de los métodos más utilizados para homologar por parte de los proveedores. Una auditoría consta de varias fases; la primera es recopilar información por diferentes métodos como encuestas, entrevistas y cuestionarios. Luego esta información obtenida es analizada para validar los puntos de mejora y si el servicio contratado cuenta con las diferentes características mínimas para ser utilizado por un usuario en específico.

- Testeo: este método de homologación lo que busca principalmente es la calidad de los productos o servicios a entregar. Se busca examinar los productos y servicios previo a ser contratados para validar si son adecuados y si cumplen con las expectativas del consumidor.

- Histórico: se establece la homologación en base a experiencias anteriores. Se evalúa la capacidad y desempeño en base a comportamientos detectados al momento de implementar los servicios.

7.3. Calidad total

El lanzamiento de un nuevo servicio debe tener como resultado el cumplimiento de las expectativas que tengan los usuarios que lo contraten. Las nuevas tecnologías no serían de ayuda para los usuarios si no se logra un servicio de calidad que se mantenga con los mismos estándares durante todo el tiempo de contratación.

La innovación es uno de los factores determinantes de los servicios emergentes, los cuales siempre están susceptibles a una mejora continua conforme los procesos de diseño, instalación y soporte vayan madurando y cualquier modificación que aporte en este aspecto es parte de la misma innovación de este.

La calidad de un servicio lo podemos relacionar con las siguientes características: el diseño de la topología, la fiabilidad de los procesos que incluye la entrega del servicio, la facilidad de mantenimiento y la seguridad brindada al usuario.

Un proveedor no solo debe buscar la calidad en la entrega de un servicio o producto, sino la calidad en diferentes áreas como lo es la gestión para la entrega trabajando con la calidad total del mismo.

La calidad total tiene un enfoque hacia todos los grupos de interés del servicio o producto, es decir, el usuario, así como al cliente interno por lo que la satisfacción sobre la entrega de un servicio o producto también debe incluir la satisfacción de los empleados que están involucrados en la entrega o elaboración del este; teniendo una mejora continua sobre el servicio o producto a entregar y también una mejora en los procesos de la organización.

Los resultados de presentar un servicio o producto que cuenta con calidad total son: clientes leales, reducción de tiempos, reducción de costos para resolución de problemas y un ambiente laboral que respalda y estimula el trabajo en equipo.

7.3.1. Ventajas de la calidad total

La calidad total ha dado lugar a la creación de un modelo de excelencia en la gestión de entrega de servicios o productos. Tendiendo la siguiente utilidad en cuanto la gestión:

- Identificar los productos o servicios con los principios de excelencia empleando un marco de gestión que está formado por buenas prácticas que son aplicables a diferentes campos en la industria.

- Es un instrumento de autoevaluación para el personal interno de las organizaciones, permitiendo dar reconocimiento y aumentando la identificación de los empleados con los principios y valores de la empresa mejorando la cultura laboral.

7.4. Redes MPLS (*Multiprotocol label switching*)

Los avances que han surgido en las telecomunicaciones han tenido como resultado que aparezcan nuevas tecnologías siendo MPLS (*Multiprotocol label switching*) una de ellas. MPLS vino a cubrir las necesidades de conectividad y seguridad en redes que tienen mayor cobertura haciendo que los servicios puedan ser entregados de forma más eficaz. Una red MPLS puede servir para el transporte de distintos servicios como lo son: Voz, datos y video que utilizan una dirección IP para comunicarse con otros sitios. Brindando un recurso que supera limitaciones de velocidad que otras tecnologías poseen y mejora el flujo de trabajo de la transmisión.

MPLS es una técnica para la entrega de enlaces, no un servicio, por lo que puede ofrecer distintas configuraciones, desde VPN hasta metro Ethernet. Las

empresas han contratado servicios corporativos sobre MPLS para establecer comunicación con sus diferentes sitios remotos que necesitan acceso a datos o aplicaciones que se encuentran en la central de datos de la sede central de la empresa o en el sitio donde centralizan su información.

7.4.1. Fundamentos de MPLS

MPLS o también conocido como protocolo múltiple de conmutación de etiquetas, es conocido como una tecnología de conmutación de red que es efectiva, rápida y altamente escalable que trabaja por medio del redireccionamiento de circuitos ofreciendo capacidades de multiprotocolo, quiere decir, que sus técnicas de transporte son aplicables a cualquier protocolo a nivel de red.

MPLS realiza su enrutamiento de forma flexible basándose en la asignación de flujos de rutas de un punto inicial a un punto final que estén trabajando bajo un mismo dominio autónomo.

Las etiquetas añadidas permiten la toma de decisiones de reenvío de paquetes; independientemente del protocolo con el que se realiza el enrutamiento. MPLS se puede decir que trabaja en la capa 2.5 del modelo OSI, esto es porque MPLS no encaja perfectamente en la jerarquía de las 7 capas del modelo OSI. El beneficio clave de MPLS es la capacidad que posee de separar el reenvío de paquetes del servicio de datos que se encuentra subyacente. Es decir, MPLS es capaz de crear tablas para ejecutar el reenvío de paquetes bajo cualquier protocolo que tenga de *underlay*. Por estas características MPLS es un protocolo utilizado en redes troncales IP.

Al combinar las tecnologías con las que trabaja de enrutamiento de capa red y la manera de conmutar los paquetes de capa de datos, MPLS combina de forma eficiente la flexibilidad del enrutamiento IP y la simplicidad de la conmutación de la capa de datos. MPLS utiliza la construcción de túneles para su transmisión, pero no es un servicio ni una aplicación.

La etiqueta de MPLS se encuentra compuesto de cuatro partes:

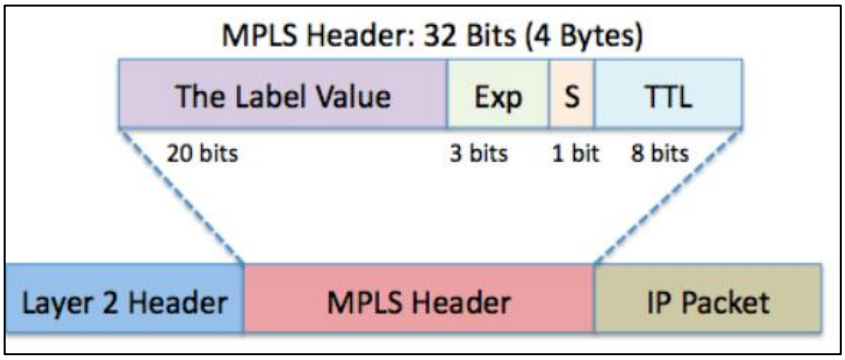
- La etiqueta (*Label*): la etiqueta contiene la parte donde se encuentra la información de los equipos que enrutan los paquetes MPLS para determinar dónde se debe de enviar el paquete.

- Experimental: los *bits* que se identifican como experimentales son los que son utilizados para determinar la calidad de servicio (QoS), con estos se puede determinar la prioridad con la que será transportado el paquete que se etiqueta a través de la red.

- *Bottom-of-Stack*: indica en los equipos que realizan el enrutamiento de MPLS si son el último equipo tramo en el camino determinado para el paquete y no se encuentran más etiquetas de las cuales se debe preocupar para el direccionamiento del tráfico. Esto generalmente indica que ese *router* es el *router* de salida.

- *Time-To-Live*: identifica cuántos saltos puede dar un paquete antes de ser descartado.

Figura 4. **Estructura de una etiqueta MPLS**

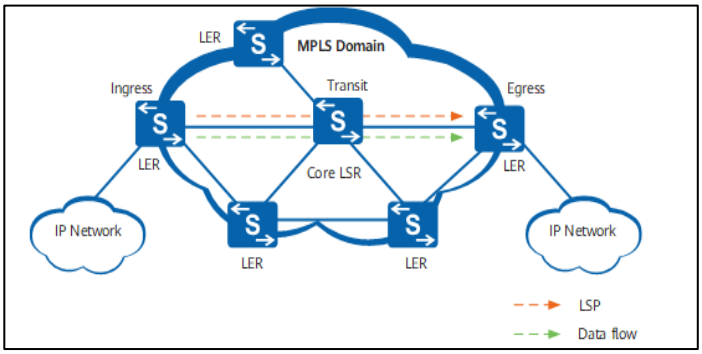


Fuente: Huawei. (2021). *MPLS VPN*. Consultado el 13 de septiembre de 2021. Recuperado de https://support.huawei.com/enterprise/en/doc/EDOC1000178173/2edd846/mpls-vpn.

7.4.2. Estructura de la red MPLS

Una red MPLS típica trabaja reenviando los paquetes basándose en etiquetas. Los dispositivos de red son los encargados de intercambiar las etiquetas MPLS y envían los paquetes por los enrutadores de conmutados de etiquetas (LSR) que en conjunto forman un dominio de MPLS. Los equipos LSR que se encuentran en los extremos del dominio MPLS y que se encuentran conectados a otras redes o tecnologías de transmisión se llaman enrutadores de borde de etiqueta (LER), y los equipos LSR que se encuentran dentro del dominio MPLS son los LSR centrales (Core).

Figura 5. **Estructura de una red MPLS**



Fuente: Tech Club. (2019). *Red MPLS*. Consultado el 8 de septiembre de 2021. Recuperado de https://techclub.tajamar.es/red-mpls/.

Cuando unos paquetes IP ingresan a una red que es MPLS, estos son analizados por el LER que se encuentra en el extremo inicial para luego agregar las etiquetas necesarias para la transmisión. Todos los LSR de la red MPLS que se encuentran en el mimo dominio envían los paquetes según las etiquetas que se agregaron en el LER inicial. Cuando los paquetes IP salen de la red MPLS, el LER de salida muestra las etiquetas que han sido agregadas en el trayecto del paquete.

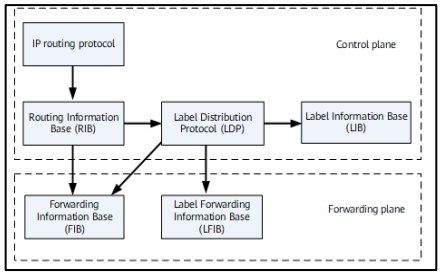
La ruta en la cual se transmiten los paquetes IP en una red MPLS se denomina LSP o ruta de etiqueta conmutada. Un LSP es una ruta unidireccional que define el camino que recorren los paquetes de datos. El dispositivo LER que se encuentra en el extremo inicial de un LSP se denomina nodo de entrada y el dispositivo LER que se encuentran en el extremo final del LSP se le conoce como nodo de salida. Los distintos dispositivos LSR que se encuentra entre el nodo de entrada y el nodo de salida a lo largo del LSP son conocidos como los nodos de tránsito. Un LSP puede llegar a tener de cero hasta varios nodos de tránsito en toda su trayectoria, pero solo un nodo de entrada y uno de salida.

7.4.3. Arquitectura de una red MPLS

En una red MPLS cuando un paquete ingresa por primera a este se le asigna una etiqueta donde se la clase de servicio de reenvío (CoS) con la que trabajará, esto también es conocido como la clase de equivalencia de reenvío (FEC), la cual se indica en el paquete agregando una secuencia de bits corta (la etiqueta) en este. Estas clases suelen indicar que tipo de tráfico transportan lo que nos permite etiquetar el tráfico según la prioridad de transmisión que estos tengan: tiempo real, tráfico crítico y *best effort*; ubicando cada aplicación en una de las clases definidas. En otro protocolo de enrutamiento es imposible separar el tráfico en función del rendimiento, siendo esta otra ventaja de MPLS. La arquitectura de MPLS es la clave ya que las etiquetas permiten adjuntar información al paquete más allá de lo que un *router* maneja para el direccionamiento del tráfico.

La arquitectura de una red de un mismo dominio MPLS consta de dos planos: un plano de control y un plano de reenvío.

Figura 6. **Modelo Arquitectónico de una red MPLS**



Fuente: Huawei. (2021). *Basic MPLS Architecture.* Consultado el 8 de septiembre de 2021. Recuperado de https://support.huawei.com/enterprise/en/doc/EDOC1000178173/7c5ca4fb/basic-mpls-architecture.

La arquitectura de una red MPLS está conformada por los siguientes componentes.

7.4.3.1. Plano de control

Es el plano en el que se genera y mantiene la información de etiquetas MPLS y de enrutamiento con el que se enviaran los paquetes en la red, este se encuentra compuesto por:

- Base de Información de Enrutamiento (RIB): se genera con los datos de la información de enrutamiento IP y es lo que los distintos equipos que componen la red utilizan para selección de rutas.

- Protocolo de Distribución de Etiquetas (LDP): asigna etiquetas en los dispositivos, creando una base de información de etiquetas que se manejan en la red (LIB) y con esta información se establecen o se eliminan los diferentes LSP.

- Base de Información de Etiquetas (LIB): esta información es generada por LDP al momento de asignar etiquetas y se utiliza para que los dispositivos administren las mismas.

7.4.3.2. Plano de reenvío (planos de datos)

Es en plano donde se realiza el redireccionamiento y envío de paquetes IP y paquetes MPLS en una red de un proveedor.

- Base de información de reenvío (FIB): esta base es genera con la información de los distintos protocolos de enrutamiento que brinda la base

de información de enrutamiento (RIB) y se función es para poder reenviar los paquetes comunes de IP que se transportan en el dominio de una red de MPLS.

- Base de enrutamiento de reenvío de etiquetas (LFIB): es creada por el protocolo de distribución de etiquetas (LDP) en un dispositivo LSR para poder reenviar los datos con las etiquetas MPLS a través de los equipos que componen la red.

7.4.4. Escenarios de aplicación para MPLS

Se describirán los escenarios comunes de configuración de una red MPLS.

7.4.4.1. VPN MPLS

En una VPN tradicional la transmisión de datos en la red privada se realiza a través de distintos protocolos de tunelización, siendo algunos de estos protocolos: el encapsulado de enrutamiento genérico (GRE), el protocolo de tunelización de capa 2 (L2TP) y el protocolo de tunelización punto a punto (PPTP).

En MPLS se configuran las rutas de etiquetas conmutadas (LSP) para el intercambio de etiquetas y paquetes de información que no cuentan con ningún encapsulamiento ni cifrado. Por estas características, MPLS es una técnica de enrutamiento cuya forma de transmitir los datos permite que la configuración de VPN sea fácil de implementar.

En una red VPN MPLS se puede configurar de forma segura una red privada de manera muy similar a una red *Frame Relay* (FR). En las redes VPN MPLS los dispositivos de última milla o CPE no necesitan de la configuración de túneles (GRE o L2TP) para construir esta topología, esta se construye dentro del mismo MPLS sin ser un servicio adicional sobre el transporte.

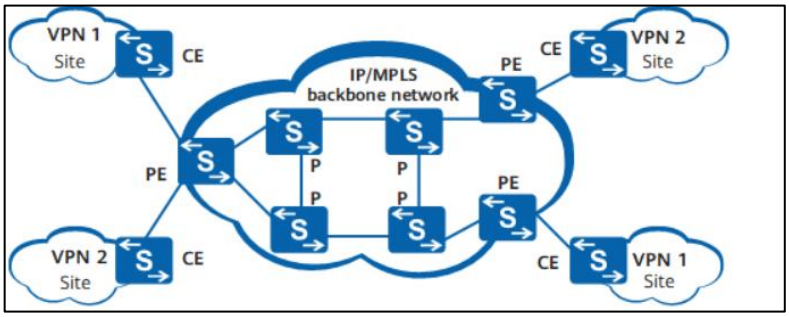
Una red VPN MPLS por medio de un LSP unificado logra la conexión de todos los equipos en los que se quiere configurar la red privada. La red VPN MPLS está compuesta por los siguientes dispositivos.

- Cliente final (CE): se implementa en uno de los equipos de borde de la red entre el proveedor y el cliente. Puede ser un *router*, un *switch* o un *host*.

- Borde del proveedor (PE): se implementa en el borde de una red troncal IP / MPLS.

- Un dispositivo de proveedor (P): este dispositivo en una red troncal IP/MPLS no está conectado directamente a los CE. El dispositivo del proveedor sólo necesita proporcionar capacidades de reenvío MPLS básicas y no mantiene información de VPN, es un equipo de tránsito.

Figura 7. **Arquitectura de una red VPN MPLS**



Fuente: Huawei. (2021). *MPLS VPN.* Consultado el 9 de septiembre de 2021. Recuperado de https://support.huawei.com/enterprise/en/doc/EDOC1000178173/2edd846/mpls-vpn.

Una VPN MPLS tiene las siguientes características:

- Los PE administran usuarios de VPN, configuran LSP entre PE y anuncian información del protocolo de enrutamiento con la que trabajan los usuarios que se encuentran en una VPN.

- Los PE utilizan MP-BGP para anunciar la información de enrutamiento de VPN.

- La VPN basada en MPLS admite la multiplexación de direcciones IP entre sitios, así como la interconexión de diferentes VPN.

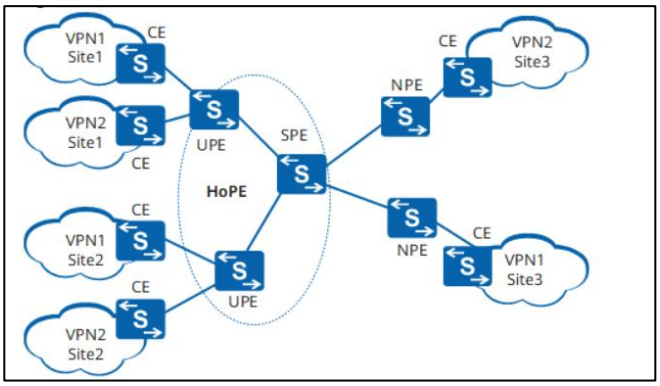
7.4.4.1.1. HVPN

La mayoría de los diseños de redes utilizan actualmente una arquitectura jerárquica. Sin embargo, una red BGP/VPN MPLS IP utiliza un modelo plano para la transmisión de paquetes. Esto quiere decir que todos los dispositivos PE están ubicados en el mismo plano. Para implementar servicios VPN en una estructura

de red jerárquica, el modelo plano de BGP/VPN MPLS IP debe convertirse en un modelo jerárquico. La solución de jerarquía de VPN (HVPN) ayuda con este proceso de conversión.

La solución HVPN distribuye las funciones de un PE a varios PE. Estos PE juegan diferentes roles y forman una arquitectura jerárquica. La solución HVPN también se denomina solución de jerarquía de PE (HoPE).

Figura 8. **Arquitectura de una red VPN MPLS HVPN**



Fuente: Huawei. (2021). *HVPN*. Consultado el 13 de septiembre de 2021. Recuperado de https://support.huawei.com/enterprise/es/doc/EDOC1000178179/b295b528/hvpn.

Los componentes de una red HVPN son:

- UPE: se conecta directamente a las CE y proporciona servicios de acceso a los usuarios.

- SPE: son los dispositivos conectados a UPE y ubicados en el núcleo de una red. Las SPEs administran y publicitan rutas VPN existentes.

- NPE: son los equipos que se conectan a los SPEs y ubicados en la parte de la red de distribución.

El reenvío de etiquetas se utiliza entre una SPE y una UPE; solo se requiere una interfaz SPE para conectarse a la UPE. La SPE no necesita proporcionar numerosas interfaces para conectarse a los usuarios.

MP-IBGP o MP-EBGP se pueden utilizar entre una UPE y una SPE, dependiendo de si pertenecen al mismo AS o a diferentes AS. Cuando se usa MP-IBGP, un SPE funciona como un RR de múltiples UPE para anunciar rutas entre pares IBGP. Para reducir el número de rutas en las UPE, se recomienda evitar utilizar la SPE como RR para otras PE.

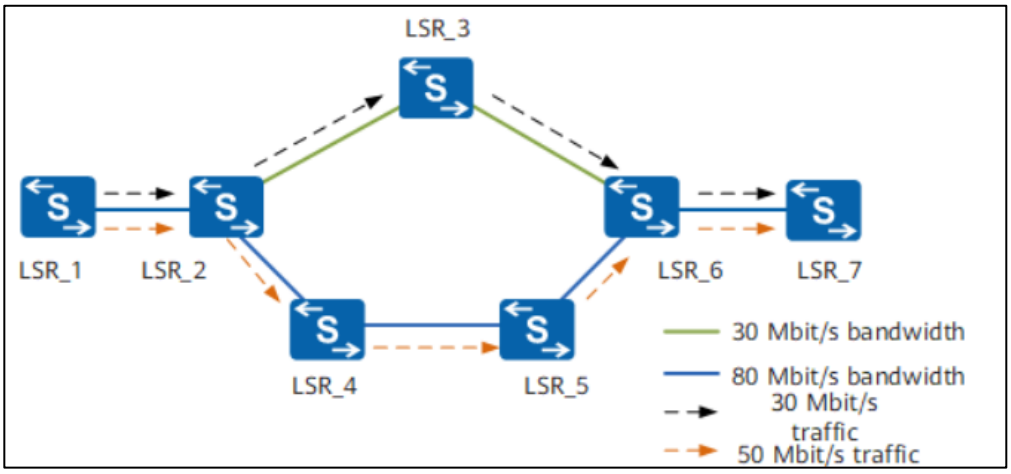
7.4.4.2. MPLS TE

En las redes IP tradicionales, los *routers* seleccionan la ruta más corta como ruta preferida independientemente de otros factores que pueden afectar la comunicación, como el ancho de banda. El tráfico en una ruta no se cambia a otras rutas, incluso si la ruta está congestionada. Como resultado, la primera regla de la ruta más corta puede causar problemas graves en las redes en las cuales se tiene transporte de tráfico crítico.

La ingeniería de tráfico (TE) verifica los distintos datos enviados en una red y la carga de los dispositivos que componen la misma para luego ajustar los parámetros como la gestión del tráfico, el enrutamiento y los parámetros de restricción de recursos en tiempo real según las necesidades establecidas por el administrador de la red. Estos ajustes ayudan a prevenir la congestión de la red causada por la distribución desequilibrada del tráfico.

La ingeniería de tráfico (TE) se puede implementar en una red troncal a gran escala utilizando una solución simple y escalable. MPLS, un modelo de superposición permite establecer una topología virtual sobre una topología física y mapea el tráfico a la topología virtual. MPLS se puede integrar con TE para implementar MPLS TE.

Figura 9. **Arquitectura de una red MPLS TE**



Fuente: Huawei (2021). *MPLS TE.* Consultado el 9 de septiembre de 2021.Recuperado de https://support.huawei.com/enterprise/en/doc/EDOC1000178173/622a51a3/mpls-te.

MPLS TE puede reservar recursos configurando diferentes LSP en todo el recorrido de una ruta determinada para el transporte para evitar la congestión en los dispositivos de red y equilibrar el tráfico que se transmite por medio del dominio de MPLS.

Una red MPLS con TE tiene las siguientes ventajas:

- MPLS TE es capaz de garantizar el uso de los recursos para obtener la calidad de los servicios durante el establecimiento de LSP.

- La manera de trabajar de un LSP se puede controlar fácilmente en función de los atributos del LSP, como la prioridad y el uso de la capacidad del servicio.

- Cuando se establece un LSP el consumo de recursos es mínimo y no interfiere a cualquier otro servicio que esté funcionando en la red.

- La ruta de respaldo y el redireccionamiento rápido (FRR) protegen la transmisión de información en la red en caso de tener un inconveniente en un enlace o un nodo.

Estas ventajas hacen de MPLS TE la solución TE óptima. MPLS TE permite a las empresas encargadas de brindar servicios (SP) aprovechar al máximo los recursos de red existentes para proporcionar diversos servicios, optimizar los recursos de red y administrar de manera eficiente la red.

7.5. SD-WAN

Los últimos años se ha visto un rápido aumento en la adopción de la computación en la nube y un aumento generalizado de dispositivos móviles para ofrecer aplicaciones comerciales y de consumo. Las empresas han utilizado principalmente enlaces MPLS para establecer conexiones seguras entre sus centros de datos, en donde sus aplicaciones se encontraban alojadas en los servidores físicos, y los sitios de las sucursales.

Sin embargo, a medida que se han agregado más dispositivos y aplicaciones y que las aplicaciones han pasado de ejecutarse solo en centros de datos privados a operar también en múltiples nubes, la conexión de usuarios y dispositivos a aplicaciones ahora desafía la arquitectura de seguridad

centralizada y la red tradicional. Por lo general, requieren retroceso de todo el tráfico, incluido el tráfico destinado a la nube, desde las sucursales hasta el centro de datos central o central donde se pueden aplicar servicios de inspección de seguridad avanzados. El retraso causado por el retorno afecta el rendimiento de la aplicación, lo que da como resultado una mala experiencia del usuario y una pérdida de productividad. La necesidad de simplificar, escalar y asegurar la red ha creado un requisito para nuevos enfoques en donde SD-WAN propone una topología que unifica el transporte tradicional MPLS con la nube.

En la actualidad las empresas buscan cada vez más acceso distribuido a Internet en todos los sitios y dependen de conexiones de Internet dedicadas para acceder a aplicaciones de *software* como servicio (SaaS) y entornos de múltiples nubes. Las VPN MPLS continúan brindando conectividad de sitio a sitio para las aplicaciones adecuadas (por ejemplo, voz, video o aplicaciones comerciales críticas). Este uso de múltiples conexiones WAN y acceso a Internet distribuido, combinado con la necesidad de reducir el costo y la complejidad mientras se mantiene la seguridad, ha transformado la red y la arquitectura de seguridad, dificultando el trabajo de administración.

Los proveedores de servicios y las empresas están adoptando soluciones basadas en redes definidas por *software* (SDN) para brindar servicios administrados con mayor rapidez y agilidad. Estas soluciones SDN automatizan la arquitectura de red y seguridad, lo que facilita la programación de políticas basadas en el usuario, el dispositivo, la aplicación, la red, entre otros. Estas soluciones brindan visibilidad y control en profundidad, y reducen el costo y la complejidad, lo que acorta el tiempo que lleva implementar la red y hace que la administración de cambios sea más rápida y sencilla.

La solución SD-WAN proporciona una VPN segura y unificada en varias WAN públicas y privadas. Esta solución integra completamente los servicios virtualizados para permitir que las empresas y los proveedores de servicios implementen una solución SD-WAN administrada de forma centralizada.

7.5.1. Beneficios de SD-WAN

SD-WAN es una solución que tiene la inteligencia, la confiabilidad, el rendimiento y la escala necesarios para garantizar una experiencia de red superior. Algunos de los beneficios que tiene SD-WAN son.

- Orquestación y automatización: SD-WAN proporcionan una orquestación completa centralizada de todas las funciones WAN, como lo son enrutamiento de paquetes, las políticas de seguridad que incluyen los servicios de seguridad avanzados y la optimización de la WAN en la transmisión de tráfico. Cuando las empresas necesitan implementar nuevas políticas o cuando se requiere un cambio, SD-WAN hace posible que los cambios necesarios se implementen en unos minutos en lugar de semanas o meses.

- Autoaprendizaje continuo: SD-WAN impulsada ofrece un rendimiento óptimo de las aplicaciones en cualquier condición o cambio de la red, incluida la congestión y cuando se producen deterioros por fallas en los medios de transmisión. A través del monitoreo continuo y el autoaprendizaje, SD-WAN responde automáticamente en tiempo real a cualquier cambio en el estado de la red; adaptándose continuamente a las variaciones que ocurren en una red lo que permite a los clientes conectarse siempre a la aplicación sin la intervención manual.

- Calidad de experiencia (QoEx): SD-WAN tiene la capacidad de brindar servicio activamente por medio de múltiples formas de transporte WAN. SD-WAN supervisa y gestiona de forma inteligente todos los servicios de transporte que se encuentran en el *underlay*. Puede identificar la pérdida de paquetes, la latencia y *jitter* en la transmisión y realizar los cambios necesarios de forma automática para ofrecer niveles altos de rendimiento de la aplicación y QoEX a los usuarios, incluso cuando los servicios de transporte WAN tengan fallas; maneja una interrupción total del transporte sin problemas.

- Microsegmentación de servicio: SD-WAN proporciona capacidades de seguridad en todo el tramo de transmisión. Además de admitir un firewall de última generación, la plataforma SD-WAN debe orquestar y hacer cumplir la microsegmentación para abarcar todo el tráfico que se dirige del centro de datos LAN-WAN y a la nube LAN-WAN. Las políticas de seguridad al ser aplicadas de forma centralizada son más consistentes debido a la menor cantidad de errores creando un aumento en la eficiencia operativa al mismo tiempo que reduciendo cualquier brecha de seguridad.

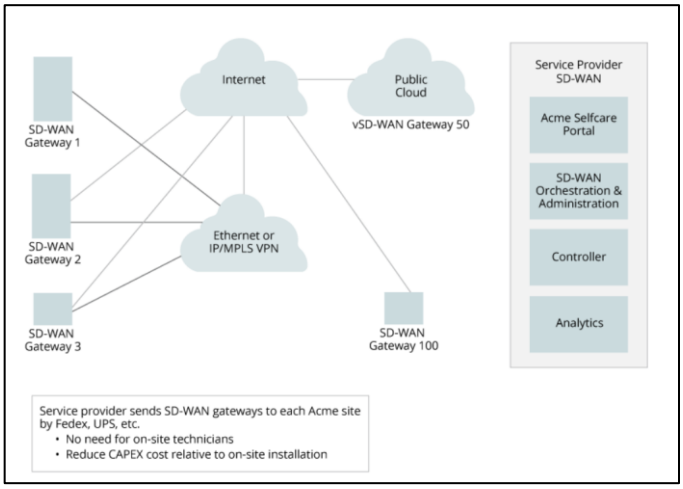
Salida de Internet local para aplicaciones en la nube. SD-WAN se adapta continuamente a los cambios y proporciona definiciones de aplicaciones automatizadas y actualizaciones de direcciones IP. Eliminando la interrupción de la aplicación y los problemas de productividad del usuario.

7.5.2. Arquitectura SD-WAN

La arquitectura de implementación de SD-WAN consta de dos componentes básicos: los nodos de cabeceras (*Headend*) y nodos de *branch* (borde). Un nodo

de cabecera consta de un controlador, un director u orquestador y *cluster* de analítica.

Figura 10. **Arquitectura de una solución SD-WAN**



Fuente: Versa Networks. (2021). *Arquitectura de una solución SD-WAN.* Consultado el 13 de septiembre de 2021. Recuperado de https://docs.versa-networks.com/Reference/Architecture/02_SD-WAN_Solution_Architecture.

7.5.2.1. Nodo de cabecera (*Headend*)

Un nodo de cabecera consta de: un controlador, un director u orquestador y un *cluster* de Analítica. La cabecera se puede implementar en un centro de datos o en una nube compartida, pública o privada. En la mayoría de las implementaciones, se utilizan cabeceras redundantes para lograr una alta disponibilidad. Por lo general, se encuentran en dos centros de datos geográficamente separados u otras ubicaciones centralizadas, o en la nube en zonas o regiones separadas.

Los componentes de la cabecera (*Headend*) establecen la comunicación por medio de un enlace de control seguro basado en IP y trabajan en conjunto para administrar la red de equipos finales que se encuentran en las sucursales. Los dispositivos de la sucursal están conectados entre sí y a la cabecera por medio de una red pública (como internet), de una red privada (como una red MPLS), o a través de ambos.

7.5.2.1.1. Controlador (*Controller*)

El controlador proporciona el elemento del plano de control para todas las instancias virtuales en la red, incluidas las sucursales (*branch*) donde se encuentran los dispositivos finales, los concentradores y las puertas de enlace (nodos). Por lo general, se encuentra en una ubicación centralizada (centro de datos, oficina central o nube pública) desde la cual se conecta a todos los nodos de la red. Los túneles de superposición de control desde cada nodo hasta los controladores forman lo que se conoce como el plano de control de los servicios SD-WAN. Estos túneles transportan tráfico IPsec y MP-BGP.

El controlador es responsable de las siguientes funciones:

- El controlador usa certificados para autenticar las instancias virtuales de los dispositivos finales junto con el orquestador, se recomienda el uso de autenticación de dos factores para autenticar dispositivos de sucursal.

- Mantiene un canal de control seguro con cada nodo. El canal seguro transporta todo el tráfico de control entre los nodos de las sucursales y controlador, que luego se comunica con los nodos del director y la Analítica. Usando el canal seguro, el controlador maneja todas las actividades de administración entre los nodos remotos y de cabecera,

como usar *Netconf* sobre SSH para impulsar plantillas de configuración y activar servicios, y distribuir información del plano de control usando MP-BGP.

- Distribuir la información de accesibilidad para todos los nodos. El controlador distribuye las rutas BPG hacia las VPN y los *tenant*. Utiliza un *route* reflector MP-BGP de múltiples instancias personalizado para distribuir información de las rutas y la información de seguridad (SA) a los nodos de sucursal (*branch*) en el grupo de red, según el *tenant* o la VPN a la que pertenezcan. Cuando un nodo de sucursal anuncia su información de ruta de *overlay*, incluye una SA de entrada para establecer la conexión segura. El controlador redistribuye las actualizaciones de rutas de BGP, las etiquetas (en el caso de VPN de múltiples *tenant*) y las SA para que las sucursales de destino puedan establecer canales de datos seguros hacia todos los CPE de nodos de sucursal en la misma VPN. Según cómo se configure la política de redistribución, se crea la topología adecuada (*Hub-and-Spoke*, malla completa o malla parcial).

- Habilita la conectividad IPsec entre sucursales sin la sobrecarga de mantener una malla completa de claves de seguridad entre todas las sucursales: esta optimización evita la sobrecarga de administrar enlaces y claves N2, en lugar de que el controlador distribuya la información de SA. El enlace IPsec entre el nodo de la sucursal y el controlador SD-WAN distribuye las claves IPsec a otros nodos de la sucursal. El resultado es que los nodos de sucursal (*branch*) deben mantener claves N + 1 en lugar de claves N2.

Puede implementar un controlador para cada red SD-WAN o puede implementar varios controladores para proporcionar alta disponibilidad.

7.5.2.1.2. Director u orquestador

El director es una plataforma de administración y aprovisionamiento que realiza las siguientes funciones:

- Configuración, administración y supervisión centralizadas de un solo panel de control de los controladores, las sucursales y los sitios de concentradores.

- Gestión del ciclo de vida de las instancias de los dispositivos finales.

- Alta disponibilidad (HA) a nivel del sistema implementada como un par activo-pasivo para la redundancia.

- Servidor de ensayo durante el proceso de arranque.

- Administrador de funciones de red virtual (VNFM).

- Aprovisionamiento sin intervención (ZTP) de dispositivos con sistema operativo virtual en sucursales y centros.

Las características principales de funcionamiento del director incluyen:

- Soporte de superposición de red: toda la comunicación hacia el sistema operativo virtual se realiza mediante un túnel de red superpuesto (*overlay*), lo que proporciona una gestión coherente en diversos entornos WAN.

- Control de acceso basado en roles (RBAC): le permite limitar el acceso y definir las capacidades de lectura y escritura de los usuarios que ingresen a la plataforma.

- *Multi tenant* jerárquico: particionamiento de la administración y la conectividad, con hasta cinco niveles de jerarquía.

- Monitoreo de dispositivos: capacidades de crear tableros en todos los dispositivos para realizar diferentes pruebas remotas, incluidas las pruebas de velocidad y el monitoreo del ancho de banda.

El director proporciona las capacidades de aprovisionamiento esenciales para la red y los servicios de seguridad de la solución. Estas capacidades incluyen conectividad, configuración, implementación, orquestación y monitoreo. El director utiliza varias herramientas para la orquestación y la gestión del ciclo de vida, incluidas *Netconf*, API, GUI y CLI. Las API permiten la integración con aplicaciones de administración de nube de terceros existentes.

Cuando varios sitios, sucursales o instancias de dispositivos finales tienen configuraciones similares, puede crear plantillas y aplicarlas a las instancias, lo que garantiza la coherencia entre los sitios. Las plantillas de configuración pueden contener variables para adaptarse a parámetros específicos de la rama (*branch*), como subredes del lado LAN, grupos DHCP, reglas de políticas de acceso y reglas de reenvío basado en políticas (PBF).

7.5.2.1.3. Analítica

La analítica es una plataforma de análisis diseñada específicamente para dispositivos finales y servicios administrados. La plataforma proporciona

visibilidad de los dispositivos. Puede utilizar los datos analizados para realizar líneas base, correlaciones y predicciones sobre los dispositivos. La analítica proporciona datos históricos y en tiempo real, y puede crear informes sobre patrones de uso, tendencias, eventos de seguridad y alertas. El director también proporciona acceso basado en roles a la plataforma de analítica permitiendo brindar acceso a los clientes como al administrador de red a la información según los perfiles definidos.

Los dispositivos *branch* proporcionan continuamente a la plataforma el estado y la información cuantitativa sobre sus enlaces, rutas de red y servicios. Además, cada servicio que se ejecuta en una instancia de VOS, como NGFW y filtrado de URL, genera mensajes de registro agregados y de nivel de flujo que se envían para tener registro. Con esta información, la plataforma realiza una serie de funciones, que incluyen análisis y optimización de toda la red, resolución de problemas, tendencias, planificación de capacidad, control de tráfico dinámico basado en aplicaciones y análisis forense de seguridad. La plataforma de analítica pasa los resultados de sus análisis al director.

Un nodo de analítica consta de tres componentes:

- Recopilador y exportador de registros: el recopilador de registros recibe y almacena registros de dispositivos y puede transmitirlos a recopiladores de terceros. Los registros se pueden enviar a través de conexiones TCP, UDP y SSL y en varios formatos de registro, incluidos IPFIX y *syslog*. Los registros más antiguos se archivan.

- Motor de base de datos, búsqueda y análisis: el motor de base de datos, búsqueda y análisis proporciona servicios de almacenamiento, búsqueda y análisis, y replica automáticamente los datos en uno o más nodos de la

analítica. Los análisis de seguridad, redes y aplicaciones aprovechan el sistema de gestión de bases de datos para el análisis en memoria de alta velocidad. La búsqueda se puede realizar mediante consultas genéricas y personalizadas, y los servicios de correlación se pueden realizar mediante API.

- Aplicación de analítica: la aplicación proporciona servicios basados en API a la interfaz de usuario de la analítica y a aplicaciones personalizadas de terceros. Junto con el director, también proporciona servicios de autenticación y autorización para acceder al nodo de analítica.

Debido a que las funciones de búsqueda y análisis consumen muchos recursos, normalmente implementa un par de nodos de analítica como un clúster, con un nodo realizando la función de búsqueda y el segundo nodo realizando la función de análisis. Para alta disponibilidad (HA), cada clúster debe tener un mínimo de cuatro nodos, dos para datos analíticos y dos para datos de búsqueda. Cada par de nodos de un clúster está en modo activo-activo y los datos se replican entre cada par de nodos.

Cada grupo de nodos de analítica forma una instancia de analítica. La instancia puede residir en uno o más centros de datos o regiones. Puede implementar cada nodo en servidores *bare-metal*, dispositivos de caja blanca de terceros o como una máquina virtual.

7.5.2.2. Nodos *branch*

Los nodos de sucursal (*branch*) en una solución SD-WAN proporcionan funciones de red y seguridad consolidadas en una única instancia virtual que se puede implementar en un dispositivo x86 físico o como una máquina virtual (VM).

Los nodos de sucursales (*branch*) se encuentran, como su nombre lo indica, en los sitios de las sucursales. Están conectados entre sí y a la cabecera (*headend*) por medio de una red pública (como Internet), a través de una red privada (como un dominio de red MPLS), o a través de ambos.

7.5.2.2.1. Cajas blancas

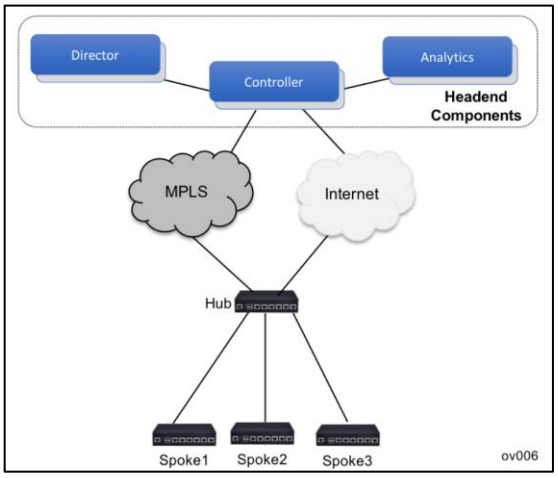
Un dispositivo de caja blanca es un componente de red que se ensambla a partir de componentes básicos estandarizados. Para optimizar una orquestación en la nube, la mayoría de las aplicaciones y prácticas comerciales se llevan a cabo mediante VNF (funciones de red virtualizadas), que incluyen *vFirewall / vDDoS, vBRAS, SD-WAN, vLoad Balancer, vUnified Communication, vIP Security, vWAN Optimizer y vProbe/Service Assurance*. Por lo tanto, son necesarias las adopciones de procesadores de múltiples núcleos y un alto número de núcleos.

7.5.2.2.2. Topologías de nodos *branch*

Se pueden implementar nodos de sucursal (*branch*) en las siguientes topologías:

- *Hub-and-Spoke*: permite elegir si los nodos *spoke* se comunican entre sí y de qué manera, según los requisitos de su negocio. Las topologías *de hub-and-spoke* se implementan ampliamente porque son más fáciles de configurar y administrar y, por lo general, son menos costosas que las topologías de malla completa o parcial. En las implementaciones de sucursales de *hub-and-spoke*, al menos un nodo se configura como *Hub* y uno o más nodos se configuran como *spoke*.

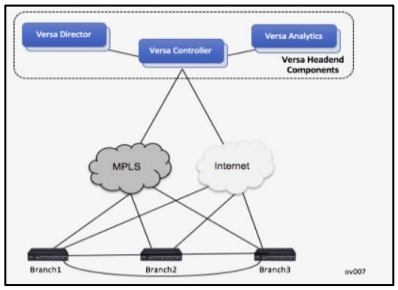
Figura 11. **Arquitectura de red *Hub-and-Spoke***



Fuente: Versa Network. (2021). *Arquitectura de red Hub-and-Spoke.* Consultado el 10 de septiembre de 2021. Recuperado de https://docs.versa-networks.com/Getting_Started/Versa_Product_Solution/04_Solution_Architecture.

- Malla completa: en una topología de *branch* de malla completa, todos los nodos de *branch* pueden comunicarse directamente con todos los demás nodos de rama. Es una topología altamente redundante y tolerante a fallas, dado que se puede llegar a todos los sitios mediante múltiples rutas, no hay un solo punto de falla. Sin embargo, se necesita más tiempo y esfuerzo para crear y mantener una topología de malla completa.

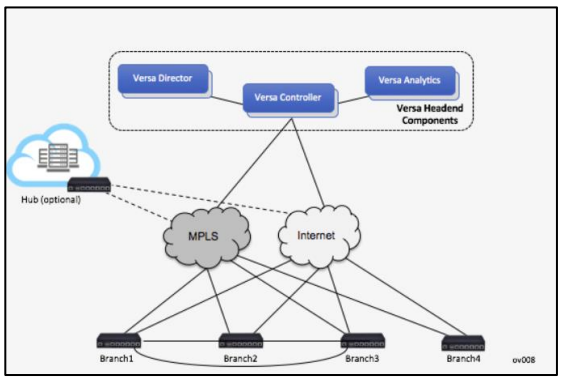
Figura 12. **Arquitectura de red *Full Mesh***



Fuente: Versa Network (2021). *Arquitectura de red Full Mesh.* Consultado el 10 de septiembre de 2021. Recuperado de https://docs.versa-networks.com/Getting_Started/Versa_Product_Solution/04_Solution_Architecture.

- Malla parcial: en una implementación de malla parcial, dos o más nodos están conectados entre sí para formar una topología de malla completa, mientras que otros nodos se comunican a través de un *Hub* (opcional) o se conectan directamente a un controlador.

Figura 13. **Arquitectura de red *Full Mesh***



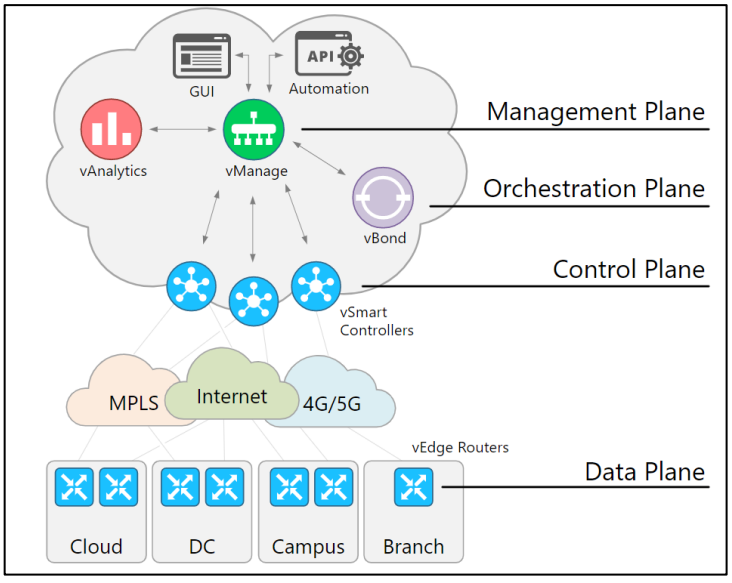
Fuente: Versa Network (2021). *Arquitectura de red Full Mesh.* Consultado el 10 de septiembre de 2021. Recuperado de https://docs.versa-networks.com/Getting_Started/Versa_Product_Solution/04_Solution_Architecture.

En un entorno de varios *tenant,* se puede implementar la topología deseada por *tenant*. El director proporciona flujos de trabajo para guiarlo a través de la configuración de nodos de sucursal en la topología deseada.

7.5.3. Componentes de una solución SD-WAN

SD-WAN se compone de cuatro planos separados los cuales son: orquestación, gestión, control y datos. Cada plano tiene sus propias funciones y responsabilidades y se abstrae de los otros planos. Por ejemplo, si reemplaza un dispositivo en el plano de datos, eso no afecta el plano de control / administración u orquestación. Lo mismo se aplica si reemplaza un controlador en el plano de control o en la parte de la gestión.

Figura 14. **Componentes de una solución SD-WAN**



Fuente: Network Academy. (2021). *Componentes de una solución SD-WAN*. Consultado el 14 de septiembre de 2021. Recuperado de https://www.networkacademy.io/ccie-enterprise/sdwan/what-is-sd-wan.

7.5.3.1. Plano de administración

Ejecuta la interfaz de usuario del sistema y es el panel de control con el que los administradores de red interactúan a diario. Es responsable de recopilar datos de telemetría de red, ejecutar análisis y alertar sobre eventos en la estructura SD-WAN. También es la herramienta que utilizan los administradores para crear plantillas de dispositivos, insertar configuraciones y realizar ingeniería de tráfico de superposición.

7.5.3.2. Plano de orquestación

Su trabajo es orquestar el proceso de incorporación de nuevos dispositivos no configurados a la estructura SD-WAN. Es responsable de la autenticación y la creación de listas blancas de los dispositivos finales y la distribución de información de control / gestión hacia estos.

7.5.3.3. Plano de control

Los controladores son el cerebro de la estructura de superposición (*overlay*). Anuncian enrutamiento, políticas y seguridad. Se colocan como *routers Hub* en la topología del plano de control y todos los dispositivos finales se emparejan con todos los controladores. Los controladores son como los *route reflectors* de BGP; sin embargo, es importante comprender que estos dispositivos no forman parte del plano de datos y no participan en el reenvío de paquetes.

7.5.3.4. Plano de datos

Los dispositivos finales representan el plano de datos del sistema SD-WAN. Se colocan en los extremos de los dispositivos que componen la WAN para

formar la arquitectura de la red, siendo los que unen los dispositivos del cliente y a la superposición de SD-WAN. Todo lo que se encuentra conectado a la LAN de los dispositivos finales es típicamente una red tradicional: oficinas, data center y sitios remotos (sucursales). Todo lo que se encuentra en la WAN de los dispositivos finales es el propio sistema SD-WAN.

7.5.4. Funciones de una solución SD-WAN

SD-WAN es una solución flexible y escalable, al ser virtualizada permite que las características con la que trabajarán los dispositivos finales sean elegidas por el administrador de la red según las necesidades de cada topología. Algunas de las funciones con las que cuentan los servicios SD-WAN son.

7.5.4.1. Funciones de *software* de red

Los dispositivos con sistemas operativos virtualizados brindan protocolos de enrutamiento de red de nivel de operador que le permiten usar un dispositivo final como un enrutador virtual independiente o como parte de una solución SD-WAN de extremo a extremo.

Los protocolos de enrutamiento permitidos por la parte de *software* son:

- Reenvío bidireccional (BFD): detecta la vitalidad de los pares BGP, los vecinos OSPF y los siguientes saltos de la ruta estática.

- *Border gateway protocol* (BGP) y *Multiprotocol* BGP (MP-BGP): BGP y MP-BGP son protocolos de *gateway* exterior estandarizados (EGP) que permiten el intercambio de información de enrutamiento entre dispositivos en diferentes sistemas autónomos (AS). Estos protocolos definen la

accesibilidad de la red en función de los prefijos de IP que forman parte de un AS.

- Enrutamiento de múltiples rutas de igual costo (ECMP): los dispositivos finales admiten hasta 16 rutas ECMP a cualquier destino.

- *Open shortest path first* (OSPF): utiliza métodos dinámicos para determinar las rutas a los destinos de la red. OPSF utiliza anuncios de estado de enlace (LSA) para compartir información de ruta con otros enrutadores. Al usar esta información de ruta y asignar un costo a cada interfaz de enrutador, OSPF toma decisiones de enrutamiento. OSPF procesa una gran cantidad de información de ruta de forma dinámica, por lo que requiere un procesador más rápido y más memoria que otros protocolos.

- Redistribución de rutas: las reglas de política redistribuyen las rutas desde un protocolo de enrutamiento de origen (BGP, OSPF y estático) a un protocolo de destino (BGP y OSPF).

- Enrutamiento estático: configura rutas estáticas para reenviar el tráfico en la red.

- Enrutamiento y reenvío virtual (VRF) y VRF múltiple: permiten que existan varias instancias de una tabla de enrutamiento simultáneamente en un solo enrutador para que se puedan usar direcciones IP idénticas o superpuestas sin causar conflictos.

- Protocolo de redundancia de enrutador virtual (VRRP): permite a los hosts de una LAN utilizar plataformas de enrutamiento redundantes en la LAN simplemente configurando una única ruta predeterminada en los hosts.

Se admiten las siguientes funciones de reenvío de capa 2:

- Dominio de puente: un conjunto de interfaces lógicas en un conmutador virtual que forman parte del mismo dominio de transmisión.

- Conmutador virtual: un objeto de software que funciona como un conmutador de capa 2 basado en *hardware*. Un conmutador virtual permite que un dispositivo con finales realice las funciones de un conmutador estándar.

- VXLAN: un protocolo de encapsulación de plano de datos que le permite ejecutar VPN Ethernet de capa 2 (EVPN) a través de una red IP de capa 3 utilizando encapsulación VXLAN estándar a través de UDP.

- VLAN, QinQ: una VLAN es una agrupación lógica de dispositivos en el mismo dominio de transmisión. Q-in-Q (encapsulación 802.1Q) es un método que agrega una etiqueta VLAN a las tramas VLAN Ethernet para que los conmutadores sepan a qué VLAN pertenece el tráfico.

- MSTP: el protocolo de árbol de expansión múltiple (MSTP) es un protocolo que crea varios árboles de expansión para cada VLAN en una sola red física, lo que permite que cada VLAN tenga un puente raíz configurado y una estructura que trabaja el reenvío.

- RSTP: *Rapid Spanning Tree Protocol* (RSTP) permite una rápida convergencia del árbol de expansión simplificando los estados de los puertos y cambiando la forma en que los puertos pasan de un estado a otro. RSTP es compatible con versiones anteriores del Protocolo de árbol de expansión (STP).

- ZTP: el aprovisionamiento sin contacto (ZTP) es una forma de configurar y aprovisionar automáticamente los dispositivos de red, lo que elimina la necesidad de que los administradores manejen las tareas de tese manualmente.

7.5.4.2. Funciones del software de seguridad

Las funciones de seguridad se dividen en tres categorías generales: seguridad de capa 4, seguridad de capa 7 y gestión unificada de amenazas (UTM).

Las características de seguridad de la capa 4 incluyen:

- NAT de nivel de operador (CG-NAT): el NAT empleado a gran escala traduce varias direcciones IPv4 privadas a un número limitado de direcciones IPv4 públicas mediante métodos de traducción de direcciones de red y puertos (NAPT). Puede definir direcciones IPv4 privadas en su red y utilizar CG-NAT para administrar la traducción de direcciones a direcciones IPv4 públicas.

- Prevención de denegación de servicio (DoS): protege contra ataques DoS, proporcionando protección tanto de zona como de final. Las capacidades de prevención de DoS pueden reconocer y brindar protección contra

denegaciones de capa 3 y capa 4, técnicas de suplantación de identidad, escaneos y anomalías de paquetes.

- Compatibilidad con IPsec: IPsec es un conjunto de protocolos que utiliza servicios de cifrado para proteger las comunicaciones a través de redes IP. IPsec proporciona integridad, protección de reproducción, confidencialidad, control de acceso y autenticidad.

- Servicios de firewall con estado: habilite la configuración e implementación de servicios de firewall con estado basados en la capa 4. Estos servicios incluyen objetos configurables, como direcciones, zonas y horarios; y políticas de acceso, como coincidencias y acciones.

Las características de seguridad que son aceptados en de la capa 7 incluyen:

- Identificación de la aplicación: identifica automáticamente la aplicación que utiliza el tráfico de red cuando las funciones de red de Capa 7, como el firewall de próxima generación (NGFW), están habilitadas.

- Identificación y filtrado de dispositivos: mecanismos de registro y huellas digitales que hacen que las operaciones de seguridad y de red sean más visibles, incluida la identificación del sistema operativo, el análisis de encabezados de agente de usuario HTTP y el análisis basado en direcciones MAC.

- Equilibrio de carga y proxy de DNS: compatibilidad con el modo de proxy dividido y el modo de proxy transparente. En el modo de proxy dividido, un servidor proxy divide las consultas de DNS según la interfaz y los nombres

de dominio. En el modo de proxy transparente, un servidor proxy DNS transparente, que redirige las solicitudes y respuestas sin modificarlas, se encuentra entre un *host* e Internet. (Un servidor proxy no transparente es aquel que modifica solicitudes y respuestas). Puede utilizar el modo proxy transparente para reenviar las consultas DNS de un cliente a servidores DNS designados o conocidos.

- Cortafuegos de próxima generación (NGFW): identifica aplicaciones y administra y protege los flujos de tráfico de aplicaciones mediante políticas. Las acciones de la política de NGFW incluyen permitir, denegar, restringir el acceso, redireccionar, administración y registro de acceso de aplicaciones basadas en portales cautivos y acciones avanzadas, como secuencias de comandos.

- Filtrado y reputación de URL: examina el tráfico web para determinar si representa un riesgo de seguridad, no cumple con las políticas de la empresa, debe filtrarse para control parental o debe autenticarse o autorizarse más para el acceso u otros fines. Puede utilizar categorías de URL predefinidas y definir clases personalizadas.

- Control a nivel de usuario y de grupo: capacidades de control integradas basadas en el usuario Puede crear y ejecutar servicios específicos para usuarios y grupos, como la orientación de los padres, el cumplimiento del cumplimiento de la empresa, las políticas de acceso y autorización y las políticas diseñadas para usuarios especializados.

Las características de seguridad de la administración unificada de amenazas (UTM) incluyen:

- Antivirus: proporciona detección de virus de varias capas mediante heurística, coincidencia de firmas y emulación.

- Filtrado de archivos: protege contra virus y vulnerabilidades asociados con varios tipos de archivos y atributos de archivos. El filtrado de archivos puede bloquear transferencias de archivos potencialmente riesgosas según los atributos del archivo, como la aplicación del archivo, el tamaño del archivo, el protocolo de transferencia y la ruta del tráfico. El filtrado de archivos admite FTP, HTTP, IMAP, MAPI y SMTP.

- Proxy HTTP y SSL: proporciona seguridad SSL de un extremo a otro al descifrar de forma transparente el tráfico SSL entrante y saliente, inspeccionar el tráfico descifrado en busca de amenazas y volver a cifrar el tráfico a clientes y servidores. El descifrado SSL le permite aplicar políticas coherentes para aplicaciones, seguridad, contenido y cumplimiento. El proxy HTTP y SSL incluye capacidades optimizadas para HTTPS, SMTP, SSH y otros flujos, y le permite administrar claves públicas y privadas con control de acceso basado en roles (RBAC).

- Detección y prevención de movimientos laterales: los motores de dispositivos finales para IPS y antivirus protegen contra las amenazas de movimientos laterales. El motor antivirus detecta binarios de *malware* que utilizan técnicas de movimiento lateral. El motor del sistema de prevención de intrusiones (IPS) inspecciona los paquetes enviados a través de la red para identificar las actividades de *ransomware* y *malware*.

- IPS de próxima generación: proporciona un conjunto sólido de capacidades de detección, prevención, registro y generación de informes,

y sirve como una herramienta para detectar usuarios y aplicaciones que no cumplen las normas.

7.5.4.3. Calidad de servicio

La función de QoS le permite definir y controlar la calidad del servicio para la transmisión de información en tiempo real y de uso de la capacidad del enlace que es propenso a fluctuaciones y latencia, como VoIP, video a pedido y conferencias de voz. QoS proporciona colas, programación y enrutamiento con reconocimiento de aplicaciones según la hora del día, el tipo de enlace (MPLS, Internet y LTE), los requisitos de la aplicación (ancho de banda, latencia, *jitter* y tasa de errores) y el rendimiento del enlace.

El marco de QoS permite:

- Priorizar la transmisión de datos en la red y el funcionamiento de las aplicaciones.

- Proporcione la cantidad adecuada de ancho de banda requerido por diferentes subredes, usuarios o clases en una red.

- Asignar ancho de banda al tráfico interno y externo.

- Aplique QoS para el tráfico de carga y el tráfico de descarga, o ambos.

- Garantizar una latencia menor para el envío de datos en la red que genera ingresos.

- Implemente la creación de perfiles de tráfico de aplicaciones para garantizar el uso del ancho de banda.

- Asocie los requisitos de SLA con determinadas clases de tráfico y luego elija las rutas que cumplan con estas características de SLA.

Puede configurar QoS asignando perfiles y políticas de QoS a interfaces de red, para optimizar y priorizar el flujo de tráfico de red en las interfaces, configurar el uso de la capacidad asignada a la interfaz y reescribir campos en los distintos paquetes. Con la configuración de QoS, puede controlar el flujo de datos en diferentes puntos a través de todo el camino que recorre el tráfico.

7.5.4.4. Control de SLA y dirección del tráfico

La solución SD-WAN ayuda a los proveedores de servicios a cumplir sus acuerdos de nivel de servicio (SLA) con sus clientes al monitorear y medir continuamente el desempeño de la red WAN y al tomar decisiones de enrutamiento inteligente basadas en estos datos de desempeño.

Para las implementaciones empresariales, la supervisión de SLA y SD-WAN ayudan a garantizar la continuidad empresarial resistente al brindar servicios de manera confiable y con calidad, creando una infraestructura automatizada que se ajusta dinámicamente según sea necesario.

Puede medir y actuar según los siguientes criterios de SLA: *Jitter*, latencia, pérdida de paquetes, MOS y porcentaje de utilización del enlace.

Para habilitar la supervisión de SLA, defina perfiles de SLA, perfiles de reenvío y políticas de reenvío basadas en aplicaciones. Los perfiles de SLA definen los criterios de la red a monitorear y los valores de umbral para cada uno.

Los perfiles de reenvío definen lo que debe suceder cuando se producen infracciones de SLA, que incluyen:

- Si el tráfico debe reenviarse, descartarse o estrangularse.

- Qué circuitos tienen prioridad cuando no hay una violación de SLA en el circuito. El tráfico fluye por el circuito de mayor prioridad hasta que se produce una infracción de SLA, momento en el que cambia a un circuito de menor prioridad que no infringe un SLA.

- Cuando el flujo de tráfico normal puede regresar después de que se resuelva una infracción de SLA.

Se pueden utilizar las configuraciones de políticas de SLA para hacer coincidir los tipos datos que se transmiten en las aplicaciones con la tabla de reenvío que debe usarse para ese tipo de tráfico de aplicaciones. En las políticas, también puede configurar las direcciones IP para que sean monitoreadas y una acción a tomar si las direcciones IP son inalcanzables.

El funcionamiento de las políticas es si la métrica de latencia de enlace o la métrica de fluctuación máxima viola el SLA al exceder los límites configurados, el tráfico de la aplicación se cambia de la interfaz principal a la secundaria. Cuando se resuelve la infracción del SLA, el tráfico de la aplicación vuelve a la interfaz principal.

8. PROPUESTA DE ÍNDICE DE CONTENIDOS

5. METODOLOGÍA

6. TÉCNICAS DE ANÁLISIS

CONCLUSIONES

REFERENCIAS

APÉNDICES

ANEXOS

9. METODOLOGÍA

9.1. Diseño de la Investigación

Es una investigación no experimental porque se estudiarán las plantillas para luego validar la percepción de las áreas sobre las mejoras de las mismas, siendo revisión documental necesaria para proponer cambios en las configuraciones realizadas, con la propuesta de cambio se realizará un diseño de plantilla que será brindada para los cambios sobre las variables donde se encontró mejora en la revisión documental.

Se clasificó como no experimental porque no se construye ninguna situación, sino que se observan situaciones, en este caso configuraciones ya existentes y sobre esas se realiza el tema de investigación.

Como indica Hernández, Fernández y Baptista (2014):

> La investigación no experimental es aquella que se realiza sin manipular deliberadamente variables. Es decir, es investigación donde no hacemos variar intencionalmente las variables independientes. Lo que hacemos en la investigación no experimental es observar fenómenos tal y como se dan en su contexto natural, para después analizarlos. (p. 125)

Las variables independientes en este caso se determinaron los servicios a configurar ya no pueden ser manipuladas las existentes ya que no se tiene control sobre lo ya aprovisionado, sino que trabajaremos sobre las mismas y se le

agregarán características para complementar el alcance y finalizar la definición de la homologación.

Al ser una investigación no experimental se estará trabajando con un diseño transversal.

Según García, López, Jiménez, Ramírez, Lino y Reding (2014):

> El diseño de estudios transversales se define como el diseño de una investigación observacional, individual, que mide una o más características o enfermedades (variables), en un momento dado. La información de un estudio transversal se recolecta en el presente y, en ocasiones, a partir de características pasadas o de conductas o experiencias de los individuos. (p. 133)

Como se indicó se estará trabajando con la recolección de información sobre servicios existentes y sobre esos realizar mejoras y agregar los servicios de valor agregados; adicional se estará basando sobre la experiencia de las áreas involucradas en las entregas: preventa implementaciones y soporte; para ver la mejora en la percepción de configuración y diseño de nuevas topologías de solución.

Este estudio también va a tener una característica descriptiva como indica Veiga, Fuente y Zimmermann Verdejo (2008):

> En los estudios descriptivos, el investigador se limita a medir la presencia, características o distribución de un fenómeno en una población en un momento de corte en el tiempo, tal sería el caso de estudios que describen la presencia de un determinado factor ambiental, una determinada

> enfermedad, mortalidad en la población, entre otros. Pero siempre referido a un momento concreto y sobre todo, limitándose a describir uno o varios fenómenos sin intención de establecer relaciones causales con otros factores. (p. 82)

Como se puede ver en este caso se estará haciendo análisis de las configuraciones para establecer el catálogo, pero ninguna configuración estará relacionada una con la otra para poder existir.

9.2. Paradigma de la investigación

El enfoque de esta investigación es sobre el paradigma del pospositivismo conociendo que, ya que, aunque se considera una investigación de carácter cuantitativo ya que por medio de diferentes indicadores se podrá medir la eficiencia y la eficacia de las configuraciones realizadas también tendrá características cualitativas, pero más orientadas al positivismo que al constructivismo en la que se da mayor importancia a un ámbito social.

Para Miller (2007):

> Describe los componentes básicos de una teoría postpositivista como compuesta de unidades básicas o ideas y temas de interés, (leyes de interacciones) entre las unidades y una descripción de los límites para la teoría. Una teoría postpositivista también incluye indicadores empíricos para conectar la teoría con fenómenos observables, e hipótesis que se pueden probar usando el método científico. (p. 84)

Las características cualitativas a analizar irán amarradas a los indicadores de calidad para mostrar un nivel de satisfacción sobre los servicios brindados

tanto para cliente interno como para cliente externo. Se tomará la experiencia de las áreas involucradas para determinar si la plantilla elaborada cuenta con las características requeridas tanto por cliente interno como por cliente externo.

9.3. Enfoque de la Investigación

> El enfoque de la investigación es mixto revisando tanto características cuantitativas como cualitativas. En las últimas décadas, numerosos investigadores han apuntado a un método mixto, que integra ambos enfoques, argumentando que al probar una teoría a través de dos métodos pueden obtenerse resultados más confiables. Este enfoque aún es polémico, pero su desarrollo ha sido importante en los últimos años. (Hernández, Fernández y Baptista, 2014, p. 112)

Se eligió de esta manera debido a que se cuantificarán los elementos que componen la plantilla de configuración, direcciones IP asignadas, túneles configurados, QoS, políticas de seguridad, entre otros.

Viendo la optimización en cuanto al aprovisionamiento y la mejora del rendimiento de los enlaces. La información será obtenida de las plantillas que se han generado con diferentes configuraciones realizadas. En cuanto a la parte cualitativa se tomará en cuenta también características en cuanto la experiencia del área de preventa, implementación y soporte sobre las plantillas utilizadas y cómo los cambios brindarán una mejor perspectiva tanto al cliente interno como externo. Para esto se realizarán encuesta a las personas de dichas áreas.

9.4. Población de estudio

El estudio se llevará a cabo para la región centroamericana que constituye los países de Guatemala, Honduras, El Salvador, Nicaragua, Costa Rica y Panamá en donde se tiene existencia de una red MPLS que interconecta todos los países de la región con diferentes tecnologías de transmisión siendo estas: por medio de fibra o Wireless (excluyendo servicios de móviles: 3G y LTE). La población también abarca las operaciones de estos países de un mismo Proveedor de Servicio y no redes entregadas por terceros.

9.5. Tipo de muestreo

El tipo de muestreo a trabajar es un muestreo no probabilístico utilizando un muestreo por conveniencia porque, aunque la población es el área centroamericana, la muestra a trabajar será únicamente sobre la operación de Guatemala (operación local) en donde se puede tener la revisión de documentación, los indicadores históricos tanto de calidad de configuración como de satisfacción de cliente para poder crear la comparativa y las mejoras necesarias para la elaboración de la plantilla homologada.

Según Cottrell (2014), “en un muestreo no probabilístico, los individuos se seleccionan en base a criterios no aleatorios, y no todos los individuos tienen la posibilidad de ser incluidos” (p. 83).

Este tipo de muestra es más fácil y barata de acceder, pero tiene un mayor riesgo de sesgo de muestreo. Esto significa que las inferencias que puede hacer sobre la población son más débiles que con las muestras probabilísticas, y sus conclusiones pueden ser más limitadas. Si se utiliza

> una muestra no probabilística, hay que intentar que sea lo más representativa posible de la población. (Bastis Consultores, 2021, párr. 41)

9.6. Tamaño de la muestra

Se trabajarán con dos muestras, la primera es la cantidad de plantillas a analizar para realizar la revisión documental se revisará la totalidad de configuraciones realizadas en las configuraciones de clientes ya existentes. La segunda muestra es la cantidad de personas a entrevistar para conocer el nivel de satisfacción y la facilidad de implementación que se tiene; trabajando con una población de 15 personas y manejando un nivel de confianza de 99 % y un margen de error de 10 % la muestra será la totalidad de la población.

10. TÉCNICAS DE ANÁLISIS DE LA INFORMACIÓN

Para la recolección de documentación se utilizará la revisión de documentos para el análisis de los indicadores que se trabaja actualmente y la mejora por medio de la experimentación y el ajuste de los parámetros.

La técnica de investigación a trabajar para la segunda muestra será encuestas que serán realizadas en línea por medio de un formulario en el que se podrá ver la satisfacción sobre los siguientes temas: facilidad de implementación, facilidad de gestión de cambios, facilidad de soporte y satisfacción del cliente. Los temas serán divididos por tres preguntas por tema a tratar teniendo un total de 20 preguntas por cada encuesta.

10.1. Instrumentos de recolección de datos

Teniendo que como técnica de Investigación será encuestas para el caso cualitativo y la recolección de información para la parte cuantitativa los instrumentos para la recolección de datos será por medio de una encuesta en línea como se explicó anteriormente y para la parte de observación serán las 18 plantillas que se tienen como muestra, el análisis de sus configuraciones, su tiempo de entrega e indicadores históricos que se tienen en la parte de analítica de la plataforma SD-WAN.

10.2. Técnicas de análisis de datos

Para la parte de información cualitativa que sería sobre la experiencia con el servicio tanto de cliente interno como de cliente externo se tendrá un proceso

de análisis de datos cualitativos se compone de distintas fases. Las fases principales incluyen:

- El descubrimiento y la obtención de los datos por medio de las encuestas.

- La preparación, revisión y transcripción de los datos, en su caso, a texto. Esto sería automático al hacer un cuestionario en línea se trabajará con un archivo Excel para poder trabajar la información.

- La organización de los datos según criterios, esto se encontrará dentro de los cinco temas principales que se plantearon y clasificando por el nivel de satisfacción en cada uno de los procesos.

- La categorización, etiquetado y codificación de los datos, que los prepara para el análisis.

- El análisis de los datos y generación de propuestas de mejoras en la plantilla homologada para que se cuente con el criterio de calidad total.

La información cuantitativa que se analizará será por medio de una media aritmética para ver el promedio del comportamiento de las configuraciones realizadas en cuanto a las medidas de por ejemplo los match de las políticas de seguridad, QoS y SLA aplicados en la configuración para validar que esto sí cubra las necesidades de las diferentes topologías en una única plantilla para servicios.

A partir de tener el promedio de la información recolectada para ver la tendencia de las configuraciones se trabajará con una prueba de hipótesis para realizar los cambios sobre la información que se obtuvo para verificar que las

configuraciones propuestas si cumplan con las necesidades de los clientes corporativos que contraten los servicios.

11. CRONOGRAMA

El presente capítulo presenta la organización cronológica del proceso de solución, organizado por semanas, abarcando una duración total de 21 semanas, desde la fase 1 que es la recolección de datos hasta la fase 6 que es la elaboración del plan de capacitación.

Tabla I. **Cronograma**

No.	Actividades	Enero				Febrero				Marzo				Abril					Mayo				Junio			
	Semanas	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
1	Recopilación de información																									
2	Análisis de Configuraciones																									
2	Elaboración de catálogo de Servicios																									
3	Diseño de plantilla General																									
4	Diseño de plantilla de configuraciones atipicas y de valor agregado																									
5	Consolidación de plantilla Homologada																									
6	Prueba de plantilla Homologada																									
7	Mejoras y cambios de plantilla Homologada																									
8	Documentación: Ingeniería, ATP, Support Kit y Welcome Kit																									
9	Elaboración de plan de capacitación y manuales																									

Fuente: elaboración propia, empleando Microsoft Excel.

12. FACTIBILIDAD DEL ESTUDIO

Para la elaboración de la investigación se deberá de contar con los siguientes recursos: topología SD-WAN desplegada con acceso al director y al menos a dos equipos físicos (configurando uno como *HUB* y otro como *branch*).

Para realizar el diseño de la plantilla se utilizará un espacio de pruebas de una solución SD-WAN de un proveedor de servicio que se encuentra desplegada en Centroamérica, pero los equipos físicos a probar serán aprovisionados en Guatemala ya que se utilizarán los equipos de laboratorio de un proveedor de servicio que se encuentra en Guatemala. No se tendrá que tener un gasto adicional ya que al ser un espacio de prueba POC no se tiene cobro por el uso de licencias para el aprovisionamiento de los equipos y el enlace MPLS que se utilizara es con el que se cuenta en el laboratorio.

En estos precios se incluye OPEX y CAPEX teniendo estos la siguiente división:

- CAPEX: equipos, licencias, inversión plataforma de monitoreo e inversión de medio de última milla.

- OPEX: mantenimiento por un año.

Para la documentación a revisar se trabajará con la información que se tiene en el director SD-WAN que se encuentra en producción del mismo proveedor, así como la información de la analítica que se tenga. La muestra de la población a encuestar serán las personas del área de implementaciones, primera y segunda

línea de soporte del proveedor de servicios que se encuentra ubicado en Guatemala.

Los costos aproximados de los servicios que se utilizarán son:

Tabla II. **Costos factibilidad**

Item	Tamaño	Equipo	Licencia	Cantidad	Precio	Precio por mega
Servicio *branch*	*Small*	Lanner-FW-7551sec-V120	Mic Custom 25Mbps – 101 200 *branches*	1	$380.00	$20.00
Servicio *HUB*	Extra *large*	Lanner-NCA-5510A-V100	Mic custom 200Mbps 101 200 *branches*	1	$1500.00	$15.00
		Total			$ 1880.00	$ 35.00

Fuente: elaboración propia, empleando Microsoft Excel.

13. REFERENCIAS

1. Bastis Consultores. (3 de mayo, 2021). Muestreo probabilístico y no probabilístico. [Mensaje de blog]. Recuperado de https://online-tesis.com/muestreo-probabilistico-no-probabilistico/#:~:text=M%C3%A9todos%20de%20muestreo%20no%20probabil%C3%ADstico&text=Este%20tipo%20de%20muestra%20es,conclusiones%20pueden%20ser%20m%C3%A1s%20limitadas.

2. Cottrell, S. (2014). *Dissertations and Project Reports: A Step-by-Step Guide*. Basingstoke, Inglaterra: Palgrave Macmillan.

3. Delgado, G. y Rubiano, A. (2018). *Renovación Tecnológica Sd-Wan Cliente Corporativo* (Tesis de licenciatura). Universidad de Santo Tomas, Colombia.

4. Figueiras, A. (2002). *Una panorámica de las telecomunicaciones.* Madrid, España: Pearson Education S.A.

5. García, J., López, J., Jiménez, P., Ramírez, Y., Lino, L. y Reding, A. (2014). *Metodología de la investigación bioestadística y bioinformática en ciencias médicas y de la salud.* España: McGraw Hill.

6. Hernández, R., Fernández, C. y Baptista, P. (2014). *Metodología de la investigación.* México: McGrwall Hill.

7. Huawei. (9 de septiembre, 2021). MPLS TE. [Mensaje de blog]. Recuperado de https://support.huawei.com/enterprise/en/doc/EDOC1000178173/622a51a3/mpls-te.

8. Huawei. (13 de septiembre, 2021). HVPN. [Mensaje de blog]. Recuperado de https://support.huawei.com/enterprise/es/doc/EDOC1000178179/b295b528/hvpn.

9. Huawei. (8 de septiembre, 2021). Basic MPLS Architecture. [Mensaje de blog]. Recuperado de https://support.huawei.com/enterprise/en/doc/EDOC1000178173/7c5ca4fb/basic-mpls-architecture.

10. Huawei. (8 de septiembre, 2021). MPLS VPN. [Mensaje de blog]. Recuperado de: https://support.huawei.com/enterprise/en/doc/EDOC1000178173/2edd846/mpls-vpn.

11. Intriago, W. (2017) *Estudio del protocolo Openflow usando el modelo de red definida por Software (Software Define Networks)* (Tesis de maestría). Pontificia Universidad Católica del Ecuador, Ecuador.

12. López, J. (2020). *Emulación de una red SD-WAN (Software-Defined Wide Area Network) utilizando tecnología Fortinet y el software GNS3* (Tesis de licenciatura). Escuela Politécnica Nacional de Quito, Ecuador.

13. Miller, K. (2007). *Teorías de la comunicación: Perspectivas, procesos y contextos*. Beijing, China: Universidad de Pekín.

14. Nazareno, S. (2019). *Diseño e implementación de un prototipo SD-WAN basado en RASPBERRY PI* (Tesis de licenciatura). Universidad de Guayaquil, Ecuador.

15. Network Academy. (14 de septiembre, 2021). Componentes de una solución SD-WAN. [Mensaje en un blog]. Recuperado de https://www.networkacademy.io/ccie-enterprise/sdwan/what-is-sd-wan.

16. Tech Club. (22 de mayo, 2019). Red MPLS. [Mensaje de blog]. Recuperado de https://techclub.tajamar.es/red-mpls/.

17. Veiga, J., Fuente, E. y Zimmermann, M. (marzo, 2008). Modelos de estudios en investigación aplicada: conceptos y criterios para el diseño. *Medicina y Seguridad del Trabajo, 54*(2010), 81-88*.*

18. Versa Network (10 de septiembre, 2021). Arquitectura de red Full Mesh. [Mensaje en un blog]. Recuperado de https://docs.versa-networks.com/Getting_Started/Versa_Product_Solution/04_Solution_Architecture.

19. Versa Network. (10 de septiembre, 2021). Arquitectura de red Hub-and-Spoke. [Mensaje en un blog]. Recuperado de https://docs.versa-networks.com/Getting_Started/Versa_Product_Solution/04_Solution_Architecture.

20. Versa Networks. (13 de septiembre, 2021). Arquitectura de una solución SD-WAN. [Mensaje de blog]. Recuperado de https://docs.versa-networks.com/Reference/Architecture/02_SD-WAN_Solution_Architecture.