UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

DISEÑO DE INVESTIGACIÓN DE UNA PROPUESTA DE IMPLEMENTACIÓN DE RED INDUSTRIAL A NIVEL DE ACCESO, CON TECNOLOGÍA SDN A LA INFRAESTRUCTURA DE RED DE UNA PLANTA DE PRODUCCIÓN DE ALIMENTOS UBICADA EN LA ANTIGUA GUATEMALA

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA

FACULTAD DE INGENIERIA

POR

JOSÉ PABLO MARROQUÍN VILLATORO

ASESORADO POR EL MAESTRO ING. CRISTIAN OBDULIO JOVEL DE LEÓN

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO ELECTRÓNICO

GUATEMALA, ABRIL DE 2022

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANA	Inga. Aurelia Anabela Córdova 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 Cruz Lorente
VOCAL V	Br. Fernando José Paz González
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Pedro Antonio Aguilar Polanco
EXAMINADOR	Ing. Walter Giovanni Alvarez Marroquín
EXAMINADOR	Ing. Guillermo Antonio Puente Romero
EXAMINADOR	Ing. Julio Rolando Barrios Archila
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 PROPUESTA DE IMPLEMENTACIÓN DE RED INDUSTRIAL A NIVEL DE ACCESO, CON TECNOLOGÍA SDN A LA INFRAESTRUCTURA DE RED DE UNA PLANTA DE PRODUCCIÓN DE ALIMENTOS UBICADA EN LA ANTIGUA GUATEMALA

Tema que me fuera asignado por la Dirección de la Escuela de Estudios de Postgrado, con fecha 30 de octubre de 2021.

José Pablo Marroquín Villatoro

ESCUELA DE ESTUDIOS DE POSTGRADO
FACULTAD DE INGENIERÍA

EEPFI-PP-0183-2022
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 PROPUESTA DE IMPLEMENTACIÓN DE RED INDUSTRIAL A NIVEL DE ACCESO CON TECNOLOGÍA SDN A LA INFRAESTRUCTURA DE RED DE UNA PLANTA DE PRODUCCIÓN DE ALIMENTOS UBICADA EN LA ANTIGUA GUATEMALA**, el cual se enmarca en la línea de investigación: **Infraestructura de red - Infraestructura de red**, presentado por el estudiante **José Pablo Marroquín Villatoro** carné número **9712155**, 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"

Mtro. Cristian Obdulio Jovel De León
Asesor(a)

Cristian Obdulio Jovel de León
INGENIERO EN SISTEMAS DE INFORMACIÓN Y CIENCIAS DE LA COMPUTACIÓN
COLEGIADO No. 14,631

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

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

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

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

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÍA

EEP-EIME-0183-2022

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 PROPUESTA DE IMPLEMENTACIÓN DE RED INDUSTRIAL A NIVEL DE ACCESO CON TECNOLOGÍA SDN A LA INFRAESTRUCTURA DE RED DE UNA PLANTA DE PRODUCCIÓN DE ALIMENTOS UBICADA EN LA ANTIGUA GUATEMALA**, presentado por el estudiante universitario **José Pablo Marroquín Villatoro**, 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.309.2022

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 PROPUESTA DE IMPLEMENTACIÓN DE RED INDUSTRIAL A NIVEL DE ACCESO, CON TECNOLOGÍA SDN A LA INFRAESTRUCTURA DE RED DE UNA PLANTA DE PRODUCCIÓN DE ALIMENTOS UBICADA EN LA ANTIGUA GUATEMALA,** presentado por: **José Pablo Marroquín Villatoro,** 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	Fuente de vida y sabiduría.
Mis padres	César Augusto Marroquín Figueroa y Lilian Gracelene Villatoro Morales, por su apoyo incondicional en todo momento.
Mi novia	Sucely Avidail Chacón Arana, por creer en mí.
Mis hermanos	Brenda, Cesar y Daniel Marroquín; Mildred Tol, Evelin Chacón, e Israel Abaj; porque al final si se pudo.
Mis sobrinos	Pamela y Augusto Hernández, Flavio Tol, Cristian Abaj; porque ustedes vienen detrás y también lo lograrán.

AGRADECIMIENTOS A:

Universidad San Carlos de Guatemala	Por ser mi alma mater.
Facultad de Ingeniería	Porque en ella fomenté mi formación académica.
Mi asesor	Maestro Ing. Cristian Obdulio Jovel De León, por su amistad y colaboración en este trabajo.
Compañeros	Por su apoyo y solidaridad.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

LISTA DE SÍMBOLOS

Símbolo	Significado
Δ	Delta
f	frecuencia
GHz	Giga Hertz
Hz	Hertz
=	Igualdad
n	Índice de difracción
m	Índice de modulación
MHz	Mega Hertz
Ω	Ohm
1G	Primera generación de redes móviles

GLOSARIO

Acceso	Enlace entre un abonado y la red de telecomunicación.
Abonado	Usuario suscrito a un servicio de telecomunicación.
Ancho de banda	Rango de frecuencias en el espectro de difusión que se encuentra ocupada por una señal.
API	*Aplication Program Interface*. Conjunto de rutinas o funciones que constituyen un interfaz o forma de diálogo entre las aplicaciones de los usuarios y el sistema operativo.
Autentificación	Mecanismos del sistema de información para poder identificar a los usuarios que acceden a sus recursos, y asegurar la integridad y autenticidad de los datos.
Canal	Ruta de transmisión de comunicaciones a través de cualquier clase de medio de transmisión: cable conductor, radio, fibra óptica o de cualquier otro tipo.
CDMA	Solución técnica que permite reutilizar el mismo canal de transmisión (la misma frecuencia), al mismo tiempo y por más de un usuario.

Cifrado	Técnicas utilizadas para hacer inaccesible la información a personas no autorizadas. Se suele basar en una clave, sin la cual la información no puede ser descifrada.
Cloud	Significa, literalmente, nube. En términos informáticos, se refiere a un paradigma que permite ofrecer servicios de computación a través de una red; que normalmente es Internet. El concepto de nube se refiere al almacenamiento de datos fuera de nuestros dispositivos.
Conmutación	Conjunto de operaciones necesarias para unir entre sí los circuitos, con el fin de establecer una comunicación temporal entre dos o más estaciones o puestos.
Fibra óptica	Método para transmisión de información (sonido, vídeo, datos), en el cual la luz es modulada y transmitida a través de filamentos muy delgados de vidrio de alta pureza.
Firewall	Un firewall, también llamado cortafuegos, es un sistema cuya función es prevenir y proteger a nuestra red privada de intrusiones o ataques de otras redes, bloqueándole el acceso.

Gigahercio	Unidad de frecuencia equivalente a un millón de millones de hercios (un millón de millones de ciclos por segundo).
Hub and Spoke	Es un modelo de red para administrar de manera eficiente las comunicaciones o los requisitos de seguridad comunes.
ISP	Empresa encargada de ofrecer la infraestructura de acceso para que los clientes puedan conectarse a Internet utilizando los medios de acceso estándar (módem, RTC, RDSI y ADSL).
LAN	Red de área local (*Local Area Network*)
NFV	La virtualización de las funciones de red (NFV) es un enfoque de red en evolución que permite la sustitución de dispositivos de hardware dedicados y costosos, tales como routers, firewalls y equilibradores de carga con dispositivos de red, basados en software que se ejecutan como máquinas virtuales en servidores estándares de la industria.
Nodo	Es el elemento de red, ya sea de acceso o de conmutación, que permite recibir y enrutar las comunicaciones.
Protocolo	Conjunto de reglas que gobiernan las comunicaciones entre sistemas de telecomunicación.

Rack	Es un término inglés que se emplea para nombrar a la estructura que permite sostener o albergar un dispositivo tecnológico.
SAP	Es un Sistema de Gestión Empresarial (ERP) que brinda las mejores prácticas de mercado a empresas de diferentes segmentos, con la intención de mejorar la eficiencia, control y gestión de la información y los datos de las empresas.
SDN	Son un conjunto de técnicas relacionadas con el área de redes computacionales, cuyo objetivo es facilitar la implementación e implantación de servicios de red de una manera determinista, dinámica y escalable, evitando al administrador de red gestionar dichos servicios a bajo nivel.
SERVER	Un servidor es un equipo diseñado para procesar solicitudes y entregar datos a otros ordenadores a los que podríamos llamar clientes.
TCP/IP	*Transport Control Protocol / Internet Protocol.* Protocolo estándar desarrollado por la agencia de investigación de la defensa de USA como base para la red ARPANET (1983) y que es el utilizado por defecto en sistemas operativos abiertos y en la red Internet. Se utiliza para el intercambio de información entre ordenadores conectados a una red.

VPN	Es una herramienta digital que redirige el tráfico de internet a través de un túnel seguro, ocultando la dirección IP y encriptando los datos.

RESUMEN

El objetivo del documento es presentar el diseño de investigación de una propuesta de implementación de red industrial a nivel de acceso, con tecnología SDN a la infraestructura de red de una planta de producción de alimentos ubicada en la Antigua Guatemala. La investigación se enfoca en el estudio de la infraestructura de red ethernet interna de una planta de producción, el diseño de una topología que permita el fácil acceso a los recursos e información contenida en la base de datos SAP; unidad que alberga todos los movimientos de la empresa.

Analizar aspectos que interfieran en los procesos y que retarden los movimientos comerciales. Que los colaboradores puedan tener acceso a la carga de nóminas directamente a SAP, las sucursales tengan conectividad directa a la base de datos sin comprender qué tipo de infraestructura que atraviesen los datos a través del ISP que brinde el servicio de internet; igualmente que la telemetría se configure directamente a SAP. Entre los beneficios más importantes que otorga este aporte es el de reducir los tiempos de gestión y administración de la red, centralizando el punto de control por medio de un software.

La metodología que se utilizó para la investigación consiste en cuatro fases: análisis de situación actual de la red; diagnosticar y clasificar los equipos que soportan la actualización de la red; diseñar una topología de red SDN que alcance los objetivos de la empresa; y apoyo a los colaboradores para migrar al nuevo diseño de red.

De la fase inicial se establecieron delimitaciones del proyecto, se revisaron los documentos del panorama actual que ayudaron a establecer los antecedentes y marco teórico.

En la segunda fase se definieron los equipos que satisfacen el nivel tecnológico para la implementación de la red SDN, se clasificó y analizó toda la red para determinar si la infraestructura existente satisface las necesidades. Programar reuniones con el personal a cargo para verificar el listado de las posibles pautas a implementar y analizar el alcance de cada una de ellas.

En la tercera fase se desarrolló la propuesta de red SDN, se determinaron las configuraciones, costos económicos y tecnológicos, se diseñó la propuesta de red SDN, tomando en cuenta los recursos *open source* disponibles y las variantes comerciales disponibles que satisfagan el éxito de la implementación.

La última fase se centra en la capacitación de los colaboradores que tendrán acceso a la red, diagnosticar el funcionamiento y monitorizar la red para garantizar su desempeño y minimizar los problemas de la migración.

1. INTRODUCCIÓN

Este trabajo de investigación es una innovación para el diseño de una propuesta de implementación de tecnología SDN a la infraestructura de red en una planta de producción de alimentos.

Las empresas se clasifican según el ámbito de actividad. Nos enfocaremos en las compañías que se dedican a la fabricación de productos alimenticios. Como el propósito de la empresa es la producción de alimentos, la preocupación por la infraestructura de red no es su mayor prioridad, pero si es importante por el movimiento comercial del producto.

La facturación es el centro de la actividad comercial, porque parten de ese punto para analizar el estatus de cada una de las áreas que se interconectan; como bodega de producto terminado, producción, bodega de materias primas, bodega y la propia área de facturación en gerencia. Pero, cuando se habla de una red IP que interconecta cada una de estas áreas podemos mencionar recursos humanos, las distintas gerencias, ventas y una aplicación de servicio móvil de Tigo, el departamento de IT (lugar donde se realizan las configuraciones), inclusive garitas de acceso, combustible, área de video vigilancia y todo eso para enlistar únicamente la planta de producción.

La planta posee su propio centro de datos con *multihoming* a dos centros que le brindan servicio de conexión a internet. El servidor, firewall, PBX (central análoga/digital), *router* y switches son administrados localmente en el centro de datos. Posee vlans, configuraciones de ruteo y listas de control de acceso

básicas para la seguridad interna de la red. La empresa se encuentra en una etapa de migración de un sistema basado en COBOL a SAP BO, el software ERP gestiona la Data Base (DB) donde se encuentra toda la información importante para los movimientos de la empresa, ubicada en un servidor físico DELL. Dentro de la empresa aún se gestionan algunos procesos de manera manual (con la ayuda de ofimática).

La empresa ha expandido sus operaciones tanto a nivel nacional como a nivel centroamericano, tiene sucursales en el área de San Marcos, Peten, Zacapa y en los países centroamericanos, a excepción de Panamá (en desarrollo). La infraestructura de red en estas sucursales es de capa 2, con servicio a internet sin redundancia. Existen operaciones donde aún se utiliza el sistema cardex para el control de movimiento y archivos físicos para el de procesos.

Automatizar la red, consiste en utilizar una lógica programable para administrar y gestionar los recursos con los que cuenta y los servicios que pudiera proporcionar. Consiste en configurar, integrar y proteger los dispositivos involucrados en el procesamiento de datos dentro de la infraestructura de la red IP de una manera más eficiente, evitando malas configuraciones e incongruencias al hacerlas de manera manual.

La tecnología *Sd-Access* está diseñada para ser implementada en esta evolución, es una solución desarrollada para la gestión automatizada del acceso de los usuarios a los servicios de la red y recursos en la nube, permitiendo a los usuarios acceder desde cualquier punto de la red directamente a la información. Construyendo una red híbrida permite a las sucursales tener acceso a la data generada por el ERP SAP BO, ubicado en un servidor en la nube. Utilizando una API de gestión como DNA center de marca, se puede realizar la gestión desde un punto central (el departamento de IT ubicado en la planta en este caso).

El aporte del presente trabajo de investigación consiste en desarrollar una propuesta que contenga un análisis de viabilidad para la implementación de la tecnología SD-Access, con el fin de minimizar actividades innecesarias que consuman recursos y reducir las probabilidades de daños al momento de acontecer un evento de fallo.

En el capítulo I se presentará el marco teórico. Se hará la descripción de conceptos involucrados en la propuesta de implementación tecnológica; los conceptos de virtualización dentro de una red híbrida, la automatización de una red IP a través de una tecnología SD-Access en proceso de evolución, interfaces gráficas que facilitan la gestión y administración de una red, datos importantes a considerar cuando se adquiere dispositivos con la capacidad de ser administrables por medio de la tecnología, comparativas de costo beneficio.

En el capítulo II se presentarán los resultados obtenidos por medio del trabajo de investigación. Se presentarán los resultados del análisis de operación actual de la planta que evidencien la factibilidad de implementación de la propuesta, y que permitan mejoras en los procesos administrativos e incrementos costo/beneficio de los procesos comerciales.

En el capítulo III se discutirán los resultados, se hará mención si la investigación amerita otros temas de investigación y si los datos se pueden generalizar a otros ambientes.

2. ANTECEDENTES

Edgeworth, B., Garza, R., Hucaby, D., & Gooley, J. (2020), en su libro de guía para la certificación CCNP y CCIE, redacta las características e inconvenientes que produce la gestión y mantenimiento de una red IP tradicional, así como la exposición a los errores cuando existe un entorno en constantes cambios manuales en la red o el índice de crecimiento aumenta, provocando inconsistencias en las políticas. Convirtiendo la red tradicional IP a un entorno de red híbrida, con el apoyo de SDN se puede construir una red evolucionada que aborde las necesidades de las redes de campo existentes al aprovechar las funcionalidades de automatización, seguridad, virtualización, movilidad y segmentación. El aporte de la investigación es brindar los conocimientos que se necesitan para el diseño de una red que satisfaga las necesidades mezclando diferentes tipos de topologías (redes híbridas) y cómo se pueden implementar redes virtuales a través de la red de una empresa de servicios ISP. La metodología utilizada es cualitativa transversal, debido a que es una investigación basada en el análisis de datos muestreados dentro del depto. IT en un periodo de tiempo definido. Con los resultados obtenidos de la investigación se podrá analizar la relación costo beneficio que respalden la viabilidad de la implementación.

Ariganello, E. & Sevilla, E.B. (2010) describen en su libro *Redes cisco ccnp a fondo guía de estudio para profesionales* que las funcionalidades y configuraciones de la virtualización de rutas VPN entre las distintas sucursales (site-to-site como lo describe el libro, capítulos 27 y 30) y los límites establecidos por los ISPs, características de la plataforma de gestión para automatización por una marca propietaria. Características y configuraciones necesarias en los

equipos dentro de la localidad del cliente para su conexión a un ISP (con redundancia si existiera), que brinde la conexión a internet y comunicación virtual entre un punto distante a la planta donde se encuentra el centro de datos. El aporte de la investigación es el auxilio al diseño y configuraciones necesarias dentro de los equipos en las sucursales que permitan la migración a una red más evolutiva y que permitan su conectividad. La metodología utilizada es cualitativa transversal, debido a que se hará un análisis de funcionalidades que a su vez proporcionaran datos que corroboren las acciones deseadas y la validez de las características físicas de los equipos instalados para su adecuación dentro del plan evolutivo a una red híbrida. Se busca reutilizar los equipos para una disminución de costos en las sucursales.

Cisco, (2020), en su libro *Guía de configuración de Multipunto dinámico VPN, Cisco IOS 15M&T*, describe como verificar si las características de la versión del IOS permite las configuraciones para implementar los enlaces virtuales de una red VPN. Dentro del contenido del documento se encuentran los comandos básicos para implementar una conexión punto a multipunto entre una central a varias sucursales de la empresa y que estas detecten conectividad directa y desconozcan toda la infraestructura que atraviesan inclusive al ISP que los transporta. Información necesaria para determinar si los equipos actuales satisfacen las características técnicas que se necesitan; puedan ser reutilizables para validar la adquisición de nuevos equipos o reconfigurar los existentes y de esta manera ser contemplado dentro del diseño de la propuesta. El aporte de la investigación es proporcionar un resume básico de las líneas de comando y consideraciones técnicas para los dispositivos de red y estimaciones de costos para una posible implementación. La metodología utilizada es cualitativa transversal; se harán pruebas en un entorno de laboratorio paralelo al sistema de producción, para obtener datos importantes a través de observación y análisis para la pronta emigración de red definida por software.

Por aparte, Gooley, J., & Hasan, R., & Vemula, S. (2020), en su libro *Acceso definido por software y seguridad empresarial de CISCO,* redacta una amplia descripción de la tecnología SD-Access de una marca propietaria, pero aplica a otras marcas de desarrollo en el mercado tecnológico. Dentro del contenido del documento se puede hallar la importancia de la implementación en un entorno de producción, características de la tecnología, funcionalidades específicas de la tecnología, aspectos de gestión y mantenimiento, seguridad de gestión de acceso. Información necesaria para el diseño de la implementación y consideraciones técnicas a validar dentro del plan de la propuesta. El aporte de la investigación es proporcionar un respaldo físico al diseño del desarrollo de la propuesta, para la implementación de la tecnología SD-Access a la red ya existente. La metodología utilizada es cualitativa transversal; se harán pruebas en un entorno de laboratorio paralelo al sistema de producción y así obtener datos importantes a través de observación y análisis para la pronta emigración de red definida por software.

Tavares (1999) redacta la investigación sobre “la tendencia que se percibe en los gerentes de mantenimiento” (p. 167). Recibiendo mayores responsabilidades, en muchos casos, con una estructura reducida buscan responder las nuevas exigencias de los consumidores, a través de mayor capacitación e intercambio de información. El aporte de la investigación es proporcionar nuevas prácticas o mejorar las existentes, relacionadas con la gestión y el mantenimiento de las aplicaciones y protocolos dedicados al monitoreo de la red. La metodología utilizada es cualitativa transversal, debido a que se define como un estudio de las prácticas que se realizan con base en registros de operaciones en el departamento de IT para un mejor rendimiento de la red. En los resultados de la investigación se podrán presentar datos que demuestran que se necesita atención especializada para el área del centro de datos interno o externo, para mejorar la calidad del manejo de datos.

3. PLANTEAMIENTO DEL PROBLEMA

La manipulación de información utilizando métodos manuales causa recepciones tardías, discrepancias, inclusive pérdidas de datos; tener una infraestructura de red aislada crea un ambiente con falta de sincronismo, exponiendo debilidades técnicas que amenazan montos monetarios en los procesos comerciales.

3.1. Descripción del problema

El problema está en la distribución de procesos que se evidencia en las sucursales dentro de toda la empresa. Las sucursales carecen de conectividad directa al SAP BO instalado en la empresa, por lo tanto, son tratados como vendedores; la razón radica en que solo existe una planta de producción, por lo cual las demás instancias son puntos de distribución (bodegas). Las sucursales no cuentan con conectividad a la base de datos (no hay redundancia y se gestiona un nuevo servidor) instalada en el servidor del centro de equipos. Los pedidos se crean en un archivo de Excel (se envía por correo electrónico donde se recibe y se modifica el formato para ingresarlo al ERP); actualmente se procesa la migración de COBOL a SAP BO (software ERP).

Únicamente cuando la documentación está cargada a SAP se genera un reporte utilizando software de reportería (Crystal Report), que para políticas de la empresa es necesario para los vehículos de transporte presentarlo en garita de la planta (Sacatepéquez, Guatemala) y así permitir su salida. Aplicando un proceso similar existen diversos servicios como control de ingreso (gestiona la

asistencia de los colaboradores a final del mes para pago de KPI y salarios). Estos procesos generan retrasos a gerencia los días de facturación (viernes).

3.2. Delimitación del problema

Existe una red funcional y aislada entre la planta de producción y las sucursales. El problema es la falta de conectividad directamente al sistema SAP, para el proceso de logística y los diferentes servicios que se ven afectados por procedimientos complementarios innecesarios que agilicen su objetivo. Todo refleja la falta de una infraestructura de red que centralice las operaciones de control y gestión, para el acceso a los servicios y recursos que necesitan los usuarios o colaboradores para que la logística comercial sea más eficiente.

3.3. Formulación de preguntas orientadoras

Las siguientes preguntas orientarán sobre el camino racional y ordenado a seguir en el proceso de la investigación.

3.3.1. Pregunta central

¿Cómo desarrollar una propuesta de infraestructura de red que mejore el acceso a los recursos y servicios de IT, con la implementación de una red industrial a nivel de acceso con tecnología SDN y que además facilite su control y gestión?

3.3.2. Preguntas auxiliares

- ¿Cómo centralizar el control de operaciones IT para eliminar inconsistencias en los datos físicos y digitales, para que todo sea gestionado desde la planta de producción en Guatemala y tener acceso al sistema de gestión de SAP BO en la planta?

- ¿Qué tipo de diseño de red o tecnología permitiría automatizar las operaciones desde una interfaz gráfica, para disminuir la cantidad de errores por configuraciones manuales?

- ¿Qué beneficios aporta a una red LAN emplear procedimientos de gestión y monitoreo de la red en la capa de acceso, para la creación de políticas de seguridad más consistentes para los colaboradores?

- ¿Cómo identificar los principales problemas para la implementación y gestión de la infraestructura de red, evaluando la gestión y socialización entre departamentos?

4. JUSTIFICACIÓN

El presente trabajo de investigación se desarrolla dentro del perfil de la línea de infraestructura de red de la maestría en ingeniería para la industria, con especialidad en telecomunicaciones de la facultad de ingeniería de la Universidad de San Carlos de Guatemala. Los cursos que se relacionan son infraestructura de redes híbridas, nos describe el funcionamiento de los tipos de redes y los parámetros necesarios para relacionar los diferentes tipos de red existente. Redes inalámbricas, parámetros utilizados en redes que transfieren datos a través del espacio RF. Computación en la nube, espacios en infraestructuras públicas o privadas ubicados en la web. Infraestructura del IoT, como todas las cosas emigran al internet de las cosas. Administración de las cosas, desarrollo de protocolos de gestión y mantenimiento de una red híbrida.

La importancia de una implementación de SD-Access para la administración de una red se enfoca en la centralización de operaciones, eliminando errores producidos por malas configuraciones, estandarizándolas y gestionándolas por medio de una interfaz fácil de utilizar. Interconectando todos los puntos a través de redes virtuales que atraviesan el internet y simularán conectividad punto a punto entre las sucursales y la central de producción.

La necesidad de implementar la nueva estructura de red se centra en unificar los procesos comerciales y administrativos a través del software SAP BO y que toda información sea la misma, almacenada en los servidores colocados en la nube y evitar pérdidas de información o incongruencias en la información solicitada en el momento oportuno por gerencia.

La motivación del investigador que suscribe el presente documento radica en implementar los conocimientos adquiridos con respecto a la tecnología SD-Access, para utilizarlas en una red de producción y que mejore considerablemente la red convencional. Modificar la red para poder seguir utilizándola como la base (red subyacente) para una red virtualizada (red superpuesta), gestionada a través del ISP para interconectar todas las sucursales con la central (*red hub and spoke*) y de esta manera minimizar costos.

Los beneficios que se obtienen con el trabajo de investigación es desarrollar un diseño que brinde estabilidad a la red. Gracias a la automatización en la implementación de políticas de acceso, los colaboradores podrán interactuar con cualquier dispositivo dentro de la red con seguridad. Utilizando la infraestructura de red subyacente mejora la eficiencia y efectividad en el procesamiento de datos, minimizando operaciones gracias a la conectividad directa al servidor. Elimina el uso de cárdex y el inconveniente de tras papeleo de información. Centraliza los procesos de gestión y monitoreo de todas las entidades por su directa interacción con la base de datos generada por SAP BO.

Los principales beneficiarios de esta propuesta de desarrollo son: la empresa como principal, al garantizar la información oportuna del movimiento comercial entre vendedores ruteros, bodega de producto terminado que despacha los pedidos, área de producción que satisface la demanda, bodega de materias primas que mantiene en stock los insumos, facturación que ve cómo se elevan las ventas, las sucursales que se abastecen de manera directa a la planta sin los inconvenientes de la documentación, todos los colaboradores administrativos por tener acceso a la información necesaria, las aplicaciones y su conectividad a la red.

El análisis de un buen diseño de monitoreo y gestión. Políticas adecuadas de mantenimiento de la red y pruebas de conectividad que garanticen el buen funcionamiento de la red, aplicando mantenimientos preventivos y predictivos a tiempo que minimicen fallas y la aplicación de mantenimientos correctivos eficientes a los diferentes equipos de red dentro de la planta de producción como en cualquiera de las sucursales ubicadas fuera del país.

.

5. OBJETIVOS

5.1. General

Desarrollar una propuesta de infraestructura de red que mejore el acceso a los recursos y servicios de IT de una planta de producción de alimentos, con la implementación de una red industrial a nivel de acceso con tecnología SDN y que además facilite su control y gestión

5.2. Específicos

- Centralizar el control de operaciones IT para eliminar inconsistencias en los datos físicos y digitales, para que todo sea gestionado desde la planta de producción en Guatemala y de esta manera acceder al sistema de gestión de SAP BO en la planta.

- Utilizar los beneficios que brinda la tecnología SDN, automatizando las operaciones desde una interfaz gráfica que disminuyan la cantidad de errores por configuraciones manuales.

- Emplear procedimientos de gestión y monitoreo de la red en la capa de acceso, que brinden la creación de políticas de seguridad más consistentes para los colaboradores.

- Identificar los principales problemas para la implementación y gestión de la infraestructura de red, evaluando la gestión y socialización entre departamentos.

6. NECESIDADES POR CUBRIR Y ESQUEMA DE SOLUCIÓN

La necesidad de implementar una solución con la tecnología SDN es la de centralizar los recursos de red y servicios prestados por la misma, para mejorar y asegurar el acceso por los colaboradores desde cualquier punto de la empresa, no importando su ubicación geográfica ni la infraestructura de red existente de por medio.

La principal necesidad por cubrir en el aspecto laboral con el estudio de investigación es realizar un aporte metodológico y procedimental, que permita en una red ethernet existente el estudio y la implementación de la tecnología SDN, para mejorar la gestión y control de los recursos y servicios. De esta manera, se eliminarán procedimientos manuales innecesarios y procesos desactualizados dentro de las ITs.

Al realizar el estudio de la propuesta se tendría el conocimiento de su funcionamiento y todo sería realizado en base a nuestro enfoque.

Para comenzar, se necesita realizar un *checklist* de los procesos que se realizan y que luego se cargaran a SAP BO; conocer el plano físico y lógico de la red ethernet; realizar una inspección para verificar modelos y series de los equipos, para enlistar los que soportan la tecnología de virtualización e implementación de SDN. Además, analizar si los servidores físicos se pueden emigrar al *cloud*, elaborar un estudio de posibles APIs SDKs de SAP, adquisición de información en cuanto a aspectos legales con el ISP (ISPs por *multihoming*), inspeccionar infraestructura de red física y dispositivos de telemetría.

Luego que se tenga una visión del estado físico del sistema, se procederá a inventariar los dispositivos a disposición para verificar que coincidan con los datos de condiciones especiales a la fecha de la investigación, contando los instalados. Se fabricará un afiche por cada ítem que se encuentre dentro del inventario para tener un control de seguimiento.

Se requiere personal para brindar un mejor despliegue dentro de las instalaciones. Se capacitará al personal en áreas especializadas de modo que todos se enfoquen en el mismo objetivo.

Se realizarán cotizaciones que incluyan los dispositivos, actualizaciones de los sistemas operativos, prestación de servicios, licenciamiento y capacitación del personal para mejores prácticas de desarrollo.

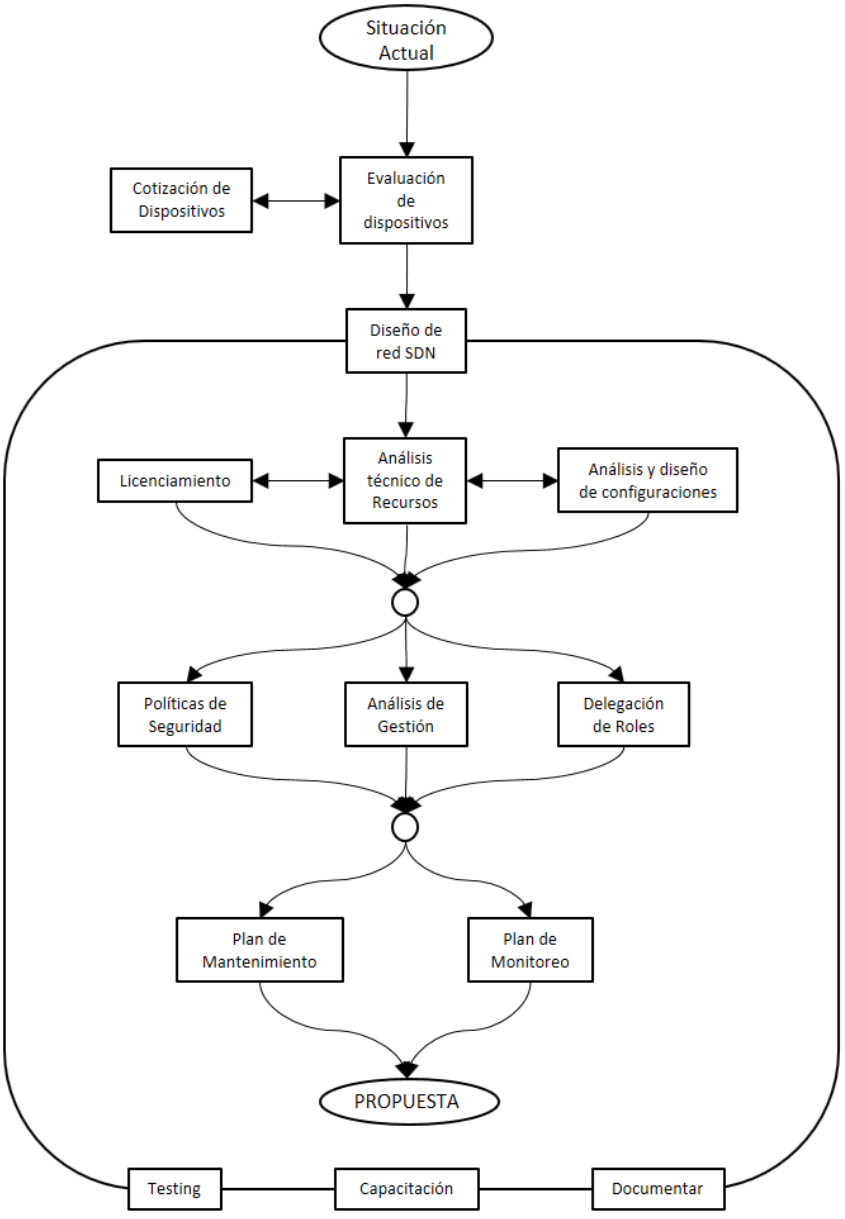
Después de efectuar el análisis inicial se procederá a desarrollar el mecanismo para centralizar el control y gestión de la red.

El contenido teórico de redes IP no posee el nivel de importancia que contiene dentro del ámbito profesional, ya que en la actualidad no existe mucho (pero existe) contenido o estudios de implementación de los mismos. La importancia que posee la automatización de red en una infraestructura existente otorga cierto grado de originalidad a este estudio.

El trabajo de investigación es de carácter pertinente porque desea mejorar la relación existente en el aspecto técnico-económico.

Él tiene validez técnica porque busca la implementación de una tecnología actualizada que ayude a monitorear, gestionar y configurar de manera eficiente cada elemento que conforma la red IP de la empresa.

Figura 1. **Esquema de solución**



Fuente: elaboración propia, hecho con Microsoft Power Point.

7. MARCO TEÓRICO

7.1. Redes definidas por software (SDN)

Las redes SDN surge a finales de la de cada del 2,000 en una universidad de los Estado Unidos. La finalidad de la tecnología SDN (*software define network*) consiste en minimizar las actividades de los operadores de red. Permite gestionar la infraestructura de red, la QoS (*quality of service*), velocidad, ingeniería de tráfico y logs, entre otros.

Jason Gooley (2018) define la tecnología SDN como una arquitectura que controla y reenvía paquetes dentro de distintas redes en forma dinámica. La cantidad de información que se maneja en la actualidad necesita un amplio ancho de banda, el cual es manejable gracias a las características de esta tecnología. Entre sus cualidades, destaca la separación de la data plane y el control plane. La separación muestra cuál será el trayecto del flujo de datos (control plane) dentro de la red subyacente, así como los datos que se reenvían hacia su destino (data plane). Los analistas, programadores y desarrolladores de esta tecnología afirman que SDN simplificará la creación de redes.

Las redes definidas por software (SDN) son redes que controlan el flujo de datos y el control de los mismos utilizando controladores como su nombre lo indica basados en software y aplicaciones desarrolladas con algún lenguaje de programación diseñadas para tareas especifica (API, Application Programming Interface). Las redes SDN definen estándares y

> protocolos que permiten la comunicación con la infraestructura física de la red, llamada red subyacente. (Rapp, 2021, p. 1)

Las redes SDN mejoran la arquitectura de una red tradicional basada en hardware, porque permiten su control por medio de las APIs o diseñar redes virtuales y poder gestionarlas.

En la actualidad las redes empresariales crecen a pasos agigantados, se han desarrollado mecanismos que ayudan a atenuar tal impacto como lo es la virtualización. La virtualización nos permite conectar dispositivos de red diseñados en software, crear redes dentro de un mismo equipo físico o crear segmentos de red dentro de dos diferentes equipos de red. Mientras que la virtualización nos permite diseñar redes con software, las redes SDN nos permite controlarlas.

7.1.1. Cómo funcionan las redes SDN

Uno de los aportes que introdujeron las redes SDN al *networking* es que el encargado del *forwarding* (data plane) y el encargado de analizar hacia donde enviar el tráfico (control plane) trabajen separados: el software y el hardware se desvinculan. La tecnología SDN permite controlar y administrar la red de una forma centralizada, utilizando alguna interfaz de programación de aplicaciones API, y ya no realizarlos de manera individual en cada dispositivo.

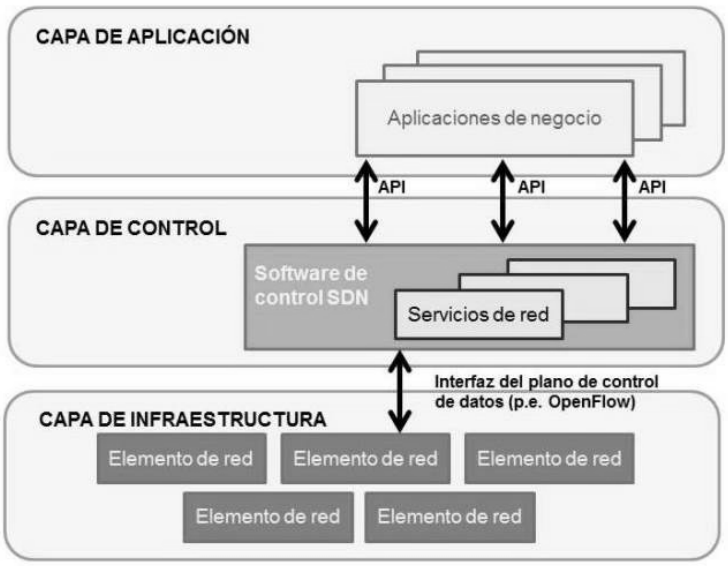
La red SDN está constituida por:

- Aplicaciones: desde donde se puede gestionar solicitudes o manejo de información.

- Controladores: realiza el análisis de enrutamiento basado en la información recibida de las aplicaciones.
- Dispositivos de red: mueve los datos de acuerdo al análisis realizado por los controladores.

Estos elementos puedes estar ubicados en el mismo dispositivo o en diferentes dispositivos, según sea necesario.

Figura 2. **Estructura SDN**



Fuente: Millán (2014). *SDN: El futuro de las redes inteligentes*. Consultado el 9 de septiembre del 2021. Recuperado de https://www.ramonmillan.com/tutoriales/sdnredesinteligentes.php.

Ventajas de las redes SDN:

- Velocidad y flexibilidad con mayor control: con la ayuda de las redes SDN no es necesario configurar equipo por equipo, porque se puede integrar

un controlador que lo realice ya sea de forma masiva o individual; para estas operaciones existen versiones de código abierto, tanto para el controlador como para el protocolo, que permite la comunicación con un dispositivo en específico.

- Personalizar la red: La red SDN permite la asignación de recursos y configurar la red física en tiempo real para darle prioridad al flujo de datos o aplicaciones que lo requieran.

- Seguridad: Al poder configurar y administrar la red de manera centralizada, permite un mejor control de toda la red para protegerla de cualquier intrusión no deseada o para poder dar prioridad a cierto grupo de dispositivos.

Modelos de redes SDN:

- SDN Abierta: La red es administrada por el protocolo OpenFlow.

- SDN por API: Se utiliza APIs para administrar y gestionar una red.

- SDN por superposición: Se crea una red virtual (VPN's) por encima de la red física (red superpuesta) para interconectar distintos puntos como datacenters locales y remotos.

- SDN Híbrida: Permite la interacción de los protocolos tradicionales con la red SDN, tratando de satisfacer de forma inteligente los diferentes sectores de la red.

7.1.2. Controlador basado en software de estándar abierto

Mencionaremos un software de código abierto que se está usando en el mundo de *networking*. Por ser un robusto controlador con grandes características técnicas, mencionaremos:

- *OpenDayLight*
- *OpenFlow*

7.1.2.1. *OpenDayLight*

Con el apoyo de grandes empresas en el campo de las redes, el software *OpenDayLight* es un código *open source* con el propósito de otorgar mejoras al estándar de las redes SDN (por sus siglas en inglés o redes definidas por software RDS en español).

Figura 3. **OpenDayLight**

Fuente: Blog.desdelinux.net (2015). *OpenDayLight: El Futuro de las Redes Definidas por Software (SDN)*. Consultado el 9 de septiembre de 2021. Recuperado de https://blog.desdelinux.net/opendaylight-el-futuro-de-las-redes-definidas-por-software-sdn/#comments

OpenDayLight es una plataforma *open source* que tiene el propósito de convertirse en una herramienta *multivendor* y ser el análogo de *OpenStack* en Cloud Computing o Hadoop en *BigData*. Esta tecnología rompe los estereotipos de las redes tradicionales que han permanecido estáticas y que evolucionaran con la implementación de la tecnología SDN.

Siguiendo el proceso normal de enrutamiento dentro de una red tradicional; el paquete que ingresa al conmutador y este procesa el paquete de acuerdo a la configuración establecida de fábrica internamente, donde se determina hacia donde se reenviara el paquete. El switch procesará cada paquete que ingresa de la misma manera como fue establecido. Los switches administrables están diseñados con características especiales que liberan el CPU del proceso de *forwarding* a través de circuitos integrados (ASIC) diseñados específicamente para el enrutamiento, que procesan cada paquete y tratan de manera diferente si así se requiere. La desventaja de estos dispositivos es su elevado costo.

> En una SDN, un administrador de red; utilizará una interfaz centralizada para conectarse al conmutador sin la necesidad de hacerlo físicamente y cambiar la configuración, estableciendo prioridades, calidad de servicio o inclusive apagar el dispositivo de red si fuera necesario. Los niveles de control pueden ser muy detallados incluso a distancia. (Blog.desdelinux.net, 2015, p. 3)

Es una tecnología con características multi usuarios especialmente cuando se utiliza *cloud computing* (computación en la nube), donde se necesita administrar de una mejor manera los flujos de datos. Esta tecnología ayuda al administrador de la red a reducir significativamente la cantidad de dispositivos

con limitados recursos, y al reducirlos hay un mejor control de los activos de red y por consiguiente del control del tráfico de red.

Las redes SDN son una implementación de cisco que permite la interacción de cualquier marca, por eso es considerada “asesina de cisco”. SDN permite dispositivos *multivendor* o circuitos integrados de aplicaciones específicos, que los ingenieros de red pueden implementar en las redes *fabric* (redes superpuestas). *OpenFlow* es un software abierto y el estándar más utilizado en el diseño de redes SDN para controlar las tablas de enrutamiento; esto lo realiza el ingeniero de red de manera remota.

7.1.2.2. *OpenFlow*

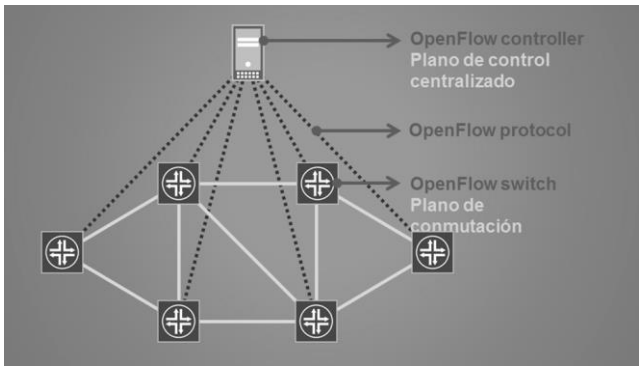
Intriago (2017) indica que el método de control que utilizan los dispositivos de red, con capacidad de analizar la ruta de destino y que almacenan la información en las tablas TCAMs, también son los utilizados para implementar firewalls, políticas de servicio (QoS), traslación de direcciones de red (NATs) y para recolectar datos estadísticos; Los routers y los switches poseen una serie de funcionalidades y el objetivo de *OpenFlow* consiste en explotar estas funciones. Una de las ventajas es la facilidad con la que se puede controlar el manejo de aplicaciones dentro de las distintas arquitecturas y emular sistemas operativos desarrollados para otras marcas.

Una de las novedades y razón por la que *OpenFlow* ha ganado popularidad es porque ha cubierto cierto espacio o discrepancia que presentan los sistemas abiertos dentro de sus atributos, algo presente dentro de la virtualización. *OpenFlow* es un protocolo con mucha demanda porque posee muchos atributos que permiten la virtualización.

Intriago (2017) indica que *OpenFlow* es el protocolo *open source* que permite controlar la tabla de reenvió que posee un *router* y un conmutador multi marca. Además, permite separar la red de producción de la de investigación, ya que los ingenieros dedicados al análisis del comportamiento de una red emulan escenarios ficticios para el enrutamiento de paquetes, así como el trato que recibirá cada paquete. Dentro de este esquema, es posible analizar nuevas políticas de seguridad, algunos protocolos nuevos, diferentes esquemas de direccionamiento mientras que la red de producción se aísla y se procesa de manera estándar.

Las redes SDN poseen muchas variantes importantes, entre ellas la utilización de APIs, que permite la gestión de redes virtuales establecidas en la nube, en los centros de datos, ISPs, entre otros. Y el uso de software abierto como lo es *OpenFlow* para el control y administración de las tablas de ruteo, además de que es posible la interacción con hipervisores, para el control básico de reenvió de paquetes mediante switches que realizan la tarea de conectar el tráfico entre las interfaces físicas y las máquinas virtuales.

Figura 4. **Estructura OpenFlow**



Fuente: Turmero (2014). *OpenFlow y SDN*. Consultado el 9 de septiembre de 2021. Recuperado de https://www.monografias.com/trabajos107/openflow-y-sdn/openflow-y-sdn.shtml

El *Switch* procesa cada paquete que ingresa por las interfaces de la siguiente manera:

- Se desempaqueta la cabecera y se buscan coincidencias en los campos del paquete.

- La tabla de flujos definida por *OpenFlow*, donde se establecen las reglas que serán aplicadas a cada paquete que ingresa; recordando que la primera regla coincidente será aplicada. Cuando un paquete ingresa al switch, existen campos que pueden coincidir con algún argumento establecido (condiciones). Para una configuración con ANY en la tabla de flujos, este parámetro hará match con todos los paquetes.

- Se analizan las entradas y al existir una coincidencia se ejecutan las acciones para esa entrada. De lo contrario los 200 bytes correspondientes son procesados por el controlador.

7.1.2.2.1. *OpenFlow Switch*

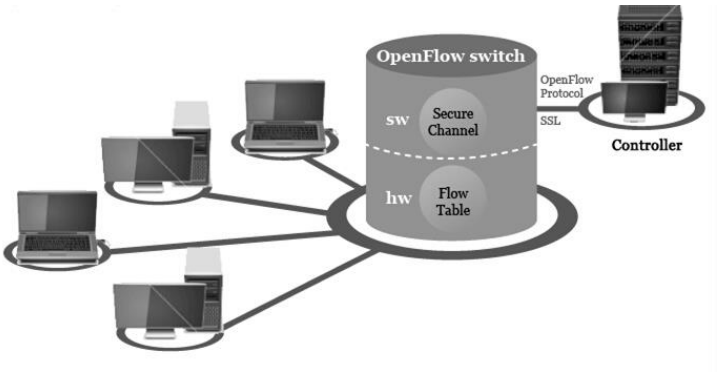
OpenFlow Switch es un protocolo desarrollado para el control de la conectividad que utiliza una interfaz central dentro de una red SDN. *OpenFlow* Switch posee una variedad de funciones. Para que el protocolo *OpenFlow* pueda ser implementado se debe contemplar aspectos como poseer un Switch *OpenFlow* con los requerimientos básicos como:

El *switch OpenFlow* está constituido por tres partes. La primera, la tabla de flujos donde se vinculan las acciones con las entradas en la tabla, donde se le indicara al switch como procesar el reenvió de datos. En segundo lugar, se

establece un canal seguro que conecta el *switch* al *controller* para compartir instrucciones o comandos que utilizan el protocolo *OpenFlow*, que establece una ruta abierta y estandarizada de comunicación. Por último, el controlador, que es capaz de administrar al eliminar o agregar entradas en la tabla de flujos. El procesamiento de capa 2 y 3 no está soportado por los *Switches OpenFlow*.

Los *switch OpenFlow* dedicados: dentro de las especificaciones definidas en el *switch OpenFlow* se establecen las funciones que soportan y la estructura de los encabezados; las rutas para reenvió se almacenan dentro del *switch*. La gráfica muestra el *OpenFlow*.

Figura 5. ***OpenFlow switching***



Fuente: Jin (2016). *OpenFlow Switch with Hardware Flow Table*. Consultado el 9 de septiembre de 2021. Recuperado de https://learn.linksprite.com/project/openflow-switch-with-hardware-flow-table/

Mencionaremos tres acciones básicas asociadas a las entradas de la tabla de flujos que soportan los *Switch OpenFlow*:

- El flujo de paquetes es enrutado a través de la red hacia un puerto especifico; este proceso se realiza de acuerdo a la velocidad de la línea.

- Cuando la comunicación se establece, el primer paquete se encapsula y se envía al *controller* dentro de un canal seguro; el *controller* analiza si el flujo de paquetes deberá ser agregado a la tabla de flujos. También son utilizados de forma experimental al enviar todos los paquetes para ser procesados.

- El control de flujo de paquetes en la red proporciona seguridad, bloquea vulnerabilidades como el ataque a los servicios, la reducción del falso tráfico creado por medio de broadcast, que envía los dispositivos finales.

7.1.3. Tecnología SD-ACCESS

Es la solución de Cisco para las redes a nivel de SDN. Existe un gran reto dentro de las operaciones de las redes empresariales, debido a la configuración en los dispositivos de red que se realizan de forma manual. Porque los cambios en las configuraciones son lentos y conducen a errores que causan que los servicio en la red sean interrumpidos, y la situación se agrava en un entorno en constante cambio donde se agregan constantemente más usuarios, puntos finales y aplicaciones.

El crecimiento de los usuarios y puntos finales hace que la configuración de credenciales de usuario y el mantenimiento de una política coherente en toda la red sean muy complejos. Si las políticas son inconsistentes, hay una complejidad adicional involucrada en el mantenimiento de políticas separadas entre las redes cableadas e inalámbricas que dejan a la red vulnerable a las brechas de seguridad. A medida que los usuarios se mueven por la red del campus, localizar a los usuarios y resolver problemas también se vuelve más

difícil. En otras palabras, las redes de campus tradicionales no abordan las necesidades de red de campus existentes.

Con SD-Access se puede construir una red de campus evolucionada que aborde las necesidades de las redes de campus existentes al aprovechar las siguientes capacidades, características y funcionalidades:

- Automatización de red: SD-Access reemplaza las configuraciones manuales en los dispositivos de red con una administración de red desde un único punto de automatización. La administración y control de funciones de red mediante el uso de Cisco DNA Center. Esto simplifica el diseño y el aprovisionamiento de la red y permite una implementación muy rápida y de menor riesgo de los dispositivos y servicios de la red al utilizar las mejores prácticas.

- Análisis y garantía de la red: SD-Access permite la predicción proactiva de los riesgos relacionados con la red y la seguridad al usar la telemetría para que la red presente un mejor rendimiento, las aplicaciones, incluido el tráfico cifrado hacia los usuarios finales.

- Movilidad del host: SD-Access proporciona movilidad del host tanto para clientes cableados como inalámbricos.

- Servicios de identidad: Cisco Identity Services Engine (ISE) identifica a los usuarios y dispositivos que se conectan dentro de la red. Además, proporciona la información contextual requerida para la implementación de políticas de seguridad que limiten el acceso y permitan la segmentación de la red.

- Aplicación de políticas: las listas de control de acceso (ACL) tradicionales pueden ser difíciles de implementar, mantener y escalar, porque dependen de direcciones IP y subredes. La creación de políticas de acceso y aplicación, basadas en políticas grupales utilizando las listas de control de acceso de grupo de seguridad (SGACL), proporciona una forma mucho más simple y escalable de aplicación de políticas basada en la identidad en lugar de una dirección IP.

- Segmentación segura: con SD-Access es más fácil segmentar la red para admitir invitados, empresas, instalaciones e infraestructura habilitada para IoT.

- Virtualización de red: SD-Access permite aprovechar una única infraestructura física para admitir múltiples instancias de enrutamiento y reenvío virtual (VRF), denominadas redes virtuales (VN), cada una con un conjunto distinto de políticas de acceso.

SD-Access tiene dos componentes principales:

- Solución fabric Cisco Campus
- Cisco DNA Center

La estructura del campus es una solución de superposición de estructura validada por Cisco, que incluye todas las características y protocolos (*control plane, data plane, management plane* y *policy plane*) para operar la infraestructura de red. Cuando la solución de estructura de campus se gestiona utilizando la CLI como interfaz para el ingreso de comandos o una API como interfaz de aplicaciones y el uso del Protocolo de configuración de red (NETCONF) / YANG, la solución es considerada como parte de una estructura

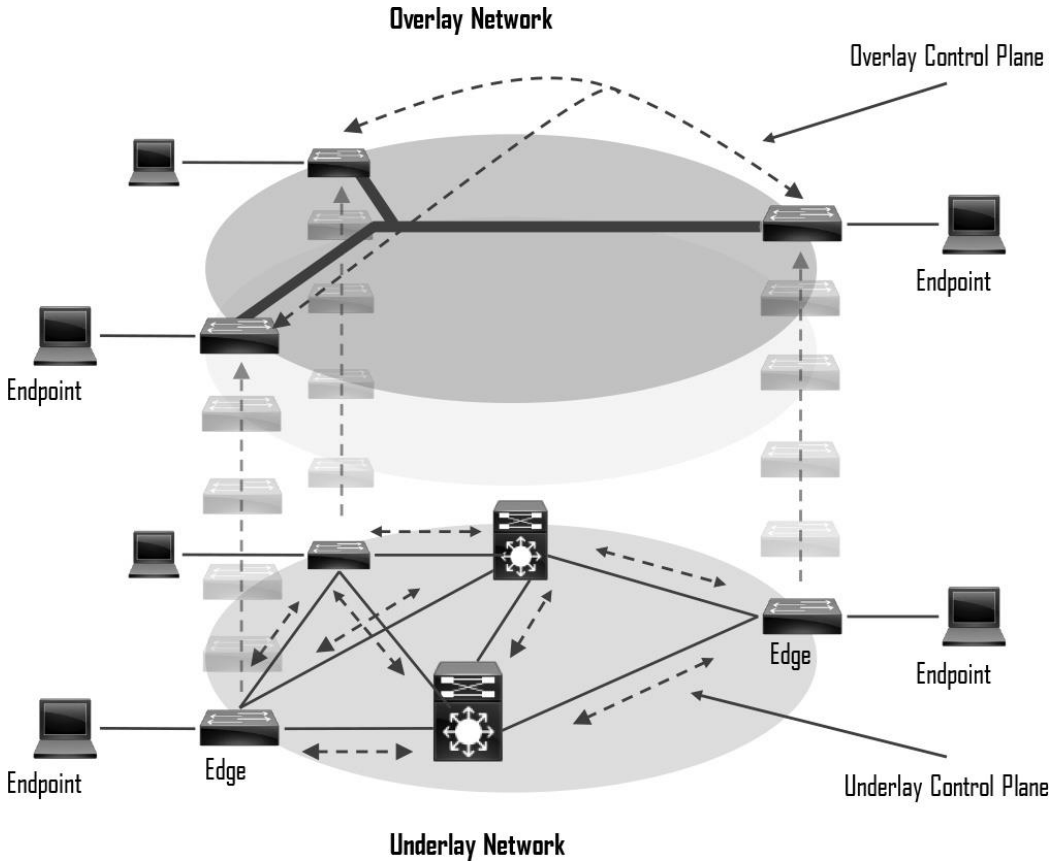
de campus. Cuando la solución de estructura del campus se administra a través del Cisco DNA Center, se considera que la solución es SD-Access.

Figura 6. **Solución de acceso SD**

Fuente: Edgeworth, B., & Garza, R., & Gooley, J., & Hucaby, D. (2020). *Guía Oficial de Certificación CCNP and CCIE Enterprise Core ENCOR 300-401*. Consultado el 30 de agosto de 2021. Recuperado de https://pdfcoffee.com/ccnp-and-ccie-enterprise-core-encor-350-401-official-cert-guidepdf-pdf-free.html

Infraestructura de una red con SD-ACCESS implementado.

Figura 7. **Redes subyacentes y superpuestas**



Fuente: Edgeworth, B., & Garza, R., & Gooley, J., & Hucaby, D. (2020). *Guía Oficial de Certificación CCNP and CCIE Enterprise Core ENCOR 300-401*. Consultado el 8 de septiembre de 2021. Recuperado de https://pdfcoffee.com/ccnp-and-ccie-enterprise-core-encor-350-401-official-cert-guidepdf-pdf-free.html

7.1.4. WAN Definida por software (SD-WAN)

La administración de redes empresariales se está volviendo más compleja, con clientes que adoptan un enfoque de múltiples nubes, las aplicaciones que se mueven a la nube, los dispositivos móviles y de IoT crecen exponencialmente en la red, y el borde de Internet se traslada a la sucursal. Esta

transformación digital está impulsando la adopción de SD-WAN por clientes que buscan hacer lo siguiente:

- Reducir los costos y los riesgos con la simple automatización y orquestación de WAN.

- Extender sus redes empresariales (como sucursales o locales) sin problemas a la nube pública.

- Proporcionar una experiencia de usuario óptima para aplicaciones SaaS.

- Aprovechar una WAN independiente del transporte para un menor costo y una mayor diversidad. Esto significa que la red subyacente puede ser cualquier tipo de red basada en IP, como Internet, MPLS, 3G / 4G LTE, satélite o circuitos dedicados.

- Mejorar la visibilidad de la aplicación y usar esa visibilidad para mejorar el rendimiento con el control de ruta inteligente, para cumplir con los SLA para aplicaciones empresariales críticas y en tiempo real.

- Proporcionar encriptación y segmentación de tráfico WAN de extremo a extremo para proteger los recursos informáticos críticos de la empresa.

Cisco actualmente ofrece dos soluciones SD-WAN:

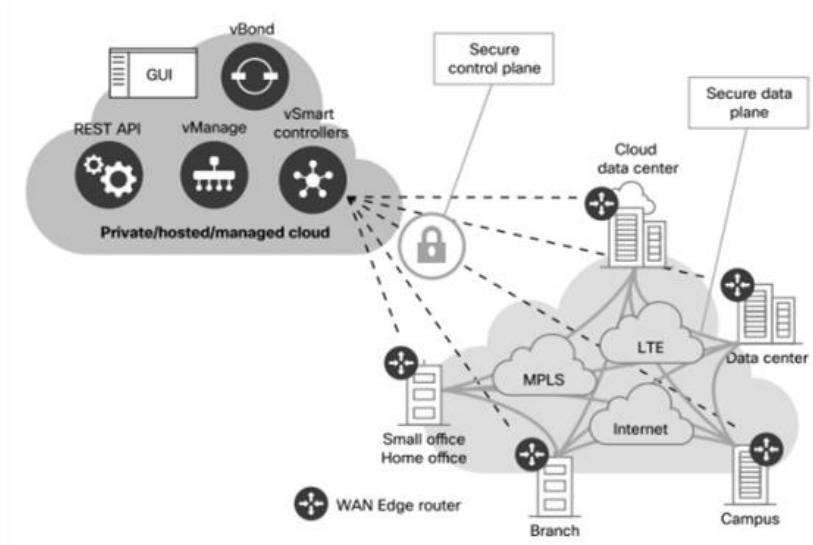
- Cisco SD-WAN (basado en Viptela): esta es la opción preferida para las organizaciones que requieren una solución SD-WAN, con iniciativas basadas en la nube y que brinden segmentación granular, enrutamiento

avanzado, seguridad avanzada y topologías complejas mientras se conectan a instancias de la nube.

- Meraki SD-WAN: esta es la solución recomendada para organizaciones que requieren soluciones de gestión de amenazas unificadas (UTM) con funcionalidad SD-WAN, o que son clientes existentes de Cisco Meraki que buscan expandirse a SD-WAN. UTM es una solución de seguridad todo en uno, que se entrega en un solo dispositivo y generalmente incluye las siguientes características de seguridad: firewall, VPN, prevención de intrusiones, antivirus, antispam y filtrado de contenido web.

Las dos soluciones SD-WAN pueden alcanzar objetivos de diseño similares, pero este capítulo solo cubre Cisco SD-WAN basado en Viptela.

Figura 8. **Topología Cisco SD-WAN**



Fuente: Suarez (2020). *Redes WAN definidas por software. SD-WAN*. Consultado el 9 de septiembre de 2021. Recuperado de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/116386/8/astifrTFG 0620memoria.pdf

7.1.5. Automatización de la red

Con el crecimiento de las empresas, aumenta la necesidad de más colaboradores y la cantidad de puntos de acceso a la red. Las topologías aumentan y la posibilidad de cometer errores o incongruencias en las configuraciones es más probable; la automatización de las redes ethernet fue desarrollada para erradicar este tipo de fallas en las redes. Consiste en configurar, controlar, gestionar y realizar pruebas utilizando software a un dispositivo de red o a varios de ellos, con la finalidad de mejorar el rendimiento y la eficiencia de la red, reduciendo los gastos de operación y errores cometidos al configurar cada dispositivo de forma manual.

Una red automatizada permite configurar desde una asignación de IP hasta el desarrollo de configuraciones complejas que definen la ruta de los datos en la red, como aspectos de administración, gestión de la red y control de servicios virtualizados de la red.

Dentro de las redes SDN, la automatización es una característica importante porque permite estructurar la red, también el aprovisionamiento de forma automática de los servicios de red dentro de un entorno empresarial.

Este proceso consiste en desarrollar una serie de comandos sucesivos dentro de la CLI de cualquier dispositivo que disponga de esta función o sistema operativo, o de algún otro software definido previamente para la automatización.

Para automatizar una red existen varias maneras, como también muchos dispositivos que pueden ser automatizados. Las dos maneras prácticas que existen para automatizar una red son: la primera es mediante comandos con argumentos dentro de la CLI o configurar comandos secuenciales dentro de

archivos de texto; estos archivos son llamados scripts. La segunda es utilizar un software con características especiales para la automatización de la red, seleccionando y ejecutando desde una interfaz gráfica ciertas tareas programadas previamente. Las API permite la interacción entre los usuarios y el software.

7.1.5.1. Herramientas para automatización de una red

Las herramientas de automatización de red tienen una variedad de características. Las herramientas más utilizadas son aquellas que integran todo tipo de funciones, como monitoreo de rendimiento, de enlaces WAN, de interfaces, análisis de tráfico y ancho de banda, configuración y cambios en las mismas, switches y control de acceso, y asignación de direcciones. Estas son herramientas que en un futuro reemplazarán a las existentes porque ofrecen soluciones que realizan las mismas operaciones, pero de una forma más eficiente y rápida.

Si lo observamos desde otra perspectiva, existen herramientas que realizan tareas más específicas; herramientas dedicadas a gestionar todo tipo de configuración en los dispositivos. Esta herramienta está diseñada para facilitar las configuraciones, ya que cumple con las normas establecidas, siguen siendo muy útiles y a menudo son accesorios para cumplir con varios estándares regulatorios. Tecnológicamente existe una gran diversidad de herramientas de automatización con características propias. Existen herramientas que permiten la gestión de configuraciones más complejas pero los costos son superiores. Deberá considerar la herramienta que satisfaga los requerimientos de operación de la empresa y no por los costos. Cabe la posibilidad que una herramienta de menor costo realice la tarea que se necesita. Por ejemplo, las herramientas que

ya cumplen con una función no necesitan ser reemplazadas por otra herramienta de automatización que realice la misma tarea.

Python es un lenguaje que ha tomado mucho auge en la actualidad por ser un lenguaje sencillo y robusto. Python lo podemos encontrar en muchas aplicaciones tecnológicos; las redes ethernet son parte de las tecnologías que se han aprovechado de este lenguaje. Existen varios más, pero es Python uno de los más utilizados por marcas propietarias y por marcas *open source*.

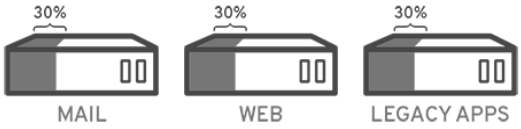
7.2. Virtualización

VMWare (2016) indica que “la metodología de la virtualización otorga muchas mejoras en la escalabilidad de una red, flexibilidad y agilidad de la misma red, brindando un ahorro de recursos y aportes económicos” (p. 3). La virtualización otorga mejoras a la red porque permite asignación dinámica de los recursos, mayor disponibilidad de los recursos, permite ser administrable implementando automatización en los procesos de networking, provoca que la administración de la red o infraestructura de TI sea más simple. Además, reduce los costos de operación y de adquisición.

> La virtualización es la evolución de la tecnología que permite la creación de servicio de infraestructuras que están vinculados a algún hardware, distribuyendo su capacidad o funcionalidad dentro del entorno. Es decir, los recursos físicos o reales los distribuye dentro de los requerimientos de cada usuario o entorno. Permitiendo utilizar eficientemente la maquina en su totalidad. (Red Hat, 2021, p. 2)

Para una explicación práctica, dentro del centro de datos local existen tres servidores que ejecutan cada uno tareas específicas; por ejemplo, servidor de correo, servidor web y el tercero una serie de aplicaciones internas.

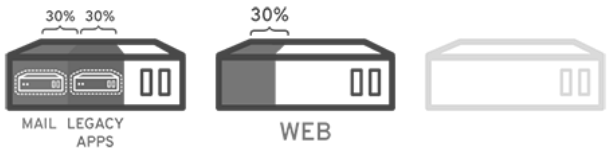
Figura 9. **Tres servidores, aplicación práctica**



Fuente: Red Hat (2021). *Funciones y Seguridad de la Virtualización*. Consultado el 9 de septiembre de 2021. Recuperado de https://www.redhat.com/es/topics/virtualization/what-is-virtualization

Asignar operaciones individuales a servidores individuales es algo sencillo. Pero el desarrollo tecnológico cada día es más exigente y la necesidad de asignar más de una tarea a un servidor aumenta, no es una tarea sencilla. La virtualización permite crear dos servidores lógicos en un servidor físico, asignando procesos independientes a cada servido lógico; por ejemplo, dentro del servidor de correo agregar el servidor lógico de aplicaciones. Ahora existe un servidor físico que se puede reutilizar con otra tarea.

Figura 10. **Hospedaje de dos servidores lógicos, aplicación práctica**



Fuente: Red Hat (2021). *Funciones y Seguridad de la Virtualización*. Consultado el 9 de septiembre de 2021. Recuperado de https://www.redhat.com/es/topics/virtualization/what-is-virtualization

Este diseño libera un servidor para utilizarse luego o no, pero además ayuda a reducir costos de espacio y temperatura (relativamente).

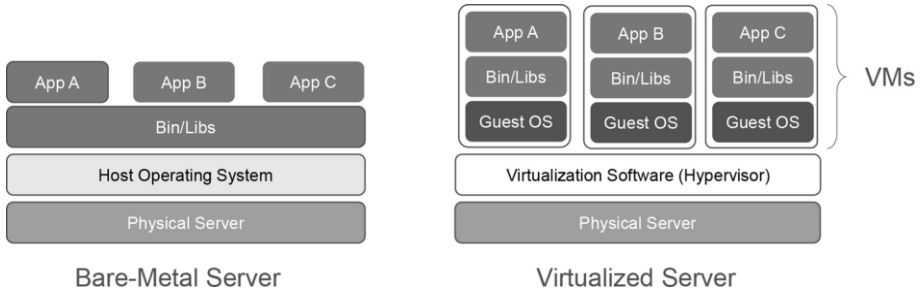
Uno de los principales impulsores de la virtualización del servidor fue que los recursos de hardware del servidor estaban siendo subutilizados; Los servidores físicos normalmente ejecutaban un solo sistema operativo con una sola aplicación y solo usaban entre el 10 % y el 25 % de los recursos de la CPU. Las máquinas virtuales y los contenedores aumentan la eficiencia general y la rentabilidad de un servidor al maximizar el uso de los recursos disponibles.

7.2.1. Cómo funciona la virtualización

Una máquina virtual (VM) es una emulación de software de un servidor físico con un sistema operativo. La máquina virtual permite que un servidor virtual tenga la apariencia física real, incluidos todos sus componentes, como CPU, memoria y las tarjetas físicas de la interfaz de red. El software de virtualización que crea máquinas virtuales permite que varias máquinas virtuales se ejecuten simultáneamente se conoce como hipervisor. Microsoft Hyper-V, Citrix XenServer, VMWare vSphere y Red Hat Kernel-based Virtual Machine (KVM) son

los hipervisores más populares en el mercado de virtualización de servidores. La siguiente figura proporciona una comparación lado a lado de un servidor sin conexión y un servidor que ejecuta software de virtualización.

Figura 11. **Servidor virtual y servidor virtualizado**



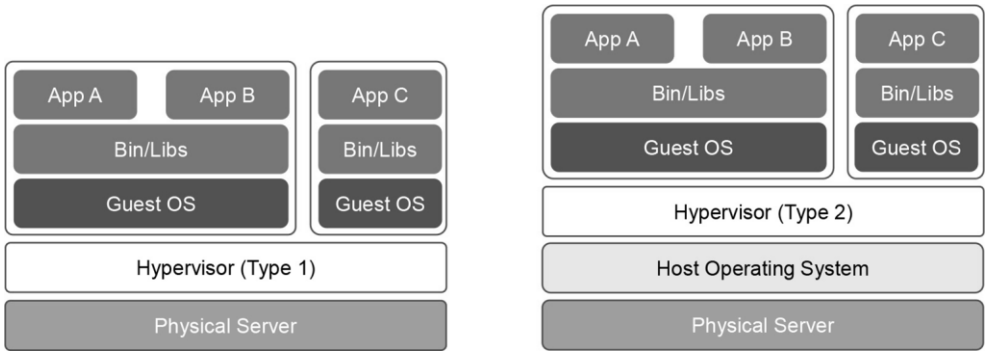
Fuente: Edgeworth, B., & Garza, R., & Gooley, J., & Hucaby, D. (2020). *Guía Oficial de Certificación CCNP and CCIE Enterprise Core ENCOR 300-401*. Consultado el 8 de septiembre de 2021. Recuperado de https://pdfcoffee.com/ccnp-and-ccie-enterprise-core-encor-350-401-official-cert-guidepdf-pdf-free.html

Hay dos tipos de hipervisores:

- Tipo 1: este tipo de hipervisor se ejecuta directamente en el hardware del sistema. Se llama *bare metal* o nativo.

- Tipo 2: este tipo de hipervisor (por ejemplo, VMWare Fusión) requiere un sistema operativo host para ejecutarse. Este es el tipo de hipervisor que suelen utilizar los dispositivos cliente.

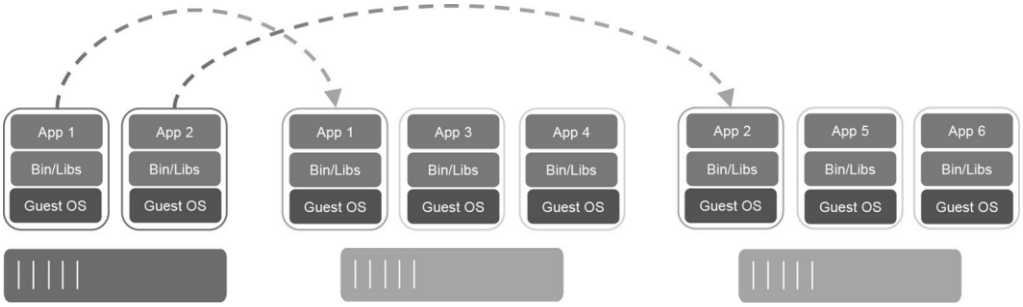
Figura 12. **Hipervisores tipo 1 y tipo 2**



Fuente: Edgeworth, B., & Garza, R., & Gooley, J., & Hucaby, D. (2020). *Guía Oficial de Certificación CCNP and CCIE Enterprise Core ENCOR 300-401*. Consultado el 8 de septiembre de 2021. Recuperado de https://pdfcoffee.com/ccnp-and-ccie-enterprise-core-encor-350-401-official-cert-guidepdf-pdf-free.html

Una capacidad clave de las máquinas virtuales es que se pueden migrar de un servidor a otro al tiempo que se preserva la integridad transaccional durante el movimiento. Esto puede permitir muchas ventajas; por ejemplo, si se necesita actualizar un servidor físico (por ejemplo, una actualización de memoria), las máquinas virtuales se pueden migrar a otros servidores sin tiempo de inactividad. Otra ventaja es que proporciona alta disponibilidad; por ejemplo, si un servidor falla, las máquinas virtuales se pueden activar en otros servidores de la red.

Figura 13. **Migración de VM**



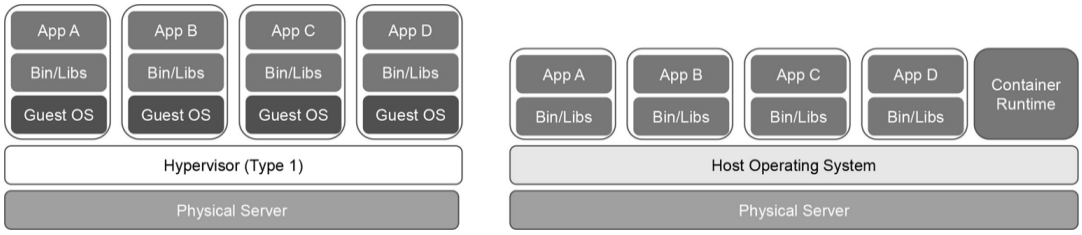
Fuente: Edgeworth, B., & Garza, R., & Gooley, J., & Hucaby, D. (2020). *Guía Oficial de Certificación CCNP and CCIE Enterprise Core ENCOR 300-401*. Consultado el 8 de septiembre de 2021. Recuperado de https://pdfcoffee.com/ccnp-and-ccie-enterprise-core-encor-350-401-official-cert-guidepdf-pdf-free.html

7.2.2. Contenedores

Un contenedor es un entorno aislado donde se ejecutan aplicaciones en contenedores. Contiene la aplicación, junto con las dependencias que la aplicación necesita para ejecutarse. Los contenedores no son lo mismo que las máquinas virtuales a pesar de que tienen estas y muchas otras similitudes, y no deberían denominarse máquinas virtuales ligeras.

La siguiente figura muestra una comparación lado a lado de máquinas virtuales y contenedores. Hay que tomar en cuenta que cada VM requiere un SO y que todos los contenedores comparten el mismo SO mientras permanecen aislados unos de otros.

Figura 14. **Comparación lado a lado de máquinas virtuales y contenedores**



Fuente: Edgeworth, B., & Garza, R., & Gooley, J., & Hucaby, D. (2020). *Guía Oficial de Certificación CCNP and CCIE Enterprise Core ENCOR 300-401*. Consultado el 8 de septiembre de 2021. Recuperado de https://pdfcoffee.com/ccnp-and-ccie-enterprise-core-encor-350-401-official-cert-guidepdf-pdf-free.html

Una VM incluye un sistema operativo invitado, que generalmente viene con una gran cantidad de componentes (incluidos ejecutables, bibliotecas y dependencias) que realmente no son necesarios para que la aplicación se ejecute; depende del desarrollador quitarle los servicios o componentes no deseados para que sea lo más liviano posible. Una VM es básicamente un servidor físico virtualizado, lo que significa que incluye todos los componentes de un servidor físico, pero de manera virtual.

Los contenedores, por otro lado, comparten los recursos subyacentes del sistema operativo host y no incluyen un SO huésped, como lo hacen las máquinas virtuales; Por lo tanto, los contenedores son livianos (tamaño pequeño). La aplicación, junto con las dependencias específicas (archivos binarios y bibliotecas) que necesita ejecutar, se incluyen dentro del contenedor. Los contenedores se originan a partir de imágenes de contenedores. Una imagen de contenedor es un archivo creado por un motor de contenedor que incluye el código de la aplicación junto con sus dependencias. Las imágenes de contenedor se convierten en contenedores cuando son ejecutadas por el motor de

contenedor. Debido a que una imagen de contenedor contiene todo lo que el código de la aplicación necesita para ejecutarse, es extremadamente portátil (fácil de mover o migrar). Las imágenes de contenedor eliminan algunos problemas típicos, como las aplicaciones que funcionan en una máquina, pero no en otra y las aplicaciones que no se ejecutan, porque las bibliotecas necesarias no forman parte del sistema operativo y deben descargarse para que se ejecute.

Un contenedor no intenta virtualizar un servidor físico como lo hace una VM; en cambio, la abstracción es la aplicación o los componentes que componen la aplicación.

Aquí hay un ejemplo más para aclarar la diferencia entre máquinas virtuales y contenedores: cuando se inicia una máquina virtual, el sistema operativo debe cargarse primero, y una vez que está operativo, la aplicación en la máquina virtual puede comenzar y ejecutarse. Todo este proceso generalmente toma minutos. Cuando se inicia un contenedor, aprovecha el núcleo del sistema operativo host, que ya se está ejecutando, y normalmente tarda unos segundos en iniciarse.

Hay en disponibilidad muchos motores de contenedores para crear, ejecutar y administrar contenedores. El motor contenedor más popular es el Docker. Lista de opciones de motor de contenedor disponibles:

- Contenedor RTK
- Iniciativa de contenedores abiertos
- LXD (contenedor "lexdi"), de Canonical Ltd.
- Linux-VServer
- Contenedores de Windows

7.2.3. Tipos de virtualización

- Virtualización de datos: consiste en consolidar los datos que están repartidos en una sola fuente de datos. La virtualización de datos toma todas las fuentes y las emula de tal manera que a nivel empresarial se vea como una cadena de datos dinámica.

- Virtualización de escritorio: Consiste en crear escritorios virtuales o simulados conectados a un solo sistema operativo, permitiendo configurar y actualizar de forma masiva los mismos. No consiste en la virtualización de sistemas operativos, pero suele confundirse.

- Virtualización de servidores: Un servidor es una computadora más robusta, diseñada para tareas específicas y que otras computadoras puedan conectarse a él. La virtualización de servidores permite, con la ayuda de un contenedor, simular varios servidores en uno solo y que este realice varias tareas específicas.

- Virtualización de sistemas operativos: Los sistemas operativos virtuales se configuran en el núcleo (kernel). En la industria es común observar que se utilizan sistemas operativos virtualizados; es una práctica que brinda varios beneficios, entre los que podemos mencionar: reducción de costos, disminución del tiempo de servicio y aumento de la seguridad.

- Virtualización de funciones de red (NFV): la virtualización de funciones de red (NFV) es un marco arquitectónico creado por el Instituto Europeo de Estándares de Telecomunicaciones (ETSI). La ETSI define estándares para desacoplar funciones de red de dispositivos propietarios basados en hardware y hacer que se ejecuten en software, en servidores estándar

x86. También define cómo administrar y orquestar las funciones de la red. La función de red (NF) se refiere a la función realizada por un dispositivo físico, como un firewall o una función de enrutador.

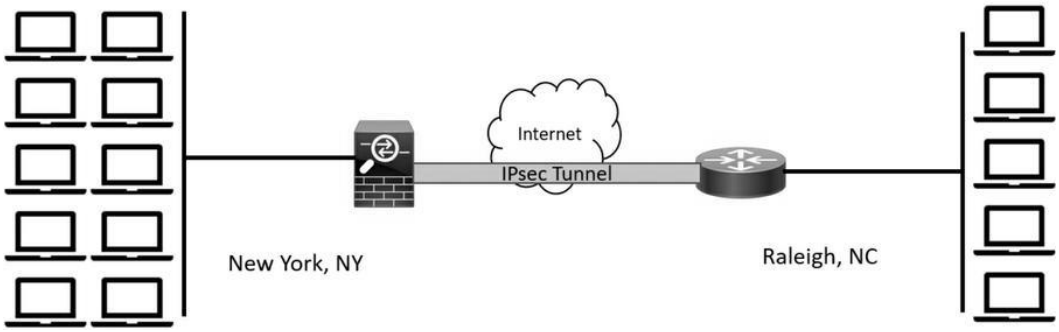
7.2.4. VPN (virtual private network)

Las conexiones VPN's no es una tecnología nueva, sus orígenes coinciden con el desarrollo del internet mismo. Fueron los trabajos en conjunto de la Universidad de Columbia y AT&T Bell Labs lo que dio vida a la primera modalidad de una VPN, conocida como Swipe; creación que fue mejorada luego. Las VPN's originalmente fueron desarrolladas para un nivel empresarial. Las empresas cuando aún no se implementaban las VPN's estaban expuestas a amenazas que vulneraban la integridad y confidencialidad de su información, por utilizar conexiones directas y abiertas a las redes externas (internet).

Los servicios de VPN cobraron popularidad gracias a la seguridad, desarrollando conexión con características distintas; cada conexión debería cumplir con los requerimientos del usuario. Las VPN's ofrecen seguridad site-to-site (punto a punto) además de velocidad y acceso a contenidos con un alcance a todos los usuarios.

VPN son redes privadas virtuales. Su nombre define su uso, si se toma como palabra clave virtual; palabra que engloba el uso de las VPN's en sí, para conectarte a otros dispositivos de red.

Figura 15. **VPN de punto a punto**



Fuente: Santos (2020*). Guía Oficial de Certificación CCNP and CCIE Security Core SCOR 350-701*. Consultado el 30 de agosto de 2021. Recuperado de ttps://pdfcoffee.com/ccnp-and-ccie-security-core-scor-350-701-official-cert-guide-pdf-free.html

Santos (2020) indica que las VPN proporcionan autenticación, integridad y cifrado para garantizar la confidencialidad de los paquetes que atraviesan una red desprotegida o Internet. Las VPN se diseñaron originalmente para evitar el costo de líneas arrendadas innecesarias. Sin embargo, ahora juegan un papel fundamental en la seguridad y, en algunos casos, en la privacidad. Las personas usan VPN para conectarse a su red corporativa, pero también las usan para su privacidad.

7.2.4.1. Protocolos para la implementación VPN

Durante el desarrollo de la implementación de las conexiones VPN's se han utilizado una diversidad de protocolos dentro de las cuales se incluyen las siguientes:

- GRE (*Generic Routing Encapsulation*)
- MPLS (conmutación de etiquetas multiprotocolo)

- Seguridad del protocolo de Internet (IPSec)
- Capa de *sockets* seguros (SSL)
- Servicios *open source* (Open VPN)

7.2.4.1.1. Tunnel GRE

Moisa (2019) indica en una publicación de la comunidad cisco, que el túnel GRE (desarrollado por cisco *System*) conecta dos puntos de red de manera virtual; es decir, son encapsulados de tal manera que únicamente los dos extremos lo puedan interpretar para que pueda viajar de un punto a otro en la red en un denominado túnel, una ruta superpuesta a la red subyacente.

Los túneles GRE permiten la comunicación entre dos puntos en dos dispositivos que atraviesan una red donde no se tiene acceso o control, posee restricciones como los son las redes públicas, redes corporativas o la red propia de los ISPs, los cuales brindan el servicio de internet. Este desarrollo es tan práctico que no significa que únicamente se pueda configurar túneles privados dentro de redes externas.

Cuando se crea un túnel GRE los datos se encapsulan con un encabezado GRE, pero no garantiza que los datos estén seguros; es por eso que las VPN GRE se complementa con un *stack* de protocolos llamados IPSec, que es el mecanismo más popular en la actualidad porque otorga seguridad punto a punto dentro de una red.

Figura 16. **Imagen básica del Tunnel GRE**

Fuente: Huawei (2021). *Conceptos básicos sobre Túnel GRE - HCIA R&S parte 1*. Consultado del 7 de septiembre de 2021. Recuperado de https://forum.huawei.com/enterprise/es/conceptos-b%C3%A1sicos-sobre-t%C3%BAnel-gre-hcia-r-s-parte-1/thread/741435-100235

La configuración básica del Túnel GRE posee la siguiente sintaxis:

- Interface Tunnel (0-2147483647)
- Ip address (la dirección IP del túnel, los dos extremos deberán pertenecer a la misma red lógica)
- Tunnel source (dirección IP de la interfaz {física | lógica } de origen)
- Tunnel destination (dirección IP de la interfaz de destino)

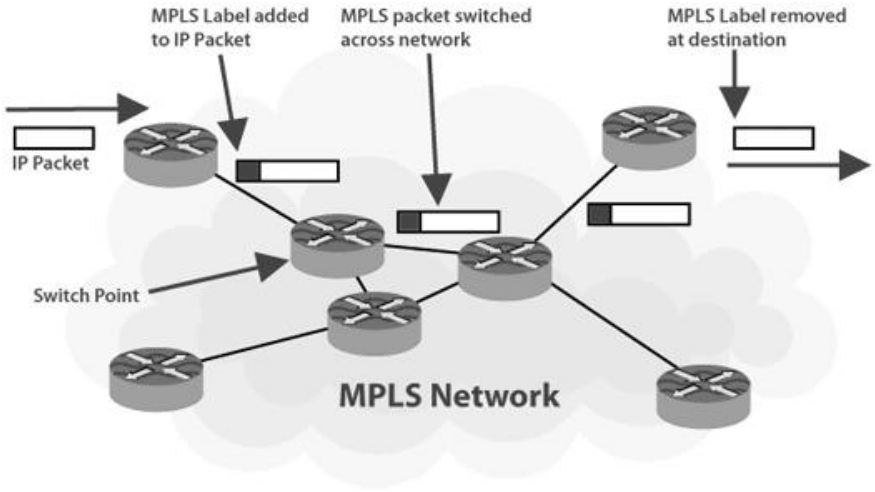
7.2.4.1.2. MPLS (Multiprotocol Label Switching)

Tapasco (2008) describe en su tesis de grado al protocolo MPLS como un estándar IP de conmutación de paquetes brinda un mejor rendimiento de CPU en el proceso de ingreso de datos al *router*, optimizando los recursos del *router* en la red. MPLS trabaja en la capa 2.5 del modelo OSI porque se encuentra en un punto intermedio a la capa de enlace de datos y la capa tres de red.

MultiProtocol Label Switching (MPLS, por sus siglas en inglés) fue desarrollado para mejorar el proceso de forwarding dentro de una red transporte, dentro de los beneficios que brinda se menciona la aplicación de QoS, ingeniería de tráfico, soporte de VPN's e interacción con varios protocolos (multiprotocolo); estas características son las que diferencian a las redes MPLS y las WAN.

MPLS se caracteriza principalmente por la integración de etiquetas al sistema de enrutamiento, vincula un prefijo a una etiqueta durante el *forwarding*. Dentro de los routers de borde se asignan etiquetas únicas a cada ruta (prefijos, direcciones IP).

Figura 17. **Red MPLS**



Fuente: Curvature (2021). *Tecnologías MPLS*. Consultado el 7 de septiembre de 2021. Recuperado de https://www.curvature.com/es/managed-it-services/mpls-technologies/.

Pepeinjak (2001) describe como el protocolo MPLS asigna etiquetas a los paquetes para su transporte a través de redes de paquetes o celulares. El proceso de *forwarding* consiste en intercambiar etiquetas dentro de la red. A los

paquetes se les asigna una etiqueta que le indica a los nodos en la red MPLS como ser procesado salto por salto y a seleccionar la mejor ruta de reenvió.

7.2.4.1.3. IPSec

De Luz (2021) redacta en una publicación del sitio web www.redeszone.net como el protocolo IPSec ha adquirido el reconocimiento de ser uno de los protocolos de seguridad más utilizado, por la garantía que ofrece al ser configurado dentro de un túnel VPN. Este protocolo es utilizado tanto en empresas como en sitios domésticos; es tan popular que existen en el mercado múltiples variantes que permiten la construcción de túneles VPN's, tanto de marcas propietarias como open source (Open VPN es el más reconocido).

El protocolo IPSec ofrece seguridad en la capa de red IP como también en la capa de transporte donde se alojan los protocolos TCP y UDP; gracias a esta característica la comunicación es segura entre una central y otra sucursal de la empresa. Por tal motivo IPSec es crucial en una VPN.

> Una característica muy importante de IPSec es que trabaja en la capa 3 de OSI (capa de red). Dentro de los protocolos VPN que trabajan en la capa 4 mencionaremos OpenVPN o WireGuard que basan su seguridad den TLS o DTLS respectivamente. (De Luz, 2001, p. 7)

IPSec trabaja en la capa de red, encapsula el paquete agregándole un nuevo encabezado de seguridad y los servicios de seguridad que ofrece son los descritos en la tabla siguiente:

Tabla I. **Servicios de seguridad IPSec**

Security Services	Description	Methods Used
Peer authentication	Verifies the identity of the VPN peer through authentication.	° Pre-Shared Key (PSK) ° Digital certificates
Data confidentiality	Protects data from eavesdropping attacks through encryption algorithms. Changes plaintext into encrypted ciphertext.	° Data Encryption Standard (DES) ° Triple DES (3DES) ° Advanced Encryption Standard (AES) The use of DES and 3DES is not recommended.
Data Integrity	Prevents man-in-the-middle (MitM) attacks by ensuring that data has not been tampered with during its transit across an unsecure network.	Hash Message Authentication Code (HMAC) function: ° Message Digest 5 (MD5) algorithm ° Secure Hash Algorithm (SHA-1) The use of MD5 es not recommended.
Replay detection	Prevents MitM attacks where an attacker captures VPN traffic and replays it back to a VPN peer with the intention of building an illegitimate VPN tunnel.	Every packet is marked with a unique sequence number. A VPN device keeps track of the sequence number and does not accept a packet with a sequence number it has already processed.

Fuente: Edgeworth, B., & Garza, R., & Gooley, J., & Hucaby, D. (2020). *Guía Oficial de Certificación CCNP and CCIE Enterprise Core ENCOR 300-401*. Consultado el 8 de septiembre de 2021. Recuperado de https://pdfcoffee.com/ccnp-and-ccie-enterprise-core-encor-350-401-official-cert-guidepdf-pdf-free.html

En el proceso IPSec se encapsulan los paquetes de datos con dos tipos diferentes de encabezados para gestionar el servicio que se describe en la tabla anterior. Estos encabezados son:

- Encabezado de autenticación: El encabezado de autenticación IP que agrega IPSec a los paquetes proporciona autenticación, integridad y protección contra ataques maliciosos por parte de agentes externos a la red. Este encabezado garantiza que los paquetes no sean modificados en su trayectoria a través de la red pública.

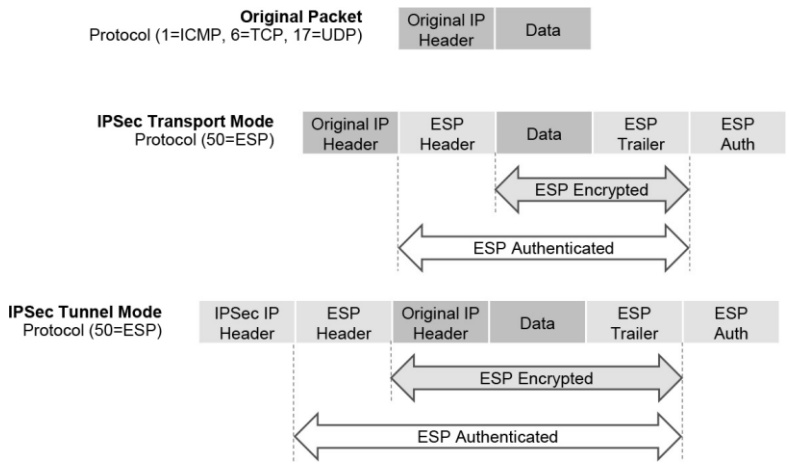
- Carga de seguridad de encapsulación (ESP): Encapsulating Security Payload (ESP) es el encabezado de seguridad ESP de IPSec que proporciona confidencialidad, autenticación y protección contra ataques maliciosos por parte de agentes externos a la red. El Payload hace referencia a los datos reales sin los encabezados, pero dentro de ESP, el payload o carga útil es el paquete que se encapsula dentro de IPSec. Existen dos maneras con las cuales IPSec transporta los paquetes:

- Modo de túnel: encripta todo el paquete original y agrega un nuevo conjunto de encabezados IPSec.

- Modo de transporte: cifra y autentica solo la carga útil del paquete.

En la gráfica se visualizan los dos modos de transporte que utiliza IPSec.

Figura 18. **Modos de transporte IPSec**



Fuente: Edgeworth, B., & Garza, R., & Gooley, J., & Hucaby, D. (2020). *Guía Oficial de Certificación CCNP and CCIE Enterprise Core ENCOR 300-401*. Consultado el 8 de septiembre de 2021. Recuperado de https://pdfcoffee.com/ccnp-and-ccie-enterprise-core-encor-350-401-official-cert-guidepdf-pdf-free.html

7.2.4.1.4. Capa de sockets seguros (SSL)

F5 (2021) describe en su sitio web “Una conexión VPN SSL es una red privada virtual (VPN) de capa de conexión segura (SSL), para crear una conexión segura y cifrada a través de su trayectoria” (p. 1).

Las redes VPN SSL fueron desarrolladas para complementar las complejidades de base que mostraba IPSec, principalmente a la falta de soporte brindada a los usuarios remotos como usuarios finales. Las VPN SSL dentro de sus características ofrece acceso remoto seguro por medio de un website, y la otra característica es el acceso remoto a la empresa a través de un túnel seguro SSL. Una VPN SSL ofrece seguridad y privacidad en el transporte de datos. Estas características permiten a los colaboradores o usuarios conectarse por medio de navegadores estándar como google Chrome o Firefox, sin la necesidad de instalaciones de terceros y conectarse a la IP del dispositivo configurado con la VPN.

Santos (2021) indica que “las VPN basadas en SSL aprovechan el protocolo SSL. SSL es un protocolo heredado y ha sido reemplazado por Transport Layer Security (TLS)” (p. 1002). Aunque en la actualidad las VPN’s basadas en TLS son llamadas VPN SSL. IETF desarrollo TLS para estandarizar todas las versiones de SSL. Es una solución práctica porque permite a cada colaborador o usuario acceder a los servicios empresariales como sitio web o email desde cualquier punto.

Santos (2021) señala que “HTTPS proporciona una comunicación web segura entre un navegador y un servidor web que admite el protocolo HTTPS. SSL VPN permite que los usuarios accedan a los servicios empresariales que pueden o no admitir HTTPS, o incluso HTTP” (p. 1009).

7.2.4.1.5. Servicios VPN de código abierto (OpenVPN)

Jiménez (2020) indica en una publicación de redeszone.com la importancia de las conexiones VPN y la oportunidad de encontrar soluciones gratuitas de código abierto. Son interesantes los beneficios que ofrece el código abierto.

De Luz (2020) describe que OpenVPN es un software de código abierto cliente/servidor multiplataforma, que se adapta a los OS's como Windows, Linux, macOs incluso a Android e iOS. Es importante considerar que muchos vendors lo incorporan a sus dispositivos. Con OpenVPN se pueden diseñar dos tipos de arquitecturas:

- VPN punto a punto: Permite la implementación de conexión con cifrado entre sedes o sucursales de manera segura.

- VPN con acceso remoto: Permite establecer un servidor VPN y varios clientes para conectarse de forma centralizada.

De Luz (2020) indica que si creamos un servidor en la oficina central nos permite conectarnos a una red pública de manera segura no importando si es cableada (ethernet) o inalámbrica (wifi), ya sea con cifrado WEP/WPA o sin él. Al tener instalado un servidor VPN en la central nos permite conectarnos a cualquier servicio instalado o que brinda una dependencia o sucursal o viceversa.

OpenVPN fue desarrollado con los protocolos SSL/TLS. OpenVPN trabaja en la capa 2 o 3; cuando trabaja en la capa de transporte podemos definir dos tipos de funcionamiento:

- TUN: Este controlador permite emular dos dispositivos punto a punto de capa 3, permitiendo crear túneles operando con el protocolo IP.

- TAP: Emula una interfaz ethernet dentro del funcionamiento de capa 2.

OpenVPN es un software de código abierto que permite todo tipo de criptografía, que proporcionará seguridad en el diseño de red para transportar los datos de un punto a otro a través de la red pública como internet.

7.2.5. *Cloud computing*

La computación en la nube o *cloud computing* como se conoce en el medio, es un tema bastante extenso y que crece a pasos agigantados en las infraestructuras de red. El *cloud* consiste en todos los servicios que están destinados a IT ahora alojados en centros de datos en algún punto del internet. A continuación, mencionaremos algunas características:

- Se automatiza la acción de liberar los recursos conforme la demanda lo exija, sin la intervención de los administradores.
- Las empresas pueden optimizar los recursos de manera dinámica, utilizando solo los recursos que se necesitan en ese momento de demanda.
- La negociación solo involucra los recursos utilizados.
- Los servicios prestados están garantizados por los proveedores.
- Existe la facilidad de brindar los servicios o datos desde o entre nubes, ya sea de forma manual o automática.

7.2.5.1. Tipos de nube

El *cloud* posee varios modelos y se usará el que satisfaga las necesidades de recursos. Entre los modelos se mencionan:

- Nube pública: se denomina pública porque cualquier usuario de internet tiene accesibilidad a ella. Los servidores están alojados dentro de la infraestructura de los ISPs (proveedores de servicio de internet); el cliente contrata únicamente el espacio de almacenamiento y ancho de banda que necesite. Un servicio que puede contratar de manera dinámica.

- Nube privada: se denominan privadas porque es la empresa la que brinda los servicios a los usuarios. Una empresa puede contar con su propia infraestructura de "red en la nube" instalada en sus propias instalaciones o en las de otra empresa que brinde el servicio como un proveedor externo.

- Nube híbrida: posee características de las dos anteriores. Se pueden priorizar los datos almacenando; los de menor importancia en la nube publica y el resto de datos críticos dentro de la nube privada. En cuanto a costos otorgados a la seguridad la distribución puede variar o el uso de la nube pública puede ir acorde a la demanda de espacio exigido para el cumplimiento de los requerimientos.

- *Multicloud*: es una configuración de nubes donde varias pueden trabajar simultáneamente, compartiendo distintos servicios. Esta característica se implementa, incluso cuando el requerimiento está enfocado en la disponibilidad o redundancia.

7.2.5.2. Servicios dentro del *cloud computing*

Cloud computing otorga distintos tipos de servicio los cuales son agrupados de esta manera:

Figura 19. **Servicios del Cloud**

Fuente: Neteris (2019). *Servicios en la Nube para Empresas*. Consultado el 9 de septiembre de 2021. Recuperado de https://neteris.com/tendencias/servicios-en-la-nube/

- IaaS (Infrastructure as a Service) o Infraestructura como Servicio: el proveedor externo proporciona todos los recursos, como servidores, almacenamiento en un centro de datos o los dispositivos para la red. El servicio que otorga el ISP abarca todos los recursos; el ISP cuenta con los recursos para proporcionar un entorno de virtualización. Con este servicio los usuarios hosts tienen mayor control, siendo el que más otorga este beneficio. IaaS es el más complicado por el nivel de configuración y de recursos que posee; ideal para desarrollar porque tiene la capacidad de brindar todo lo necesario. En la actualidad las marcas reconocidas que proporcionan un servicio IaaS son Microsoft (Azure) y Amazon (AWS).

- PaaS (Platform as a Service) o Plataforma como Servicio: Este modelo proporciona la base o plataforma para desarrollar aplicaciones, así como su mantenimiento y gestión. El servicio que ofrece el proveedor proporciona las bases donde estarán contenidas todas las aplicaciones, la plataforma donde estarán albergados, tanto las aplicaciones como los servicios http(s). La entidad que ofrece el servicio posee el control de la infraestructura de almacenamiento y no el usuario, como en el IaaS. Es dinámico, es decir, de acuerdo a las necesidades así se otorgan los recursos; por tanto, es totalmente escalable. Un ejemplo donde todo desarrollador puede realizar aplicaciones es el Google App Engine (de google), un ejemplo de PaaS.

- SaaS (Software as a Service) o Software como Servicio: Para este modelo, se proporciona el acceso al software alojado en la nube. Por tal razón, el cliente es responsable únicamente del software o aplicaciones alojadas; el mantenimiento, gestión, administración y soporte de la infraestructura es responsabilidad únicamente de la empresa donde todo se encuentra albergado. Para la infraestructura de este servicio, el cliente solo es dueño de la información y la empresa es la que proporciona el sitio donde almacenarla; un ejemplo de SaaS es Gmail o cualquier almacenaje de correo.

7.3. Monitoreo y diagnóstico

Monitorear la red proporciona información que permite identificar vulnerabilidades o fallos en tiempo real. Las herramientas para el monitoreo de una red como software o dispositivos de red permiten la identificación del buen funcionamiento, prever ataques maliciosos o sencillamente ratificar el buen funcionamiento de la misma de manera activa o proactiva.

7.3.1. Herramientas de diagnóstico de red

Muchas herramientas de diagnóstico de red están fácilmente disponibles. Esta sección cubre algunas de las herramientas más comunes disponibles y proporciona casos de uso y ejemplos de cuándo usarlas.

7.3.1.1. Ping

El Ping es la herramienta que brinda de solución de problemas más útiles y subestimadas en cualquier red. Cuando se sigue un flujo o lógica de solución de problemas, es fundamental cubrir primero los conceptos básicos. Por ejemplo, si no aparece una adyacencia de emparejamiento BGP, tendría sentido verificar la accesibilidad básica entre los dos pares antes de realizar cualquier solución de problemas o depuración de BGP de inmersión profunda. Los problemas a menudo radican en un nivel inferior del modelo OSI; el problema de la capa física, como la desconexión de un cable, se puede encontrar con un ping rápido.

7.3.1.2. *Traceroute*

Traceroute es otra herramienta de solución de problemas común. *Traceroute* generalmente se usa para solucionar problemas cuando se trata de determinar dónde está fallando el tráfico, así como qué ruta toma el tráfico en toda la red. *Traceroute* muestra las direcciones IP o los nombres DNS de los saltos entre el origen y el destino. También muestra cuánto tiempo se tarda en llegar al destino en cada salto, medido en milisegundos. Esta herramienta se usa con frecuencia cuando hay más de una ruta disponible para el destino o cuando hay más de un salto al destino.

7.3.1.3. Depuración

La depuración puede ser una parte muy poderosa para solucionar problemas complejos en una red. La depuración también es informativa. Uno de los casos de uso más comunes para la depuración es cuando es necesario ver las cosas a un nivel más profundo (cuando los protocolos de enrutamiento tienen problemas de adyacencia). Hay un flujo normal que se toma desde una perspectiva de solución de problemas, dependiendo del protocolo de enrutamiento. Sin embargo, hay momentos en que se han tomado estos pasos, y el problema no es evidente.

7.3.1.4. SNMP (Protocolo simple de administración de red)

Los equipos que operan dentro de la red a menudo tienen que confiar en las alertas que reaccionan dentro de los equipos de red para recibir una notificación cuando algo está sucediendo, como algo que falla o ciertos eventos que suceden en un dispositivo. La herramienta típica para esto es el Protocolo simple de administración de redes (SNMP). SNMP también se puede usar para configurar dispositivos, aunque este uso es menos común. Regularmente, cuando los equipos de ingeniería de redes necesitan configurar dispositivos, se utilizan herramientas de administración de configuración como Cisco Prime Infrastructure para marcas propietarias o Nagios Core y Zabbix para marcas de código abierto.

SNMP envía trampas no solicitadas a un recopilador SNMP o sistema de administración de red (NMS). Estas trampas son en respuesta a algo que sucedió en la red. Por ejemplo, se pueden generar trampas para eventos de estado de

enlace, autenticación de usuario inadecuada y fallas de suministro de energía. Estos eventos se definen en la base de información de administración (MIB) de SNMP. La MIB es un depósito de parámetros del dispositivo que se puede utilizar para activar alertas. Actualmente hay tres versiones de SNMP. A continuación, la tabla II enumera las versiones y sus diferencias.

Tabla II. **Comparación de la versión SNMP**

Version	Level	Authentication	Encryption	Result
SNMPv1	noAuthNoPriv	Community string	No	Uses a community string match for authentication
SNMPv2c	noAuthNoPriv	Community string	No	Uses a community string match for authentication
SNMPv3	noAuthNoPriv	Username	No	Uses a username match for authentication
SNMPv3	authNoPriv	Message Digest 5 (MD5) or Secure Hash Algorithm (SHA)	No	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms
SNMPv3	authNoPriv (requires the cryptographic software image)	MD5 or SHA	Data Encryption Standard (DES) or Advances Encryption Standard (AES)	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Allow specifyng the user-based Security Model (USM) with these encryption algorithms: DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard. 3DES 168-bit encryption. AES 128-bit, 192-bit, or 256-bit encryption.

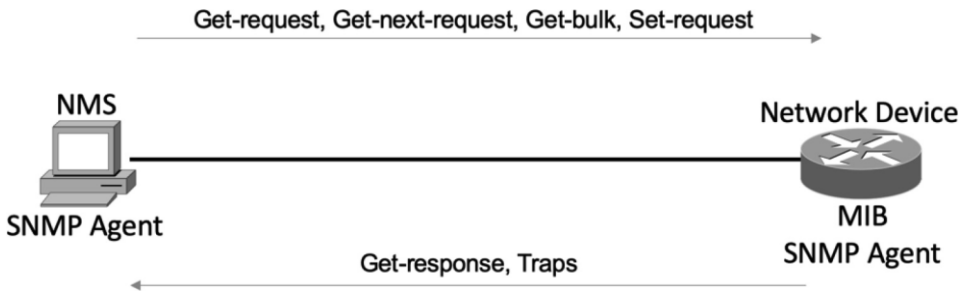
Fuente: Edgeworth, B., & Garza, R., & Gooley, J., & Hucaby, D. (2020). *Guía Oficial de Certificación CCNP and CCIE Enterprise Core ENCOR 300-401*. Consultado el 8 de septiembre de 2021. Recuperado de https://pdfcoffee.com/ccnp-and-ccie-enterprise-core-encor-350-401-official-cert-guidepdf-pdf-free.html

SNMPv3 proporciona la mayoría de las opciones de seguridad y capacidades de cifrado. SNMPv3 utiliza nombres de usuario y SHA o MD5 para la autenticación, lo que hace que SNMPv3 sea muy seguro en comparación con SNMPv1 o SNMPv2c. El uso de SNMP se considera la mejor práctica en producción. Sin embargo, los ejemplos en esta sección usan SNMPv2c por

simplicidad. SNMPv1 y SNMPv2c usan listas de acceso y una contraseña o cadena de comunidad para controlar qué administradores de SNMP pueden comunicarse con los dispositivos a través de SNMP. Estas cadenas de comunidad pueden ser solo de lectura (RO) o de lectura/escritura (RW). Como los nombres implican, solo lectura permite el sondeo de dispositivos para obtener información de los dispositivos. La lectura/escritura permite enviar información a un dispositivo o la configuración de un dispositivo. Es fundamental limitar el acceso SNMP a estos dispositivos mediante el uso de listas de acceso, como se mencionó anteriormente en esta sección. Sin listas de acceso, existe un riesgo potencial ya que los dispositivos podrían ser atacados por usuarios no autorizados.

Ahora que se han enumerado las operaciones básicas de SNMP, es importante mirar una MIB para comprender parte de la información o los valores que se pueden sondear o enviar trampas desde SNMP.

Figura 20. **Comunicación SNMP entre el host NMS y el dispositivo de red**



Fuente: Edgeworth, B., & Garza, R., & Gooley, J., & Hucaby, D. (2020). *Guía Oficial de Certificación CCNP and CCIE Enterprise Core ENCOR 300-401*. Consultado el 8 de septiembre de 2021. Recuperado de https://pdfcoffee.com/ccnp-and-ccie-enterprise-core-encor-350-401-official-cert-guidepdf-pdf-free.html

7.3.1.5. *Syslog*

Es una gran cantidad de información útil lo que generan los dispositivos, incluidos los mensajes enviados a la consola, al búfer de registro y a los recopiladores de registro del sistema fuera de la caja. De hecho, a los tres se les puede enviar el mismo tipo de mensaje o uno diferente. Por defecto, todos los mensajes de *syslog* se envían a la consola; así es como se muestran los comandos de depuración en el puerto de consola. Sin embargo, esto se puede ajustar, al igual que los mensajes que se envían al búfer de registro o al colector de registro del sistema. Es importante que antes de configurar dispositivos para enviar información de registro, la fecha y la hora del reloj deben configurarse correctamente para una hora precisa. Si no es así, las marcas de tiempo en todos los mensajes de registro no reflejarán la hora adecuada y precisa, lo que hará que la solución de problemas sea mucho más difícil porque no podrá correlacionar problemas con los registros utilizando las marcas de tiempo generadas. Asegurarse de que NTP esté configurado correctamente, ayuda con este problema.

Los mensajes que se generan tienen niveles de gravedad específicos asociados a ellos, pero estos niveles se pueden cambiar. El nivel de gravedad predeterminado de cada tipo de mensaje se enumera en la tabla.

Tabla III. **Niveles de gravedad de mensajes de syslog**

Level Keyword	Level	Description	Syslog Definition
emergencies	0	System unstable	LOG_EMERG
alerts	1	Inmediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT

Continuación de la tabla III

errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant conditions	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

Fuente: Edgeworth, B., & Garza, R., & Gooley, J., & Hucaby, D. (2020). *Guía Oficial de Certificación CCNP and CCIE Enterprise Core ENCOR 300-401*. Consultado el 8 de septiembre de 2021. Recuperado de https://pdfcoffee.com/ccnp-and-ccie-enterprise-core-encor-350-401-official-cert-guidepdf-pdf-free.html

Estos mensajes se pueden usar para proporcionar información valiosa al personal de operaciones de la red, o pueden ser tan abrumadores que dificultan el tamizaje para encontrar o identificar un problema. Para encontrar una falla no basta con tener configurado *Syslog*, todavía se necesita la habilidad adecuada para poder mirar los mensajes y determinar la causa raíz del problema. *Syslog* es, sin embargo, muy útil para guiar hacia el problema en cuestión.

7.3.1.6. NetFlow y NetFlow flexible

Recopilar estadísticas sobre una red durante sus operaciones no solo es útil sino importante. Reunir información estadística sobre los flujos de tráfico es necesario por varias razones. Algunas empresas, como los proveedores de servicios, lo usan para facturar a los clientes. Otras empresas lo utilizan para determinar si el tráfico fluye de manera óptima a través de la red. Algunos lo usan para solucionar problemas si la red no funciona correctamente. NetFlow es muy versátil y proporciona una gran cantidad de información sin mucha carga de configuración. Dicho esto, NetFlow tiene dos componentes que deben

configurarse: NetFlow Data Capture y NetFlow Data Export. Las estadísticas de tráfico son capturadas por NetFlow Data Capture. Un recopilador de NetFlow sustrae los datos de NetFlow Data Export.

Para habilitar NetFlow desde un enfoque de diseño hay que considerar lo siguiente. Primero, los recursos de memoria que consume NetFlow. Las estadísticas de tráfico se capturan en la memoria caché. El tamaño predeterminado del caché es específico de la plataforma y debe investigarse antes de habilitar NetFlow. Este es especialmente el caso con plataformas más antiguas que potencialmente tienen menos recursos de memoria disponibles.

Los datos entrantes y salientes del dispositivo son capturados por NetFlow.

Tabla IV. **Descripción del tráfico de entrada y salida de NetFlow**

Ingress	Egress
IP to IP packets	NetFlow accounting for all IP traffic packets
IP to Multiprotocol Label Switching (MPLS) packets	MPLS to IP packets
Frame Relay terminated packets	
ATM terminated packets	

Fuente: Edgeworth, B., & Garza, R., & Gooley, J., & Hucaby, D. (2020). *Guía Oficial de Certificación CCNP and CCIE Enterprise Core ENCOR 300-401*. Consultado el 8 de septiembre de 2021. Recuperado de https://pdfcoffee.com/ccnp-and-ccie-enterprise-core-encor-350-401-official-cert-guidepdf-pdf-free.html

7.3.1.7. Tecnologías de Análisis de Puertos Conmutados (SPAN)

El famoso dicho sobre tres lados de cada historia es válido cuando se solucionan problemas basados en la red, donde existen las perspectivas del dispositivo local, el dispositivo remoto y lo que se transmite por cable. Independientemente de si un dispositivo es un enrutador, un cortafuego, un equilibrador de carga o una computadora, a menudo existen herramientas que permiten la resolución local de procesos en el dispositivo.

Comprender lo que se transmitió en el cable puede ayudar a detectar problemas. Obtener la perspectiva de lo que sucede en el cable puede ser más complicado. Cuando el problema parece ser un problema de Capa 2, hay algunas opciones:

- Inserte un divisor entre los dispositivos. Los divisores son generalmente aplicables a las conexiones ópticas, ya que dividen la luz a través de un prisma. La fuente original permanece intacta y se puede enviar una segunda transmisión a un analizador de tráfico.

- Configure el dispositivo de red para reflejar los paquetes en el nivel del plano de datos a un destino adicional. El destino puede ser un puerto local o un puerto remoto que esté conectado a un analizador de tráfico.

- Inserte un interruptor entre los dos dispositivos y luego configúrelo para reflejar el tráfico transitorio en un analizador de tráfico.

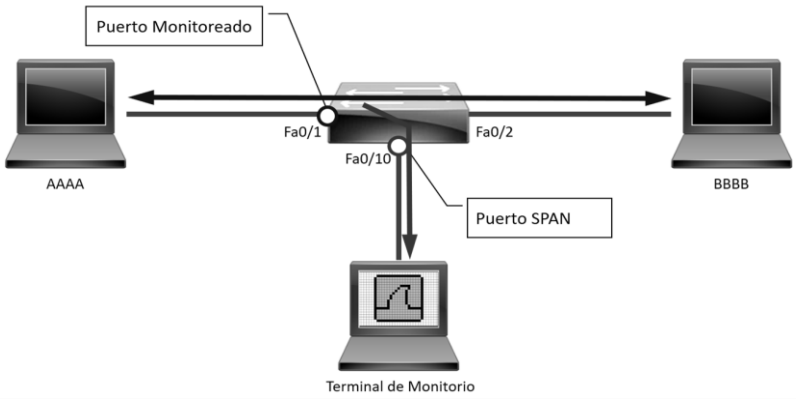
Los *switches catalyst* proporcionan el analizador de puertos conmutados (SPAN), que permite capturar paquetes utilizando las dos segundas opciones anteriores mediante las siguientes técnicas:

- Analizador local del puerto conmutado: puede capturar los datos entrantes y salientes de la red local en un conmutador y enviar una copia de los datos de la red a un puerto local conectado a algún tipo de analizador de tráfico.

- Analizador de puerto de conmutación remota (RSPAN): puede capturar el tráfico de red en un conmutador remoto y enviar una copia del tráfico de red al conmutador local, a través de la capa 2 (conmutación) hacia un puerto local conectado a algún tipo de analizador de tráfico.

- Analizador remoto del puerto conmutado (ERSPAN): puede capturar el tráfico de red en un dispositivo remoto y enviar el tráfico al sistema local a través de la capa 3 (enrutamiento), hacia un puerto local conectado a algún tipo de analizador de tráfico.

Figura 21. **Topología de SPAN**



Oscar Gerometta (2018). *SPAN – Gráfica*. Consultado el 9 d1e septiembre de 2021. Recuperado de http://librosnetworking.blogspot.com/2018/01/span-grafica.html

7.3.1.8. IP SLA

IP SLA es una herramienta que viene por defecto en el IOS de Cisco y que permite monitorear la red y realizar un análisis continuo de varios aspectos. Los diferentes tipos de sondas que se pueden configurar para monitorear el tráfico dentro de un entorno de red incluyen lo siguiente:

- Retraso (ida y vuelta e ida)
- Jitter (direccional)
- Pérdida de paquete (direccional)
- Secuencia de paquetes (pedido de paquetes)
- Camino (por salto)
- Conectividad (direccional)
- Tiempo de descarga del servidor o sitio web
- Puntajes de calidad de voz

IP SLA ha demostrado ser una herramienta muy útil, ya que proporciona una variedad de opciones de monitoreo flexibles. Por lo general, cualquier SLA recibido de un SP (Service Provider) solo monitorea o garantiza el tráfico a medida que viaja dentro de la red del SP. Esto no proporciona un SLA o visibilidad de extremo a extremo, para el caso. Sin embargo, IP SLA es una herramienta robusta que puede ayudar con la resolución de problemas.

7.3.1.9. Cisco DNA Center Assurance

Las redes se han vuelto muy complejas. La afluencia de dispositivos móviles a la red agota los recursos. El factor de la seguridad ha aumentado su

valor dentro de la red, y los usuarios esperan una mejor experiencia. Los clientes exigen una forma simple de administrar las operaciones del día 0–2 y requieren un enfoque escalable y simple para ejecutar la red. Cisco DNA Center Assurance proporciona una herramienta para manejar los requisitos más relevantes del cliente. Tradicionalmente, se requerían múltiples herramientas de administración para cubrir todos los procesos empresariales en términos de administración, operación y solución de problemas de red. Todo esto cambia con Cisco DNA Center Assurance. Desde un alto nivel, Cisco DNA Center Assurance ofrece algunas de las siguientes capacidades (así como muchas más):

- Configuración del tejido Cisco SD-Access
- Software de gestión de imágenes (SWIM)
- Aprovisionamiento simplificado para dispositivos
- Gestión de red inalámbrica
- Políticas de seguridad simplificadas.
- Plantillas de configuración
- Integración de terceros
- Aseguramiento de la red
- Conecta y reproduce

Esta sección cubre algunos de los flujos de trabajo con los que Cisco DNA *Center Assurance* está diseñado para ayudar a las empresas. Normalmente, cuando surge un problema en la red, se crea un *ticket* de servicio de asistencia. Sin embargo, cuando el equipo de operaciones de la red obtiene el *ticket* asignado, el problema se resuelve por sí solo o la información provista en el ticket para ayudar a solucionar el problema está obsoleta o desactualizada. Otro escenario típico es que los usuarios dicen cosas como "el martes pasado a las 3 p.m. No pude acceder a la red inalámbrica ". En una red tradicional, si alguien dice que tuvo un problema la semana pasada, no hay mucho que se pueda hacer

al respecto. Sin embargo, Cisco DNA *Center Assurance* tiene *Network Time Travel*, y es tan genial como parece. *Network Time Travel* actúa como una grabadora de video digital (DVR) para la red. Pero en lugar de grabar televisión y permitir que el usuario reproduzca programas en un momento posterior, *Network Time Travel* registra lo que está sucediendo en el entorno, utilizando telemetría de transmisión, y puede reproducir algo que sucedió en el pasado. También puede mostrar cómo está funcionando la red ahora, así como usar cosas como sensores para proporcionar análisis predictivos sobre cómo funcionará la red en el futuro.

7.4. Sistemas de gestión y mantenimiento

La gestión y mantenimiento son aspectos vitales en toda empresa de producción, la tecnología brinda un mejor desempeño de ambos.

7.4.1. Sistema ERP en los procesos de logística comercial

La demanda comercial exige a las empresas actualizarse tecnológicamente para ser competitivas y optimizar los procesos comerciales, buscando ofrecer mejores resultados. Las empresas deberán incorporarse a la evolución tecnológica para realizar sus procesos, impulsando una escalabilidad en su accionar comercial, y tener claro todo el panorama de sus operaciones para que sus colaboradores tengan el mejor rendimiento.

SAP BO es un software de soporte que permite controlar todos los recursos empresariales de manera versátil, es un software robusto con varias aplicaciones que proporciona datos reales y específicos en toda la cadena de suministros, automatizando las tareas simplifica la gestión; centralizándola en una base de datos. Datos que puede ser mostrados a través de reportes

automatizados en tiempo real, por medio de la red desde cualquier punto de acceso.

Permite el control de gastos de mantenimiento y operación de cada departamento. Incorporando los datos necesarios para el análisis de contabilidad y finanzas, ubica los pedidos, las entregas y las ventas en una sola plataforma, para agilizar y controlar los movimientos de inventarios; es un soporte con diversas funciones de análisis y reportes en tiempo real.

Da un soporte para administrar al personal dentro de las empresas con continuos cambios o rotaciones, programación de horarios y contrataciones. Cualquier colaborador con autoridad y accesos puede gestionar las ausencias y reemplazos del personal. Además, es una herramienta ideal para el área de logística por las diversas funciones que posee. Integra seguridad a los datos que se registran, tanto del personal como del cliente, para que los encargados de la gestión tengan acceso a los recursos aun después de algún fallo eléctrico, una violación a las políticas de seguridad o cualquier otro evento que provoque un fallo.

7.4.2. SAP BUSSINES ONE (SAP BO)

SAP BO es una solución tan versátil que se adapta a cualquier empresa no importando el tipo de procesos que en ella se realicen. La importancia que posee un software con sus características es que ayuda a mejorar la gestión de la industria y a la obtención de datos, ya que posee una estructura tan amplia que se adapta a todos los departamentos; esto permite la toma de decisiones y elimina la incertidumbre, agilizando las tareas administrativas. SAP BO es un

software que da soporte a una base de datos robusta con toda la información empresarial.

SAP BO brinda una ventaja competitiva a toda empresa que posee el software instalado, por todos los atributos que posee y las funcionalidades para realizar tareas complejas. Es un software de gestión empresarial que permite el acceso rápido a la información y permite un detallado análisis a la hora de toma de decisiones gerenciales.

Figura 22. **Descripción SAP BO**

Fuente: Inforges (2018). *Que es SAP*. Consultado el 9 de septiembre de 2021. Recuperado de https://www.inforges.es/Blog/iblog/2018/04/13/que-es-sap-business-one

7.4.2.1. Características de SAP Business One

SAP Business One tiene todas las características que cubren las necesidades del rigor de la empresa:

- Es asequible y con valor de uso reducido.
- El software posee una solución para cada uno de los departamentos en la empresa.
- Disponible para ponerlo en producción al ser requerido.
- Es un software robusto que satisface los procesos empresariales.
- Tiene soluciones modulares para cada necesidad del departamento.
- Cuenta con versiones en varios idiomas que se adapta a las necesidades empresariales y cuenta con asistencia multidivisa.

7.4.2.2. Ventajas que aporta SAP *Business One*

- Escalabilidad y puede soportar toda la información relevante de la empresa concentrada en un solo punto.
- *Data analytics* integrado es una función que responde a las interrogantes del negocio.
- Es amigable al usuario.
- Permite a los colaboradores conectarse y trasferir datos por medio de una aplicación móvil.
- Está diseñado para satisfacer las necesidades PYME.
- Permite la conectividad a los procesos empresariales.

7.4.2.3. Sistema ERP

Un sistema ERP (*Enterprise Resource Planning*) es una estructura de planificación empresarial. Es un software orientado a almacenar todos los datos recabados de cada uno de los procesos realizados dentro de la empresa; fue diseñado para otorgarle a los administradores empresariales una herramienta capaz de darle un enfoque completo del funcionamiento del negocio. Con un software como este es posible tomar decisiones de manera rápida, eficiente y eficaz en tiempo real. De esta manera se canaliza un crecimiento y la rentabilidad empresarial.

Pensar en una empresa gestionada por un software que le facilite el proceso, es pensar en esa empresa con un ERP instalado y administrable. El sistema facilita la operación de los procesos centrales de la empresa: recursos humanos, finanzas, suministros, producción, compras, facturación, gerencia, contabilidad, entre otros, e integra todos los departamentos en un solo sistema de gestión.

Un sistema ERP se ha convertido en una solución ideal para todas las empresas nuevas y las ya establecidas, para ser competitivas en el mercado, porque le permite mantener el control de los departamentos de compras, ventas, finanzas y almacén, entre otros.

7.4.3. Mantenimiento de una red

Una de las tareas más importantes en toda red ethernet es el mantenimiento que se pueda proporcionar para garantizar la disponibilidad, seguridad y escalabilidad.

7.4.3.1. Mantenimiento preventivo de la red

Tal vez es uno de los mantenimientos más importantes y uno de los procesos cruciales dentro de cualquier empresa. Consiste en realizar inspección visual como prueba no destructiva dentro de la empresa. Se basa en realizar visitas e inspeccionar el estado del cableado estructurado de toda la red que cubre oficinas y planta, analizar el rendimiento de los dispositivos intermedios, inspeccionar los circuitos de corriente de alimentación eléctrica, inspeccionar cada uno de los puntos de red, canalización y nodos finales, para predecir posibles fallas y realizar los cambios pertinentes que las prevean.

Diseñar bitácoras bien planificada, registros técnicos, antecedentes de cada dispositivo dentro de la red. Mantener actualizados los planos de la red donde se detalla cada uno de los servicios: telefonía, datos, almacenamiento, telemetría, conexiones y acometidas de la red eléctrica, centro de datos, routers, switches y firewall, entre otros.

7.4.3.2. Mantenimiento predictivo de una red

El mantenimiento predictivo de la red permite obtener un diagnóstico del sistema previo a que ocurra una falla. Aquí es donde adquieren importancia los mecanismos de diagnóstico y monitoreo de la red, que prevén la deficiencia e inconsistencias de la red ethernet. Lo mejor de este mantenimiento es que predice lo que acontecerá.

Es esencial contar con sistema de monitorización porque es la mejor manera para visualizar el desempeño de la red. Se pueden automatizar ciertos

procesos o indicadores que identifiquen fallos o que garanticen su buen desempeño.

7.4.3.3. Mantenimiento correctivo de una red

Este es el mantenimiento que todos desean evitar, por el trabajo que genera o los costos que producen. Consiste en cambios de componentes, fallas en el cableado, irregularidades en la energía, actualización de firmware, actualización de software, sistemas operativos, máquinas virtuales y agregación de hosts, entre otros. Toda falla que provoque que la red se caiga, desbalanceo de carga, acceso inapropiado por parte de los colaboradores, malas conexiones, cables en mal estado.

7.4.4. Metodología de migración

Es importante el proceso debido a los cambios establecidos. Cuando la migración de cualquier actualización de red se basa en normas y estándares y se respalda bajo buenas prácticas procedimentales, se garantiza el buen funcionamiento de la red después de la migración, tanto como infraestructura como la seguridad de los usuarios finales al sentirse cómodos con los servicios que garantiza la actualización.

Cabe destacar que el administrador deberá estar al tanto de los cambios para dar apoyo en la migración y que esta no afecte su rendimiento. Por lo que al realizar la actualización se debe cubrir ciertos aspectos como:

- Técnicos de terceros que dañen o corten los cables.

- Falta de uso de las normas y estándares para los cables de corriente y de datos dentro de una canaleta por parte de los electricistas.
- Mala colocación de tomacorrientes para dispositivos que no pertenecen al área de *networking*.
- Pérdida de la señal por interferencia en los cables.
- Mala práctica de reingeniería del cableado estructurado.
- Cables de teléfono cruzados.
- Mala configuración de las conexiones a internet.
- Dispositivos de su red que muestren fallas debido a una mala configuración.
- Existen numerosos casos que pudiesen afectar a la red.

Es importante enlistar las operaciones a la hora de realizar ventanas de mantenimiento:

- La reparación de la falla.
- Nuevas instalaciones o actualizaciones.
- Sustitución de dispositivos o configuraciones.
- *Testing* de conectividad.
- Etiquetado de dispositivos e identificación de conexiones.
- Actualización de IOS, *firmware*.
- Diagnóstico del sistema y presentación de reportes.

8. PROPUESTA DE ÍNDICE DE CONTENIDOS

1.2.4. VPN (Virtual private network)

1.2.4.1. Protocolos para la implementación de VPN

1.2.4.1.1. Tunnel GRE

1.2.4.1.2. MPLS (Multiprotocol Label Switching)

1.2.4.1.3. IPSec

1.2.4.1.4. Capa de sockets seguros (SSL)

1.2.4.1.5. Servicios VPN de código abierto (OpenVPN)

1.2.5. Cloud Computing

1.2.5.1. Tipos de nube

1.2.5.2. Servicios dentro del cloud computing

1.3. Monitoreo y diagnostico

1.3.1. Herramientas de diagnóstico de red

1.3.1.1. Ping

1.3.1.2. Traceroute

1.3.1.3. Depuración

1.3.1.4. Protocolo simple de administración de red (SNMP)

1.3.1.5. Syslog

1.3.1.6. NetFlow y NetFlow flexible

1.3.1.7. Tecnologías de Análisis de Puertos Conmutados (SPAN)

1.3.1.8. IP SLA

1.3.1.9. Cisco DNA Center Assurance

1.4. Sistemas de Gestión y Mantenimiento

1.4.1. SAP BUSSINES ONE

1.4.1.1. Características de SAP Business One

1.4.1.2. Ventajas que aporta SAP Business One

1.4.1.3. Sistema ERP

9. METODOLOGÍA

La metodología de la investigación es la disciplina de conocimiento encargada de elaborar, definir y sistematizar el conjunto de técnicas, métodos y procedimientos que se deben seguir durante el desarrollo de un proceso de investigación.

El método será descriptivo porque el nivel de investigación se orientará a describir el comportamiento de las variables de estudio.

9.1. Diseño

Dado que el objetivo del estudio será analizar el diseño de una propuesta de implementación de red industrial, a nivel de acceso con tecnología SDN, a la infraestructura de red de una planta de producción de alimentos ubicada en la Antigua Guatemala, se recurrirá a un diseño no experimental que se aplicará de manera transversal; considerando que el tema de investigación tiene un sustento teórico suficiente, se procedió a realizar una investigación de tipo descriptivo, para conocer a detalle la forma en que el tipo de topología y configuración de la red ethernet afectaba el desempeño de los procesos comerciales que se desarrollan dentro de la empresa.

El diseño de la investigación no es experimental porque no se manipulan variables en laboratorio como parte de la información, únicamente se realizará la revisión documental necesaria, para proponer el procedimiento en una actualización de la infraestructura de la red empresarial interna y los mecanismos para su mantenimiento informático. Los diseños de investigación transversales

recolectan datos para ser analizados por tiempos determinados. Los datos necesarios serán obtenidos con software capaz de medir el desempeño de la red ethernet, con el objetivo de hacer un análisis en los puntos donde se planteará efectuar mejoras.

9.2. Paradigma

La investigación tendrá como base epistemológica el paradigma socio-critico, y el método analítico como guía o ruta crítica para su elaboración. La elección de este paradigma es porque es el que mejor se adapta a las características y necesidades de la investigación.

Este paradigma se fundamenta en la satisfacción social con base en el apoyo técnico, con miras a la transformación de la realidad tecnológica existente.

El paradigma sociocrítico y su consecuente enfoque cualitativo permitirá comprender la percepción de los usuarios o colaboradores, sobre la metodología operacional de la red IP de la planta de producción ubicada en la ciudad colonial de la Antigua Guatemala, así como la opinión de los dirigentes en cuanto a los beneficios que otorga a la productividad, con el objetivo de generar mayores ganancias.

9.3. Enfoque

Dado que no se busca comprobar una hipótesis, así como los objetivos trazados, el presente trabajo será diseñado bajo el planteamiento metodológico del enfoque cualitativo, puesto que este es el que mejor se adapta a las características y necesidades de la investigación.

El enfoque cualitativo hace uso de la recolección de la información sin ningún análisis numérico exacto, para definir o redactar preguntas acerca de la investigación que ayuden en el proceso de interpretación de fenómenos, por la siguiente razón: cualitativo porque utilizará la revisión documental al estudiar los antecedentes del problema; del enfoque cualitativo se tomará la técnica de Grupo Focal o *Focus Group* para describir la percepción del funcionamiento de la infraestructura de red, siendo la fuente de estudio. Se efectuarán entrevistas para obtener la opinión de los colaboradores que interactúan con la misma.

9.4. Tipo

El tipo de estudio es evolutivo porque busca responder interrogantes expuestas por el planteamiento del problema, basado en los datos de registro y con la toma de datos actuales; realizar un análisis sobre las desviaciones de resultados para indicar la necesidad de implementar un diseño que mejoren los resultados.

9.5. Alcance

El alcance metodológico es descriptivo porque no se realizará alguna implementación, solo se presentará una propuesta porque se cuenta con datos de registro (al realizar la instalación), que permiten evaluarla. Además, se posee lo necesario para un estudio y determinar procedimientos operativos.

9.6. Variables e indicadores

Las variables e indicadores a estudiar durante el proceso de esta investigación serán las que determinen el análisis de la investigación. El método a través del cual serán medidas o analizadas las variables, de acuerdo con los indicadores y técnicas, se describen en la siguiente tabla**.**

Tabla V. **Operativización de variables**

Objetivo	Variable	Tipo de variable	Indicadores	Técnica	Plan de Tabulación
Centralizar el control de operaciones IT para eliminar inconsistencias en los datos físicos y digitales y que todo sea gestionado desde la planta de producción en Guatemala y de esta manera acceder al sistema de gestión de SAP BO en la planta	Configuraciones, ancho de banda, seguridad	Dependiente, nominal, cuantitativa, cualitativa	Latencia, jitter, logs	Monitoreo	Registros
Utilizar los beneficios que brinda la tecnología SDN, automatizando las operaciones desde una interfaz grafica que disminuyan la cantidad de errores por configuraciones manuales.	Configuraciones, ancho de banda, seguridad, tecnología, costos	Dependiente, nominal, cuantitativa, cualitativa	Latencia, jitter, logs	Monitoreo	Registros
Emplear procedimientos de gestión y monitoreo de la red en la capa de acceso, que brinden la creación de políticas de seguridad mas consistentes para los colaboradores.	Conectividad, seguridad, KPIs	Dependiente, nominal, cuantitativa, cualitativa	Latencia, jitter, logs, Informes	Monitoreo	Registros
Identificar los principales problemas para la implementación y gestión de la infraestructura de red, evaluando la gestión y socialización entre departamentos.	KPIs, información, plan de mantenimiento	Dependiente, nominal, cuantitativa, cualitativa	KPIs, tiempo	Políticas, reuniones, charlas	Registros

Fuente: elaboración propia, hecho con Microsoft Excel.

9.7. Fases

Fase 1: Revisión documental para la realización de los antecedentes y marco teórico.

Fase 2: Definir los equipos que satisfacen el nivel tecnológico para la implementación de la red SDN; clasificar y analizar toda la red para determinar si la infraestructura existente satisface las necesidades. Reunión con el personal a cargo para verificar el *checklist* de las posibles pautas a implementar y analizar el alcance de cada una de ellas.

Fase 3: Desarrollar la propuesta de red SDN, determinar configuraciones, costos económicos y tecnológicos, diseñar la propuesta de red SDN, tomando en cuenta los recursos *open source* disponibles, y las variantes comerciales disponibles que satisfagan el éxito de la implementación.

Fase 4: Capacitar a los colaboradores que tendrán acceso a la red, diagnosticar el funcionamiento y monitorizar la red para garantizar su desempeño.

9.8. Resultados esperados

Diagnóstico del rendimiento de la infraestructura de red actual y describir las actividades que se deben agregar a los procesos que se realizan a través de la red, así como las gestiones administrativas que se pudieran automatizar dentro de los recursos de red interna.

Establecer una clasificación de los dispositivos de red, circuitos de cableado estructurado y dispositivos finales que conforman la red empresarial, según su funcionalidad y características capaces de ser reutilizables en la actualización de red para una infraestructura SDN.

Se espera tener un listado de todas las operaciones que generan retardos en los procesos operativos, de logística y de generación de reportes de información.

Se espera definir un plan de monitoreo y mantenimiento de la red SDN de la red empresarial local y del punto donde se alberga la base de datos que contiene toda la información de SAP BO, administrada por la planta.

Finalmente, se espera poder establecer el diseño de la propuesta de la infraestructura de la red de acceso, utilizando tecnología SDN que corresponde al trabajo final de investigación, con base en las directrices establecidas por la Escuela de Estudios de Postgrado de la Facultad de Ingeniería.

9.9. Población y muestras

Se va a utilizar la población en su totalidad; todos los datos obtenidos durante el proceso de medición serán parte del análisis de resultados.

10. TÉCNICAS Y ANÁLISIS DE LA INFORMACIÓN

En la primera fase se analizará la información obtenida en la revisión documental durante el proceso de la investigación, para determinar su utilidad y alcanzar los objetivos. Esta información será obtenida por medio de la observación directa, toma de datos generados por los equipos de red, entrevistas y revisión de documentos (fichas técnicas).

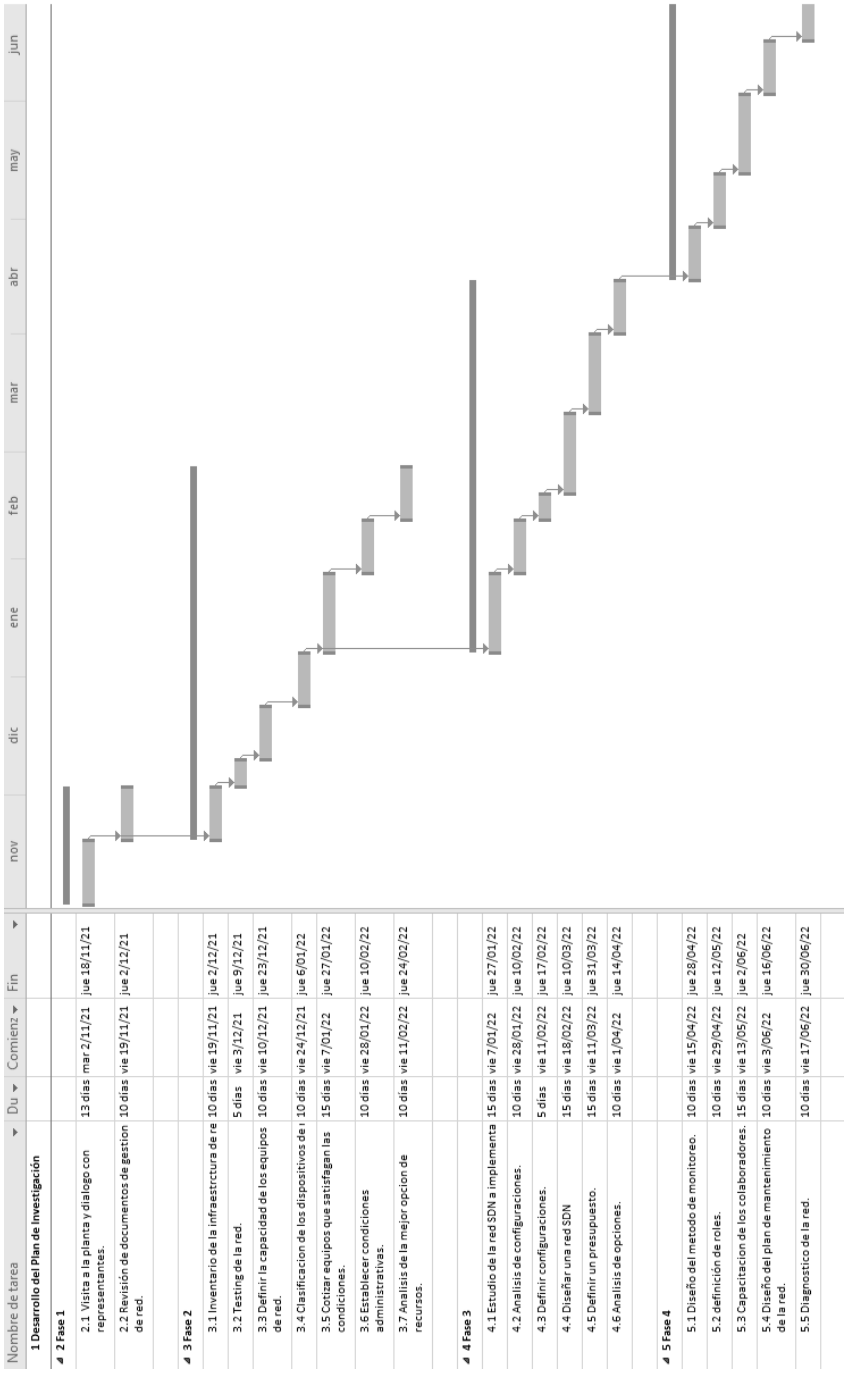
En la segunda fase se analizará y clasificará la información, respaldados por las fichas de los fabricantes a los equipos capaces de ser integrados a una red SDN; además de todos los complementos que permitan la conectividad, por ejemplo, cableado estructurado, licenciamiento, colaboradores y aspectos legales y técnicos. Reunión con algún representante a cargo para la verificación de las actividades a realizar, que permita la implementación de una red SDN y las competencias de los involucrados en la operatividad de la red.

La tercera fase consiste en desarrollar la propuesta de red SDN bajo un criterio de costos económicos y tecnológicos; el diseño de la propuesta deberá satisfacer los recursos a utilizar, como *open source* disponibles en el mercado, bajo las variantes comerciales de licenciamientos, aspectos legales y administrativos. El estudio de implementar los servidores en la nube. El análisis de un plan de mantenimiento y monitoreo de la red de manera centralizada (departamento de IT ubicado en la central de producción en la Antigua, Guatemala).

La cuarta fase consistirá en la presentación de un plan de buenas prácticas de adaptación a la nueva red, lo que incluye la capacitación al personal a cargo

y adiestramiento de todos los colaboradores involucrados en el manejo de datos y adquisición de los mismos (usuarios finales). Diagnosticar el desempeño de la red y los cambios realizados a la misma, así como el monitoreo de la red. Presentación del diseño de red físico y lógico, como el inventario de los equipos reciclados y los equipos nuevos necesarios para la implementación de la red SDN.

11. CRONOGRAMA DE ACTIVIDADES



Nombre de tarea	Du	Comienz	Fin
1 Desarrollo del Plan de Investigación			
2 Fase 1			
2.1 Visita a la planta y dialogo con representantes.	13 días	mar 2/11/21	jue 18/11/21
2.2 Revisión de documentos de gestion de red.	10 días	vie 19/11/21	jue 2/12/21
3 Fase 2			
3.1 Inventario de la infraestrctura de re	10 días	vie 19/11/21	jue 2/12/21
3.2 Testing de la red.	5 días	vie 3/12/21	jue 9/12/21
3.3 Definir la capacidad de los equipos de red.	10 días	vie 10/12/21	jue 23/12/21
3.4 Clasificacion de los dispositivos de i	10 días	vie 24/12/21	jue 6/01/22
3.5 Cotizar equipos que satisfagan las condiciones.	15 días	vie 7/01/22	jue 27/01/22
3.6 Establecer condiciones administrativas.	10 días	vie 28/01/22	jue 10/02/22
3.7 Analisis de la mejor opcion de recursos.	10 días	vie 11/02/22	jue 24/02/22
4 Fase 3			
4.1 Estudio de la red SDN a implementa	15 días	vie 7/01/22	jue 27/01/22
4.2 Analisis de configuraciones.	10 días	vie 28/01/22	jue 10/02/22
4.3 Definir configuraciones.	5 días	vie 11/02/22	jue 17/02/22
4.4 Diseñar una red SDN	15 días	vie 18/02/22	jue 10/03/22
4,5 Definir un presupuesto.	15 días	vie 11/03/22	jue 31/03/22
4.6 Analisis de opciones.	10 días	vie 1/04/22	jue 14/04/22
5 Fase 4			
5.1 Diseño del metodo de monitoreo.	10 días	vie 15/04/22	jue 28/04/22
5.2 definición de roles.	10 días	vie 29/04/22	jue 12/05/22
5.3 Capacitacion de los colaboradores.	15 días	vie 13/05/22	jue 2/06/22
5.4 Diseño del plan de mantenimiento de la red.	10 días	vie 3/06/22	jue 16/06/22
5.5 Diagnostico de la red.	10 días	vie 17/06/22	jue 30/06/22

Fuente: elaboración propia, hecho con Microsoft Project.

12. FACTIBILIDAD DE LA INVESTIGACIÓN

Es factible el estudio de investigación para el diseño de una propuesta de implementación de red industrial, a nivel de acceso con tecnología sdn, a la infraestructura de red de una planta de producción de alimentos, porque se cuenta con todos los recursos necesarios para ejecutar cada una de las etapas, logrando alcanzar los objetivos de este trabajo y el tiempo definido en el cronograma. El financiamiento del proyecto será compartido entre la jefatura y el investigador.

Para el recurso humano, será imprescindible el apoyo de un representante asignado por gerencia y colaboradores del departamento de IT para ingresar a las instalaciones del cuarto de los equipos de red o dispositivos de acceso, entrevistas con el técnico de mantenimiento para acceder a la información requerida como registros almacenados en el servidor, manuales, diagramas, procedimientos, inventarios de equipos, procedimientos y experiencia en la práctica. También se necesitará ayuda del ingeniero de red, como apoyo, para ejecutar ciertos procesos imposibles de ejecutar sin su presencia.

Recursos Materiales y tecnológicos. Para llevar a cabo esta investigación es necesario disponer de planos de la topología física y lógica de la red y equipo para realizar *testing* de la red con acceso a los servidores (computadora, manuales y diagramas); también se contará con la disposición de acceso a las instalaciones de la planta.

Recurso financiero. Establecer los recursos necesarios, como material y humano, para el desarrollo del trabajo de investigación. Es necesario definir los costos económicos que serán aportados por el investigador, los cuales se definen en la siguiente tabla.

Tabla VI. **Monto aproximado de la investigación**

No.	Recurso	Descripción	Monto
1	Humano	Tiempo invertido por el investigador	Q3,000.00
2		Pago de asesoría	Q2,000.00
3	Transporte	Combustible	Q1,400.00
4	Material	Computadora (Laptop)	Q2,450.00
5		Papelería y Útiles	Q100.00
6	Equipo	Dispositivos de medición	Q3,000.00
7	Varios	Imprevistos	Q500.00
Veinticuatro mil cuatrocientos cincuenta quetzales			Q12,450.00

Fuente: elaboración propia, hecho con Microsoft Excel.

13. REFERENCIAS

1. Ariganello, E. B. (2010). *Redes Cisco CCNP a Fondo Guia de estudio para Profesionales*. Mexico DF: Alfaomega.

2. Blog.desdelinux.net. (2015). *Opendaylight*. [Mensaje en un blog]. Recuperado de https://blog.desdelinux.net/opendaylight-el-futuro-de-las-redes-definidas-por-software-sdn/

3. Brad Edgeworth, R. G. (2020). *CCNP and CCIE Enterprise Core ENCOR 300-401 Official Cert Guide.* Indianápolis, Indiana, Estados Unidos: Cisco Press.

4. Coing, C. (2018). *Formacion Profesiona Jesuita*. Barcelona, España. [Mensaje en un blog]. Recuperado de https://fp.uoc.fje.edu/blog /tipos-de-mantenimiento-informatico-predictivo-preventivo-y-correctivo/

5. Curvature, S. (2021). Tecnologías MPLS. *Park Place Technologies* 17(7), 3-12. Recuperado de https://www.curvature.com/es/managed-it-services/mpls-technologies/

6. F5. (2021). *¿Que es la VPN SSL?* F5 Glossary. Recuperado de https://www.f5.com/es_es/services/resources/glossary/ssl-vpn

7. GARCÍA, M. O. (2008). *MPLS, EL PRESENTE DE LAS REDES IP.* (tesis de licenciatura). Universidad Tecnológica de Pereira, Colombia Recuperado de http://repositorio.utp. edu.co/dspace/bitstream/ handle/11059/1311/0046T172.pdf?sequence=1&isAllowed=y

8. Hat, R. (2021). *funciones y seguridad de la virtualización*. Red Hat. Recuperado de https://www.redhat.com /es/topics/virtualization/what-is-virtualization

9. Hortua, E. U. (2019). *EVALUACIÓN DE LA RED LAN PARA LAS SEDES DE LA CALLE 25 Y.* (tesis de licenciatura). Universidad Cooperativa de Colombia. Recuperado de https://es.scribd.com/document/483654088/2019-Evaluacion-Red-LAN

10. Huawei, C. (16 de 3 de 2021). *Conceptos básicos sobre Túnel GRE - HCIA R&S parte 1*. Huawei, Corp. Recuperado de https://forum.huawei.com/enterprise/es/ conceptos-b%C3%A1sicos-sobre-t%C3%BAnel-gre-hcia-r-s-parte-1/thread/741435-100235

11. Inforges. (2018). *Que es Sap*. [Mensaje en un blog]. Recuperado de https://www.inforges.es/Blog/iblog/2018/04/13/que-es-sap-business-one

12. Ivan Pepeinjak, J. G. (2001). *MPLS and VPN Architectures.* Indianapolis, indiana: CiscoPress. Recuperado de https://doc.lagout.org/network/Cisco/CCIE/CCIE%20SP/CiscoPress%20-%20MPLS%20and%20VPN%20Architectures%20-%20VolumeII.pdf

13. Jason Gooley, R. H. (2018). *Cisco Software-Defined Access Cisco Secure Enterprise.* Indianapolis, Indiana, Estados Unidos: Cisco Press

14. Jimenez, J. (2020). *Conoce estos servicios VPN de código abierto*. RedesZone.net. Recuperado de https://www.redeszone.net/tutoriales/ vpn/servicios-vpn-codigo-abierto/

15. Julian Camilo Sombredero Alfonso, E. F. (2014). *Análisis Comparativo de prestaciones entre sdn (software defined networking) y redes ip convencionales.* (tesis de licenciatura). Universidad Santo Tomas. Bogota: Recuperado de https://repository.usta.edu.co/ bitstream /handle/11634/764/analisis%20comparativo%20de%20 prestaciones%20entre%20sdn%20y%20redes%20convencionales.pd f?sequence=1&isAllowed=y

16. LANNER. (2016). *SDN se muestra prometedor en la industria 4.0*. [Mensaje de un blog]. Recuperado de https://www.lanner-america.com/es/blog-es/sdn-se-muestra-prometedor-en-la-industria-4-0

17. Luz, S. D. (2021). *Mejora la seguridad de tu VPN con el protocolo IPsec*. RedesZone.net. Recuperado de https://www.redeszone.net/tutoriales /vpn/ipsec-que-es-como-funciona/

18. Moisa, J. E. (12 de 6 de 2019). *Tunnel GREE.* Comunidad de Cisco. Recuperado de https://community.cisco.com/t5/documentos-routing-y-switching/t%C3%BAnel-gre/ta-p/3181793

19. MTNET. (2018). *Las redes y su importancia para una estrategia de nube hibrida*. MTNET.com. Recuperado de https://www.mtnet.com.mx/ las-redes-y-su-importancia-para-una-estrategia-de-nube-hibrida/

20. Rapp, J. (2021). *Evolution of software-defined networking for dummies*. VMWARE. Recuperado de https://www.vmware.com/es/topics/ glossary/ content/software-defined-networking.html

21. Release, C. (2020). *Dynamic Multipoint VPN Configuration Guide, Cisco*

IOS. San Jose, California, Estados Unidos: Cisco.

22. Romero, W. I. (2017). *Estudio del protocolo Openflow usando el modelo de red definida por Software (Software Define Networks).* (tesis de licenciatura). Universidad Técnica de Manabí. Quito, Peru. Recuperado de http://repositorio.puce.edu.ec/bitstream/ handle/ 22000/14424/TESIS%20WILSON%20-%20PUCE-10-11-17.pdf? sequence=1&isAllowed=y

23. Rubio, D. S. (2020). *Redes wan definidas por software. SD-wan.* (tesis de licenciatura). Cataluña, España. Recuperado de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/116386/8/astifrTFG0620memoria.pdf

24. Santos, O. (2020). *CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide.* River St. Hoboken, NJ 07030 USA: CiscoPress. Recuperado de https://pdfcoffee.com/ccnp-and-ccie-security-core-scor-350-701-official-cert-guide-pdf-free.html

25. Sercaman. (2019). Mantenimiento a una red funcional. [Mensaje de un blog]. Recuperado de https://sercaman.es/mantenimiento-y-soporte/mantenimiento-cableado-de-redes/

26. Tavares, L. A. (1986). *Administracion Moderna de Mantenimiento.* Sau Paulo, Brasil: Novo Polo.

27. Tejedor, R. J. (2014). *SDN: El futuro de las redes inteligentes*. Consultoría estrategica en tecnología de la informacion y comunicaciones. Recuperado de https://www.ramonmillan.com/tutoriales/ sdnredesinteligentes.php

28. Velásquez, C. D. (2020). *DISEÑO DE ARQUITECTURA DE RED SDN / NFV.* (tesis de licenciatura). Universidad de San Carlos de Guatemala. Recuperado de http://www.repositorio.usac.edu.gt/13530/1/Carlos% 20Daniel%20Alvarado%20Vel%C3%A1squez.pdf

29. vmware. (2016). *¿En qué consiste la virtualización?* VMWARE. Recuperado de https://www.vmware.com/latam/solutions/virtualization.html#:~:text=La%20virtualizaci%C3%B3n %20utiliza%20el%20software,aplicaciones%2C%20en%20un%20solo%20servidor