**Facultad de Ingenierías**

**Título del Trabajo**

Desarrollo de Cisco SD-Access para la Gestión Centralizada y Automatización de la Red LAN en la empresa Mervasa en 2023.

**Línea de Investigación:**

Tecnologías de la Información y la Comunicación

**Modalidad de Titulación:**

Propuesta Tecnológica

**Carrera:**

Ingeniería en Sistemas y telecomunicaciones.

**Título a Obtener:**

Ingeniero en Sistemas con énfasis en Administración en Redes

**Autor**

Vaca Vega William Roberto

**Tutor**

Mgtr. Manuel Ramirez

**Guayaquil, 2023**

## DEDICATORIA Y/O AGRADECIMIENTO

Deseo primero ante todo agradecer a Dios, que me ha bendecido en este arduo camino, A mis ángeles que se encuentra en el cielo que todo lo que hago y dejo de hacer es por ellos Hilda Villavicencio y Gerardo Vega, a mis pilares en la vida y apoyo incondicional mis padres William Vaca e Hilda Vega, mi luz de ejemplo Rosita Vaca.

Un agradecimiento especial a mis amigos de vida que gracias a ellos lo he logrado todo, aunque ellos no lo sepan Eduardo Casañas, Pablo Cedeño, Patricio Tovar, Wilson Luna y Nicole Garzón.

Y no menos importante a la persona que hoy en día cree en mi a pesar de todo y eso me hace quererla de corazón Denisse Merchán.

## CERTIFICADO DE REVISIÓN FINAL

### CERTIFICADO DE APROBACIÓN DEL TUTOR PARA LA PRESENTACIÓN A REVISIÓN DEL TRABAJO DE TITULACIÓN

Samborondón, 11 de julio de 2023

Magíster

**Erika Ascencio Jordán**

**Decana de la Facultad**

**Ingeniería**

Universidad Tecnológica ECOTEC

De mis consideraciones:

Por medio de la presente comunico a usted que el trabajo de titulación TITULADO: Desarrollo de Cisco SD-Access para la Gestión Centralizada y Automatización de la Red LAN en la empresa Mervasa en 2023, según su modalidad, PROPUESTA TECNOLÓGICA ; fue revisado, siendo su contenido original en su totalidad, así como el cumplimiento de los requerimientos establecidos en la guía para la elaboración del trabajo de titulación, Por lo que se autoriza a: Vaca Vega William Roberto para que proceda a su presentación para la revisión de los miembros del tribunal de sustentación.

**ATENTAMENTE,**

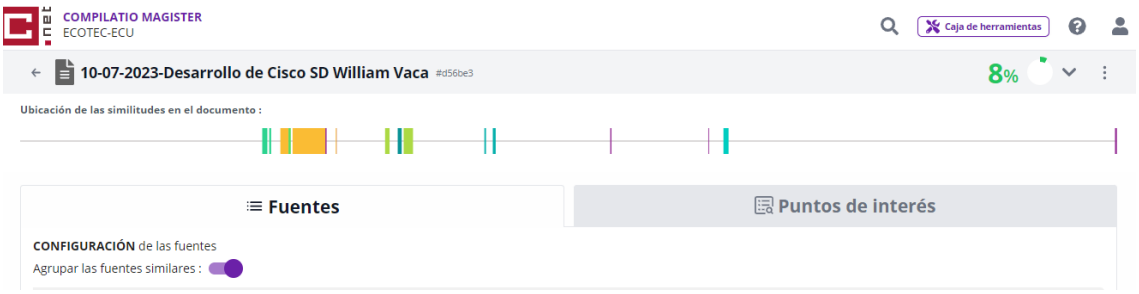

**Ing. Manuel Ramírez Pírez, Msc**

**Tutor**

## CERTIFICADO DE PORCENTAJE DE COINCIDENCIAS DE PLAGIO

### CERTIFICADO DEL PORCENTAJE DE COINCIDENCIAS

Habiendo sido nombrado Manuel Osmany Ramírez Pírez, tutor del trabajo de titulación Desarrollo de Cisco SD-Access elaborado por: William Roberto Vaca Vega, con mi respectiva supervisión como requerimiento parcial para la obtención del título de Ingeniero en Sistemas. Se informa que el mismo ha resultado tener un porcentaje de coincidencias 8 (%) mismo que se puede verificar con el print de pantalla de dicho resultado.




Firmado electrónicamente por:
MANUEL OSMANY RAMIREZ PIREZ

_____

**FIRMA DEL TUTOR**

**NOMBRES Y APELLIDOS DEL TUTOR**

**CERTIFICADO DE APROBACIÓN DEL TUTOR PARA LA PRESENTACIÓN DEL TRABAJO DE TITULACIÓN CON INCORPORACIÓN DE LAS OBSERVACIONES DE LOS MIEMBROS DEL TRIBUNAL**

Samborondón, 21 de agosto de 2023

Magíster

**Erika Ascencio Jordan**

**Decano(a) de la Facultad**

**Ingenierías.**

Universidad Tecnológica ECOTEC

De mis consideraciones:

Por medio de la presente comunico a usted que el trabajo de titulación TITULADO: **Desarrollo de Cisco SD-Access para la Gestión Centralizada y Automatización de la Red LAN en la empresa Mervasa en 2023** según su modalidad PROPUESTA TECNOLÓGICA; fue revisado y se deja constancia que el estudiante acogió e incorporó todas las observaciones realizadas por los miembros del tribunal de sustentación por lo que se autoriza a: **William Roberto Vaca Vega,** para que proceda a la presentación del trabajo de titulación para la revisión de los miembros del tribunal de sustentación y posterior sustentación.

**ATENTAMENTE,**

Firmado electrónicamente por:
MANUEL OSMANY RAMIREZ PIREZ

**Mgtr/ Manuel Ramírez Pirez**

**Tutor**

## RESUMEN

El problema de eficiencia operativa en la administración de redes está relacionado con la urgente necesidad de implementar una solución SD-Access para lograr una gestión centralizada y automatizada de la red LAN por parte de la empresa Mervasa. Este estudio tuvo como objetivo general el diseño de una solución SD-Access para la gestión centralizada y automatizada de la red LAN de la empresa Mervasa. Para lograrlo, se empleó una metodología exploratoria y descriptiva, permitiendo la identificación de conceptos innovadores y perspectivas en la gestión de redes con SD-Access. La investigación descriptiva proporcionó una descripción detallada de la infraestructura de red diseñada, las políticas de seguridad establecidas y el control centralizado basado en los niveles del fabricante. Se utilizó el análisis de datos como instrumentos y métodos para llevar a cabo el estudio. Como resultado se diseñó la solución SD-Access de la manera más adecuada; la cual, permite la gestión centralizada y automatizada de la red LAN a través del software DNA Center de Cisco. Esto posibilitó la administración integral de la red en todas las ubicaciones donde se encontraban los dispositivos de comunicación. Además, se logró la automatización de la red, donde los dispositivos se configuraban automáticamente al conectarlos a la red, gracias al controlador (DNA) de SD-Access que gestionaba y configuraba todos los parámetros correspondientes a cada dispositivo, los cuales podían variar según la ubicación. En conclusión, la solución SD-Access en Mervasa resultó en beneficios significativos. La gestión centralizada y automatizada de la red LAN permite un control más eficiente y una respuesta más rápida a los cambios y requerimientos de la red. Las políticas de seguridad y acceso establecidas garantizaron la protección de los datos y la privacidad de la información de la empresa. Asimismo, la solución SD-Access ofrece mayor flexibilidad y

escalabilidad, permitiendo a la empresa adaptarse fácilmente a las necesidades futuras de su red.

**Palabras clave:** SD-Access, Gestión centralizada, Automatización de red, Políticas de seguridad de red, Red LAN.

## ABSTRACT

The problem of operational efficiency in network administration is related to the urgent need to implement an SD-Access solution to achieve centralized and automated management of the LAN network by the Mervasa company. This study had as general objective the design of an SD-Access solution for the centralized and automated management of the LAN network of the Mervasa company. To achieve this, an exploratory and descriptive methodology was used, allowing the identification of innovative concepts and perspectives in network management with SD-Access. The descriptive research provided a detailed description of the designed network infrastructure, established security policies, and centralized control based on vendor levels. Data analysis was used as instruments and methods to carry out the study. As a result, the SD-Access solution was designed in the most appropriate way; which allows the centralized and automated management of the LAN network through the Cisco DNA Center software. This enabled comprehensive network management at all locations where communication devices were located. In addition, network automation was achieved, where the devices were automatically configured when connected to the network, thanks to the SD-Access controller (DNA) that managed and configured all the parameters corresponding to each device, which could vary according to the location. In conclusion, the SD-Access solution at Mervasa resulted in significant benefits. The centralized and automated management of the LAN network allows for more efficient control and a faster response to changes and requirements of the network. The established security and access policies guaranteed the protection of data and the privacy of company information. In addition, the SD-Access solution offers greater flexibility and scalability, allowing the company to easily adapt to the future needs of its network.

**Keywords:** SD-Access, Centralized management, Network automation, Network security policies, LAN network.

## ÍNDICE GENERAL

## ÍNDICE DE TABLAS

pp.

## ÍNDICE DE FIGURAS

pp.

# INTRODUCCIÓN

El propósito de este estudio es crear un diseño SD-Access de CISCO, con el fin de lograr una administración centralizada y automatizada de la red LAN (Red de Área Local) de la empresa Mervasa. Con esta solución, se espera abordar problemas como la escalabilidad y el acceso a la infraestructura actual de manera más efectiva, y reemplazar la red tradicional actual con una red inteligente que proporcione información detallada al administrador de la red. Esto permitiría diagnosticar problemas que podrían afectar significativamente a los usuarios y reducir el rendimiento de sus tareas. La gestión de redes cableadas e inalámbricas se ha vuelto una prioridad en las empresas, ya que toda la información se transmite a través de estos medios y es crucial mantener la seguridad de dicha información para asegurar las ganancias.

La importancia del diseño de una solución SD-Access para la administración centralizada y automatizada de la red LAN de la empresa Mervasa radica en la mejora de la escalabilidad, la eficiencia y la seguridad de la red. Al implementar una solución SD-Access, la empresa puede mejorar la visibilidad de la red, reducir el tiempo de acceso, ahorrar personal encargado del monitoreo de la red y mejorar la experiencia del usuario final. Además, la solución puede ayudar a la empresa a hacer frente a los problemas de escalabilidad y acceso a la infraestructura actual de manera más efectiva.

En las redes LAN, la escalabilidad es una propiedad importante que debe ser desarrollada ya que las empresas buscan un crecimiento continuo y para ello es necesario adaptar la tecnología (Ayala et al., 2015). La solución SD-Access permitirá automatizar las políticas de acceso a los usuarios y ofrecerles una experiencia estable en toda la red, sin comprometer su seguridad.

Al implementar una infraestructura basada en SD-Access, se obtienen beneficios como una mayor visibilidad de toda la red y la capacidad de transformar los datos para la planificación. Aprovechando las ventajas de una red centralizada

y automatizada, se puede reducir el tiempo de acceso y ahorrar personal encargado del monitoreo de la red LAN en la empresa para obtener el máximo beneficio. Es pertinente abordar este tema en este momento porque la gestión de redes cableadas e inalámbricas se ha vuelto una prioridad en las empresas, especialmente en el contexto actual donde el trabajo remoto y la conectividad se han vuelto críticos para la continuidad del negocio.

Además, la implementación de soluciones SD-Access está en línea con la tendencia actual de la transformación digital y la adopción de tecnologías avanzadas para mejorar la eficiencia y la seguridad de las empresas. Por lo tanto, abordar este tema en este momento puede ayudar a la empresa Mervasa a mantenerse competitiva y preparada para el futuro.

**Planteamiento del problema**

La empresa Mervasa enfrenta una necesidad importante, debido a la falta de eficiencia operativa en la administración de su red LAN debido a una estructura inadecuada. La ausencia de una gestión centralizada y automatizada ha generado problemas de eficiencia y costos en la administración de la red. Además, el crecimiento continuo de la empresa ha dado lugar a una cadena de suministro y logística más compleja, lo cual agrava aún más los desafíos en la gestión de la red LAN.

El problema de falta de eficiencia operativa en la administración de redes de la empresa está estrechamente relacionado con la necesidad de desarrollar una solución SD-Access que permita una gestión centralizada y automatizada de la red LAN. Debido al crecimiento constante de la empresa, tanto el diseño lógico como físico de la red han adquirido mayor complejidad, generando problemas adicionales de eficiencia y costos en su administración.

Además, como empresa, Mervasa tiene recursos limitados para invertir en soluciones de automatización costosas, lo que complica aún más la implementación de una solución efectiva para la gestión de la red. Es por eso que es importante

diseñar una solución que sea escalable y eficiente, pero también asequible y fácil de implementar y mantener.

La solución SD-Access permitirá automatizar las políticas de acceso a los usuarios y ofrecerles una experiencia estable en toda la red, al tiempo que se reduce el tiempo de acceso y se ahorra personal encargado del monitoreo de la red LAN en la empresa (Zamora et al., 2020). Esto ayudará a mejorar la eficiencia operativa en la administración de redes de Mervasa, lo que a su vez reducirá los costos asociados con la gestión de la red. Además, la solución proporcionará una mayor visibilidad de toda la red y permitirá la transformación de datos para la planificación, lo que ayudará a la empresa a mejorar su cadena de suministro y logística en general.

La solución SD-Access no solo resolverá el problema específico de la falta de eficiencia en la administración de redes de Mervasa, sino que también proporcionará beneficios adicionales para la empresa. Dicho lo anterior, es necesario realizar un diseño para una solución SD-Access que permita la gestión centralizada y automatizada de la red LAN de la empresa Mervasa.

## Formulación del problema

¿En qué medida la implementación de la red centralizada y automatizada mejoraría la gestión de la red LAN de la empresa Mervasa?

## Objetivos de la investigación

### Objetivo general

Diseñar una solución SD-Access que permita la gestión centralizada y automatizada de la red LAN de la empresa Mervasa.

### Objetivos específicos

- Diagnosticar la estructura actual de la red LAN de la empresa Mervasa.
- Definir las políticas de seguridad y acceso en conformidad con los estándares de CISCO, que permitan la gestión centralizada y automatizada de la red LAN de Mervasa.
- Diseñar la infraestructura de red con la solución SD-Access de CISCO, tomando en cuenta los periféricos y dispositivos necesarios para su implementación.

## Justificación

La implementación de la solución SD-Access en Mervasa ofrece la posibilidad de mejorar significativamente la eficiencia operativa en la administración de redes, lo que a su vez se traducirá en una reducción de los costos asociados con la gestión de la red. Al automatizar las políticas de acceso de usuarios y asegurar la estabilidad de la red en toda la empresa, se logrará disminuir el tiempo de acceso y minimizar la necesidad de personal dedicado al monitoreo de la red LAN, lo que conducirá a una reducción concreta de los costos operativos.

La solución SD-Access de CISCO representa una tecnología emergente en el ámbito de las redes de computadoras. La necesidad de profundizar en su comprensión y aplicación radica en su capacidad para revolucionar la administración de redes. Esta investigación permitirá un análisis profundo de cómo esta tecnología puede ser implementada de manera efectiva en la empresa Mervasa, mejorando en última instancia su eficiencia operativa.

La gestión centralizada de la red LAN de Mervasa, habilitada por esta solución, aumentará la visibilidad y transparencia de la red. Este aspecto brindará a la empresa una comprensión más completa de su infraestructura, permitiéndole tomar decisiones fundamentadas y basadas en datos para optimizar su cadena de suministro y logística en general.

El diseño propuesto no solo aplicará los estándares de seguridad de CISCO en políticas, sino que también garantizará el cumplimiento de las mejores prácticas en la administración de redes, asegurando así la protección de la red y de los datos que circulan por ella.

**Tipo de investigación**

El tipo de investigación que se llevará a cabo en este estudio es de carácter exploratorio y descriptivo. El enfoque exploratorio permitirá identificar conceptos novedosos y explorar perspectivas innovadoras en la gestión de redes. La investigación descriptiva, por otro lado, ofrecerá una descripción detallada de la infraestructura de red diseñada, las políticas de seguridad establecidas y el control centralizado basado en los tres niveles del fabricante.

Este enfoque de investigación es especialmente adecuado para abordar el tema de la gestión de redes, ya que permite obtener una comprensión profunda y detallada de su aplicación en el contexto específico de la empresa Mervasa. Además, servirá como base para futuras investigaciones y mejoras en la gestión de redes en la empresa.

La exploración detallada y su aplicación en la empresa Mervasa permitirá identificar áreas de mejora en la gestión de redes, así como identificar oportunidades para reducir costos y mejorar la eficiencia operativa. Además, este estudio permitirá profundizar en el conocimiento de la solución SD-Access de CISCO, que es una tecnología emergente en el campo de las redes de computadoras.

La combinación de métodos exploratorios y descriptivos en este estudio permitirá obtener un conocimiento más profundo y completo en la gestión centralizada y automatizada de la red LAN en la empresa Mervasa.

# CAPÍTULO I

# MARCO TEÓRICO

El marco teórico es una parte fundamental de cualquier investigación, ya que sirve como base teórica para el estudio y permite situar el problema de investigación en un contexto más amplio. En él se incluyen los conceptos, teorías, modelos y antecedentes relevantes que son necesarios para comprender el problema que se aborda y las posibles soluciones que se proponen.

## 1.1. Antecedentes de la investigación

Salazar Chacón, G. D. (2021). Hybrid Networking SDN y SD-WAN: Interoperabilidad de arquitecturas de redes tradicionales y redes definidas por software en la era de la digitalización (Tesis doctoral, Universidad Nacional de La Plata). En esta tesis se examinó la evolución de las redes de datos hacia el paradigma SDN y sus diversas adopciones (SD-Access, SD-Data Center y SD-WAN) con el objetivo de verificar su viabilidad de implementación.

Para ello, se abordaron los fundamentos de estas tecnologías, partiendo del desacoplamiento del Plano de Control del Plano de Datos en los equipos de red y explorando el concepto de cambio cultural y tecnológico conocido como NetDevOps, el cual resulta esencial para el funcionamiento adecuado del ecosistema ágil de SDN.

Asimismo, se realizó un análisis de los protocolos estandarizados de próxima generación, como LISP, VXLAN, OMP y Segment-Routing, que permiten la implementación de estos entornos en redes reales. Durante el proceso de investigación, se llevaron a cabo pruebas de concepto (PoCs) en entornos de emulación y con equipos físicos, lo que permitió validar la integración de SDN basadas en programabilidad con redes tradicionales. Esta tesis doctoral representa una contribución significativa en este campo de estudio.

En su investigación "Propuesta de diseño de una red de datos de área local bajo la arquitectura de redes definidas por software para la Red Telemática de la Universidad Nacional Mayor de San Marcos", Chafloque (2018) presentó una

propuesta de diseño de una red de datos de área local bajo una arquitectura de redes definidas por software (SDN) con el objetivo de mejorar la eficiencia de la gestión e interoperabilidad entre los diferentes dispositivos o equipos de red que conforman la red de datos de área local (LAN) de la Red Telemática de la Universidad Nacional Mayor de San Marcos - UNMSM.

Chafloque (2018) describió detalladamente el funcionamiento de las redes definidas por software, incluyendo los protocolos y plataformas que se utilizan en su desarrollo. Asimismo, llevó a cabo un análisis exhaustivo de la forma en que se gestiona una red LAN tradicional, como la Red Telemática, y la arquitectura de los dispositivos de red convencionales.

La propuesta del diseño de red se realizó de forma simulada bajo el software Mininet, donde se explicó la topología a diseñar, así como la descripción del controlador SDN a utilizar y finalmente se presentaron las pruebas y resultados obtenidos de la simulación. Con los resultados obtenidos, se compararon los beneficios que brinda la arquitectura SDN con respecto a la red LAN actualmente implementada, presentando las conclusiones y recomendaciones del proyecto de investigación.

En las conclusiones de su tesis, Chafloque (2018) afirmó que el simulador de red Mininet permitió diseñar una red LAN bajo la arquitectura SDN para la Red Telemática de la UNMSM en un entorno de simulación usando el controlador Opendaylight. Además, se logró observar el potencial de las redes SDN incluso en un entorno de red virtualizado, y Mininet permitió ejecutar las aplicaciones, módulos y comandos del sistema Linux desde los hosts virtuales sin inconvenientes.

Se pudo poner en evidencia que el controlador Opendaylight es capaz de administrar todos los dispositivos de red que tengan habilitado Openflow, además el controlador tiene la total visibilidad de la red de manera centralizada permitiendo una gestión unificada. Las redes definidas por software permitirían a la Red Telemática habilitar la programación de la red mediante distintas APIs de

programación, lo cual permitiría cambiar los dispositivos de red actuales por dispositivos que permiten ser programados según las necesidades del administrador.

Los resultados obtenidos en las pruebas de conectividad permiten concluir que el controlador Opendaylight puede manejar tráfico TCP y UDP. Una vez establecida la conexión y la instalación de las tablas de flujo en los switches, los tiempos de respuesta son menores con respecto a los primeros paquetes enviados. Chafloque señaló que SDN brinda la oportunidad a los investigadores de desarrollar las líneas de investigación en el campo de la automatización de la red, seguridad de las redes de forma proactiva, convergencia en la red y desarrollo de aplicaciones proactivas de QoS.

Cuba y Becerra (2015) presentaron en su tesis "Diseño e implementación de un controlador SDN/OpenFlow para una red de campus académica". El objetivo de esta investigacion fue el diseño e implementación de un controlador SDN para una red de campus académico, como la Red PUCP. El cual utilizo un diseño modular, y toma como base la plataforma de controlador Floodlight, a la que se le añaden, y en algunos casos se modifican, módulos específicos para mejorar la escalabilidad de una red Ethernet de Capa 2; además, considera una implementación gradual (por etapas), permitiendo la coexistencia de elementos (oislas) de red SDN/OpenFlow y Legacy.

En cuanto a las conclusiones, se logró el objetivo principal de la tesis. El controlador demostró ser escalable para el tráfico unicast mediante el mecanismo utilizado por el módulo Clustering, lo que permitió un 25% de uso en las TCAM de los Switches y en la capacidad del controlador. El Timeout de las Flow Entries tuvo un impacto directo en el porcentaje de uso de las TCAM de los Switches y en la capacidad del controlador, y, por lo tanto, en la escalabilidad del sistema.

Además, el módulo Circuit Tree permitió la escalabilidad de las TCAM de los Switches de acceso correspondientes cuando la distribución de destinos se

concentraba en unos pocos hosts. Bajo el nuevo esquema de subnetting, se observó un aumento en el tráfico Broadcast, para lo cual el controlador ofreció módulos para evitar tormentas de broadcast y saturación de enlaces, además de proporcionar la información necesaria para optimizar el enrutamiento. El controlador pudo coexistir con elementos Legacy y servir como punto de partida para una migración gradual a OpenFlow. El diseño del controlador permitió una migración completa de la Red PUCP a SDN.

## 1.2. Bases teóricas

Estas bases teóricas proporcionarán los fundamentos conceptuales y teóricos necesarios para comprender y analizar los aspectos clave de la tecnología SD-Access y su aplicación en la gestión y automatización de redes LAN. Así como también, los modelos de gestión centralizada y automatización de redes LAN. Se abordarán los avances tecnológicos que han llevado al desarrollo de SD-Access, como el paradigma de redes definidas por software (SDN), la virtualización de redes y los protocolos de comunicación modernos.

Además, se examinarán las ventajas y beneficios potenciales que ofrece SD-Access en términos de flexibilidad, escalabilidad, seguridad y eficiencia en la gestión de la red LAN. Se analizarán también los desafíos y consideraciones asociados con la implementación de SD-Access, como la integración con la infraestructura existente, la seguridad de la red y la capacitación del personal.

### 1.2.1. Gestión Centralizada de una Red LAN

Desde los últimos años las empresas están intentando hacerse con un abanico de herramientas que les permitan conseguir unagestión más centralizada. La característica de la gestión centralizada permite que usted maneje y configure los múltiples dispositivos al mismo tiempo, para proporcionar la mayor confiabilidad, flexibilidad y escalabilidad dentro de su Red, permitiendo que usted maneje de

manera global mientras que cumple con las políticas locales (Chara y San Martin, 2022).

- **Principales ventajas de una Gestión Centralizada:**

Esta es la principal ventaja al gestionar servicios de formacentralizada, ya que, si se desea configurar ciertos permisos enciertos equipos en un esquema descentralizado, debería acudirequipo por equipo aplicando los cambios. En una red extensa (de 100 a 2000 equipos) este trabajo puede llevar incluso variosdías. Sin embargo, si se gestiona desde un único servidor es posible realizar la tarea en unos pocos minutos.

Así mismo, en la gestión centralizada de redes se obtienen beneficios como la optimización de la seguridad al minimizar la probabilidad de errores o configuraciones erróneas al controlar todo desde un único punto. Además, se logra una mayor capacidad de análisis al obtener información directamente desde el servidor en cuestión de minutos. También es posible organizar los equipos en grupos según el departamento al que pertenecen, lo que permite aplicar configuraciones específicas según los parámetros de la empresa, independientemente de su ubicación física (Jiménez y Patiño, 2018).

### 1.2.2. Automatización de una Red LAN

La automatización de la red utiliza la lógica programable para gestionar los servicios y los recursos de red. Permite que los equipos de operaciones de red configuren, ajusten, protejan e integren la infraestructura de red y los servicios de aplicacionesmás rápido que cuando los usuarios lo hacen de forma manual (Smeke, 2012). Elimina los pasos manuales que se necesitan para gestionar lasredes, como iniciar sesión en enrutadores, conmutadores, equilibradores de carga y firewalls para cambiar las configuraciones manualmente antes de cerrar sesión. Este proceso se basa en scripts encadenados que se programan en la interfaz de la línea de comandos (CLI) de un sistema operativo(SO) o de un software de automatización definido previamente.

Así mismo, esta consiste en usar la tecnología para realizar tareas, sin necesidad de una persona. La automatización de la TI se basa en el uso de sistemas de software para crear instrucciones y procesos repetibles, a fin de reemplazar o reducirla interacción humana con los sistemas de TI (Vélez y Fernanda, 2022). El software de automatización funciona dentro de los límites de esas instrucciones, herramientas y marcos, para realizar las tareas con muy poca o sin ninguna intervención humana.

Además, es conveniente automatizar las redes, ya que, a pesar de que las tecnologías subyacentes han evolucionado, la gestión de lasredes lleva décadas sin sufrir grandes cambios. Las redes por logeneral se crean, operan y mantienen de forma manual. Sin embargo, los enfoques manuales tradicionales para la configuración y las actualizaciones de la red son demasiado lentos y propensos a errores para respaldar de forma efectiva las necesidades de las cargas de trabajo, que cambian rápidamente. Cuando se automatizan la gestión de servicios y los recursos de red, los equipos de operaciones de red adquieren más agilidad y flexibilidad para respaldar las demandas empresariales modernas de manera eficiente.

Conjuntamente, para entender el correcto funcionamiento de la automatización de la red, tenemos que entender lo siguiente. No solo hay muchas maneras de automatizar una red, sino también muchos elementos de red que pueden automatizarse (Copara, 2022). La mayoría de las soluciones de automatización de la red se encuentran entre dos extremos: la automatización de la línea de comandos y el software de automatización.

En principio, puede automatizar los elementos de red mediante comandos y argumentos de CLI estándar (Erazo, 2020). Por ejemplo, losadministradores del sistema operativo Linux pueden utilizar operadores de Bash para encadenar eventos en función de los aciertos o los errores de los comandos anteriores. O bien, los usuarios podrían compilar listas de comandos en archivos de texto, conocidos

como scripts de shell, que pueden tener lugar todos a la vez y reiteradamente con un solo comando de ejecución.

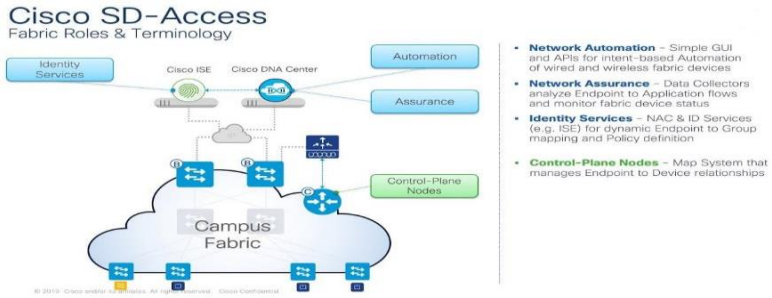
Por ello, los productos de software de automatización consolidan las tareas de red en programas predefinidos que se pueden seleccionar, programar y ejecutar desde el frontend de la aplicación. Por ejemplo, es posible utilizar algunos programas ya conocidos por los administradores de red para automatizar las redes y sus permisos. Para ello, las interfaces de programación de aplicaciones (API), los plugins, los inventarios y los módulos se empaquetan en playbooks que los usuarios pueden analizar, seleccionar y ejecutar para automatizar actividades como la configuración de la red, la seguridad, la organización de sistemas y la implementación, entre otras, en proveedores de servicios como AWS, Microsoft y Cisco.

### 1.2.3. SD-ACCESS

Es una solución diseñada para gestionar el acceso de usuarios a contenidos en la nube. Esta gestión, se puede realizar desde cualquier tipo de dispositivo móvil, desde teléfonos a ordenadores. El objetivo es proporcionar la posibilidad de que los usuarios entren bajo un control (Ponce, 2020).

Por lo que, esta herramienta multifuncional le puede ayudar a trabajar mejor en la empresa donde labora. No en vano, mejoraran los dispositivos de acceso, podrá acceder a datos de red para comprobar tendencias, tendrá una política de acceso común y, además, mejorara su eficiencia. En la actualidad, con la políticade protección de datos global se hace imprescindible tenercontroles de acceso que cumplan con la legislación. Ya que no hay que arriesgarse a las sanciones que establece el Reglamento Europeo de Protección de Datos (RGPD). Las Tecnologías de la Información (TI) proporcionan una transferencia de datos rápida y eficaz. En consecuencia, leinteresara utilizar este software si tiene una red con varios accesos (Ponce, 2020).

**Figura 1.** Ilustración de los distintos componentes de SD-ACCESS




*Fuente: CISCO Live! 2019*

### *1.2.3.1. Relación con SDN*

SD-Access (Software-Defined Access) es una tecnología que se basa en el paradigma de las redes definidas por software (SDN). SDN es un enfoque de redes que separa el plano de control (Control Plane) del plano de datos (Data Plane), permitiendo una mayor flexibilidad y programabilidad en la gestión de redes (Salazar, 2021).

En el contexto de SD-Access, SDN se utiliza para centralizar y automatizar la gestión de la red LAN. SD-Access proporciona una arquitectura de red que permite la segmentación virtual de la red, la asignación de políticas de acceso y la implementación dinámica de servicios de red. Utilizando los principios de SDN, SD-Access centraliza la gestión de la red y proporciona una visibilidad y control granular a través de un controlador de red.

Así mismo, el controlador de SD-Access se encarga de tomar decisiones y realizar configuraciones de forma centralizada, permitiendo la automatización de tareas de gestión de red como la configuración de políticas de seguridad, la asignación de VLANs y la gestión de acceso de dispositivos. Además, SD-Access utiliza la tecnología de virtualización de red para crear segmentos virtuales a través de la red física, lo que facilita la implementación de políticas de seguridad y la separación de tráfico (Salazar, 2021).

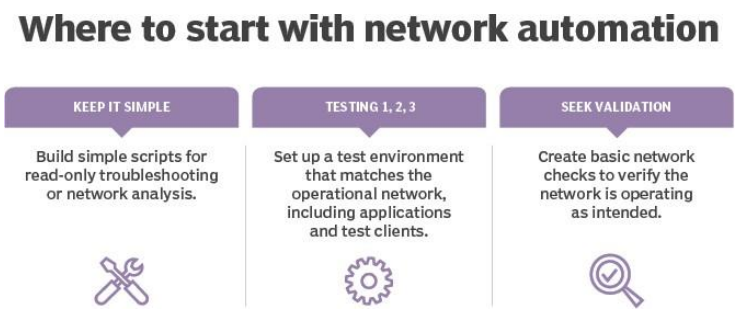
#### *1.2.3.2. Network Automation*

La automatización de redes es una técnica en la que el software configura, administra, prueba y provee automáticamente los dispositivos de una red, utilizada por empresas y proveedores de servicios para mejorar la eficiencia, disminuir el error humano y reducir los gastos operativos (Vargas, 2022). Las herramientas de automatización de red brindan funciones desde el mapeo básico de la red y la identificación de dispositivos hasta los flujos de trabajo complejos, como la administración de la configuración de red y la asignación de recursos de red virtual.

Consecuentemente, la automatización de red es crucial en las redes definidas por software, la virtualización de red y la orquestación de la red, permitiendo el aprovisionamiento automatizado de los inquilinos y funciones de la red virtual. La automatización de red se puede emplear en diversos tipos de redes, incluyendo LAN, WAN, redes de centros de datos, redes en la nube y redes inalámbricas. Cualquier recurso de red controlado a través de una CLI o API se puede automatizar (Chafloque, 2018). La automatización de redes basada en scripts utiliza lenguajes de programación y scripts para ejecutar tareas de forma consistente y precisa.

Así mismo, los lenguajes de programación de código abierto más recientes, como Ansible, Phyton y Ruby, son cada vez más populares debido a su facilidad de uso y flexibilidad. La automatización de redes basada en software, también conocida como automatización de red inteligente, se coordina a través de un portal administrativo que elimina la necesidad de escribir comandos manualmente y proporciona plantillas para crear y ejecutar tareas basadas en políticas de lenguaje sencillo.

**Figura 2.** Por dónde empezar con la automatización de la Red.

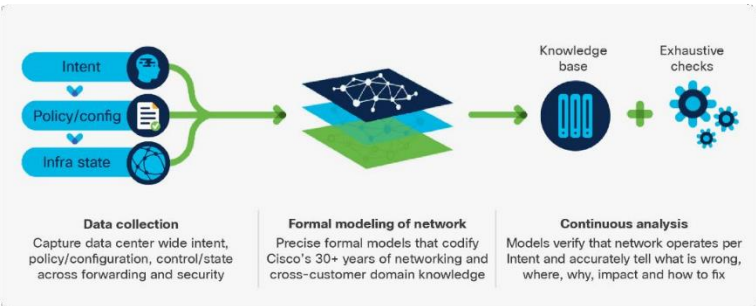



*Fuente: CISCO Live! 2019*

### *1.2.3.3. Network Assurance*

La garantía del servicio de red se refiere a las políticas y procesos establecidos por los proveedores de red y telecomunicaciones para asegurar una excelente experiencia para el cliente, lo cual se ha vuelto más difícil debido a la virtualización y las redes definidas por software. Para lograr esto, los proveedores utilizan análisis de datos de la red para identificar problemas y cumplir los acuerdos de nivel de servicio. Cisco ha abordado este desafío con su solución de software Network Assurance Engine, que utiliza técnicas de verificación formal para verificar y validar la corrección de redes enteras de manera matemática, lo que acelera la resolución de problemas y permite a los administradores de red anticipar problemas potenciales. Esto mantiene altos niveles de servicio con menos esfuerzo (Cisco, 2019).

**Figura 3.** Motor de Garantía de Red de Cisco

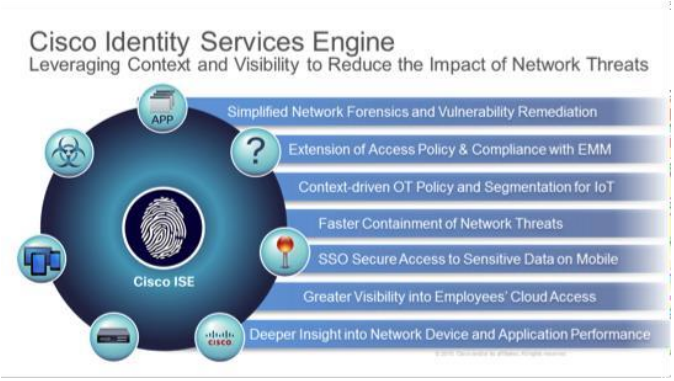



*Fuente: CISCO Live! 2019*.

### *1.2.3.4. Identity Services*

La red de la empresa ya no se limita a estar dentro de las paredes seguras de la oficina, sino que se extiende a donde quiera que vayan los empleados y los datos. Con la movilidad y el Internet de las cosas (IoE) en constante evolución, los empleados demandan acceso a los recursos profesionales desde una variedad de dispositivos y redes no corporativas. Sin embargo, con la proliferación de nuevos dispositivos conectados a la red y las brechas de seguridad cada vez más comunes, la seguridad del acceso a una red empresarial es de suma importancia (Cisco, 2019).

**Figura 4.** Motor de Servicios de Identidad de Cisco.




*Fuente: CISCO Live! 2019.*

### 1.2.4. Componentes SD-ACCESS

Dentro de la arquitectura de SD-Access, se identifican diferentes componentes clave que trabajan en conjunto para proporcionar una gestión centralizada y automatización de la red LAN. Estos componentes según Chara y San Martin (2022) son:

- Controlador SD-Access: Es el corazón de la arquitectura y se encarga de gestionar y controlar toda la red. El controlador SD-Access es responsable de tomar decisiones de configuración y políticas de acceso, así como de coordinar las funciones de todos los componentes. Proporciona una interfaz centralizada para la administración y el monitoreo de la red LAN.
- Fabric SD-Access: Es la infraestructura física de red compuesta por switches y routers compatibles con SD-Access. Estos dispositivos de red deben tener capacidades específicas para admitir las características de SD-Access, como la segmentación virtual de red y la asignación dinámica de políticas. Los switches y routers se comunican con el controlador SD-Access para recibir instrucciones de configuración y enviar información sobre el estado de la red.
- Identity Services Engine (ISE): Es una plataforma de seguridad que se integra con SD-Access para proporcionar políticas de acceso basadas en la identidad del usuario y del dispositivo. ISE autentica y autoriza a los usuarios

y dispositivos, y aplica las políticas de seguridad definidas en la red. Permite una segmentación granular y control de acceso basado en roles.

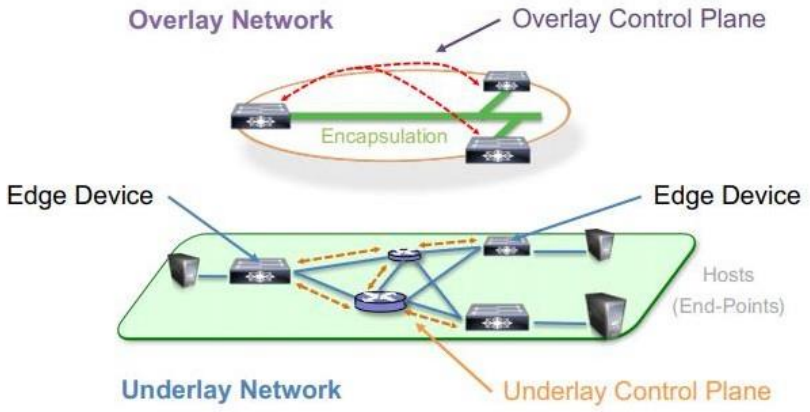
- Cisco DNA Center: Es una herramienta de gestión de redes que proporciona una interfaz gráfica y una plataforma unificada para la administración y el control de SD-Access. Permite la configuración, el monitoreo y la resolución de problemas de la red. Además, integra otras funcionalidades, como la gestión de políticas, la administración de dispositivos y la visualización de la topología de red.

Estos componentes trabajan en conjunto para habilitar la gestión centralizada y la automatización de la red LAN en el entorno de SD-Access. El controlador SD-Access se encarga de tomar las decisiones de configuración, mientras que el fabric SD-Access proporciona la infraestructura física para el transporte de datos. ISE garantiza la seguridad y la autenticación, y Cisco DNA Center ofrece la interfaz de gestión unificada para administrar y controlar la red.

**Figura 5.** Plano de datos del Fabric basado en VXLAN

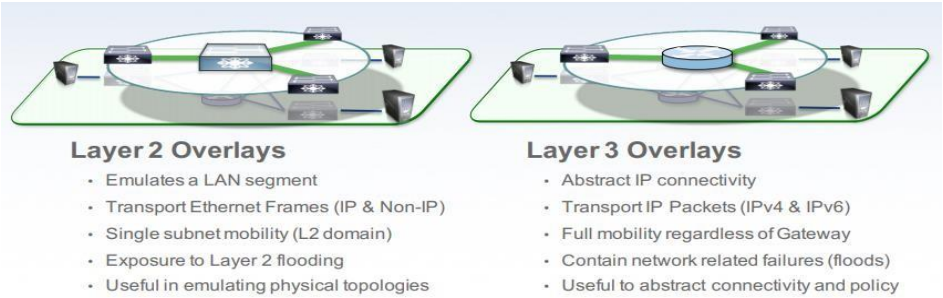

*Fuente: CISCO Live! 2019*

**Figura 6.** Overlay Network y Underlay Network.




*Fuente: CISCO Live! 2019.*

**Figura 7.** Overlay Network de Capa 2 y Capa 3.




*Fuente: CISCO Live! 2019.*

### 1.2.5. Arquitectura basa en controladores

Las redes convencionales presentan un enfoque de gestión basado en dispositivos, lo que es propenso a errores humanos y complejidades. SD-Access, en cambio, utiliza DNA Center como el centro de control y comando de la red basada en DNA para lograr una orquestación y operación más efectivas de los elementos de la red, incluyendo la configuración inicial de dispositivos y políticas para usuarios y dispositivos que se conectan a la red. El controlador proporciona una capa de abstracción de la red para manejar los detalles de los diferentes elementos de la red. Además, DNA Center ofrece API REST al norte para permitir el desarrollo de servicios personalizados por parte de terceros o internos (Chara y San Martin, 2022).

### 1.2.6. Tejido de red

Al tener un controlador en su lugar, se puede considerar la construcción de la red en bloques lógicos llamados entramados. SD-Access Fabric utiliza redes virtuales superpuestas para permitir la movilidad, segmentación y programación a gran escala. La superposición de redes virtuales utiliza un plano de control para mantener actualizado el mapeo de los puntos finales a su ubicación en la red a medida que se mueven (Chara y San Martin, 2022). Al separar el plano de control del plano de reenvío, se reduce la complejidad y se mejora la escala y la convergencia en comparación con las técnicas tradicionales de redes. SD-Access Fabric proporciona varias capacidades importantes, como la movilidad del host independientemente del volumen y tamaño de la red, la segmentación de Capa 2 y Capa 3 y la integración inalámbrica. Además, ofrece servicios inteligentes para el reconocimiento de aplicaciones.

### 1.2.7. Infraestructura programable

Cisco está trabajando en equipar tanto sus dispositivos actuales como futuros con capacidades avanzadas para permitir la administración completa del ciclo de vida de la infraestructura, todo esto manteniendo una arquitectura abierta, basada en estándares y que sea fácilmente extensible (Cisco, 2019). Estas tecnologías incluyen diversas características importantes, tales como:

- Aprovisionamiento automatizado de dispositivos, que engloba funciones bien conocidas como la configuración sin intervención y Plug and Play.
- Interfaz API abierta.
- Visibilidad granular, usando capacidades de telemetría como NetFlow.
- Actualizaciones de software sin problemas, con parches de software en vivo.

## 1.3. Definición de términos básicos

ACCESS CONTROL APPLICATION (ACA): una aplicación utilizada para controlar el acceso a una red, permitiendo o denegando el acceso a usuarios y dispositivos de acuerdo con las políticas de seguridad establecidas.

BGP (Border Gateway Protocol): un protocolo utilizado para intercambiar información de enrutamiento entre routers en internet y otras redes.

EMBEDDED WIRELESS LAN CONTROLLER: un controlador de red inalámbrica integrado en un dispositivo de red, como un switch, que proporciona funciones de gestión y control para los puntos de acceso inalámbricos conectados.

EXTRANET: una red privada que permite a ciertos usuarios autorizados acceder a recursos y servicios específicos de una organización desde fuera de la red.

FABRIC-IN-A-BOX: un enfoque de diseño de red que permite la creación de redes virtualizadas que pueden escalar y adaptarse a las necesidades de la organización.

IoT EXTENSION FOR SD-ACCESS: una extensión de SD-Access que permite la integración de dispositivos IoT en la red y la aplicación de políticas de seguridad específicas para estos dispositivos.

IPv6 SUPPORT: la capacidad de una red o dispositivo para utilizar el protocolo de Internet versión 6 (IPv6), que proporciona más direcciones IP y características de seguridad mejoradas en comparación con IPv4.

IS-IS (Intermediate System to Intermediate System): un protocolo de enrutamiento utilizado para intercambiar información de enrutamiento entre routers dentro de una red.

LAN AUTOMATION: una función que permite la automatización de la implementación de dispositivos de red en una red de área local (LAN), simplificando el proceso de configuración y eliminando errores humanos.

LAYER 2 BORDER: un dispositivo o función de red que conecta dos redes de área local (LAN) diferentes en la capa 2 del modelo OSI, permitiendo la comunicación entre ellas.

LAYER 2 FLOODING: un proceso en el que un switch de red envía un paquete a todas las interfaces de red conectadas, excepto a la interfaz desde la que se recibió el paquete.

MULTICAST (NATIVE): un tipo de transmisión de datos en el que un paquete se envía a múltiples dispositivos de red simultáneamente, pero solo aquellos que han solicitado específicamente ese paquete lo procesarán.

VN ANCHORING: una función que permite a una red virtual (VN) conectarse a recursos externos y otras redes, manteniendo la misma identidad de red virtual.

VRF (Virtual Routing and Forwarding): una técnica de virtualización de redes que permite que múltiples instancias de una red se ejecuten en un único dispositivo de red.

VXLAN (Virtual Extensible LAN): un protocolo de red que permite la creación de redes virtuales escalables en centros de datos, mediante la encapsulación de paquetes de red en otros paquetes, lo que permite la comunicación entre dispositivos que no están en la misma red física.

Al revisar la literatura existente, se identifican las teorías, modelos y enfoques relacionados con el tema de investigación, lo que le permite fundamentar su estudio en conocimientos previos. Esta revisión exhaustiva ayuda a establecer la importancia de la investigación y justificar los objetivos y enfoques propuestos.

Además, esta sección contribuye a identificar el problema de investigación de manera clara y precisa. Al explorar la literatura existente, el autor identifica brechas o áreas poco investigadas en el conocimiento actual, lo que le permite definir el problema de investigación que busca abordar. La utilidad del marco teórico también se extiende al diseño de la investigación. Al revisar la literatura existente, el autor identifica las variables relevantes, las hipótesis o preguntas de investigación pertinentes, y los métodos apropiados para recopilar y analizar datos. Además, el marco teórico proporciona los conceptos clave y las definiciones necesarias para establecer un lenguaje común en el estudio.

Asimismo, este permite situar la investigación en relación con otros estudios similares. El autor puede comparar y contrastar sus hallazgos con los de otros investigadores, identificando similitudes, diferencias o tendencias en el campo. Esta contextualización y comparación fortalece la validez y la relevancia de los resultados obtenidos. Por último, el marco teórico también puede generar nuevas ideas y perspectivas para el autor. Al revisar la literatura existente, es posible encontrar conceptos, teorías o enfoques que inspiren nuevas ideas para el estudio. Esto abre la puerta a explorar nuevas perspectivas y desarrollar enfoques metodológicos innovadores.

# CAPITULO II

# METODOLOGÍA DEL PROCESO DE DESARROLLO DE LA PROPUESTA TECNOLÓGICA

El marco metodológico es una parte esencial de cualquier investigación, ya que proporciona una guía para la recopilación, el análisis y la interpretación de los datos. Este marco incluye la descripción de los métodos y técnicas utilizados para recopilar información, así como la definición de las herramientas que se utilizarán para analizar y presentar los datos.

## 2.1. Enfoque la investigación

El enfoque de la investigación es mixto, ya que se están utilizando tanto métodos empíricos como estadísticos para recopilar y analizar los datos, y se están empleando herramientas y estándares de software/hardware para lograr la solución propuesta. Además, se realizan diagnósticos y diseñando soluciones en profundidad, lo que sugiere una exploración exhaustiva de los fenómenos. Por lo tanto, se combinan el enfoque cuantitativo y cualitativo para obtener una comprensión más completa del problema y su solución.

## 2.2. Tipo de investigación

El tipo de investigación que se llevará a cabo en este estudio es de carácter exploratorio y descriptivo. El enfoque exploratorio permitirá identificar conceptos novedosos y explorar perspectivas innovadoras en la gestión de redes a través de la solución SD-Access. La investigación descriptiva, por otro lado, ofrecerá una descripción detallada de la infraestructura de red diseñada, las políticas de seguridad establecidas y el control centralizado basado en los tres niveles del fabricante.

Este enfoque de investigación es especialmente adecuado para abordar el tema de la gestión de redes con la solución SD-Access, ya que permite obtener una comprensión profunda y detallada de su aplicación en el contexto específico de la

empresa Mervasa. Además, servirá como base para futuras investigaciones y mejoras en la gestión de redes en la empresa.

La exploración detallada de la solución SD-Access y su aplicación en la empresa Mervasa permitirá identificar áreas de mejora en la gestión de redes, así como identificar oportunidades para reducir costos y mejorar la eficiencia operativa. Además, este estudio permitirá profundizar en el conocimiento de la solución SD-Access de CISCO, que es una tecnología emergente en el campo de las redes de computadoras.

La combinación de métodos exploratorios y descriptivos en este estudio permitirá obtener un conocimiento más profundo y completo de la solución SD-Access en la gestión centralizada y automatizada de la red LAN en la empresa Mervasa.

## 2.3. Período y lugar donde se desarrolla la propuesta tecnológica

La propuesta tecnológica se desarrolla en MERVASA S.A., una empresa ubicada en la Av. Benjamin Carrion No. VILLA 12 Esq. Mz 22, GUAYAQUIL, Guayas. Esta empresa es el lugar donde se implementará la tecnología SD-Access para la gestión centralizada y automatización de la red LAN. El periodo en el que se llevará a cabo esta implementación es el año 2023.

## 2.4. Universo y muestra

Las muestras de información fueron tomadas de la red LAN tradicional de una empresa de Mervasa de los cuales se obtuvieron los datos reales de la infraestructura anterior y comparar con la nueva infraestructura implementada con la solución SD-Access.

## 2.5. Definición y comportamiento de las principales variables incluidas en el estudio.

### 2.5.1. Variable dependiente

- Desarrollo de la gestión centralizada de la red LAN
- Automatización de la red LAN

### 2.5.2. Variable independiente

- Solución CISCO SD-ACCESS

### 2.5.3. Operacionalización de variables

**Tabla 1.** Operacionalización de variables

| VARIABLE | DEFINICIÓN | DIMENSIONES | INDICADORES | INSTRUMENTOS Y/O MÉTODOS |
|---|---|---|---|---|
| Solución CISCOSD-ACCESS | El acceso definido por software (SD-Access), una solución dentro de la arquitectura de red digital de Cisco (Cisco DNA) que se basa en principios de redes basadas en la intención, proporciona un cambio transformacional en la construcción, administración y protección de redes, haciéndolas más rápidas y fáciles de operar, con una mayor eficiencia empresarial | Componente cognoscitivo | Experiencia y conocimiento en uso de esta nueva tecnología | Análisis de datos |
| | | Accesibilidad Económica | Disponibilidad económica para cubrir ese gasto de implementación | Análisis de datos |

| | | | | |
|---|---|---|---|---|
| Desarrollo de una gestión centralizada de la red LAN | Gestión centralizada significa manejar y configurar los dispositivos múltiples al mismo tiempo, para proporcionar la mayor confiabilidad, la flexibilidad, y la escalabilidad dentro de su red, permitiendo gestionarla de manera global mientras que cumple con las políticas locales. | Flexibilidad de la red LAN | Tiempo medido en horas y minutos que tarda el administrador de la RED en solucionar un incidente o requerimiento | Observación directa Entrevistas |
| Automatización dela red LAN | La automatización de red es el proceso de automatizar la configuración, la administración, las pruebas, la implementación y la operación de dispositivos físicos y virtuales en una red. La disponibilidad de los servicios en red mejora al automatizar las tareas y funciones de red cotidianas, y controlar y administrar automáticamente los procesos repetitivos. | Escalabilidad de la red LAN | Cantidad de tiempo utilizado en la configuración de nuevos dispositivos de red para continuar con la escalabilidad | Análisis de datos |

## 2.6. Métodos empleados e instrumentos de la investigación

En este estudio se utilizan métodos empíricos para cumplir con los objetivos específicos. Para realizar el diagnóstico de la estructura actual de la red LAN de la empresa Mervasa, se emplea una combinación de observación y entrevistas con el personal encargado de la red. Estos métodos permiten identificar problemas y deficiencias en la red, tales como latencia, deficiencias en el cableado y limitaciones de ancho de banda.

Además, se utiliza el análisis de datos, para obtener información relevante sobre el desempeño y las limitaciones de operatividad de los dispositivos pertenecientes a la infraestructura de red tradicional. Con base en los resultados de estas evaluaciones y análisis, se diseñará la infraestructura de red con la solución SD-Access de CISCO, definiendo políticas de seguridad y acceso en conformidad con los estándares de CISCO.

## 2.7. Procesamiento y análisis de la información.

Para el procesamiento y análisis de la información en este proyecto, se va a seguir una metodología de trabajo basada en el ciclo de vida del software y el modelo de desarrollo en cascada. Esto implica dividir el proyecto en diferentes fases o etapas, que permitan una gestión adecuada de los recursos y una mejor planificación y seguimiento del proyecto.

En la primera etapa, se realizará un diagnóstico de la estructura actual de la red LAN de la empresa Mervasa, mediante la aplicación de métodos empíricos como la observación. En la segunda etapa, se definirán las políticas de seguridad y acceso para la red, en conformidad con los estándares de CISCO.

Los estándares de seguridad de CISCO incluyen la Arquitectura de Seguridad CISCO, las Operaciones de Inteligencia de Seguridad CISCO y la Respuesta a Amenazas CISCO. En cuanto a las herramientas de análisis de vulnerabilidades, CISCO ofrece varios productos como Cisco Identity Services Engine (ISE), Cisco Advanced Malware Protection (AMP) y Cisco Stealthwatch. En la tercera etapa, se diseñará la infraestructura de red utilizando la solución SD-Access de CISCO. Se seleccionarán los periféricos y dispositivos necesarios para su implementación.

# CAPITULO III

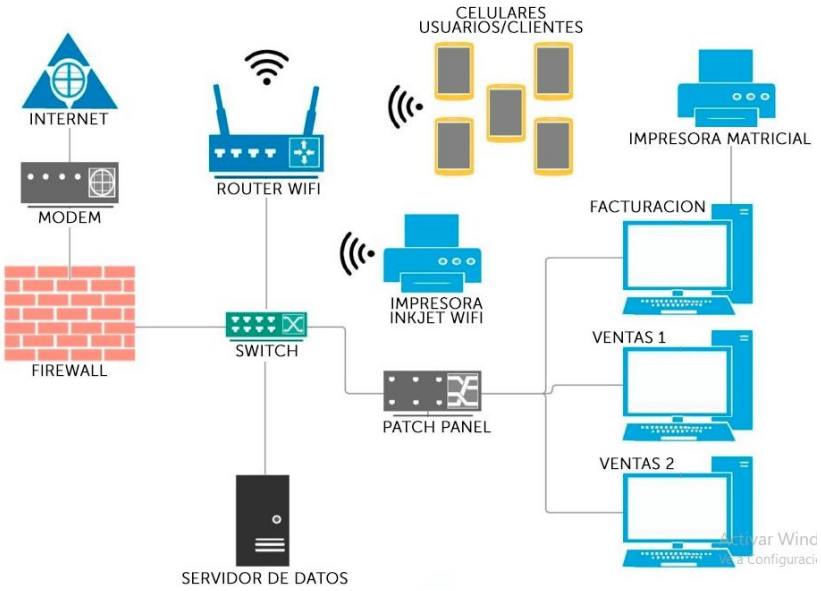
# ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS

## 3.1. Infraestructura actual

La empresa Mervasa S.A se basa típicamente en un enfoque de red local con tecnología inalámbrica y a su vez Ethernet, así como también la afectación de periféricos tales como switch y router. Aunque este enfoque ha sido ampliamente utilizado, en la actualidad no existe afectaciones con soluciones en la nube.

Cabe mencionar que el diseño expuesto a continuación presenta muchas falencias en su recepción de paquetes  a a partir del enlace que existe entre el patch panel como también en sus tiempos de respuesta (actualizaciones) de nivel de acceso Hostname, al momento de realizar requerimientos internos.

**Figura 8.** Topología de Red Tradicional de la Empresa

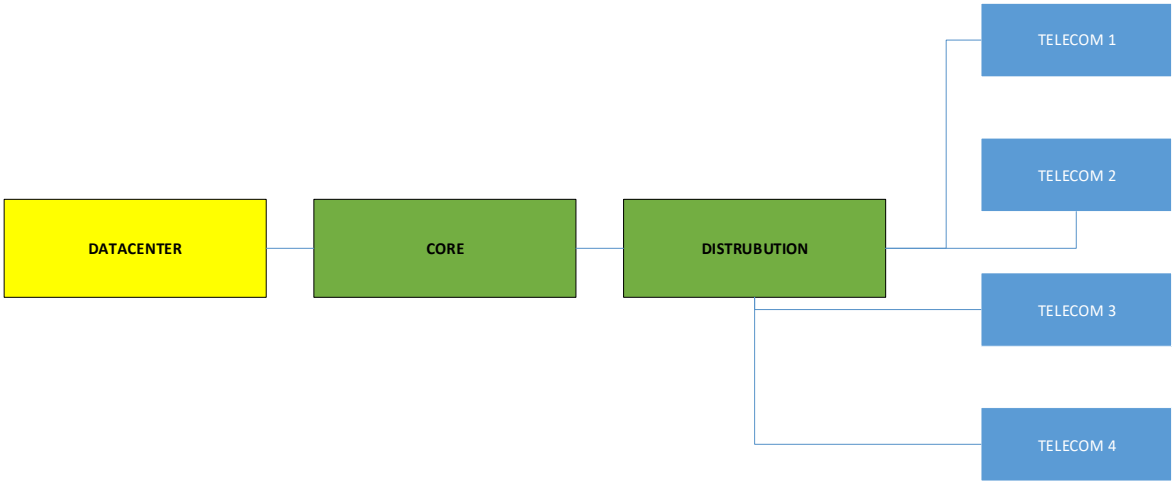



*Fuente: Elaboración por parte del Departamento Sistema Mervasa S.A.*

## 3.2. Infraestructura propuesta

La Infraestructura Tecnológica para la red corporativa de una empresa de Mervasa se compone de una solución de hardware que utiliza Switches Catalyst de la serie 9000, los cuales están integrados en la arquitectura de acceso a la red definida por software de Cisco Systems, conocida como Cisco Software-Defined Access (SD-Access). Como se representa en el diagrama de bloques a continuación:

**Figura 8.** Diagrama de Bloques de Arquitectura de Interconexión

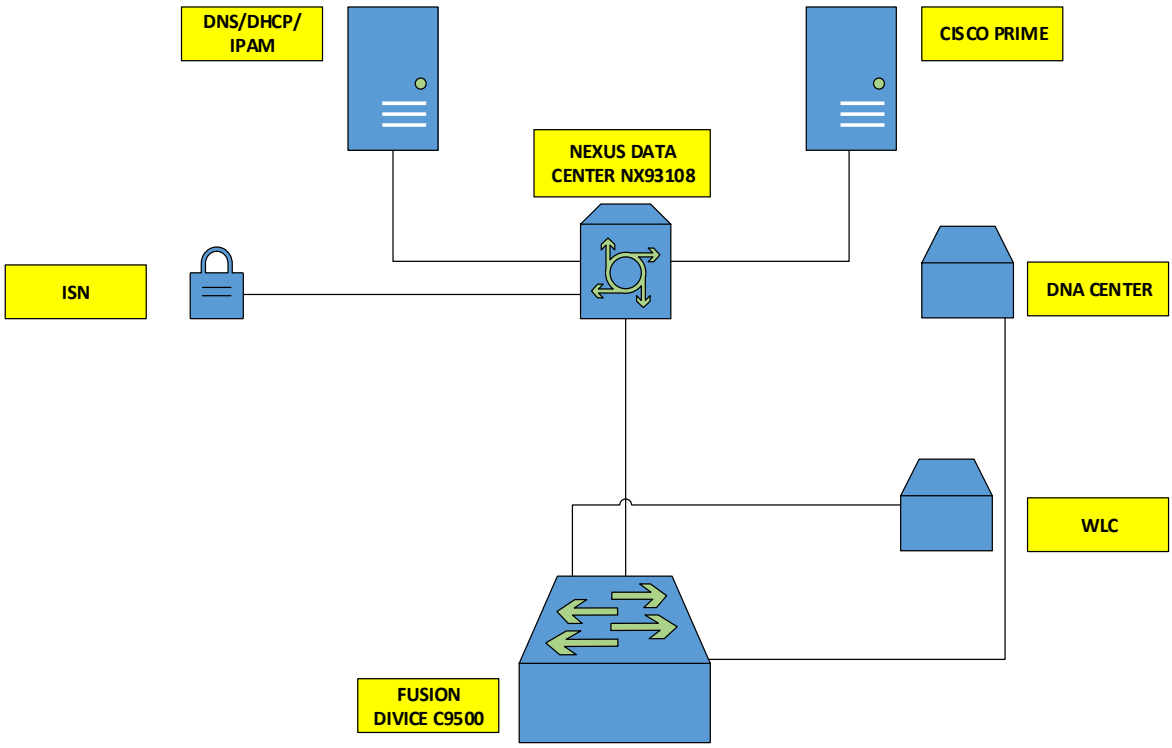



*Fuente: Elaboración propia*

Se propone la implementación de cinco Switches Nexus 9k en el Data Center, los cuales operarán en modo redundante para garantizar la continuidad del servicio. Estos switches proporcionarán la conectividad necesaria para los servidores que también forman parte del proyecto.

## 3.3. Tipología final

**Figura 9.** Topología de servicios Data Center de la Empresa Mervasa




*Fuente: Elaboración propia*

La topología de servicios del Data Center de la empresa Mervasa incluye varios dispositivos y componentes que permiten el funcionamiento de la infraestructura de red. A continuación, se describe cada uno de ellos:

Fusion Device C9500: Se trata de un switch de la serie Catalyst 9500 de Cisco, que ofrece alto rendimiento y capacidad de procesamiento para la red del Data Center. Este dispositivo es capaz de gestionar una gran cantidad de conexiones y tráfico de datos, garantizando una comunicación eficiente y segura.

Wireless LAN Controller (WLC): El controlador WLAN es responsable de administrar y controlar los puntos de acceso inalámbricos (AP) en el Data Center. Proporciona servicios de gestión centralizada, seguridad y configuración para la red inalámbrica, permitiendo una conectividad confiable y estable para los dispositivos móviles.

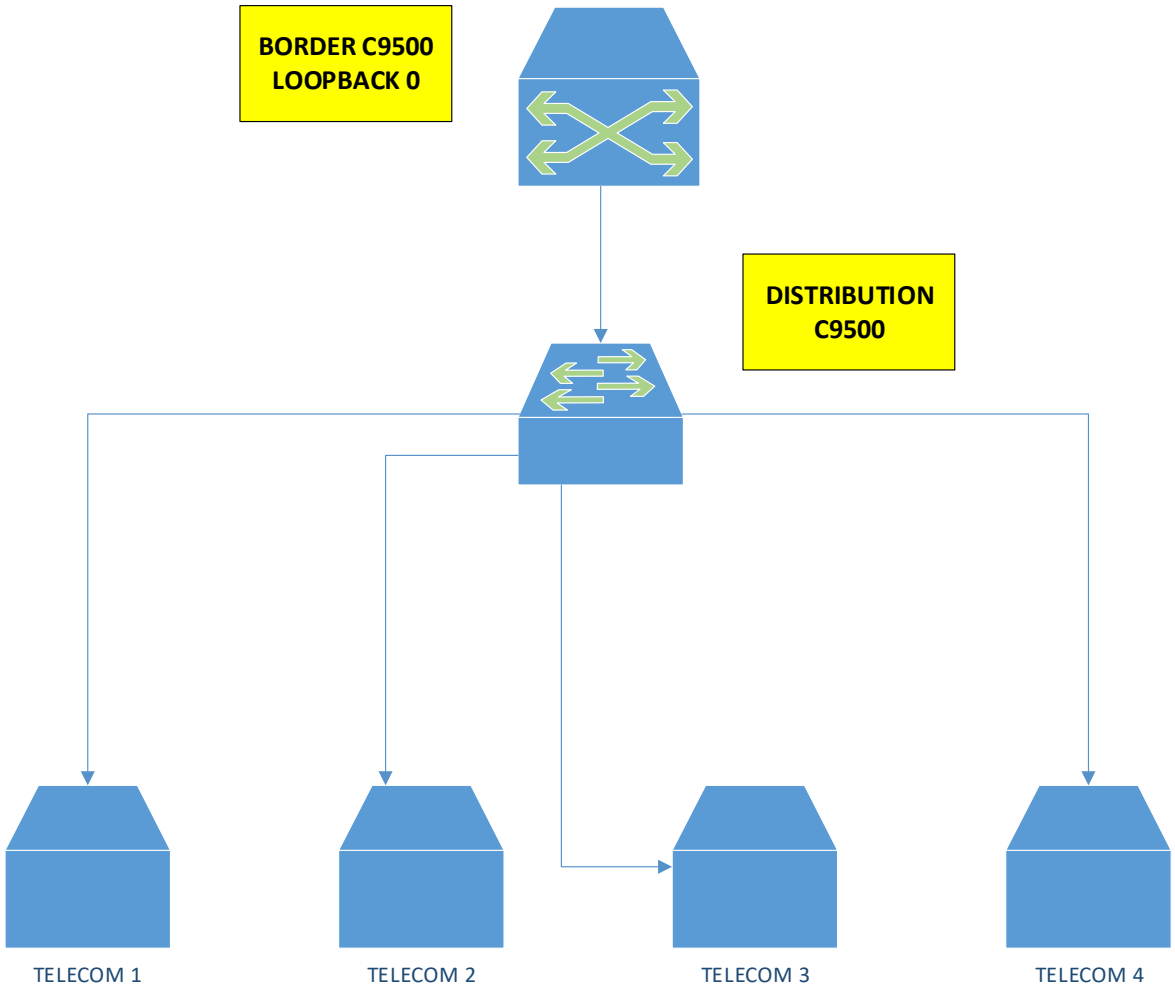
Cisco Prime: Cisco Prime es una plataforma de gestión de red que ofrece capacidades de monitoreo, configuración y solución de problemas. Permite una administración centralizada de la red, lo que facilita la supervisión y el control de los dispositivos y servicios en el Data Center de Mervasa.

Nexus Data Center NX93108: Es un switch de alta densidad diseñado para entornos de centro de datos. Proporciona una conectividad de alta velocidad y baja latencia para equipos de servidores, almacenamiento y otros dispositivos en el Data Center de Mervasa. Su capacidad de conmutación y enrutamiento avanzados garantizan un rendimiento óptimo de la red.

DNS/DHCP/IPAM: Estas siglas corresponden a los servicios de DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol) e IPAM (IP Address Management). Estos servicios son esenciales para la administración y asignación de direcciones IP, así como la resolución de nombres de dominio en la red. Proporcionan un funcionamiento fluido de la red y facilitan la conectividad de los dispositivos en el Data Center de Mervasa.

Así mismo, esta topología de servicios en el Data Center de la empresa Mervasa incluye dispositivos como switches Catalyst 9500 y Nexus NX93108, un controlador WLAN, la plataforma de gestión Cisco Prime, así como servicios de DNS, DHCP e IPAM. Estos componentes trabajan en conjunto para brindar una infraestructura de red confiable, segura y de alto rendimiento en el Data Center de Mervasa.

**Figura 10**.Topología de Red SD-ACCESS de la Empresa Mervasa




*Fuente: Elaboración propia*

La topología de red SD-Access de la empresa Mervasa se compone de varios dispositivos y componentes que permiten la implementación y gestión de una red definida por software (SDN, por sus siglas en inglés). A continuación, se describe cada uno de ellos:

Distribution C9500: Se trata de un switch de la serie Catalyst 9500 de Cisco, que desempeña el papel de distribución en la topología SD-Access. Este switch es responsable de conectar los dispositivos de acceso (como puntos de acceso inalámbricos, cámaras IP, etc.) a la red y proporcionarles conectividad hacia los

demás componentes de la infraestructura. El Distribution C9500 también puede implementar políticas de seguridad y calidad de servicio para el tráfico de la red.

Border C9500: Este switch Catalyst 9500 funciona como el borde de la red SD-Access de Mervasa. Su función principal es establecer la conexión con redes externas, como Internet o redes de otras sucursales de la empresa. El Border C9500 implementa políticas de seguridad y control de acceso para proteger la red SD-Access de amenazas externas.

Loopback 0: La interfaz de loopback 0 es una interfaz virtual que se utiliza para asignar una dirección IP lógica a un dispositivo de red. En la topología SD-Access de Mervasa, la interfaz de loopback 0 se utiliza probablemente para proporcionar una dirección IP virtual al switch Distribution C9500 o al Border C9500, lo que facilita su administración y conectividad dentro de la red.

Telecom: Esta referencia a Telecom indica la conexión de la red SD-Access de Mervasa con proveedores de servicios de telecomunicaciones externos. Puede ser a través de enlaces de conexión dedicados o de servicios de conectividad de terceros que permiten la comunicación con redes externas y el acceso a servicios de Internet.

La topología de red SD-Access de la empresa Mervasa incluye dispositivos como los switches Catalyst 9500 (Distribution y Border), la interfaz de loopback 0 y conexiones de telecomunicaciones externas. Estos componentes trabajan juntos para crear una red definida por software, permitiendo una gestión centralizada y automatizada de la red, así como la implementación de políticas de seguridad y control de acceso en Mervasa.

## 3.4. Hardware

La red a implementar contará con el siguiente equipamiento:

- 05 Switches Datacenter Nexus 9300.
- 01 Fusion Device Catalyst 9500.
- 01 Servidores DNA Center DN2-HW APL.
- 01 Servidores ISE 3615.
- 01 Wireless LAN controllers C9800.
- 01 Switches Borde Catalyst C9500-32C-A.
- 01 Switches de Distribución Catalyst c9500-32QC-A.
- 4 Switches Catalyst C9300-48PA.

## 3.5. Equipamiento del Proyecto

Cisco DNA Center es la piedra angular de la automatización en la solución SD-Access. Dentro de Cisco DNA Center, se encuentra un paquete de aplicación que forma parte del software y permite el diseño, aprovisionamiento, aplicación de políticas y la creación de un entorno inteligente tanto para la red cableada como inalámbrica en el campus. Para garantizar la alta disponibilidad, se implementará un DNA Center DN2-HW-APL en configuración de alta disponibilidad (HA), lo cual se considera como el sistema de automatización de la red.

**Figura 11.** Topología e Interconexiones DNA Center


*Fuente: Elaboración propia*

**Tabla 2.** Direccionamiento IP DNA Center Fuera de Banda

| INTERFACE CIMC | Host IP address | Default Gateway |
|---|---|---|
| DNA | 186.42.137.100 | 186.42.137.1 |

*Fuente: Elaboración propia*

**Tabla 3.** Direccionamiento DNA Center Enterprise.

| INTERFACE ENTERPRISE | VLAN | Host IP address | Default Gateway |
|---|---|---|---|
| DNA | VLAN 71 | 192.168.0.171 | 192.168.0.1 |
| DIRECCIÓN VIRTUAL DEL CISCO DNA | VLAN 71 | 192.168.0.170 | 192.168.0.1 |

*Fuente: Elaboración propia*

La topología e interconexiones del DNA Center de la empresa Mervasa involucra varios dispositivos y componentes clave para el funcionamiento y la gestión de la infraestructura de red. A continuación, se describe cada uno de ellos:

Nexus: Los switches Nexus son dispositivos de alto rendimiento diseñados específicamente para entornos de centro de datos. Estos switches proporcionan una conectividad de alta velocidad y baja latencia, así como características avanzadas de conmutación y enrutamiento. En la topología del DNA Center de Mervasa, los switches Nexus se utilizan probablemente para la conectividad dentro del centro de datos y la interconexión con otros componentes de la infraestructura.

Cisco DNA: Cisco DNA (Digital Network Architecture) es una arquitectura de red que proporciona un enfoque de diseño y gestión basado en políticas para la infraestructura de red. En la topología del DNA Center de Mervasa, Cisco DNA juega un papel fundamental en la configuración y gestión centralizada de la red.

Proporciona una plataforma para definir políticas de red, implementar cambios de configuración, realizar monitoreo y solución de problemas, y automatizar tareas de red.

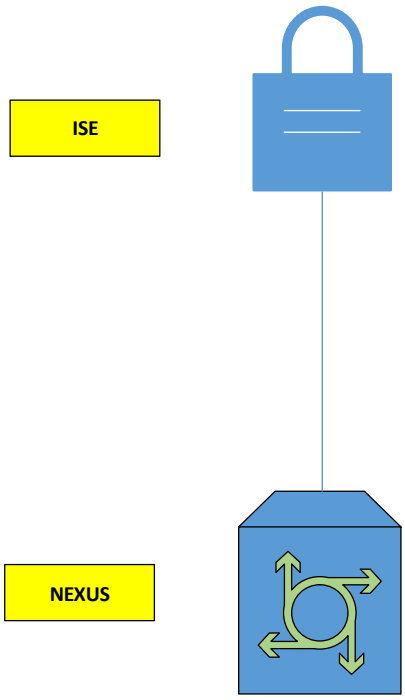
Fusion Device C9500: El Fusion Device C9500 es un switch de la serie Catalyst 9500 de Cisco que combina capacidades de conmutación y enrutamiento con funciones de seguridad y administración avanzadas. En la topología del DNA Center de Mervasa, el Fusion Device C9500 se utiliza para proporcionar conectividad y servicios en la red, así como para implementar políticas de seguridad y calidad de servicio.

### 3.6. Identify Service Engine (ISE)

Cisco ISE es una plataforma de seguridad de acceso a la red que desempeña un papel fundamental en la gestión, control y consistencia de los usuarios y dispositivos que se conectan a la red de una organización. En el marco de SD-Access, ISE es una pieza esencial para la implementación de políticas, perfilado y control de acceso a la red.

La solución de implementación de ISE constará de 1 servidor Cisco SNS-3615-K9, los cuales estarán equipados con la versión de software 2.7 y los parches 2 y 3 instalados. Estas actualizaciones garantizan el funcionamiento óptimo y la seguridad de la plataforma ISE en el entorno de red.

**Figura 12.** Topología y conexiones Cisco ISE




*Fuente: Elaboración propia*

**Tabla 4.** Direccionamiento IP CISCO ISE.

| SOLUCION CISCO ISE | VLAN | Host IP address | Default Gateway |
|---|---|---|---|
| ISE | VLAN 71 | 172.40.71.176 | 172.40.71.1 |

*Fuente: Elaboración propia*

## 3.7. WLC

En una red inalámbrica, es posible utilizar un Controlador de LAN Inalámbrica (Wireless LAN Controller) para centralizar el control de los puntos de acceso (APs) en lugar de gestionar individualmente cada uno de ellos.

En este caso, el rol del controlador inalámbrico está compuesto por un WLC Catalyst. Estos controladores son responsables de administrar y supervisar los puntos de acceso, lo que permite una gestión más eficiente y simplificada de la red inalámbrica en su conjunto.

**Tabla 5.** Direccionamiento IP WLC.

| CONTROLADORES DE ACCESO INALÁMBRICO | VLAN | Host IP address | Default Gateway |
|---|---|---|---|
| WLC1 | VLAN 71 | 190.100.50.191 | 190.100.50.1 |
| DIRECCIÓN VIRTUAL DE ESTOS EQUIPOS | VLAN 71 | 190.100.50.190 | 190.100.50.1 |

*Fuente: Elaboración propia*

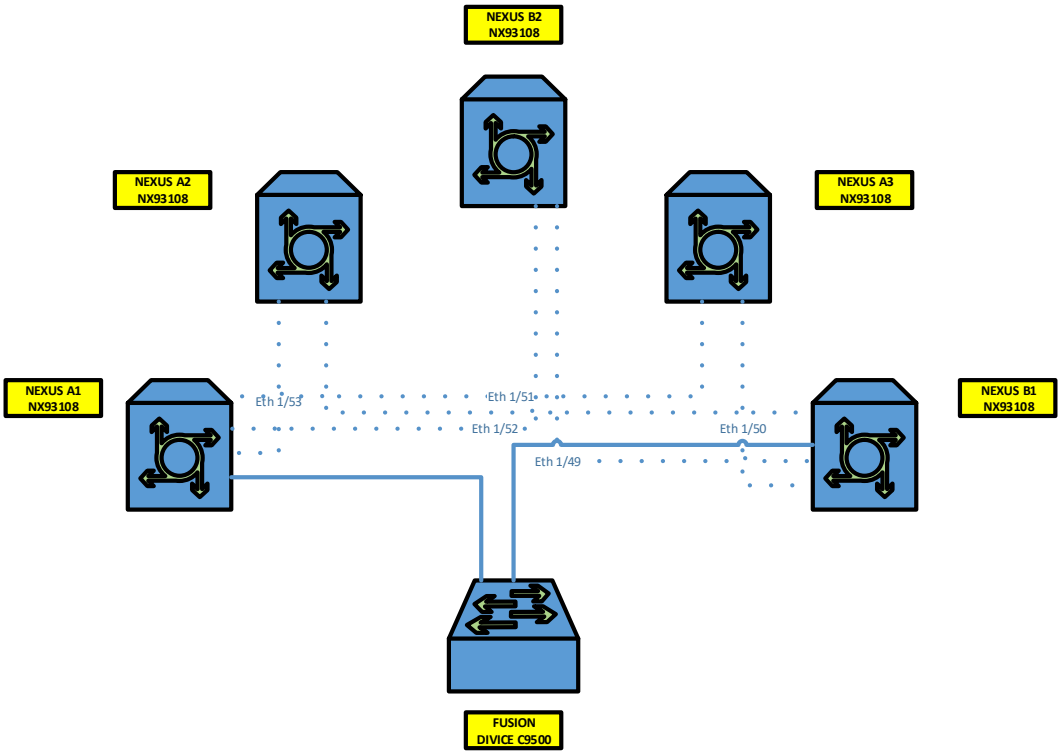
## 3.8. Nexus Data Center

Se planea utilizar un total de cinco switches para el centro de datos, de los cuales dos serán utilizados como switches principales del núcleo del centro de datos, mientras que los tres restantes se destinarán a la conexión de los servicios compartidos, como Cisco DNA Center, Cisco ISE y DNS/DHCP/IPAM.

Los switches seleccionados para la implementación pertenecen a la serie Nexus N9K-C93108TC-EX, los cuales son adecuados tanto para entornos de centro de datos como para servidores. Estos switches se interconectarán siguiendo un modelo de redundancia de capa 2 tradicional. Los dos switches principales del

núcleo del centro de datos permitirán la conexión hacia el dispositivo Fusion y, a su vez, brindarán acceso a otros servicios fuera del centro de datos.

**Figura 13.** Topología Data Center - Data Center




*Fuente: Elaboración propia*

**Tabla 6.** Direccionamiento IP Switches Nexus.

| HOST | VLAN | Host IP address | Default Gateway |
|---|---|---|---|
| NEXUS 1A | VLAN 70 | 186.42.137.91 | 186.42.137.1 |
| NEXUS 1B | VLAN 70 | 186.42.137.92 | 186.42.137.1 |
| NEXUS 2A | VLAN 70 | 186.42.137.93 | 186.42.137.1 |
| NEXUS 2B | VLAN 70 | 186.42.137.94 | 186.42.137.1 |
| NEXUS 3A | VLAN 70 | 186.42.137.95 | 186.42.137.1 |

*Fuente: Elaboración propia.*

## 3.9. Fusion Device

El término "dispositivo de fusión" o "enrutador de fusión" se deriva de la tecnología MPLS Layer 3 VPN. El concepto principal es que este tipo de dispositivo es consciente de los prefijos disponibles dentro de cada VPN (VRF), ya sea mediante la configuración estática de enrutamiento o mediante la sincronización de rutas, y puede fusionar estas rutas en una sola. La función principal de un dispositivo de fusión genérico es enrutar el tráfico entre VRF separadas o dirigir el tráfico desde y hacia una VRF hacia un conjunto compartido de recursos en servidores globales, como DHCP y DNS.

En el contexto de una implementación de SD-Access, el dispositivo de fusión tiene una responsabilidad específica: brindar acceso a los servicios compartidos para los dispositivos finales en la infraestructura. Para cumplir con esta función, se utilizarán un switch Catalyst C9500-24Y4C-A. Este switch se encargarán de facilitar el acceso a los servicios compartidos dentro del entorno SD-Access.

## 3.10. Diseño

En primer lugar, se debe en consideración para realizar las pruebas luego de la instalación del DNA Center es ingresar al apartado de diseño.

### 3.10.1. Network Settings

Dentro de Network Settings se deben definir los parámetros y servicios generales de la red como DHCP, DNS, servidores AAA, NTP, zona horaria, etc.

### 3.10.2. Credenciales

En esta configuración, se establecen las credenciales de usuario que serán utilizadas por DNA Center para acceder de forma remota a los equipos. Además, se agregan las comunidades SNMP durante el proceso de provisionamiento.

### 3.10.3. Wireless

En la sección de Diseño, también deben brindar la posibilidad de crear redes inalámbricas. DNA se integra con los controladores LAN inalámbricos (WLC) y asume la responsabilidad de administrar las redes inalámbricas. Es importante destacar que DNA no reemplaza la funcionalidad de los WLC, sino que envía la configuración a los WLC mediante el protocolo Netconf, permitiendo así una gestión centralizada.

## 3.11. Policy

Una vez finalizado el diseño de la red SD Access, se avanza hacia la configuración de las políticas. Es fundamental asegurarse de que en este punto el Identity Services Engine (ISE) esté integrado con DNA para permitir la replicación de políticas entre ambos sistemas. Esta integración garantiza un enfoque coherente y eficiente en la aplicación y gestión de las políticas de seguridad en toda la infraestructura.

DNA Center ofrece una interfaz intuitiva de políticas que permite configurar el acceso basado en identidades, de manera similar a ISE. En esta matriz de políticas, los filtros se aplican considerando el origen y el destino en función de las identidades. DNA Center se encarga de enviar las políticas a ISE, que a su vez se encarga de ejecutar el control de acceso.

Así mismo, a diferencia de las listas de acceso convencionales, las políticas en SD-Access no se aplican en función de las direcciones IP origen y destino, sino en base a identidades. Estas identidades están representadas por etiquetas conocidas como "Scalable Group Tags" (SGT).

El SGT es asignado a los dispositivos finales que se conectan a la red y que comparten políticas de red similares. Cada SGT tiene un valor único que lo identifica. La asignación de un host a un SGT puede ser estática o dinámica, basada en el perfilamiento en ISE. Estas etiquetas se pueden utilizar como clasificadores en las políticas de red, ofreciendo una nueva forma de clasificar la identidad de los equipos finales.

### 3.11.1. Virtual Network (VN)

En un entorno SD-Access, las Virtual Network (VN) ofrecen una segmentación a nivel macro que permite agrupar servicios y pools de direcciones IP de acuerdo a los requisitos. Se puede entender una VN como una equivalente de una VRF (Virtual Routing and Forwarding) en una red tradicional.

Las VNs proporcionan una forma eficiente de organizar y aislar diferentes servicios y recursos dentro de la infraestructura. Cada VN puede tener su propio conjunto de políticas de acceso, permitiendo un control granular sobre la conectividad y los recursos compartidos en el entorno SD-Access.

Al igual que las VRF en las redes tradicionales, las VNs permiten una gestión más eficiente de la red al proporcionar una separación lógica entre los diferentes dominios y requerimientos de la red. Esto facilita la implementación de políticas de

seguridad, el aislamiento de tráfico y la optimización del rendimiento en el entorno SD-Access.

### 3.12. Integración DNA – ISE

Para lograr una integración efectiva entre Cisco ISE y DNA Center, se utiliza PxGrid como mecanismo de comunicación. Una vez que se establece esta conexión, ambos sistemas pueden compartir información relevante, como datos de dispositivos, políticas de acceso y Scalable Group Tags (SGTs), con el fin de garantizar el cumplimiento de las restricciones de acceso establecidas.

La configuración de esta integración se lleva a cabo en la sección de Configuración (Settings) de DNA Center. Desde allí, se pueden establecer los parámetros necesarios para habilitar y gestionar la comunicación bidireccional entre DNA Center y Cisco ISE. Esta configuración permite una sincronización continua de datos y asegura que ambas plataformas trabajen en conjunto de manera eficiente para aplicar y hacer cumplir las políticas de seguridad y acceso en toda la infraestructura, cabe destacar que a partir de los siguientes apartados se maneja una licencia de pago la cual no fue factible la adquisición sin embargo se detalla los paso que se toma en consideración para la integración de manera eficaz.

### 3.13. Integración Wireless SD-Access

La configuración de la red inalámbrica en SD-Access se lleva a cabo a través de DNA Center, que se encarga de aprovisionar el controlador LAN inalámbrico (WLC) utilizando el protocolo NETCONF. Para lograr esto, es necesario descubrir el WLC mediante la herramienta de Descubrimiento (Discovery) de DNA Center.

### 3.14. Configuración Fusion Device

Una vez que el sistema DNA ha finalizado la configuración en los dispositivos Borders, se cuenta con todos los datos necesarios para llevar a cabo la configuración del Fusion Device. A diferencia de los demás dispositivos que forman parte del fabric, el Fusion Device no se encuentra integrado en la infraestructura automatizada y su configuración debe realizarse de forma manual.

En la Tabla 7, podemos observar los detalles clave para la configuración del Fusion Device. Cada fila corresponde a un segmento de red específico, identificado por su VLAN ID y VN (Número de Versión). Además, se especifica la dirección de red (NETWORK) asignada a cada segmento.

Sin embargo, es importante tener en cuenta que el Fusion Device requerirá una configuración manual, lo que implica que no será gestionado directamente por el sistema DNA. Por lo tanto, los detalles específicos para su configuración, como la asignación de VLAN y los segmentos de red, deberán ser ingresados de forma manual.

Para establecer la conectividad entre el Fusion Device y el resto de la red, se utilizará la dirección IP del Border, que actuará como punto de enlace entre ambos. Es fundamental asegurarse de que esta configuración se realice correctamente para garantizar la comunicación adecuada entre el Fusion Device y los demás dispositivos de la red.

**Tabla 7.** Direccionamiento IP por VRF: Fusion – Border.

| VLAN ID | VN | NETWORK | FUSION | BORDER |
|---|---|---|---|---|
| Vlan219 | VN 1 | 190.100.50.0 /30 | 190.100.50.1 | 190.100.50.2 |
| Vlan3021 | VN 2 | 190.100.51.40 /30 | 190.100.51.42 | 190.100.51.41 |
| Vlan3023 | VN 3 | 190.100.51.48 /30 | 190.100.51.49 | 190.100.51.54 |
| Vlan3024 | VN 4 | 190.100.51.52 /30 | 190.100.51.53 | 190.100.51.58 |
| Vlan3025 | VN 5 | 190.100.51.56 /30 | 190.100.51.57 | 190.100.51.86 |
| Vlan3032 | VN 6 | 190.100.51.84 /30 | 190.100.51.85 | 190.100.51.94 |
| Vlan3034 | VN 7 | 190.100.51.92 /30 | 190.100.51.93 | 190.100.51.102 |
| Vlan3036 | VN 8 | 190.100.51.100 /30 | 190.100.51.101 | 190.100.51.110 |
| Vlan3038 | VN 9 | 190.100.51.108 /30 | 190.100.51.109 | 190.100.51.107 |

*Fuente: Elaboración propia*

### 3.15. Integración SD-Access – Red Tradicional

La conectividad entre un dominio SD-Access y las redes externas se establece a través de un Border Node y un dispositivo de Fusión. Estos dos elementos colaboran para compartir las rutas y permitir la comunicación entre el dominio SD-Access y las redes externas utilizando el protocolo EBGP (External Border Gateway Protocol).

El Border Node, con el número de Sistema Autónomo (AS) 65520, actúa como el punto de conexión entre el dominio SD-Access y las redes externas. Este dispositivo se encarga de recibir y enviar las rutas hacia y desde las redes externas.

El dispositivo de Fusión, con el número de Sistema Autónomo (AS) 65521, se integra con el Border Node para establecer una comunicación eficiente y segura

entre el dominio SD-Access y las redes externas. Ambos dispositivos intercambian información de rutas utilizando el protocolo EBGP, lo que permite la correcta transmisión de datos entre el dominio SD-Access y las redes externas.

# CAPÍTULO 4

# PROPUESTA DE LA SOLUCIÓN TECNOLÓGICA

Una vez diseñada la topología de red y definido el enrutamiento para la solución SD-Access en la empresa Mervasa y al no contar con la infraestructura, equipos y licencia de para los programas de cisco; se plantea a continuación una propuesta de implementación teórica, detallando los pasos necesarios para llevar a cabo dicha implementación en un entorno real en el futuro.

## 4.1. Preparación del entorno

- **Verificación de la disponibilidad y compatibilidad del hardware necesario para la implementación, como los switches Catalyst 9000 y Nexus 9000, así como los controladores WLAN.**

En esta etapa, se debe realizar una verificación exhaustiva para asegurarse de que el hardware necesario esté disponible y sea compatible con la solución SD-Access. Se verifica que se cuenten con los switches Catalyst 9000 y Nexus 9000 recomendados por Cisco, así como los controladores WLAN adecuados para la implementación. Es importante asegurarse de que los dispositivos seleccionados sean compatibles con la arquitectura SD-Access y cumplan con los requisitos de capacidad y funcionalidad necesarios para la empresa Mervasa.

- **Configuración de las direcciones IP y los parámetros de red de los dispositivos, asegurándose de que cumplan con los requisitos de la topología diseñada.**

Una vez verificada la disponibilidad y compatibilidad del hardware, deben proceder a realizar la configuración de las direcciones IP y los parámetros de red de cada dispositivo. Es esencial asignar direcciones IP únicas a cada dispositivo y establecer las configuraciones de enrutamiento de acuerdo con la topología diseñada. Además, se deben configurar las VLAN y los parámetros de puertos necesarios para cada dispositivo, asegurándose de que se alineen con la topología diseñada previamente.

- **Establecimiento de conexión segura entre el DNA Center y los dispositivos de red para permitir la gestión y configuración centralizada.**

Con el fin de facilitar la gestión y configuración centralizada de los dispositivos de red, es fundamental establecer una conexión segura entre el DNA Center y los dispositivos de la red LAN de Mervasa. Para lograrlo, se deben utilizar protocolos de gestión como SNMP, SSH o NETCONF. Además, de configurar adecuadamente los parámetros de seguridad, como las credenciales de autenticación y encriptación, para garantizar la protección de la comunicación entre el DNA Center y los dispositivos de red.

Al completar este paso, se habrá preparado el entorno para la implementación de la solución SD-Access en la empresa Mervasa. Es importante tener en cuenta que estos son solo los primeros pasos de la implementación teórica, y que se requerirá continuar con los pasos restantes para llevar a cabo la implementación completa.

## 4.2. Lineamientos del DNA Center

- **Se propone instalar y configurar el software Cisco DNA Center en un servidor dedicado.**

En esta etapa, se debe instalar y configurar el software Cisco DNA Center en un servidor dedicado que actuará como la plataforma centralizada de gestión de la red. Se siguen los pasos de instalación proporcionados por Cisco para asegurar una configuración correcta del DNA Center. Esto puede incluir la instalación de los archivos de software, la configuración de las opciones de conectividad de red y la asignación de recursos adecuados al servidor.

- **Se debe corroborar mediante la conectividad entre el DNA Center y los dispositivos de red, utilizando protocolos de gestión como SNMP, SSH y NETCONF.**

Una vez que el DNA Center está instalado, se debe configurar la conectividad entre esta plataforma y los dispositivos de red de la empresa Mervasa. y utilizar protocolos de gestión estándar como SNMP (Simple Network Management Protocol), SSH (Secure Shell) y NETCONF (Network Configuration Protocol) para establecer una comunicación segura y bidireccional. Esto permitirá que el DNA Center recopile información de los dispositivos, realice cambios de configuración y monitoree el estado de la red de manera centralizada.

- **Se plantea que los parámetros de red ha utilizar, son DHCP, DNS, AAA y NTP, en el DNA Center con el fin de mantener un funcionamiento adecuado de la red.**

En esta fase, es preciso que los parámetros de red esenciales en el DNA Center para garantizar un funcionamiento fluido de la red. Así como, establecer opciones de configuración como DHCP (Dynamic Host Configuration Protocol) para la asignación automática de direcciones IP, DNS (Domain Name System) para la resolución de nombres de dominio, AAA (Authentication, Authorization, and Accounting) para la autenticación y el control de acceso, y NTP (Network Time Protocol) para la sincronización horaria precisa. Se debe priorizar que el DNA Center pueda gestionar eficazmente los servicios de red necesarios para el entorno de la empresa Mervasa, cabe mencionar que por ser una empresa Pymes en crecimiento se necesita la innovación de sus periféricos debido a que los equipos soportan configuraciones de uso de conectividad con fallas.

Al finalizar este paso, el DNA Center estará correctamente asignado y listo para la siguiente fase de implementación. Es importante destacar que estos pasos forman parte de la configuración teórica del DNA Center y deben adaptarse a los requisitos y políticas específicas de la empresa Mervasa.

## 4.3. Configuración de políticas de seguridad y acceso

- **Se deberá integra el Identity Services Engine (ISE) con el DNA Center para sincronizar las políticas de acceso y seguridad.**

En esta etapa, se debe llevar a cabo la integración entre el Identity Services Engine (ISE) y el DNA Center para asegurar la sincronización de las políticas de acceso y seguridad en la red. Mediante esta integración, el DNA Center puede compartir información relevante con el ISE, como datos de dispositivos, políticas de acceso y Scalable Group Tags (SGT). Esto permite una gestión centralizada y automatizada de las políticas de seguridad en toda la infraestructura de red de la empresa Mervasa.

- **Se definen las políticas de seguridad y acceso basadas en identidades, utilizando etiquetas como los Scalable Group Tags (SGT) para clasificar los dispositivos finales.**

En esta fase, se deben definir las políticas de seguridad y acceso que se aplicarán en la red basándose en identidades. Se deben utilizar etiquetas como los Scalable Group Tags (SGT) para clasificar y agrupar los dispositivos finales según políticas comunes. Cada SGT tiene un valor único que identifica un conjunto específico de políticas de acceso y seguridad. Esta clasificación basada en identidades permite una gestión más granular y eficiente de las políticas de seguridad en la red.

- **Se establecerán las reglas y restricciones de acceso en función de las identidades y políticas definidas, garantizando la seguridad y el cumplimiento de los estándares.**

En esta etapa, es preciso cumplir con reglas y restricciones de acceso en función de las identidades y políticas previamente establecidas. Estas reglas determinan qué dispositivos finales tienen acceso a qué recursos y servicios de la red, y qué tipo de tráfico está permitido. Se aplican políticas de seguridad como autenticación, autorización y control de acceso para garantizar la protección de la red y el cumplimiento de los estándares de seguridad establecidos por la empresa Mervasa. Estas reglas y restricciones de acceso se implementan y aplican de manera centralizada a través del DNA Center, asegurando una gestión coherente y eficiente de la seguridad en la red.

Al completar este paso, se habrán definido las las políticas de seguridad y acceso en la red de la empresa Mervasa, utilizando la integración entre el ISE y el DNA Center. Estas políticas garantizarán un entorno seguro y cumplirán con los estándares de seguridad establecidos. Es importante destacar que los detalles y configuraciones específicas de las políticas dependerán de los requisitos y políticas internas de la empresa Mervasa.

### 4.4. Implementación de las Virtual Networks (VN)

- **En este paso, se deberá crear las Virtual Networks (VN) en el DNA Center, utilizando los datos previamente establecidos durante el diseño. El objetivo es definir los distintos segmentos (departamentos) de red y agrupar los servicios y recursos según los requisitos específicos de la empresa Mervasa.**

Utilizando la interfaz de administración del DNA Center, se debe acceder a la sección de configuración de redes virtuales. Aquí, crearán las VN necesarias de acuerdo con la topología diseñada, considerando los segmentos de red requeridos y las políticas de agrupación o aislamiento establecidas.

Cada VN se debe configurar con su respectivo rango de direcciones IP y máscara de red, asegurándose de que no haya conflictos de direccionamiento con otras VN o redes existentes. Además, asignarán los servicios y recursos necesarios a cada VN, como puertas de enlace, servidores DHCP, servidores DNS, etc. Esto deben realizarlo según las especificaciones y necesidades de la empresa, garantizando una correcta segmentación y organización de la red.

- **Creación de las VN, asignar los dispositivos finales a las VN correspondientes, ya sea de forma estática o dinámica, basada en el perfilamiento en el ISE. Esto permitirá que los dispositivos finales se conecten a la red de manera segura y accedan a los recursos y servicios asignados a su VN específica.**

En el caso de la asignación estática, se debe identificar los dispositivos finales y se configurará manualmente su pertenencia a la VN correspondiente en el DNA Center. Esto se puede lograr utilizando identificadores únicos de dispositivo, como direcciones MAC o direcciones IP estáticas asignadas previamente.

En cuanto a la asignación dinámica, deben utilizar los datos de perfilamiento almacenados en el ISE. Basándose en los atributos y políticas de acceso definidos en el ISE, el DNA Center asignará automáticamente los dispositivos finales a las VN correspondientes durante su conexión a la red. Esto se logra mediante la autenticación y autorización de los dispositivos a través del ISE, que proporciona información sobre el perfil y las políticas de acceso de cada dispositivo.

Al completar este paso, se habrá llevado a cabo la implementación de las Virtual Networks (VN) en el DNA Center, definiendo los segmentos de red y agrupando los servicios y recursos según los requisitos de la empresa. Además, se habrá realizado la asignación de los dispositivos finales a las VN correspondientes, ya sea de forma estática o dinámica. Esto permitirá una gestión más eficiente de la red, asegurando que los dispositivos finales accedan únicamente a los recursos y servicios permitidos de acuerdo con las políticas establecidas.

## 4.5. Configuración de dispositivos de borde y fusión

- **En este paso, es preciso que los dispositivos de borde, específicamente los switches Nexus detallados previamente, con el objetivo de establecer la conexión con redes externas y garantizar la seguridad y el control de acceso en el entorno SD-Access.**

Se debe acceder a la interfaz de administración de los switches Nexus y proceden a configurar los parámetros de conexión con las redes externas. Esto implica establecer las interfaces de conexión, asignar las direcciones IP correspondientes y configurar los protocolos de enrutamiento necesarios para permitir la comunicación con las redes externas. También, aplicarán medidas de seguridad, como listas de control de acceso (ACL), para controlar el tráfico entrante y saliente.

Además, deben implementar mecanismos de control de acceso, como autenticación y autorización basadas en el ISE, para asegurar que los dispositivos y usuarios que intentan acceder a la red desde el borde cumplan con las políticas de seguridad establecidas. Esto se logra a través de la integración del ISE con los switches Nexus, lo que permite verificar la identidad y aplicar las políticas de acceso adecuadas.

- **Se mantiene el direccionamiento del dispositivo de fusión, en este caso, el Fusion Device Catalyst 9500. Este dispositivo desempeña un papel crucial en el entorno SD-Access al proporcionar acceso a los servicios compartidos y la conectividad adecuada dentro de la red.**

Deben acceder a la interfaz de administración del Fusion Device para llevar a cabo su configuración. Esto incluye la asignación de las interfaces de conexión, la configuración de direcciones IP y la definición de los protocolos de enrutamiento necesarios para garantizar la conectividad interna en el entorno SD-Access.

Además, de implementar las políticas de acceso y seguridad en el Fusion Device, de acuerdo con las directrices establecidas en el DNA Center y el ISE. Esto asegurará que los dispositivos finales que se conecten al Fusion Device cumplan con las políticas de seguridad y acceso definidas, y solo puedan acceder a los servicios compartidos y recursos autorizados.

Al completar este paso, se habrá llevado a cabo la configuración de los dispositivos de borde, como los switches Nexus, estableciendo la conexión con redes externas y garantizando la seguridad y el control de acceso. Además, se habrá configurado el dispositivo de fusión, el Fusion Device Catalyst 9500, para brindar acceso a los servicios compartidos y la conectividad adecuada dentro del entorno SD-Access. Esto permitirá un funcionamiento eficiente y seguro de la red, asegurando que tanto las comunicaciones externas como internas estén correctamente configuradas y protegidas.

### 4.6. Verificación y pruebas

En este paso, se deberá proceder con las pruebas de conectividad para asegurarse de que los dispositivos de la red puedan comunicarse correctamente y que se estén aplicando las políticas de seguridad y acceso definidas. Enviarán paquetes de prueba entre los diferentes dispositivos y debe verificar que se establezcan las conexiones esperadas, cabe mencionar que la conectividad existe sin embargo no centralizadas y conjuntamente a fin a las policitas y necesidades que desea alcanzar le empresa Mervas s.a.

Además de las pruebas de conectividad, se deben realizar con una verificación exhaustiva del funcionamiento de los servicios compartidos en la red

que ya existe. Esto implica verificar que servicios como DHCP (Dynamic Host Configuration Protocol), DNS (Domain Name System) y AAA (Authentication, Authorization, and Accounting) estén disponibles y operativos correctamente. Al igual que las pruebas de asignación de direcciones IP a los dispositivos finales, resolución de nombres de dominio y autenticación de usuarios para asegurarse de que estos servicios esenciales estén funcionando de manera óptima.

Por último, llevar a cabo esta propuesta conjuntamente con el departamento de sistema por motivo de innovación de la empresa, las pruebas de escalabilidad y rendimiento para evaluar el desempeño de la solución SD-Access y garantizar que cumpla con los requisitos de capacidad y eficiencia establecidos por la empresa. Esto puede implicar generar un alto volumen de tráfico en la red el cual persiste en la empresa con la finalidad de evaluar su capacidad de manejo y verificación de los dispositivos y enlaces estén dimensionados adecuadamente.

Una vez completados estos pasos con la propuesta, la solución SD-Access estará implementada teóricamente en la empresa Mervasa, permitiendo una gestión centralizada y automatizada de la red LAN. Es importante destacar que esta implementación teórica servirá como guía para una futura implementación real, adaptando los pasos y configuraciones según las necesidades y requisitos específicos de la empresa.

## CONCLUSIONES

Se realizó un análisis exhaustivo de la infraestructura de red existente en Mervasa. Esto permitió identificar las fortalezas y debilidades de la red, así como los desafíos que enfrentaba en términos de gestión y seguridad. El diagnóstico proporcionó una base sólida para el diseño de la solución SD-Access.

Se estableció el proceso de SD- Access por su principal acción que es proporcionar la posibilidad de que los usuarios entren bajo un control y acceso con los estándares de CISCO. Estas políticas garantizaron la protección de los activos de información de Mervasa y permitieron una gestión centralizada y automatizada de la red LAN. Al seguir las mejores prácticas de CISCO, se aseguró la confiabilidad y la integridad de la red.

Se diseñó una infraestructura de red optimizada utilizando la solución SD-Access de CISCO. Se tuvieron en cuenta los periféricos y dispositivos necesarios para implementar la solución, como el DNA Center, los controladores LAN inalámbricos (WLC), el Border Node y el dispositivo de Fusión. Este diseño aseguró una gestión eficiente y escalable de la red LAN de Mervasa.

La solución SD-Access resulta en beneficios significativos para Mervasa; ya que, la gestión centralizada y automatizada de la red LAN permite un control más eficiente y una respuesta más rápida a los cambios y requerimientos de la red. Además, las políticas de seguridad y acceso garantizaron la protección de los datos y la privacidad de la información de la empresa. La solución SD-Access también ofrece una experiencia de usuario mejorada que permite obtener una red más rápida, de mayor seguridad, más sencilla de gestionar y más eficiente.

## RECOMENDACIONES

En el caso de migrar redes externas a SD-Access que ya estén configuradas y en funcionamiento en los nodos finales, se propone la implementación de un switch externo. Esta solución permite establecer una conexión directa con el switch de fusión de la infraestructura externa de SD-Access.

Se considera que los switches compatibles con la solución SD-Access, como la serie Catalyst 9300, tenían un límite mínimo de velocidad de transmisión de 100 Mbps. Sin embargo, al migrar una red tradicional, se encuentran dispositivos que operaban a 10 Mbps, Por lo tanto, se recomienda un estudio de las velocidades de funcionamiento de cada dispositivo de la red para asegurar que todos funcionaran correctamente al migrar a SD-Access.

Se recomienda contar con un mapeo completo de todos los segmentos de red presentes en la red LAN tradicional. Esto era crucial para asegurar que, durante la migración a SD-Access, los dispositivos en esa red no perdieran conectividad cuando se encontraran fuera de su ubicación original. es de suma importancia garantizar que los usuarios no se queden sin acceso a la red al migrar su red tradicional a SD-Access.

## REFERENCIAS Y BIBLIOGRAFÍAS


Chafloque Mejia, J. D. (2018). Propuesta de diseño de una red de datos de área local bajo la arquitectura de redes definidas por software para la Red Telemática de la Universidad Nacional Mayor de San Marcos.

Chafloque, J. (2018). Propuesta de diseño de una red de datos de área local bajo la arquitectura de redes definidas por software para la Red Telemática de la Universidad Nacional Mayor de San Marcos [Undergraduate thesis, Universidad Nacional Mayor de San Marcos]. Retrieved from https://cybertesis.unmsm.edu.pe/handle/20.500.12672/10017

Chara Conocc, J. V. A., & San Martin Soria, F. R. (2022). Diseño de una gestión centralizada y automatización de la red lan utilizando la solución cisco SD-Access en una empresa de aeronavegación.

Cisco. (2016). Authentication, Authorization, and Accounting Configuration Guide – Cisco IOS Release 15M&T. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/15-mt/sec-usr-aaa-15-mt-book.pdf

Cisco. (2019). Aprovisionamiento de fabric de Software-Defined Access. Guía de implementación prescriptiva. https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Campus/Localization/sda-fabric-deploy-2019jul_es_es.pdf

Cisco. (2019). Cisco Software-Defined Access – Enabling intent-based networking (2nd ed.). https://www.cisco.com/c/dam/en/us/products/se/2018/1/Collateral/nb-06-software-defined-access-ebook-en.pdf

Cisco. (n.d.). At a Glance: Cisco Software-Defined Access. https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/software-defined-access/at-a-glance-c45-738181.pdf

Cisco. (n.d.). Cisco Catalyst 9300 Series Switches Data Sheet. https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.pdf

Cisco. (n.d.). Cisco data center spine-and-leaf architecture: Design overview white

Cisco. (n.d.). Cisco DNA Center 2.2.2.0 Data Sheet. https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06-dna-center-data-sheet-cte-en.pdf

Cisco. (n.d.). Cisco Identity Services Engine Data Sheet. https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/data_sheet_c78-656174.pdf

Cisco. (n.d.). Cisco Nexus 9300-EX Series Switches Data Sheet. https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-742283.pdf

Cisco. (n.d.). Cisco Prime Infrastructure 3.x Data Sheet. https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/prime-infrastructure/datasheet-c78-735696.pdf

Cisco. (n.d.). Cisco Software-Defined Access: Introducing an Entirely New Era in Networking Solution Overview. https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/software-defined-access/solution-overview-c22-739012.pdf

Cisco. (n.d.). Cisco Software-Defined Networking: Different Solutions for Different Needs White Paper. https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-735863.pdf

Cisco. (n.d.). Configure VXLAN. https://www.cisco.com/c/en/us/support/docs/switches/nexus-9000-series-switches/118978-config-vxlan-00.pdf

Cisco. (n.d.). Guía de configuración BGP [System configuration guide]. Retrieved from https://www.cisco.com/c/es_mx/support/docs/ip/border-gateway-protocol-bgp/17612-bgp.pdf

Cisco. (n.d.). Intermediate System-to-Intermediate System (IS-IS) [Web page]. Retrieved from https://www.cisco.com/c/en/us/products/ios-nx-os-software/intermediate-system-to-intermediate-system-isis/index.html#:~:text=IS%2DIS%20is%20a%20link,ongoing%20enhancements%20to%20the%20protocol

Cisco. (n.d.). Virtual route forwarding design guide. https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucme/vrf/design/guide/vrfDesignGuide.pdf

Copara Suárez, W. Z. (2022). Automatización de redes utilizadas para EOT: automatización de seguridades para redes EOT (Bachelor's thesis, Quito: EPN, 2022.).

Cuba, G., & Becerra, J. (2015). Diseño e implementación de un controlador SDN/OpenFlow para una red de campus académica [Undergraduate thesis, Pontificia Universidad Católica del Perú]. Retrieved from https://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/7149

Data Collection Concepts – Cisco Prime Infrastructure 3.1, Cisco. (2017). Retrieved from https://www.cisco.com/c/dam/en_us/training-events/product-training/prime-infrastructure-31/ja-datacoll/PI31_DataCollectionConcepts.pdf

Design Zone for Campus - Cisco SD-Access Solution Design Guide (CVD). Cisco. (n.d.). Retrieved from

https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-design-guide.pdf

Erazo Solarte, L. F. (2020). Automatización de la configuración de los servicios Carrier Ethernet e IP Next Generation (CE/IPNG) en la topología de red MPLS Huawei de InterNexa Colombia.

Espinoza, E. (2018). Desarrollo e implementación de un sistema de control de acceso a redes inalámbricas mediante RADIUS [Undergraduate thesis, Universidad Nacional Mayor de San Marcos]. Retrieved from http://cybertesis.unmsm.edu.pe/bitstream/handle/20.500.12672/10018/Espinoza_ae.pdf?sequence=1&isAllowed=y

Huawei. (n.d.). VXLAN Configuration - S7700 V200R011C10 Configuration Guide - VXLAN. https://support.huawei.com/enterprise/en/doc/EDOC1000178306/2f28023c/vxlan-configuration

IBM. (2014). Redes – Sistema de nombres de dominio (DNS). https://www.ibm.com/docs/es/ssw_ibm_i_72/rzakk/rzakkpdf.pdf

INCIBE – Instituto Nacional de Ciberseguridad. (n.d.). Seguridad en redes wifi: una guía de aproximación para el empresario. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia-de-seguridad-en-redes-wifi.pdf

Jiménez Botero, D. F., & Patiño Gómez, J. G. (2018). Diseño e implementación de una infraestructura de gestión centralizada para la administración de estaciones de trabajo y servicios de red con sistema operativo LINUX.

Karhunen, P. (2020). Improving Information Security in Healthcare Networks With Software-Defined Networking.

Karmarkar, K. (2017). DNA Software Defined-Access – Integrating with Existing Network [Conference session]. Cisco Live!. Retrieved from https://www.ciscolive.com/c/dam/r/c

L. Hernández, R. García & C. Macías. (2017). Tutorial para diseño y configuración de redes WLAN considerando el estándar 802.11n [Tesis de Pregrado, Universidad Cooperativa de Colombia]. https://repository.ucc.edu.co/bitstream/20.500.12494/7481/1/2017_tutorial_configuracion_wlan.pdf

López, F. (2002). El estándar IEEE 802.11 Wireless LAN [Research paper, Universidad Politécnica de Madrid]. Retrieved from https://www.dit.upm.es/~david/tar/trabajos2002/08-802.11-Francisco-Lopez-Ortiz-res.pdf

López. (2017). Diseño y simulación con ISE (identity services engine) para mitigar accesos no autorizados a una red corporativa [Tesis de Pregrado, Universidad Tecnológica del Perú]. https://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/935/Carlos%20Lopez_Tesis_Titulo%20Profesional_2017.pdf?sequence=1&isAllowed=y

M. Hospina. (2017). Diseño e implementación de VLANS para mejorar la eficiencia en la transmisión de datos en la Municipalidad Provincial de Huancayo [Tesis de Pregrado, Universidad Nacional del Centro del Perú]. http://repositorio.uncp.edu.pe/bitstream/handle/UNCP/5038/T010_47190108_T.pdf?sequence=1&isAllowed=y

Nakao, L. Peterson & A. Bavier. (2003). A Routing Underlay for Overlay Networks [Paper, Princeton University]. https://www.cs.princeton.edu/courses/archive/fall06/cos561/papers/nakao03.pdf

Nuñez, A. (2015). Red Definida por Software (SDN) en base a una infraestructura de software de libre distribución [Undergraduate thesis, Universidad Técnica de Ambato]. Repositorio Institucional UTA. https://repositorio.uta.edu.ec/jspui/bitstream/123456789/10587/1/Thesis_982ec.pdf

Ponce Yumbato, G. (2020). SD-ACCESS, Redes Definidas por Software.

Reina, F., & Ruiz, J. (2002). Redes de área local [Research paper, Universidad Nacional del Nordeste]. Retrieved from http://ing.unne.edu.ar/pub/local.pdf

Rodríguez, E. (2020). Diseño y simulación de una red definida por software para la implementación de un laboratorio avanzado de datos para la EP de Telecomunicaciones de la Facultad de Ingeniería Electrónica y Eléctrica de la Universidad Nacional Mayor de San Marcos [Undergraduate thesis, Universidad Nacional Mayor de San Marcos]. Retrieved from https://cybertesis.unmsm.edu.pe/bitstream/handle/20.500.12672/16021/Rodriguez_ge.pdf?sequence=1&isAllowed=y

Salazar Chacón, G. D. (2021). Hybrid Networking SDN y SD-WAN: Interoperabilidad de arquitecturas de redes tradicionales y redes definidas por software en la era de la digitalización (Doctoral dissertation, Universidad Nacional de La Plata).

Smeke, J. A. M. (2012). Programación y Aplicación de Redes Industriales con Controladores Lógicos (Doctoral dissertation, Universidad Autónoma de Querétaro).

T. Hess, & N. Matau. (2016). Enterprise Network Virtualization using IP and MPLS Technologies: Introduction [Conference session]. Cisco Live!. https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2016/pdf/LTRMPL-2102.pdf

V. Hafner. (2019). Cisco SD-Access – Connecting to the Data Center, Firewall, WAN and More [White paper]. Cisco IMAGINE INTUITIVE. https://www.cisco.com/c/dam/m/hr_hr/training-events/2019/cisco-connect/pdf/VH-Cisco-SD-Access-Connecting.pdf

Vargas Pérez, L. G. (2022). Automatización e integración de sistemas para los dispositivos de red en las compañías de la industria de telecomunicaciones en América Latina.

VÉLEZ, A., & FERNANDA, M. (2022). ESTUDIO DE FACTIBILIDAD PARA LA AUTOMATIZACIÓN DE PROCESOS EN LA DESINFECCIÓN Y PREVENCIÓN DE VIRUS COVID-19. Jipijapa. UNESUM. Facultad de Ciencias Tecnicas. 88pg (Bachelor's thesis, Jijpijapa. UNESUM).

VMware. (n.d.). NSX-T Data Center Quick Start Guide. VMware Docs Home. https://docs.vmware.com/es/VMware-NSX-T-Data-Center/3.1/nsxt_31_admin.pdf

W. Intriago. (2017). Estudio del protocolo Openflow usando el modelo de red definida por Software (Software Define Networks). Caso de estudio la Universidad Técnica de Manabí [Tesis de Pregrado].

W. Stallings, Redes e Internet de alta velocidad: protocolos de transporte y aplicación, 2da edición, Madrid, España: Pearson Educación, 1999.

X. Wu, J. Zhang & W. Lou, “Secure and Efficient Data Transmission for Cluster-based Wireless Sensor Networks”, IEEE Transactions on Parallel and Distributed Systems, vol. 19, no. 7, pp. 939-948, 2008. DOI: 10.1109/TPDS.2007.70778.

Y. Liu & D. Agrawal, “An Energy-Efficient Reliable Data Collection Framework for Wireless Sensor Networks”, IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 2, pp. 369-378, 2013. DOI: 10.1109/TPDS.2012.138.

Z. Xu, Y. Wang, K. Liu & J. Wang, “Fast and Lightweight Inter-Controller Communication for OpenFlow-Based Software Defined Networks”, Journal of Network and Systems Management, vol. 24, no. 1, pp. 118-136, 2016. DOI: 10.1007/s10922-014-9336-9.