Implementación de soluciones SDN en redes NGN para optimizar la gestión de tráfico y la eficiencia de la red

Edgar Javier Vargas Sosa

Asesor: Javier Enrique Arévalo Peña

Universidad Nacional Abierta y a Distancia - UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería - ECBTI

Especialización Redes de Nueva Generación

2026

Agradecimientos

Quiero expresar mi más sincero agradecimiento a todas aquellas personas y entidades que aportaron, de manera considerable, su ayuda para la elaboración de esta monografía; en primer lugar, agradecer a mi familia, ya que su apoyo incondicional y su ánimo constante fueron decisivos para solventar los obstáculos en los que me vi enfrentado a confianza en mí fue una fuente inagotable de motivación.

A mi tutor/a, gracias por su sabiduría, su templanza y sabias recomendaciones que me ayudaron a desarrollar la investigación adecuadamente. Su dedicación y su saber hacer fueron clave para abordar y fundamentar este trabajo.

También quiero mostrar mi gratitud a todos/as compañeros/as y amigos/as que, con sus aportaciones, sus críticas y sus comentarios, enriquecieron cada una de las etapas de la investigación. Su disposición y generosidad para intercambiar ideas y experiencias fueron inestimables.

Por último, agradecer a la Universidad y a sus docentes por contribuir a facilitar un entorno académico y de recursos que hicieron posible el desarrollo de este trabajo. A todos vosotros/as, gracias por ser partícipes de mi éxito.

Compromiso de autor

Yo Edgar Javier Vargas Sosa con documento de identidad número 1020733585 y estudiante del programa de especialización de redes de nueva generación NGN doy fe que:

El contenido del presente documento es un fiel reflejo de un trabajo arduo y una investigación elaboradas por mi persona y manifiesto que, cualquier notificación de plagio, copia o falta de fuente original, soy responsable en cuanto a todo sin recargar al asesor del trabajo, a la universidad y a cuantas personas hayan colaborado en el trabajo del que se trata.

Resumen

El presente trabajo monográfico trata sobre la implementación de las Redes Definidas por Software (SDN) en las Redes de Nueva Generación (NGN) como una alternativa innovadora que permita controlar el tráfico de red y mejorar la eficiencia operativa de las telecomunicaciones, así como las ventajas y los inconvenientes de esta integración de tecnologías, prestando particular interés a la centralización del control de la red, a la reducción de la latencia y a la mejora de la calidad de servicio (QoS). El trabajo analiza casos de éxito a nivel internacional y regional con un enfoque particular en las implementaciones realizadas en Colombia, así como verificar también el coste, la eficiencia, como la rentabilidad que producen la transición hacia SDN y SD-WAN. Adicionalmente, se identifican los retos relacionados con la interoperabilidad, seguridad y capacitación del personal técnico, proponiendo estrategias y marcos de buenas prácticas para una adopción efectiva de estas tecnologías. Este análisis busca ofrecer una referencia valiosa para operadores y empresas que enfrentan los desafíos de la creciente demanda de conectividad, destacando la importancia de las redes SDN como un pilar esencial en el futuro de las telecomunicaciones.

Palabras clave: SD-WAN, redes definidas por software, redes de nueva generación.

Abstract

This monograph addresses the implementation of Software-Defined Networking (SDN) in Next-Generation Networks (NGN) as an innovative solution to optimize traffic management and enhance operational efficiency in telecommunications. The study analyzes the advantages and challenges of this technological integration, emphasizing SDN's capability to centralize network control, reduce latency, and improve Quality of Service (QoS). The research reviews significant global and regional success cases, with a particular focus on implementations in Colombia. It also explores financial implications, highlighting how transitioning to SDN and SD-WAN can achieve significant cost savings and improve network scalability. Additionally, the study identifies challenges related to interoperability, security, and technical staff training, proposing strategies and best practices for effective adoption of these technologies. This analysis aims to provide a valuable reference for operators and companies facing the challenges of increasing connectivity demands, underscoring the importance of SDN networks as a cornerstone for the future of telecommunications.

Keywords: SD-WAN, software-defined networks, next-generation networks.

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Lista de Apéndices

Introducción

La necesidad creciente de servicios de alta velocidad y el aumento de aplicaciones y dispositivos interconectados representa un reto en la gestión y operación de las redes de telecomunicaciones. Las redes de nueva generación emergieron como una solución para ofrecer múltiples servicios sobre una única infraestructura, proporcionando flexibilidad y escalabilidad. Sin embargo, las nuevas redes requieren herramientas avanzadas que permitan gestionar el tráfico de datos en tiempo real, optimizar el rendimiento y ofrecer calidad de servicio QoS. En este contexto las redes definidas por software SDN son capaces de ofrecer una solución innovadora que permite a los administradores gestionar de forma centralizada y programable la infraestructura de la red.

SDN supone un cambio de modelo respecto a la arquitectura de red clásica debido a la separación del plano de control de datos que proporciona mayores flexibilidad y adaptabilidad a la hora de gestionar el tráfico y los recursos de red. Esta separación no solo permite una mejor asignación de recursos, sino que también permite la automatización y la programación de políticas de red en tiempo real que mejoran la eficiencia operativa y la rápida respuesta a las demandas de los usuarios y las aplicaciones (Paul Goransson, 2016) (Kreutz, 2015).

Con esta investigación se busca analizar la implementación de soluciones SDN sobre redes NGN, centrándose con como estas tecnologías pueden optimizar la gestión del tráfico y mejorar la eficiencia de la red en general.

Problema

Planteamiento del Problema

Con el avance acelerado de las aplicaciones que requieren un gran ancho de banda como el streaming, las videoconferencias, el vídeo en 4K, la realidad virtual y los servicios en la nube, las redes NGN tienen dificultades significativas en la gestión del tráfico y en la optimización de los recursos. Las redes tradicionales legacy presentan una falta de flexibilidad para hacer frente al crecimiento del tráfico en tiempo real, y tiene un efecto negativo sobre la calidad del servicio, aumenta los costos de operación por la sobrecarga e ineficiencia de la infraestructura (Kreutz, 2015).

Las redes SDN surgen como una solución para mejorar la gestión del tráfico de redes NGN, gracias a la programación centralizada y a una arquitectura centrada en la separación entre el plano de control y el plano de datos, haciendo la respuesta más dinámica ante la demanda de tráfico (Paul Goransson, 2016). La arquitectura SDN favorece la automatización y la adaptación a cambios en las condiciones del tráfico, lo que permite a los operadores de la red responder con mayor rapidez a las fluctuaciones de la demanda, mejorando la experiencia del servicio para el usuario final.

No obstante, no podemos obviar el hecho de que la inclusión de SDN en entornos NGN, esconde muchos inconvenientes; las infraestructuras de red tradicionales tienen dificultades de interoperabilidad y la integración de SDN en una nueva red, puede ser un desafío importante. Y, finalmente, la centralización del control, si bien es buena para la administración y la flexibilidad, introduce nuevos riesgos de seguridad, puesto que es un punto central que puede ser objetivo de ataques (Raj Jain, 2013).

Tabla 1

Tabla de Riesgos de Seguridad en la Implementación de Controladores Centralizados SDN.

Riesgo de seguridad	Descripción	Impacto	Mitigación
Ataques de denegación de servicio DoS	Un atacante puede saturar el controlador central con un gran volumen de solicitudes, impidiendo que gestione la red.	Alta	Implementar técnicas de balanceo de carga y mecanismos de detección temprana de ataques.
Compromiso del Controlador	Dado que el controlador es el punto central de control, su compromiso puede permitir a un atacante obtener control total de la red.	Crítico	Uso de autenticación fuerte, cifrado de comunicaciones y segmentación del controlador.
Intercepción de Tráfico	Un atacante podría interceptar o manipular el tráfico entre dispositivos y el controlador al explotar vulnerabilidades en el canal de comunicación.	Alta	Implementar cifrado TLS en las comunicaciones entre el controlador y los dispositivos.
Modificación de Políticas	Un atacante que accede al controlador puede modificar las políticas de red, redirigiendo o bloqueando el tráfico.	Crítico	Configurar autenticación multi-factor para el acceso al controlador y monitorear logs.
Amenazas de Insiders	Empleados con acceso al controlador pueden realizar cambios maliciosos o no autorizados.	Media	Aplicar control de acceso basado en roles (RBAC) y auditorías regulares.
Fallas en la Resiliencia	La dependencia de un único controlador central puede llevar a un punto único de fallo.	Alta	Implementar controladores redundantes y protocolos de alta disponibilidad.

Nota. Esta tabla presenta los principales riesgos de seguridad asociados con la implementación de controladores centralizados en redes definidas por software (SDN), así como sus posibles impactos y estrategias de mitigación. *Adaptado de.* Software Defined Networks: A Comprehensive Approach (2016) de Paul Goransson y Chuck Black, y Software Defined Networking (2013) de Raj Jain.

Con el incremento de la demanda global de tráfico, incentivada por la adopción masiva de dispositivos del Internet de las Cosas y de los servicios en la nube, la capacidad de las redes para escalar y mantener una calidad del servicio óptima se encuentra amenazada. Las soluciones de red tradicionales tienen dificultades para manejar el volumen de tráfico actual, lo que provoca degradación del servicio y aumento de costos operativos (Cisco Systems, 2023). Por este motivo, los operadores están intentando orientar el uso de SDN como medio para mejorar el uso de los recursos de red, incrementar la calidad del servicio y disminuir costos (Bruno Astuto A. Nunes, 2014).

Tabla 2

Cuadro Comparativo de Costos de Implementación: Redes Tradicionales vs Redes SDN

Característica	Redes Tradicionales	Redes SDN	Ejemplos Reales	Indicadores Clave de Desempeño (KPI)
Costos de Equipos	Altos, debido a la necesidad de switches y routers propietarios de alto costo.	Reducidos, ya que se utilizan switches genéricos controlados por software.	La implementación de SD-WAN por Cisco ha demostrado reducir costos de hardware en empresas como Capital One en un 30%	Reducción del costo por dispositivo: Evaluación de los costos totales de hardware antes y después de la implementación (disminución del 30%-50%)
Costos de Mantenimiento	Elevados, ya que cada dispositivo requiere configuración y actualización manual.	Menores, debido a la automatización y centralización del control.	La Universidad Politécnica de Cataluña reportó una reducción del 40% en costos de mantenimiento al migrar a SDN.	Reducción del tiempo de mantenimiento: Número de horas dedicadas a la configuración y soporte por dispositivo antes y después de SDN.
Escalabilidad	Limitada y costosa, requiere actualización de hardware para aumentar la capacidad.	Altamente escalable mediante la adición de controladores y recursos virtuales.	La red de Microsoft Azure utiliza SDN para escalar de forma dinámica sus centros de datos.	Incremento en la capacidad de red: Cantidad de nodos o dispositivos adicionales que se pueden incorporar

				sin interrupciones (incremento del 40%-60%)
Tiempo de Implementación	Prolongado, debido a la configuración manual de cada dispositivo.	Rápido, ya que la configuración se gestiona desde un punto central.	Google ha implementado SDN en sus centros de datos, reduciendo el tiempo de aprovisionamiento en un 50%.	Reducción del tiempo de aprovisionamiento: Tiempo promedio para implementar nuevos dispositivos o servicios en la red (reducción del 30%-50%)
Flexibilidad	Baja, debido a la falta de centralización en el control de la red.	Alta, permite la reconfiguración dinámica sin necesidad de cambiar hardware.	Amazon AWS reportó un aumento del 60% en la eficiencia operativa gracias a SDN.	Eficiencia operativa: Evaluación de la capacidad para ajustar configuraciones de red en tiempo real y sin interrupciones (mejoras operativas del 50%-70%).
Latencia	Alta, debido a rutas ineficientes y congestión en la red.	Baja, gracias a la optimización de rutas mediante controladores centralizados.	Cisco reportó una disminución del 40% en la latencia de redes corporativas implementadas con SD-WAN.	Latencia promedio: Tiempo de ida y vuelta para paquetes de datos (disminución del 30%-50%).
Ancho de Banda	Subutilizado debido a la falta de priorización y balance de tráfico.	Mejor aprovechamiento mediante la priorización dinámica de aplicaciones y balance de carga.	Vodafone Colombia optimizó el uso del ancho de banda en un 60% al implementar SD-WAN.	Uso del ancho de banda: Medición del porcentaje de utilización efectiva del ancho de banda total disponible antes y después de la implementación.
QoS (Calidad de Servicio)	Limitada, con prioridades de tráfico rígidas y sin flexibilidad para cambios dinámicos.	Mejorada, mediante políticas dinámicas que priorizan aplicaciones críticas en tiempo real.	BBVA Colombia mejoró los niveles de QoS en sus sucursales al implementar políticas automatizadas con Cisco SD-WAN.	Nivel de cumplimiento de QoS: Porcentaje de cumplimiento de los parámetros establecidos (latencia, pérdida de paquetes, jitter)

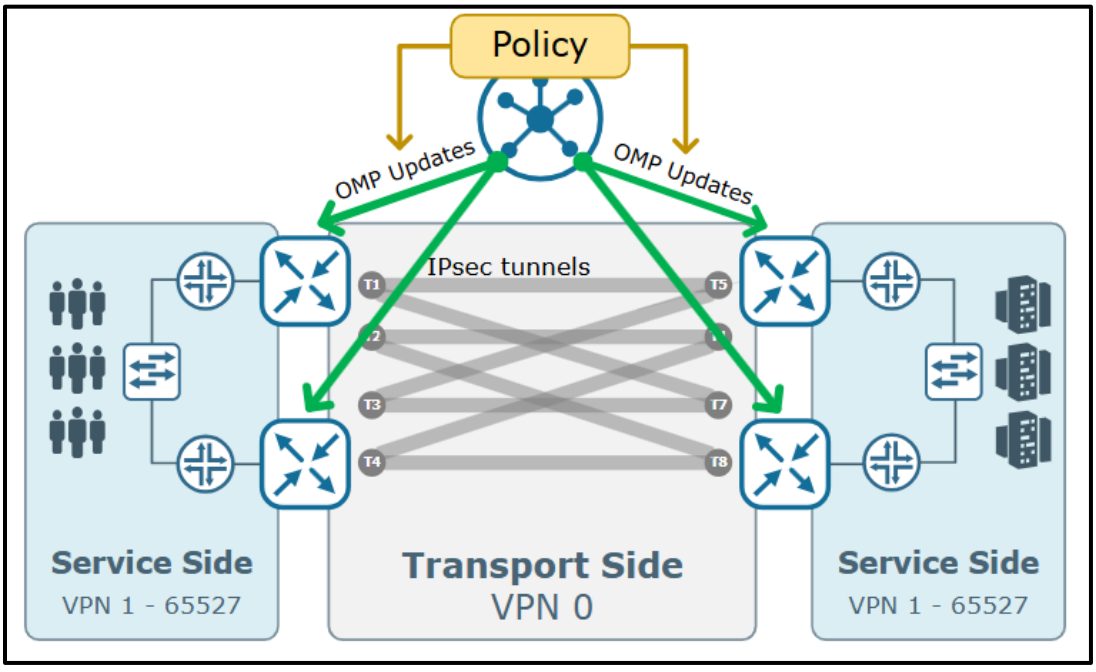
	en aplicaciones críticas (aumento del 40%-70%).

Nota. Esta tabla presenta una comparación entre redes tradicionales y redes definidas por software (SDN), considerando aspectos de costos, desempeño y eficiencia operativa, junto con ejemplos reales de implementación. *Adaptado de* Cisco Systems (2023) y Nunes, B. A. A. et al. (2014).

Además, en NGN la utilización de SDN permite una gestión centralizada basada en políticas que puede priorizar diferentes tipos de tráfico instantáneamente, mejorando el uso del ancho de banda y la calidad de servicio. Es relevante tener en cuenta que los operadores deben también el presupuesto para formación de personal y adaptación de su infraestructura para afrontar las nuevas tecnologías de forma óptima (Garavito, 2022).

Figura 1

Gestión de la Red Mediante Políticas Centralizadas



Nota. Tomado de NetworkAcademy (2020*).*

Finalmente alcanzamos la conclusión de que la necesidad de contar con redes no sólo más eficientes sino también más flexibles surge como un requerimiento directamente proporcional al transmitir información con la misma velocidad que surge una creciente demanda de conectividad. El uso de redes SDN sobre NGN supone una respuesta factible aunque no está exenta de dificultades a resolver convenientemente antes de abordar la migración. Por ello la investigación en métodos que coronen dicha integración para una migración de calidad del servicio y satisfacer la eficiencia operativa son de vital importancia.

Antecedentes Históricos

Las redes que son implementadas con tecnología SDN (Software Defined Networks) permitirán reconfigurar la red de forma más eficiente y flexible en tiempo real. Se mejorará la aparición de imprevistos cuando haya congestión o fluctuaciones del tráfico. Las soluciones SDN permiten centralizar el control de toda la red, optimizando la asignación de rutas y recursos haciendo uso de algoritmos avanzados que monitorean y analizan el tráfico para reducir la latencia y mejorar la calidad del servicio (Cisco Systems, 2023) (Hassan, Arlimatti, Elbreiki, & Habbal, 2016). Sin embargo la arquitectura SDN también implica retos como la seguridad centralizada del controlador y la complejidad en la integración con sistemas legados (legacy) que tendrá que ser afrontados para lograr una implementación de sistema seguro y efectivo (Kreutz, 2015) (Bruno Astuto A. Nunes, 2014).

Definición del Problema

Problema General

¿cómo puede la adopción de soluciones SDN sobre redes NGN optimizar la gestión del tráfico y mejorar la eficiencia de la red para soportar adecuadamente las demandas actuales de conectividad y calidad de servicio?

Problemas Específicos

¿Cómo la centralización del plano de control en SDN puede mejorar la capacidad de respuesta ante eventos de congestión de tráfico en tiempo real en redes NGN?

¿Cuáles son los desafíos de interoperabilidad y seguridad con la integración de redes SDN con NGN y de qué manera se pueden abordar correctamente?

Este enunciado pone de manifiesto la necesidad de un sistema de gestión más inteligente y adaptable de las redes modernas que optimice el tráfico y minimice los costes que se relacionan con las tradicionales infraestructuras rígidas, al tiempo que permitiría a las redes de nueva generación facilitar la creciente demanda de servicios de calidad.

Justificación

Ante el auge de las aplicaciones que requieren un alto nivel de disponibilidad, una baja latencia y un ancho de banda mayor, como el streaming de video, teletrabajo o los dispositivos IoT, han llevado a las redes tradicionales al límite (Cisco Systems, 2023); en este problema, las redes definidas por software SDN se ha convertido en una alternativa novedosa y atractiva, puesto que permiten administrarlas de forma flexible y eficiente, aprovechando así los recursos y aportando una mejor experiencia de los usuarios finales (Paul Goransson, 2016).

Las redes de nueva generación permiten la implementación de redes definidas por software SDN, ya que resulta fácil gestionar el tráfico de tiempo real. Para (Bruno Astuto A. Nunes, 2014) la integración de las redes de nueva generación y las SDN optimiza la infraestructura a la que se tiene acceso, además de permitir a los operadores un control centralizado de recursos que les permita priorizar el tráfico e información críticas y mejorando la calidad del servicio; la centralización de las SDN constituye una opción adecuada para mejorar la seguridad, ya que permite establecer normas o políticas más complejas y robustas que limitan el peligro de comprometer la estabilidad de la red (Raj Jain, 2013).

El presente trabajo resulta de interés para los operadores de telecomunicaciones que deseen apropiarse de tecnología nueva para mejorar todos sus procesos operacionales pues, al implementarse SDN en NGN, no solo optimiza la gestión del tráfico, sino que, además, reduce los costes operativos a través de la reconfiguración de los recursos (Kreutz, 2015); esta característica es extremamente importante en ambientes que son propensos a las fluctuaciones de la red de nivel alto ya que su explotación puede verse muy afectada por las demandas variables (Garavito, 2022).

Por otra parte, algunas investigaciones previas han demostrado que la implementación de las redes SDN, junto con la virtualización de funciones de red NFV, aportan a la recepción de servicios avanzados (tales como la computación en la nube y el IoT), y mejoran la reacción de las redes frente a las nuevas exigencias del mercado. Traídos por estudios realizados en la universidad politécnica de Cataluña, la combinación de SDN y NGN permitirá a las empresas reducir muy considerablemente la latencia y, además, incrementar la eficiencia operativa al priorizar los tipos de tráfico solicitados (Cataluña, Calidad de Servicio en Redes NGN, 2021).

Por último, esta investigación puede servir para promover el conocimiento de la implementación y adopción de buenas prácticas de la SDN en redes NGN, donde también podría ser un marco de referencia de uso para los operadores en la instalación de su infraestructura (Aplicadas, 2023). Los resultados de este estudio pueden ser utilizados por empresas de todas las industrias para incrementar su eficiencia operativa, aumentar la resiliencia de la red y aumentar la experiencia global del usuario dentro de un entorno siempre más digitalizado (Cataluña, Gestión y control de Calidad de Servicio de redes SDN en tiempo real, 2022).

Objetivos

Objetivo General

Evaluar la implementación de soluciones de Redes Definidas por Software (SDN) en Redes de Próxima Generación (NGN) para optimizar la gestión del tráfico y mejorar la eficiencia operativa en entornos de telecomunicaciones.

Objetivos Específicos

Analizar el impacto de la adopción de tecnologías SDN en la reducción de la latencia y la mejora de la calidad del servicio (QoS) en redes NGN.

Identificar los desafíos de seguridad y las soluciones necesarias para proteger las redes NGN basadas en SDN, garantizando su estabilidad y resiliencia ante amenazas.

Proponer un marco de buenas prácticas para la implementación de redes SDN en infraestructuras de telecomunicaciones, con el fin de optimizar el uso de recursos y reducir costos operativos.

Evaluar el impacto social y ambiental de las redes definidas por software, incluyendo aspectos como el acceso equitativo a la conectividad, la sostenibilidad energética, y la reducción de la huella ambiental en las redes de telecomunicaciones.

Marco Teórico

Marco Histórico

Las redes definidas por software, para ser más específicos las SDN, han modificado, en cierta forma, la arquitectura y el funcionamiento de las redes de telecomunicaciones. En la medida en que las redes de la nueva generación NGN, continúan expandiéndose para abastecer a la demando conectividad creciente por parte de los usuarios, las redes de la nueva generación SDN se convierten en una alternativa esencial para la administración del tráfico y la optimización del funcionamiento de la red.

Con el presente proyecto tratamos de sentar las bases necesarias y de tener un mejor entendimiento, en cuanto a las tecnologías SDN, de forma conjunta con las NGN sean capaces de mejorar la eficiencia de las redes de telecomunicaciones, mientras que se contempla la gestión del tráfico y la optimización de los recursos. (Cisco Systems, 2023). El presente proyecto investigativo pretende sentar las bases a partir de la cual ser capaz de comprender, como las tecnologías SDN, de forma conjunta con soluciones concretas como es el caso de SD-WAN, pueden mejorar de forma significativa la eficiencia operativa de las redes de telecomunicaciones, teniendo centrado el enfoque en la gestión del tráfico y la optimización de recursos.

Marco Conceptual

Redes de Próxima Generación (NGN)

Las redes de nueva generación NGN constituyen el ejemplo clásico de la práctica de gestionar las redes de telecomunicaciones. A diferencia de las redes tradicionales, donde cada servicio (datos, voz) dispone de una infraestructura dedicada, en las NGN se da la convergencia de los servicios sobre una infraestructura IP única que, además, permite reducir la complejidad de la implementación y de los costos de operación. Las NGN mejoran la escalabilidad y la

flexibilidad de la red (Next generation networks and IMS, 2021). Estas redes están destinadas a soportar la implantación de tecnologías emergentes como IoT y computación en la nube, obedeciendo a su carácter como plataforma avanzada de servicios (Next generation networks and IMS, 2021)

Las redes de nueva generación se orientan a los servicios avanzados, a saber, transmisión de datos a altas velocidades, transmisión de medios e interactividad, todos ellos por encima de una infraestructura compartida. La implementación de las NGN también permite la integración satisfactoria de las tecnologías emergentes como IoT y computación en la nube. (Next generation networks and IMS, 2021).

Redes Definidas por Software (SDN)

SDN es un enfoque de la arquitectura de redes, que separa el plano de control del plano de datos, lo que permite una gestión más flexible y programable de la red. En las redes tradicionales legacy, el plano de control y el plano de datos están integrados en un solo dispositivo, lo que aun actualmente limita la capacidad de los administradores para optimizar el tráfico de la red y responder más ágilmente a las demandas cambiantes. Con SDN el plano de control se separa en un controlador centralizado, mientras que el plano de datos se queda relegado a los dispositivos de red, que actúan bajo las órdenes del controlador (Kreutz, 2015).

Paul (2016) describen SDN como una tecnología revolucionaria la cual permite a los administradores de red programar la infraestructura de red, de manera similar a como se gestionan los recursos en la nube. Esto permite una mayor agilidad en la operación de la red y capacidad de optimizar el uso de los recursos.

Arquitectura de SDN

SDN se fundamenta en tres elementos principales: el plano de aplicación, el plano de control y el plano de datos.

Plano de aplicación. En este plano residen las aplicaciones y servicios que se comunican con la red a través de las API que les brinda el controlador SDN. El administrador puede modificar estas aplicaciones para desempeñar tareas específicas: la gestión del tráfico, la seguridad y la supervisión del rendimiento (Brandon Heller, 2012).

Plano de control. Este plano constituye el "corazón" de la arquitectura SDN. El controlador dirige, gestiona y controla todo el tráfico de datos que viaja a través de la red tomando decisiones basadas en políticas definidas y el estado de las condiciones del tráfico en tiempo real (Brandon Heller, 2012).

Plano de datos. Por último, el plano de datos se encarga del tráfico que se genera en la red. Los dispositivos de la red, como switches y routers, retransmiten los paquetes de datos bajo las órdenes y directrices dadas por el controlador SDN. Esa desconexión entre el plano de control y el plano de datos permite mayor flexibilidad y gestión del tráfico (Cisco Systems, 2023).

SDN en Redes NGN

La unión de redes de nueva generación con las SDN produce algunos beneficios importantes que son capaces de aumentar el rendimiento de las telecomunicaciones y la eficiencia en su operación en términos generales. Uno de los beneficios que se produce es que las redes SDN permiten optimizar el tráfico de la red, ya que los controladores proceden a realizar una optimización dinámica de la ruta de datos en tiempo real, proporcionando prioritización a algunos tipos de tráfico en función de las necesidades del usuario y el estado de la red. (Bruno Astuto A. Nunes, 2014).

La gestión que lleva a cabo SDN de las redes de nueva generación (NGN) para gestionar adecuadamente el tráfico de aplicaciones de banda ancha, tales como video streaming o aplicaciones en la nube, incluso logra optimizar la asignación de los recursos de la red para minimizar, al mismo tiempo, la latencia y maximizar el rendimiento. (Bruno Astuto A. Nunes, 2014).

Gestión del Tráfico y Optimización de Recursos

Uno de los principales beneficios de SDN es su capacidad para manejar de una forma dinámica y adaptativa el tráfico de la red. En la actualidad el tráfico de la red varía mucho y puede cambiar rápidamente dependiendo de las demandas de los usuarios. Las redes tradicionales no tienen la suficiente flexibilidad para reaccionar a estos cambios de forma efectiva, lo que puede llevar al congestionamiento de la red y la utilización de todo el potencial de la red - Zhaogang Shu (2016).

Por el contrario, SDN permite la aplicación de políticas para la gestión del tráfico en el cual el controlador centralizado puede modificar automáticamente las rutas de los datos para evitar cuellos de botella y que el uso de los recursos de la red sea efectivo. Según Zhaogang Shu (2016) el control centralizado que nos proporciona SDN es esencial ya que permite la recolección en tiempo real de datos sobre el estado de la red, pudiendo facilitar una gestión de tráfico proactiva.

Además, Cisco Systems (2023) indica que el uso de SD-WAN, una aplicación especifica de SDN para redes WAN, permite la optimización en el manejo del tráfico de manera eficiente en redes de nueva generación, mejorando no solamente el rendimiento de esa red sino también disminuyendo los costos operativos.

Seguridad en Redes de Nueva Generación NGN

La seguridad siempre ha sido una preocupación en cualquier red de telecomunicaciones, y las redes SDN no son menos. A pesar de que la SDN permite aún más flexibilidad y control sobre la propia red, también conlleva la introducción de nuevos riesgos de seguridad que deben ser asumidos. Uno de los retos básicos es que como se tiene centralizado el plano de control, este plano se convierte en una forma de punto para ataques cibernéticos (Cisco Systems, 2023).

(Cisco Systems, 2023) proporciona soluciones de seguridad específicas para SD-WAN, como por ejemplo la aplicación de políticas de seguridad centralizadas junto con la segmentación de la red para tratar de limitar el impacto de los ataques. Además, (Raj Jain, 2013) añaden que las redes SDN pueden implementar técnicas avanzadas de virtualización para aislar diferentes tipos de tráfico y así garantizar que los ataques en una parte de la red no se propaguén al resto de la red.

Virtualización de Redes SDN

La virtualización es una tecnología que se complementa de manera excepcional con la SDN, ya que permite a los operadores crear distintas redes virtuales sobre una sola infraestructura física, mejorando de este modo la eficiencia de los recursos y facilitando la implementación de políticas de seguridad y la optimización del tráfico (Raj Jain, 2013). (Kreutz, 2015) sostiene que la combinación de la virtualización de redes permite crear infraestructuras altamente escalables y flexibles capaces de adaptarse de forma rápida y sencilla a las exigencias cambiantes de usuarios y aplicaciones; esto resulta especialmente relevante en redes NGN, donde la demanda de servicios de alta velocidad y de baja latencia sigue creciendo.

Retos en la Implementación de SDN en NGN

Aunque son muchos los beneficios que proporciona SDN sobre NGN, hay que resolver muchos desafíos por delante que deben ser superados para poder llevar a cabo una implementación exitosa. Uno de los desafíos principales es la interoperabilidad entre las redes legacy y las redes SDN, dado que muchas redes NGN actuales se componen de tecnologías tradicionales que no son compatibles con SDN (Ashutosh Dutta, 2020).

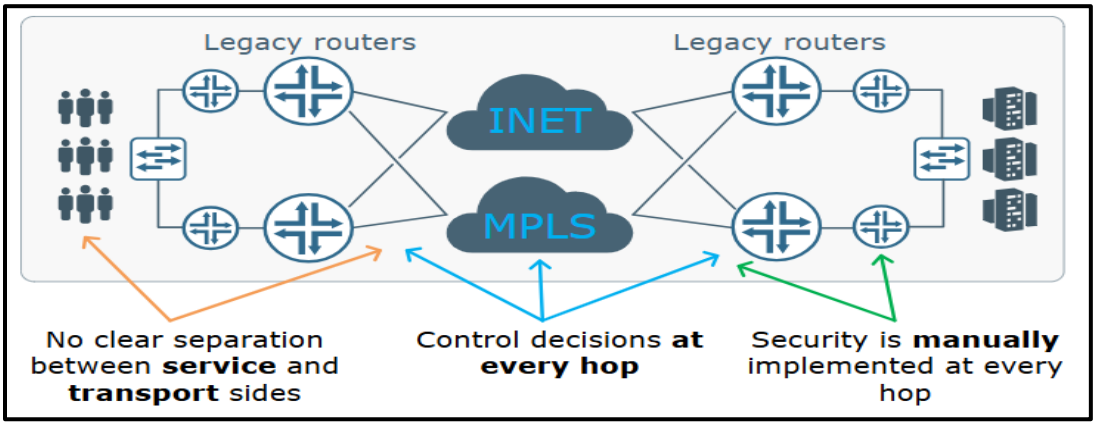
Por otro lado, (Ashutosh Dutta, 2020) observa otros desafíos que debe enfrentar SDN, como la escalabilidad del controlador SDN y la necesidad de mejorar la seguridad en redes distribuidas. Pero, también muestran que SDN tiene oportunidades que explorar como, por ejemplo, en el contexto de redes 5G, donde SDN puede llegar a ser de gran utilidad en la gestión del creciente consumo de datos y la complejidad de las redes.

SD-WAN: Extensión de SDN en Redes WAN

Cisco SD-WAN es una solución basada en los principios de SDN que mejora la conectividad y el rendimiento en el caso de las WAN (redes de área amplia). A diferencia de las arquitecturas WAN tradicionales que dependen de las costosas conexiones MPLS (Multiprotocol Label Switching) (MPLS), que si bien son más seguras son menos flexibles, SD-WAN permite utilizar conexiones menos costosas como el uso de Internet y LTE, con el consiguiente aumento de la flexibilidad, así como también de la reducción de los costos operativos (Cisco Systems, 2023).

Figura 2

Topología de la WAN Tradicional.



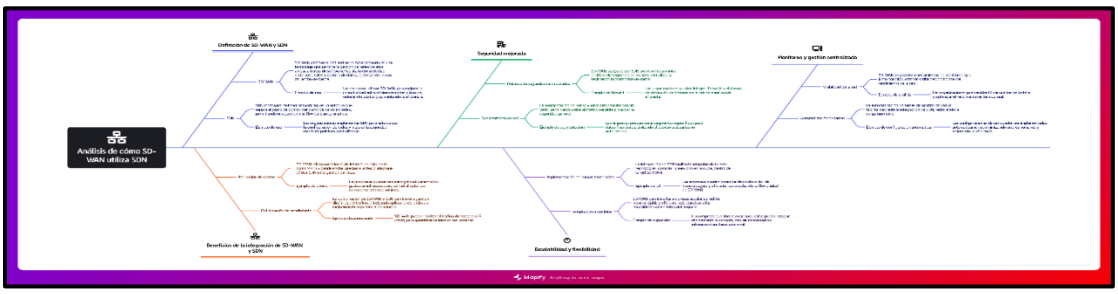
Nota. Tomado de NetworkAcademy (2020).

SDN Frente a SD-WAN

SD-WAN es, en muchos aspectos, SDN para la WAN. Es el caso de uso SDN mas popular y más ampliamente implementado, dada su popularidad; el modelo SDN se convirtió en el más popular para la abstracción de la infraestructura de red dentro del mismo centro de datos y otras secciones dentro del perímetro de la empresa. En la siguiente sección se observa cómo SD-WAN se sostiene en SDN.

Figura 3

Análisis de Como SD-WAN Utiliza SDN.



Nota. Adaptado de https://mapify.so/share-link/zvcI2YSLth

Principales Beneficios de SD-WAN en SDN Comparado con Redes Tradicionales

Flexibilidad y Escalabilidad. La solución SD-WAN facilita a las organizaciones la adaptación rápida a los cambios en la demanda del tráfico de red, dado que es capaz de gestionar el tráfico de forma dinámica, adaptándose a los diferentes escenarios de funcionamiento al escalar la infraestructura de red sin necesidad de realizar grandes configuraciones manuales para el tráfico de la red, la cual responde como mejor responde (Cisco Systems, 2023).

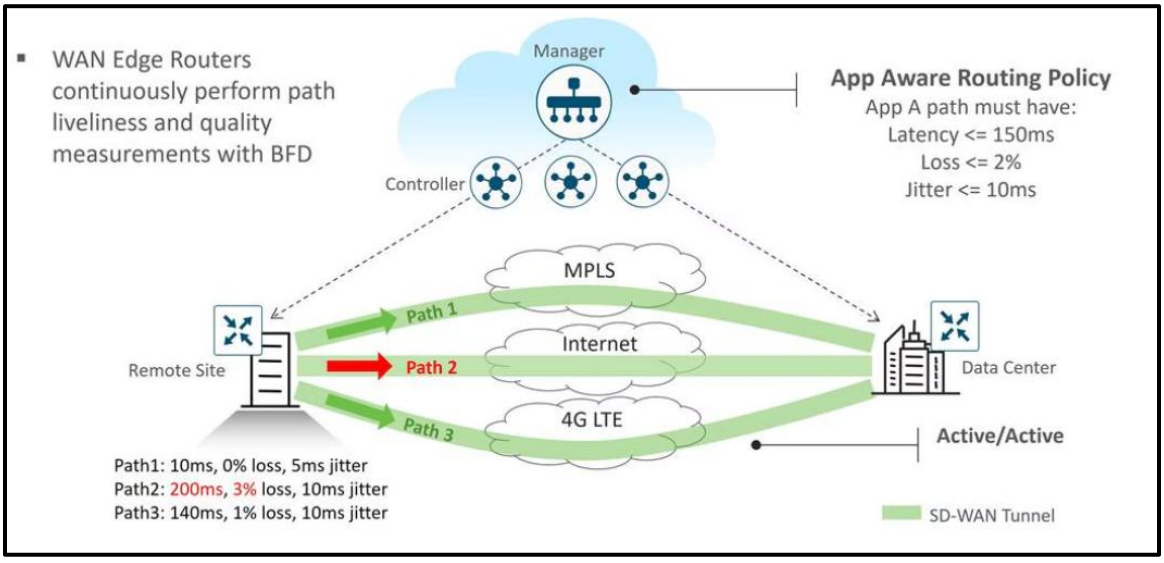
Por otro lado, las redes tradicionales tienden a requerir configuraciones manuales y no pueden adaptarse ante situaciones inesperadas o repentinas por lo que es difícil de operar (Cisco Systems, 2023).

Reducción de costos operativos. Las redes legacy tradicionales dependen de conexiones MPLS costosas para garantizar la calidad del servicio. SD-WAN, al aprovechar conexiones de menor costo como internet BA y LTE, puede reducir significativamente los costos sin dejar al lado la calidad del servicio. Al utilizar SDN para optimizar el tráfico, SD-WAN permite a las empresas minimizar los costos de infraestructura y mejorar el rendimiento de la red en general.

Optimización del tráfico y calidad de servicio (QoS). SD-WAN optimiza el tráfico mediante la selección automática de rutas, asegurando que las aplicaciones criticas reciban prioridad. Esto se realiza mediante controladores SDN que se encargan de analizar en tiempo real el estado de la red para optimizar el uso del ancho de banda y reducir la latencia. Al contrario, las redes tradicionales no tienen la capacidad de selección dinámica de rutas, lo que puede llevar a cuellos de botella y pérdida de calidad en aplicaciones sensibles al tiempo (Raj Jain, 2013).

Figura 4

Enrutamiento Basado en Aplicaciones.



Nota. Tomado de Cisco (2024). Representa la protección del tráfico mediante selección de la mejor ruta basada en el rendimiento.

Gestión Centralizada y Automatización

Con cisco SD-WAN, los administradores de red pueden gestionar toda la red desde una plataforma centralizada (como Cisco Vmanage), lo que simplifica la implementación de políticas y actualizaciones de red. Con las redes tradicionales se requieren configuraciones manuales en cada dispositivo, lo que es propenso a errores y consume mucho tiempo.

Elementos que Componen la Arquitectura SD-WAN de Cisco. La arquitectura de Cisco Catalyst SD-WAN se compone de planos separados de orquestación, gestión, control y datos.

El plano de orquestación ayuda a la incorporación automática de los enrutadores SD-WAN.

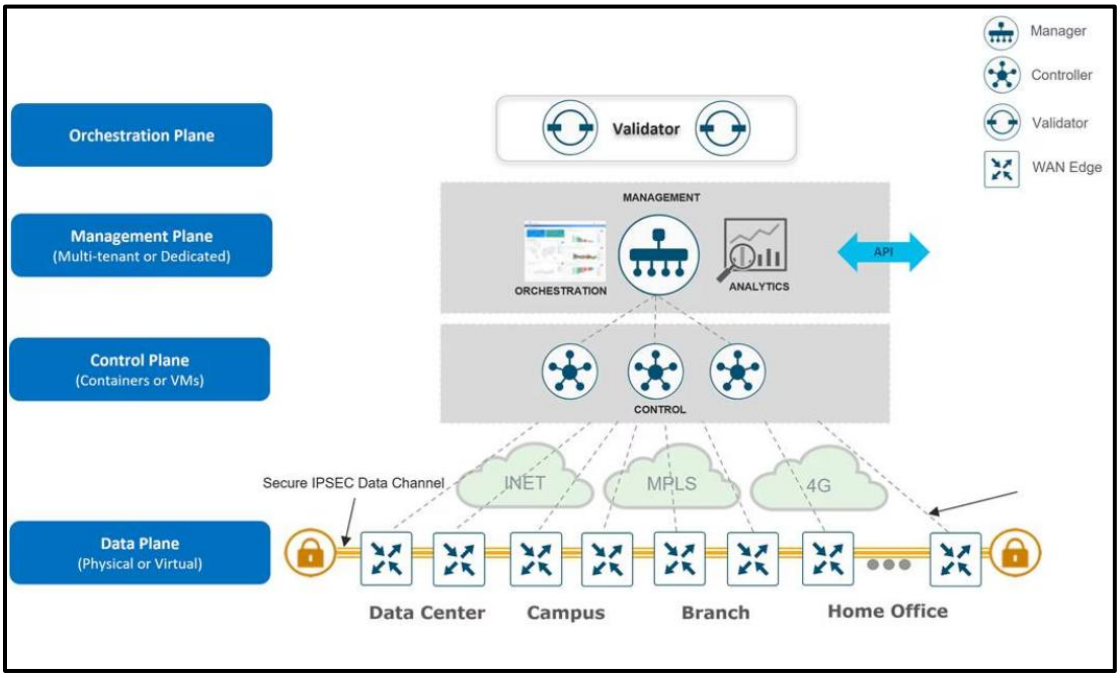
El plano de gestión es responsable de la configuración y la supervisión central.

El plano de control construye y mantiene la topología de la red y toma decisiones sobre donde fluye el tráfico.

El plano de datos es responsable de reenviar paquetes según las decisiones del plano de control.

Figura 5

Descripción General de los Planos que Componen la Solución Cisco Catalyst SD-WAN.



Nota. Tomado de Cisco (2024).

Los componentes principales de la solución de cisco para SD-WAN consisten en el sistema de administración de red mánager (plano de administración), el controlador SD-WAN (plano de control), el validador SD-WAN (plano de orquestación) y el enrutador WAN Edge (plano de datos).

SD-WAN Manager. Es el sistema de gestión de red centralizado, está basado en software y proporciona una interfaz gráfica de usuario para supervisar, configurar y mantener fácilmente

todos los dispositivos Cisco Catalyst SD-WAN y sus enlaces conectados en la red subyacente y superpuesta. Proporción un único panel de control para las operaciones (Cisco, 2024).

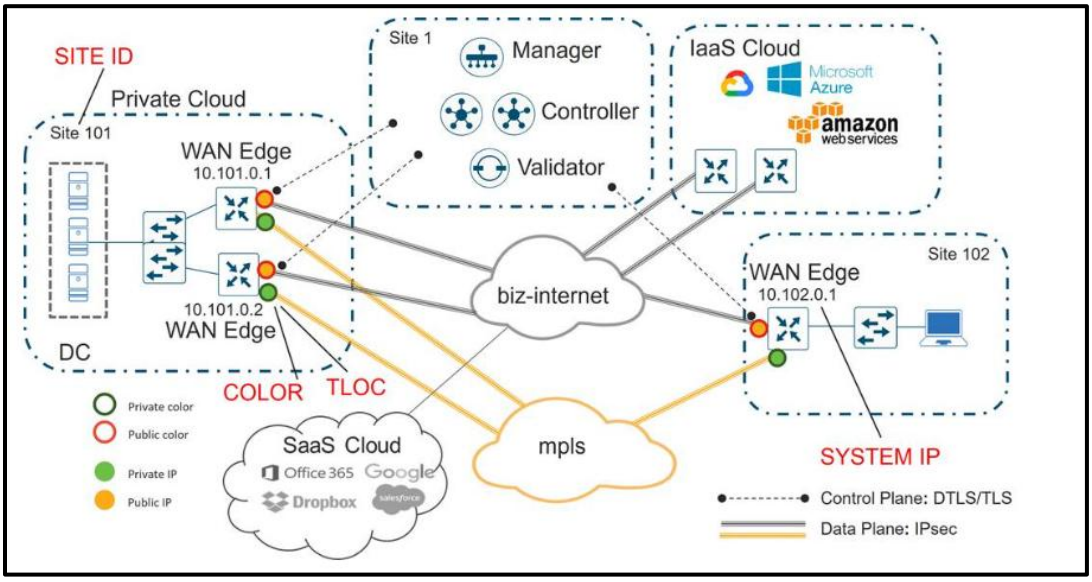
Controlador SD-WAN. Este componente basado en software y es responsable del plano de control centralizado de la red SD-WAN. Mantiene una conexión segura con cada enrutador WAN Edge y distribuye rutas de políticas a través del protocolo de administración de superposición OMP el cual actual como un reflector de rutas. También organiza la conectividad segura del plano de datos entre los enrutadores WAN Edge al reflejar la información de claves criptográficas que se origina en lo enrutadores WAN Edge, lo que permite una arquitectura muy escalable y sin IKE (Cisco, 2024).

Validador SD-WAN. Este componente también es basado en software, realiza la autenticación inicial de los dispositivos WAN Edge y organiza la conectividad entre el controlador SD-WAN, el administrador y el borde WAN. También tiene un papel crucial a la hora de permitir la comunicación entre dispositivos que se encuentran detrás de un NAT.

Enrutador de borde WAN. Este dispositivo, disponible como dispositivo de hardware o enrutador basado en software, se ubica en un sitio físico o en la nube y brinda conectividad segura en el plano de datos entre los sitios a través de uno o más transportes WAN. Es responsable del reenvió de tráfico, la seguridad, el cifrado, la calidad del servicio QoS, los protocolos de enrutamiento como BGP y OSPF, entre otros (Cisco, 2024).

Figura 6

Ejemplo de Topología SD-WAN



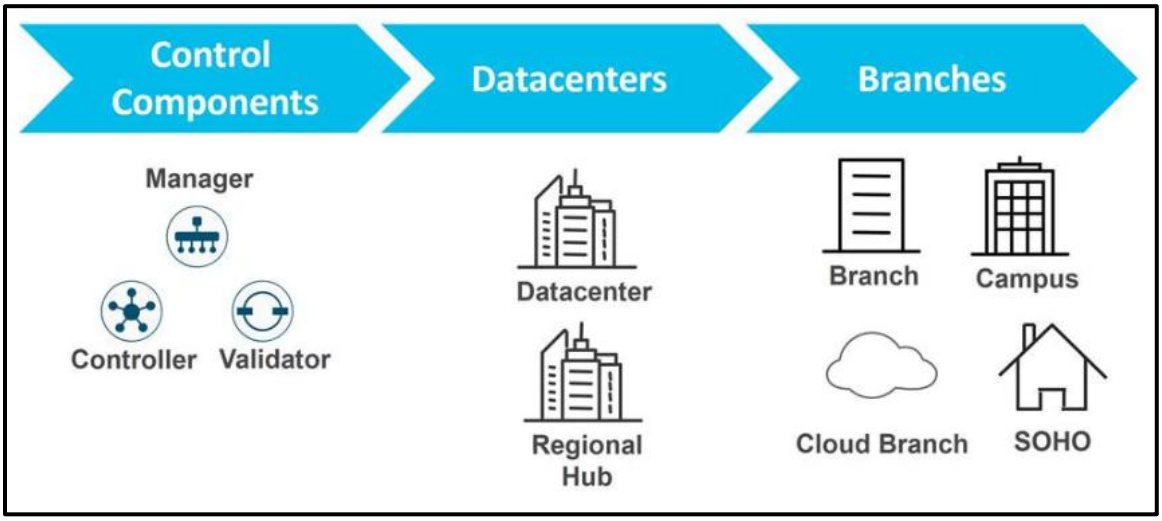
Nota. Tomado de Cisco (2024).

Métodos de Implementación de Cisco SD-WAN

En cualquier escenario de implementación de SD-WAN, primero se implementan y configuran los componentes de control, luego los sitios principales del centro de datos y por ultimo los sitios remotos. A medida que se implementa cada sitio, primero se establece el plano de control, seguido automáticamente por el plano de datos. Se recomienda que se utilicen sitios centrales para enrutar entre sitios SD-WAN y sitios que no son SD-WAN a medida que los sitios se migran a SD-WAN (Cisco, 2024).

Figura 7

Secuencia de Implementación de SD-WAN.



Nota. Tomado de Cisco (2024).

Los componentes o plano de control se pueden implementar de diferentes maneras:

En una nube alojada por el proveedor en este caso cisco: este es el modelo recomendado y los componentes de control de pueden implementar en la nube de AWS o AZURE. Hay zonas únicas o múltiples disponibles para la implementación. La mayoría de las organizaciones que deciden migrar a SD-WAN optan alojar los componentes de control en la nube de cisco debido a la facilidad de implementación y la flexibilidad en la escalabilidad. Cisco se encarga de aprovisionar los componentes de control con certificados y cumplir con los requisitos de escalabilidad y redundancia. Para este caso Cisco es el responsable de las copias de seguridad y la recuperación ante desastres. El cliente final tiene acceso al SD-WAN Manager para crear plantillas de configuración y políticas de control y datos para sus dispositivos (Cisco, 2024).

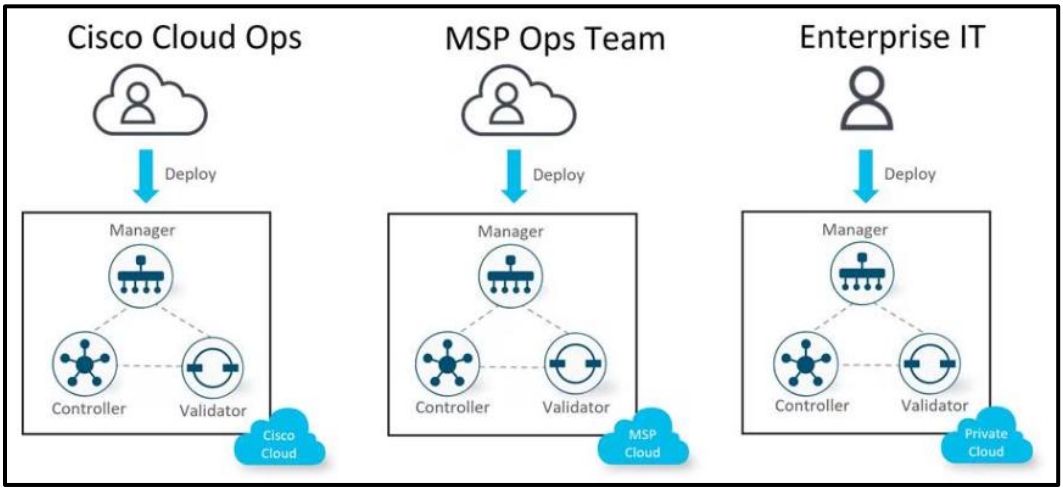
En una nube alojada por un proveedor de servicios administrados (MSP) o un socio: Puede estar alojada en una nube privada o en una nube pública e implementarse en AWS o

Azure. El MSP o socio suele ser responsable de aprovisionar los componentes de control y de las copias de seguridad y la recuperación ante desastres (Cisco, 2024).

Local en una nube privada o centro de datos propiedad de una organización: El cliente normalmente es responsable de aprovisionar los componentes de control y de las copias de seguridad y la recuperación ante desastres. Algunos clientes, como instituciones financieras o entidades gubernamentales, pueden optar por ejecutar implementaciones locales principalmente por razones de seguridad y cumplimiento.

Figura 8

Opciones de Implementación de Componentes de Control



Nota. Tomado de Cisco (2024).

Investigaciones o Antecedentes de Estudio

Diferentes estudios han explorado la integración de SDN con NGN para optimizar la gestión del tráfico y mejorar la eficiencia de la red. Según un estudio realizo por la escuela colombiana de ingeniería Julio Garavito, la implementación de SDN en entornos empresariales permite una administración centralizada que optimiza tanto el tráfico como la seguridad de la red, esto mejora la eficiencia general de toda la infraestructura (Garavito, 2022).

Un segundo estudio proveniente de la universidad politécnica de Cataluña enfatiza la necesidad de garantizar la calidad del serviccio QoS) a través de redes NGN hacia redes SDN, analizando estrategias como DiffServ y MPLS que, combinadas con SDN, pueden hacer la gestión adecuada del tráfico para aplicaciones críticas (Cataluña, 2021). Un proyecto en Perú analizó la introducción de SDN en una cadena de supermercados para garantizar una mejor gestión del tráfico y una menor intermitencia de comunicaciones internas y el resultado de toda esta investigación fue que el uso de SDN provoca una respuesta más ágil ante la variación de la alta demanda y una mejora considerable para el usuario final (Aplicadas, 2023).

En Venezuela, la universidad central plantea consideraciones de diseños para el despliegue SDN en campus empresariales, en el que se trata la importancia de hacer las planificaciones adecuadas para maximizar la interoperabilidad y la seguridad (Venezuela, 2022) por lo que esta investigación advierte que en un despliegue SDN se necesita analizar y aplicar políticas de segmentación de red y control de acceso a esta en algunos casos de vulnerabilidad.

Por último, un trabajo reciente realizado en la universidad politécnica de Cataluña presenta una aplicación sobre el tema basada en SDN llamada Pathfinder, que asegura la calidad de servicio adecuada en aplicaciones en tiempo real a través de la gestión dinámica del tráfico (Cataluña, Gestión y control de Calidad de Servicio de redes SDN en tiempo real, 2022) y demuestra incluso que esa flexibilidad de SDN puede mejorar la experiencia de los usuarios en aplicaciones sensibles al tiempo.

Transición de Redes Tradicionales Legacy a SDN y SDWAN

La transición de redes tradicionales (legacy) a tecnologías emergentes como SDN (Software Defined Networks) o SD-WAN (Software Defined Wide Area Networks) plantea un desafío para las organizaciones dado el sustrato muy distinto en el que se hallan ambas

arquitecturas. Mientras que las redes legacy se caracterizan por un control y datos acoplados dentro de dispositivos concretos, SDN o SD-WAN separan el plano de control del de datos, para que el control sea central, programable y flexible; el resto del trabajo propone soluciones (basadas en la investigación y en casos de éxito) para facilitar este horizonte de transición.

Implementación escalonada y modular. Una forma adecuada de hacer compatibles tecnologías emergentes con las tecnologías legacy es hacer uso de la implementación escalonada, que consiste en:

Identificar áreas críticas. determinar qué segmentos de la red tendrán mejor retorno de la adopción de SD/SD-WAN, tales como sedes o centros de datos.

Implementar en módulos. utilizar SD-WAN en sedes y oficinas regionales, manteniendo como vías de respaldo las conexiones MPLS legacy.

Casos de éxito relacionados

Grupo Éxito en Colombia. SD-WAN fue implementado en centros de distribución, manteniendo conexiones MPLS en otras localidades para asegurar que las operaciones no se vean afectadas; Cisco Systems (2023).

Interoperabilidad por Medio de Protocolos Estándar

La interoperabilidad entre tecnologías es determinante para evitar problemas operativos. Protocolos estándar que se pueden usar son los siguientes:

BGP y OSPF. Para garantizar la interoperación entre los segmentos de red legacy y los de sdN.

OpenFlow. Asegura la interoperabilidad de dispositivos legacy con controladores sdN para conseguir una visión homogénea y unitaria para la gestión de las redes.

Casos de éxito. BBVA Colombia. Usó la adopción de políticas centralizadas, cuyos estándares se basan el uso de políticas abiertas, que gestionaba tanto enlaces MPLS como conexiones SD-WAN, asegurando el rendimiento de la red (Cisco Systems, 2023).

Virtualización de Funciones de Red (NFV)

La virtualización de funciones de red (NFV) permite reducir la dependencia de hardware legacy, habilitando la migración a soluciones más flexibles. Con NFV:

Se abstraen funciones como cortafuegos y balanceadores de carga, moviéndolas a entornos virtuales.

Se reduce la necesidad de nuevos dispositivos físicos, disminuyendo costos de transición.

Casos de Éxito Relacionados

Vodafone Colombia. Aprovechó NFV para consolidar funciones de red en entornos virtualizados mientras implementaba Cisco SD-WAN, reduciendo costos operativos en un 40% (TNG, 2023).

Capacitación y Gestión del Cambio

La formación del personal es crítica para una transición exitosa:

Capacitación continua en SDN y SD-WAN. Los equipos de TI deben estar familiarizados con nuevas herramientas, como Cisco Vmanage y OpenFlow.

Gestión del cambio. Involucrar a todos los niveles de la organización para asegurar una adopción fluida. Proveedores de servicio y soluciones de TI como Axity que Ofreció programas de capacitación para los equipos técnicos de sus clientes, lo que facilitó la adopción de SD-WAN en empresas de telecomunicaciones y manufactura (Axity, 2023).

Híbrido Legacy-SD-WAN. Las soluciones híbridas hacen posible la transición por etapas en el tráfico de una red sin una interrupción del servicio: es posible usar el MPLS y el SD-WAN

de manera simultánea (usando SD-WAN para el tráfico de las aplicaciones críticas como el VoIP y MPLS para el tráfico de otro tipo como el de los proveedores de servicios públicos).

Beneficios:

Garantiza la resiliencia de la red.

Minimiza riesgos asociados a fallos en la implementación inicial.

Casos de éxito relacionados:

Cadena de supermercados en Perú: Utilizó un modelo híbrido durante la implementación de Cisco SD-WAN, manteniendo MPLS para ubicaciones críticas mientras migraba gradualmente otras oficinas (Cladirect, 2023).

Monitoreo y Evaluación Constante

El monitoreo y la evaluación continua del rendimiento de ambas tecnologías (MPLS y SD-WAN) es fundamental para saber si se es compatible con las aplicaciones críticas de negocio y ajustarlas.

Herramientas de análisis de tráfico: como el Cisco vAnalytics, que permite ver en tiempo real cómo se comportan tanto el MPLS como el SD-WAN; comportamiento de las políticas de red: en función de los datos obtenidos de la evaluación continua de ciertas métricas, como el de latencia o el de pérdida de paquetes.

Ejemplo de casos de éxito relacionados:

ITNG en un caso de éxito en Colombia: por ejemplo, implementó el Cisco vAnalytics para el monitoreo y la evaluación de las mejoras en la continuidad de servicio en caso de que los clientes tengan que migrar a SD-WAN (Fortinet, 2023).

Impacto Social y Ambiental de SDN y SD-WAN

Impacto social de SDN y SDWAN. Inclusión Digital y acceso a la información: La aplicación de SD-WAN mejora las capacidades de comunicación y conectividad en las áreas rurales y remotas donde generalmente las infraestructuras de las redes son escasas o inexistentes. Al soportar conexiones de menos coste (por ejemplo, banda ancha y LTE), se eliminan muchas de las dificultades económicas para el establecimiento de redes en estas áreas, se favorece la inclusión digital y se prestan servicios online de educación, salud y administración pública (Fortinet, 2023). Al respecto, Cisco Systems informa que la flexibilidad de SD-WAN permite a las organizaciones responder a las peticiones cambiantes del tráfico, lo que es clave para proveer servicios en áreas con una infraestructura muy limitada (Cisco Systems, 2023).

Mejora la calidad de los servicios públicos: Desde la llegada de las tecnologías de SDN y SD-WAN a las administraciones y entidades públicas, la eficiencia y la calidad de los servicios que se prestan para la ciudadanía mejora. Por ejemplo, en el sector sanitario, estas tecnologías permiten la gestión de la información de los pacientes o la comunicación entre centros médicos, lo que se traduce en una atención más oportuna y de mejor calidad (Technoymás, 2023). Un estudio hecho por la universidad Politécnica de Cataluña concluye que la integración de SDN junto con QoS mediante DiffServ y MPLS mejora la gestión del tráfico de aplicaciones críticas y es aplicable en entornos de entidades y administraciones y servicios públicos (Cataluña, Calidad de Servicio en Redes NGN, 2021).

Fomento del Teletrabajo y Educación a Distancia: La pandemia de la COVID-19 aceleró la implementación del teletrabajo y de la educación a distancia. SD-WAN ha sido clave en asegurar que existan conexiones de alta calidad y seguras para los trabajadores y estudiantes en un entorno en casa, permitiendo que se mantengan las actividades laborales y educativas

(Fortinet, 2023); la flexibilidad y la escalabilidad de SD-WAN dan a las organizaciones la capacidad de adaptarse con rapidez a cualquier cambio en la demanda de tráfico, lo que resulta fundamental si hay que soportar el crecimiento del teletrabajo y de la educación en línea (Cisco Systems, 2023).

Impacto Ambiental de SDN y SD-WAN. Reducción del Consumo Energético: La gestión de tráfico con que las redes SDN y SD-WAN ofrecen contribuye a una utilización más óptima de los recursos de red, lo que significa una menor necesidad de consumo energético. Al optimizarlas rutas de los datos y reducir la necesidad del hardware adicional, estas tecnologías contribuyen a reducir la huella de carbono de las infraestructuras de telecomunicaciones (Geographic, 2019).

Disminución de Residuos Electrónicos: con la virtualización y centralización de funciones de red mediante SDN reducen la dependencia de hardware físico, esto disminuye la generación de residuos electrónicos. Al prolongar la vida útil de los dispositivos existentes y minimizar la necesidad de nuevos equipos, se contribuye a una gestión más sostenible de los recursos tecnológicos (BNzero, 2023).

Optimización del Uso de Recursos Naturales: la implementación de SDN y SD-WAN permite una gestión mas eficiente del trafico de los recursos de red, lo que trae un uso mas racional de recursos naturales como la energía y el agua. Al reducir la necesidad de infraestructuras físicas extensivas y optimizar el uso de las existentes, estas tecnologías contribuyen a la sostenibilidad ambiental (Greentech, 2023).

Casos de Éxito de Implementaciones de Cisco SD-WAN

Casos de Éxito Globales de Implementaciones de Cisco SD-WAN. National Instruments: es una empresa líder en soluciones de prueba y medición, enfrentaba desafíos

debido al creciente consumo de ancho de banda que impactaba su presupuesto tecnológico. Al implementar Cisco SD-WAN, la compañía logro ofrecer a sus usuarios un ancho de banda 30 veces mayor por un tercio del costo anterior. Esta solución permitió a National Instruments satisfacer la creciente demanda de sus servicios sin comprometer la calidad ni incurrir en gastos excesivos (Red, 2023).

Universidad de Wollongong: Mejora en la Experiencia del Usuario: la universidad de Wollongong situada en Australia buscaba habilidad la calidad de conexión, para sus estudiantes, profesores e investigadores. Al aplicar Cisco SD-WAN la universidad logró una red más eficiente, descargas de datos más veloces, una resolución más rápida de incidentes y las aplicaciones online utilizadas por la comunidad universitaria proporcionaron una experiencia de usuario gratificante (Red, 2023).

Café Rio: Optimización de la Experiencia del Cliente: Café Rio, una conocida cadena de restaurantes, se encontraba enfrentando una situación problemática a la hora de garantizar la vinculación de su página web con la gestión de los pedidos en línea; pues bien, la aplicación de Cisco SD-WAN fue capaz de mejorar tanto la velocidad de la vinculación con el comportamiento de la red, garantizando así una experiencia de usuario más que satisfactoria tanto en la página web de la cadena de cafeterías como en su aplicación para móviles, y con ello, lograr que Café Rio mejorara la eficiencia operativa y la satisfacción del cliente con respecto a anterioridad (Red, 2023).

Riedel Networks: Innovación en Comunicaciones Automotrices: La empresa Riedel Networks, en asociación con Cisco, desarrolló una arquitectura de comunicaciones que proporciona control de automóviles de carreras utilizando Cisco SD-WAN después de que la arquitectura de Cisco Catalyst 8300 Edge. Esta solución generó una conexión de conmutación

por etiquetas (MPLS) directa sobre enlace por fibra, desafiando el estatus que de la industria automotriz y engageó la flexibilidad de Cisco SD-WAN en entornos altamente exigentes (Cisco Systems, 2023).

Casos de Éxito de Cisco SD-WAN en América Latina. Banco Pichincha: Transformación Digital en Ecuador: Banco Pichincha, uno de los bancos más grandes de Ecuador, iniciaron su proceso de transformación digital con el propósito de enriquecer la experiencia de los servicios ofrecidos a sus clientes. Con ello, comenzaron a implementar la solución Cisco SD-WAN que optimizaría su infraestructura de red y que les permitiría mejorar la eficiencia de sus operaciones y la experiencia del cliente. Dicha solución les permitiría una gestión centralizada de su red y mayor flexibilidad en su red (Cisco Systems, 2023).

Operador de Telecomunicaciones en Brasil: Solución SD-WAN para Clientes Corporativos: Un operador de telecomunicaciones, en Brasil, en asociación con Logicalis, hizo uso de una solución Cisco SD-WAN para sus clientes corporativos, lo que permitió que las empresas lograran una comunicación entre las oficinas y los centros de datos inteligente por medio de la diversidad del transporte, lo que propició más flexibilidad, redondeo de los costos, visibilidad del tráfico e incremento de la seguridad en las oficinas remotas (Logicalis, 2023).

Cadena de Supermercados en Perú: Gestión Eficiente del Tráfico: Una cadena de supermercados en Perú implementó Cisco SD-WAN para mejorar la gestión del tráfico y reducir la intermitencia en la comunicación interna. Esta solución permitió una respuesta más ágil ante fluctuaciones en la demanda, mejorando la experiencia del usuario y optimizando las operaciones diarias de la cadena (Cladirect, 2023).

Banco en Latinoamérica: Unificación y Control Remoto de Sedes: Un banco destacado de Latinoamérica estaba buscando unificar y controlar de manera remota tres tipologías de

oficinas y sedes, situadas en un país, que al mismo tiempo querían soltar el tráfico de los datos para que no se interrumpiera el flujo del servicio. Con la implementación de Cisco SD-WAN, se lograba obtener mayor conectividad y asegurar la continuidad del servicio a partir de las oficinas, con la buena experiencia del cliente (Bismark, 2023).

Casos de Éxito de Cisco SD-WAN en Colombia. Vodafone: Mejora de Servicios en Colombia: Vodafone, aliándose estratégicamente con Cisco, lanzó una solución SD-WAN que facilitó la eliminación de cuellos de botella en aplicaciones de red y, además de eso, redujo el tiempo de este tipo de implementaciones de infraestructura junto con los clientes en Colombia. Esto fue posible gracias a que la solución ofrecía una configuración de red automatizada y simplificada, gestionada de manera centralizada, lo que permitía que los clientes desplegaran servicios de manera más rápida y también respondieran a las solicitudes comerciales con mayor rapidez (TNG, 2023).

Grupo Éxito: Grupo Éxito, una de las cadenas mayoristas de más envergadura que opera en Colombia, consideró valioso implementar Cisco SD-WAN para transformar su estructura tecnológica. Antes de la implementación, su infraestructura tecnológica le generaba dificultades de conectividad, así como inconvenientes operativos que ponían en peligro la experiencia de su cliente. Cisco SD-WAN permitió optimizar la resiliencia de su red, mejorar el rendimiento de aplicaciones críticas y gestionar la TI de forma simplificada. Esta tecnología contribuyó a reducir las interrupciones del servicio y a soportar un entorno de alta demanda, como en el caso del Black Friday (Cisco Systems, 2023).

BBVA Colombia: La entidad bancaria BBVA seleccionó para su estrategia de modernización tecnológica a Cisco SD-WAN, lo que le permitió al banco consolidar su infraestructura de red con el objetivo de reducir costes y mejorar el rendimiento de las

aplicaciones bancarias de primera línea. La implementación de SD-WAN garantizó una mayor experiencia de usuario en las sucursales por medio de una conectividad fiable para operaciones como transacciones, atención al cliente y soporte remoto. Los efectos de implementar SD-WAN fueron la centralización de la administración de las políticas de red y la posibilidad de escalar con agilidad ante nuevas demandas tecnológicas (Cisco Systems, 2023).

Axity Colombia: Axity, un socio estratégico de Cisco en el país cafetero ha sido pionero en la introducción de Cisco SD-WAN en empresas de múltiples sectores desde manufactura hasta telecomunicaciones. La empresa ha puesto en el centro de la propuesta de valor el diseño de soluciones integrales, es decir, la combinación de las partes que conforman las redes inalámbricas, la conectividad y la SD-WAN, maximizando los tiempos de operación y generando una mayor resiliencia de la red en los clientes. Entre los beneficios que esta empresa ha reportado a sus clientes se encuentran: disminución de interrupciones en los servicios, visibilidad del tráfico y optimización de costos operativos (Axity, 2023).

ITNG: ITNG se ha unido a Cisco para brindar soluciones de SD-WAN a empresas instaladas en Colombia con el propósito de optimizar el desempeño de sus aplicaciones y la disponibilidad de la red. La empresa ha desplegado esta tecnología en empresas que deseen mejorar sus operaciones y garantizar el negocio en todo momento, aun en condiciones de alta actividad. El SD-WAN ha permitido a ITNG ayudar a empresas a desplegar aplicaciones que son criticas a sus operaciones, mejorar la experiencia de los clientes y garantizar conectividad en todo Colombia (Cisco Systems, 2023).

Capacitaciones Personal Técnico que Administra la Solución

La formación del personal técnico es un elemento fundamental para asegurar que la migración hacia SD-WAN tenga éxito. En este sentido, a continuación, se presenta un plan de

formación global, dirigido específicamente a todos aquéllos administradores de red que estarán encargados de gestionar la solución SD-WAN y que de este modo se asegura que se produzca una migración sin cortes.

Objetivos del plan

Proporcionar a los administradores de red conocimientos solidos sobre SD-WAN y sus componentes.

Desarrollar habilidades prácticas en la configuración, monitoreo y optimización de Cisco SD-WAN.

Garantizar la capacidad para gestionar la coexistencia de redes legacy y SD-WAN durante el periodo de transición.

Asegurar la adopción de mejores prácticas de seguridad y rendimiento de la red.

Tabla 3

Estructura del Plan de Formación

Módulo	Contenido	Duración	Costo Estimado (COP)
1. Introducción a SD-WAN	- Principios básicos de SD-WAN - Diferencias entre SDN y SD-WAN - Beneficios y casos de uso	1 semana	$1,000,000
2. Componentes de Cisco SD-WAN	- Arquitectura de Cisco SD-WAN - Planos de gestión, control, datos y orquestación - Herramientas como Cisco vManage	1 semana	$1,500,000
3. Configuración y Operación	- Configuración inicial de dispositivos Edge - Políticas de control	2 semanas	$2,000,000

	y rutas - Gestión del tráfico		
4. Integración con Redes Legacy	- Interoperabilidad con enlaces MPLS - Migración gradual hacia SD-WAN - Protocolos de integración (BGP, OSPF)	1 semana	$1,500,000
5. Monitoreo y Solución de Problemas	- Uso de Cisco vAnalytics - Identificación de fallos y resolución - Métricas clave de rendimiento	1 semana	$1,500,000
6. Seguridad en SD-WAN	- Configuración de políticas de seguridad - Cifrado de datos y segmentación de red - Mitigación de vulnerabilidades	1 semana	$1,500,000
7. Optimización de Redes y QoS	- Ajustes para aplicaciones críticas - Gestión dinámica del ancho de banda - Priorización de tráfico	1 semana	$1,000,000

Nota. La tabla presenta la estructura del plan de formación propuesto para la capacitación en tecnologías SD-WAN, incluyendo módulos temáticos, duración estimada y costos aproximados asociados a cada componente formativo.

Tabla 4

Calendario del Plan de Formación

Fase	Fechas	Duración Total	Actividades Clave
Fase 1: Preparación	15/01/2025 - 22/01/2025	1 semana	Selección del personal, coordinación con el proveedor de formación, y

			preparación de material didáctico.
Fase 2: Formación	23/01/2025 - 08/03/2025	7 semanas	Ejecución de los módulos del plan de formación.
Fase 3: Evaluación	09/03/2025 - 16/03/2025	1 semana	Evaluación de habilidades adquiridas mediante ejercicios prácticos y exámenes.
Fase 4: Seguimiento	17/03/2025 - 31/03/2025	2 semanas	Supervisión de las primeras operaciones realizadas por los administradores capacitados.

Nota. Esta tabla describe el cronograma propuesto para el desarrollo del plan de formación en SD-WAN, incluyendo las fases de preparación, formación, evaluación y seguimiento.

Tabla 5

Costo Total Aproximado del Plan de Formación.

Categoría	Detalle	Costo Estimado (COP)
Capacitación Formal	Contratación de formadores certificados	$8,000,000
Material de Capacitación	Manuales, software de simulación, y guías	$2,000,000
Licencias Temporales	Acceso temporal a Cisco SD-WAN para pruebas	$5,000,000
Horas personal	Tiempo de dedicación del personal	$5,000,000
Total		$20,000,000

Nota. La tabla muestra el costo estimado del plan de formación requerido para capacitar al personal en la implementación y gestión de redes SD-WAN.

Beneficios de Implementar un Plan de Formación

Un plan de formación bien orientado tanto para las organizaciones como para los proveedores trae consigo una serie de beneficios, a continuación, se detallan algunos:

Reducción de errores: La capacitación minimiza fallos operativos y acelera la resolución de problemas.

Transición sin interrupciones: Los administradores capacitados pueden gestionar redes legacy y SD-WAN simultáneamente.

Optimización del rendimiento: Habilidades en monitoreo y ajustes permiten maximizar el uso de la red y priorizar aplicaciones críticas.

Seguridad mejorada Los conocimientos de políticas de seguridad disminuyen las probabilidades de sufrir un ciberataque.

Este plan de formación se asegura que los administradores de red sean capaces de gestionar de forma óptima la infraestructura SD-WAN, asegurando el éxito de la migración y, por tanto, el retorno de la inversión en tecnología.

Análisis Financiero de la Implementación de SDN y SD-WAN

La implementación de SDN (Software-Defined Networking) y SD-WAN (Software-Defined Wide Area Networking) no son más que una inversión estratégica por parte de las empresas con especial consideración en un entorno tan competitivo como puede ser el colombiano. Este tipo de soluciones permiten optimizar la infraestructura de red, optimizar costes y maximizar el rendimiento. Por último, a continuación, se presenta un análisis financiero

aproximado en el que se detallan costes y beneficios en el caso de empresas en las que, de igual modo, hay ejemplos reales de la misma en el caso concreto de Colombia.

Costos de implementación de SDN y SD-WAN. Los costos iniciales varían según la magnitud de la red y las necesidades específicas de cada empresa. En general, estos costos incluyen:

Tabla 6

Costos Aproximados de Implementación de SDN y SD-WAN.

Categoría	Detalle	Costo Aproximado (COP)
Equipos de Red	- Routers Edge (e.g., Cisco Catalyst 8000) - Dispositivos secundarios	$20,000,000/unidad
Licencias	- Licencias Cisco SD-WAN anuales por dispositivo	$5,000,000/dispositivo
Infraestructura en la nube	- Servicios en AWS/Azure para el plano de control	$3,000,000/mes
Capacitación	- Capacitación para administradores de red	$8,000,000
Servicios de Consultoría	- Diseño e implementación inicial	$10,000,000
Mantenimiento	- Contrato anual de soporte técnico	$8,000,000

Nota. Los costos presentados son valores aproximados basados en estimaciones del mercado para la implementación de soluciones SDN y SD-WAN en entornos empresariales, y pueden variar según el proveedor, la escala de la infraestructura y los requerimientos técnicos de la organización.

Ejemplo: Grupo Éxito

El Grupo Éxito implementó Cisco SD-WAN en más de 200 sucursales en Colombia. Los costos iniciales de la infraestructura incluyeron equipos y licencias, con un gasto estimado de $4,500 millones COP, incluyendo la configuración y capacitación del personal

Beneficios Financieros de Implementar SDN y SD-WAN

Reducción de Costos Operativos

Ahorro en enlaces MPLS: SD-WAN permite sustituir enlaces MPLS costosos por conexiones de Internet de banda ancha y LTE, reduciendo costos en un 50%-70% (Cisco Systems, 2023).

Ejemplo: BBVA Colombia: El banco reportó ahorros de aproximadamente $1,200 millones COP anuales al optimizar su red con Cisco SD-WAN.

Optimización de Recursos

Aprovechamiento del ancho de banda: SD-WAN mejora la utilización del ancho de banda mediante la selección automática de rutas.

Ejemplo: Vodafone en Colombia: La implementación permitió un incremento del 60% en la eficiencia del uso del ancho de banda, reduciendo la congestión en redes corporativas (TNG, 2023).

Reducción del Tiempo de Implementación

Automatización y gestión centralizada: Permite una configuración más rápida y reduce el tiempo de puesta en marcha en un 40%-50%.

Ejemplo: Axity Colombia: Implementó SD-WAN en empresas de telecomunicaciones, logrando reducir el tiempo de implementación de nuevas sedes de 3 semanas a 1 semana (Axity, 2023).

Mejora en la Calidad del Servicio (QoS) Prioridad para aplicaciones críticas: SD-WAN garantiza que las aplicaciones críticas tengan un rendimiento óptimo.

Ejemplo: BBVA Colombia: Mejoró sus niveles de QoS en sucursales, logrando un cumplimiento del 95% en sus indicadores de calidad (Cisco Systems, 2023).

Mayor Escalabilidad Fácil expansión: SDN y SD-WAN permiten añadir nuevos dispositivos y oficinas sin necesidad de grandes cambios en la infraestructura.

Ejemplo: Grupo Éxito: La solución permitió integrar nuevas tiendas en menos de una semana, reduciendo costos asociados a la expansión (Cisco Systems, 2023).

Tabla 7

Comparación Financiera: Redes Legacy vs SD-WAN.

Aspecto	Redes Legacy	Cisco SD-WAN
Costo de conectividad	Alto (dependencia de enlaces MPLS)	Bajo (uso de Internet y LTE)
Tiempo de configuración	Prolongado (configuración manual)	Rápido (gestión centralizada desde Cisco vManage)
Escalabilidad	Limitada (costosa y lenta)	Alta (rápida y flexible)
Costo total por sucursal	$10,000,000 - $15,000,000 COP/sucursal	$5,000,000 - $8,000,000 COP/sucursal

Nota. Los costos presentados corresponden a estimaciones aproximadas basadas en implementaciones empresariales de redes tradicionales y soluciones SD-WAN.

Tabla 8

Análisis Escenarios Financieros.

Escenario	Costos de Implementación (COP)	Ahorros en Conectividad Anuales (COP)	Mejora en Productividad Anual (COP)	Beneficios Anuales Totales (COP)	ROI (%)	Payback (Años)
Empresa Mediana con 10 Sucursales	145,000,000	45,000,000	20,000,000	65,000,000	44.8	2.2
Gran Empresa	710,000,000	200,000,000	100,000,000	300,000,000	42.3	2.4

con 50 Sucursales

Nota. El análisis presenta escenarios financieros estimados para la implementación de soluciones SD-WAN en empresas con diferentes escalas operativas, considerando costos iniciales, ahorros anuales y retorno de inversión (ROI).

Resultados

Impacto de SDN en la Latencia y Calidad de Servicio (QoS)

Para cumplir con el objetivo de analizar el impacto de la adopción de tecnologías SDN en la reducción de la latencia y la mejora de la calidad del servicio (QoS) en redes NGN, se revisaron y analizaron estudios académicos que documentan casos reales y simulados en distintos entornos de telecomunicaciones. Estos trabajos abarcan desde la optimización de plataformas multimedia y aplicaciones de tele diagnóstico, hasta la gestión del tráfico WAN, el análisis comparativo de protocolos, la aplicación de políticas de QoS en entornos SDN y la evaluación de estándares inalámbricos avanzados.

A través de la síntesis de resultados cuantitativos como la reducción porcentual de la latencia, disminución del jitter, incremento del ancho de banda y disminución de la pérdida de paquetes, así como de conclusiones cualitativas sobre estrategias y configuraciones de red, se identifica cómo las soluciones basadas en SDN y la gestión avanzada de QoS contribuyen a optimizar el rendimiento y la eficiencia operativa en redes de próxima generación.

El trabajo de González Pino (2022) explora diversas estrategias para optimizar la QoS en plataformas multimedia, evaluando si acercar el contenido a los usuarios reduce la latencia y descongestiona la red. Entre las pruebas realizadas se incluyeron comparaciones de requisitos técnicos en distintas plataformas, análisis de la percepción de los usuarios, trazado de rutas hacia servidores y simulaciones de topologías de red con protocolos de encaminamiento diversos. Los resultados evidenciaron que la proximidad del contenido mejora la velocidad de acceso y disminuye la saturación de los servidores centrales, lo que impacta positivamente en la experiencia del usuario.

El este estudio también permite alcanzar el objetivo porque demuestra que, sin cambiar el hardware de red, se puede optimizar la latencia y la QoS a través de técnicas de distribución inteligente del contenido y la selección apropiada de los protocolos de encaminamiento. Esto puede ser trasladado a los entornos NGN, donde se puede implantar políticas de routing dinámico sobre las arquitecturas SDN permitiendo que el controlador, en base a la información obtenida de la red, decida de forma dinámica e instantánea la localización lógica de los recursos para mejorar la experiencia

Además, la propia metodología permitida en el estudio da lugar a un modelo replicable para hacer pruebas de distintas configuraciones y de distintas topologías antes de la verdadera implantación de estas. La esencia de las redes definidas por software favorece la simulación de escenarios y la aplicación de cambios sin causar una interrupción del servicio. Por tanto, el caso de estudio demuestra que la combinación de simulaciones previas a la implantación del mismo y cambios controlados de un entorno de red pueden optimizar la gestión del tráfico y disminuir la latencia de la misma.

Finalmente, el estudio ejecutado por las universidades y la inclusión de las métricas técnicas y métricas perceptuales permiten mostrar una visión completa de cómo la gestión del contenido y la topología de red puede ser un catalizador de la QoS que puede ayudar a la toma de decisiones para mejorar el rendimiento de las redes de próxima generación.

El trabajo de Guerrero Loaiza (2021) se centra en redes de sensores multimedia inalámbricos (WMSN), donde la QoS es crítica por el tipo de datos que se transporta —video, audio e imágenes—. La investigación compara distintos protocolos de enrutamiento evaluando métricas como ancho de banda, retardo extremo a extremo, pérdida de paquetes y jitter. Los resultados mostraron que algunos protocolos, como OLSR optimizado, ofrecen un desempeño

sustancialmente mejor en términos de latencia y estabilidad de transmisión frente a otros enfoques.

En relación con el objetivo planteado, este estudio evidencia cómo la selección del protocolo adecuado y su optimización pueden influir directamente en la latencia y la QoS en entornos NGN controlados por SDN. Un controlador SDN, al tener conocimiento global de la red, podría aplicar dinámicamente el protocolo más eficiente para cada tipo de tráfico, replicando los resultados positivos observados en el estudio.

El enfoque experimental utilizado, que incluye simulaciones y análisis comparativo bajo métricas estandarizadas, ofrece un marco metodológico útil para pruebas en redes NGN. Esto es especialmente relevante en entornos SDN, donde la capacidad de cambiar protocolos y rutas de manera centralizada es una de sus principales ventajas.

En síntesis, este trabajo refuerza la idea de que las mejoras en QoS no solo dependen de la capacidad física de la red, sino de la gestión inteligente del enrutamiento, un aspecto en el que SDN tiene un papel fundamental.

La investigación de Vicente Ramos y colaboradores (2022) implementa un modelo de gestión de tráfico en una red WAN corporativa, evaluando métricas de throughput, latencia, jitter y pérdida de paquetes. Los resultados son contundentes: el throughput aumentó más de un 600 %, la latencia se redujo en un 93,77 %, el jitter disminuyó en un 99,12 % y la pérdida de paquetes bajó en un 84,82 %.

Estos datos constituyen evidencia empírica del impacto que un modelo de gestión eficiente puede tener sobre la QoS, y son extrapolables a entornos SDN, donde estas políticas pueden aplicarse de forma centralizada y adaptativa. En redes NGN, la combinación de

monitoreo en tiempo real y reconfiguración dinámica que permite SDN es ideal para replicar este tipo de mejoras.

El estudio también destaca la importancia de usar métricas objetivas y pruebas estadísticas para validar los resultados, algo que se integra perfectamente en la filosofía de las redes definidas por software, que permiten una trazabilidad completa de los cambios aplicados.

En suma, este caso demuestra que la aplicación de modelos de gestión del tráfico bien diseñados puede lograr reducciones drásticas en la latencia y mejoras sustanciales en la QoS, reforzando el papel de SDN como plataforma para la optimización continua.

La investigación de Barba Vera (2025) aborda un problema relevante en las redes académicas: las amenazas internas (insider threats) que concurren a la vez la seguridad y la QoS. La investigación establece una metodología de cuatro etapas —diagnóstico, detección en tiempo real, selección de amenaza a controlar y aplicación de políticas de QoS— implementada sobre una arquitectura SDN, en este caso FloodLight. Los resultados muestran mejoras en distintas métricas de rendimiento, mejora del rendimiento en términos de delay, jitter o pérdida de paquetes y mejor aprovechamiento del ancho de

De acuerdo con el objetivo que se persigue, este trabajo muestra que la SDN no solo es capaz de optimizar la QoS ajustando la topología o los protocolos de red, sino que también puede incorporar mecanismos de seguridad que actúan directamente sobre el rendimiento. El control centralizado de la SDN permite aplicar políticas de QoS de forma selectiva, protegiendo la red contra comportamientos anómalos sin comprometer el rendimiento.

Metodológicamente, la investigación es notable por incorporar en un mismo marco de investigación el análisis de la seguridad y el análisis del rendimiento, siendo poco común entre las investigaciones que se centran exclusivamente en la QoS. Esta dualidad es especialmente

pertinente en NGN pues la convergencia de servicios críticos y datos de usuario requieren una conciliación entre rendimiento y protección.

Por último, este caso aporta al objetivo demostrando que la reducción de latencia y mejora de QoS en entornos SDN no tiene que estar aislada de otras funciones de red. La implementación de políticas de QoS como respuesta a incidentes de seguridad abre una línea de investigación y desarrollo que combina resiliencia, eficiencia y adaptabilidad.

Cevallos Troya y Parra Balza (2022) verifican cómo el estándar IEEE 802.11ax (WiFi 6) puede influir en la latencia, velocidad de conexión, capacidad y seguridad de redes inalámbricas corporativas. De su trabajo obtengo como resultado los siguientes aspectos: la disminución de tiempos de latencia, la velocidad de conexión de 2402 Mbps, la estabilidad de enlace y la cobertura que se logra con la transmisión de forma simultánea con las bandas de 2,4 GHz y 5 GHz. Asimismo, consideran que el uso de cifrado WPA3 compatible no tiene un efecto negativo en la QoS.

Este trabajo contribuye a los objetivos por demostrar que la adopción de estándares avanzados en entornos NGN puede coexistir con el uso de SDN para conseguir un plus. En un escenario SDN, la orquestación inteligente de recursos inalámbricos puede propiciar la asignación de canales y la priorización del tráfico de forma dinámica y continuar con los aspectos positivos de la aplicación del estándar 802.11ax.

En cuanto a la metodología, está compuesta por simulaciones de migración de infraestructuras y por pruebas de rendimiento, generando un plan que muestra la forma de evaluar mejoras de QoS previa a la implementación real de los resultados descritos. Esta estrategia es coherente con el enfoque experimental de las redes definidas por software, que exigirán pruebas previas para restar potenciales riesgos de degradación de la calidad del servicio.

En conclusión, este caso confirma que la latencia y la QoS pueden optimizarse no solo mediante cambios en la lógica de red, sino también mediante la adopción de nuevas tecnologías físicas y estándares, cuya integración con SDN permitiría un control aún más granular del rendimiento en redes NGN.

El proyecto de Cocha Muquinche (2025) aplica técnicas de QoS en una red LAN en una institución militar para mejorar el aprovechamiento del ancho de banda y priorizar aplicaciones consideradas como críticas. La metodología PPDIOO de Cisco ha orientado el análisis, diseño y la simulación de una red segmentada implementando VLAN, tráfico modelado, marcado DSCP y colas de priorización configuradas en un dispositivo FortiGate. Los resultados denotan incrementos en lo que respecta a la estabilidad, a la escalabilidad y a la capacidad de dar soporte a las aplicaciones clave, y, a su vez, reducciones de latencia y de jitter apreciables.

Este caso es de gran importancia para el objetivo por el hecho de que muestra cómo las políticas de QoS, aplicadas de un modo estructurado, pueden optimizar el tráfico de forma efectiva en entornos benefactores de alta demanda y que presentan un rendimiento en materia de seguridad estricta. En un entorno SDN, las políticas de esta forma pueden ser aplicadas y adaptadas de un modo automático y centralizable mejorando la adaptabilidad.

La combinación segmentación mediante VLAN y priorización basada en DSCP es totalmente complementaria con el discurso SDN, donde el controlador puede realzar en tiempo real las prioridades y las rutas con motivo del estado de la red, permitiendo, de esta forma, como mínimo, no sólo mantener la QoS, sino también reaccionar ante picos de tráfico.

Tabla 9

Comparación

Estudio	Tecnología / Enfoque	Resultados Clave
González Pino (2022)	Optimización QoS en plataformas multimedia; acercamiento de contenido y simulación de topologías	Reducción de latencia y congestión; múltiples alternativas para mejorar QoS
Guerrero Loaiza (2021)	Comparación de protocolos WMSN y propuesta de mejora	Protocolos optimizados reducen retardo y mejoran QoS en entornos multimedia
Ormachea Mejía et al. (2022)	Modelo de gestión de tráfico WAN	Incremento de tasa de transferencia (+609%), reducción de retardo (−93,77%), jitter (−99,12%) y pérdida de paquetes (−84,82%)
Barba Vera (2025)	SDN + políticas QoS para control de amenazas internas	Mejora significativa en delay, jitter, pérdida de paquetes y ancho de banda
Cevallos Troya & Parra Balza (2022)	IEEE 802.11ax (WiFi 6) + simulación de migración	Latencia más baja, velocidad hasta 2402 Mbps, mayor estabilidad y cobertura

Nota. La tabla presenta una comparación de estudios recientes relacionados con la optimización de redes, calidad de servicio (QoS) y tecnologías emergentes utilizadas para mejorar el rendimiento y la eficiencia de las infraestructuras de comunicación.

En la NGN, la integración de SDN tiene la facultad de cambiar la forma en que operan y gestionan las redes de telecomunicaciones. SDN no sólo permite gestionar el tráfico en forma más flexible y eficiente, sino que también puede incrementar el rendimiento de la red, reducir costes operativos y mejorar su seguridad (Cisco Systems, 2023). La evolución de las redes de nueva generación también requiere la integración de SDN para afrontar los retos del futuro de

forma que las NGN puedan responder a la demanda de las aplicaciones y de los usuarios (Kreutz, 2015).

La combinación de NGN y SDN no sólo propone mejoras de carácter técnico a las telecomunicaciones; además, requiere un cambio estratégico de cómo las organizaciones/operadores de telecomunicaciones gestionen sus infraestructuras. Con la expansión de la adopción de redes SDN, las redes futuras estarán más dispuestas a gestionar el tráfico adecuadamente, así como las telecomunicaciones constituirán hasta el futuro una plataforma fiable y flexible (Bruno Astuto A. Nunes, 2014).

Desde la visión social, el SDN y el SD-WAN facilitan la inclusión digital y la calidad de los servicios públicos, posibilitando el acceso a servicios muy relevantes en áreas rurales y remotas, y en cuanto a los aspectos ambientales, los SDN y el SD-WAN contribuyen, gracias a la mejora de los recursos de red y la vida útil de los dispositivos de red existentes y contra el desperdicio electrónico y la reducción del consumo energético (Geographic, 2019).

Por lo tanto, el uso del SDN y el SD-WAN es una opción válida y adecuada para resolver las problemáticas que deben resolver las redes de telecomunicaciones a causa de las exigencias de la operación diaria y con efectos positivos en cuanto a la eficiencia de la operación de la red, pero también a la vez en el desarrollo social y el desarrollo ambiental. Este trabajo da pie a futuras continuaciones e investigaciones en el impacto del SDN y el SD-WAN sobre la solución en sectores específicos y también sobre el potencial para transformar la conectividad en el contexto planetario y local.

Desafíos de Seguridad y las Soluciones Necesarias para Proteger las Redes NGN Basadas en SDN

A partir de este punto, los resultados se estructuran con base en el análisis cualitativo realizado a las entrevistas aplicadas a cinco expertos del sector de telecomunicaciones y redes, cuyos aportes fueron codificados de acuerdo con los ejes temáticos definidos en la investigación; el proceso de codificación se desarrolló mediante una lectura analítica, identificando categorías emergentes relacionadas con vulnerabilidades, riesgos, estrategias de mitigación, buenas prácticas y correspondencias normativas; las citas textuales que se presentan a continuación fueron integradas tras una revisión interpretativa y se referencian por entrevistado numerado del 1 al 5, de manera que la interpretación se fundamente tanto en la evidencia empírica como en la revisión documental técnica y normativa (Anexo A); adicionalmente, en el anexo digital disponible en el repositorio institucional se puede consultar una de las entrevistas completas, que respalda la triangulación metodológica (ver Entrevista 1 en: https://drive.google.com/file/d/1-v3HfzmPKoqfnUC4PIhqR4xAFw4C76uF/view?usp=drive_link).

Principales Vulnerabilidades Identificadas

Los hallazgos derivados de las entrevistas llegan a la conclusión de que las redes de nueva generación fundadas en Software Defined Networking presentan vulnerabilidades polares en el plano de control, la autenticación de dispositivos y la exposición de las APIs, lo que se encuentra alineado con los informes técnicos del IEEE (2023) y con las directrices de la Open Networking Foundation (ONF, 2022) donde indicaban que el desacoplamiento entre control y reenvío daba lugar a nuevos vectores de ataque.

El entrevistado 1 hizo referencia a que “los controladores deben replicarse para garantizar resiliencia frente a fallas o ataques”, lo que deja entrever una de las preocupaciones centrales de

la disponibilidad del servicio y la descendencia operativa frente a ataques de denegación del servicio o compromisos del plano lógico, en la misma línea el entrevistado 5 apuntó que “si vulneran el controlador, comprometen toda la red”, resaltando el riesgo sistémico de la centralización de decisiones y que también, según Li et al. (2023) es una de las debilidades estructurales más comúnmente estudiadas en los entornos SDN.

Por su parte, el entrevistado 4 amplía el debate al afirmar que “el auténtico reto está en cómo proteger la red de las amenazas que traerá consigo la computación cuántica”, desde una lectura prospectiva del asunto de la seguridad, en la que es preciso contar con algoritmos criptográficos que sean recursivos para poder eludir la capacidad de tratamiento cuántico que vulnerará a los actuales protocolos de cifrado simétrico y asimétrico; esta preocupación no estaba tan explícitamente explicitada en los marcos técnicos primigenios de ITU-T Y.3300 (2019), pero comienza a asomarse en estudios recientes sobre la resiliencia en redes definidas por software en el contexto de aceleración tecnológica y, finalmente, los entrevistados coinciden en que la exposición de los interfaces abiertos, la mala gestión de los certificados y la falta de una segmentación adecuada aumentan su superficie de ataque, confirmándose lo expuesto por Kreutz et al. (2021) sobre la vulnerabilidad de las aplicaciones norte-sur en el entorno multiusuario.

Riesgos por Planos de Arquitectura

La estructura de tres planos propia de SDN —el plano de aplicación, el plano de control y el plano de infraestructura— conlleva riesgos diferenciados que los participantes reconocieron con claridad; así, el entrevistado 2 comentó que “sólo los equipos autenticados con certificado pueden conectarse al entorno de red”, poniendo de manifiesto que la autenticación mutua entre controlador y dispositivos de reenvío representa una solución base para la seguridad del plano de

infraestructura, instando, el entrevistado 3 a hacer uso de “políticas que aíslan segmentos ante una intrusión”.

Lo que corrobora una comprensión funcional del principio de segmentación dinámica y micro aislamiento que queda recogido en las indicaciones del NIST SP 800-207 (2020) sobre arquitecturas Zero Trust; así, el riesgo se distribuye jerárquicamente, encontrando el plano de control con un riesgo en el ataque por denegación de servicio, manipulación de reglas, escalado lateral y el plano de aplicación en riesgo por inyección de código o manipulación de políticas a través de APIs expuestas.

Desde un punto de vista documental, los informes de la ONF (2022) proponen que se implemente cifrado TLS en las comunicaciones entre planos, control de acceso por roles (RBAC) y el monitoreo continuo de flujos, tal y como también hizo el propio entrevistado 2 en la descripción del uso de certificados digitales y de segmentación en el modelo operativo; esta concordancia entre teoría y práctica hace ver que, aún cuando los marcos normativos ya nos plantean directrices de seguridad, la verdadera efectividad dependerá de su correcto aplicar y mantener, por otro lado, la mera replicación de controladores puede llegar a ser ineficaz con el no haber verificado de forma periódica la integridad.

Estrategias Técnicas de Mitigación

Las estrategias puestas de manifiesto, a través del análisis de los temas identificados, evidencian tres enfoques complementarios: la redundancia estructural, la autenticación mejorada y la detección anticipada de anomalías mediante aprendizaje automático; los informantes 1 y 5 estuvieron de acuerdo en evidenciar la implementación de la redundancia geográfica de controladores y la sincronización entre dominios como prácticas fundamentales para mantener la disponibilidad correspondiente con las recomendaciones que la RFC 7426 del IETF (2021)

establece sobre la arquitectura SDN y la resiliencia; además, los informantes sobre estos aspectos subrayan que la segmentación dinámica y la automatización de las políticas de aislamiento reducen el tiempo de contacto ante un ataque, facilitando la reconfiguración inmediata de rutas o flujos.

En la revisión técnica, Ranjbar et al. (2022) llegaron a la conclusión de que la incorporación de módulos de Machine Learning para detectar intrusiones en controladores OpenFlow disminuye el tiempo de respuesta ante tráfico malicioso en un 35 %, lo cual complementa lo declarado por el entrevistado 3, que afirmó que existen "políticas que aíslan segmentos ante una intrusión", reforzando así la importancia de las estrategias contención activa; a su vez, el decreto de políticas Zero Trust así como el seguimiento contemporáneo de logs son considerados por Moriarty y Kent (2023) como mecanismos críticos de mitigación ante accesos no autorizados en entornos de control programable.

Buenas Prácticas y Estándares

El contraste y comparación mediante entrevistas y revisión documental hizo posible la identificación de la consonancia con los marcos internacionales de referencia, en particular la norma ISO/IEC 27033 de seguridad de redes, la guía NIST SP 800-207 de arquitecturas Zero Trust y las recomendaciones ONF Security WG 2022, que destacan la autenticación continua, la segmentación y la gestión de vulnerabilidades, donde los entrevistados hacen referencia a mecanismos de integración de certificados digitales, auditorías del firmware, cifrado TLS, control de acceso por roles, encontrando similitudes con la sugerencia de la ITU-T X.805 (2021) en materia de seguridad de la infraestructura crítica.

El entrevistado 2 precisó que "solamente los equipos que han sido autenticados con certificado pueden acceder al entorno de red", una afirmación que muestra la incorporación de

las buenas prácticas de identidad digital, mientras que el entrevistado 1 añadió que “debe estar replicados los controladores”, afirmando la incorporación de principios de disponibilidad establecidos dentro de las políticas de continuidad operacional, en este sentido la adopción de estándares no va reñida sólo con la formalidad, sino más bien como una garantía de interoperabilidad y de trazabilidad frente a auditorías de seguridad o de ciberincidente.

Perspectiva de los Expertos

La interpretación transversal de las cinco entrevistas permite concluir que los especialistas entienden la seguridad en SDN no como una cierta configuración estática sino como un proceso dinámico y continuo, dado que la elasticidad de la red necesita de mecanismos de defensa del mismo carácter; el entrevistado 4 introduce el factor computacional cuántico como posible amenaza futura, abriendo el debate acerca de la necesidad de incluir mecanismos criptográficos post cuánticos en la arquitectura SDN, mientras que el entrevistado 3 reitera que la segmentación y el aislamiento automático son las herramientas más potentes para hacer frente a ataques de tipo lateral o persistente.

Además, todos los participantes coincidieron en que el nivel de madurez de las implementaciones en entornos NGN depende no solo de la infraestructura técnica, sino también de la capacitación del personal y la actualización constante de políticas, un aspecto que también resalta Tafur y Carrillo (2023) al indicar que la ciber resiliencia institucional se fortalece mediante la cultura de seguridad y la auditoría preventiva.

Tabla 10

Relación entre Hallazgos Empíricos y Revisión Normativa Sobre Seguridad en SDN/NGN

Eje Analizado	Evidencia Empírica (Entrevistas)	Correspondencia Normativa / Técnica	Conclusión Integrada
Vulnerabilidades principales	Riesgo en el controlador central (Entrev. 5)	RFC 7426, IEEE 802.1X	Se requiere redundancia y autenticación reforzada
Riesgos por planos	Segmentación dinámica (Entrev. 3)	NIST SP 800-207	Zero Trust reduce exposición lateral
Estrategias de mitigación	Replicación geográfica (Entrev. 1)	ONF Security WG 2022	Mejora la disponibilidad ante fallas
Buenas prácticas y estándares	Certificados digitales (Entrev. 2)	ISO/IEC 27033	Autenticación basada en identidad digital
Perspectiva prospectiva	Amenazas cuánticas (Entrev. 4)	ITU-T X.805	Exige transición hacia criptografía post-cuántica

Nota. La tabla integra los hallazgos empíricos obtenidos mediante entrevistas con referentes normativos y técnicos internacionales sobre seguridad en redes definidas por software (SDN) y redes de próxima generación (NGN). “Entrev.” corresponde a las entrevistas realizadas a especialistas durante el proceso de investigación.

La compatibilidad entre los hallazgos empíricos y las normas técnicas examinadas pone de relieve una coherencia conceptual entre práctica y teoría; pero también existe evidencia de

vacíos de aplicación a nivel local, en la medida en que, si bien las medidas de replicación, autenticación y aislamiento están en perfecta correspondencia con las normas de ISO/IEC 27033 y guías de la ONF (2022), los encuestados inciden en que las organizaciones colombianas aún no cuentan con políticas de gestión de riesgo que tengan en cuenta el contexto SDN, lo cual puede poner en riesgo la efectividad de las medidas de seguridad

En todo caso, los retos de la seguridad en redes NGN sobre SDN se agrupan sobre la base de tres ejes: la vulnerabilidad estructural del plano de control, la falta de autenticación y la falta de automatización en la detección de incidentes; frente a ellos, las medidas más eficaces integran redundancia, cifrado, monitoreo y segmentación, siempre con el soporte de la adopción de marcos normativos internacionales, pero requieren consolidar capacidades institucionales y técnicas que garanticen la estabilidad y resiliencia de la infraestructura crítica del país.

Marco de Buenas Prácticas para la Implementación de Redes SDN en Infraestructuras de Telecomunicaciones

Los especialistas consultados coinciden en que la adopción de una infraestructura en SDN comporta una renovación tecnológica, pero también un cambio cultural y organizativo drástico, ya que el control desde un proceso programado y la centralización de políticas requieren de capacidad distinta a la requerida por la administración tradicional de las redes, el operador 1 apuntó que “cada una de estas modificaciones queda registrada y versionada para evitar errores y retroceder ante los fallos para revertirlos rápidamente”, lo cual pone de manifiesto la adopción de un modelo de desarrollo y operaciones (DevOps) que une la operación de la gestión con el control de versiones, la práctica del control de versiones que para Cisco (2022) constituyen un fundamento de la red automatizada en la medida que garantizan la trazabilidad y la reversibilidad ante incidentes.

Del mismo modo el operador 3 agregó que “la automatización evita errores humanos, pero además da una respuesta mucho más rápida, incrementando la disponibilidad del propio servicio”, dejando claro que la automatización no solo mejora los tiempos de respuesta sino que también provoca que la estabilidad aumente en el entorno de producción, este planteamiento es coherente con lo expuesto por Huawei (2022) en su documento Intelligent Network Operations, que dice que los sistemas de tareas basados en la IA y en flujos declarativos pueden reducir hasta en un 40% el coste en coste de las tareas manuales de configuración, reafirmando así la relación entre la automatización, la eficiencia y la resiliencia.

Los entrevistados también mencionaron que la puesta en marcha debe realizarse partiendo de un entendimiento pleno sobre el estado del ámbito técnico y organizacional, por este motivo el entrevistado 4 hizo hincapié en que “una buena implementación depende de un levantamiento pormenorizado y de la automatización”, poniendo de manifiesto que la preparación del entorno para la ejecución de una implementación, así como la recopilación de información, son pasos que determinan la estabilidad del despliegue, ya que las cuestiones descritas se encuentran en línea con los planes que expone el Project Management Institute (PMI, 2021) y la forma de prestar servicios según las guías ITIL v4, las cuales establecen la necesidad de planificar, validar y documentar antes de llevar a cabo cualquier modificación en las infraestructuras críticas.

Errores Comunes en la Implementación

La investigación empírica indicó generar una lista de errores comunes en las pruebas realizadas de los proyectos adoptados de SDN que repercuten directamente en la eficiencia del sistema y la sostenibilidad operativa de los mismos, siendo los de faltar una documentación previa, no llevar a cabo pruebas de interoperabilidad o implementar simultáneamente en toda la

red sin un piloto, el entrevistado 2 indicó "primero probamos en un entorno controlado antes de masificar la solución de SDN", el cual evidencia una comprensión metodológica que cumple con las recomendaciones de ONF (2022) las cuales estipula la realización de pruebas piloto como fase obligatoria antes de la adopción completa con un fin de evitar riesgos que puedan ser de incompatibilidad o fallos al no ser sincronizados

Asimismo, los entrevistados indicaron que otro de los errores más comunes consistía en restar importancia al entrenamiento del personal, llevando a que las ventajas teóricas de la arquitectura SDN se diluyeran en la práctica, al no haber una base sólida de compresión del modelo declarativo, la ONF (2021) insiste en que el manejo basado en intenciones es necesario un personal que comprenda los principios de orquestación, programación y monitoreo continuo, sin ellos la red comienza a operar y se ejecutan con las limitantes de un sistema tradicional, sin llegar a la optimización y la disminución de costos.

El entrevistado 5 comentó también que, “en primer lugar, se documenta y, luego, se estandariza antes de aplicar los cambios”, identificando como erróneo el hecho de no establecer políticas de documentación antes de la etapa de despliegue, una práctica que Cisco (2023) considera como un desencadenante de sobrecostes de hasta un 25 % en condiciones de operación, relacionado con la no existencia de trazabilidad, tal cual es expuesto y definido por el citado autor, el cual se conecta con lo que se denomina modelo, el factor técnico está unido al administrativo, se pone de manifiesto que las buenas prácticas no son únicamente configuraciones técnicas, sino que también se parecen a procedimientos de gobernanza tecnológica que aseguran la sostenibilidad y eficiencia de forma relativamente continuada.

Buenas Prácticas Documentadas

La coincidencia entre la evidencia empírica y la documentación técnica analizada permite elaborar un conjunto de buenas prácticas, las cuales constituyen el núcleo del marco propuesto, y las agrupamos en tres niveles complementarios: planificación y diseño, automatización y control, y evaluación y mejora continua.

En el nivel de planificación y diseño, se resalta que hay que realizar un levantamiento exhaustivo de la red existente, documentar dependencias, determinar políticas de seguridad y hacer diseño de arquitecturas modulares que permitan escalabilidad, el entrevistado 4 reiteró que el levantamiento inicial es lo que habilita al proyecto, afirmando que "una buena implementación depende frecuentemente de un levantamiento exhaustivo", y esta idea ha sido corroborada por los autores de Huawei (2023) en la SDN Deployment Guide, donde se habla de mapas de dependencias y de puntos de fallo antes de la decisión del flujo de control centralizado.

En el nivel de automatización y control, los testimonios enfatizan la necesidad de integrar herramientas de orquestación que minimicen la intervención humana, en este punto el entrevistado 3 resaltó que "la automatización evita errores humanos y acelera procesos", lo que enlaza con los principios de eficiencia definidos por Cisco DNA Center y las metodologías DevNet Automation, donde se establece que la reducción de tiempos operativos depende directamente del grado de automatización de flujos y de la coherencia entre scripts y políticas de red, este enfoque, sustentado en la teoría de la gestión declarativa, demuestra que los sistemas SDN no solo sustituyen dispositivos por software, sino que transforman el paradigma operativo hacia un modelo predictivo y autoajustable.

En relación con el aspecto de evaluación y mejora continua de las versiones, todos los entrevistados mostraron acuerdo en la realización de pruebas de aceptación, así como

simulaciones, antes de lanzar nuevas versiones o configurar nuevas versiones del sistema. En ello, los entrevistados explican la necesidad de implementar entornos de staging donde estén permitidos los cambios y donde éstas estén sometidas a pruebas sin que estén en funcionamiento en la red productiva. En el caso del entrevistado 2, éste corroboró las afirmaciones de la idea anterior al decir “primero hacemos una prueba en un entorno controlado antes de masificar la solución”; así mismo, la idea también pone de manifiesto la importancia de los pilotos progresivos, los cuales también forman parte del ciclo de mejora continua de las prácticas ITIL v4, y donde cada cambio ha de ser revisado, auditado y optimizado antes de ser puesto en funcionamiento en la operación.

Integración Empírica-Documental

Las diferencias entre el resultado del trabajo de campo y las fuentes documentales muestran que existe una coincidencia estructural entre lo que los especialistas aplican en la práctica y lo que prescribe el estándar internacional, en el que por ejemplo la ONF (2022) indica que solo se puede hablar de eficiencia operativa de la SDN cuando el plano de control se vuelve un plano programable, monitorizable y replicable, condición que también aparece reflejada en las narrativas que los entrevistados han ofrecido, quienes reivindican la automatización, la documentación y la estandarización como ejes esenciales de sostenibilidad

Los lineamientos de Cisco (2023) y Huawei (2022) expresan que la gobernanza de red se debe asentar en políticas versionadas, gestión del cambio controlada y en monitoreo mediante telemetría en tiempo real, prácticas que han sido reivindicadas por los participantes, pero que han tenido especial énfasis en el participante 1, quien hace hincapié en el registro y la versión de cada cambio en línea con la metodología DevOps, la cual junta la operación con el desarrollo para garantizar la continuidad del servicio.

De igual forma, la literatura académica que representa Kreutz et al. (2021) y Li et al. (2023) expone que la eficiencia de SDN depende de la capacidad que tienen las redes de automatizar y auditar los procesos de red, disminuyendo el coste de mantenimiento y aumentan así la fiabilidad de los servicios, en este sentido, dicha afirmación se confirma empíricamente en las entrevistas, donde los expertos destacaron la disminución de los tiempos de diagnóstico, el fácil retorno de los cambios, así como la mejora en la disponibilidad del servicio, consolidando así una base empírica fuerte para la elaboración del marco de buenas prácticas.

Propuesta de Marco de Buenas Prácticas

Desde el cruce de la evidencia empírica a partir del campo y de la revisión documental, se obtiene un marco de buenas prácticas para la implementación de redes SDN en infraestructuras de telecomunicaciones orientado a optimizar los recursos tecnológicos, a reducir los costes de explotación y a maximizar la resiliencia del sistema, el cual está compuesto por cinco principios que van en línea con la evidencia empírica y con la revisión técnica especializada.

Gobernanza y documentación continua. La cual establece que cada proceso de modificación, de despliegue o de actualización debe estar documentado, versionado y validado antes de la ejecución, en la misma línea argumentativa dada por el entrevistado 5 por cuanto y en coherencia con lo que recomiendan ITIL v4 y Cisco (2023), esta práctica garantiza trazabilidad y una reducción de la posibilidad de error por falta de control documental.

Implementación y pruebas en entornos controlados. Que se trata de ejecutar despliegues controlados en entornos de pruebas según lo que la ONF (2022) describe, conforme a lo que expresa el entrevistado 2, permitiendo medir el impacto antes del despliegue masivo y así reducir la posibilidad de que se interrumpan los servicios.

Inteligencia de la automatización y orquestación. Compendiando con funcionalidades de software que reduzcan la intervención humana, permitan la consistencia y agilicen la respuesta ante incidentes, principio que se obtiene a partir de las apreciaciones expresadas por el entrevistado 3 ; refutado por las guías técnicas de Huawei (2022) acerca de las redes autónomas

Levantamiento detallado y planificación previa. Que nos indica realizar diagnósticos exhaustivos de la infraestructura, las dependencias y los recursos antes de comenzar la implementación, tal y como se sugiere por el entrevistado 4; recopilando todos los enfoques de la gestión del cambio del PMI (2021)

Estandarización y mejora continua. Que indica que se deben generar documentación técnica, guías y políticas internas de operación a partir de métricas del rendimiento y revisiones periódicas de documentos, siguiendo tanto los principios de la ONF como las estrategias de gobernanza tecnológica descritas en las entrevistas.

Tabla 11

Matriz de Propuesta: Marco de Buenas Prácticas para la Implementación de Redes SDN en Infraestructuras de Telecomunicaciones

Etapa / Fase	Descripción Técnica y Actividades Específicas	Responsables	Tiempo Estimado	Recursos y Materiales Requeridos	Resultados Esperados / Indicadores
1. Diagnóstico y levantamiento de infraestructura actual	Realizar un levantamiento completo del entorno físico y lógico de red, identificando topologías, equipos legados, controladores existentes, flujos de datos y políticas actuales; elaborar un mapa de dependencias y un inventario de activos críticos; aplicar herramientas de descubrimiento automático y auditoría (como Cisco Network Assistant o SolarWinds); validar compatibilidad con controladores SDN (OpenDaylight, ONOS, Cisco ACI).	Ingeniero líder de red, analista de infraestructura, equipo de soporte NOC	2 a 3 semanas	Herramientas de monitoreo, software de topología, hojas de cálculo normalizadas, acceso remoto a nodos, manuales técnicos	Inventario validado, matriz de compatibilidad SDN, mapa de riesgos inicial, documentación base para diseño
2. Planeación estratégica y diseño del entorno SDN	Diseñar la arquitectura SDN adaptada a la red NGN, definiendo capas de control, datos y aplicación; seleccionar el protocolo de comunicación (OpenFlow, NETCONF o REST API) según interoperabilidad; establecer políticas de segmentación y	Arquitecto de red, jefe de proyecto SDN, comité técnico	3 a 4 semanas	Diagramas de arquitectura (Visio o GNS3), documentación ONF TR-521, guías Cisco/Huawei, manuales ITIL v4	Diseño lógico y físico validado, plan de implementación aprobado, matriz de riesgos y dependencias técnicas

	seguridad Zero Trust; definir plan de migración por fases; validar capacidad de redundancia de controladores y switches; documentar los KPIs técnicos (latencia, throughput, resiliencia).				
3. Implementación piloto controlada	Instalar un entorno piloto en un segmento de la red (por ejemplo, un dominio de acceso o agregación); configurar controladores SDN y switches compatibles; aplicar scripts de automatización (Python/Ansible); ejecutar pruebas de flujo de datos, balanceo de carga, failover y monitoreo; medir indicadores base (latencia, pérdida de paquetes, consumo energético).	Ingenieros de implementación, DevOps, analistas QA	4 a 6 semanas	Laboratorio virtualizado (EVE-NG o VMware), switches SDN, servidores controladores, licencias de software	Validación funcional del entorno SDN, métricas de desempeño, reporte de incidencias, plan de ajuste
4. Estandarización y documentación operativa	Elaborar y aprobar protocolos estandarizados de operación y mantenimiento basados en ITIL, ISO/IEC 20000 y ONF Core Models; incluir políticas de cambio, rollback y control de versiones; crear manuales de procedimientos y guías de buenas prácticas; versionar documentación en repositorio Git; capacitar al personal técnico.	Coordinador de calidad, ingeniero de documentación, líder de capacitación	2 a 3 semanas	Plantillas ITIL, software de gestión documental (Confluence, GitLab), guías de ONF	Manual de operación SDN aprobado, base documental accesible, cumplimiento de estándares de gobernanza tecnológica

5. Automatización y orquestación de servicios	Implementar herramientas de orquestación y automatización (Ansible, Terraform o Cisco NSO) para desplegar configuraciones masivas y coherentes; aplicar políticas de aprovisionamiento automático, gestión de fallos y recuperación ante incidentes; integrar con plataformas de monitoreo (Prometheus, Grafana).	Ingeniero DevOps, arquitecto SDN, especialista en orquestación	3 a 4 semanas	Herramientas de automatización, scripts de despliegue, controladores SDN, servidores de monitoreo	Red automatizada y coherente, reducción de errores humanos, disminución del tiempo de configuración en un 30%
6. Evaluación de desempeño y optimización de costos	Monitorear indicadores de eficiencia energética, disponibilidad y costos operativos; comparar métricas antes y después de la implementación SDN; realizar análisis ROI (retorno de inversión) y TCO (costo total de propiedad); aplicar algoritmos de optimización de tráfico y recursos según la carga; ajustar políticas de QoS.	Equipo de ingeniería financiera, analista de datos, ingeniero de red	4 semanas	Herramientas de análisis financiero (Power BI, Excel avanzado), logs de red, reportes de rendimiento	Disminución del OPEX en al menos 20%, mejora de disponibilidad >99.9%, informe de resultados y sostenibilidad
7. Expansión y mejora continua	Escalar la solución SDN a otros dominios de la red; integrar funciones de seguridad avanzada (NFV, IDS/IPS virtuales); incorporar análisis predictivo con IA para gestión proactiva; actualizar documentación periódicamente.	Comité de innovación tecnológica, ingeniero SDN, coordinador de seguridad	3 a 6 meses (fase continua)	Plataformas NFV, software de IA, sistema de tickets, dashboard de indicadores	Red escalable, resiliente y optimizada, mejora continua del servicio, sostenibilidad a largo plazo

*Nota***.** La tabla presenta el marco de buenas prácticas propuesto para la implementación progresiva de redes definidas por software (SDN).

Este marco no solo responde a la necesidad de uniformar procedimientos técnicos, sino que también constituye una herramienta estratégica para las organizaciones que buscan reducir la dependencia de intervenciones manuales, optimizar recursos humanos y materiales, y garantizar la continuidad de los servicios en redes de nueva generación, por tanto, la eficiencia en la implementación de SDN se fundamenta en una combinación equilibrada entre automatización, control documental y aprendizaje organizacional permanente, lo que convierte la arquitectura definida por software en un eje de transformación tecnológica y administrativa dentro del ecosistema de telecomunicaciones contemporáneo.

Evaluación del Impacto Social y Ambiental de las Redes Definidas por Software

A partir del marco de buenas prácticas propuesto para la implementación de redes definidas por software, surge la necesidad de analizar su impacto social y ambiental, considerando que toda innovación tecnológica debe evaluarse no solo por su eficiencia operativa, sino también por su capacidad de generar equidad, sostenibilidad y bienestar colectivo, en este sentido, el presente apartado desarrolla los resultados correspondientes al objetivo de evaluar el impacto social y ambiental de las SDN.

Enfoque Social y Ético de SDN

La introducción de las redes definidas por software en los ecosistemas de telecomunicaciones ha supuesto un avance no solo técnico -casi diría subjetivo- sino también ético y social, toda vez que su diseño flexible, programable y descentralizado modifica la manera en que las comunidades acceden, gestionan y perciben en torno a la conectividad, dado que la virtualización de los recursos y la automatización de los procesos permiten optimizar la infraestructura, pero al mismo tiempo conllevan desafíos en términos de equidad, de derechos a

la vida privada, a la inclusión digital, etcétera, retos que hacen necesario abordar desde un marco de responsabilidad tecnológica y de justicia social.

De hecho, informes como el ICT Development Index (ITU, 2023) señalan que la transformación digital requiere garantizar la accesibilidad universal, la neutralidad de la red y la protección de los datos personales, principios que, aplicados a las arquitecturas SDN, requieren de diseñar políticas de gobernanza enfocadas en la ética y en la razón de ser, sabiendo que, en cualquier caso, la tecnología no es una finalidad en sí misma sino un medio de eliminar desigualdades.

Quienes participaron en la entrevista coincidieron en señalar que el despliegue de SDN lleva consigo una importante carga ética porque el acceso al control de red y a la gestión de recursos debe democratizarse, no dejando fuera a usuarios o territorios por razones económicas o geográficas y que, tal como indicaba el entrevistado 2, “las decisiones técnicas deben ser coherentes con la función social del acceso a la red, porque la red, al final, también es un servicio público” (entrevistado 2, 2025).

Lo que coincide con el planteamiento de la ONU (2022) que afirma que la conectividad digital debe ser considerada como un derecho habilitador del desarrollo humano y no como un privilegio que sólo tienen acceso los agentes económicos de mercado o que se define por el poder adquisitivo, algo que lleva a planificar de un modo ético las redes definidas por software que debe tener en consideración, no sólo la eficiencia y el rendimiento sino también la justicia distributiva y la sostenibilidad social en el uso de los recursos tecnológicos.

Sostenibilidad Energética y Medioambiental

Desde el punto de vista ambiental, las redes SDN pueden ser una ayuda significativa para que sean energéticamente sostenibles, ya que la capacidad de automatizar y programar

dinámicamente los flujos de datos permite descansar los nodos inactivos, soportar en equilibrio las cargas y reducir el impacto del sobre aprovisionamiento, que en las infraestructuras tradicionales conllevaba despilfarrar grandes cantidades de energía.

Tal como menciona Huawei (2023) quien apunta que con la implementación de arquitecturas SDN en redes de telecomunicaciones se pueden llegar a reducir anualmente el gasto de energía hasta en un treinta por ciento gracias a algoritmos de gestión inteligente del tráfico y políticas operativas en función de su eficiencia, lo cual lleva a una red de telecomunicaciones más ecológica y más resiliente ante la creciente necesidad de conectividad global, ya que la lógica definida por software permite la implementación de políticas verdes de un modo centralizado en tiempo real.

En línea con dicho posicionamiento, el entrevistado 4 expresó que “la virtualización nos permite medir la eficiencia energética y ajustar las cargas a la demanda, evitando el gasto superfluo” (entrevistado 4, 2025), lo que muestra una preocupación ambiental incluida en la práctica de tecnologías, pero el entrevistado 5 logró destacar la incorporación de fuentes renovables y las políticas de apagado inteligente para equipos bajos tráficos, lo que también coincide con las recomendaciones de la ITU-T L.1470 sobre Green ICT Strategies que promueven el diseño de las redes de bajo parte de las emisiones de carbono y la medición continua de la huella de la energía digital; en este sentido, la sostenibilidad del SDN no se refiere solamente a una disminución del consumo eléctrico, sino que abarca totalmente el ciclo de la vida tecnológica, desde la fabricación hasta la disposición de final de los equipos envolvidos, incluyendo los motivos de la economía circular o la predicción de mantenimiento.

Vinculación con los ODS

El efecto social y medioambiental que produce SDN está asociado directamente con diversos ODS (Objetivos de Desarrollo Sostenible), especialmente el ODS 7, que favorece la energía asequible y no contaminante; el ODS 9, cuyo fin es el desarrollo de infraestructuras resilientes y la modernización industrial; y el ODS 13, que busca adoptar medidas urgentes frente al cambio climático; el Informe Global sobre Sostenibilidad Digital (ONU, 2023) explica que las arquitecturas definidas por software siguen contribuyendo a estos ODS gracias a la eficiencia energética, la optimización del uso de recursos y la reducción de emisiones asociadas al mantenimiento físico intensivo así como el acceso inclusivo a las tecnologías de la información y la comunicación, lo cual también fortalece el ODS 10 orientado a reducir las desigualdades sociales.

Según Huawei (2024), la adopción de SDN con mecanismos de gestión energética que sepan en qué condiciones hay poca o nula carga de trabajo puede reducir un 40% de la huella de carbono asociada a los datacenters y a las backbone networks y en paralelo la automatización de procesos administrativamente permite dirigir recursos humanos y financieros a programas de desarrollo local, educación digital y participación ciudadana, fortaleciendo la dimensión social del desarrollo sostenible; de esta manera, la integración de SDN de los sistemas de telecomunicaciones no solo responde a una necesidad técnica

La evaluación final del impacto social y ambiental de las redes definidas por software permite concluir que estas constituyen un modelo de transformación tecnológica coherente con los principios de sostenibilidad, equidad y eficiencia que exige la sociedad contemporánea, pues al permitir la gestión inteligente de recursos y la automatización de procesos, SDN optimiza la infraestructura, disminuye el consumo energético y amplía el acceso equitativo a la conectividad,

aspectos fundamentales para el desarrollo humano y la protección del planeta; sin embargo, esta evaluación también evidencia que los beneficios no son automáticos, sino que dependen de la implementación de políticas de gobernanza, control ético y regulación ambiental que aseguren el uso responsable y equitativo de la tecnología.

La articulación entre los aportes de los entrevistados y los informes institucionales demuestra que la sostenibilidad de SDN debe entenderse de manera integral, considerando tanto la eficiencia técnica como el bienestar social y el equilibrio ecológico, por lo cual el éxito del modelo radica en su capacidad de conjugar la innovación tecnológica con la justicia social y ambiental; en consecuencia, el impacto de SDN no se limita a los indicadores de desempeño, sino que se proyecta como un catalizador del cambio estructural hacia una economía digital sostenible, inclusiva y ética, que impulse el cumplimiento de los Objetivos de Desarrollo Sostenible y fortalezca la gobernanza tecnológica responsable en el ámbito global.

Conclusiones

La investigación conduce a una comprensión ampliada de qué manera la adopción de Software-Defined Networks transforma la arquitectura y la operación de las Redes de Próxima Generación entendiendo que la presencia de un control centralizado y de la separación lógica entre planos facilita la administración grupal eficiente y predictiva de los flujos de datos resultando de gran significado ante el aumento acelerado del tráfico digital y la demanda de servicios de gran disponibilidad dejando expuesto que las SDN no solo significan un avance tecnológico sino que son también una transformación de las formas de gestionar infraestructuras complejas en el ámbito de las telecomunicaciones.

Mediante el análisis del impacto de la latencia y del servicio se llega a la conclusión que las SDN permiten una mejor ruta y que los algoritmos de balanceo de carga son capaces de reaccionar de forma dinámica ante la congestión en lo que supuso la identificación de una mejora significativa en caso de que la estabilidad y el tiempo de respuesta son de sumo interés para aplicaciones que están en el ámbito de la telemedicina, la educación virtual, los cloud services, o las plataformas multimedia destacando que dicha optimización no sólo produce una mejora en la experiencia del usuario final sino que también hace más competitivos a los operadores pues las provisiones de servicios son más robustas y adaptativas.

El estudio establece que la adaptabilidad de la arquitectura SDN permite gestionar mejor el ancho de banda, priorizar el tráfico crítico, y segmentar lógicamente lo que se traduce en un uso racionalizado de los recursos, especialmente con redes donde la variabilidad de la demanda es alta, revelando que la automatización supone reducir de forma notable los tiempos de intervención humana, y mejorar la implementación de políticas coherentes en toda la

infraestructura, incrementando la eficiencia que se traduce en la reducción de los costes de mantenimiento y operación.

Con respecto a los retos en términos de seguridad se vio que la centralización del controlador es un paso clave hacia la unificación de políticas, pero al mismo tiempo este se convierte en un punto potencialmente vulnerable que ha de tener medidas de protección que sean más sofisticadas por lo que se evidenció la importancia de incorporar autenticación en múltiples capas, segmentación dinámica, detección temprana de anomalías y arquitecturas de confianza cero para reforzar la resiliencia de las NGN y asegurar que la implementación de SDN no genere afectaciones negativas en el ecosistema digital sino que sea capaz de mejorar el nivel de protección frente a las amenazas emergentes.

En paralelo este trabajo dio lugar a que se pudiera desarrollar un marco de buenas prácticas en cuanto a la implementación responsable de SDN en las infraestructuras de telecomunicaciones con criterios técnicos operativos económicos ambientales y sociales lo que otorga a los operadores una hoja de ruta clara que favorece la implementación escalable de las tecnologías involucradas teniendo en cuenta aspectos como la disponibilidad de recursos formados, la coexistencia con redes heredadas, la planificación de riesgos, la gobernanza del controlador y de los requerimientos regulatorios que se traducen en un recurso aplicable en contextos públicos y privados.

En base a los impactos sociales se pudo determinar que las SDN contribuyen a la reducción de las brechas digitales debido a que permiten modelos de gestión que mejoran la disponibilidad de servicio en zonas rurales y periurbanas donde la infraestructura tradicional no presenta alternativas y demuestran que una gestión de la red basada en SDN puede aumentar su alcance favorecer políticas de inclusión digital mejorar el acceso a plataformas de educación y

salud y reducir desigualdades asociadas al acceso a información y a servicios críticos, con esto, se convierte a las redes definidas por software en un instrumento tecnológico dotado de gran valor social.

En lo que respecta a los impactos ambientales se obtuvo que la eficiencia energética propia de las SDN reduce significativamente la electricidad consumida debido al procesamiento y al enrutamiento tradicionales al poder la centralización del control apagar enlaces o nodos no utilizados optimizar rutas con menor demanda energética y gestionar recursos bajo esquemas inteligentes que reducen la huella de carbono. También se pudo comprobar que la virtualización limita la dependencia de hardware físico al menoscabar la vida útil de los equipos y reducir residuos electrónicos siendo las SDN una alternativa alineada con principios de sostenibilidad tecnológica.

La síntesis de los resultados permite concluir que la implementación de SDN en redes NGN permite en buena medida mejorar el rendimiento técnico y la eficiencia operativa pero además presenta unos beneficios en los ámbitos de la equidad social la sostenibilidad ambiental la innovación estratégica y la optimización de los recursos convirtiéndose en una solución integral en la que se puede abordar los grandes desafíos del sector de las telecomunicaciones en el se hace necesario insistir en la necesidad de seguir potenciando procesos de adopción de la tecnología de SDN procesos de formación de recursos humanos de inversión en infraestructuras programables y de dotar de políticas de regulación que acompañen el progreso de la tecnología de SDN a fin de que los beneficios que derivan de las redes de telecomunicaciones puedan ser sostenibles solidarios e inclusivos para todos y todas las personas.

Recomendaciones

Se sugiere que los operadores y los administradores de red vayan adoptando poco a poco esquemas de migración hacia arquitecturas SDN mediante pilotos controlados que se puedan utilizar para evaluar la operatividad en condiciones reales, dado que esta estrategia disminuye los riesgos operativos, facilita la interoperabilidad con redes heredadas y aporta pruebas empíricas para la toma de decisiones de inversión, así como para la adecuada formación del personal, permitiendo validar con antelación las compatibilidades de las tecnologías implicadas, favoreciendo en última instancia una migración estable, estructurada y basada en datos verificables.

De igual manera se recomienda fortalecer las capacidades institucionales en materia de las tecnologías de ingeniería de automatización y programación de redes dado que el funcionamiento de SDN necesita habilidades que son más avanzadas que las prácticas tradicionales de operación en redes de tipo NGN, fomentando la formación continua, certificaciones específicas y laboratorios de experimentación, que favorecen el aprendizaje de lenguajes como Python y frameworks como OpenFlow, aumentando así la eficacia operativa, reduciendo el factor humano de error y preparando a los equipos técnicos ante los nuevos retos que surgen en la operativa de la infraestructura programable.

Igualmente, se propone obtener una consolidación de políticas fuertes relacionadas con la seguridad en entornos centralizados en relación con la protección de sus controladores así como el plano de comunicaciones, incluir mecanismos de autenticación multifactor arquitecturas de confianza cero monitoreo continuo y segmentación dinámica garantizará que la flexibilidad de SDN no implique vulnerabilidades adicionales y sí, por el contrario, sea una oportunidad para

incrementar la capacidad de protección y resiliencia frente a las amenazas cada vez más sofisticadas que afectan a las redes modernas.

Se propone también extender el uso de herramientas analíticas y de orquestación con el objetivo de la automatización de procesos críticos tales como balanceos de carga, la asignación de rutas de forma dinámica y el aprovisionamiento sobre demanda, así como fomentar el uso de modelos declarativos que reduzcan la intervención manual y puedan incrementar la disponibilidad del servicio, ya que esta práctica permite una mejora en la eficiencia energética, disminución de los costes operativos y la toma de decisiones lideradas por métricas relacionadas con el comportamiento real del tráfico y del consumo.

Se sugiere que los operadores integren criterios de sostenibilidad ambiental en los planes de ampliación y modernización de infraestructura incorporando modelos de virtualización energética eficaz y de monitoreo inteligente del consumo de los nodos dado que las SDN permiten la desconexión automática de recursos ociosos y la administración óptima de los enlaces lo que ayuda a disminuir la huella de carbono los residuos electrónicos y la sujeción al hardware impulsando una transición responsable hacia redes más limpias y en línea con los ODS.

En términos de impacto social se aconseja la utilización de las capacidades de administración centralizada para extender la cobertura de servicios en regiones rurales y escasamente pobladas donde las restricciones del equipamiento de infraestructura convencional impiden la realización de conectividad o bien organizar programas públicos privados que utilicen SDN para implementar redes comunitarias educativas o de salud con el fin de asegurar un acceso equitativo que ayude a reducir la brecha digital ejecutar la inclusión tecnológica y democratizar las oportunidades procedentes del entorno digital contemporáneo.

Referencias Bibliográficas

Axity. (2023). Colombia: Axity y Cisco, puentes al futuro digital. Recuperado de https://axity.com

Barba Vera, R. G. (2025). *Metodología basada en políticas de QoS en SDN para el control de amenazas internas y mejora del rendimiento en intranets académicas* [Tesis de maestría, Pontificia Universidad Católica del Perú]. Repositorio institucional PUCP. http://hdl.handle.net/20.500.12404/31075

Bismark. (2023). Caso de uso SD-WAN en sedes bancarias. Recuperado de https://bismark.net.co

Brandon Heller, R., Sherwood, R., & McKeown, N. (2012). The controller placement problem. Proceedings of the First Workshop on Hot Topics in Software Defined Networks, 7-12. ACM. https://doi.org/10.1145/2342441.2342444

Cevallos Troya, D. F. (2022). *Evaluación de QoS, rendimiento, capacidad y seguridad de una red inalámbrica con estándar IEEE 802.11 ax* [Tesis de maestría, Universidad Tecnológica Israel]. Repositorio Universidad Israel. https://repositorio.uisrael.edu.ec/handle/47000/2854

Cisco Systems. (2023). *Cisco SD-WAN overview and architecture*. Cisco Press.

Cisco Systems. (2023). *Cisco SD-WAN security: Enabling secure network transformation*. Cisco Press.

Cisco Systems. (2023). *Software Defined Networking Deployment and Automation Guide*. Cisco Press.

Cladirect. (2023). Caso de éxito: Implementaciones de SD-WAN. Recuperado de https://www.cladirect.com

Escuela Colombiana de Ingeniería Julio Garavito. (2022). Redes Definidas por Software (SDN), un nuevo mundo para la seguridad de red. Recuperado de https://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2901/Trabajo%20de%20grado.pdf?sequence=1

Fortinet. (2023). SD-WAN explained. Recuperado de https://www.fortinet.com

González Pino, D. (2022). *Mejora de la calidad de servicio para plataformas multimedia* [Trabajo de fin de máster, Universidad Complutense de Madrid]. Repositorio Institucional UCM. https://hdl.handle.net/20.500.14352/73965

Goransson, P., Black, C., & Culver, T. (2016). *Software defined networks: A comprehensive approach*. Morgan Kaufmann.

Guerrero Loaiza, P. (2021). *Estudio comparativo de protocolos de enrutamiento de WMSN atendiendo a QoS y propuesta de mejora* [Tesis de máster, Universitat Politècnica de València]. RiuNet. https://riunet.upv.es/handle/10251/174420

Gupta, A., & Shah, A. (2020). *Modern networking concepts with Cisco SDN solutions*. McGraw-Hill Education.

Heller, B., Sherwood, R., & McKeown, N. (2012). The controller placement problem. En *Proceedings of the First Workshop on Hot Topics in Software Defined Networks* (pp. 7-12). ACM. https://doi.org/10.1145/2342441.2342444

Huawei Technologies. (2022). *Intelligent Network Operations: Automation for SDN Environments*. White Paper.

Impact of SD-WAN on modern network architectures. (2023). Global Telecom News. https://www.globaltelecomnews.com/sd-wan-impact/

Instituto de Ingenieros Eléctricos y Electrónicos (IEEE). (2023). *Security considerations for Software Defined Networking*. IEEE Standards Association.

International Telecommunication Union (ITU-T). (2021). *Recommendation X.805: Security architecture for systems providing end-to-end communications*. Geneva.

Jain, R., & Paul, S. (2013). Network virtualization and software-defined networking for cloud computing: A survey. *IEEE Communications Magazine, 51*(11), 24-31. https://doi.org/10.1109/MCOM.2013.6658658

Kreutz, D., Ramos, F., Veríssimo, P., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S. (2015). Software-defined networking: A comprehensive survey. *Proceedings of the IEEE, 103*(1), 14-76. https://doi.org/10.1109/JPROC.2014.2371999

Kreutz, D., Ramos, F., Verissimo, P., Rothenberg, C., Azodolmolky, S., & Uhlig, S. (2021). *Software-Defined Networking: A Comprehensive Survey*. *Proceedings of the IEEE*, 103(1), 14–76.

Kreutz, D., Ramos, F., Verissimo, P., Rothenberg, C., Azodolmolky, S., & Uhlig, S. (2021). *Software-Defined Networking: A Comprehensive Survey*. *Proceedings of the IEEE*, 103(1), 14–76.

Li, J., Zhang, Y., & Chen, L. (2023). *Controller vulnerabilities in SDN environments: Risk analysis and mitigation frameworks*. *Computer Networks*, 225, 109552.

Li, J., Zhang, Y., & Chen, L. (2023). *Efficiency and scalability in SDN architectures: empirical and simulation insights*. *Computer Networks*, 224, 109521.

Logicalis. (2023). Caso de éxito: Solución SD-WAN para clientes corporativos en Brasil. Recuperado de https://www.la.logicalis.com

Moriarty, K., & Kent, S. (2023). *Security Automation and Continuous Monitoring in SDN*. *Journal of Network Security*, 19(2), 77–98.

National Institute of Standards and Technology (NIST). (2020). *SP 800-207: Zero Trust Architecture*. U.S. Department of Commerce.

Next generation networks (NGN) and IMS in telecom. (2021). Telecom Resources. https://www.telecomresources.com/ngn-ims/

Nunes, B. A. A., Mendonça, M., Nguyen, X. N., Obraczka, K., & Turletti, T. (2014). A survey of software-defined networking: Past, present, and future of programmable networks. *IEEE Communications Surveys & Tutorials, 16*(3), 1617-1634. https://doi.org/10.1109/SURV.2014.012214.00180

Open Networking Foundation (ONF). (2022). *Best Practices for SDN Implementation and Operation*. Palo Alto, CA.

Open Networking Foundation (ONF). (2022). *Security Recommendations for SDN and OpenFlow Environments*. Palo Alto.

Ormachea Mejía, M. J., Almidón Ortiz, C. A., Vicente Ramos, W. E., & Pacheco Moscoso, L. E. (2022). Gestión del tráfico de red en la calidad de servicio “QoS” WAN en Tambopata-Perú 2021. *Revista de Ciencias Sociales*, 28(2), 300–318. https://dialnet.unirioja.es/servlet/articulo?codigo=8378018

Patel, M., Naughton, B., Chan, C., & Kong, W. (2022). *Cisco SD-WAN solution design guide*. Cisco Technical Documentation. https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/Cisco_SD-WAN/

Project Management Institute (PMI). (2021). *PMBOK Guide: A Guide to the Project Management Body of Knowledge* (7th ed.). PMI.

Ranjbar, H., Bahrami, M., & Khan, S. (2022). *AI-based intrusion detection in SDN controllers*. *IEEE Access*, 10, 99874–99889.

SCC en la Red. (2023). Casos prácticos de SD-WAN: experiencias exitosas. Recuperado de https://www.sccenlared.es

Serrano, F. (2015). *Redes definidas por software (SDN): OpenFlow* (Trabajo de fin de grado). Universidad Politécnica de Valencia. https://riunet.upv.es/bitstream/handle/10251/62801/SERRANO%20-%20Redes%20Definidas%20por%20Software%20%28SDN%29:%20OpenFlow.pdf?sequence=3

Software-defined networking and SD-WAN in next-gen networks. (2022). Networking Trends News. https://www.networkingtrendsnews.com/sdn-sd-wan/

Tafur, C., & Carrillo, D. (2023). *Ciberresiliencia y gestión de riesgos en infraestructuras críticas de telecomunicaciones*. *Revista Colombiana de Tecnologías Avanzadas*, 17(3), 45–63.

The role of SDN in NGN evolution. (2022). Telecom Insights. https://www.telecominsights.com/sdn-ngn-evolution/

TNG. (2023). Caso de éxito Vodafone: Implementación de SD-WAN en Colombia. Recuperado de https://www.itng.com.co

Universidad Central de Venezuela. (2022). Consideraciones de Diseño Para el Despliegue de Redes SDN en Campus Empresariales. Recuperado de https://saber.ucv.ve/bitstream/10872/20507/1/TesisGustavoPereira_SDN.pdf

Universidad Peruana de Ciencias Aplicadas. (2023). Diseño de un sistema de gestión de tráfico aplicando la tecnología SDN en la Red LAN de una cadena de Supermercados. Recuperado de https://repositorioacademico.upc.edu.pe/handle/10757/670181?show=full

Universidad Politécnica de Cataluña. (2021). Calidad de Servicio en Redes NGN. Recuperado de https://upcommons.upc.edu/bitstream/handle/2099.1/16049/CALIDAD_DE_SERVICIO_EN_REDES_NGN.pdf?sequence=4

Universidad Politécnica de Cataluña. (2022). Gestión y control de Calidad de Servicio de redes SDN en tiempo real. Recuperado de https://upcommons.upc.edu/bitstream/handle/2099.1/22178/Resum.pdf%3Bsequence%3D2

Viloria Ramírez, V. A. (2023). *Mejoramiento de la calidad de servicios (QoS) en aplicaciones de telediagnóstico basado en redes definidas por software (SDN): caso de estudio Clínica Monte Sinaí* [Trabajo de titulación, Universidad de Cuenca]. DSpace Universidad de Cuenca. https://dspace.ucuenca.edu.ec/handle/123456789/41443

Zhang, H., Jiang, C., & Ni, J. (2019). Challenges and opportunities in 5G SDN: A review. *IEEE Communications Surveys & Tutorials, 21*(1), 125-160. https://doi.org/10.1109/COMST.2018.2866661

Zhang, Y., Le Fèvre, J., & Robert, F. (2017). Traffic engineering for SDN: Measurement and data collection. *Springer Briefs in Computer Science*. https://doi.org/10.1007/978-3-319-59626-1

Apéndices

Apéndice A

Guia Entrevista

Guía de Entrevista Semiestructurada

Objetivo: Identificar los desafíos de seguridad y las soluciones necesarias para proteger las redes NGN basadas en SDN, garantizando su estabilidad y resiliencia ante amenazas.

Introducción:

Buenos días/tardes. Mi nombre es Edgar Javier Vargas Sosay actualmente me encuentro desarrollando una investigación cuyo objetivo es evaluar la implementación de soluciones de Redes Definidas por Software (SDN) en Redes de Próxima Generación (NGN), enfocándome en la optimización de la gestión del tráfico, la mejora de la eficiencia operativa y, específicamente en este caso, en los desafíos y soluciones de seguridad que se presentan en su implementación.

Esta entrevista tiene como fin recopilar información cualitativa basada en su experiencia profesional. La información que nos comparta será utilizada únicamente con fines académicos y se manejará de manera confidencial. ¿Está de acuerdo en participar? (esperar respuesta)

¿Autoriza que la entrevista sea grabada para facilitar su posterior análisis? (esperar respuesta)

Sección 1 – Perfil del entrevistado

1. Para comenzar, ¿podría contarme brevemente sobre su experiencia profesional en el área de telecomunicaciones y, en particular, en proyectos que involucren redes SDN o NGN?
2. ¿En qué tipo de organización se desempeña actualmente? (por ejemplo, operador de telecomunicaciones, proveedor de servicios, integrador, consultor, sector académico).

Sección 2 – Desafíos de seguridad

3. Desde su experiencia, ¿cuáles considera que son las principales vulnerabilidades o amenazas que enfrenta una red NGN basada en SDN?
4. En su opinión, ¿en qué parte de la arquitectura se concentran más riesgos: en el plano de control, en el plano de datos o en el plano de aplicación? ¿Por qué?
5. ¿Ha identificado riesgos específicos asociados al controlador SDN? Si es así, ¿cuáles son los más relevantes?

   Sección 3 – Soluciones y estrategias
6. En su experiencia, ¿qué medidas técnicas han resultado más efectivas para mitigar los riesgos de seguridad en redes SDN? (por ejemplo, cifrado, autenticación robusta, segmentación, monitoreo continuo).
7. ¿Qué buenas prácticas recomendaría para garantizar la estabilidad y resiliencia de este tipo de redes?
8. ¿Conoce o ha implementado protocolos, normativas o estándares específicos que fortalezcan la seguridad en SDN?

   Sección 4 – Lecciones aprendidas y tendencias
9. Según su experiencia, ¿cuáles son los errores más comunes que se deben evitar al implementar seguridad en redes SDN?
10. Mirando hacia el futuro, ¿cómo cree que evolucionarán los riesgos y las soluciones de seguridad en los próximos cinco años para redes NGN basadas en SDN?

    Cierre:

Agradezco mucho el tiempo y la información que me ha compartido. Sus aportes serán de gran utilidad para la investigación y para comprender mejor los retos y oportunidades que presentan las redes SDN en entornos NGN.

Apéndice B

Codificación Entrevistas

Matriz 1. Entrevista – David Osorio			
Fragmento clave ampliado	**Eje / Objetivo específico**	**Cita literal sugerida**	**Comentario analítico / interpretación ampliada**
El entrevistado enfatiza que la latencia disminuye notablemente con la adopción de redes definidas por software, ya que los controladores pueden analizar de forma continua la congestión y redistribuir el tráfico en tiempo real, evitando los cuellos de botella característicos de las redes tradicionales.	**Eje 1: Impacto en latencia y QoS**	"Con SDN los paquetes se enrutan por el canal de menor congestión, reduciendo la latencia y manteniendo la calidad del servicio estable incluso en momentos de alta demanda."	Este fragmento demuestra cómo SDN sustituye los protocolos estáticos por mecanismos dinámicos de gestión de tráfico, lo cual eleva la QoS al priorizar rutas eficientes. Reafirma el principio central de la arquitectura SDN: separar el plano de control del plano de datos para maximizar la flexibilidad operativa.
La centralización del control permite balancear enlaces de manera activa, sin desperdiciar recursos.	**Eje 1**	"Ya no tenemos enlaces en espera, todos trabajan de forma simultánea."	El balanceo activo-activo evidencia la eliminación de redundancias pasivas. Refleja una nueva lógica de eficiencia, en la que la disponibilidad no depende del sobredimensionamiento físico sino del manejo lógico inteligente.
Destaca la replicación de controladores y redundancia geográfica como mecanismo de seguridad y resiliencia.	**Eje 2: Desafíos y soluciones de seguridad**	"Los controladores deben estar replicados para garantizar resiliencia ante fallas o ataques."	Este planteamiento vincula la ciberseguridad con la continuidad operativa. Muestra una comprensión integral del riesgo sistémico, anticipando posibles vulnerabilidades en el plano de control.
Se promueve la documentación continua y la automatización de	**Eje 3: Buenas prácticas de implementación**	"Cada cambio queda registrado y versionado para evitar errores y	Esta práctica está alineada con las recomendaciones de ITIL y DevOps, integrando buenas prácticas en la gestión de

tareas para evitar errores humanos.		revertir fallos rápidamente.”	cambios dentro del entorno SDN.
Menciona que la virtualización reduce el consumo energético y la necesidad de equipos físicos.	**Eje 4: Impacto social y ambiental**	“Con la virtualización reducimos consumo energético y espacio físico en el centro de datos.”	Representa la transición hacia infraestructuras sostenibles, contribuyendo a objetivos de responsabilidad ambiental empresarial.

Matriz 2. entrevista – Eduard Rincón			
Fragmento clave ampliado	**Eje / Objetivo específico**	**Cita literal sugerida**	**Comentario analítico / interpretación ampliada**
El entrevistado señala que la red detecta congestión y ejecuta conmutación automática de tráfico sin intervención manual, garantizando estabilidad.	Eje 1: Impacto en latencia y QoS	“Si un enlace se satura, la red conmuta automáticamente al alterno, sin que el usuario perciba degradación.”	Esto valida empíricamente la capacidad adaptativa del modelo SDN, donde las políticas predefinidas en el controlador actúan como mecanismos de resiliencia automática.
Describe que se implementan certificados digitales, segmentación de red y autenticación de dispositivos, reduciendo riesgos.	Eje 2: Desafíos y soluciones de seguridad	“Solo los equipos autenticados con certificado pueden acceder al entorno de red.”	Este enfoque corresponde al paradigma Zero Trust, en el que la verificación continua sustituye la confianza implícita, fortaleciendo la seguridad a nivel perimetral y lógico.
Recomienda una implementación gradual mediante pilotos, permitiendo medir impacto antes de la adopción masiva.	Eje 3: Buenas prácticas de implementación	“Primero probamos en un entorno controlado antes de masificar la solución.”	Esta estrategia refleja una gestión del cambio responsable, asociada a metodologías ágiles y a la minimización del riesgo de interrupción en servicios críticos.
Destaca el impacto social al conectar comunidades rurales a través de SDN y enlaces móviles.	Eje 4: Impacto social y ambiental	“Podemos conectar comunidades remotas con enlaces 4G o satelitales gracias a la flexibilidad de SDN.”	La visión social de la tecnología se materializa en la reducción de brechas digitales, alineada con los Objetivos de

			Desarrollo Sostenible (ODS 9 y 10).

Matriz 3. entrevista – Enrique Aldana			
Fragmento clave ampliado	**Eje / Objetivo específico**	**Cita literal sugerida**	**Comentario analítico / interpretación ampliada**
Relata que la automatización minimiza errores humanos y acelera la respuesta ante fallos.	Eje 3: Buenas prácticas de implementación	"La automatización evita errores humanos y acelera procesos, mejorando la disponibilidad del servicio."	Este testimonio evidencia el principio de confiabilidad operativa que SDN introduce frente a la administración manual, confirmando la superioridad del modelo declarativo.
Subraya el monitoreo continuo de latencia y pérdidas de paquetes.	Eje 1: Impacto en latencia y QoS	"El controlador muestra métricas de latencia y jitter en tiempo real, facilitando decisiones inmediatas."	Este elemento empírico valida la capacidad de observabilidad y control granular, crucial para la gestión proactiva del rendimiento.
Menciona políticas de aislamiento ante ataques y mecanismos de respaldo.	Eje 2: Desafíos y soluciones de seguridad	"Contamos con políticas que aíslan segmentos ante una intrusión."	Esto revela el principio de segmentación dinámica como componente de ciberresiliencia.
Comenta que la centralización y virtualización reducen la huella física.	Eje 4: Impacto social y ambiental	"Antes cada sede tenía su router físico, ahora todo está centralizado."	La virtualización no solo optimiza recursos sino que reduce emisiones y residuos tecnológicos.

Matriz 4. entrevista – Jesús Barrios			
Fragmento clave ampliado	Eje / Objetivo específico	Cita literal sugerida	Comentario analítico / interpretación ampliada
Explica que con SDN se logra balanceo activo-activo, mejorando la eficiencia de los enlaces.	Eje 1: Impacto en latencia y QoS	"Con SDN se aprovechan los dos enlaces activos; ya no se paga por un enlace que está inactivo."	Este fragmento conecta la eficiencia técnica con la optimización de costos, evidenciando el impacto económico derivado del mejor uso del ancho de banda.
Destaca la inteligencia del sistema en redireccionar tráfico según latencia.	Eje 1	"La red detecta degradaciones y redirige el tráfico según la latencia más baja."	Esta cita representa la evolución hacia redes autorreguladas, basadas en políticas contextuales.

Identifica riesgos emergentes de computación cuántica y exposición por redes públicas.	Eje 2: Desafíos y soluciones de seguridad	"El reto está en cómo proteger la red ante las amenazas que traerá la computación cuántica."	Este aporte introduce una perspectiva prospectiva sobre seguridad, anticipando vulnerabilidades futuras.
Enumera las buenas prácticas: levantamiento detallado, automatización y pruebas de aceptación.	Eje 3: Buenas prácticas de implementación	"Una buena implementación depende de un levantamiento detallado y automatización."	Este enfoque muestra la madurez metodológica del entrevistado y se ajusta a los estándares PMP y ITIL.
Resalta la telemetría inteligente para ahorro energético.	Eje 4: Impacto social y ambiental	"Los puertos se apagan automáticamente en horarios sin uso para ahorrar energía."	Se evidencia un compromiso ambiental a través del uso eficiente de energía y reducción de huella de carbono.

Matriz 5. entrevista – Carlos Hernández			
Fragmento clave ampliado	**Eje / Objetivo específico**	**Cita literal sugerida**	**Comentario analítico / interpretación ampliada**
Asegura que SDN reduce caídas y tiempos de indisponibilidad, optimizando la calidad del servicio.	Eje 1: Impacto en latencia y QoS	"La automatización evita fallas repetitivas y mejora la disponibilidad de la red."	Corrobora la mejora tangible en la continuidad operativa, respaldando los hallazgos de estudios previos (IEEE, 2023).
Advierte el riesgo de vulneración del controlador como punto crítico de ataque.	Eje 2: Desafíos y soluciones de seguridad	"Si vulneran el controlador, comprometen toda la red."	Representa una debilidad estructural reconocida en la literatura técnica y resalta la necesidad de redundancia y autenticación reforzada.
Propone estandarizar y documentar procesos antes de la implementación.	Eje 3: Buenas prácticas de implementación	"Primero se documenta y luego se estandariza antes de aplicar cambios."	Refleja el principio de gobernanza tecnológica como base de sostenibilidad operativa.
Afirma que SDN disminuye consumo energético y costos de mantenimiento.	Eje 4: Impacto social y ambiental	"Con SDN usamos menos equipos físicos y consumimos menos energía."	Este argumento vincula la innovación tecnológica con el desarrollo sostenible empresarial.

Glosario

- API (Interfaz de Programación de Aplicaciones): Conjunto de protocolos y funciones que permite la comunicación entre aplicaciones o sistemas en el entorno SDN.
- Arquitectura SDN: Modelo de red que separa el plano de control del plano de datos que permite la gestión centralizada y programable.
- Automatización: Ejecución automática de los procesos de configuración y gestión de la red, logrado a través de la sencillez de los scripts y la complejidad de sistemas inteligentes.
- Brecha digital: Diferencias sociales y geográficas en el uso de las distintas tecnologías de la información y de conectividad.
- Calidad de Servicio (QoS): Mecanismos que permiten dar prioridad al tráfico de red para conseguir un rendimiento estable en servicios sensibles.
- Ciberresiliencia: Capacidad de una red para resistir ataques cibernéticos y, en caso de sufrir uno, continuar operando.
- Controlador SDN: El componente más importante de la infraestructura de la red SDN, el recurso que conecta el plano de control con el plano de datos, estandariza y se encarga de la edición y la operación de las políticas, y es el que centraliza las acciones que llevan a cabo los recursos del plano de datos.
- Eficiencia operativa: La capacidad de las redes para operar con un bajo consumo de recursos, un alto nivel de disponibilidad y un mínimo de intervención manual.
- Huella ambiental: El impacto ecológico derivado del consumo energético, de los residuos, de las emisiones generadas al uso de sistemas tecnológicos.
- Interoperabilidad: La capacidad de diferentes sistemas y equipos de fabricantes diferentes para funcionar de forma conjunta, basándose todos ellos en estándares abiertos.

- Latencia: El tiempo que tarda un paquete en viajar de un origen a un destino dentro de la red.
- NGN (Next Generation Networks): Redes de próxima generación basadas en IP que admiten servicios avanzados y arquitectura de tipo SDN.
- ONF (Open Networking Foundation): Organización que establece estándares y buenas prácticas para el diseño o la implementación de SDN.
- Plano de control: Componente que toma decisiones sobre las rutas a seguir, las reglas o las políticas de la red.
- Plano de datos: Capa responsable del reenvío físico de los paquetes, atendiendo a las reglas definidas por el plano de control.
- Redes definidas por software (SDN): Tecnología que permite una red de programación a través de software proporcionando flexibilidad y control centralizado.
- Resiliencia: Capacidad que tiene la red de funcionar pese a los fallos, ataques o sobrecargas.
- Seguridad perimetral: Conjuntos de controles que protegen ese acceso inicial a la red por autenticación o filtrado.
- Sostenibilidad energética: Proceso de optimizar el consumo a través de tecnologías de mayor eficiencia y mecanismos de ahorro.