PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR

FACULTAD DE INGENIERIA

ESCUELA DE SISTEMAS

TEMA:

ESTUDIO PARA LA IMPLEMENTACION DE REDES SD-WAN PARA EMPRESAS

CASO DE ESTUDIO CENTRIC S.A.

AUTOR:

BRYAN EDUARDO MORALES COLOMA

QUITO DM, 2024

TABLA DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

CAPÍTULO 1- INTRODUCCIÓN

En este capítulo, se establecerá los principios del estudio y se dejará definido el arranque del trabajo de titulación. Lo cual incluirá la justificación, planteamiento del problema, objetivos, antecedentes y el alcance del trabajo.

TEMA:

ESTUDIO PARA LA IMPLEMENTACIÓN DE REDES SD-WAN PARA EMPRESAS, CASO DE ESTUDIO CENTRIC S.A.

1.1. JUSTIFICACIÓN

En la era digital actual, las redes empresariales se enfrentan a una creciente demanda de mayor ancho de banda, fiabilidad y seguridad para satisfacer las necesidades de aplicaciones críticas y usuarios distribuidos. Ante este desafío, las redes definidas por software de área amplia (SD-WAN) han surgido como una solución prometedora para mejorar la eficiencia y el rendimiento de las redes empresariales.

La implementación de SD-WAN en una empresa representa un paso significativo hacia la modernización de la infraestructura de red, permitiendo una gestión más flexible, una optimización inteligente del tráfico y una mejora en la experiencia del usuario final. Sin embargo, este proceso no está exento de desafíos, que van desde la planificación y diseño adecuados hasta la integración con la infraestructura de red existente y la gestión del cambio organizacional. (Aharonov, 2024)

El propósito de este estudio es investigar el proceso de implementación de SD-WAN en una empresa, con el objetivo de comprender los desafíos enfrentados, las estrategias utilizadas y los resultados obtenidos. A través de un enfoque de estudio de caso, se examinará en detalle el proceso desde la planificación inicial hasta la validación de la solución implementada, analizando los beneficios tangibles e intangibles de la adopción

de SD-WAN en términos de optimización del tráfico, mejora de la seguridad y eficiencia operativa.

Este estudio no solo busca contribuir al cuerpo de conocimiento existente sobre SD-WAN en entornos empresariales, sino también proporcionar recomendaciones para empresas que consideran implementar esta tecnología en su infraestructura de red. Al comprender los desafíos y las mejores prácticas asociadas con la implementación de SD-WAN, las organizaciones pueden tomar decisiones informadas y maximizar el valor de esta tecnología emergente en su transformación digital.

1.2. PLANTEAMIENTO DEL PROBLEMA

En el entorno empresarial actual de Centric S.A., la creciente demanda de conectividad confiable y eficiente, junto con la proliferación de aplicaciones en la nube y la movilidad de los usuarios, ha puesto a prueba la capacidad de las redes empresariales tradicionales para proporcionar un rendimiento óptimo. Las redes de área amplia (WAN) convencionales, basadas en tecnologías heredadas como el enrutamiento estático y los circuitos dedicados, a menudo resultan inflexibles, costosas de mantener y limitadas en su capacidad para adaptarse a las necesidades cambiantes del negocio.

En este contexto, las redes definidas por software de área amplia (SD-WAN) han surgido como una solución prometedora para abordar los desafíos de conectividad y rendimiento en entornos empresariales distribuidos. Sin embargo, la implementación exitosa de SD-WAN en una empresa plantea una serie de desafíos y preguntas que requieren una atención cuidadosa.

Uno de los principales desafíos radica en el proceso de migración de una infraestructura de red existente a una arquitectura SD-WAN, que implica la integración de múltiples tipos de conexiones de red, la reconfiguración de políticas de enrutamiento y seguridad, y la gestión del cambio organizacional. Además, la selección de proveedores de SD-WAN

y la evaluación de las opciones de implementación pueden resultar abrumadoras para las empresas que buscan adoptar esta tecnología.

La medición y cuantificación de los beneficios obtenidos de la implementación de SD-WAN, tanto en términos de mejora del rendimiento de la red como de eficiencia operativa, plantea una serie de desafíos. Por lo tanto, surge la necesidad de investigar en profundidad el proceso de implementación de SD-WAN en una agencia de prueba para identificar los desafíos específicos asociados con esta iniciativa y explorar las estrategias efectivas para superarlos.

1.3. OBJETIVOS DE LA INVESTIGACIÓN

1.3.1. Objetivo General

Proponer un Plan de Despliegue utilizando los protocolos de comunicación de SD-WAN para mejorar la infraestructura de red de la empresa y que proporcione una conectividad más eficiente, segura y adaptable para una futura implementación.

1.3.2. Objetivos Específicos

1. Analizar el estado actual de la infraestructura de red de la agencia de la empresa antes de realizar la propuesta de implementación de SD-WAN, identificando sus limitaciones y áreas de mejora.
2. Evaluar diferentes proveedores y soluciones de SD-WAN disponibles en el mercado, considerando sus características, capacidades y compatibilidad con los objetivos empresariales.
3. Diseñar la arquitectura para la integración a futuro con los servicios actuales de la empresa usando la nueva tecnología SD-WAN.

4. Desarrollar un plan detallado de despliegue que establezca los fundamentos necesarios para una futura implementación de SD-WAN en todas las agencias de la empresa.

1.4. ANTECEDENTES

La empresa Centric S.A. se encarga principalmente de la administración BackOffice de empresas del Grupo Baca, en el área de Sistemas específicamente en Infraestructura se tienen las agencias del grupo con una distribución de red de datos e internet la cual funciona como conexión al data center y brinda todos los servicios a las agencias, adicional se presenta un internet SB (Small Business) contratado para cada una de las agencias y brindar el internet de clientes, el cual está separado del mencionado anteriormente y cuenta con una velocidad de aproximadamente 20 Mbps. Esta distribución centralizada dificulta el trabajo de los colaboradores cuando se presenta una caída del servicio del proveedor de datos e internet contratado para tener conexión al data center de Centric y servicio de internet en la agencia, los colaboradores se ven obligados a conectarse al SB (Small Business) que tienen contratado para los clientes y de esta manera poder seguir trabajando conectados a internet, sin embargo este internet al ser de visitas no cuenta con la suficiente velocidad y capacidad para conectar tantos usuarios a la vez, por este motivo se presentan problemas tanto de velocidad de conexión como perdidas de los servicios que están conectados al data center los cuales necesitan esta interconexión para estar operativos. Servicios como caja o aplicativos de gestión empresarial conocidos en Centric como SCB y S3S se ven afectados por la pérdida del proveedor de datos e internet y la conexión hacia el data center, lo que ocasiona en todos los casos una pérdida de ingreso en las empresas del grupo durante todo el tiempo en el que el proveedor demora en resolver la caída del enlace principal.

Es por estos antecedentes que se identificó una manera para poder mantener la conexión con el data center mediante un túnel autogestionado de conexión balanceando el tráfico de internet para los servicios corporativos en caso de que el proveedor de datos e internet llegara a tener problemas con el servicio.

1.5. ALCANCE

Se evaluará la viabilidad, beneficios y desafíos de implementar una solución SD-WAN en una agencia del grupo de empresas para las que trabaja Centric S.A. Se analizarán las limitaciones de las redes WAN tradicionales en el entorno empresarial y se identificarán los requisitos técnicos y de negocio necesarios para una implementación exitosa de SD-WAN. Se investigarán y compararán diferentes proveedores y soluciones SD-WAN, evaluando sus características, funcionalidad y costos.

Con base en estos análisis, se diseñará una arquitectura de red SD-WAN específica para la agencia seleccionada, considerando topología, políticas de enrutamiento, QoS y seguridad. Finalmente, se desarrollará un plan de despliegue detallado, que incluirá fases de implementación, gestión del cambio y estrategias de mitigación de riesgos. Los resultados esperados incluyen una mejor comprensión de los desafíos de las redes WAN tradicionales, identificación de los beneficios de SD-WAN y recomendaciones prácticas para su implementación en empresas.

CAPÍTULO 2- MARCO TEÓRICO

Este capítulo se enfoca en definir los conceptos fundamentales, explorar las limitaciones de las WAN tradicionales, y destacar las ventajas y componentes principales de las SD-WAN. Se examinarán los fundamentos tecnológicos que sustentan la virtualización de redes, el enrutamiento inteligente, la gestión de la calidad de servicio (QoS) y las características avanzadas de seguridad que SD-WAN ofrece para proporcionar una comprensión integral de cómo SD-WAN puede transformar la infraestructura de red empresarial, mejorando la eficiencia, flexibilidad, y seguridad en comparación con las soluciones WAN tradicionales.

2.1. INTRODUCCIÓN A LAS REDES WAN

En este apartado revisaremos la definición y características principales de las Redes de Área Amplia (WAN). Abordaremos su cobertura geográfica extensa, la interconexión de redes locales, el uso de diversos medios de comunicación, enrutamiento y conmutación, y los protocolos de comunicación utilizados. También destacaremos la importancia de las WAN en el entorno empresarial.

2.1.1. Definición y Tipos

Una Red de Área Amplia (WAN, por sus siglas en inglés, Wide Area Network) es un sistema de comunicación de datos que conecta dispositivos y redes de computadoras ubicadas en diferentes lugares geográficos, a menudo separados por grandes distancias (Roch, 2024). A diferencia de las redes de área local (LAN) que cubren un área limitada como una oficina o un edificio, las WAN abarcan regiones más amplias, incluyendo ciudades, países o incluso continentes (TecnoDigital, 2023).

Existen diversas opciones para establecer conexiones de red de área amplia (WAN) que se adaptan a diferentes necesidades y entornos. A continuación, se describen algunos de los tipos más comunes de conexiones WAN:

- Conexiones Punto a Punto: Estas conexiones establecen un enlace directo entre dos ubicaciones utilizando circuitos dedicados, como líneas T1/E1 o conexiones de fibra óptica. Son ideales para enlaces de alta velocidad y baja latencia entre ubicaciones principales.
- Redes Privadas Virtuales (VPN): Utilizando la infraestructura de red pública (como Internet), las VPNs crean una red segura entre sitios remotos a través de túneles encriptados. Son una opción económica y flexible, aunque la calidad del servicio puede depender de la conexión de Internet subyacente.
- Redes MPLS (Multiprotocol Label Switching): Estas redes proporcionan conectividad confiable y segura mediante la creación de circuitos virtuales en una red de proveedor de servicios. MPLS asegura calidad de servicio (QoS) y puede priorizar el tráfico según las necesidades del negocio.
- Redes Celulares: Utilizan tecnologías móviles como 4G LTE o 5G para ofrecer conectividad WAN a ubicaciones remotas donde las opciones de cableado son limitadas o costosas. (Roch, 2024)

2.1.2. Características Principales de las WAN

1. Cobertura Geográfica Extensa: Las WAN están diseñadas para cubrir grandes áreas geográficas, permitiendo la conexión de múltiples ubicaciones de una organización, independientemente de la distancia entre ellas(Roch, 2024).
2. Interconexión de Redes Locales: Una WAN conecta múltiples LANs (Redes de Área Local), facilitando la comunicación y el intercambio de datos entre diferentes oficinas o sucursales.

3. Uso de Medios de Comunicación Diversos: Las WAN pueden utilizar una variedad de medios de comunicación para transmitir datos, incluyendo líneas telefónicas, enlaces de satélite, cables de fibra óptica, conexiones inalámbricas y circuitos dedicados.
4. Enrutamiento y Conmutación: Las WAN utilizan dispositivos de red como routers y switches para encaminar el tráfico de datos a través de la red, asegurando que la información llegue a su destino de manera eficiente y segura.
5. Protocolos de Comunicación: Las WAN emplean diversos protocolos de comunicación para garantizar la correcta transferencia de datos. Algunos de los protocolos más comunes incluyen TCP/IP, MPLS (Multiprotocol Label Switching), y Frame Relay (Ellor, 2023).

2.1.3. Importancia de las WAN en el Entorno Empresarial

1. Conectividad Global: Las WAN permiten a las empresas conectar sus operaciones a nivel global, facilitando la comunicación y la colaboración entre empleados, socios y clientes ubicados en diferentes partes del mundo.
2. Acceso a Recursos Centralizados: Las WAN permiten a los empleados acceder a recursos centralizados, como servidores, bases de datos y aplicaciones empresariales, desde cualquier ubicación. Esto es crucial para empresas con múltiples sucursales o que operan de manera distribuida.
3. Mejora de la Productividad: Al proporcionar una conectividad rápida y confiable, las WAN mejoran la productividad de los empleados al permitir un acceso continuo a las herramientas y datos necesarios para su trabajo, sin importar su ubicación física.
4. Soporte para Aplicaciones Críticas: Las WAN soportan aplicaciones críticas para el negocio, como sistemas ERP (Enterprise Resource Planning), CRM (Customer

Relationship Management) y otros sistemas de gestión empresarial que requieren una conectividad robusta y confiable.

5. Facilitación del Comercio Electrónico: Para empresas que dependen del comercio electrónico, las WAN son esenciales para garantizar que los sistemas de ventas, inventario y atención al cliente funcionen de manera integrada y eficiente, permitiendo transacciones en tiempo real.
6. Reducción de Costos: Al centralizar recursos y optimizar la comunicación entre diferentes ubicaciones, las WAN pueden ayudar a reducir costos operativos asociados con la infraestructura de TI, las telecomunicaciones y los viajes de negocios (Edraw, 2024).

2.2. PROBLEMAS Y LIMITACIONES DE LAS WAN TRADICIONALES

A continuación, revisaremos los problemas y limitaciones de las WAN tradicionales. Trataremos los altos costos de instalación y operación teóricamente, la escalabilidad limitada, la rigidez en la configuración y la dependencia de proveedores. Revisaremos también los problemas de rendimiento, y abordaremos las preocupaciones de seguridad, de estas redes.

2.2.1. Costos

Altos Costos de Instalación: La configuración inicial de una WAN tradicional a menudo requiere una inversión significativa en infraestructura, incluyendo la adquisición de routers, switches, líneas arrendadas y otros equipos de red. Los enlaces dedicados como MPLS (Multiprotocol Label Switching) son costosos debido a la necesidad de infraestructura física específica y acuerdos de servicio con proveedores de telecomunicaciones.

Costos Recurrentes Elevados: Las WAN tradicionales suelen tener altos costos operativos recurrentes, incluidos los costos de mantenimiento de la infraestructura, tarifas de

servicios de telecomunicaciones y cargos por ancho de banda. Las actualizaciones de hardware y software necesarias para mantener la red operativa y segura representan una inversión continua.

Costos de Personal: La gestión y el mantenimiento de una WAN tradicional requieren personal altamente capacitado, lo que incrementa los costos de nómina. La complejidad de las redes WAN tradicionales a menudo demanda la contratación de consultores externos o servicios de gestión especializados(Bustos, 2023).

2.2.2. Flexibilidad

Escalabilidad Limitada: Ampliar una WAN tradicional para incluir nuevas ubicaciones puede ser un proceso lento y costoso, ya que implica la adquisición de nuevos enlaces dedicados y la configuración de equipos adicionales. La infraestructura física necesaria para soportar una WAN tradicional no se adapta fácilmente a cambios rápidos en la demanda de ancho de banda.

Rigidez en la Configuración: Las WAN tradicionales tienen configuraciones estáticas que dificultan la rápida reconfiguración de la red para adaptarse a nuevas necesidades empresariales o cambios en el tráfico de red. La reconfiguración y adaptación a nuevas topologías de red a menudo requieren intervenciones manuales y tiempo de inactividad.

Dependencia de Proveedores: Las organizaciones a menudo están atadas a contratos a largo plazo con proveedores de telecomunicaciones, lo que limita la capacidad de cambiar de proveedor o ajustar los servicios contratados sin incurrir en penalizaciones (Campos Jiménez & Santana Pastrano, 2008).

2.2.3. Rendimiento

Latencia y Retardos: Las WAN tradicionales pueden experimentar alta latencia debido a la distancia física entre ubicaciones y la dependencia de múltiples saltos a través de la

infraestructura de red. Las aplicaciones críticas y sensibles al tiempo, como VoIP y videoconferencias, pueden verse afectadas negativamente por la latencia y los retardos en la transmisión de datos.

Pérdida de Paquetes y Jitter: Los enlaces de red sobrecargados o mal gestionados pueden resultar en pérdida de paquetes y jitter, afectando la calidad del servicio y el rendimiento de las aplicaciones. Las WAN tradicionales pueden tener dificultades para manejar tráfico de datos en picos de demanda, resultando en una degradación del rendimiento.

Ancho de Banda Limitado: La capacidad de ancho de banda en las WAN tradicionales puede ser insuficiente para soportar aplicaciones modernas y servicios basados en la nube, lo que provoca congestión y ralentización del tráfico de red. La gestión ineficiente del ancho de banda puede llevar a una asignación inadecuada de recursos de red, afectando el rendimiento de aplicaciones críticas(Bustos, 2023).

2.2.4. Seguridad

Exposición a Amenazas: Las WAN tradicionales a menudo están expuestas a una amplia gama de amenazas de seguridad, incluyendo ataques DDoS, interceptación de datos y malware. Las infraestructuras WAN que dependen de enlaces públicos o menos seguros son particularmente vulnerables a la interceptación y ataques.

Gestión de Políticas de Seguridad: La gestión de políticas de seguridad en una WAN tradicional puede ser compleja y propensa a errores, especialmente en redes grandes y distribuidas. La implementación y actualización de políticas de seguridad de manera consistente en todas las ubicaciones puede ser un desafío significativo.

Protección de Datos: Garantizar la privacidad y protección de los datos en tránsito a través de la WAN requiere medidas avanzadas de cifrado y autenticación, que pueden ser complicadas de implementar y mantener. La falta de mecanismos de seguridad integrados

en algunos componentes de la infraestructura WAN tradicional puede dejar lagunas de seguridad explotables.

Respuesta a Incidentes: La capacidad de detectar y responder rápidamente a incidentes de seguridad en una WAN tradicional puede estar limitada por la falta de visibilidad centralizada y herramientas de monitorización avanzadas. La dispersión geográfica de las redes WAN tradicionales complica la coordinación de respuestas y la implementación de medidas de mitigación en tiempo real (Agudelo, 2004).

2.3. INTRODUCCIÓN A SD-WAN

A continuación, abordaremos la definición y conceptos básicos de SD-WAN, sus principios fundamentales como la virtualización de la red, control centralizado, enrutamiento dinámico y seguridad integrada. También describiremos los componentes esenciales de SD-WAN, incluyendo el controlador, dispositivos de borde y enlaces de transporte. Finalmente, destacaremos las ventajas de SD-WAN, como la reducción de costos, mejora del rendimiento, aumento de la flexibilidad y escalabilidad, mayor seguridad y simplificación de la gestión de la red.

2.3.1. Definición y Conceptos Básicos de SD-WAN

SD-WAN (Software-Defined Wide Area Network) es una tecnología de red que utiliza principios de virtualización de redes para optimizar y gestionar de manera eficiente la conectividad WAN entre diferentes ubicaciones geográficas. A diferencia de las WAN tradicionales, SD-WAN permite la administración centralizada y automatizada de la infraestructura de red mediante software, proporcionando una mayor flexibilidad, eficiencia y control (*¿Qué Es SD-WAN?*, 2021).

2.3.2. Principios Fundamentales de SD-WAN

Virtualización de la Red: SD-WAN virtualiza la infraestructura de red, permitiendo que múltiples tipos de conexiones (como MPLS, Internet de banda ancha y LTE) se integren y gestionen como una sola red lógica.

Control Centralizado: La gestión de la red se realiza desde un controlador centralizado que aplica políticas de red, monitorea el rendimiento y ajusta dinámicamente las rutas de tráfico según las necesidades de la red.

Optimización del Enrutamiento: SD-WAN utiliza algoritmos de enrutamiento dinámico para seleccionar las rutas óptimas para el tráfico de datos, mejorando la eficiencia y el rendimiento de la red.

Seguridad Integrada: Las soluciones SD-WAN incluyen funciones de seguridad avanzadas, como cifrado de datos, firewalls y políticas de acceso, para proteger el tráfico de red y los datos sensibles (Tekpyme, 2023).

2.3.3. Componentes de SD-WAN

Controlador SD-WAN: Actúa como el cerebro del sistema SD-WAN, gestionando y orquestando todas las operaciones de la red desde una ubicación centralizada. Es responsable de aplicar políticas de red, gestionar la configuración de los dispositivos de borde, monitorear el rendimiento de la red y ajustar dinámicamente las rutas de tráfico.

Dispositivos de Borde (Edge Devices): Se sitúan en los extremos de la red, en cada ubicación de la organización, y se encargan de enrutar el tráfico según las políticas establecidas por el controlador. Pueden ser hardware dedicado o soluciones virtuales, y son responsables de la conectividad local, el enrutamiento del tráfico, y la aplicación de políticas de seguridad.

Enlaces de Transporte: Proveen la conectividad física entre las distintas ubicaciones. Los enlaces pueden incluir conexiones MPLS, Internet de banda ancha, LTE y otras opciones de transporte de datos. La capacidad de SD-WAN para usar múltiples tipos de enlaces simultáneamente permite una mayor flexibilidad y optimización del tráfico (NeuroThinking, 2024).

2.3.4. Ventajas de SD-WAN

Reducción de Costos:

- Uso de Conexiones Económicas: SD-WAN permite la utilización de conexiones de Internet de bajo costo en lugar de depender exclusivamente de enlaces MPLS caros, reduciendo significativamente los costos operativos.
- Optimización de Ancho de Banda: La capacidad para enrutar el tráfico de manera eficiente utilizando múltiples enlaces reduce la necesidad de ancho de banda excesivo, optimizando los costos de telecomunicaciones.(Telefónica, 2023)

Mejora del Rendimiento:

- Enrutamiento Inteligente: Los algoritmos de enrutamiento dinámico seleccionan las mejores rutas para el tráfico de datos, mejorando la latencia, el jitter y la pérdida de paquetes.
- Calidad de Servicio (QoS): SD-WAN prioriza el tráfico crítico de aplicaciones, asegurando que las aplicaciones esenciales para el negocio funcionen de manera óptima. (Ikusi, 2024)

Aumento de la Flexibilidad y Escalabilidad:

- Implementación Rápida: La virtualización de la red y la gestión centralizada permiten la rápida implementación de nuevas ubicaciones y la reconfiguración de la red según las necesidades del negocio.

- Escalabilidad Simplificada: Las organizaciones pueden escalar su red de manera eficiente añadiendo nuevos dispositivos de borde y enlaces de transporte sin una reconfiguración compleja. (Tekpyme, 2023)

Mejor Seguridad:

- Seguridad Integrada: SD-WAN incluye características de seguridad avanzadas como cifrado de extremo a extremo, firewalls y políticas de acceso que protegen el tráfico de red contra amenazas.
- Gestión Centralizada de Políticas: La aplicación de políticas de seguridad desde un punto centralizado garantiza una protección coherente y robusta en todas las ubicaciones. (Check Point, 2023)

Simplificación de la Gestión de la Red:

- Monitorización y Gestión Centralizadas: Todas las operaciones de la red se pueden supervisar y gestionar desde un único panel de control, simplificando la administración y reduciendo la necesidad de intervención manual.
- Automatización de Procesos: La automatización de tareas como el enrutamiento del tráfico y la aplicación de políticas reduce la carga operativa del equipo de TI y minimiza los errores humanos. (Check Point, 2023)

2.4. FUNDAMENTOS TECNOLÓGICOS DE SD-WAN

En este apartado, exploraremos los fundamentos tecnológicos de SD-WAN, incluyendo la virtualización de la red que permite la gestión centralizada y adaptable mediante una red overlay, la separación de planos de control y datos para mejorar la eficiencia y resiliencia, el enrutamiento inteligente que optimiza las rutas de tráfico en tiempo real, la Calidad de Servicio (QoS) que prioriza el tráfico crítico para asegurar un rendimiento consistente, y las medidas de seguridad integradas como el cifrado, la segmentación de la

red, funciones de firewall, y autenticación y control de acceso para proteger el tráfico y los datos sensibles.

2.4.1. Virtualización de la Red

La virtualización de la red en SD-WAN implica la abstracción de los recursos físicos de la red para crear una capa de red lógica que puede ser gestionada de manera centralizada. Esto se logra mediante la utilización de software para gestionar y orquestar el tráfico de red a través de múltiples enlaces de transporte, como pueden ser MPLS, Internet de banda ancha, y LTE. (Fortinet, 2023b)

Componentes Clave:

- Overlay Network: La red superpuesta (overlay) es una capa lógica que se establece sobre la infraestructura de red física (underlay). Los dispositivos de borde SD-WAN crean túneles seguros a través de los enlaces físicos para formar la red overlay.
- Orquestación Centralizada: Un controlador centralizado gestiona la configuración, supervisión y políticas de red a través de la red overlay, lo que permite una gestión más eficiente y adaptable.

Beneficios:

- Flexibilidad: Permite utilizar cualquier tipo de conexión de red disponible, optimizando el uso de los recursos y facilitando la adaptación a cambios en la demanda de tráfico.
- Agilidad: Facilita la rápida implementación y reconfiguración de la red sin necesidad de realizar cambios físicos en la infraestructura. (IBM, 2023)

2.4.2. Separación de Planos

En SD-WAN, se realiza una separación clara entre el plano de control y el plano de datos, lo que mejora la eficiencia y la capacidad de gestión de la red. El plano de control gestiona las políticas de enrutamiento y las decisiones de administración de la red, generalmente centralizado en el controlador SD-WAN, que puede estar en la nube o en un centro de datos de la organización. Sus responsabilidades incluyen la configuración de rutas, la aplicación de políticas de QoS y seguridad, la supervisión de la red y la toma de decisiones de enrutamiento dinámico. El plano de datos, encargado de la transmisión real de datos a través de la red, está distribuido entre los dispositivos de borde SD-WAN en cada ubicación. Este plano se encarga de encaminar el tráfico de datos según las políticas establecidas por el plano de control, manejar la encapsulación y el cifrado de los paquetes de datos. Los beneficios de esta separación incluyen una gestión más eficiente y escalable de la red, con decisiones de enrutamiento y políticas centralizadas que se aplican dinámicamente, así como una mejora en la resiliencia de la red al permitir que los dispositivos de borde operen de manera autónoma en caso de pérdida de conexión con el controlador. (Cloudflare, 2023)

2.4.3. Enrutamiento Inteligente

SD-WAN utiliza algoritmos avanzados de enrutamiento dinámico para seleccionar las rutas óptimas para el tráfico de red en tiempo real. Esto incluye la monitorización continua de las condiciones de la red y la adaptación del enrutamiento para maximizar el rendimiento y la eficiencia.

Características:

- Monitorización en Tiempo Real: Los dispositivos SD-WAN monitorean constantemente parámetros como latencia, pérdida de paquetes y jitter en cada enlace disponible.
- Selección de Ruta Dinámica: Basado en las métricas de rendimiento, el plano de control ajusta dinámicamente las rutas de tráfico para evitar congestión y garantizar la calidad del servicio.
- Políticas de Enrutamiento: Las políticas pueden definir prioridades para diferentes tipos de tráfico (por ejemplo, priorizar VoIP sobre tráfico de correo electrónico) y seleccionar rutas en consecuencia.

Beneficios:

- Optimización del Rendimiento: Mejora la experiencia del usuario final al optimizar las rutas para aplicaciones críticas y sensibles al rendimiento.
- Resiliencia y Redundancia: Proporciona rutas alternativas en caso de fallos de enlace, garantizando la continuidad del servicio. (Flores, 2023)

2.4.4. Calidad de Servicio (QoS)

La Calidad de Servicio (QoS) en SD-WAN es una función clave que permite priorizar el tráfico de red para asegurar que las aplicaciones críticas y sensibles al rendimiento reciban los recursos necesarios.

Componentes de QoS:

- Clasificación del Tráfico: El tráfico se clasifica en diferentes categorías basadas en la importancia y los requisitos de rendimiento de las aplicaciones.
- Priorización del Tráfico: Las políticas de QoS definen qué tráfico debe recibir mayor prioridad y recursos de red. Por ejemplo, el tráfico de VoIP y videoconferencia puede recibir mayor prioridad sobre el tráfico de correo electrónico.

- Gestión de Ancho de Banda: La asignación de ancho de banda se gestiona dinámicamente para garantizar que las aplicaciones críticas tengan suficiente capacidad, incluso durante picos de demanda.

Beneficios:

- Rendimiento Consistente: Garantiza una experiencia de usuario consistente y de alta calidad para aplicaciones críticas.
- Utilización Eficiente del Ancho de Banda: Optimiza el uso del ancho de banda disponible, evitando congestión y asegurando el mejor rendimiento posible para todas las aplicaciones. (Fortinet, 2023).

2.4.5. Seguridad Integrada

SD-WAN incorpora una serie de características de seguridad avanzadas que protegen el tráfico de red y los datos sensibles.

Cifrado:

- Función: Todos los datos transmitidos a través de la red SD-WAN están cifrados, típicamente utilizando estándares como IPsec o SSL, para protegerlos contra interceptaciones y accesos no autorizados.
- Beneficio: Garantiza la confidencialidad e integridad de los datos en tránsito.

Segmentación de la Red:

- Función: Permite la creación de segmentos de red lógicos separados (microsegmentación) para aislar el tráfico de diferentes aplicaciones, departamentos o usuarios.
- Beneficio: Mejora la seguridad al limitar la propagación de amenazas y facilitar la aplicación de políticas específicas para cada segmento.

Funciones de Firewall:

- Función: SD-WAN integra firewalls avanzados que inspeccionan y filtran el tráfico basado en políticas predefinidas, detectando y bloqueando amenazas.
- Beneficio: Proporciona una capa adicional de protección contra ataques, intrusiones y tráfico malicioso.

Autenticación y Control de Acceso:

- Función: Implementa mecanismos de autenticación fuerte para verificar la identidad de los dispositivos y usuarios antes de permitir el acceso a la red.
- Beneficio: Previene el acceso no autorizado y garantiza que solo usuarios y dispositivos legítimos puedan acceder a los recursos de red. (*¿Qué Es SD-WAN?*, 2021)

2.5. ESTRATEGIAS DE IMPLEMENTACIÓN DE SD-WAN

A continuación, cubriremos las estrategias de implementación de SD-WAN, comenzando con la evaluación de requisitos donde se analiza el tráfico de red actual y se documentan los problemas existentes, seguido de la selección de proveedores y soluciones basadas en rendimiento, seguridad, facilidad de gestión y costo total de propiedad. Luego se revisará la manera de diseñar la arquitectura SD-WAN incluyendo la topología de red, políticas de enrutamiento y QoS, y la integración de medidas de seguridad. Posteriormente, se revisará como realizar pruebas piloto para validar la funcionalidad y el rendimiento antes del despliegue completo, y como planificar la integración con la infraestructura existente, asegurando compatibilidad e interoperabilidad. Finalmente, veremos cómo realizar un despliegue gradual en fases, monitoreando continuamente el rendimiento y la seguridad, manteniendo comunicación con todas las partes interesadas y desarrollando un plan de contingencia.

2.5.1. Evaluación de Requisitos

- Análisis de tráfico: realizar un análisis exhaustivo del tráfico de red actual para identificar patrones de uso, aplicaciones críticas, y requerimientos de ancho de banda. Identificar los tipos de tráfico (por ejemplo, voz, video, datos) y su importancia relativa para la operación del negocio.(Fortinet, 2024b).
- Identificación de Problemas: Documentar las limitaciones y problemas actuales de la red WAN tradicional, como la latencia, pérdida de paquetes, costos elevados y problemas de escalabilidad. Entender los desafíos de seguridad y rendimiento que enfrentan las ubicaciones remotas.(Tecnozero, 2024)
- Requisitos de Negocio: Establecer objetivos claros alineados con las metas estratégicas del negocio, como mejorar la agilidad, reducir costos, mejorar la seguridad y aumentar el rendimiento de las aplicaciones. Considerar los requisitos de cumplimiento normativo y las políticas de seguridad empresarial.
- Evaluación de la Infraestructura Actual: Revisar la infraestructura de red existente para determinar qué componentes pueden integrarse con la solución SD-WAN y cuáles necesitan ser reemplazados o actualizados. Evaluar la capacidad de los enlaces de transporte actuales y considerar la necesidad de nuevos enlaces.(Fortinet, 2024b)

2.5.2. Selección de Proveedores y Soluciones

- Rendimiento y Escalabilidad: Evaluar el rendimiento de las soluciones en términos de latencia, pérdida de paquetes y capacidad de ancho de banda. Considerar la capacidad de la solución para escalar según el crecimiento del negocio.

- Funciones de Seguridad: Verificar las características de seguridad integradas, como cifrado, firewalls, segmentación y autenticación. Asegurarse de que la solución cumpla con los estándares de seguridad y regulaciones de la industria.
- Facilidad de Gestión: Evaluar la interfaz de gestión centralizada y su facilidad de uso. Considerar la capacidad de automatización y las herramientas de monitoreo y análisis(Check Point, 2024)
- Soporte y Servicios: Revisar el nivel de soporte técnico y los servicios adicionales ofrecidos por el proveedor, como asistencia en la implementación, capacitación y soporte postventa. Analizar las opciones de SLA (Acuerdos de Nivel de Servicio) ofrecidas.
- Costo Total de Propiedad (TCO): Considerar todos los costos asociados, incluyendo la implementación, licencias, mantenimiento y costos operativos recurrentes. (Fortinet, 2024b) Comparar el TCO de diferentes proveedores y soluciones.

2.5.3. Diseño de la Arquitectura SD-WAN

- Topología de la Red: Decidir sobre la topología más adecuada (hub-and-spoke, full mesh, etc.) según las necesidades de conectividad de las ubicaciones. Planificar la redundancia y las rutas de respaldo para asegurar la alta disponibilidad.
- Distribución de Dispositivos de Borde: Seleccionar los dispositivos de borde SD-WAN apropiados para cada ubicación según el tamaño, la carga de trabajo y los requisitos de conectividad.
- Políticas de Enrutamiento y QoS: Definir políticas de enrutamiento que prioricen el tráfico crítico y optimicen el uso del ancho de banda. Establecer políticas de

QoS para asegurar que las aplicaciones más importantes tengan los recursos necesarios.

- Integración de Seguridad: Incorporar medidas de seguridad integradas en el diseño de la red, como segmentación, cifrado de datos en tránsito y firewalls.
- Compatibilidad e Integración: Asegurar la compatibilidad con la infraestructura de red existente y planificar la integración con otros sistemas y herramientas de gestión de red. (Fortinet, 2024b) (Check Point, 2024).

2.5.4. Pruebas Piloto

- Objetivos de la Prueba Piloto: Validar la funcionalidad y el rendimiento de la solución SD-WAN en un entorno controlado antes del despliegue completo. Identificar posibles problemas y ajustes necesarios en el diseño y la configuración.
- Selección del Sitio Piloto: Elegir una o varias ubicaciones representativas para la prueba piloto, que tengan una mezcla adecuada de tráfico y aplicaciones críticas.
- Configuración y Ejecución: Implementar la solución SD-WAN en el sitio piloto siguiendo las mejores prácticas de configuración. Monitorear el rendimiento, la seguridad y la gestión de la red durante un periodo de tiempo definido.
- Evaluación y Ajustes: Recoger datos y feedback del sitio piloto para evaluar el rendimiento y la funcionalidad. Realizar los ajustes necesarios en las políticas, la configuración y el diseño de la red.
- Documentación de Resultados: Documentar los resultados de la prueba piloto y desarrollar un plan de despliegue basado en las lecciones aprendidas. (Fortinet, 2024b) (Check Point, 2024)

2.5.6. Integración con Infraestructura Existente

- Evaluación de Compatibilidad: Evaluar la compatibilidad de la solución SD-WAN con la infraestructura de red existente, incluyendo routers, switches y firewalls. (Check Point, 2024)
- Planificación de la Migración: Desarrollar un plan detallado de migración que minimice el impacto en las operaciones diarias. Considerar una estrategia de migración gradual, integrando SD-WAN con segmentos específicos de la red en fases.
- Interoperabilidad: Asegurar que la solución SD-WAN pueda interoperar con las soluciones de red y seguridad actuales. Implementar mecanismos de interoperabilidad, como túneles IPsec, para conectar SD-WAN con la red MPLS existente.
- Formación y Capacitación: Proveer capacitación al personal de TI para garantizar que comprendan la nueva arquitectura SD-WAN y cómo gestionarla.
- Pruebas de Integración: Realizar pruebas exhaustivas para asegurarse de que la integración no afecta negativamente el rendimiento y la seguridad de la red.

2.5.5. Despliegue Gradual

- Despliegue por Fases: Implementar SD-WAN en fases, comenzando con las ubicaciones menos críticas para minimizar el riesgo. Evaluar el rendimiento y ajustar la configuración en cada fase antes de continuar con el despliegue.
- Monitoreo Continuo: Monitorear continuamente el rendimiento y la seguridad de la red durante el despliegue. Utilizar herramientas de análisis y monitoreo para identificar y resolver problemas rápidamente.(Check Point, 2024)
- Comunicación y Coordinación: Mantener una comunicación clara y constante con todas las partes interesadas durante el proceso de despliegue. Coordinar con los

equipos locales en cada ubicación para asegurar una implementación sin problemas.

- Plan de Contingencia: Desarrollar y documentar un plan de contingencia para revertir cambios en caso de problemas críticos durante el despliegue.
- Documentación y Retroalimentación: Documentar cada paso del proceso de despliegue y recoger feedback para mejorar futuras fases. Ajustar las políticas y configuraciones basadas en la retroalimentación y los resultados del despliegue. (Martis, 2023)

CAPÍTULO 3- METODOLOGÍA

Este capítulo incluye la selección del caso de estudio, la recopilación de datos evaluando aspectos clave como costos, rendimiento, y beneficios potenciales. Al final, los hallazgos serán sintetizados para ofrecer una guía clara para la propuesta del plan de despliegue de SD-WAN y con que proveedor resulta ser más adecuado realizar en un futuro la implementación en la empresa.

3.1. DISEÑO DE LA INVESTIGACIÓN

El diseño de la investigación seguirá un enfoque de estudio de caso único para explorar la implementación de SD-WAN en un entorno empresarial.

3.1.1. Enfoque de estudio de caso

Abordaremos los siguientes aspectos:

1. **Identificar las motivaciones de la migración:** Antes de empezar a diseñar la nueva red SD-WAN, es importante definir claramente que quiere alcanzar la empresa como resultados de la implementación en las agencias. Esto ayudarán a tomar decisiones más informadas en cuanto al diseño de la nueva red.
2. **Realizar una revisión exhaustiva de la literatura sobre redes WAN tradicionales y SD-WAN para identificar limitaciones y ventajas:** Analizar a detalle la infraestructura de red existente para evaluar la red WAN actual de la agencia seleccionada, con el fin de identificar problemas y recopilar datos sobre el rendimiento.
3. **Evaluar los proveedores de SD-WAN:** Hay muchos proveedores de SD-WAN en el mercado, cada uno con sus propias características y funcionalidades. Es importante investigar y evaluar cuidadosamente los proveedores disponibles antes de tomar una decisión. Se tomará en cuenta factores como el rendimiento, la

escalabilidad, la facilidad de gestión, costos de licenciamiento y la interoperabilidad con la red existente.

4. **Diseñar la nueva arquitectura:** Una vez elegido el proveedor de SDWAN, se procederá a diseñar la nueva arquitectura de red. Esto puede incluir la selección de los enlaces WAN, la topología de la red, y la configuración de las políticas de enrutamiento y priorización de tráfico. Se desarrollará un plan de despliegue detallado, incluyendo fases de implementación como gestión del cambio y estrategias de mitigación de riesgos para asegurar que la empresa tenga una migración exitosa cuando se ponga en marcha la implementación teniendo como base esta investigación.

3.2. RECOPILACIÓN DE DATOS DEL CASO DE ESTUDIO

A continuación, se detallará la presentación de la empresa Centric S.A., destacando su papel en la estrategia administrativa y su colaboración con diversas empresas del sector automotriz. Se describirá la infraestructura de red existente en la agencia de prueba, resaltando la configuración y funciones de firewalls, concentradores de red, equipos de enlace de datos, conexiones WAN, internet corporativo y Small Business, switch de capa 3, controladoras de puntos de acceso inalámbrico, y cámaras de seguridad. Además, se analizarán los motivos que impulsan la adopción de SD-WAN, como la optimización del tráfico WAN, la flexibilidad operativa, la mejora en seguridad, la gestión centralizada y automatización, la experiencia mejorada del usuario, y la posible reducción de costos operativos.

3.2.1. Presentación de la empresa

Centric S.A. es una empresa de Servicios Compartidos, actualmente lidera la estrategia administrativa para que las empresas se enfoquen en la estrategia del negocio. Cuenta con el respaldo del grupo Baca y Vásquez.

Centric S.A. trabaja con diferentes empresas que se enfocan en diversos sectores automotrices, entre ellos la venta de vehículos, compra y venta de vehículos multimarca, venta de repuestos automotrices, venta de planes de compra programada y talleres para mantenimientos de vehículos. Además, trabaja con empresas conocidas como: Casabaca, Nexumcorp, Suzuki Ecuador, 1001Carros, Mansuera, Certero. (Centric S.A., 2021)

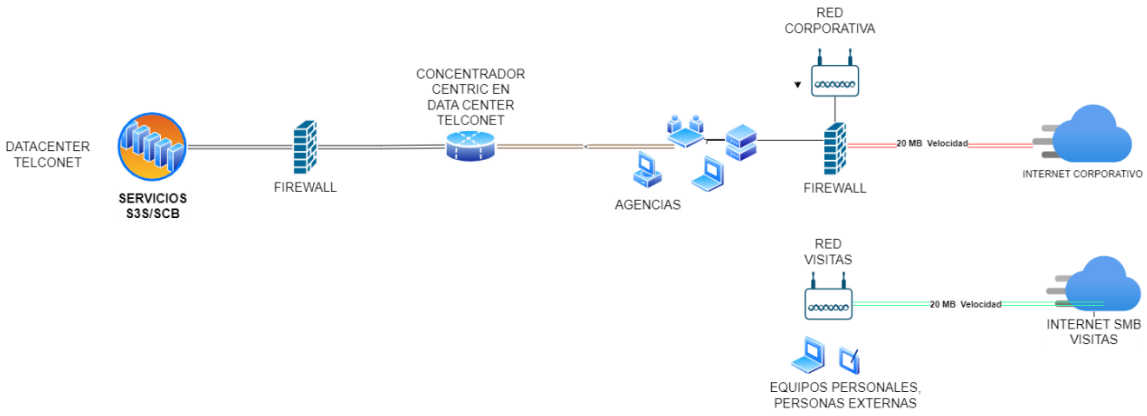
Misión y Visión:

- *Liderar la estrategia administrativa para que las empresas se enfoquen en la estrategia del negocio.*
- *Ser el referente de prestación de servicios y soluciones administrativas en el país.* (Centric S.A., 2023)

3.2.2. Infraestructura de red existente

Actualmente la empresa Centric S.A. tiene su Data Center principal ubicado en Telconet que interconecta todas las agencias del Grupo Baca utilizando una topología de red "hub-and-spoke". En esta configuración, todas las agencias (los "spokes") están interconectadas a un único centro de datos centralizado que es el Data Center (el "hub") desde el cual se gestiona los aplicativos empresariales, servidores y bases de datos de la empresa. A continuación, se anexa un esquema general de la conexión entre las agencias con el DC:

Figura 1 - Conexión agencias con DC



Fuente: Elaboración propia

En el esquema presentado se puede observar como las agencias del Grupo Baca se encuentran conectadas al Data Center de Centric S.A. Cabe señalar que cada agencia cuenta con equipo Fortinet que brinda un enlace de datos provisto por Telconet para mantener la conexión al Data Center, facilitando así la administración centralizada y eficiente de los recursos de la red a través de un enrutamiento que permite que todas las subredes se mantengan separadas para mejorar la seguridad y la eficiencia en la agencia, además cuentan con un internet separado Small Business para usuarios que no forman parte de la red corporativa principal.

Sobre el enrutamiento de red mencionado anteriormente se tiene configurado de la siguiente manera:

- Red LAN: 172.19.7.0/24 (IP específica por agencia)
    - Función: Proporciona conectividad de red a dispositivos cableados como computadoras de escritorio, impresoras y servidores locales.
    - Propósito: Permitir la comunicación interna y el acceso a recursos compartidos dentro de la agencia.
- Red Wifi: 172.19.57.0/24 (IP específica por agencia)
    - Función: Conecta dispositivos inalámbricos como laptops, smartphones y tablets.
    - Propósito: Facilitar la movilidad de los empleados y visitantes dentro de la agencia, asegurando una conexión a internet sin cables.
- Red Telefonía: 172.19.107.0/24 (IP específica por agencia)
    - Función: Conecta teléfonos IP y sistemas de comunicación de voz.
    - Propósito: Soportar el sistema de telefonía de la agencia, asegurando una comunicación eficiente y separada del tráfico de datos común.
- Red Admin Equipos: 172.19.207.0/24 (IP específica por agencia)

- Función: Conecta equipos de administración y dispositivos de gestión de red.
- Propósito: Facilitar el acceso y control de dispositivos críticos de red y servidores de administración.

Con esta configuración se tiene a cada subred separada con su propio rango de direcciones IP, lo que permite organizar y gestionar mejor el tráfico de red, asegurando que el tráfico interno de cada segmento no interfiera con los demás, y permitiendo aplicar políticas de red específicas a cada una. Es importante destacar que cada agencia cuenta con diferentes rangos de IPs por subred para poder identificarlas. Las IPs colocadas en el enrutamiento anterior pertenecen únicamente a la agencia de prueba.

También en cada una de las agencias se tiene configuradas las siguientes VLANs (Virtual Local Area Networks) para segmentar y aislar el tráfico según las subredes mencionadas anteriormente:

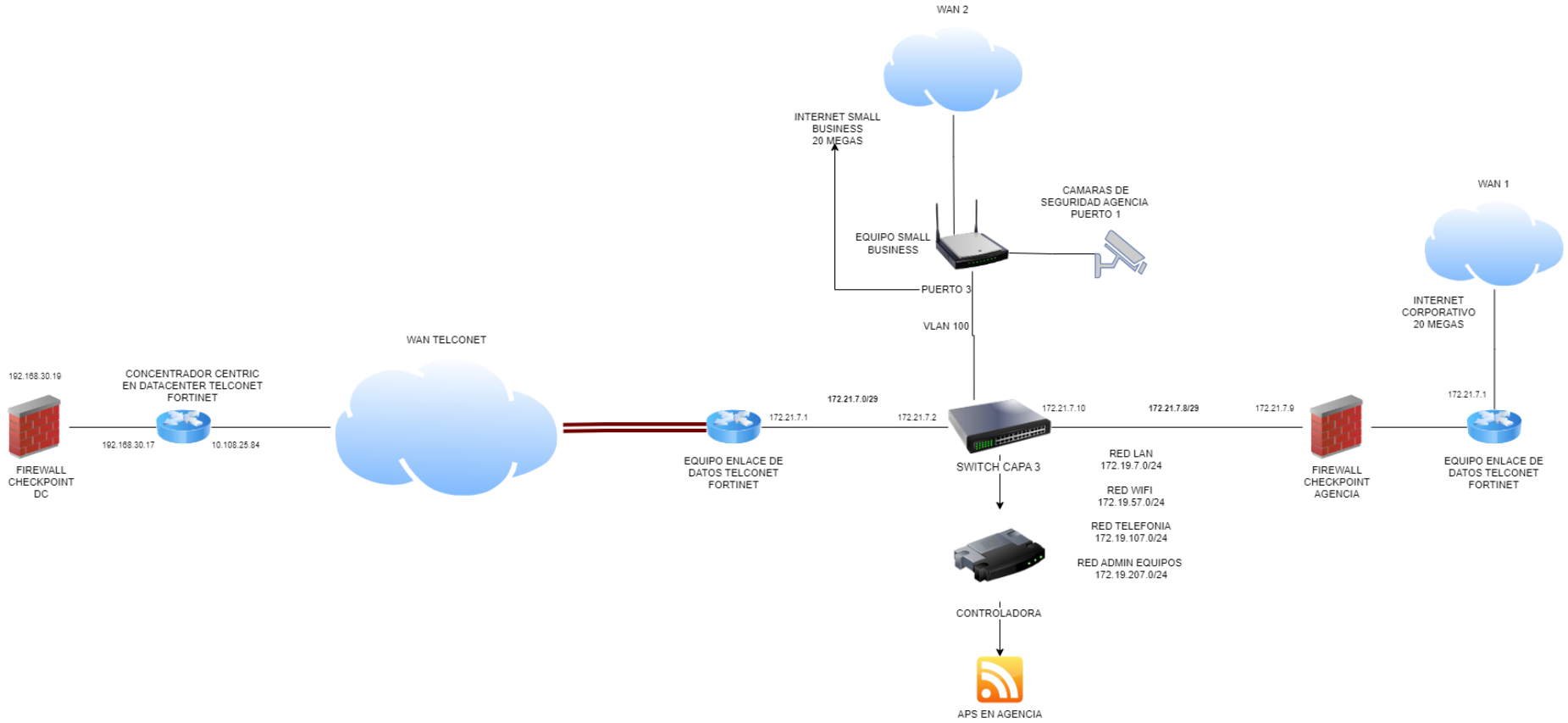
- VLAN Datos: 172.19.7.0/24.
- VLAN Wifi: 172.19.57.0/24.
- VLAN Telefonía: 172.19.107.0/24.
- VLAN 100 (Small Business): 192.168.100.0/24 (Separada de las anteriores)

Estás VLANs tienen el mismo nombre en todas las agencias para poder identificarlas sin embargo el rango de IPs se selecciona por las subredes creadas en el enrutamiento previo, por lo que cada agencia cuenta con sus propias VLANs para sus propias subredes.

Tanto las agencias como el Data Center cuentan con las respectivas medidas de seguridad incorporadas a través de Firewalls (Check Point), mientras que las redes internas se encuentran gestionadas mediante un Switch de capa 3 conectado al equipo de enlace de datos Telconet (Fortinet) y una controladora para los puntos de acceso inalámbricos.

Para realizar un análisis más exacto se anexa un esquema de la infraestructura de red actual de la agencia de prueba con su conexión al Data Center (todas las agencias cuentan con la misma infraestructura).

Figura 2 – Infraestructura actual agencia de prueba



Fuente: Elaboración propia

A continuación, se detalla cada elemento del esquema con su respectiva funcionalidad partiendo de izquierda a derecha:

Tabla 1 – Detalle de equipos Infraestructura actual

Dispositivo	Función	Configuración
Firewall Check Point (Data Center)	Punto de defensa contra amenazas externas en DC	- Filtro de tráfico entrante y saliente, permitiendo únicamente las conexiones necesarias.
Concentrador Centric en Data Center Telconet (Fortinet)	Centraliza y gestiona las conexiones de red de las diversas agencias.	- Conexión a WAN Telconet - Utiliza la IP 10.108.25.84 para la comunicación con el equipo de enlace.
WAN Telconet	Proporciona red de área amplia para aplicaciones críticas y comunicaciones corporativas.	- Protocolo de comunicación: MPLS.
Equipo de Enlace de Datos Telconet (Fortinet)	Conecta la red interna de la agencia con la WAN de Telconet.	- Redirecciona el tráfico entre la WAN de Telconet y la red interna de la agencia
Switch de Capa 3	Gestiona el tráfico de red interno a nivel de capa 3, incluyendo enrutamiento entre VLANs.	- Puertos configurados para diversas VLANs
Equipo Small Business	Proporciona conexión a Internet para usos cotidianos y menos críticos.	- Conexión física al switch de la agencia mediante una VLAN 100 separada de las demás conexiones.
Cámaras de Seguridad	Monitorean la seguridad en la agencia.	- DVR conectado al equipo Small Business para separar el tráfico de seguridad del tráfico general.
WAN 2	Proporciona red de área amplia para conexión a Internet	- Protocolo de comunicación: Banda Ancha
Controladora	Administra los puntos de acceso inalámbrico (APs) en la agencia.	- Conectada al Switch de Capa 3. - Gestiona la configuración y seguridad de los APs.
APs en Agencia	Proporcionan conectividad Wifi a dispositivos dentro de la agencia.	- Administrados por la controladora. Asignación de SSIDs y políticas de seguridad.
Firewall Check Point (Agencia)	Proporciona seguridad y control de tráfico hacia el Internet Corporativo.	- Filtrado y monitoreo de tráfico corporativo.
WAN 1	Proporciona red de área amplia para conexión a Internet de alta capacidad	- Protocolo de comunicación: Dedicado

Fuente: Elaboración propia

A partir del esquema y el detalle de cada uno de los equipos podemos validar que las agencias mantienen una infraestructura de red robusta ya que tenemos el mismo escenario en todas las agencias del grupo.

En el esquema podemos observar que el equipo Enlace de datos Telconet (Fortinet) está repetido, esto se debe a que es el mismo equipo, pero de esta manera visual podemos identificar como este router realiza la conexión con el Data Center a través de la WAN Telconet a la vez que realiza la salida de Internet en la agencia a través de la WAN 1.

Como está detallado en la *Tabla 1* – Detalle de equipos Infraestructura actual la agencia se conecta a una red de área amplia (WAN) proporcionada por Telconet en el Data Center desde el Concentrador de Centric con un rango de IP específico y un protocolo de comunicación MPLS que permite la comunicación entre diferentes ubicaciones de manera confiable y rápida. A este concentrador se encuentra conectado también un Firewall Check Point que como se mencionó con anterioridad brinda una capa de seguridad a la red interna

El equipo de Enlace de datos (Fortinet) actúa como el punto de conexión entre la red interna de la agencia y la WAN de Telconet para tener conexión a los servicios administrativos de la empresa. Está configurado para redirigir el tráfico de manera eficiente, y en caso de fallo de una conexión, puede conmutar a la otra, manteniendo la continuidad del servicio.

La agencia cuenta también con el Internet Small Business destinada principalmente para usos cotidianos y menos críticos. Esta conexión proporciona un ancho de banda limitado, adecuado para tareas como navegación web general, y otras aplicaciones que no requieren altos niveles de ancho de banda o baja latencia como redes sociales. Su rol es crucial como una alternativa o respaldo para garantizar la continuidad operativa y proporcionar conectividad básica cuando el Internet Corporativo tiene algún tipo de afectación.

También se tiene un DVR (Digital Video Recorder) en la agencia que es un dispositivo electrónico que graba video digital desde cámaras de seguridad, permitiendo almacenar y gestionar grabaciones de vigilancia. Este dispositivo está conectado al Internet Small Business para separar el tráfico de cámaras de seguridad del tráfico general como se mencionó también en la tabla.

La combinación de estas conexiones proporciona redundancia. Si una conexión falla, la otra puede seguir proporcionando servicio.

La redundancia en la infraestructura de red de la agencia proporciona una mayor resiliencia y fiabilidad, asegurando que los servicios críticos y las operaciones diarias puedan continuar sin interrupciones significativas. Sin embargo, si los enlaces de Internet Corporativo se ven afectados tanto el MPLS como el dedicado, la agencia únicamente podría operar con el internet Small Business el cual no cuenta con la conexión al data center ni la optimización de la red principal ocasionando pérdidas significativas en la gestión de los colaboradores que utilizan los servicios internos de la empresa.

La gestión y optimización de múltiples conexiones WAN, podría mejorar significativamente con SD-WAN, permitiendo una mejor utilización del ancho de banda, optimización del tráfico y una gestión centralizada más eficiente, lo cual es crucial para adaptarse dinámicamente a las necesidades cambiantes de la red y garantizar un rendimiento óptimo en todo momento.

3.2.3. Motivación para la adopción de SD-WAN

La adopción de SD-WAN en Centric S.A. está motivada por la necesidad de optimizar el tráfico de la red WAN, mejorar la flexibilidad y agilidad en la gestión de múltiples conexiones, reforzar la seguridad con funciones avanzadas, simplificar la administración mediante una gestión centralizada, mejorar la experiencia del usuario al priorizar aplicaciones críticas, y reducir costos operativos mediante la optimización del uso de

ancho de banda y la consolidación de dispositivos de red para que las agencias puedan seguir operando inclusive si los enlaces de datos e internet corporativo se ven afectados. A continuación, abordaremos los aspectos claves para implementar SD-WAN en las agencias de la empresa:

1. Optimización del Tráfico WAN: SD-WAN puede mejorar la eficiencia y el rendimiento de la red WAN al optimizar el enrutamiento del tráfico. Esto es especialmente relevante dado que en la infraestructura de red actual se está utilizando MPLS para conectar las agencias con el data center en Telconet, también hay que tener en cuenta que se tiene una conexión de Internet Small Business de banda ancha que está separada de esta gestión.
2. Flexibilidad y Agilidad: Con SD-WAN, se podrá gestionar de manera más flexible y dinámica múltiples conexiones WAN (como MPLS, dedicado y Small Business), lo que podría proporcionar más opciones para mejorar la disponibilidad y la calidad del servicio.
3. Seguridad Reforzada: Aunque ya se cuenta con firewalls Check Point y medidas de seguridad implementadas, SD-WAN puede integrar funciones avanzadas de seguridad como cifrado de tráfico y segmentación de red, lo cual es crucial para proteger el tráfico sensible y cumplir con regulaciones de seguridad.
4. Gestión Centralizada y Automatización: Con SD-WAN se podrá tener una gestión centralizada desde una consola única, lo cual simplifica la administración de la red y permite configuraciones automatizadas y basadas en políticas. Esto puede reducir la complejidad operativa y los costos asociados.
5. Mejora en la Experiencia del Usuario: Con SD-WAN se podrá permitir la selección inteligente de rutas y la priorización de aplicaciones críticas, esto puede

mejorar la experiencia de usuario al garantizar un rendimiento óptimo de las aplicaciones en la red.

6. Reducción de Costos: Aunque ya se tiene conexiones redundantes, SD-WAN puede ayudar a optimizar el uso de ancho de banda y reducir costos.

3.3. EVALUACIÓN Y SELECCIÓN DE LA SOLUCIÓN SD-WAN

A continuación, se realizará una evaluación detallada de los proveedores y tecnologías disponibles para Centric S.A y se escogerá la más adecuada para la implementación con la infraestructura de red actual en las agencias.

3.3.1. Evaluación de proveedores y tecnologías

En Centric S.A. se ha venido manejando contratos tanto con Check Point como con Fortinet, ambos representados respectivamente por las empresas TeUno y Telconet. Tanto Check Point como Fortinet, son reconocidos en el mercado por sus soluciones de seguridad y redes. A continuación, se detalla las capacidades y beneficios de las soluciones SD-WAN ofrecidas por ambas tecnologías:

Fortinet (Fortinet, 2024):

- Integración con NGFW (Next-Generation Firewall):
    - FortiGate NGFW: Fortinet ofrece SD-WAN integrado en los firewalls FortiGate, proporcionando una solución unificada que combina la seguridad avanzada con la optimización de red. Esto es útil para la agencia, ya que simplifica la infraestructura y la gestión.
- Alto Rendimiento y Escalabilidad:
    - ASICs para SD-WAN: Fortinet utiliza ASICs para optimizar el rendimiento del SD-WAN, lo que garantiza una latencia mínima y un alto rendimiento incluso en condiciones de tráfico pesado. Esto es crucial para

garantizar que las aplicaciones críticas de la agencia funcionen sin problemas.

- Gestión Centralizada:
    - FortiManager y FortiAnalyzer: Permiten la gestión centralizada de la red y la visibilidad del tráfico. Esto facilita la configuración, el monitoreo y la resolución de problemas desde una única consola, lo cual es esencial para gestionar múltiples agencias de manera eficiente.
- Optimización de Tráfico y Calidad de Servicio:
    - Routing Inteligente: Fortinet SD-WAN utiliza algoritmos avanzados para dirigir el tráfico de manera óptima, asegurando que las aplicaciones críticas tengan prioridad y mantengan un rendimiento constante.
    - WAN Path Controller: Monitoriza el rendimiento de los enlaces WAN y selecciona dinámicamente la mejor ruta para cada tipo de tráfico.
- Seguridad Integrada:
    - Inspección de Tráfico: Fortinet proporciona inspección profunda de paquetes (DPI) y otras funciones de seguridad dentro de la solución SD-WAN, garantizando que todo el tráfico esté protegido.

Check Point (Check Point, 2022):

- Foco en la Seguridad:
    - Integración de Seguridad: Check Point integra SD-WAN con sus soluciones de seguridad avanzadas, proporcionando una capa de seguridad robusta para el tráfico de red. Esto es beneficioso para la protección contra amenazas avanzadas.
- Rendimiento y Fiabilidad:

    - Dynamic Path Selection: Check Point SD-WAN ofrece selección dinámica de rutas basada en el rendimiento en tiempo real, lo que mejora la fiabilidad y el rendimiento de las aplicaciones.
    - Redundancia y Failover: Proporciona conmutación por error automática y balanceo de carga entre múltiples enlaces WAN, asegurando alta disponibilidad.
- Gestión y Visibilidad:
    - SmartConsole: La consola de gestión centralizada de Check Point permite una visibilidad completa y el control de la red SD-WAN, facilitando la administración y el monitoreo.
    - Análisis de Tráfico: Proporciona herramientas avanzadas para el análisis y la visibilidad del tráfico, ayudando a identificar y resolver problemas rápidamente.
- Optimización de Aplicaciones:
    - Priorización de Aplicaciones: Check Point SD-WAN puede priorizar el tráfico de aplicaciones críticas, garantizando un rendimiento óptimo para las aplicaciones más importantes para la agencia.
    - Optimización de Enlaces WAN: Permite la optimización del uso del ancho de banda, asegurando que los recursos se utilicen de manera eficiente.
- Facilidad de Implementación:
    - Despliegue y Configuración: Check Point ofrece soluciones que pueden ser implementadas rápidamente con configuraciones predefinidas, lo que reduce el tiempo y esfuerzo de despliegue.

Check Point es conocido por su enfoque en seguridad avanzada, lo cual puede resultar en un costo más elevado. Sus soluciones están diseñadas para ofrecer niveles de seguridad

muy altos. Además, las licencias de Check Point para SD-WAN y seguridad tienden a ser más caras debido a las características avanzadas y la robustez de las soluciones. Lo mismo sucede con los dispositivos los cuales suelen ser más caros en comparación con los de Fortinet, lo que puede incrementar el costo total de propiedad.

- Check Point Appliances: Los dispositivos de Check Point pueden comenzar alrededor de $1,000 para modelos básicos y superar los $10,000 para modelos más avanzados.
- Licencias de SD-WAN (Check Point): Las licencias para soluciones de SD-WAN de Check Point pueden costar entre $500 a $1,500 por año por dispositivo, dependiendo del paquete de servicios y características de seguridad incluidas.
- FortiGate SD-WAN Appliances: El costo de un dispositivo FortiGate puede variar desde unos $500 para modelos básicos hasta varios miles de dólares para modelos de alto rendimiento.
- Licencias de SD-WAN (Fortinet): Las licencias para SD-WAN pueden costar entre $100 a $500 por año por dispositivo, dependiendo del nivel de funcionalidad y soporte.

Además de lo mencionado anteriormente, Fortinet suele ser percibido como una opción más económica para soluciones de SD-WAN por varias razones clave:

- Las licencias de Fortinet para SD-WAN y otras funcionalidades de seguridad son generalmente competitivas y pueden ser más económicas.
- Fortinet a menudo ofrece opciones de licenciamiento flexibles, como suscripciones anuales, que pueden ajustarse a diferentes presupuestos y necesidades financieras.
- La administración centralizada y la facilidad de uso de la plataforma de Fortinet pueden reducir los costos operativos y de administración.

- La flexibilidad en la selección de dispositivos puede resultar en una implementación más coste-efectiva.

Según estos puntos revisados de ambos proveedores de para la implementación de SD-WAN en Centric S.A. podemos destacar la robustez y especialización de ambas soluciones. Fortinet ofrece una integración avanzada con firewalls NGFW, alto rendimiento mediante ASICs, gestión centralizada eficiente y costos competitivos en licencias y dispositivos. Por otro lado, Check Point sobresale en seguridad avanzada, selección dinámica de rutas y alta disponibilidad, aunque con costos iniciales y de licenciamiento más elevados.

3.3.2. Selección de proveedor y tecnologías

Check Point es una opción sólida que ofrece una capa avanzada de protección y gestión especializada en seguridad. Sin embargo, Fortinet sería la elección más adecuada para la solución SD-WAN en la agencia debido a su integración más completa y unificada de seguridad y rendimiento de red. A diferencia de Check Point, Fortinet ofrece una plataforma todo en uno que combina firewall, VPN, control de aplicaciones, IPS y filtrado de contenido, optimizando automáticamente las rutas de tráfico y mejorando la experiencia del usuario. La administración centralizada a través de FortiManager y FortiAnalyzer simplifica la supervisión y gestión. Además, Fortinet proporciona una solución más costo-efectiva, reduciendo los costos de implementación y mantenimiento, y ofreciendo un mejor retorno de inversión debido a la reducción de interrupciones y el aumento de la eficiencia operativa lo que significa que la inversión en esta tecnología produce mayores beneficios tanto operativos como financieros. La facilidad de implementación, la gestión simplificada y la plataforma unificada de Fortinet aseguran una transición fluida y optimizada hacia una infraestructura de red SD-WAN robusta y eficiente.

3.4. TOPOLOGÍA DE RED ÓPTIMA PARA LA SOLUCIÓN SD-WAN SELECCIONADA

La topología óptima para la solución SD-WAN utilizará los enlaces MPLS, Dedicado y Small Business para alta disponibilidad y balanceo de carga. La configuración centralizada y la integración con la controladora Wifi y APs aseguran una red segura, eficiente y escalable. Se tomará en cuenta los siguientes puntos para realizar la topología para la nueva red:

- FortiGate SD-WAN Gateway: Se tiene dispositivos Fortinet en todas las agencias del Grupo y en el data center, se deberá activar el módulo de SD-WAN para poder realizar la migración en un futuro.
- Switch de Capa 3: Para gestionar el tráfico interno y la segmentación de VLANs.
- Firewall Check Point Existente: Mantener el uso de Check Point para funciones específicas de seguridad avanzada si es necesario.
- Controladora y APs: Para gestionar y proporcionar conectividad Wifi tal y como se está realizando en la infraestructura actual.
- MPLS, Dedicado y Small Business: Utilizar tanto MPLS como enlaces de Internet de Small Business y Corporativo para redundancia y balanceo de carga.

Se tendrá que tomar en cuenta algunos aspectos de la configuración de red actual y ejecutar nuevas configuraciones para que la migración sea exitosa:

- Conexión a Internet Corporativo y Small Business:
    - FortiGate SD-WAN configurado para utilizar ambas conexiones de Internet (Corporativo y Small Business) con balanceo de carga y conmutación por error.
        - El Internet Corporativo será la conexión principal para aplicaciones críticas.

        - El Internet Small Business actuará como respaldo y para tráfico menos crítico.
    - Conexión MPLS:
        - Mantener el enlace MPLS de Telconet como una conexión redundante de alta disponibilidad para tráfico de datos entre la agencia y el data center

Segmentación de Red y VLANs

- Switch de Capa 3 (L3):
    - Se tiene el equipo Fortinet (Equipo de Enlace de Datos Telconet) conectado al switch de capa 3 lo cual servirá para gestionar el tráfico interno.
    - Configuración de múltiples VLANs para segmentar el tráfico de red (Como se tiene actualmente configurado).

Integración de Controladora y APs

- Controladora Wifi:
    - Conectar la controladora a través del switch L3.
    - Configurar la controladora para gestionar todos los APs y asignar SSIDs específicos con las políticas de seguridad apropiadas para la nueva red

Seguridad Avanzada

- FortiGate NGFW:
    - Configurar políticas de seguridad avanzadas en FortiGate para inspección profunda de paquetes, control de aplicaciones, y prevención de intrusiones.
    - Integrar FortiGate con los firewalls Check Point existentes para una capa adicional de seguridad si es necesario.

Configuración en FortiGate SD-WAN

- Configuración de Interfaces
    - WAN1: Conexión a Internet Corporativo (Dedicado)
    - WAN2: Conexión a Internet Small Business.
    - WAN3: Conexión MPLS.
- SD-WAN Rules (Reglas de SD-WAN)
    - Load Balancing: Configurar reglas para distribuir el tráfico entre WAN1 y WAN2 basado en políticas de tráfico y ancho de banda disponible.
    - Failover: Configurar la conmutación por error (failover) para que si WAN1 (Internet Corporativo) falla, el tráfico crítico se redirija automáticamente a WAN2 (Small Business) o WAN3 (MPLS).
    - Performance SLA: Configurar los acuerdos de nivel de servicio (SLA) para monitorear el rendimiento de cada enlace y tomar decisiones de enrutamiento basadas en latencia, pérdida de paquetes y jitter.
- Políticas de Seguridad
    - Inspección de Tráfico: Configurar políticas para inspeccionar y filtrar el tráfico entrante y saliente.
    - Segmentación de VLANs: Aplicar políticas de seguridad específicas a cada VLAN para aislar y proteger diferentes tipos de tráfico.

Gestión y Monitoreo

- FortiManager: Para la gestión centralizada de todas las políticas y configuraciones de SD-WAN.
- FortiAnalyzer: Para la recolección y análisis de registros, proporcionando visibilidad completa y reportes detallados del rendimiento y seguridad de la red.

Con está topología tendremos beneficios significativos para la agencia. Primero, garantiza alta disponibilidad y redundancia mediante el uso de múltiples enlaces WAN, incluyendo Internet Corporativo, Small Business y MPLS, asegurando así la continuidad operativa incluso en caso de fallos de enlace. Además, FortiGate proporciona seguridad avanzada integrada, consolidando funciones de seguridad en un solo dispositivo y simplificando la gestión. Los algoritmos de balanceo de carga y conmutación por error optimizan el uso del ancho de banda, mejorando la experiencia del usuario y garantizando un rendimiento óptimo.

Esta topología es altamente escalable, permitiendo la expansión fácil y aumenta la capacidad a medida que la agencia crece, asegurando que la infraestructura de red pueda adaptarse al crecimiento del negocio de manera eficiente mientras que en el data center se mantiene la topología de red "hub-and-spoke" para la interconexión con las agencias la cual no se verá afectada por la implementación.

3.5. PROPUESTA DE PLAN DE DESPLIEGUE

Esta propuesta para el plan de despliegue describe las fases y actividades necesarias para implementar a futuro SD-WAN de manera efectiva y ordenada en la agencia de Centric S.A. asegurando que todas las etapas críticas y aspectos operativos sean considerados y manejados adecuadamente. Se presenta a continuación la ejecución planeada para cada fase:

Fase 1: Preparación de Infraestructura y Políticas SD-WAN

- Evaluación inicial de la infraestructura de red actual de la agencia: Análisis detallado de la infraestructura de red existente para identificar capacidades, limitaciones y requisitos específicos.
- Diseño conceptual de la arquitectura SD-WAN: Elaboración de un diseño preliminar que incluya la topología de red, los componentes principales como

FortiGate SD-WAN, switch de Capa 3, controladora WiFi, entre otros, y la integración con la infraestructura existente.

- Definición de políticas de enrutamiento, seguridad y QoS: Establecimiento de políticas y configuraciones para dirigir el tráfico de red de manera eficiente, garantizando la seguridad y priorizando el tráfico crítico mediante QoS (Calidad de Servicio).

Fase 2: Planificación de la Gestión del Cambio

- Desarrollo de un plan de comunicación: Creación de estrategias de comunicación para informar a todos los empleados y partes interesadas sobre el proyecto de implementación de SD-WAN, destacando los beneficios y los cambios esperados.
- Propuesta para capacitación al personal de TI: Planificación de sesiones de capacitación para el personal de TI y otros usuarios clave sobre cómo operar y mantener la nueva infraestructura de SD-WAN.
- Plan de soporte y monitoreo durante y después de la implementación: Establecimiento de procedimientos para monitorear y resolver problemas durante la implementación, así como la definición de roles y responsabilidades para el soporte continuo después del despliegue inicial.

Fase 3: Estrategias de Mitigación de Riesgos

- Identificación de riesgos asociados con la implementación de SD-WAN: Evaluación de posibles problemas técnicos, operativos o de seguridad que podrían surgir durante la implementación y la transición.
- Desarrollo de planes de contingencia: Creación de planes de acción específicos para abordar cada riesgo identificado, asegurando una respuesta rápida y efectiva en caso de problemas.

- Marco para la evaluación continua del desempeño de SD-WAN: Establecimiento de métricas y procedimientos para evaluar el rendimiento de SD-WAN después de la implementación, garantizando ajustes y mejoras continuas.

Fase 4: Cronograma de Implementación

- Creación de un cronograma detallado: Desarrollo de un calendario con fechas aproximadas para cada fase de la migración,
- Elaboración de hitos clave como pruebas, capacitaciones y la implementación final de SD-WAN.
- Roles y responsabilidades: Asignación clara de roles y responsabilidades a los miembros del equipo de proyecto, asegurando una ejecución eficiente y coordinada.

CAPÍTULO 4- DESARROLLO DEL PLAN DE DESPLIEGUE

En este capítulo se abordarán fases clave como el diseño conceptual de la arquitectura SD-WAN, la planificación de la gestión del cambio, estrategias de mitigación de riesgos y la creación de un cronograma de implementación con la finalidad de que las empresas puedan preparar una adopción exitosa de SD-WAN, optimizando su infraestructura de red y maximizando los beneficios esperados sin interrumpir sus operaciones actuales.

4.1. PREPARACIÓN DE INFRAESTRUCTURA Y POLÍTICAS SD-WAN

En la fase inicial de preparación, se realizará una evaluación exhaustiva de la infraestructura actual de red de la agencia para identificar capacidades y requisitos específicos basándonos en la revisión realizada a los equipos que tenemos y sus respectivas funciones. Se elaborará un diseño preliminar de la arquitectura SD-WAN, y se especificarán políticas detalladas de enrutamiento, seguridad y calidad de servicio (QoS) para gestionar eficientemente el tráfico y garantizar la seguridad de la red.

4.1.1. Evaluación inicial de la infraestructura de red actual de la agencia

A continuación, se presentará un inventario detallado que proporcionará una visión clara de la infraestructura de red actual de la agencia en base a la *Figura 2* – Infraestructura actual agencia de prueba, facilitando la planificación para la implementación de la adopción de SD-WAN, es necesario considerar que todas las IPs detalladas son únicamente de la agencia que está sirviendo de ejemplo, todas las demás agencias cuentan con sus propias IPs.

Tabla 2 - Firewalls

Firewalls	Ubicación Física	Modelo	Dirección IP de Gestión	Políticas de Seguridad
Firewall Check Point DC	Data Center Telconet	Quantum 6400	192.168.30.19	Filtro de tráfico entrante y saliente
Firewall Check Point	Agencia	Quatum Spark 1550	172.21.7.9	Filtrado y monitoreo de tráfico corporativo

Fuente: Elaboración propia

Tabla 3 - Routers

Routers	Ubicación física	Modelo	Dirección IP de gestión	Configuración de interfaces WAN y LAN	Configuración de protocolos de enrutamiento
Concentrador Centric (Fortinet)	Data Center Telconet	FortiGate 600F	192.168.30.17	Conexión a WAN TELCONET	Centraliza y gestiona las conexiones de red de todas las agencias
Equipo de Enlace de Datos Telconet (Fortinet)	Agencia	FortiGate 40F	172.21.7.1	Conexión a WAN TELCONET y WAN 1	Redirecciona el tráfico entre la WAN y la red interna
Equipo Small Business	Agencia	Huawei EG8145V5	192.168.100.1	Conexión a WAN 2	No tiene protocolos de enrutamiento

Fuente: Elaboración propia

Tabla 4 - Switchs

Switch de Capa 3	
Ubicación física	Agencia
Modelo	Cisco 2960
Dirección IP de gestión	172.21.7.2

Fuente: Elaboración propia

Tabla 5 - APs

Access Point	
Ubicación física	Varias ubicaciones dentro de la agencia
Modelo	Cisco 3702E
Dirección IP de gestión	IPs Fijas por AP
Configuración de SSIDs	Administrados por la controladora
Políticas de seguridad WLAN	Configuradas por la controladora

Fuente: Elaboración propia

Tabla 6 – Controladora Wifi

Controladora	
Ubicación física	Sala de servidores
Modelo	Cisco 5500 Wireless Controller
Función	Administra la configuración y seguridad de los APs

Fuente: Elaboración propia

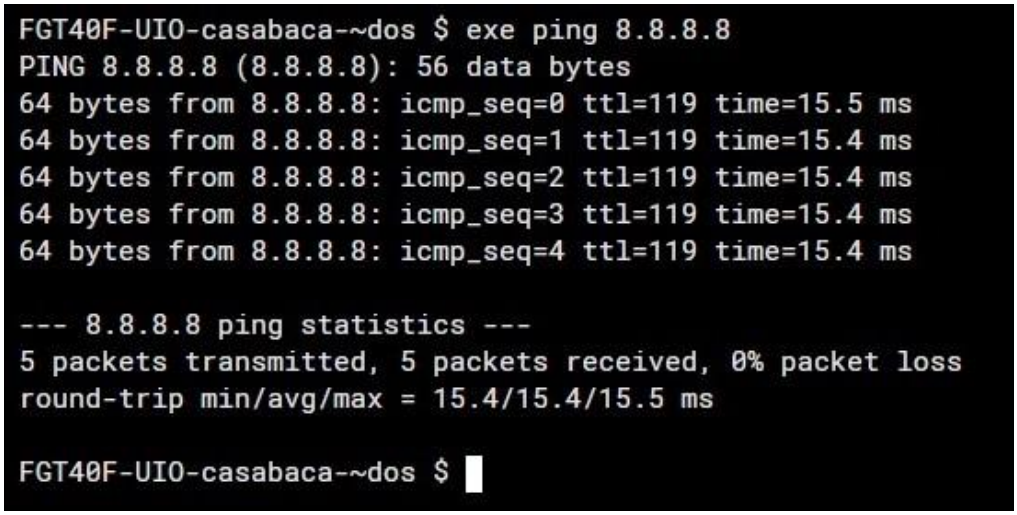
Tabla 7 – Cámaras de seguridad

Cámaras de seguridad (DVR)	
Función	Monitoreo de seguridad en la agencia.
Configuración	Conectadas a Internet Small Business en VLAN 100 para separar el tráfico de seguridad del tráfico general.

Fuente: Elaboración propia

Para validar el rendimiento actual de la red se realizó PING al servidor interno y externo para verificar la conexión al data center y salida de internet, aquí mismo se pudo verificar que no se tiene perdida de paquetes, a continuación, anexo PING:

Figura 3 – PING Google



Fuente: Obtención propia

Figura 4 – PING Servidor Interno

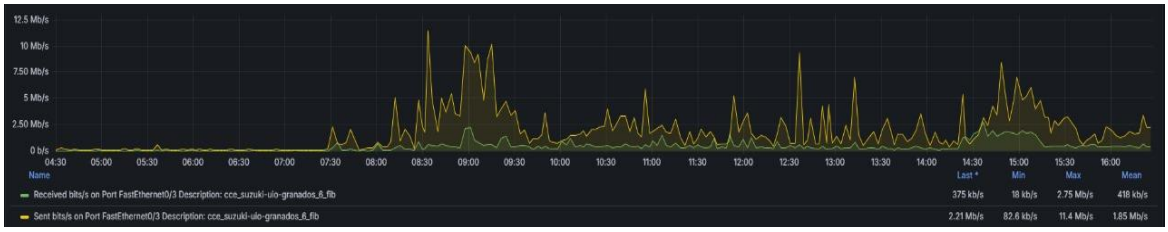
```
PING 192.168.30.17 (192.168.30.17): 56 data bytes
64 bytes from 192.168.30.17: icmp_seq=0 ttl=250 time=6.1 ms
64 bytes from 192.168.30.17: icmp_seq=1 ttl=250 time=5.9 ms
64 bytes from 192.168.30.17: icmp_seq=2 ttl=250 time=6.0 ms
64 bytes from 192.168.30.17: icmp_seq=3 ttl=250 time=6.0 ms
64 bytes from 192.168.30.17: icmp_seq=4 ttl=250 time=6.0 ms

--- 192.168.30.17 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 5.9/6.0/6.1 ms
```

Fuente: Obtención propia

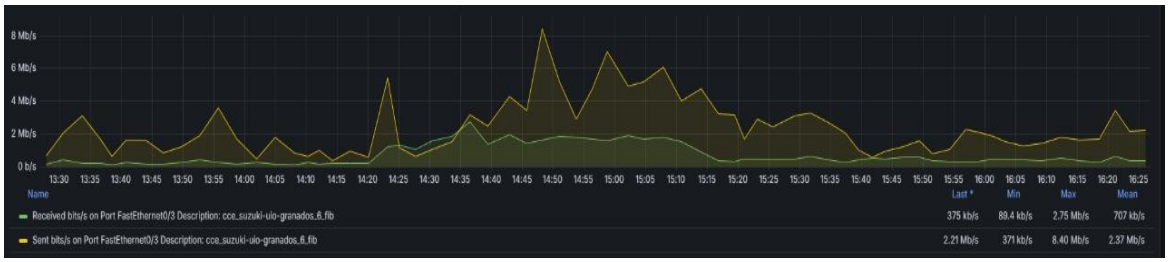
Como se logra observar no se tiene tiempos de respuesta altos por lo que se puede concluir que el servicio de internet corporativo provisto por el proveedor no tiene problemas significativos y sugiere que los enlaces están trabajando adecuadamente, adicional a esto se validó con el proveedor sobre una posible saturación en los enlaces de datos e internet durante un día completo de trabajo, a continuación, se anexan los resultados:

Figura 5 – Monitoreo enlaces de datos e internet



Fuente: Obtenido del proveedor Telconet

Figura 6 - Monitoreo enlaces de datos e internet (tarde)



Fuente: Obtenido del proveedor Telconet

Como podemos evidenciar los enlaces no cuentan con problemas de conexión relevantes, siendo el color amarillo el que representa el enlace de internet y el verde el que representa

el enlace de datos provisto por Telconet, se tienen promedios de uso aceptables y picos de tráfico no muy recurrentes para la WAN2 que es la red provista por el Small Business se valida con el proveedor sin embargo al no ser una red corporativa no se muestran graficas. A continuación, se presentan los resultados:

Tabla 8 – Ancho de banda utilizado

WAN	Promedio de Uso	Picos de Tráfico
WAN1	1,85 Mbps	11,4 Mbps (8 AM – 10 AM)
WAN2	4 Mbps	10 Mbps (1 PM - 3 PM)
WAN3 (MPLS)	418 Kbps	2,75 Mbps (2 PM – 4 PM)

Fuente: Elaboración propia

Tabla 9 - Latencia

Tipo de Ping	Dirección IP	Latencia Promedio	Picos de Latencia
Servidor Interno	192.168.30.17	6 ms	6.1 ms
Servidor Externo	8.8.8.8 (Google DNS)	15.4 ms	15.5 ms

Fuente: Elaboración propia

Tabla 10 – Pérdida de paquetes

Tipo de Ping	Dirección IP	Pérdida de Paquetes
Servidor Interno	192.168.30.17	0%
Servidor Externo	8.8.8.8	0%

Fuente: Elaboración propia

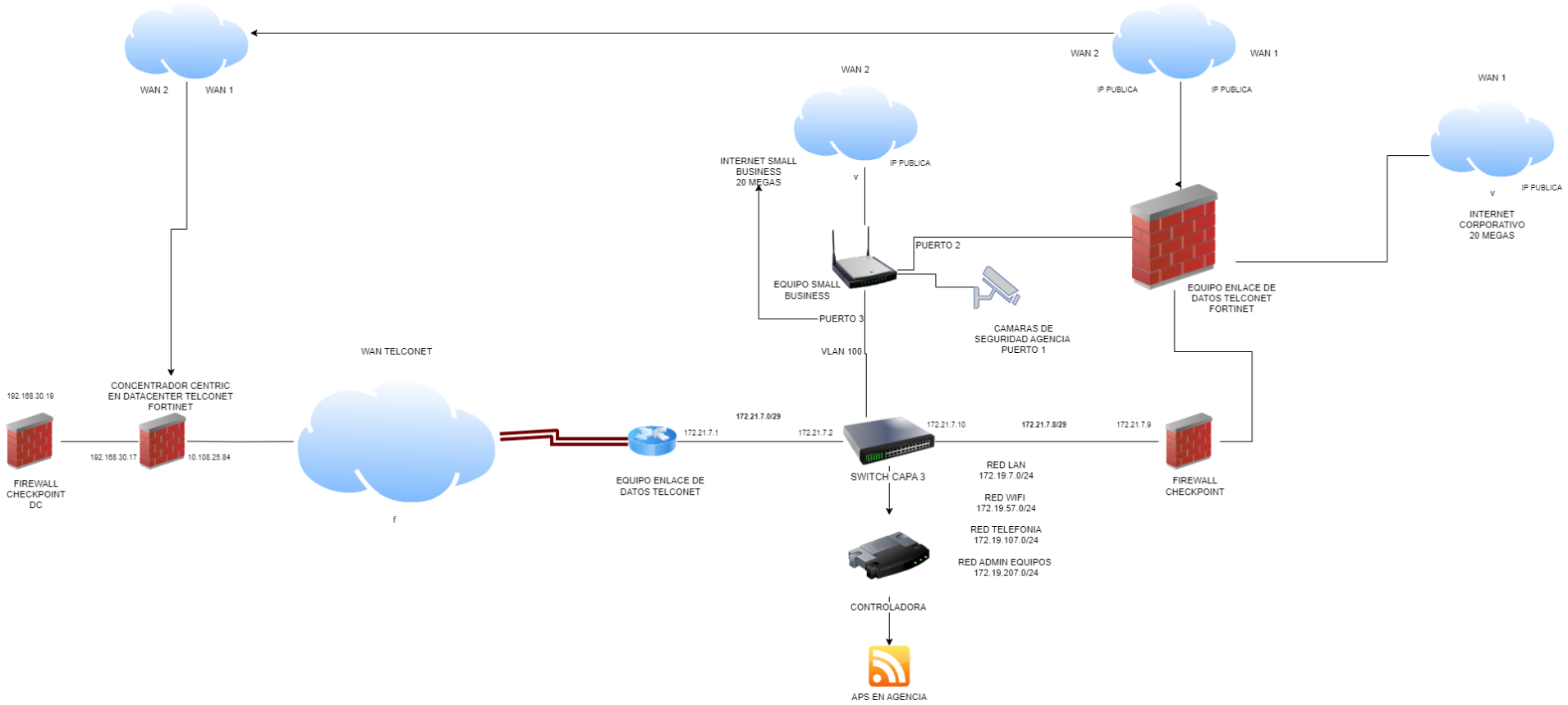
Como recomendación antes de realizar la implementación de SD-WAN en la agencia se puede considerar aumentar el ancho de banda de los enlaces, especialmente el Internet Corporativo, para manejar mejor las demandas durante las horas pico. Configurar QoS en los dispositivos de red para priorizar el tráfico crítico y asegurar que las aplicaciones esenciales reciban suficiente ancho de banda. Como pudimos evidenciar el principal inconveniente que manejan actualmente las agencias son los casos que se presentan por perdidas de enlace en el que toda la agencia se quedaría sin servicio de internet en caso de que el enlace afectado sea el mismo, o en el caso de que el enlace afectado sea el enlace de datos, la agencia perdería la conexión hacia el data center y por ende a todos los aplicativos empresariales gestionados desde acá. Después de una migración a SD-WAN

la recomendación principal sería realizar evaluaciones periódicas del rendimiento de la red para asegurarse de que los cambios implementados estén teniendo el efecto deseado.

4.1.2. Diseño conceptual de la arquitectura SD-WAN

Con todo lo validado anteriormente y en base a la infraestructura de red actual se diseñó el siguiente esquema que servirá como base para la integración con los equipos en la agencia cuando se realice una migración a SD-WAN:

Figura 7 – Diseño conceptual SD-WAN



Fuente: Elaboración propia

Como podemos apreciar en el diseño conceptual se cambió el diagrama de los routers de Fortinet, esto debido a que para SD-WAN se añadirá los modules necesarios en los que está incluido que el equipo opere como un Firewall y también añada una capa de seguridad tanto a la red corporativa en la agencia y en el data center, hay que destacar que el equipo Small Business se deberá conectar desde el puerto 2 hacia el equipo Fortinet de la agencia mediante una IP Pública para que pueda formar parte de la interfaz de gestión de SD-WAN, de esta manera se tendrán todas las conexiones WAN (Internet Corporativo, Small Business y MPLS). Se puede apreciar el túnel de conexión que existirá desde este equipo hacia el equipo Fortinet en el data center lo que permitirá que el equipo Small Business también forme parte de esta interconexión. Esto facilitará el balanceo de carga, la conmutación por error y la optimización del uso del ancho de banda. Es necesario tomar en cuenta los siguientes parámetros antes de una implementación:

- Conexiones WAN Redundantes:
    - WAN1: Internet Corporativo: Conexión principal para aplicaciones críticas y comunicaciones corporativas.
    - WAN2: Internet Small Business: Conexión secundaria para tráfico no crítico y como respaldo.
    - WAN3: MPLS: Conexión de alta disponibilidad y baja latencia para aplicaciones sensibles y comunicaciones entre agencias con el data center

También hay que destacar los siguientes puntos una vez se añada la funcionalidad de SD-WAN en los equipos Fortinet:

- FortiGate SD-WAN Appliance:
    - Proporciona la funcionalidad de SD-WAN, incluyendo balanceo de carga, conmutación por error, y optimización del tráfico.

- Integra capacidades avanzadas de seguridad como firewall, VPN, y prevención de intrusiones.

- Firewall Check Point (Opcional):
  - Proporciona una capa adicional de seguridad, especialmente para el tráfico que se dirige hacia el Internet Corporativo.
  - Monitorea y filtra el tráfico entrante y saliente.

4.1.3. Definición de políticas de enrutamiento y seguridad

Con las funcionalidades de SD-WAN integradas en los equipos Fortinet podremos tener acceso a la consola de gestión FortiGate desde la cual se tendrá que ejecutar las siguientes políticas para asegurar que funcione correctamente:

Políticas de Enrutamiento para SD-WAN:

Para dirigir el tráfico de red de manera eficiente a través de los diferentes enlaces WAN y priorizar el uso y la disponibilidad, se implementará las siguientes políticas de enrutamiento:

Tabla 11 – Aplicaciones críticas

Política para Aplicaciones Críticas	
Aplicaciones Incluidas	ERP, CRM, videoconferencias, correo corporativo
Enlace Principal	Internet Corporativo (WAN1)
Enlace Secundario (Failover)	Internet Small Business (WAN2)
Enlace de Respaldo	WAN Telconet (WAN3)
QoS (Calidad de Servicio)	Alta prioridad, garantizando un ancho de banda mínimo del 50% del total disponible en WAN1

Fuente: Elaboración propia

Esta política asegura que las aplicaciones críticas utilicen principalmente la conexión a Internet Corporativo (WAN1) y, en caso de fallo, se redirijan automáticamente a la conexión de Internet Small Business (WAN2), con una última opción de respaldo en la conexión WAN Telconet (WAN3). Además, garantiza que estas aplicaciones tengan alta prioridad en el uso del ancho de banda, reservando al menos el 50% del total disponible

en WAN1, para asegurar un rendimiento constante y minimizar cualquier interrupción en el servicio.

Tabla 12 – Aplicaciones no críticas

Política para Aplicaciones No Críticas	
Aplicaciones Incluidas	Redes sociales, YouTube, Spotify
Enlace Principal	Internet Small Business (WAN2)
Enlace Secundario (Failover)	Internet Corporativo (WAN1)
Enlace de Respaldo	WAN Telconet (WAN3)
QoS (Calidad de Servicio)	Baja prioridad, ancho de banda limitado al 20% del total disponible en WAN2

Fuente: Elaboración propia

Esta política establece que el tráfico se dirigirá principalmente a través del enlace de Internet Small Business (WAN2). En caso de fallo de este enlace, se utilizará el enlace de Internet Corporativo (WAN1) como secundario, y si ambos fallan, se recurrirá al enlace de respaldo WAN Telconet (WAN3). Además, se asignará una baja prioridad a estas aplicaciones, limitando su ancho de banda al 20% del total disponible en WAN2, garantizando así que los recursos de red se concentren en aplicaciones más críticas.

Además de estas políticas es crucial considerar las siguientes configuraciones:

- Balanceo de Carga:
    - Se configurará el balanceo de carga entre los enlaces WAN para distribuir el tráfico de manera eficiente y evitar la saturación de un único enlace.
    - Se asignará un peso mayor al Internet Corporativo para aplicaciones críticas y un peso menor al Internet Small Business para tráfico general.
- Failover:
    - Se establecerá políticas de failover que automaticen la redirección del tráfico en caso de caída de un enlace.
    - Se asegurará que el tráfico crítico tenga una ruta de respaldo eficiente a través de los otros enlaces WAN.

- Prioridades de Tráfico:
    - Se configurará QoS para priorizar el tráfico de aplicaciones críticas sobre las aplicaciones no críticas.
    - Se establecerá clases de servicio para asignar el tráfico a estas clases según la criticidad y el tipo de aplicación.
- Garantía de Ancho de Banda:
    - Se reservará ancho de banda específico para aplicaciones críticas en cada enlace WAN para asegurar su funcionamiento sin interrupciones.
    - Se limitará el ancho de banda para aplicaciones no críticas para evitar que saturen la red.
- Rutas Estáticas:
    - Se configurará rutas estáticas para aplicaciones o servicios específicos que requieran un enlace WAN en particular.
    - Se utilizará rutas estáticas para asegurar que ciertos tipos de tráfico siempre utilicen el mismo enlace.
- Rutas Dinámicas:
    - Se implementará protocolos de enrutamiento dinámico para adaptar las rutas de manera automática según las condiciones de la red.
    - Se ajustará las métricas de enrutamiento para preferir ciertos enlaces WAN para tipos de tráfico específicos.
- Monitorización Continua:
    - Implementar herramientas de monitorización continua para supervisar el rendimiento de los enlaces WAN.
    - Utilizar estos datos para ajustar las políticas de enrutamiento según sea necesario.

El balanceo de carga asegura una distribución eficiente del tráfico entre enlaces WAN, priorizando el Internet Corporativo para aplicaciones críticas y asignando menos peso al Internet Small Business para tráfico general. Las políticas de failover garantizan continuidad operativa al redirigir tráfico a enlaces alternativos durante fallos o caídas de enlace. Con QoS, se optimiza la gestión del tráfico, priorizando aplicaciones esenciales como ERP y videoconferencias para mejorar la experiencia del usuario y la eficiencia operativa. Además, se reservará ancho de banda específico para aplicaciones críticas y se establecerán rutas estáticas y dinámicas para gestionar el tráfico de manera efectiva, asegurando siempre rutas disponibles y ajustando métricas según las condiciones de red. Por último, la monitorización continua permite supervisar y ajustar las políticas de enrutamiento según sea necesario, asegurando un rendimiento óptimo de los enlaces WAN.

Implementación Técnica en Fortinet SD-WAN

Como parte técnica de la definición de políticas de enrutamiento y seguridad se anexan ejemplos de las configuraciones a realizar en la interfaz FortiGate una vez se tenga acceso a los servicios SD-WAN para la futura implementación, estos ejemplos están basados en las IPs de la agencia de prueba, para las demás agencias se deberá cambiar las IPs según corresponda.

1. Configuración de Interfaces WAN

- Definir las interfaces WAN en el FortiGate SD-WAN:
    - Acceder a la interfaz web de FortiGate.
    - Navegar a *Network* > *Interfaces*.
    - Configurar las interfaces de la siguiente manera:

Tabla 13 – Configuración interfaces WAN

Interfaz	Nombre	Dirección IP	Máscara de Subred	Puerta de Enlace	Comentarios
WAN1	Internet Corporativo	172.19.7.0	255.255.255.0	172.19.7.1	Enlace principal
WAN2	Internet Small Business	192.168.100.0	255.255.255.0	192.168.100.1	Enlace secundario
WAN3	WAN Telconet	172.21.7.1	255.255.255.248	172.21.7.2	Enlace de respaldo (MPLS)

Fuente: Elaboración propia

Se utilizará estas configuraciones para distribuir el tráfico de red de manera eficiente y balanceada, en conjunto con las políticas definidas anteriormente, las cuales a continuación se mostrará como implementarlas de manera técnica desde FortiGate.

2. Configuración de rutas estáticas

- Configurar rutas estáticas:
    - Navegar a *Network > Static Routes*.
    - Agregar las rutas necesarias:

Tabla 14 – Configuración de rutas estáticas

Dirección de Destino	Máscara de Subred	Puerta de Enlace	Interfaz	Prioridad
0.0.0.0	0.0.0.0	172.19.7.1	WAN1	10
0.0.0.0	0.0.0.0	192.168.100.1	WAN2	20
0.0.0.0	0.0.0.0	172.21.7.2	WAN3	30

Fuente: Elaboración propia

Esta configuración de rutas estáticas permite a SD-WAN dirigir el tráfico de red de manera eficiente y asegurarse de que siempre haya una ruta disponible para el tráfico de salida de la siguiente manera:

- WAN1 (Prioridad 10): Es la ruta principal y se utiliza siempre que esté disponible.
- WAN2 (Prioridad 20): Es la ruta secundaria y se utiliza si la ruta principal (WAN1) falla.

- WAN3 (Prioridad 30): Es la ruta de respaldo y se utiliza solo si las dos primeras rutas no están disponibles.

3. Definir políticas de enrutamiento:

- Navegar a *Policy & Objects > IPv4 Policy*.
- Crear políticas para el tráfico crítico y no crítico:

Tabla 15 – Política para aplicaciones críticas

Nombre	Entrada	Salida	Fuente	Destino	Servicio	Acción	Nat	Schedule
Traffic_Critical	LAN	WAN1	Todo	Todo	Todo	Permitir	Activado	Siempre

Fuente: Elaboración propia

Tabla 16 – Política para aplicaciones no críticas

Nombre	Entrada	Salida	Fuente	Destino	Servicio	Acción	Nat	Schedule
Traffic_NonCritical	LAN	WAN2	Todo	Todo	Todo	Permitir	Activado	Siempre

Fuente: Elaboración propia

Con la política estas políticas dirigiremos el tráfico crítico desde la red local (LAN) a la interfaz WAN1, que es el enlace principal de Internet corporativo para asegurarnos que el tráfico importante y sensible siempre tenga acceso a la mejor conexión disponible, activaremos NAT para asegurarnos que el tráfico pueda salir correctamente a Internet con una dirección IP pública adecuada. Por otro lado, también dirigiremos el tráfico no crítico desde la red local (LAN) a la interfaz WAN2, que es el enlace secundario de Internet Small Business, así el tráfico menos importante use un enlace diferente, reservando el ancho de banda del enlace principal para el tráfico crítico. Igualmente se tendrá NAT activado para asegurar que este tráfico pueda salir a Internet correctamente.

4. Definir perfiles de tráfico (QoS):

- Navegar a *Policy & Objects > Traffic Shaping* y crear los perfiles de tráfico.

En este apartado se deberá colocar el nombre del perfil de tráfico, la garantía de ancho de banda y el límite de esta, así crearemos dos perfiles de tráfico, uno crítico y otro para el tráfico no crítico colocándolo de la siguiente manera:

- Nombre: Critical_Traffic
    - Garantía de ancho de banda: 50%
    - Límite de ancho de banda: 80%
- Nombre: NonCritical_Traffic
    - Garantía de ancho de banda: 20%
    - Límite de ancho de banda: 50%

Critical_Traffic garantizará que el tráfico crítico siempre tenga asignado al menos el 50% del ancho de banda disponible, con un límite máximo del 80% para que las aplicaciones y servicios más importantes mantengan un rendimiento adecuado, incluso en condiciones de alta demanda de la red.

NonCritical_Traffic garantizará que el tráfico no crítico tenga asignado al menos el 20% del ancho de banda disponible, con un límite máximo del 50% para que el tráfico menos prioritario siga teniendo acceso a los recursos de la red, pero sin afectar significativamente el rendimiento del tráfico crítico.

5. Aplicar perfiles de tráfico en las políticas de enrutamiento:

- Navegar *a Policy & Objects > IPv4 Policy*.
- Editar las políticas *Traffic_Critical* y *Traffic_NonCritical*.
- Asignar los perfiles de tráfico correspondientes en la sección de *Traffic Shaping*.

Traffic_Critical: Al asignar el perfil *Critical_Traffic* a esta política, garantizaremos que el tráfico etiquetado como crítico reciba al menos el 50% del ancho de banda disponible y tenga un límite máximo del 80%.

Traffic_NonCritical: Al asignar el perfil *NonCritical_Traffic* a esta política, garantizaremos que el tráfico no crítico reciba al menos el 20% del ancho de banda disponible y tenga un límite máximo del 50%.

6. Configurar balanceo de carga:

- Navegar a *Network > SD-WAN Rules*.
    - Agregar una nueva regla de Balanceo de Carga:

Tabla 17 – Regla de balanceo de carga

Nombre	Interfaz de salida	Método de Balanceo	Peso
Load_Balancing	WAN1, WAN2, WAN3	Spillover	WAN1 (10), WAN2 (20), WAN3 (30)

Fuente: Elaboración propia

Esta regla permitirá al FortiGate administrar el tráfico saliente distribuyéndolo de manera equitativa o priorizada entre las interfaces WAN configuradas (WAN1, WAN2, WAN3) según las condiciones de la red y los pesos asignados. Se coloca el método de balanceo como "Spillover" ya que se utilizará un método de balanceo de carga basado en prioridades.

7. Configurar failover:

- Navegar a *Network > SD-WAN Rules*.
    - Agregar una nueva regla de failover:

Tabla 18 – Regla de failover

Nombre	Interfaz de Salida	Método de Enrutamiento	SLA Monitor	SLA Prioridad
Failover_Rule	WAN1, WAN2, WAN3	SLA basado en rendimiento	Activar monitorización para pérdida de paquetes, latencia y jitter	WAN1 (1), WAN2 (2), WAN3 (3)

Fuente: Elaboración propia

Esta regla failover se activará automáticamente si se detecta que una interfaz WAN no cumple con los parámetros de rendimiento definidos en los SLA (Service Level Agreements) configurados. Lo que significa que, en caso de que WAN1 falle o no cumpla con los SLA establecidos, el tráfico se dirigirá automáticamente a WAN2 si está disponible y cumple con los SLA, y así sucesivamente. Esto se establecerá por la monitorización que se explica a continuación.

8. Implementar herramientas de monitorización

- Instalar y configurar *FortiManager y FortiAnalyzer*.
- Configurar alertas y reportes para supervisar el rendimiento de los enlaces WAN.
    - *Dashboard > Widgets:*

Tabla 19 – Monitoreo en tiempo real

Monitoreo en tiempo real	
Fuente	Todo
Destino	FortiManager
Servicio	Todo
Acción	Permitir
Comentarios	Monitorea en tiempo real el tráfico y eventos de seguridad en la red.
Configuración adicional	Configurar Dashboard con widgets para monitoreo en tiempo real.

Fuente: Elaboración propia

    - *Log & Report > Log Settings:*

Tabla 20 – Registro de eventos de seguridad

Registro de eventos de seguridad	
Fuente	Todo
Destino	FortiAnalyzer
Servicio	Todo
Acción	Permitir
Comentarios	Asegura que todos los eventos de seguridad sean registrados para análisis posterior.
Configuración adicional	Configurar Log Settings para enviar logs a FortiAnalyzer

Fuente: Elaboración propia

9. Ajustar configuraciones según los datos de monitorización:

- Revisar los reportes de monitorización regularmente.
- Ajustar las políticas de enrutamiento y QoS según las tendencias y patrones observados.
- Realizar pruebas de rendimiento periódicamente para asegurar que los ajustes están mejorando la eficiencia de la red.

Definición de políticas de seguridad utilizando funciones integradas de FortiGate

1. Políticas de Seguridad Básica

Tabla 21 – Bloqueo de tráfico no autorizado

Bloqueo de tráfico no autorizado (Entrante)	
Fuente	Todo (Externo)
Destino	Todo (Interno)
Servicio	Todo
Acción	Denegar
Comentarios	Bloquea cualquier tráfico no autorizado de fuentes externas.

Fuente: Elaboración propia

Crear Política para Bloqueo de tráfico no autorizado:

- Navegar a: *Policy & Objects > IPv4 Policy:*

Tabla 22 – Política de bloqueo de tráfico no autorizado

Nombre de la Política	**Bloquear_Trafico_No_Autorizado**
Origen	Seleccionar la interfaz WAN
	Todo (Para bloquear todo el tráfico entrante desde cualquier dirección IP en Internet)
Destino	Seleccionar la interfaz LAN
	Todo (Para bloquear todo el tráfico hacia cualquier dirección IP en la red interna)
Servicio	Todo (Para bloquear todos los servicios y puertos)
Acción	Denegar
Log Denied Traffic	Habilitar para monitorear y registrar el tráfico bloqueado

Fuente: Elaboración propia

Con esta política nos aseguraremos de que cualquier intento de tráfico no autorizado desde Internet hacia la red interna a través de la interfaz LAN sea bloqueado de manera efectiva, protegiendo así la seguridad y la integridad de la red interna contra posibles amenazas externas. Esta política estará ubicada después de las políticas específicas que permiten tráfico legítimo (como las políticas para permitir tráfico web y de correo electrónico que veremos a continuación).

Tabla 23 – Permitir tráfico web

Permitir tráfico web (HTTP/HTTPS)	
Fuente	Todo (Interno)
Destino	Todo (Externo)
Servicio	HTTP, HTTPS
Acción	Permitir
Comentarios	Permite el tráfico web estándar para usuarios internos.

Fuente: Elaboración propia

Crear Política para Permitir tráfico web (HTTP/HTTPS):

- Navegar a: *Policy & Objects > IPv4 Policy:*

Tabla 24 – Política para permitir tráfico web

Nombre de la Política	**Permitir_Web_HTTP_HTTPS**
Origen	Selecciona la interfaz WAN
	Todo (Permitir tráfico desde cualquier dirección IP en Internet)
DESTINO	Seleccionar la interfaz LAN
	Servidor Web Interno
Servicio	HTTP, HTTPS
Acción	Permitir
NAT	Habilitar NAT si es necesario para traducir el tráfico
Log Allowed Traffic	Habilitar para monitorear el tráfico permitido

Fuente: Elaboración propia

Con esta política nos aseguraremos de que el tráfico web HTTP y HTTPS desde Internet hacia nuestra interfaz LAN en la red interna sea permitido de manera controlada y segura, facilitando así el acceso a servicios web públicos mientras nos protegerá la red interna contra tráfico no deseado. Tendremos que monitorear los logs para asegurarse de que solo el tráfico web autorizado está siendo permitido hacia el servidor web interno.

Tabla 25 - Permitir tráfico de correo

Permitir tráfico de correo electrónico (SMTP, IMAP, POP3)	
Fuente	Todo (Interno)
Destino	Todo (Externo)
Servicio	SMTP, IMAP, POP3
Acción	Permitir
Comentarios	Permite el envío y recepción de correos electrónicos.

Fuente: Elaboración propia

Crear Política Para Permitir tráfico de correo electrónico (SMTP, IMAP, POP3):

- Navegar a: *Policy & Objects > IPv4 Policy:*

Tabla 26 – Política para permitir tráfico de correo

Nombre de la Política	Permitir_Correo_SMTP_IMAP_POP3
Origen	Seleccionar la interfaz LAN
	SMTP, IMAP, POP3
Destino	Seleccionar la interfaz WAN
	Todo (Permitir tráfico hacia cualquier dirección IP en Internet)
Servicio	SMTP, IMAP, POP3
Acción	Permitir
NAT	Habilitar NAT si es necesario para traducir el tráfico
Log Allowed Traffic	Habilitar para monitorear el tráfico permitido

Fuente: Elaboración propia

Esta política asegurará que los usuarios dentro de la red LAN puedan enviar, recibir y acceder al correo electrónico utilizando los protocolos estándar SMTP, IMAP y POP3, facilitando así la comunicación eficiente y segura con servidores de correo externos. Igualmente tendremos que monitorear los logs para asegurarse de que solo el tráfico de correo autorizado está siendo permitido.

Tabla 27 – Permitir tráfico DNS

Permitir tráfico de DNS	
Fuente	Todo (Interno)
Destino	Todo (Externo)
Servicio	DNS
Acción	Permitir
Comentarios	Permite la resolución de nombres de dominio.

Fuente: Elaboración propia

Crear Política Para Permitir tráfico de DNS

- Navegar a: *Policy & Objects > IPv4 Policy:*

Tabla 28 – Política para permitir tráfico DNS

Nombre de la Política	Permitir_Trafico_DNS
Origen	Seleccionar la interfaz LAN
	Todo (Para permitir tráfico desde cualquier dirección IP en la red interna)
Destino	Seleccionar la interfaz WAN
	Servidores DNS
Servicio	Seleccionar DNS para permitir tanto UDP/53 como TCP/53
Acción	Permitir
Log Allowed Traffic	Habilitar para monitorear y registrar el tráfico permitido

Fuente: Elaboración propia

Esta política asegurará que los dispositivos dentro de la red LAN puedan realizar consultas de resolución de nombres DNS hacia servidores DNS externos en Internet, facilitando así la navegación web y la comunicación con recursos basados en nombres de dominio fuera de la red local. Tendremos que asegurarnos de que esta política esté ubicada antes de cualquier política que bloquee el tráfico general.

2. Políticas de Protección Contra Amenazas

Tabla 29 – Filtrado de contenidos maliciosos

Filtrado de URL y contenidos maliciosos	
Fuente	Todo (Interno)
Destino	Todo (Externo)
Servicio	HTTP, HTTPS
Acción	Permitir
Comentarios	Aplica filtrado de URL y contenido para bloquear sitios maliciosos y contenido no deseado.
Configuración adicional	Activar *Web Filtering* y definir categorías a bloquear (malware, phishing, sitios de apuestas).

Fuente: Elaboración propia

Crear Política para Filtrado de Contenidos Maliciosos:

- Navegar a: *Policy & Objects > IPv4 Policy:*

Tabla 30 – Política pata filtrado de contenidos malicioso

Nombre	**Entrada**	**Salida**	**Fuente**	**Destino**	**Servicio**	**Acción**	**Nat**	**Configuración de Seguridad**	**Perfil de Seguridad**
Block_Malicious_Content	LAN	WAN1	Todo (Interno)	Todo (Externo)	HTTP, HTTPS	Permitir	Activado	Activar Web Filtering y Antivirus	Aplicar perfiles predeterminados o personalizados

Fuente: Elaboración propia

Con esta política se asegurará que todo el tráfico saliente de HTTP y HTTPS desde la red interna hacia Internet sea examinado en busca de contenido malicioso mediante filtrado web y antivirus, con el objetivo de proteger la red corporativa contra amenazas en línea.

Tabla 31 – Control de aplicaciones

Política de Control de aplicaciones	
Fuente	Todo (Interno)
Destino	Todo (Externo)
Servicio	Todo
Acción	Permitir
Comentarios	Controla el uso de aplicaciones en la red para evitar el uso de aplicaciones no autorizadas.
Configuración adicional	Activar Application Control y definir aplicaciones a bloquear.

Fuente: Elaboración propia

Crear Política de Control de Aplicaciones:

- Definir el Horario de Trabajo
  - Acceso: *System > Schedule > Recurring:*
  - A continuación, se crea el horario laboral en base a las normativas de la empresa de la siguiente manera:
    - Nombre: *Horario_Laboral*
    - Días de la semana: Monday, Tuesday, etc.
    - Horas: Horaria Laboral (09:00 – 18:00)
- Configurar la Categoría de Aplicaciones
  - Acceso: *Security Profiles > Application Control:*
  - A continuación, se crea las aplicaciones a controlar por categoría de la siguiente manera:
    - Nombre: *Bloqueo_Redes_Sociales*
    - Categorías: Social Media, Instant Messaging, etc.
- Política de Seguridad
  - Acceso: *Policy & Objects > IPv4 Policy:*

Tabla 32 – Política de control de aplicaciones

Nombre de la Política	Bloqueo_Redes_Sociales_Horario_Laboral
Origen	LAN
Destino	WAN
Servicio	Todo
Programación	Horario_Laboral
Acción	Denegar
Aplicación Control	Bloqueo_Redes_Sociales
Registro	Habilitar para monitoreo

Fuente: Elaboración propia

Esta política de control de aplicaciones restringirá el acceso a redes sociales y mensajería instantánea durante las horas laborales establecidas, ayudando a mantener la productividad y la seguridad al limitar el uso de aplicaciones que podrían distraer o comprometer la red.

Tabla 33 - Protección contra intrusiones

Protección contra intrusiones (IPS)	
Fuente	Todo (Interno)
Destino	Todo (Externo)
Servicio	Todo
Acción	Permitir
Comentarios	Aplica políticas de IPS para detectar y bloquear actividades de intrusión.
Configuración adicional	Activar IPS y aplicar el perfil de seguridad IPS predeterminado o personalizado.

Fuente: Elaboración propia

Configuración de Política IPS:

- Crear un Perfil de Protección contra Intrusiones
  - *Security Profiles* > *Intrusion Prevention* > *Create New*:

Tabla 34 - Perfil IPS

Nombre de la Política	Política_IPS_Activada
Origen	Todo (Interno)
Destino	Todo (Externo)
Servicio	Todo
Acción	Permitir
Perfiles de Seguridad	IPS
Configuración de IPS	Perfil IPS (predeterminado o personalizado)
Comentarios	Aplica políticas de IPS para detectar y bloquear actividades de intrusión.

Fuente: Elaboración propia

- Asignar el Perfil de IPS a una Política
  - *Policy & Objects > IPv4 Policy > Política Existente*
  - Dentro de la configuración de la política en la sección *Security Profiles*, se selecciona el perfil de IPS configurado previamente.

Realizando esta configuración global se permitirá que el tráfico interno y saliente sea inspeccionado por el IPS que examinará el tráfico de red en busca de actividades maliciosas o anómalas que puedan indicar intentos de intrusión o ataques, mejorando así la seguridad general de la infraestructura.

Tabla 35 – Inspección de tráfico antivirus

Inspección de tráfico antivirus	
Fuente	Todo (Interno)
Destino	Todo (Externo)
Servicio	HTTP, HTTPS, SMTP, POP3, IMAP
Acción	Permitir
Comentarios	Escanea el tráfico en busca de malware y virus.
Configuración adicional	Activar Antivirus y aplicar el perfil de seguridad antivirus predeterminado o personalizado.

Fuente: Elaboración propia

Configuración de Política de Inspección de Tráfico Antivirus:

- Crear un Perfil de Antivirus
  - *Security Profiles > Antivirus > Create New*

Tabla 36 – Perfil de Antivirus

Nombre de la política	**Antivirus_Protection_Policy**
Acciones	Eliminar, Bloquear, Permitir con advertencia
Opciones Avanzadas	
Tipo de Archivos por Escanear	Definir qué tipo de archivos vamos a escanear
Inspección SSL	Activar la inspección SSL para escanear el tráfico cifrado

Fuente: Elaboración propia

- Asignar el Perfil de Antivirus a una Política
  - *Policy & Objects > IPv4 Policy > Política Existente*
  - Dentro de la configuración de la política en la sección *Security Profiles*, selecciona el perfil de Antivirus configurado previamente.

Con esta configuración se creará un perfil de antivirus que permite al firewall FortiGate escanear archivos y tráfico en busca de malware y virus. Tendremos que definir acciones como eliminar, bloquear o permitir con advertencia para archivos sospechosos. Finalmente, este perfil se deberá asignar a una política de seguridad existente para proteger eficazmente contra amenazas en el tráfico de red.

Configuración de VPN:

- Navegar a: *VPN > SSL-VPN Settings*
- Habilitar SSL-VPN:
- A continuación, debemos configurar la VPN de la siguiente manera:
  - Puerto: 10443
  - Interface: WAN1
  - Modo: Tunnel Mode

Esta configuración permite a los usuarios remotos conectarse a la red corporativa desde cualquier ubicación, garantizando que los datos transmitidos estén protegidos contra interceptaciones y accesos no autorizados. En el caso de las agencias que gestiona Centric S.A. Fortinet facilitará el acceso seguro a los recursos del data center en Telconet,

aplicaciones empresariales, servidores y bases de datos para empleados que trabajen desde ubicaciones remotas o externas. A continuación, se indica como se debe definir el rango de IPs para asignar a los usuarios VPN y las políticas para que esta conexión se realice de manera segura.

- Configurar Rango de IPs:
  - Rango de IP: 10.10.10.1 - 10.10.10.100
- Configurar Políticas de Acceso VPN:
  - Navegar a: *Policy & Objects > IPv4 Policy:*

Tabla 37 – Acceso a VPN

Nombre	Entrada	Salida	Fuente	Destino	Servicio	Acción
SSL_VPN_Access	SSL-VPN Tunnel Interface	LAN	Todo (VPN Users)	Recursos Internos	Todo	Permitir

Fuente: Elaboración propia

Para esta política se definirá un rango de direcciones IP para asignar a los usuarios VPN. También se configurará políticas de acceso VPN que permiten el tráfico desde la interfaz SSL-VPN Tunnel hacia la LAN, permitiendo a los usuarios de VPN acceder a recursos internos a través de esta conexión segura.

3. Políticas de Acceso y Autenticación:

Tabla 38 – Permitir Acceso VPN seguro

Permitir acceso VPN seguro	
Nombre	Permitir_Acceso_VPN_Seguro
Entrada	SSL.ROOT O IPSEC
Salida	LAN
Origen	Todo (VPN)
Destino	Recursos Internos
Servicio	Todo
Acción	Permitir
Comentarios	Permite el acceso remoto seguro a la red interna a través de VPN.
Configuración adicional	Configurar IPsec VPN o SSL VPN y definir los usuarios/grupos que pueden accede

Fuente: Elaboración propia

Está política permitirá el acceso seguro desde conexiones VPN hacia la red interna (LAN) se definirá que cualquier tráfico proveniente de usuarios VPN tenga acceso a todos los recursos internos de la red, utilizando cualquier tipo de servicio.

Tabla 39 – Control de acceso interno basado en roles

Control de acceso interno basado en roles	
Nombre	Control_Acceso_Basado_En_Roles
Entrada	LAN
Salida	LAN
Origen	Usuarios Internos
Destino	Recursos Internos
Servicio	Todo
Acción	Permitir
Comentarios	Define qué recursos pueden acceder diferentes usuarios basados en roles.
Configuración adicional	Implementar *User Groups* e *Identity-Based Policies* para especificar los permisos de acceso.

Fuente: Elaboración propia

Con esta política se establecerá un control de acceso interno basado en roles dentro de la red LAN que permitirá a los usuarios internos acceder a recursos específicos dentro de la misma red, utilizando cualquier servicio necesario.

4.2. PLANIFICACIÓN DE LA GESTIÓN DEL CAMBIO

El plan de gestión del cambio para la implementación de SD-WAN en la agencia se centró en asegurar una transición suave y minimizar la resistencia al cambio a través de una comunicación efectiva y capacitación adecuada. Se identificaron diversas partes interesadas clave, y la mejor manera de desarrollar mensajes clave adaptados a cada grupo, utilizando una variedad de canales de comunicación. Además, se estableció un plan de soporte y monitoreo para garantizar la continuidad del servicio y minimizar el tiempo de inactividad durante y después de la implementación de SD-WAN en un futuro.

4.2.1. Desarrollo de un plan de comunicación

Identificar a todas las partes interesadas clave asegura que cada grupo relevante esté al tanto de cómo el proyecto afectará sus operaciones y responsabilidades. Elaborar

mensajes clave específicos para cada grupo, desde la alta dirección hasta los usuarios finales y los reguladores, garantiza que la información sea relevante y útil para cada audiencia. La selección cuidadosa de canales de comunicación adecuados, como reuniones ejecutivas, boletines informativos, sesiones de capacitación y correos electrónicos dirigidos, facilita la difusión efectiva de información en diferentes niveles de la organización. Este enfoque integral no solo mejora la transparencia y la alineación entre las diferentes áreas, sino que también fomenta el apoyo continuo y la participación en el éxito del proyecto de SD-WAN.

Para identificar a todas las partes interesadas de manera efectiva, se revisó claramente el alcance del proyecto de implementación de SD-WAN, identificando qué áreas y grupos dentro de la agencia podrían verse afectados o tener interés en los resultados del proyecto. Se incluyó también a grupos de interés externos como proveedores de servicios y reguladores, para garantizar que todas las perspectivas pertinentes fueran consideradas desde el inicio del proyecto hasta su implementación. A continuación, se presenta la Tabla de las partes interesadas en el proyecto:

Tabla 40 – Partes Interesadas

Áreas Interesadas	Influencia	Interés	Estrategia de Gestión
Gerente General	Alta	Alta	Involucrar en la toma de decisiones clave
Jefe de Sistemas	Alta	Alta	Consulta continua y reporte regular
Jefe de Infraestructura	Alta	Alta	Responsable directo del proyecto
Equipo de Infraestructura	Media	Alta	Capacitación y apoyo continuo
Personal Administrativo	Baja	Alta	Informar y capacitar
Equipo de Ventas	Baja	Media	Informar sobre beneficios
Equipo de Atención al Cliente	Baja	Media	Informar sobre beneficios
Clientes	Baja	Media	Mantener informados
Proveedores	Baja	Media	Mantener informados
Proveedor de SD-WAN (Fortinet)	Alta	Alta	Colaboración estrecha
Consultores de TI	Alta	Alta	Colaboración estrecha
Director Financiero	Alta	Media	Informes de progreso y costo
Contabilidad	Media	Baja	Informar sobre necesidades financieras
Jefe de Desarrollo Organizacional	Media	Media	Plan de gestión de cambio
Equipo de Capacitación	Media	Media	Desarrollar programas de formación
Oficial de Cumplimiento	Alta	Media	Asegurar cumplimiento normativo
Agencias Reguladoras	Alta	Media	Cumplir con requerimientos normativos

Fuente: Elaboración propia

Con las partes interesadas ya definidas se revisó los parámetros necesarios para elaborar los mensajes claves por grupo, es importante destacar que se debe utilizar un lenguaje claro y formatos de comunicación adecuados a las preferencias de cada parte interesada. Es importante establecer canales para recibir retroalimentación y ajustar los mensajes según sea necesario para mantener la relevancia y el compromiso de las partes con el proyecto.

Se tomó en cuenta lo siguientes aspectos:

- Necesidades e Intereses: Comprender qué es importante para cada grupo interesado en relación con el proyecto.
- Objetivos del Proyecto: Comunicar claramente cuáles son los objetivos y metas del proyecto de implementación de SD-WAN.

- Beneficios Esperados: Comunicar los beneficios específicos que el proyecto aportará a cada grupo.
- Impacto y Cambios: Indicar como el proyecto afectará a las partes interesadas y qué cambios pueden esperar.
- Lenguaje y Formato: Utilizar un lenguaje claro y directo que sea comprensible para cada grupo.

A continuación, se anexan 2 ejemplos de mensajes clave para los grupos de Alta Dirección y Usuarios finales internos, de esta manera se tendrá más claro los parámetros revisados:

Tabla 41 – Mensajes clave para la alta dirección

Mensajes Clave para la Alta Dirección	
Objetivo del Proyecto	La implementación de SD-WAN permitirá a la agencia del Grupo Baca optimizar el uso de sus recursos de red, mejorando la eficiencia operativa y reduciendo los costos asociados a la gestión de la red.
Beneficios Estratégicos	SD-WAN proporcionará una mayor resiliencia y flexibilidad en la red, facilitando la rápida adaptación a cambios en el mercado y soportando la expansión de nuestras operaciones.
Impacto Financiero	La inversión en SD-WAN se recuperará rápidamente gracias a la reducción de los costos operativos y al incremento de la productividad, proporcionando un retorno de inversión significativo en el corto plazo.

Fuente: Elaboración propia

Tabla 42 – Mensajes clave para usuarios finales internos

Mensajes Clave para Usuarios Finales Internos	
Beneficios para el Personal Administrativo	Con SD-WAN, la conexión a nuestras aplicaciones corporativas será más rápida y confiable, mejorando la eficiencia y la productividad en tus labores diarias.
Beneficios para el Equipo de Ventas	La nueva infraestructura permitirá un acceso más ágil a las herramientas de CRM, S3S y otros sistemas de ventas, facilitando la gestión de clientes y mejorando tu capacidad de respuesta.
Beneficios para el Equipo de Atención al Cliente	SD-WAN asegurará una conectividad estable y de alta calidad, permitiéndote atender mejor a los clientes y resolver sus requerimientos con mayor rapidez

Fuente: Elaboración propia

Una vez definida la manera correcta para redactar los mensajes clave se establecieron los diferentes canales de comunicación considerando los siguientes factores clave que

asegurarán que cada parte interesada en la implementación reciba la información de manera efectiva:

- Nivel de Influencia y Poder de Decisión
- Necesidad de Información Detallada y Técnica
- Frecuencia de Comunicación Necesaria
- Formato de Información
- Accesibilidad y Conveniencia
- Propósito de la Comunicación

A continuación, se anexan los canales de comunicación que aseguran que cada grupo recibirá la información necesaria a través del medio más adecuado, facilitando una comunicación efectiva cuando se realicé la implementación de SD-WAN:

Tabla 43 – Canales de comunicación

Grupos Interesados	Canales de Comunicación
Alta Dirección	Reuniones Ejecutivas (semanal), Informes Ejecutivos (mensual)
Departamento de TI	Reuniones de Equipo de TI (semanal), Plataforma de Gestión de Proyectos (diaria), Chat Corporativo (diaria)
Usuarios Finales Internos	Boletín Informativo Interno (quincenal), Sesiones de Capacitación (antes y durante la implementación)
Usuarios Finales Externos	Correo Electrónico a Proveedores (antes y después de la implementación)
Socios y Consultores Externos	Reuniones de Progreso del Proyecto (quincenal), Informes Técnicos (mensual)
Departamento de Contabilidad	Reuniones de Revisión de Presupuesto (mensual), Informes Financieros (mensual)
Departamento de Desarrollo Organizacional	Reuniones de Coordinación de Capacitación (semanal durante la capacitación), Boletines Internos (quincenal)
Reguladores y Compliance	Reuniones de Cumplimiento (trimestral), Informes de Cumplimiento (según normativa)

Fuente: Elaboración propia

4.2.2. Propuesta para capacitación al personal de TI

Es importante realizar esta capacitación para garantizar que el equipo de TI esté completamente preparado para manejar la nueva infraestructura, lo que permitirá una

implementación eficiente, una gestión continua sin problemas, y la maximización de los beneficios de la tecnología SD-WAN para la empresa.

Para garantizar un proceso de aprendizaje organizado, eficiente y efectivo se ha realizado una Estructura del Programa de Capacitación que asegure que todos los temas relevantes sean cubiertos, que los participantes progresen de manera lógica desde conceptos básicos a avanzados, y que se maximice el aprovechamiento del tiempo y recursos disponibles. Esto se logró tomando en cuenta los siguientes aspectos:

- Definir los Objetivos de Aprendizaje
- Desarrollar un Contenido Detallado
- Organizar los Módulos de Capacitación
- Seleccionar Métodos de Enseñanza
- Asignar Instructores y Recursos
- Establecer un Cronograma
- Incorporar Evaluaciones y Retroalimentación

A continuación, se anexa la estructura del programa de capacitación elaborada:

Tabla 44 – Programa de capacitación TI

Tema por revisar	Duración	Formato	Contenido
Introducción a SD-WAN y FortiGate	1 día	Presentación teórica y demostración práctica	- Fundamentos de SD-WAN: Conceptos y arquitectura - Beneficios de SD-WAN para la agencia - Introducción a FortiGate y sus capacidades SD-WAN - Revisión del proyecto de implementación de SD-WAN en la agencia
Configuración Básica de FortiGate SD-WAN	2 días	Taller práctico	- Instalación de dispositivos FortiGate - Configuración inicial de SD-WAN - Configuración de enlaces WAN (Internet Corporativo, Small Business, MPLS) - Creación de políticas básicas de enrutamiento
Gestión y Monitorización de SD-WAN	2 días	Taller práctico	- Uso de la interfaz de gestión de FortiGate - Monitorización del rendimiento de la red SD-WAN - Configuración de alertas y notificaciones - Prácticas de gestión y mantenimiento rutinario
Implementación de Políticas de Seguridad	1 día	Taller práctico	- Creación de políticas de firewall - Configuración de IPS (Sistema de Prevención de Intrusiones) - Implementación de inspección de tráfico antivirus - Gestión de VPNs y conexiones seguras
Resolución de Problemas y Soporte	2 días	Taller práctico y simulación de problemas	- Identificación y resolución de problemas comunes - Herramientas y técnicas para diagnóstico de red - Estrategias de recuperación ante fallos - Casos de estudio y simulaciones de incidentes

Capacitación Continua y Actualizaciones	Sesiones periódicas (1 día cada 3 meses)	Talleres y webinars	- Actualizaciones sobre nuevas características y versiones de FortiGate SD-WAN - Revisión de mejores prácticas y optimización de la red - Sesiones de resolución de problemas avanzados - Feedback y ajuste de políticas y configuraciones según las necesidades cambiantes

Fuente: Elaboración propia

Materiales y Recursos de Capacitación

- Documentación Técnica: Guías de usuario, manuales de configuración y documentos de mejores prácticas.
- Acceso a un Laboratorio Virtual: Entorno de simulación donde el personal puede practicar configuraciones y resolver problemas sin afectar la red en producción.
- Videos Tutoriales: Serie de videos que cubren diferentes aspectos de la configuración y gestión de SD-WAN.
- Soporte Post-Capacitación: Acceso a un canal de soporte dedicado para preguntas y asistencia continua.

Evaluación de la Capacitación

- Exámenes Teóricos: Evaluaciones al final de cada módulo para medir la comprensión teórica.
- Pruebas Prácticas: Tareas y simulaciones prácticas para evaluar la competencia en la configuración y resolución de problemas.
- Encuestas de Feedback: Recopilación de opiniones del personal sobre la calidad y efectividad de la capacitación.

- Revisión de Desempeño: Evaluación del desempeño del personal de TI en la gestión de la red SD-WAN durante los primeros tres meses post-implementación.

4.2.3. Plan de soporte y monitoreo durante y después de la implementación

Es crucial realizar un plan de soporte y monitoreo durante y después de la implementación de SD-WAN para garantizar que la red funcione de manera continua y eficiente, minimizando el tiempo de inactividad que podría afectar las operaciones diarias.

El plan de soporte durante la implementación asegurará la continuidad operativa de la red SD-WAN mediante un equipo dedicado on-site (en sitio) que supervisará la instalación y configuración inicial, además de ser complementado por soporte remoto. A continuación de adjunta la propuesta para el plan de soporte durante la implementación

Tabla 45 – Soporte durante la implementación

Soporte Durante la Implementación			
Equipos	**Responsabilidad**	**Disponibilidad**	**Tareas**
Equipo de Implementación On-site	Supervisar la instalación y configuración inicial de la infraestructura SD-WAN	Presente en el sitio durante todas las fases críticas de la implementación	- Verificación de la instalación del hardware. - Configuración inicial - Resolución de problemas inmediatos.
Equipo de Soporte Remoto	Proveer soporte adicional desde una ubicación remota	24/7 durante la fase de implementación	- Asistencia en tiempo real a través de herramientas de acceso remoto. - Respuesta a consultas y resolución de problemas técnicos.

Fuente: Elaboración propia

El plan de soporte post-implementación asegurará la continuidad operativa de la red SD-WAN mediante soporte técnico constante, actualización y mantenimiento del sistema, resolución de problemas y optimización de la red. Se adjunta la propuesta para este plan de soporte:

Tabla 46 – Soporte post-implementación

Soporte Post-Implementación			
Equipos	**Responsabilidad**	**Disponibilidad**	**Tareas**
Soporte Técnico Continuo	Proveer soporte técnico constante para la infraestructura SD-WAN	24/7 para emergencias; horario de oficina para soporte regular	- Resolución de problemas técnicos reportados. - Actualización y mantenimiento del sistema. - Asistencia en la optimización de la red.
Contratos de Soporte	Niveles de servicio definidos (SLA) para tiempo de respuesta y resolución	- Soporte básico: Respuesta dentro de las 24 horas. - Soporte avanzado: Respuesta dentro de las 4 horas. - Soporte crítico: Respuesta inmediata (1 hora).	- Respuesta y resolución de problemas dentro de los tiempos acordados según el nivel de soporte contratado.
Escalación de Problemas	Procedimientos claros de escalación y contactos	Según nivel de soporte	- Nivel 1: Soporte técnico básico. - Nivel 2: Especialistas en redes SD-WAN. - Nivel 3: Ingenieros senior y consultores externos.

Fuente: Elaboración propia

Para llevar a cabo el plan de monitoreo, implementaremos el Sistema de Gestión Centralizada FortiManager para la supervisión integral de los dispositivos FortiGate. Estableceremos procedimientos para la supervisión continua del rendimiento de los enlaces WAN y LAN, utilizando herramientas de detección de anomalías en el tráfico de red y sistemas de alertas proactivas. Generaremos informes periódicos que abarquen el estado de la red, el rendimiento de los enlaces, eventos de seguridad detectados y análisis de tendencias. Esto nos permitirá optimizar el uso del ancho de banda, fortalecer la seguridad y responder rápidamente a cualquier incidencia para garantizar la continuidad operativa y la eficiencia del sistema SD-WAN.

4.3. ESTRATEGIAS DE MITIGACIÓN DE RIESGOS

Revisaremos diversas estrategias de mitigación de riesgos específicamente diseñadas para abordar los desafíos asociados con la implementación de SD-WAN, destacando medidas preventivas clave para garantizar el éxito de la implementación y la protección de los activos empresariales críticos.

4.3.1. Identificación de riesgos asociados con la implementación de SD-WAN

Los riesgos asociados con la implementación de SD-WAN se basan en experiencias previas de implementaciones que han enfrentado estos tipos de riesgos, así como la documentación de proveedores y expertos. Estos riesgos pueden presentarte en cualquiera de los siguientes aspectos:

- Riesgos Técnicos
    - Fallas de Hardware
    - Problemas de Configuración
    - Incompatibilidad de Sistemas
- Riesgos de Seguridad:
    - Intrusiones y Ataques
    - Pérdida de Datos
    - Amenazas Internas
- Riesgos Operativos:
    - Interrupciones del Servicio
    - Capacitación Insuficiente
    - Dependencia de Proveedores

4.3.2. Desarrollo de planes de contingencia para cada riesgo identificado.

A continuación, se adjuntará los planes de contingencia elaborados para responder de manera rápida y efectiva ante los riesgos vistos anteriormente, garantizando que el proyecto se desarrolle de manera fluida y segura.

- Riesgos Técnicos
    - Fallas de Hardware:
        - Identificar la falla de hardware mediante monitoreo continuo.
        - Notificar al proveedor y solicitar reemplazo o reparación bajo el contrato de mantenimiento.
        - Implementar el equipo de repuesto si la reparación tarda más de 2 horas.
        - Validar la operación del nuevo equipo y actualizar la configuración si es necesario.
    - Problemas de Configuración:
        - Implementar cambios de configuración en un entorno de prueba.
        - Evaluar el impacto de las configuraciones en el rendimiento y seguridad.
        - Desplegar configuraciones aprobadas en la red de producción.
        - Monitorear el rendimiento post-implementación y revertir cambios si es necesario.
    - Incompatibilidad de Sistemas:
        - Realizar una auditoría completa de la infraestructura existente.
        - Probar la compatibilidad en un entorno controlado.
        - Implementar solo equipos y software compatibles.

        - Monitorear continuamente para detectar cualquier incompatibilidad emergente.

- Riesgos de Seguridad
    - Intrusiones y ataques:
        - Detectar intrusiones mediante sistemas de monitoreo continuo.
        - Activar respuestas automatizadas para bloquear intrusiones.
        - Notificar al equipo de seguridad y ejecutar un análisis detallado.
        - Implementar parches y actualizar políticas de seguridad.
    - Pérdida de datos:
        - Ejecutar copias de seguridad diarias de todos los datos críticos.
        - Almacenar copias de seguridad en ubicaciones geográficamente separadas.
        - En caso de pérdida de datos, iniciar el protocolo de recuperación.
        - Restaurar datos desde la copia de seguridad más reciente y verificar integridad.
    - Amenazas Internas:
        - Detectar actividad sospechosa a través de sistemas de monitoreo.
        - Iniciar investigación interna para identificar la fuente.
        - Tomar acciones correctivas, como ajustar permisos de acceso.
        - Reforzar políticas de seguridad y proporcionar capacitación adicional si es necesario.
- Riesgos Operativos
    - Interrupción del servicio:
        - Programar migración durante horarios de menor actividad.
        - Implementar cambios de manera incremental.

        - Monitorear continuamente durante y después de la migración.
        - Estar preparado para revertir cambios rápidamente si se detectan problemas.
    - Capacitación Insuficiente:
        - Identificar las necesidades de capacitación específicas.
        - Desarrollar y ejecutar un programa de capacitación detallado.
        - Realizar evaluaciones periódicas de competencia.
        - Proveer formación adicional y actualización continua.
    - Dependencia de proveedores:
        - Definir y acordar SLAs detallados con los proveedores.
        - Monitorear el cumplimiento de los SLAs mediante revisiones periódicas.
        - Mantener una lista de proveedores alternativos para emergencias.
        - Realizar revisiones regulares del desempeño de los proveedores y ajustar acuerdos si es necesario.

4.3.3. Marco para la evaluación continua del desempeño de SD-WAN

Para la futura implementación de SD-WAN, es crucial establecer métricas clave que permitan medir y evaluar de manera objetiva aspectos como la disponibilidad, latencia, utilización del ancho de banda y seguridad de la red. Estas métricas se seleccionarán en función de su relevancia para asegurar una operación efectiva y segura, utilizando herramientas adecuadas para monitorear y medir cada aspecto crucial del rendimiento y la seguridad.

Es importante señalar los siguientes puntos clave para que las métricas (KPIs) estén alineadas con los objetivos estratégicos y operativos de la empresa:

- Disponibilidad de la Red: Mantener un 99.99% de disponibilidad usando FortiManager.
- Tiempo de Respuesta: Latencia media < 50 ms, monitorizada con FortiAnalyzer.
- Utilización del Ancho de Banda: Mantener el uso < 80% con FortiGate.
- Tasa de Éxito de Failover: Alcanzar un 100% de conmutaciones exitosas usando FortiGate.
- Eficiencia de Balanceo de Carga: Equitativa distribución de tráfico con < 10% de desviación entre enlaces, evaluada con FortiAnalyzer.
- Detección y Mitigación de Amenazas: Lograr detectar y mitigar el 100% de amenazas usando FortiGate.

Después de definir las métricas adecuadas se realizará el procedimiento de Revisión y Auditoría que servirá para garantizar que la red SD-WAN opere de manera eficiente, segura y en alineación con los objetivos de rendimiento establecidos, se tiene previsto el siguiente plan de revisión:

- Revisión Diaria: Se realizará mediante el monitoreo con FortiManager y FortiAnalyzer, proporcionando un reporte diario del estado operativo de la red.
- Auditoría Semanal: Se analizará logs y eventos utilizando FortiGate y FortiAnalyzer, permitiendo identificar tendencias y posibles problemas de seguridad de manera regular.
- Revisión Mensual: Se hará una evaluación detallada del rendimiento de la red comparado con los KPIs establecidos, utilizando FortiManager y FortiAnalyzer para ajustar configuraciones y optimizar el funcionamiento.
- Auditoría Trimestral: Auditoría completa que abarcará pruebas de penetración y evaluación de políticas de seguridad, asegurando la robustez y la eficacia de las medidas de seguridad implementadas en la red SD-WAN.

Finalmente se deberá realizar una optimización continua que se iniciará con el análisis de resultados de revisiones y auditorías para identificar áreas de mejora, seguido de la planificación de acciones correctivas y mejoras específicas. Luego, estas mejoras se implementarán en la infraestructura SD-WAN si es que existen, y finalmente, se evaluará el impacto de dichas mejoras para asegurar su efectividad.

4.4. CRONOGRAMA DE IMPLEMENTACIÓN

Para concluir este plan de despliegue y basándonos en todos los aspectos revisados anteriormente, se procederá a elaborar la propuesta del cronograma de Implementación para la adopción de SD-WAN en la agencia de prueba. Este cronograma incluye fases clave como la evaluación y planificación, preparación del entorno, implementación piloto, despliegue gradual, capacitación y soporte, y evaluación post-despliegue, cada una con actividades específicas y duraciones estimadas. También se establecerá hitos clave y fechas límite hipotéticas para asegurar una transición eficiente y sin interrupciones en las operaciones, asignando roles y responsabilidades a los miembros del equipo y permitiendo ajustes según sea necesario para mantener la implementación en curso una vez iniciada.

4.4.1. Creación de un cronograma para una futura implementación de SD-WAN.

A continuación, se detalla las fases clave para la implementación de SD-WAN en la agencia, sobre los cuales estará basado el cronograma:

1. Evaluación y Planificación
    - Realización de un análisis detallado de la infraestructura actual.
    - Identificación de requisitos específicos para la implementación de SD-WAN.
    - Diseño conceptual de la arquitectura SD-WAN.

- Revisión y aprobación del diseño por todas las partes interesadas.

2. Preparación del Entorno
    - Adquisición y configuración de equipos necesarios (FortiGate, switches, controladoras, APs, etc.).
    - Instalación de software y herramientas de monitoreo.
    - Configuración inicial de políticas de enrutamiento y seguridad.
3. Implementación Piloto
    - Implementación de un entorno piloto para pruebas.
    - Realización de pruebas de funcionalidad y rendimiento.
    - Ajustes basados en los resultados de las pruebas.
4. Despliegue Gradual
    - Despliegue de SD-WAN en segmentos de la red, empezando por las áreas menos críticas.
    - Monitoreo y ajustes en tiempo real para asegurar la estabilidad.
5. Capacitación y Soporte
    - Capacitación al personal de TI y usuarios clave.
    - Establecimiento de procedimientos de soporte técnico.
    - Documentación de todos los procesos y configuraciones.
6. Evaluación Post-Despliegue
    - Evaluación del rendimiento de la red después del despliegue completo.
    - Identificación y resolución de problemas remanentes.
    - Ajustes finales y optimización continua.

A continuación, se adjunta el cronograma que detalla los plazos estimados para cada fase de la implementación:

Tabla 47 - Cronograma

CRONOGRAMA	Mes 1				Mes 2				Mes 3			
	8	15	23	30	8	15	23	30	8	15	23	30
EVALUACIÓN Y PLANIFICACIÓN												
Realización de un análisis detallado de la infraestructura actual												
Identificación de requisitos específicos para la implementación												
Diseño conceptual de la arquitectura SD-WAN												
Revisión y aprobación del diseño por todas las partes interesadas												
PREPARACIÓN DEL ENTORNO												
Adquisición y configuración de equipos necesarios												
Instalación de software y herramientas de monitoreo.												
Configuración inicial de políticas de enrutamiento y seguridad												
IMPLEMENTACIÓN PILOTO												
Implementación de un entorno piloto para pruebas.												
Realización de pruebas de funcionalidad y rendimiento.												
Ajustes basados en los resultados de las pruebas.												
DESPLIEGUE GRADUAL												
Despliegue de SD-WAN en segmentos de la red												
Monitoreo y ajustes en tiempo real para asegurar la estabilidad.												
CAPACITACIÓN Y SOPORTE												
Capacitación al personal de TI y usuarios clave.												
Establecimiento de procedimientos de soporte técnico.												
Documentación de todos los procesos y configuraciones.												
EVALUACIÓN POST-DESPLIEGUE												
Evaluación del rendimiento de la red después del despliegue completo.												
Identificación y resolución de problemas remanentes.												
Ajustes finales y optimización continua												

Fuente: Elaboración propia

Este cronograma es altamente efectivo para la implementación de SD-WAN y tiene un enfoque estructurado y secuencial, que aborda cada fase crucial del proyecto con meticulosidad y planificación estratégica. Comenzando con una evaluación exhaustiva de la infraestructura actual y los requisitos específicos lo cual se revisó anteriormente por lo que ya contamos con una base sólida para la implementación de SD-WAN. El diseño conceptual de la arquitectura SD-WAN igualmente ya fue abordado en esta investigación y será de gran ayuda para la migración de la red.

El paso de implementación piloto permite pruebas exhaustivas en un entorno controlado, ajustes antes del despliegue completo. Desplegar por fases en áreas menos críticas minimiza riesgos y permite ajustes en tiempo real para mantener la estabilidad.

La capacitación y el soporte técnico son fundamentales en el cronograma para garantizar que el personal de TI y los usuarios clave estén completamente preparados para la nueva infraestructura. Estos temas también ya fueron abordados en la presente investigación.

Finalmente, la evaluación post-despliegue se centra en evaluar el rendimiento integral de la red, abordar problemas remanentes, y realizar ajustes finales para optimizar continuamente la infraestructura SD-WAN.

4.4.2. Hitos clave y fechas límite hipotéticas para cada actividad del proyecto

Los hitos clave y fechas límite hipotéticas se plantearon con la finalidad de mantener el enfoque del equipo en objetivos específicos, y de esta manera garantizar la gestión eficiente del tiempo, y asegurar el progreso de la implementación. Se incluye a continuación los días estimados de la elaboración por fases del proyecto.

Tabla 48 – Hitos clave

Hito	Fecha Límite Hipotética
Inicio del Proyecto	Día 1
Evaluación y Planificación Completa	Día 15
Preparación del Entorno Completa	Día 30
Implementación Piloto Completa	Día 45
Despliegue Gradual Iniciado	Día 60
Capacitación y Soporte Completa	Día 75
Despliegue Completo y Evaluación Post-Despliegue	Día 90

Fuente: Elaboración propia

4.4.3. Roles y responsabilidades necesarios.

Definir roles y responsabilidades necesarios y asignar roles específicos a los miembros del equipo de proyecto es fundamental para asegurar la eficacia y eficiencia en la ejecución de tareas. Esta práctica proporciona claridad organizativa, asegurando que cada miembro se enfoque en áreas donde sus habilidades sean más relevantes. Además, establece líneas claras de responsabilidad y rendición de cuentas, lo que promueve la colaboración efectiva, mejora el desempeño del equipo y optimiza el uso de recursos. Se anexa los roles necesarios para la implementación según el cronograma elaborado:

Tabla 49 – Roles y responsabilidades

Rol	Responsabilidades
Project Manager	Responsable de la planificación general y la supervisión del proyecto. Asegura cumplimiento del cronograma.
Líder Técnico	Supervisa la configuración técnica y la implementación de SD-WAN. Coordina con el equipo de TI.
Especialista en Redes	Configura y gestiona dispositivos de red. Implementa políticas de enrutamiento y seguridad.
Especialista en Seguridad	Desarrolla y aplica políticas de seguridad. Monitorea amenazas y asegura la integridad de la red.
Especialista en Soporte Técnico	Proporciona soporte durante y después de la implementación. Responde a consultas y resuelve problemas técnicos.
Entrenador y Documentador	Capacita al personal de TI y usuarios finales. Documenta procedimientos, configuraciones y soluciones.

Fuente: Elaboración propia

CAPÍTULO 5- CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

Después de finalizar el plan de despliegue para una futura implementación de SD-WAN en las agencias que maneja Centric S.A. se puede concluir lo siguiente:

- Realizar un análisis exhaustivo de la infraestructura actual proporcionó una comprensión clara de la configuración de la red y su desempeño. Esto ayudó a determinar la capacidad de escalabilidad y la preparación de la red para soportar la futura implementación de SD-WAN.
- La evaluación a los proveedores de SD-WAN permitió asegurarse de que opción ofrece las mejores soluciones en términos de costo, rendimiento y soporte, para poder escoger la que permita reducir la resistencia al cambio y facilitar una adopción más rápida y efectiva de la nueva tecnología.
- La elaboración del diseño conceptual para la nueva red con SD-WAN facilitó la elaboración de un cronograma detallado para la futura implementación tomando en cuenta la mitigación de posibles interrupciones y la minimización de impactos negativos.
- Con SD-WAN se priorizará el tráfico de aplicaciones críticas asegurando que los recursos de red se utilicen de manera óptima, mejorando el rendimiento de aplicaciones esenciales para el negocio y fortaleciendo la seguridad de la red mediante la implementación de políticas de enrutamiento y seguridad más robustas y flexibles.
- La elaboración realizada del cronograma detallado para la futura implementación facilitará el control y seguimiento del progreso del proyecto. La identificación de hitos y la definición de plazos elaborada permitirán monitorear el avance y tomar acciones correctivas en caso de desviaciones.

5.2. RECOMENDACIONES

Las recomendaciones generadas en base al plan de despliegue realizado son las siguientes:

- Continuar evaluando a los proveedores de SD-WAN para asegurarse de que ofrecen las mejores soluciones en términos de costo, rendimiento y soporte. La colaboración estrecha con los proveedores puede proporcionar acceso a nuevas funcionalidades y mejoras tecnológicas.
- Es crucial proporcionar capacitación continua al personal de TI para que se mantengan actualizados con las últimas tecnologías y prácticas de gestión de SD-WAN. Esto asegurará que el equipo esté preparado para manejar la implementación en la red actual y solventar cualquier inconveniente que pueda surgir inclusive post-implementación.
- Fomentar la colaboración con socios tecnológicos y consultores externos para mantenerse al día con las últimas tendencias y mejores prácticas en la gestión de redes SD-WAN.
- Revisar y actualizar regularmente las políticas de seguridad para adaptarse a las nuevas amenazas y vulnerabilidades. La implementación de controles de seguridad avanzados y la respuesta rápida a los incidentes de seguridad son esenciales para proteger la infraestructura de red.
- Continuar invirtiendo en la infraestructura de red para asegurar que esté equipada con el hardware y software más recientes, garantizando así un rendimiento y seguridad óptimos para la gestión diaria en todas las agencias de la empresa.

CAPÍTULO 6- BIBLIOGRAFÍA

Agudelo, G. (2004). *TÉCNICAS PARA LA GESTIÓN DEL ANCHO DE BANDA EN LA WAN CON SOPORTE EN ROUTERS CISCO 2600*.

Aharonov, B. (2024, May 13). *La revolución de la conectividad: Cómo el SD-WAN está transformando las redes empresariales | by Benjamin Aharonov | May, 2024 | Medium*. Medium. https://medium.com/@screege/la-revoluci%C3%B3n-de-la-conectividad-c%C3%B3mo-el-sd-wan-est%C3%A1-transformando-las-redes-empresariales-7bbf4e831aea

Bustos, S. (2023). *DESARROLLO DE UN PLAN DE MIGRACIÓN DE UNA RED DE ÁREA EXTENSA DE UN PROVEEDOR DE SERVICIOS DE INTERNET A UNA RED DEFINIDA POR SOFTWARE SD-WAN*.

Campos Jiménez, L., & Santana Pastrano, P. (2008). *ESTUDIO Y DISEÑO DE UNA RED PORTADORA METRO ETHERNET PARA LA CIUDAD DE QUITO CON TECNOLOGÍAS 802.3ah, 802.1ad Y 802.1ah*.

Centric S.A. (2021). *Centric Ecuador*. LinkedIn. https://ec.linkedin.com/company/centric-s-a

Centric S.A. (2023). *Misión y Visión Centric*. S3S. https://s3s.casabaca.com/s3s-web-prime/jsf/login.xhtml

Check Point. (2022). *Los beneficios de SD-WAN*. Check Point Software. https://www.checkpoint.com/es/cyber-hub/network-security/what-is-sd-wan/benefits-of-sd-wan/

Check Point. (2023). *¿Qué son las soluciones SD-WAN? - Software*. Check Point. https://www.checkpoint.com/es/cyber-hub/network-security/what-is-sd-wan/what-are-sd-wan-solutions/

Check Point. (2024). *Modelos de implementación SD-WAN - Check Point Software*. Check Point. https://www.checkpoint.com/es/cyber-hub/network-security/what-is-sd-wan/sd-wan-deployment-models/

Cloudflare. (2023). *Qué es SD WAN y cómo funciona | Administración de redes*. Cloudflare. https://www.cloudflare.com/es-es/learning/network-layer/what-is-an-sd-wan/

Edraw. (2024, May 27). *Un tutorial sobre la red de área amplia*. Wondershare. https://www.edrawsoft.com/es/diagram-tips/wide-area-network.html

Ellor, R. (2023, November 27). *¿Cuál es la diferencia entre una LAN y una WAN?* Que Es LAN y WAN | Purple. https://purple.ai/es/blogs/cual-es-la-diferencia-entre-una-lan-y-una-wan/

Flores, L. (2023, October 10). *SD-WAN: qué es y cómo funciona*. Alestra. https://www.alestra.mx/blog/sd-wan

Fortinet. (2023a). *¿Qué es la calidad de servicio (QoS) en las redes?* Fortinet. https://www.fortinet.com/lat/resources/cyberglossary/qos-quality-of-service

Fortinet. (2023b). *¿Qué es una red SDN? Diferencia entre SDN y SD-WAN* |. Fortinet. https://www.fortinet.com/lat/resources/cyberglossary/sdn-vs-sd-wan

Fortinet. (2024a). *Firewall de próxima generación (NGFW) | Ver los productos principales*. Fortinet. https://www.fortinet.com/lat/products/next-generation-firewall

Fortinet. (2024b). *Planificación de la implementación de MVE de Fortinet Secure SD-WAN Megaport*. Megaport. https://docs.megaport.com/es/mve/fortinet/plan-deployment/

IBM. (2023). *¿Qué es SD-WAN?* IBM. https://www.ibm.com/mx-es/topics/sd-wan

Ikusi. (2024). *5 ventajas de usar SD-WAN en tu empresa*. Ikusi. https://www.ikusi.com/mx/blog/5-ventajas-de-usar-sd-wan-en-tu-empresa-2/

Martis, J. (2023, August 18). *Qué es un plan de contingencia y cómo crear uno en 8 pasos*. Asana. https://asana.com/es/resources/contingency-plan

NeuroThinking. (2024, February 6). *¿Qué es SD-WAN y cómo funciona?* Neurona Solutions. https://blm.neurona-solutions.com/blog/qu%C3%A9-es-sd-wan-y-c%C3%B3mo-funciona

¿Qué es SD-WAN? (2021). Palo Alto Networks. https://www.paloaltonetworks.lat/cyberpedia/what-is-sd-wan

Roch, E. (2024, May 9). *Redes de Área Amplia (WAN): Tipos, Características y Configuración | LovTechnology*. https://lovtechnology.com/redes-de-area-amplia-wan-tipos-caracteristicas-y-configuracion/

TecnoDigital. (2023, July 4). *Tipos de redes de computadoras y sus aplicaciones*. Tecnología Digital. https://informatecdigital.com/redes/tipos-de-redes-de-computadoras-y-sus-aplicaciones/

Tecnozero. (2024). *WAN tradicional vs SD-WAN*. Tecnozero Soluciones Informaticas. https://www.tecnozero.com/blog/wan-tradicional-vs-sd-wan-esto-es-lo-que-necesitas-saber/

Tekpyme. (2023, July 17). *Redes SD-WAN: todo lo que necesita saber sobre esta tecnología para mejorar la conectividad y seguridad de su empresa*. Linkedin. https://www.linkedin.com/pulse/redes-sd-wan-todo-lo-que-necesita-saber-sobre-esta-tecnolog%C3%ADa/

Telefónica. (2023). *Las ventajas de SD WAN frente a las infraestructuras físicas*. Telefónica. https://www.telefonica.com/es/sala-comunicacion/blog/ventajas-sd-wan/