



Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América

Facultad de Ingeniería Electrónica y Eléctrica

Escuela Profesional de Ingeniería Electrónica

**Diseño e implementación de una solución de conectividad
para una sucursal bancaria en la ciudad de Iquitos utilizando
las tecnologías SD-WAN y Starlink**

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de Ingeniero Electrónico

AUTOR

Nicolay Varosky QUISPE TACURI

ASESOR

Mg. Daniel DIAZ ATAUCURI

Lima, Perú

2026



Reconocimiento - No Comercial - Compartir Igual - Sin restricciones adicionales

<https://creativecommons.org/licenses/by-nc-sa/4.0/>

Usted puede distribuir, remezclar, retocar, y crear a partir del documento original de modo no comercial, siempre y cuando se dé crédito al autor del documento y se licencien las nuevas creaciones bajo las mismas condiciones. No se permite aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros a hacer cualquier cosa que permita esta licencia.

Referencia bibliográfica

Quispe, N. (2026). *Diseño e implementación de una solución de conectividad para una sucursal bancaria en la ciudad de Iquitos utilizando las tecnologías SD-WAN y Starlink*. [Trabajo de suficiencia profesional de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería Electrónica y Eléctrica, Escuela Profesional de Ingeniería Electrónica]. Repositorio institucional Cybertesis UNMSM.

Metadatos complementarios

Datos de autor	
Nombres y apellidos	Nicolay Varoscky Quispe Tacuri
Tipo de documento de identidad	DNI
Número de documento de identidad	47521282
URL de ORCID	No Aplica
Datos de asesor	
Nombres y apellidos	Mg. Daniel Diaz Ataucuri
Tipo de documento de identidad	DNI
Número de documento de identidad	07139361
URL de ORCID	https://orcid.org/0000-0001-5747-2795
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Dr. Jorge Elías Moscoso Sánchez
Tipo de documento	DNI
Número de documento de identidad	07206008
Miembro del jurado 1	
Nombres y apellidos	Mg. Wilbert Chavez Irazabal
Tipo de documento	DNI
Número de documento de identidad	08121733
Miembro del jurado 2	
Nombres y apellidos	Mg. Alex Alfonso Gonzales Suárez
Tipo de documento	DNI
Número de documento de identidad	07644682
Datos de investigación	
Línea de investigación	C.0.3.10. Redes de datos
Grupo de investigación	No Aplica
Agencia de financiamiento	No Aplica

Ubicación geográfica de la investigación	Edificio: Banco Ripley Perú SA País: Perú Departamento: Loreto Provincia: Maynas Distrito: San Juan Bautista Centro poblado: Iquitos Urbanización: N/A Manzana y lote: N/A Calle: Av. Capitán José Abelardo Quiñones 1050 Latitud: -3.7647661 Longitud: -73.2675127
Año o rango de años en que se realizó la investigación	Abril 2023 – Octubre 2023
URL de disciplinas OCDE	Ingeniería eléctrica, Ingeniería electrónica https://purl.org/pe-repo/ocde/ford#2.02.01 Telecomunicaciones https://purl.org/pe-repo/ocde/ford#2.02.05



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
(Universidad del Perú, DECANA DE AMÉRICA)
FACULTAD DE INGENIERÍA ELECTRÓNICA Y ELÉCTRICA
Teléfono 619-7000 Anexo 4226
Calle Germán Amezaga 375 – Lima 1 – Perú



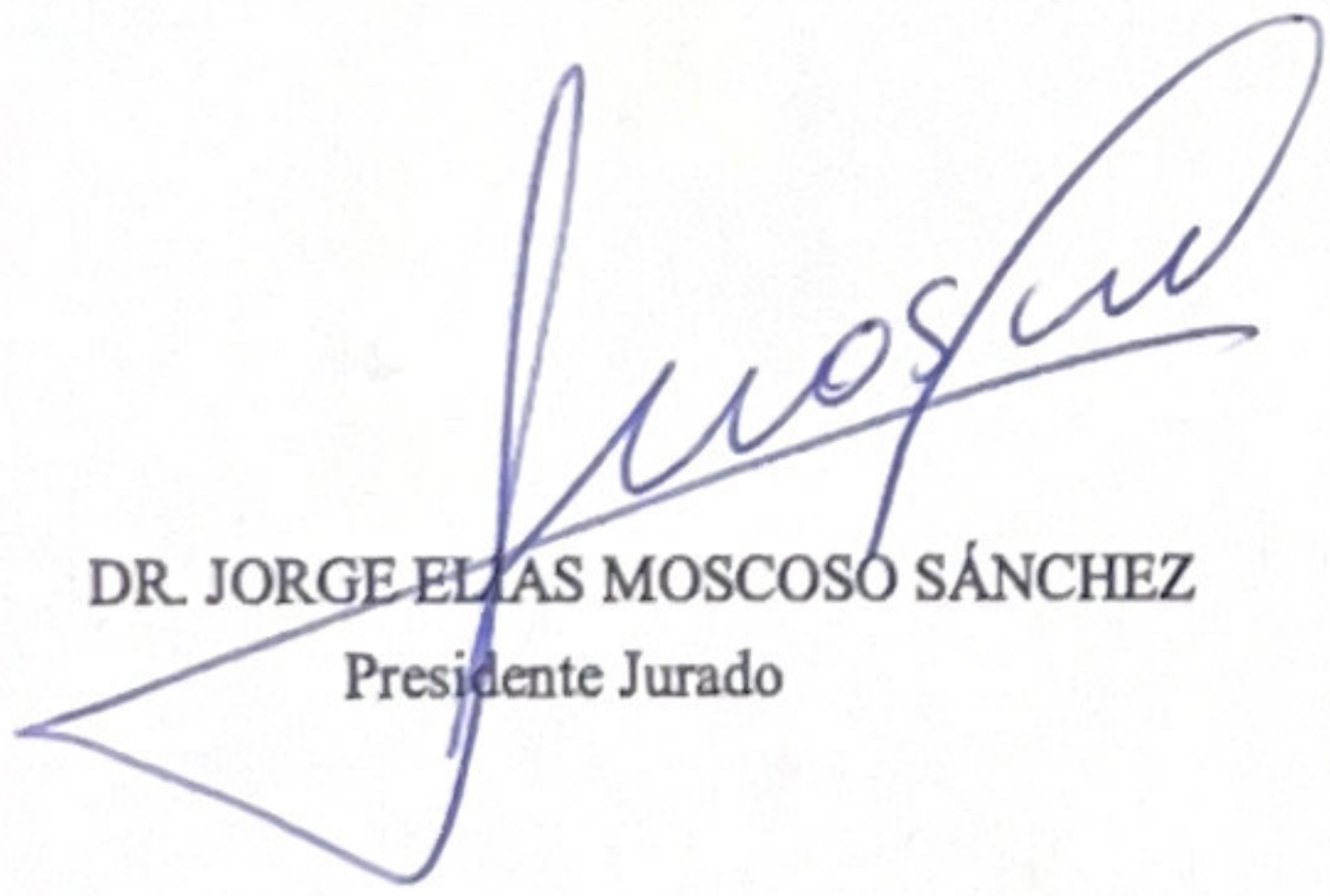
ACTA DE SUSTENTACIÓN
TRABAJO DE
SUFICIENCIA PROFESIONAL
ACTA N°12/FIEE-PPP/2026

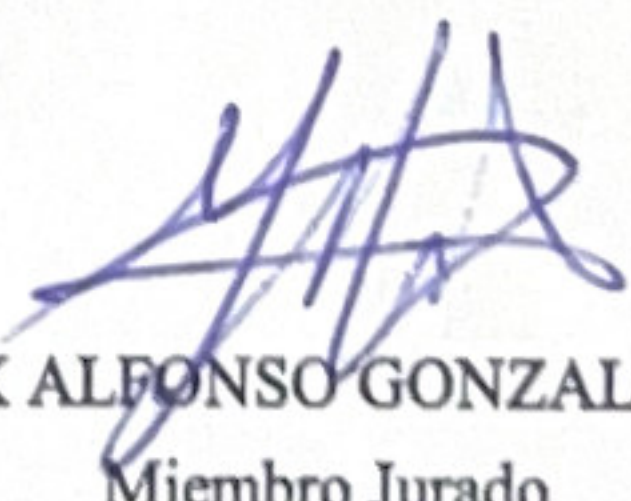
Los suscritos Miembros del Jurado, docentes permanentes de las Escuelas Profesionales de la Facultad de Ingeniería Electrónica y Eléctrica, reunidos en la fecha 22 de enero del 2026, como presidente de Jurado el **DR. JORGE ELÍAS MOSCOSO SÁNCHEZ**, integrado por el Miembro de Jurado el **MG. ALEX ALFONSO GONZALES SUÁREZ**, el Miembro de Jurado el **MG. WILBERT CHAVEZ IRAZABAL** y Miembro Asesor el **MG. DANIEL DIAZ ATAUCURI**.

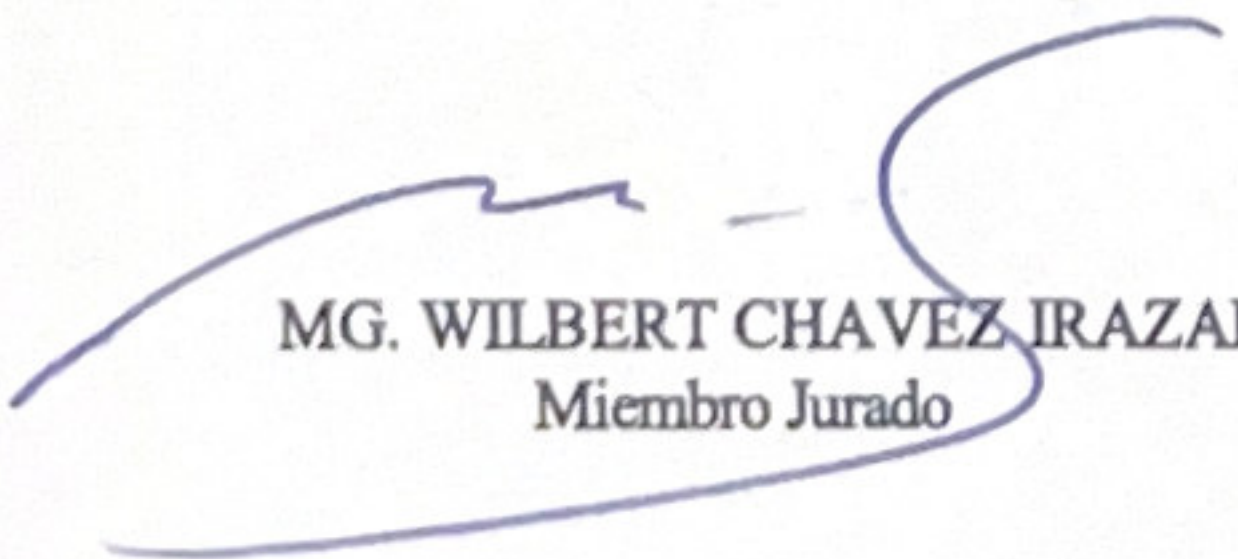
Después de escuchar la Sustentación Presencial del Trabajo de Suficiencia Profesional del Bachiller **NICOLAY VAROSCKY QUISPE TACURI** con código 09190157 que para optar el Título Profesional de Ingeniero Electrónico sustentó el Trabajo de Suficiencia Profesional titulado **DISEÑO E IMPLEMENTACIÓN DE UNA SOLUCIÓN DE CONECTIVIDAD PARA UNA SUCURSAL BANCARIA EN LA CIUDAD DE IQUITOS UTILIZANDO LAS TECNOLOGÍAS SD-WAN Y STARLINK**.

El jurado examinador procedió a formular las preguntas reglamentarias y, luego de una deliberación en privado, decidió otorgarle el calificativo de 16 (Dieciseis).

Ciudad Universitaria, 22 de enero del 2026


DR. JORGE ELÍAS MOSCOSO SÁNCHEZ
Presidente Jurado


MG. ALEX ALFONSO GONZALES SUÁREZ
Miembro Jurado


MG. WILBERT CHAVEZ IRAZABAL
Miembro Jurado


MG. DANIEL DIAZ ATAUCURI
Miembro Asesor



UNIVERSIDAD NACIONAL MAYOR DE
SAN MARCOS
Universidad del Perú, Decana de América

CERTIFICADO DE SIMILITUD

Yo , **DANIEL DIAZ ATAUCURI** en mi condición de asesor acreditado con el Dictamen N°09/FIEE-PPP/2026 del Trabajo de Suficiencia Profesional titulado **DISEÑO E IMPLEMENTACIÓN DE UNA SOLUCIÓN DE CONECTIVIDAD PARA UNA SUCURSAL BANCARIA EN LA CIUDAD DE IQUITOS UTILIZANDO LAS TECNOLOGÍAS SD-WAN Y STARLINK**, presentado por el bachiller **NICOLAY VAROSCKY QUISPE TACURI**, para optar al título profesional de Ingeniero Electrónico. CERTIFICO que se ha cumplido con lo establecido en la Directiva de Originalidad y de Similitud de Trabajos Académicos, de Investigación y Producción Intelectual. Según la revisión, análisis y evaluación mediante la plataforma PIDS, el documento evaluado cuenta con el 16% de similitud, nivel PERMITIDO para continuar con los trámites correspondientes y para su publicación en el repositorio institucional.

Se emite el presente certificado en cumplimiento de lo establecido en las normas vigentes, como uno de los requisitos para la obtención del título de Ingeniero Electrónico.

Lima, 22 de Enero del 2026


Firma del Asesor

DNI: 07139361

Nombres y apellidos del asesor:
DANIEL DIAZ ATAUCURI

DEDICATORIA

El presente trabajo es dedicado a todas las personas que amo y siempre han estado presentes apoyándome en mi carrera profesional.

AGRADECIMIENTOS

Agradezco a Dios por guiar mi camino y darme la fortaleza para cumplir mis objetivos. A mi madre Yolanda Tacuri, quién es un pilar importante en mi vida. Agradezco también a la facultad de mis amores FIEE y a la comisión de titulación por el apoyo en la elaboración de este trabajo de suficiencia profesional.

RESUMEN

El presente trabajo aborda la necesidad de una entidad bancaria de implementar una infraestructura de red redundante para su nueva sucursal ubicado en la ciudad de Iquitos; considerando tecnologías de fibra óptica, SD-WAN y la satelital. Esta solución busca garantizar altos niveles de disponibilidad en los servicios de comunicación, permitiendo así la continuidad operativa ante incidentes en los canales de comunicación.

La infraestructura de red actual de la entidad es redundante a nivel de enlaces ópticos. No obstante, no logra los niveles de disponibilidad para garantizar la operación continua de una agencia bancaria. Esta limitación se debe, en gran parte, a la dependencia de canales de comunicación provistos por un único proveedor de servicios de internet (ISP). Como consecuencia, diversas sucursales han experimentado interrupciones del servicio cuando se produce una falla en el enlace de fibra óptica, debido a que ambos canales de comunicación suelen compartir la misma ruta o nodo local.

El enfoque del proyecto es el diseño de una red para la nueva sucursal en la ciudad de Iquitos que servirá como base para replicar en otras sedes existentes. Esta nueva red minimiza los problemas de la actual infraestructura haciendo uso de tecnologías como SD-WAN y Starlink.

Palabras clave: Enlace satelital, Tecnología SD-WAN, Red eficiente, Redundancia, Disponibilidad.

ABSTRACT

This work addresses the need for a banking institution to implement a redundant network infrastructure for its new branch that, given the problems identified with the fiber optic channel, does not rely exclusively on this technology. This measure seeks to ensure high levels of availability in communication services, thus enabling operational continuity in the event of failures or incidents in the fiber optic channels.

The institution's current network infrastructure includes redundancy at the communication link level. However, it does not achieve the levels of availability required to guarantee the continuous operation of a bank branch. This limitation is largely due to the dependence on communication channels provided by a single Internet Service Provider (ISP). As a result, several branches have experienced service interruptions when a fiber optic link failure has occurred, as the main and contingency channels often share the same route or local node.

The focus of this project is the design of a network for the new branch that will serve as a replicable base for the existing branches. This new network will solve the problems of the current infrastructure by leveraging technologies such as SD-WAN and Starlink.

Keywords: Satellite link, SD-WAN technology, Efficient network, Redundancy, Availability.

INDICE GENERAL

CARÁTULA	i
DEDICATORIA	ii
AGRADECIMIENTOS	iii
RESUMEN	iv
ABSTRACT	v
INDICE GENERAL	vi
LISTA DE FIGURAS	viii
LISTA DE TABLAS	x
CAPITULO I: INTRODUCCIÓN	1
CAPITULO II: INFORMACIÓN DEL LUGAR DONDE SE DESARROLLÓ LA ACTIVIDAD	3
2.1 Institución – Actividad que desarrolla	3
2.2 Periodo de duración de la actividad.	3
2.3 Finalidad y objetivos de la entidad	3
2.4 Razón social	4
2.5 Dirección postal	4
2.6 Nombre y correo electrónico del profesional a cargo.	4
CAPITULO III: DESCRIPCIÓN DE LA ACTIVIDAD	5
3.1 Organización de la actividad	5
3.2 Finalidad y objetivos de la Actividad	5
3.2.1 Finalidad	5
3.2.2 Objetivos	6
3.3 Problemática	6
3.3.1 Problema General	7
3.3.2 Problemas Específicos	7
3.3.3 Justificación e importancia de la investigación	8
3.4 Metodología	9
3.4.1 Bases teóricas	9

	vii
3.4.2 Marco conceptual	11
3.5 Procedimiento	26
3.5.1 Situación actual de la empresa y caso de negocio	26
3.5.2 Información de las sucursales involucradas en el proyecto	27
3.5.3 Infraestructura de red de la ciudad	28
3.5.4 Diseño y dimensionamiento de la red	29
3.5.5 Diagrama de red	36
3.5.6 Etapa de factibilidad	38
3.6 Resultado de la actividad	39
3.6.1 Conectividad entre equipo Core Lima y Core Iquitos	39
3.6.2 Conectividad entre sedes remotas	40
3.6.3 Pruebas de redundancia	40
CAPITULO IV: DISCUSION DE RESULTADOS	49
4.1 Descripción de la implementación	49
4.1.1 Formulación inicial del proyecto	49
4.1.2 Implementación de los enlaces y equipos de fibra óptica – outdoor/indoor	50
4.1.3 Implementación de enlace satelital	53
4.1.4 Implementación de cableado de red y equipos LAN	54
4.1.5 Configuración de equipos networking	56
4.2 Disponibilidad de la red	57
4.3 Evaluación Económica	59
CAPITULO V: CONCLUSIONES	61
CAPITULO VI: RECOMENDACIONES	63
CAPITULO VII: BIBLIOGRAFÍA	64
CAPITULO IX: ANEXOS	68
Anexo A	68
Anexo B	69
Anexo C	73
Anexo D	76
Anexo E	77
Anexo F	79

LISTA DE FIGURAS

Figura 1: Organigrama de la entidad bancaria	5
Figura 2: Arquitectura Cisco SD-WAN	14
Figura 3: Distribución de satélites según su órbita	17
Figura 4: Órbita GEO	18
Figura 5: Órbita MEO	19
Figura 6: Órbita LEO	20
Figura 7: Topología MPLS de la entidad bancaria	26
Figura 8: Trazado referencial de la fibra óptica en Iquitos	29
Figura 9: Fortigate 100F	33
Figura 10: Cisco C9200L-24P	34
Figura 11: Diseño de red propuesto	37
Figura 12: Validación de conectividad entre DC Lima e Iquitos	39
Figura 13: Validación de conectividad entre sucursales	40
Figura 14. Configuración de performance SLA	41
Figura 15. Configuración de reglas SD-WAN	42
Figura 16: Caída de enlace de datos	43
Figura 17. Interfaces activas por orden de prioridad	44
Figura 18: Caída de enlace de internet	45
Figura 19. Interfaces activas por orden de prioridad	46
Figura 20: Caída de enlace de datos e internet	47
Figura 21. Interfaces activas por orden de prioridad	48
Figura 22: Instalación de equipo Cisco ISR4331 en gabinete de sala Data Center	51
Figura 23: Instalación de equipo ZTE F601 en gabinete de sala Data Center Iquitos	51

Figura 24: Recorrido de ingreso de cable drop de manera aérea	52
Figura 25: Instalación de equipo Cisco ISR4331 en gabinete de sala DataCenter	53
Figura 26: Instalación y anclaje de antena Starlink en azotea del CC Mall Aventura	53
Figura 27: Instalación de equipo Fortigate 40F y Power Supply para enlace Starlink	54
Figura 28: Plano de distribución de puntos de red de la agencia	55
Figura 29: Equipos Fortigate y Cisco instalados en gabinete de sala Data Center	66

LISTA DE TABLAS

Tabla 1: SD-WAN vs MPLS	15
Tabla 2: Parámetros técnico Starlink	21
Tabla 3: Información de las sedes involucradas	28
Tabla 4: Ubigeo y Coordenadas	28
Tabla 5: Características Plan Empresarial Starlink	31
Tabla 6: Distribución de capacidad de los enlaces	31
Tabla 7: Características Fortigate 100F	33
Tabla 8: Características C9200L-24P	35
Tabla 9: Dimensionamiento de equipamiento de red	36
Tabla 10: Resumen de incidentes en los servicios de proveedores 2024	58
Tabla 11: Gastos CAPEX de tecnología de la nueva sucursal	59
Tabla 12: Gastos OPEX de tecnología de la nueva sucursal	60

CAPITULO I: INTRODUCCIÓN

El presente trabajo de suficiencia profesional aborda el diseño e implementación de una infraestructura de red de alta disponibilidad para una entidad financiera, específicamente en zonas con limitada infraestructura de fibra óptica. La elección de este tema se fundamenta en la creciente necesidad de expansión de las entidades financieras hacia regiones donde la implementación de redes de fibra óptica es relativamente reciente.

Si bien la fibra óptica ofrece un canal de comunicación eficiente y de alta velocidad, ideal para las exigencias del sector financiero (que requiere interconexión y disponibilidad constante), su limitada presencia en ciertas áreas geográficas representa un desafío significativo que impacta la capacidad de estas entidades para ofrecer servicios y productos competitivos a sus clientes.

La motivación principal para realizar este desarrollo radica en la búsqueda de soluciones tecnológicas que permitan a la entidad financiera operar con la misma eficiencia y disponibilidad en áreas con menor desarrollo de infraestructura de fibra óptica, que en aquellas con mayor cobertura. Se busca, por tanto, contribuir a la inclusión financiera y a la expansión de servicios en zonas que tradicionalmente han estado marginadas de las últimas tecnologías de comunicación. Este estudio se justifica, además, por la necesidad de la empresa de contar con una alternativa viable a la fibra óptica que garantice la continuidad de sus operaciones, y por la carencia de soluciones integrales de conectividad en ciertas zonas del territorio nacional.

Este desarrollo se enfoca en el diseño e implementación de una infraestructura de red para una entidad financiera específica ubicada en la ciudad de Iquitos, considerando las limitaciones de infraestructura de fibra óptica en su área de operación y basándose en conceptos clave de las redes de telecomunicaciones, incluyendo arquitecturas de red, protocolos de enrutamiento, tecnologías de acceso (como fibra óptica y conectividad satelital), y mecanismos de redundancia y alta disponibilidad (como SLAs, Service Level Agreements). Esto permitirá un análisis profundo del diseño de una red de alta disponibilidad, utilizando tecnologías alternativas, como la conectividad satelital, como complemento o respaldo a la fibra óptica.

En el capítulo I, se da una introducción donde se detalla el origen y necesidad de la propuesta presentada a la entidad. En el capítulo II, se expone la información acerca del lugar donde se desarrolló, la duración del trabajo en las sedes de la entidad, por otro lado, también se detalla el personal encargado. En el capítulo III, se precisa los datos de la organización donde se desarrolló el proyecto, la finalidad, objetivos y problemática, la metodología referenciada en investigaciones nacionales e internacionales. En el capítulo IV, se muestra la discusión de los resultados donde se explica la justificación económica y técnica. En el capítulo V, las conclusiones.

CAPITULO II: INFORMACIÓN DEL LUGAR DONDE SE DESARROLLÓ LA ACTIVIDAD

2.1 Institución – Actividad que desarrolla

El presente trabajo de suficiencia profesional se desarrolló en el Banco Ripley Perú S.A., una entidad perteneciente al sector financiero. La empresa se encuentra en un proceso de expansión a nivel nacional, con el objetivo estratégico de ampliar su presencia en diversas ciudades del país. Este crecimiento busca acercar sus servicios y productos financieros a nuevos clientes, fortaleciendo su posicionamiento en el mercado peruano.

2.2 Periodo de duración de la actividad.

El periodo de duración fue de seis meses, específicamente desde abril del 2023 hasta octubre del 2023.

2.3 Finalidad y objetivos de la entidad

Banco Ripley Perú tiene como finalidad actuar como intermediario financiero canalizando el ahorro de personas y empresas (captando depósitos) hacia la inversión y el consumo mediante créditos.

Uno de los objetivos más importantes de la entidad es expandir su presencia geográfica en Perú, como se evidencia en su estrategia de abrir nuevas sucursales en diversas ciudades buscando consolidarse como una entidad financiera relevante en el país. Banco Ripley está estrechamente vinculado al

negocio retail de Ripley (tiendas por departamento). Uno de sus objetivos clave es aprovechar esta sinergia, ofreciendo productos financieros (especialmente tarjetas de crédito) que impulsen las ventas en las tiendas Ripley y fidelicen a los clientes. Asimismo, actualmente se está inmerso en un proceso de transformación digital. Busca innovar en sus productos y servicios, utilizando la tecnología para mejorar la experiencia del cliente, optimizar sus procesos y ser más competitivo para desarrollar relaciones a largo plazo con sus clientes, ofreciendo productos y servicios personalizados, programas de beneficios y una atención de alta calidad.

2.4 Razón social

La razón social de la empresa es BANCO RIPLEY PERU S.A.

2.5 Dirección postal

La empresa Banco Ripley Perú tiene su sede central ubicada en Av. Paseo de la República 3118, distrito San Isidro. La sede en la que se desarrolló el proyecto está ubicada en la ciudad de Iquitos Av. José Abelardo Quiñones, Lote Las Ninfas - 2, Distrito San Juan Bautista, Provincia de Maynas, Loreto.

2.6 Nombre y correo electrónico del profesional a cargo.

El jefe del proyecto a cargo fue el Ing. Cesar Alejandro Espino Guerra

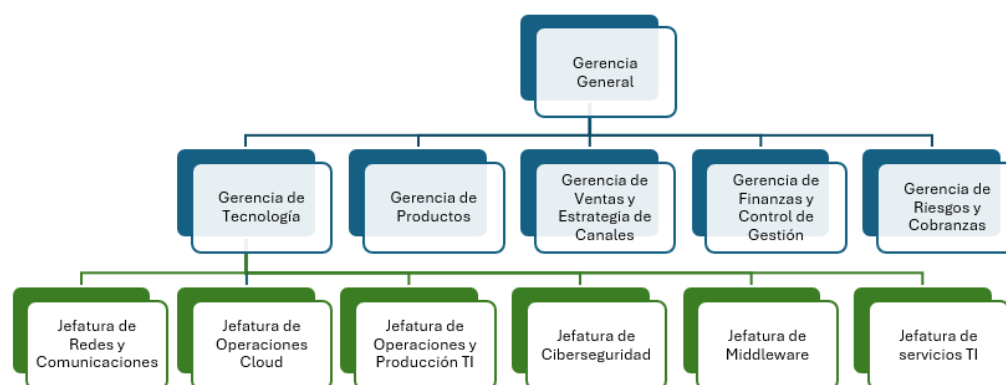
Correo electrónico: cespino@bancoripley.com.pe

CAPITULO III: DESCRIPCIÓN DE LA ACTIVIDAD

3.1 Organización de la actividad

Figura 1

Organigrama de la entidad bancaria.



Fuente: Elaboración propia a partir de documentación interna de Banco Ripley Perú.

3.2 Finalidad y objetivos de la Actividad

3.2.1 Finalidad

Realizar el diseño e implementación de una solución de conectividad para una sucursal bancaria en la ciudad de Iquitos utilizando las tecnologías SD-WAN y Starlink. Esta nueva sucursal debe contar con una infraestructura de red basada en tecnologías de fibra óptica y satelital, en configuración redundante, mediante una solución SD-WAN en alta disponibilidad usando equipos firewall de última generación.

3.2.2 Objetivos

Objetivo general

Asegurar que el servicio de la nueva sucursal bancaria cuente con una alta disponibilidad y el mínimo impacto posible ante la caída del canal principal de fibra que alimenta la ciudad de Iquitos haciendo uso de las tecnologías SD-WAN y satelital.

Objetivos específicos

1. Diseñar la infraestructura de red considerando las limitaciones geográficas y técnicas de la ciudad de Iquitos con énfasis en la disponibilidad y el uso eficiente de los recursos de red.
2. Determinar y dimensionar las tecnologías y el equipamiento necesarios, para la implementación del diseño planteado.
3. Implementar la infraestructura de red diseñada, configurando la solución SD-WAN y realizando pruebas de conectividad y rendimiento para asegurar la alta disponibilidad esperada.

3.3 Problemática

Actualmente, las agencias de Lima y provincias de la entidad bancaria Ripley cuentan con una red MPLS (MultiProtocol Label Switching) de datos contratadas a un único proveedor el cuál proporciona un enlace primario y uno secundario que opera como contingencia. El diseño actual de la red ha ocasionado que, ante una incidencia, en donde la red del proveedor cuenta con un punto único de falla, el servicio de las agencias se vea totalmente afectado ocasionando pérdidas de transacciones e insatisfacción a los clientes. Asimismo, ante el creciente uso de nuevos softwares en los equipos de cómputo y nuevos desarrollos internos del área de tecnología es importante que el ancho de banda de cada agencia pueda soportar el consumo interno y externo de los recursos, lo cual

conllea a que se requiera hacer uso de ambos canales de datos.

Ante la necesidad de ampliar la cobertura de los servicios de negocio de parte del grupo Ripley en el mercado peruano; se identificó una nueva sucursal ubicada en las instalaciones del nuevo Mall Aventura Plaza en la ciudad de Iquitos. Esta nueva sucursal requiere el diseño e implementación de una nueva red la cual debe proporcionar conectividad a los agentes y usuarios administrativos de la nueva agencia hacia los recursos internos del banco ubicados en el Data Center en la ciudad de Lima, así como conectividad hacia internet para los recursos externos. Esta nueva red debe diferenciarse de la infraestructura de las demás sedes en hacer uso de tecnología SD-WAN y Starlink con el fin de lograr el uso eficiente de los recursos, así como proporcionar estabilidad, velocidad y disponibilidad.

El presente trabajo de suficiencia profesional resuelve uno de los problemas de la entidad bancaria Ripley que es conectar una nueva sucursal en la ciudad de Iquitos a la red nacional de la entidad haciendo uso de tecnología SD-WAN y Starlink.

3.3.1 Problema General

¿Cómo puede la entidad bancaria Ripley asegurar una conectividad estable, segura y de alta disponibilidad para su nueva sucursal en la ciudad de Iquitos, considerando las limitaciones de la red actual basada en MPLS incorporando las tecnologías SD-WAN y Starlink para asegurar el acceso a recursos internos y externos?

3.3.2 Problemas Específicos

- ¿Cómo debe ser el diseño de la infraestructura de red que responda a las limitaciones actuales de conectividad en la ciudad de Iquitos, garantizando estabilidad, disponibilidad y rendimiento para la nueva sucursal bancaria?

- ¿Qué tecnologías y equipamiento deben seleccionarse y dimensionarse para implementar una solución de red que garantice conectividad eficiente y segura en la nueva sucursal de Ripley en la ciudad de Iquitos?
- ¿Cómo debe implementarse y configurarse la infraestructura de red basada en SD-WAN para lograr alta disponibilidad y rendimiento en la ciudad de Iquitos?

3.3.3 Justificación e importancia de la investigación

El presente trabajo de suficiencia profesional se justifica por la necesidad de garantizar la alta disponibilidad de los servicios de red para la nueva sucursal de una entidad bancaria en la ciudad de Iquitos. Actualmente, la dependencia de un único enlace de fibra óptica representa un riesgo significativo para la continuidad operativa de la entidad, impactando negativamente en la prestación de servicios a los clientes y en la eficiencia de las operaciones internas. La interrupción de este único canal de comunicación puede generar pérdidas económicas considerables y afectar la reputación de la institución al no garantizar el acceso continuo a los servicios financieros. Por lo tanto, este trabajo de suficiencia profesional se propone diseñar e implementar una nueva arquitectura de red que aborde esta vulnerabilidad. La solución, basada en una red de fibra óptica con tecnología SD-WAN en configuración activo-activo y un medio de transmisión alternativo a la fibra como es el uso de la tecnología satelital, no solo optimizará el uso de los recursos de red, sino que también asegurará la continuidad del servicio, incluso ante fallas del enlace principal. El desarrollo de esta solución es de suma importancia debido a su doble impacto: solucionar la necesidad actual de la entidad bancaria de contar con una red de alta disponibilidad en Iquitos y establecer un modelo replicable para las sedes existentes y las futuras expansiones, especialmente en regiones con infraestructura de comunicaciones limitada.

3.4 Metodología

3.4.1 Bases teóricas

En la actualidad, las empresas cuentan con distintos tipos de tecnologías que les permiten dar solución a los problemas de conectividad que existen. Rak et al. (2021) describen su importancia haciendo mención que, por décadas, se han optado por las redes ópticas como principal tecnología de comunicación para atender el tráfico de la red, esto debido a su alta capacidad y transmisión de larga distancia. Sin embargo, ninguna infraestructura está exenta de sufrir interrupciones, ya sea por una falla propia de la concesionaria, o por agentes externos como desastres naturales, los cuales son más posibles de ocurrir en los sitios más remotos.

Esto conlleva a que se busquen soluciones de conectividad que permitan ofrecer una alta disponibilidad para asegurar la operación de las empresas.

Ramírez et al. (2015) publicaron en su trabajo de investigación que la resiliencia de una red es la capacidad de mantener un nivel aceptable de servicio frente a diversas afectaciones que incluyen fallos de hardware y software, ataques de ciberseguridad, etc. y que abarca la recuperación de los servicios en un tiempo óptimo, así como la adaptación ante condiciones adversas como aspecto crucial. En el estudio se destaca la importancia de identificar los principales desafíos relacionados con las limitaciones de las soluciones actuales en tecnologías y redes de telecomunicaciones. Asimismo, se analizan las tendencias emergentes que pueden contribuir a mejorar la resiliencia de las redes. En el presente trabajo de suficiencia profesional se propone el uso de las tecnologías SD-WAN y satelital Starlink como tecnologías emergentes para asegurar la disponibilidad de la red.

En una red en donde se cuentan con sucursales distribuidas en distintas ubicaciones geográficas del país es importante tener un

control óptimo de todos los componentes de la red, así como poder identificar y gestionar eficientemente el tráfico prioritario para tratarlo de una forma discriminada.

En Yang et al (2019) se detalla un análisis de las arquitecturas WAN tradicionales basadas en MPLS las cuales presentan limitaciones significativas en términos de costo, flexibilidad, complejidad en la gestión y optimización de tráfico de red y propone que la tecnología SD-WAN surge como una solución disruptiva para superar estas limitaciones ofreciendo una mayor agilidad, eficiencia y rendimiento. También, se hace mención de la arquitectura y los avances tecnológicos e implicaciones de la implementación de SD-WAN dentro de las redes empresariales modernas detallando las características distintivas de esta tecnología enfocándose en la gestión centralizada, la capacidad de combinar distintas tecnologías WAN como MPLS, banda ancha, LTE, satelital logrando que se reduzca la dependencia de un único proveedor.

Según Alvaríño Herrera (2024) la infraestructura de conexión a internet en Iquitos ha experimentado mejoras significativas en los últimos años destacando la evolución de la conectividad mediante fibra óptica desde un único tendido existente que conecta Nauta con Iquitos y el sistema de conexión mediante redes microondas con Yurimaguas para acceder a las fibras nacionales de transporte (RDNFO) hasta el 2021 en que el proyecto Amazon Fiber finalizó su primera etapa que consistió en el tendido de un enlace subfluvial, aéreo y terrestre de más de 900Km entre Yurimaguas e Iquitos. Esto hace que la infraestructura de la ciudad se convierta en un elemento importante a considerar durante el diseño de la solución de conectividad de la entidad.

La integración de tecnologías como MPLS y SD-WAN ofrece importantes beneficios en términos de eficiencia, gestión y redundancia en las redes empresariales, no obstante, en escenarios donde existen limitaciones de infraestructura es fundamental evaluar soluciones

alternativas que puedan garantizar la continuidad operativa las cuales deben asegurar la disponibilidad de los servicios críticos ante posibles incidentes que afecten los canales de comunicación principales.

Campana Silverio (2023) sostiene en su trabajo de investigación que los operadores de servicios de conectividad e internet han aumentado el despliegue de fibra óptica en el territorio nacional. Sin embargo, todavía existen zonas que no tienen acceso al servicio de internet. Uno de los principales factores que contribuyen a esta situación es nuestro accidentado relieve, el cual encarece los proyectos de tendido de fibra óptica, por lo que en estos casos se recurre a soluciones satelitales. El autor concluye que la solución óptima es la implementación de un servicio satelital de la marca Starlink sobre el uso de la clásica tecnología VSAT que si bien proporciona una solución de conectividad queda en un plano menor debido a los valores de latencia, anchos de banda y costos comparado con los beneficios que ofrece el hacer uso de Starlink.

3.4.2 Marco conceptual

3.4.2.1 MPLS (Multiprotocol Label Switching)

En Cisco (s.f.-a) se describe que la tecnología MPLS permite a las empresas y a los proveedores de servicios construir redes inteligentes de próxima generación que ofrecen una amplia variedad de servicios avanzados de valor añadido sobre una única infraestructura de red. Esta solución se puede integrar sobre cualquier infraestructura de red que existe en el mercado, como IP, Frame Relay, ATM o Ethernet. Las empresas que cuentan con diferentes enlaces de acceso pueden ser añadidas a un borde de red MPLS sin requerir realizar cambios en su entorno operante debido a que MPLS es independiente de las tecnologías de acceso.

Ahmed y Basit (2014) publicaron en su investigación que el uso de la

tecnología MPLS permite que las redes sean estables, conmutables de forma escalable a alta velocidad y con capacidades de ingeniería de tráfico, lo cual mejora el cumplimiento de los acuerdos de nivel de servicio (SLA). Asimismo, se destacan sus características más relevantes como red privada virtual (VPN), ingeniería de tráfico (TE) y calidad de servicio (QoS).

3.4.2.2 SD-WAN (Software defined Wide Area Network)

Según Cato Networks (s.f.), la solución SD-WAN se define como una arquitectura WAN virtual que permite a las empresas conectar de forma segura y eficiente a los usuarios con las aplicaciones de las empresas. Esta solución tecnológica aporta agilidad y una significativa reducción de costos en las redes de telecomunicaciones. SD-WAN usa los principios de las redes definidas por software (SDN) para conectar ubicaciones y se enfoca en redes de área amplia (WAN) ofreciendo optimización en el uso de múltiples conexiones, mejora del rendimiento y reducción de costos.

La red de área amplia definida por software es considerada la arquitectura de red prometedora de próxima generación, que ofrece a los operadores de red una nueva perspectiva para el diseño de las redes. SD-WAN se propone aplicar técnicas definidas por software para lograr el propósito del control por software, y se enfoca en optimizar y gestionar dinámicamente el tráfico entre ubicaciones distribuidas a través de múltiples tipos de conexión WAN, mientras que SDN está orientada principalmente a la programación centralizada del control del tráfico dentro de redes locales o centros de datos. (Yang et al., 2019, p. 1).

La tecnología SD-WAN tiene un enfoque ágil y basado en software para redes de WAN. Sustituye el equipamiento utilizado en las redes WAN tradicional como los dispositivos configurados mediante de línea de comandos por una administración centralizada para las conexiones y

así ofrecer de manera más eficaz aplicaciones a usuarios en largas distancias. (Cisneros Paladines, 2020, p. 3)

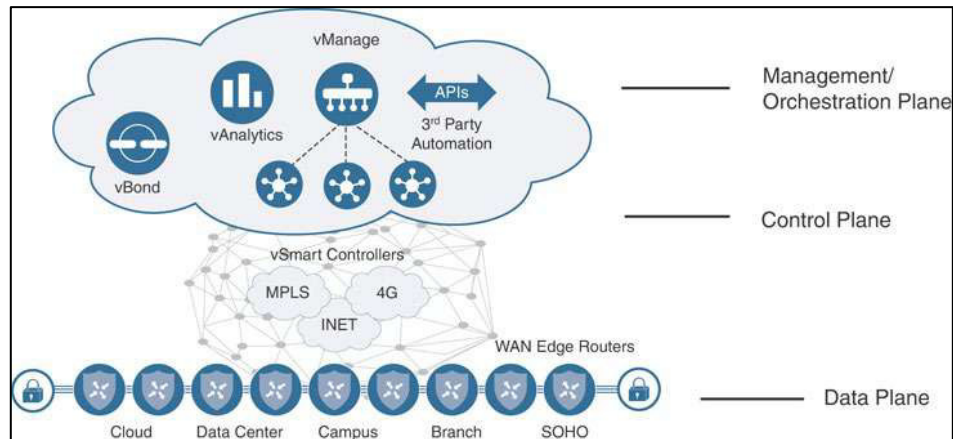
La importancia del uso de la tecnología SD-WAN radica en la mejora del rendimiento, seguridad y flexibilidad de la red WAN debido a que optimiza el flujo de datos basándose en las condiciones actuales, las necesidades de las aplicaciones y las reglas predefinidas permitiendo un mejor control sin sacrificar recursos. Se debe mencionar otro beneficio clave que es la identificación de las mejores rutas para el tráfico generando una mejora en la velocidad y calidad del servicio (Fortinet, s.f.-a).

a.- Funcionamiento de la SD-WAN

En OSTEC (2023) el autor detalla que la administración de una red WAN se ha convertido en un factor determinante que en la operación de una empresa resulta caro e inflexible, no obstante, con las características de la tecnología SD-WAN se simplifica con la aplicación de dispositivos de red programables facilitando a los administradores de redes realizar configuraciones de forma remota. SD-WAN funciona sobre una capa de software que garantiza la calidad del servicio y protección de datos de los enlaces de internet asimismo permite que el tráfico sea enrutado automáticamente a través del camino óptimo de la WAN, considerando las condiciones de seguridad, el costo asociado a cada circuito y la calidad. Esto es llevado a cabo por la toma de decisiones inteligente del software, que hace uso de métricas de calidad como el tiempo de respuesta, y creando una WAN híbrida e que puede incluir una VPN IP para empresas, servicios de internet de banda ancha y servicios inalámbricos evitando que el enrutamiento se base solo en el protocolo dinámico logrando así optimizar el uso de los recursos de red.

Figura 2

Arquitectura referencial de la tecnología SD-WAN de Cisco



Nota. Adaptado de Cisco Software-Defined Wide Area Networks: Designing, Deploying and Securing Your Next Generation WAN with Cisco SD-WAN, de Gooley et al., 2021, Cisco Press

b.- Ventajas de SD-WAN

Fortinet (s.f.-a) describe las ventajas del uso de SD-WAN como una alternativa a las arquitecturas WAN tradicionales debido a que provee mejor rendimiento, seguridad y eficiencia. Las ventajas clave son:

Rendimiento mejorado de la red. SD-WAN prioriza las aplicaciones críticas para el negocio ofreciendo rendimiento óptimo y bajos valores de latencia. Esto se logra ajustando dinámicamente los flujos de tráfico de la red en tiempo real, maximizando la utilización del ancho de banda lo que se traduce en una experiencia de usuario fluida independientemente de la sucursal de la empresa.

Seguridad mejorada. Se incorporan funciones de seguridad avanzadas como firewalls de última generación, sistemas de prevención contra intrusiones y puertas de enlace web seguras permitiendo una segmentación segura de la red aislando datos y aplicaciones sensibles de posibles amenazas.

Eficiencia de costos. Se minimiza la dependencia de enlaces MPLS costosos al beneficiarse de las conexiones de internet de banda ancha

optimizando su uso, Esto conlleva a considerables ahorros de costos sin comprometer el rendimiento ni la seguridad.

Gestión centralizada. El control y visibilidad centralizadas de la red proporciona una gestión y configuración más eficiente y los administradores de red pueden definir y aplicar políticas fácilmente, monitoreo el rendimiento y solucionar problemas desde una única interfaz. Esto genera que las operaciones sean más ágiles y la reducción de carga sobre el personal de TI.

Escalabilidad y flexibilidad. SD-WAN permite que las empresas puedan escalar de una manera fácil la red adaptándose al crecimiento y nuevas demandas.

c.- SD-WAN vs MPLS

Este trabajo de suficiencia profesional presenta el cambio de tecnología de la entidad pasando de arquitectura de red tradicional basada en MPLS al uso de SD-WAN como principal tecnología para las nuevas sucursales.

Tabla 1

Tabla comparativa de características generales de la tecnología actual de la entidad MPLS y la tecnología SD-WAN a implementar en la nueva sucursal

	SD-WAN	MPLS
Complejidad	Si la seguridad no está integrada automáticamente, se deben usar opciones complementarias.	El tráfico de internet es enrutado hacia el centro de datos.
Visibilidad	Amplia visibilidad de las aplicaciones	El enrutamiento de paquetes limita la visibilidad.

Costo	Los servicios consolidados reducen considerablemente el TCO.	Costoso de implementar y mantener.
Rendimiento & Disponibilidad	Permite el uso de MPLS, banda ancha y LTE para alta velocidad.	Ofrece un ancho de banda limitado y un único punto de falla.

Nota. Adaptado de *SD-WAN: Defined and explained*, por Fortinet, s.f., <https://www.fortinet.com/resources/cyberglossary/sd-wan-explained>, CC BY 2.0

3.4.2.3 Medios de transmisión

a.- Fibra óptica

La fibra óptica es un medio de transmisión utilizado en redes de telecomunicaciones para el transporte de datos a altas velocidades y largas distancias. Está compuesta por un filamento de material altamente transparente, usualmente vidrio o plástico, diseñado para guiar señales luminosas mediante el principio de reflexión interna, lo que permite obtener una transmisión eficiente y con mínimas pérdidas. (Info@Citel, s.f.)

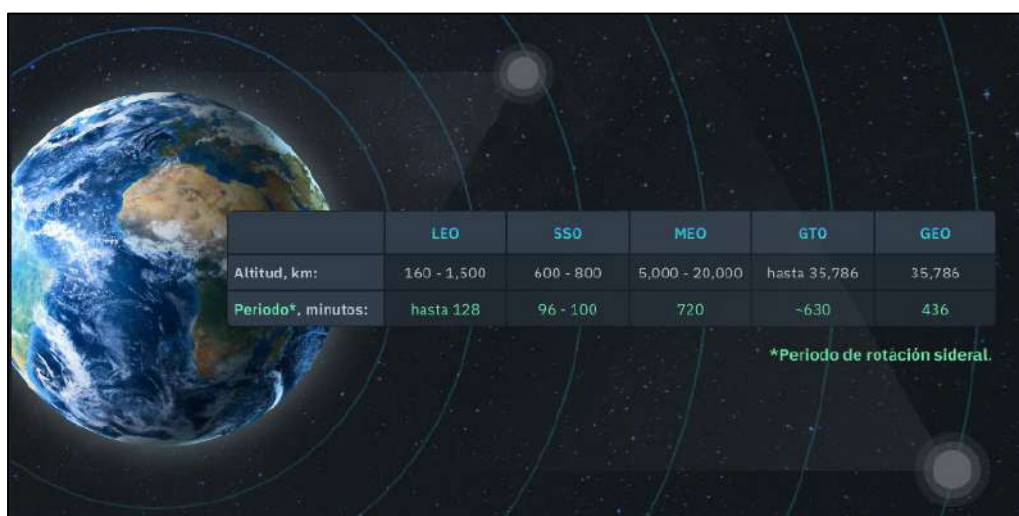
b.- Enlace satelital

Sistema de comunicación inalámbrico que hace uso de satélites artificiales que se encuentran en la órbita terrestre como repetidores para la transmisión de señales de radiofrecuencia (RF) entre dos o más puntos en la superficie.

Los satélites artificiales pueden ser clasificados según su posición orbital que es la distancia que mantienen desde la superficie terrestre en relación con su posición en el espacio.

Figura 3

Distribución y características de satélites artificiales según su órbita de su latitud orbital

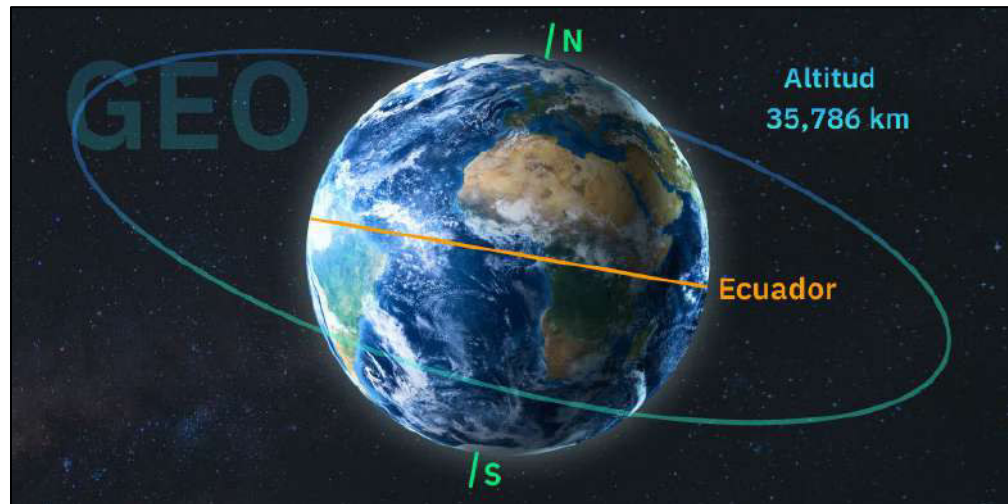


Nota. Adaptado de *Tipos de satélites: Sus órbitas y funciones* [Infografía], por K. Sergieieva, 2025, <https://eos.com/es/blog/tipos-de-satelites/>. CC BY 2.0

Órbita Geoestacionaria (GEO). Se encuentra aproximadamente 35.786 kilómetros sobre la superficie terrestre, más específicamente sobre el ecuador. Debido a su periodo orbital similar a la rotación de la tierra: 23 horas, 56 minutos y 4 segundos, los objetos en esta órbita parecen inmóviles desde la tierra. Su uso está relacionado a los servicios de comunicación siempre activos como la televisión, telefonía. Además, pueden utilizarse en meteorología para el monitoreo del tiempo en regiones concretas y seguir el desarrollo de patrones locales. El mayor desafío que afrontan los satélites GEO frente a otros tipos de satélites espaciales para la comunicación en tiempo real es el retardo de la señal ocasionado por gran distancia con la tierra. (Sergieieva, 2025)

Figura 4

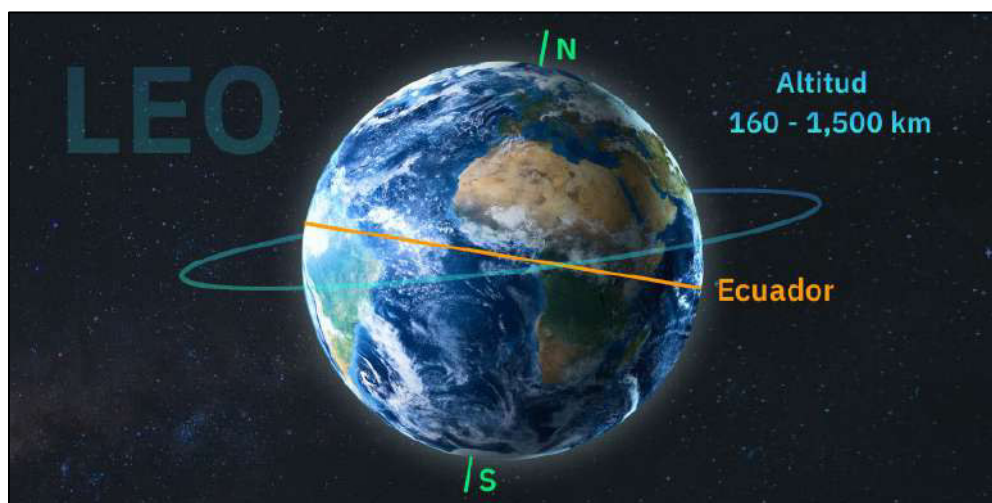
Órbita GEO.



Nota. Adaptado de *Tipos de satélites: Sus órbitas y funciones* [Infografía], por K. Sergieieva, 2025, <https://eos.com/es/blog/tipos-de-satelites/>. CC BY 2.0

Órbita terrestre baja (LEO). Los satélites en una órbita terrestre baja se mueven a una altitud aproximada de 160-1.500 kilómetros sobre la superficie de la Tierra. Tienen un periodo orbital corto, de entre 90 y 120 minutos, lo que significa que pueden dar la vuelta al planeta hasta 16 veces al día. Esto los hace especialmente adecuados para todo tipo de teledetección, observación terrestre de alta resolución e investigación científica, ya que un periodo orbital tan corto permite adquirir y transmitir datos de imágenes satelitales en tiempo real.

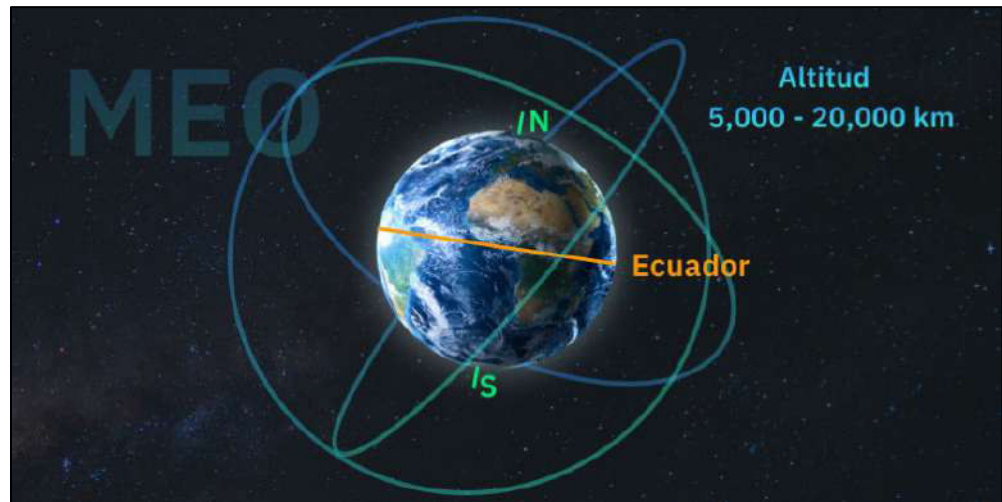
Todos los tipos de satélites en LEO pueden variar el ángulo de su plano respecto a la superficie terrestre. El tipo de órbita terrestre baja es muy común, ya que ofrece más trayectorias potenciales para las naves espaciales. Sin embargo, debido a su proximidad a la Tierra, tienen un área de cobertura menor que otros tipos de satélites. A menudo, se lanzan juntos grupos de satélites LEO, conocidos como constelaciones de satélites, para formar una especie de red que rodea la Tierra. Esto les permite cubrir grandes áreas simultáneamente trabajando juntos. (Sergieieva, 2025)

Figura 5*Órbita LEO.*

Nota. Adaptado de *Tipos de satélites: Sus órbitas y funciones* [Infografía], por K. Sergieieva, 2025, <https://eos.com/es/blog/tipos-de-satelites/>. CC BY 2.0

Órbita media (MEO). Los satélites de tipo MEO se sitúan entre las órbitas terrestre baja y la geoestacionaria, normalmente a una altitud de entre 5.000 y 20.000 kilómetros. Los servicios de posicionamiento y navegación, como el GPS, se apoyan habitualmente en satélites de tipo MEO. Gracias a su mayor periodo orbital (normalmente entre 2 y 12 horas), a diferencia de otros tipos de satélites existentes, ofrece un término medio entre área de cobertura y velocidad de transmisión de datos. Se han puesto en funcionamiento constelaciones de satélites MEO de alto rendimiento (HTS) para permitir la comunicación de datos de baja latencia a proveedores de servicios y organizaciones comerciales y gubernamentales. Los satélites MEO necesitan menos aparatos para dar cobertura mundial, pero su retardo es mayor y su señal más débil. (Sergieieva, 2025).

Figura 6*Órbita MEO.*



Nota. Adaptado de *Tipos de satélites: Sus órbitas y funciones* [Infografía], por K. Sergieieva, 2025, <https://eos.com/es/blog/tipos-de-satelites/>. CC BY 2.0

3.4.2.4 Tecnología Starlink para la comunicación Satelital

Starlink es un servicio de internet satelital operado por SpaceX, la compañía fundada en 2002 por Elon Musk. SpaceX diseña, fabrica y lanza cohetes y naves espaciales. SpaceX comenzó a lanzar satélites Starlink en 2018 y, hasta septiembre de 2022, ha lanzado más de 3000 satélites a la órbita terrestre baja (LEO) Condon (2022).

El desarrollo de esta tecnología se remonta al año 2015 cuando SpaceX anunció sus planes de construir una constelación de satélites para ofrecer Internet global. En 2018, la compañía lanzó los primeros satélites de prueba, Tintin A y Tintin B para, en 2019 realizar el primer lanzamiento oficial de 60 satélites. Hasta el 2024, la compañía ha realizado múltiples lanzamientos y desplegado alrededor de 7000 satélites Starlink expandiendo su cobertura global (Starlink, 2024).

Starlink no es solo un conjunto de satélites, debe considerarse como un ecosistema que incluye satélites, estaciones terrestres y terminales de usuarios el cual opera mediante la red de satélites LEO,

aproximadamente a 550km de altitud. A diferencia de los satélites geoestacionarios ubicados a 35,786km de altitud, Starlink reduce la latencia y mejora la velocidad de conexión.

Satélites de órbita baja. Los satélites Starlink orbitan a menor altitud, esto permite menores tiempos de respuesta comparados a otras tecnologías satelitales.

Terminales de usuarios. También conocidos como Kits Starlink, son equipos que los usuarios finales instalan en hogares o negocios para recibir la señal de internet de los satélites. Está compuesto de una antena parabólica, un router WI.FI y una fuente de alimentación.

Estaciones Terrestres. También conocidos como Gateways, son instalaciones en tierra que realizan la comunicación con los satélites y proporcionan la conexión a la red global de internet (Starlink, s.f.)

Tabla 2

Parámetros técnicos de Starlink.

Nº	Parámetro	Detalle
1	Órbita	550 km sobre la tierra (LEO)
2	Velocidad de internet	50 Mbps a 250 Mbps (Sujetas a condiciones y congestión de la red)
3	Latencia	20 ms a 40 ms
4	Frecuencia de Comunicación	Banda Ku y Ka
5	Número de satélites actuales	Más de 7000 satélites en operación hasta el 2024

Nota. Adaptado de *Starlink Technology*, por Starlink, s.f., <https://www.starlink.com/technology>, CC BY 2.0

La ficha técnica de Starlink se detalla en el anexo A.

3.4.2.5 Componentes de la red

Firewall. Según Fortinet (s.f.-b) es un dispositivo de seguridad de red diseñado para monitorear, filtrar y controlar el tráfico de red entrante y saliente basado en reglas de seguridad predeterminadas. El propósito principal de un firewall es establecer una barrera entre una red interna confiable y redes externas no confiables.

Router. Cisco (s.f.-b) define router como dispositivos que guían y dirigen los datos de red mediante paquetes que contienen varios tipos de datos, como archivos, comunicaciones y transmisiones simples como interacciones web. Los paquetes de datos tienen varias capas o secciones; una de ellas transporta la información de identificación, como emisor, tipo de datos, tamaño y, aún más importante, la dirección IP (protocolo de Internet) de destino. El router lee esta capa, prioriza los datos y elige la mejor ruta para cada transmisión. Un router perimetral, también llamado router de puerta de enlace o "puerta de enlace" para abreviar, es el punto de conexión más externo de la red con las redes externas, incluida Internet.

Los routers perimetrales están optimizados para el ancho de banda y están diseñados para conectarse a otros routers a fin de distribuir los datos a los usuarios finales. Los routers perimetrales no suelen ofrecer Wi-Fi ni la capacidad de administrar redes locales de manera completa. Por lo general, solo tienen puertos Ethernet; una entrada para conectarse a Internet y varias salidas para conectar otros routers.

Switch. Cisco (s.f.-c) Los switches administrados están diseñados para proporcionar el conjunto más completo de funciones a fin de ofrecer la mejor experiencia de aplicaciones, los niveles más altos de seguridad, el control y la administración más precisos de la red, y

ofrecen la mayor escalabilidad en la categoría de configuración fija de switches. Como resultado, los switches administrados suelen implementarse como switches de agregación o acceso en redes muy grandes, o como switches de núcleo en las redes relativamente pequeñas. Los switches administrados deben admitir los switch L2 y el enrutamiento por IP L3. Desde el punto de vista de la seguridad, los switches administrados ofrecen protección del plano de datos (tráfico de usuarios desviado), del plano de control (tráfico que se comunica entre los dispositivos de red para garantizar que el tráfico de usuario vaya al destino correcto) y del plano de administración (tráfico que se usa para administrar la red o el dispositivo mismo). Los switches administrados también ofrecen control de tormentas de red, protección contra denegación de servicio y otras funcionalidades

- Velocidad de switch de red. Las velocidades de switch de red varían. Puede encontrar switches de configuración fija con velocidades de Ethernet rápida (10/100 Mbps), Ethernet de gigabit (10/100/1000 Mbps), de diez gigabits (10/100/1000/10000 Mbps) y hasta de 40/100 Gbps. La tecnología multigigabit también está disponible en algunos switches para proporcionar velocidades de más de 1 gigabit en cables existentes de categoría 5e/6. Los switches tienen una cantidad de puertos ascendentes y una cantidad de puertos descendentes. Los puertos descendentes se conectan a los usuarios finales; los puertos ascendentes se conectan a otros switches o a la infraestructura de red.
- Cantidad de puertos. Los tamaños de switch de red varían. Los switches de configuración fija suelen venir en configuraciones de 5, 8, 10, 16, 24, 28, 48 y 52 puertos. Estos puertos pueden ser una combinación de ranuras SFP/SFP+ para conectividad de fibra, pero lo más común es que sean puertos de cobre con conectores RJ-45 en el frente, que permiten distancias de hasta 100 metros. Con los módulos

SFP de fibra, las distancias pueden ser de hasta 40 kilómetros.

- Apilabilidad de switches de red. A medida que la red crece, necesitará más switches para proporcionar conectividad de red a la cantidad creciente de dispositivos de la red. Al usar switches independientes, cada switch se administra y configura como entidad individual. Por el contrario, los switches apilables proporcionan una manera de simplificar y aumentar la disponibilidad de la red. En vez de configurar, administrar y solucionar problemas de ocho switches de 48 puertos de manera individual, puede administrar los ocho switches como una sola unidad con switches apilables. Con un switch apilable real, estos ocho switches (con un total de 384 puertos) funcionan como un solo switch; hay un solo agente de SNMP/RMON, un solo dominio de árbol de expansión, una sola interfaz web o CLI, es decir, un solo plano de administración. También puede crear grupos de agregación de enlaces que abarquen varias unidades de la pila, el tráfico de replicación de puertos de una unidad de la pila a otra o configurar ACLs/QoS que abarquen a todas las unidades. Este enfoque ofrece varias ventajas operativas valiosas.

VPN IPsec: Cloudflare (s.f.) define a VPN IPsec como un conjunto de protocolos para proteger las conexiones entre dispositivos. Las conexiones VPN se efectúan en redes públicas, pero los datos que se intercambian a través de la VPN siguen siendo privados porque están encriptados. Las VPN permiten acceder e intercambiar datos confidenciales de forma segura en una infraestructura de red compartida, como la Internet pública. Por ejemplo, cuando los empleados están trabajando en remoto en lugar de estar en la oficina, suelen utilizar las VPN para acceder a los archivos y aplicaciones

corporativas. Muchas VPN utilizan el conjunto de protocolos IPsec para establecer y ejecutar estas conexiones encriptadas.

- Intercambio de claves. Las claves son necesarias para la encriptación formada por caracteres aleatorios que puedan utilizarse para encriptar o desencriptar los mensajes. IPsec establece claves con un intercambio de claves entre los dispositivos conectados, para que cada dispositivo pueda desencriptar los mensajes del otro.
- Autenticación. IPsec proporciona autenticación por cada paquete lo cual garantiza que la data proviene de una fuente de confianza y no de un atacante. Este proceso se realiza mediante algoritmos criptográficos que permiten verificar la integridad de los datos, asegurando que no hayan sido alterados durante la transmisión.
- Encriptación. IPsec encripta las cargas útiles dentro de cada paquete y el encabezado IP de cada paquete (a menos que se utilice el modo de transporte en lugar del modo túnel. Esto hace que los datos enviados a través de IPsec se mantengan seguros y privados.
- Desencriptación. En el otro extremo de la comunicación, los paquetes se desencriptan, y las aplicaciones (por ejemplo, un navegador) pueden utilizar ahora los datos entregados.
- Transmisión. Los paquetes IPsec encriptados recorren una o más redes hasta su destino mediante el uso de un protocolo de transporte. Durante la transmisión, el tráfico IPsec se diferencia del tráfico IP normal en el uso de UDP como protocolo de transporte en lugar de TCP.

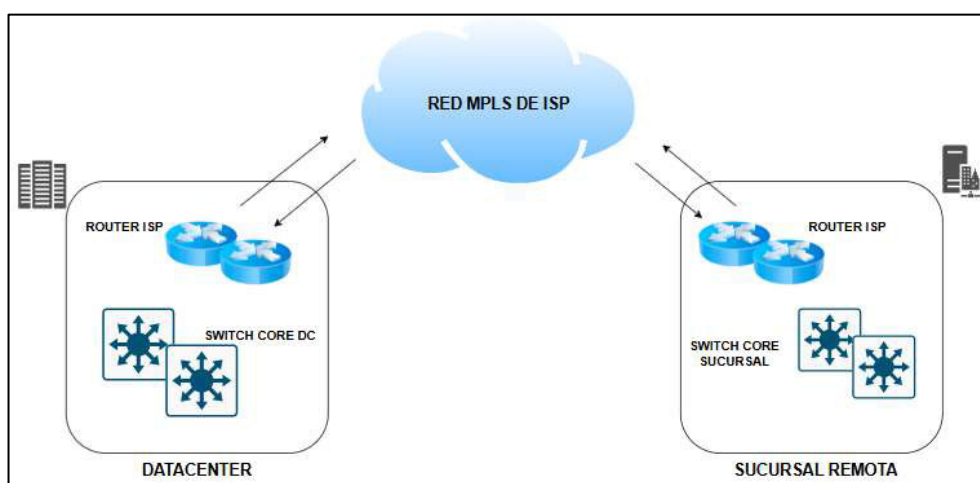
3.5 Procedimiento

3.5.1 Situación actual de la empresa y caso de negocio

La entidad financiera busca optimizar el rendimiento de su infraestructura de red, la cual actualmente cuenta con una topología compuesta por dos enlaces de datos de fibra óptica que usan tecnología MPLS en configuración activo/pasivo para la interconexión de los equipos cabecera con los equipos de las 32 sedes remotas. La red MPLS es provista por una empresa tercera que cuenta con una red desplegada a nivel nacional y que permite la comunicación con los servidores centrales y las agencias. A continuación, se muestra un diagrama topológico de la red de las agencias de la entidad.

Figura 7

Topología MPLS de la entidad bancaria.



Nota. La figura muestra la topología actual de las sedes de la entidad bancaria. Fuente: Elaboración propia.

Esta topología hace uso de equipos Cisco Nexus C9504 que sirven como equipos Core central de datos ubicados en el data center principal en Lima y en las sedes remotas equipos Cisco C3850 que sirven como equipos Core para cada agencia. En la capa de acceso se

cuentan con switches Cisco de la familia 2960 para dar servicio y conectividad a los hosts finales.

En un escenario en donde uno de los canales de fibra óptica no se encuentre disponible, el enlace de contingencia del proveedor entra en funcionamiento y mantiene el servicio de la agencia operativo mientras se ejecutan los trabajos de reparación sobre el enlace afectado.

No obstante, se han presentado situaciones en las que la caída del nodo del proveedor o la interrupción del tramo común de ambas fibras ópticas que abastecen la ciudad donde se ubica la sede remota provoca una afectación total del servicio, generando pérdidas económicas significativas para la empresa. Esta problemática conlleva a que la entidad, para su nueva sucursal, busque una topología que ofrezca mayor resiliencia por lo que se plantea la implementación de una solución basada en SD-WAN, aprovechando su capacidad balanceo de carga y selección de rutas dinámicas en conjunto con la alta disponibilidad que proporciona el servicio de internet satelital de Starlink.

3.5.2 Información de las sucursales involucradas en el proyecto

La entidad cuenta con una red de agencias distribuidas estratégicamente en las principales ciudades del territorio nacional, lo que garantiza cobertura y acceso a sus servicios. Como parte del proyecto de expansión, se ha planificado la implementación de una nueva sucursal en la ciudad de Iquitos. A continuación, se presenta un cuadro resumen con el detalle de las locaciones existentes y la nueva sede proyectada.

Tabla 3

Información general de las sucursales de la entidad involucradas en el proyecto

N°	Nombre de la empresa	RUC	Ubicación	Sede
1	Banco Ripley Perú SA	20259702411	Data Center Lince (TDP)	Cabecera
2	Banco Ripley Perú SA	20259702411	Agencia Iquitos	Sede remota

Fuente: Elaboración propia.

Tabla 4

Ubigeo y coordenadas.

Latitud	Longitud	Distrito	Ciudad	Departamento
-3.765025	-73.267098	San Juan Bautista	Iquitos	Loreto
-12.081955	-77.032452	Lince	Lima	Lima

Fuente: Elaboración propia.

3.5.3 Infraestructura de red de la ciudad

Actualmente la ciudad de Iquitos dispone de una red de fibra óptica que cubre el tramo Iquitos-Yurimaguas permitiendo la interconexión con la Red dorsal nacional de fibra óptica (RDNFO). No obstante, esta conexión depende de un único canal de fibra que atraviesa el río Amazonas, lo que representa un riesgo que debe ser considerado durante el diseño de la nueva topología de red. Ante una eventual interrupción de este canal, la nueva agencia podría quedar sin comunicación, incluso si se cuenta con un enlace redundante sobre la misma infraestructura. Debido a esto se han evaluado mecanismos adicionales que permitan una red resiliente y la continuidad operativa.

Figura 8

Trazado referencial de la fibra óptica en Iquitos.



Nota. Adaptado de Fibra óptica subfluvial Yurimaguas-Iquitos
 [Infografía], por Telecomunicaciones Perú, 2020,
<https://telecomunicaciones-peru.blogspot.com/2020/06/fibra-optica-subfluvial-yurimaguas.html>, CC BY 2.0

Si bien la fibra óptica continúa siendo el medio principal de conexión a Internet para las empresas debido a su alta capacidad y velocidad, el uso de la tecnología satelital ha cobrado relevancia como una alternativa viable. Esta tecnología ofrece anchos de banda adecuados y una estabilidad suficiente para satisfacer las necesidades de organizaciones que realizan transacciones en tiempo real, especialmente en zonas donde la infraestructura terrestre es limitada o inexistente.

3.5.4 Diseño y dimensionamiento de la red

El diseño de la red para la nueva agencia obedece a la necesidad de optimizar los recursos como equipamiento y ancho de banda para mejorar los valores de latencia y rendimiento de la red. El diseño elegido se basa en un análisis de alternativas de solución,

consideraciones técnicas, limitaciones y condiciones identificadas para la implementación de la solución.

Con respecto a la interconexión con la red existente de la entidad, se plantea el uso de un enlace de datos para lograr llegar a los servicios alojados en el data center principal ubicado en la ciudad de Lima. Esta red es proporcionada sobre la plataforma MPLS de un proveedor de servicios (ISP).

Como segundo enlace, se plantea el uso de un enlace de internet puro sobre la red de proveedor de servicios (ISP), el cuál debe ser distinto al proveedor de servicio de datos. Este enlace de datos tendrá una función de tomar el tráfico definido por la configuración SD-WAN permitiendo el balanceo de carga óptimo de la red.

Ambos enlaces se encontrarán en una configuración activo-activo permitiendo hacer uso eficiente del ancho de banda de ambos enlaces. Y al mismo tiempo son backup uno del otro, logrando así una red redundante. No obstante, es importante considerar durante el diseño que debido a la infraestructura de red existente en la región de Iquitos en la cual la conexión de ambos enlaces con la RDNFO comparte tramos comunes los cuales son convertidos en puntos de fallas críticos.

Debido a esto, se consideró el uso de una tercera contingencia basada en tecnología satelital, para lo cual se hace uso de una antena Starlink que ofrece valores técnicos esperados detallados en la tabla 5 y 6 para el funcionamiento de la operación. La función de este enlace es servir como contingencia ante la caída de ambos enlaces de fibra óptica. Para el servicio satelital a contratar se consideró el plan empresarial de Starlink con las siguientes especificaciones:

Tabla 5

Características y especificaciones técnicas del plan empresarial Starlink.

Característica	Detalle
Tipo de plan	Starlink Business
Prioridad de datos	1 TB mensual (alta prioridad en congestión)
Velocidad de descarga	40–220 Mbps (prioritaria mientras no se exceda el TB asignado)
Velocidad de carga	8–25 Mbps
Latencia	25–50 ms
Uso tras exceder 1 TB	Se continúa con datos estándar (menor prioridad)
Tipo de antena	High Performance Dish (mejor resistencia a clima y más área)
Resistencia climática	Mejor desempeño en condiciones extremas
Usuarios ideales	Empresas, oficinas remotas, ISPs rurales
Portabilidad	Disponible (debe activarse, depende del país)
Contrato / permanencia	Sin contrato a largo plazo, cancelación flexible
IP pública	No incluida por defecto (usa CGNAT)
Soporte técnico	Prioritario, especializado para empresas
Firmware / actualizaciones	Automáticas
Instalación	Autoinstalable o profesional (opcional)

Nota. Adaptado de *Planes de servicio: Starlink para empresas*, por SpaceX, 2024, <https://www.starlink.com/pe/service-plans/business>, CC BY 2.0

Los anchos de banda son distribuidos de la siguiente forma:

Tabla 6

Distribución de capacidad de los enlaces.

Enlace	Uso	Tipo	Capacidad
Datos	Activo	Fibra óptica	10Mbps

Internet	Activo	Fibra óptica	10Mbps
Satelital	Contingencia	Satelital	1TB (plan mensual)

Fuente: Elaboración propia.

También se han tomado las siguientes consideraciones para el diseño de red:

- Los router CPE por cada servicio contratado serán instalados por el proveedor y definirán el camino sobre la cuál será enviado el tráfico.
- Se establecerán 3 enlaces VPN IPSec (internet, datos y satelital) hacia la cabecera ubicada en el data center de Lima.
- Se aplicará SD-WAN para definir el tráfico que será enviado por el enlace de datos y el tráfico que se enviará por el enlace de internet. Este criterio será definido mediante pesos por cada interfaz VPN existente.
- El enlace de internet y el enlace de datos mantendrán el servicio en una configuración activo-activo. En caso uno de los enlaces presente un incidente, todo el tráfico conmutará automáticamente hacia el otro enlace.
- La interfaz VPN del enlace satelital tendrá configurado un menor peso, y solo entrará en operación cuando los enlaces de internet y datos no se encuentren disponibles.
- Se utilizará cuatro equipos de acceso a la red (capa 2) para los usuarios finales que contarán con todas las VLAN de servicio propagadas.

3.5.4.1 Equipamiento para la red propuesta

Con base en las consideraciones previamente establecidas, se determina el equipamiento requerido que cumple con las características técnicas adecuadas definidas en el diseño de red para garantizar el desempeño óptimo de la red y la alta disponibilidad esperada.

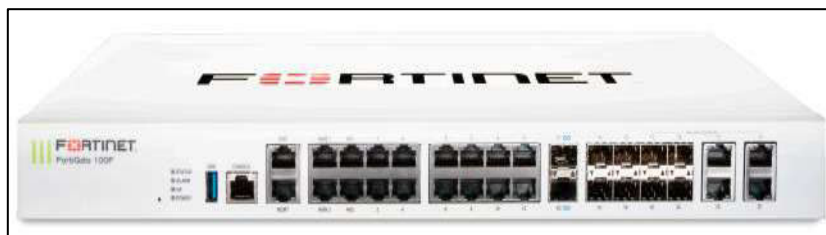
Fortigate 100F

Fortinet(s.f.-c) menciona que el equipo Fortigate 100F ofrece un alto rendimiento en el procesamiento de tráfico de red, inspección de amenazas, VPN, inspección SSL/TLS sin sufrir una degradación del rendimiento. Además de ofrecer seguridad, incluye funcionalidades SD-WAN sin coste de licencia adicional.

Esta tecnología ofrece alta densidad de puertos como GR RJ45, SFP y SPF+ de 10G, así como conectividad flexible para los diversos segmentos de red LAN y WAN adaptándose al escenario propuesto para la nueva agencia.

Figura 9

Fortigate 100F.



Nota. Adaptado de *Fortigate 100F series data sheet* [Infografía], por Fortinet, s.f.,
<https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-100f-series.pdf>, CC BY 2.0

Tabla 7

Característica Fortigate 100F.

Característica	Especificación
Rendimiento VPN IPSec	Hasta 13 Gbps
Sesiones Concurrentes	Hasta 1.5 Millones (TCP)

Interfaces de red	12 x GE RJ45 (LAN/WAN), 2 x puertos WAN GR RJ45, 2 x puertos 10GE SPF+ (Fortilink/WAN/LAN), 2 x puertos GE SFP, 1 x puerto GE RJ45 MGMT, 1 x puerto GE J45 HA
Almacenamiento integrado	1 x SSD integrado (120GB o 240GB)
Sistema Operativo	FortiOS
Factor de forma	1RU

Nota. Adaptado de *FortiGate 100F series data sheet*, por Fortinet, 2025, <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-100f-series.pdf>, CC BY 2.0

La ficha técnica con las especificaciones del equipo Fortigate 100F se detalla en el anexo B.

Cisco C9200L

Cisco (s.f.-d) destaca los beneficios de la serie 9200 de sus productos como un hardware que ofrece simplificar la complejidad, optimizar las redes y reducir el costo operacional aumentando las capacidades de operación, así como resiliencia para la continuidad del negocio. La capacidad PoE+, redundancia de fuente de poder y ventiladores, ancho de banda de stack de hasta 160Gbps, compatibilidad con funciones de capa 3 hace que de este producto una solución diferenciada en el mercado.

Figura 10

Cisco C9200L-24P.



Nota. Adaptado de *Cisco Catalyst 9200 series switches data sheet*
 [Infografía], por Cisco, 2025,
<https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9200-series-switches/nb-06-cat9200-ser-data-sheet-cte-en.html>, CC
 BY 2.0

La elección de este modelo como switch de acceso para la nueva sucursal obedece a que el modelo estándar Cisco C2960 usado en las sucursales existentes ya se encuentra discontinuado. El equipo que ofrece funcionalidades similares es el equipo Cisco C9200L-24P-4X.

Tabla 8

Características y especificaciones técnicas del equipo Cisco modelo C9200L-24P.

Característica	Especificación
Tipo de Switch	Switch de capa 2 y capa 3
UpLinks	4 puertos uplink SFP+ 10GE
Puertos Ethernet	24 x puertos G2 PoE+ (10/100/1000 Mbps)
Capacidad PoE	Hasta 370W PoE+
Capacidad de switching	128 Gbps
Sistema Operativo	Cisco IOS XE
Factor de forma	1RU

Nota. Adaptado de *Cisco Catalyst 9200 series switches data sheet*,
 por Cisco, s.f.,
<https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9200-series-switches/nb-06-cat9200-ser-data-sheet-cte-en.html> , CC
 BY 2.0

La ficha técnica del equipos switch Cisco C9200L se detalla en el anexo C.

En resumen, se consideran dos (2) equipos Fortigate 100F que cumplirán la función de Core de la nueva agencia con configuración en alta disponibilidad (HA).

Asimismo, para la red LAN de acceso se consideran cuatro (4) equipos switch Cisco C9200L-24P para la conexión de los dispositivos de usuarios (PCs, laptops, impresoras).

Tabla 9

Dimensionamiento de equipamiento de red.

Sede	Función	Cantidad	Equipo propuesto	Licenciamiento
Iquitos	Core de agencia	2	Fortigate 100F	FortiCare Premium - 3Y
Iquitos	SW Lan	4	Cisco C9200L- 24P-4X	Network Essentials

Nota. La figura muestra el dimensionamiento de equipos de red para la implementación de la nueva sucursal en la ciudad de Iquitos.

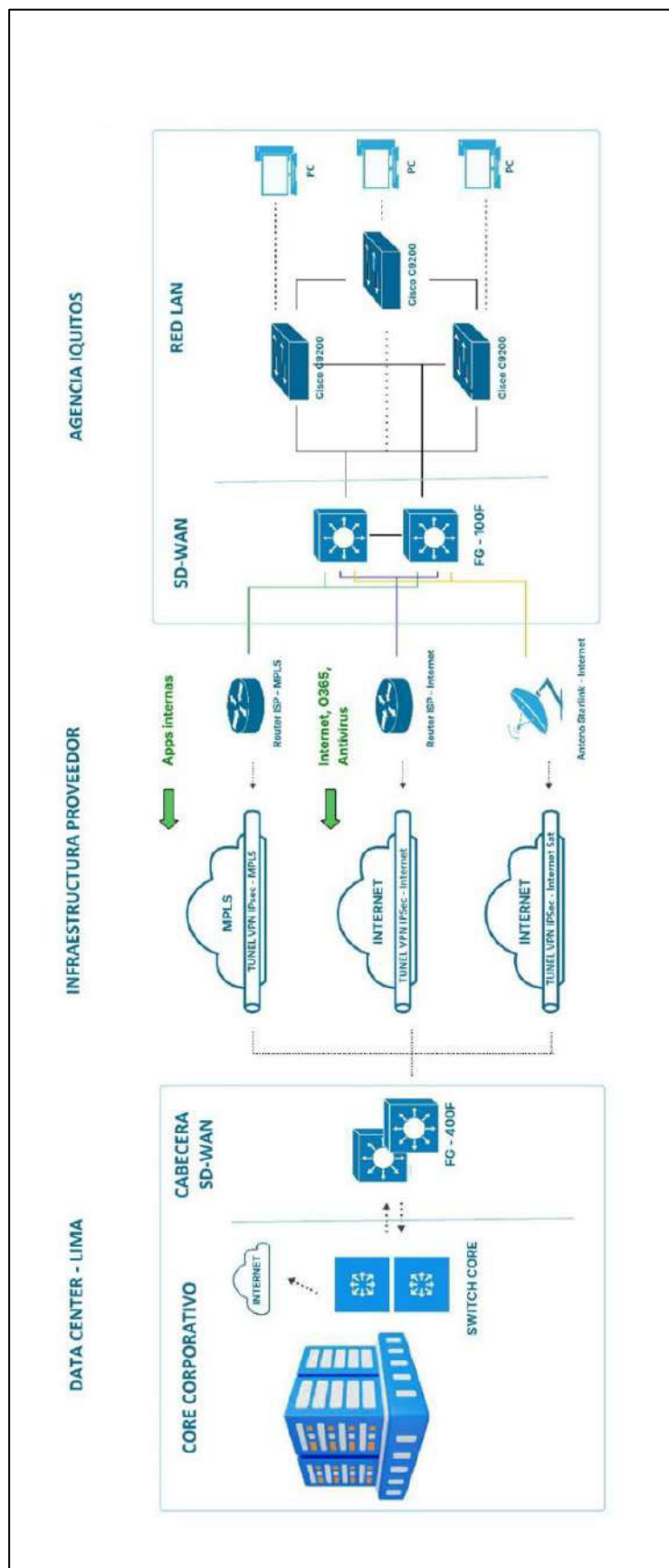
Fuente. Elaboración propia.

3.5.5 Diagrama de red

Se genera la topología propuesta para la solución requerida por la entidad acorde a las especificaciones técnicas y la elección del equipamiento según el diseño realizado.

Figura 11

Diseño de red propuesto para la nueva sucursal.



Nota. La figura muestra el diseño de red a implementar en la nueva sucursal. Fuente: Elaboración propia.

Consideraciones:

1. La cabecera SD-WAN ubicada en el data center de Lima ya se encuentra implementada, sin embargo, la primera sede en hacer uso de esta conexión es la sucursal Iquitos.
2. La red MPLS del proveedor de servicios proporciona la conectividad con las sucursales existentes a nivel nacional.
3. La red de Internet por fibra e internet satelital permiten la salida de tráfico diferenciado mediante el balanceo de carga configurado en los equipos Fortigate 100F.
4. Los canales de comunicación de fibra y satelital tienen configurado un túnel IPSec, esto con la finalidad de poder realizar el balanceo de carga y distribución de pesos en la configuración SD-WAN.
5. El túnel MPLS es responsable de la comunicación hacia los servicios internos de la entidad bancaria, mientras que el canal de internet proporciona la conectividad hacia recursos como Office365 y actualizaciones de software como Windows o antivirus.
6. La red LAN está formada por tres (3) switches Cisco C9200L-24P, un equipo adicional es almacenado en la sala data center de la sucursal como equipo de backup.

3.5.6 Etapa de factibilidad

Para este proyecto se debe considerar recursos de infraestructura provistos por el centro comercial como parte del arrendamiento de la zona bancaria hacia la entidad financiera, debido a esto, se consideran los siguientes puntos:

- **Planta Externa:** Previo a la implementación de los servicios de red en la entidad se realizó la inspección in situ y evaluación de la infraestructura del nuevo centro comercial con lo cual se determinó los recursos técnicos tales como la ruta de ingreso de la fibra óptica de los proveedores de telecomunicaciones, la interconexión del ODF del proveedor en la sala DataCenter, el

área de instalación en la azotea del CC para la antena Starlink y el cableado hasta la sala DataCenter.

- **Planta Interna:** Se realizó una inspección interna de la sala de data center y se determinó la ubicación de los equipos de networking en los gabinetes (RU), el tipo de cableado a ejecutar por parte del proveedor interno de la entidad, las posiciones que se deben habilitar dentro de la zona bancaria.

3.6 Resultado de la actividad

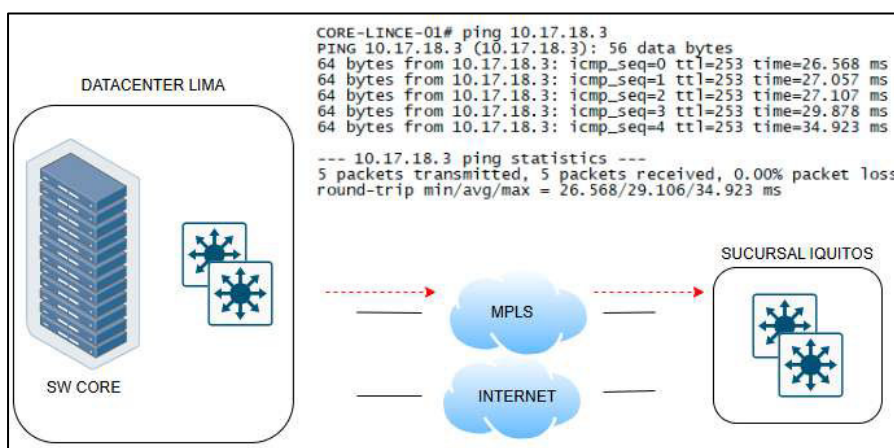
Una vez finalizada la implementación y configuración del equipamiento networking en la nueva sede se procede con las pruebas de validación.

3.6.1 Conectividad entre equipo Core Lima y Core Iquitos

Se procede a verificar la conectividad entre el Core ubicado en el data center de Lima y los equipos Core Fortigate 100F instalados en la sucursal de Iquitos. Se valida a través de la herramienta de conexión remota SecureCRT y comprobamos la comunicación en capa 1, 2 y 3:

Figura 12

Validación de conectividad entre DC Lima e Iquitos.



Nota. La figura muestra la prueba de conectividad entre la nueva sucursal y el DataCenter principal de la entidad. Fuente: Elaboración propia.

Observaciones:

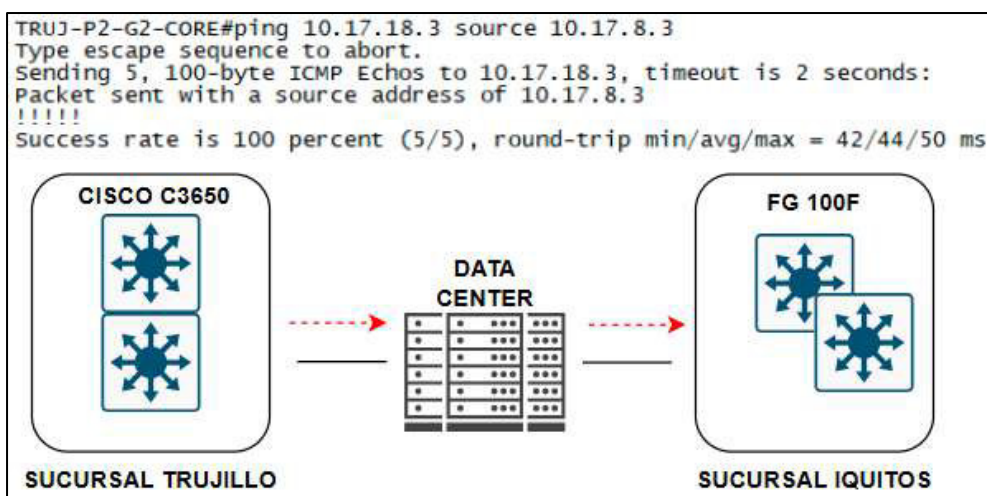
- La prueba de ping valida la conexión entre el Core de Lima y el core de Iquitos que pasa a través del enlace VPN sobre MPLS.
- Los tiempos de respuesta son los esperados para un enlace de fibra óptica.

3.6.2 Conectividad entre sedes remotas

Las redes LAN entre las sucursales deben ser alcanzables para la comunicación entre usuarios. Se procede a verificar la conectividad entre el Core de la sucursal Trujillo y el equipo Core de la sucursal Iquitos.

Figura 13

Validación de conectividad entre sucursales.



Nota. La figura muestra la prueba de conectividad entre la nueva sucursal y una sucursal remota de la entidad. Fuente: Elaboración propia.

3.6.3 Pruebas de redundancia

El propósito principal del proyecto es el diseño e implementación de una red redundante que ante la caída de un enlace de fibra el tráfico

sea derivado al otro canal activo, y ante la caída de ambos enlaces de fibra, el servicio satelital asuma toda la carga de tráfico de la sucursal.

Para la ejecución de las pruebas de redundancia es importante mencionar la configuración que permite lograr la alta disponibilidad esperada. Esto se logra mediante el monitoreo de salud (health check) y a la evaluación continua de los enlaces WAN para la toma de decisiones dinámicas en el envío de tráfico. A continuación, se muestran las configuraciones realizadas:

Performance SLA (SLA checks).

Figura 14

Configuración Performance SLA.

Edit Performance SLA

Name: SLA Lo0 HUB

Probe mode: **Active** | Passive | Prefer Passive

Protocol: **Ping** | HTTP | DNS

Server: 10.254.254.1

Participants: All SD-WAN Members | **Specify**

- CNX-TDP-LIMA ✕
- VPN-GFIBER-LIMA ✕
- VPN-LIMA-TDP ✕

SLA Target: ☐

Link Status

Check interval: 500 ms

Failures before inactive: 5

Restore link after: 5 check(s)

Actions when Inactive

Update static route: ☒

Nota. La figura muestra la configuración del Performance SLA en los equipos SD-WAN de la nueva sucursal. Fuente: Informe interno de instalación de servicio.

Probe Mode. El modo de prueba Active permite que el SD-WAN monitoree el estado de los enlaces mediante el uso de un protocolo en específico.

Protocol. La disponibilidad de los enlaces será verificada mediante el uso del protocolo ping (ICMP Echo Request).

Server. Se determina el servidor destino para las pruebas de ping la cabecera SD-WAN en Lima con IP 10.254.254.1.

Participantes. Se consideran los enlaces de datos, internet e internet satelital para el monitoreo de salud.

Check Interval. Se configura un intervalo de 500 ms para el envío de un ping al servidor destino y verificar el estado de los enlaces.

Failures before inactive. Se configura 5 intentos de ping (2.5 segundos) fallidos para que el enlace sea considerado como inactivo.

Restore link after. Se configura 5 intentos de ping (2.5 segundos) exitosos para considerar el enlace como activo nuevamente.

Update static route. Permite que la tabla de enrutamiento del Fortigate se actualice dinámicamente según el estado del enlace.

Reglas SD-WAN

Figura 15

Configuración de reglas SD-WAN.

SD-WAN Zones		SD-WAN Rules		Performance SLAs	
+ Create New		Edit	Clone	Delete	Search
ID	Name	Source	Destination	Members	
4	TO_OFFICE365_TRENDMICRO_TEAMS	all	Microsoft-Skype_Teams Microsoft-Teams.Published.Worldwide.Allow Microsoft-Teams.Published.Worldwide.Optimize Microsoft-DNS	INET1-GFIBER (INET1-GFIBER) VPN-LIMA-TDP INET2-STARLINK (INET2-STARLINK)	
2	TO_VPN_LIMA	all	all	VPN-LIMA-TDP VPN-GFIBER-LIMA CNX-TDP-LIMA	

Fuente: Informe interno de instalación de servicio.

Las reglas se han configurado usando el modo Manual para establecer las prioridades de las interfaces. Esto permite que el Fortigate envíe el

tráfico definido en la regla por las interfaces declaradas según orden de prioridad.

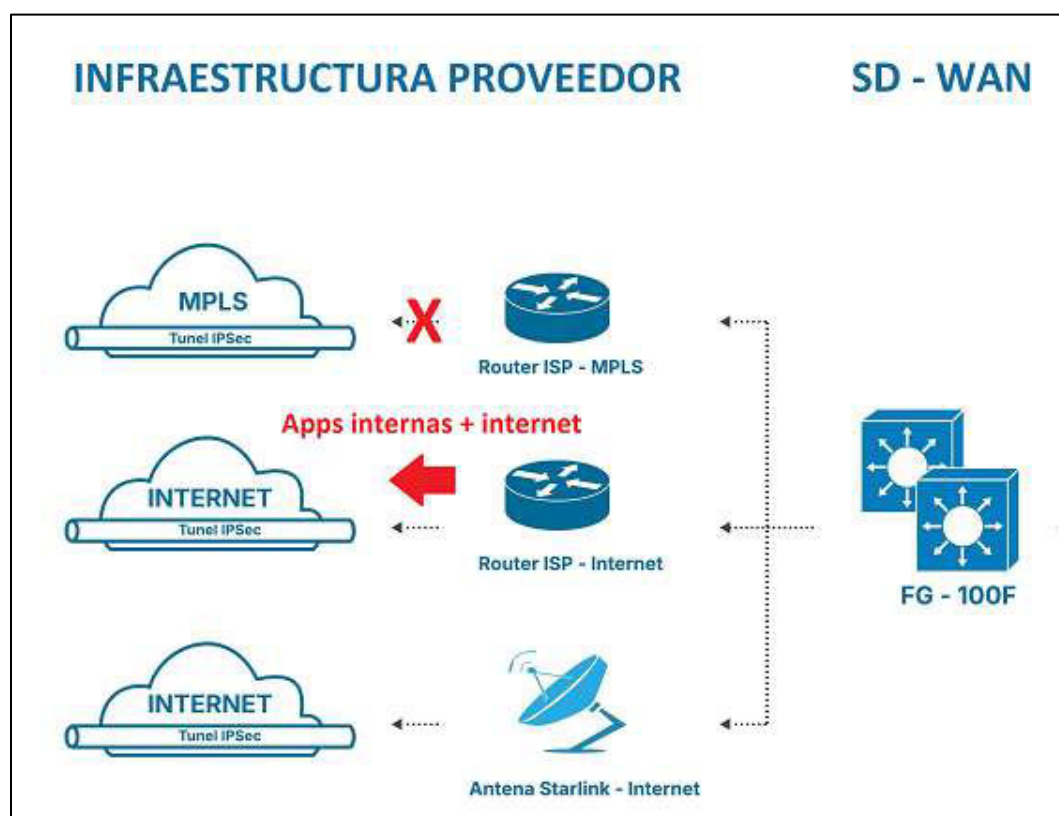
Se plantean los siguientes escenarios para las pruebas de redundancia:

3.6.3.1 Escenario 1: Caída del enlace datos

En este escenario se plantea la caída del enlace de datos MPLS, debido a la configuración activo-activo todo el tráfico debe ser asumido por el enlace de internet.

Figura 16

Caída de enlace de datos.



Nota. La figura muestra el escenario ante la caída del enlace de datos de la nueva sucursal. Fuente: Elaboración propia.

Observaciones:

- Ante la caída del canal de datos, se pierde la conectividad desde los equipos finales hacia la VPN sobre MPLS.
- La configuración SD-WAN realiza el monitoreo de salud de los enlaces (health check) haciendo uso del performance SLA y reglas configuradas. Tras la caída del túnel VPN sobre el enlace de datos VPN-LIMA-TDP, el tráfico hacia los recursos internos de la entidad es enrutado hacia el túnel VPN sobre internet VPN-GFIBER-LIMA. El tráfico hacia los recursos de internet definidos en la regla se mantiene sobre la interfaz INET1-GFIBER definida según orden de prioridad.

Figura 17

Interfaces SD-WAN del canal de internet activas por orden de prioridad debido a la caída del enlace de datos.

SD-WAN Zones				
SD-WAN Rules				
Performance SLAs				
+ Create New Edit Clone Delete Search				
ID	Name	Source	Destination	Members
IPv4 2/5				
4	TO_OFFICE365_TRENDMICRO_TEAMS	all	Microsoft-Skype_Teams Microsoft-Teams.PublishedWorldwide.Allow Microsoft-Teams.PublishedWorldwide.Optimize Microsoft-DNS	INET1-GFIBER (INET1-GFIBER) ✓ VPN-LIMA-TDP INET2-STARLINK (INET2-STARLINK)
2	TO_VPN_LIMA	all	all	VPN-LIMA-TDP VPN-GFIBER-LIMA ✓ CNX-TDP-LIMA

Fuente: Informe interno de instalación de servicio.

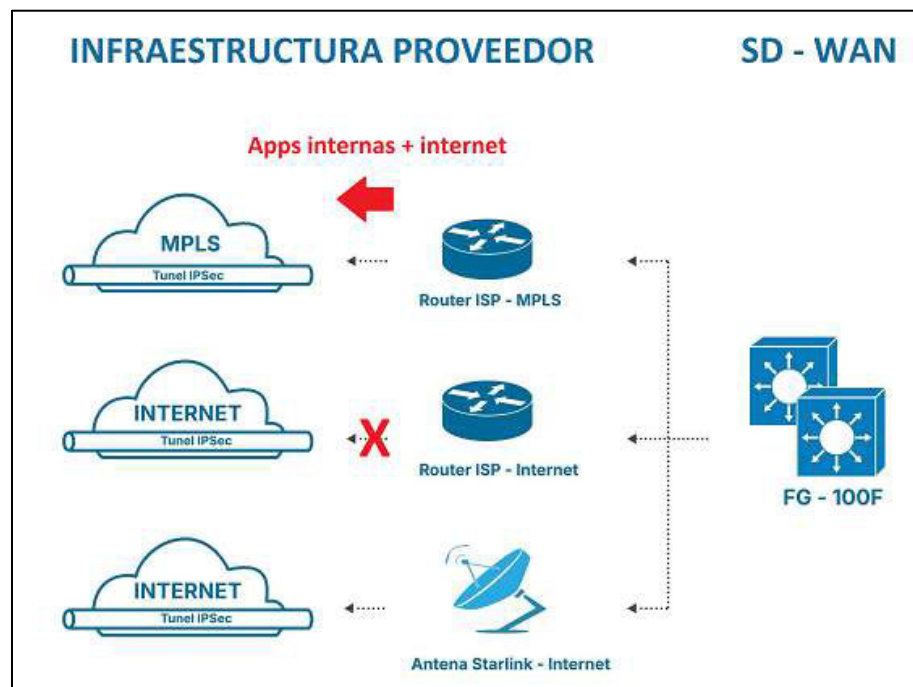
- SD-WAN determinó que el tráfico de datos ahora debe ir por el túnel VPN sobre el canal de internet VPN-GFIBER-LIMA, y así alcanzar los recursos internos de la entidad demostrando la alta disponibilidad de la red.
- Una vez superado el incidente del canal de datos, la configuración de performance SLA determina que el enlace se encuentra activo y realiza la actualización en la regla SD-WAN retornando al funcionamiento inicial.

3.6.3.2 Escenario 2: Caída del enlace de internet

En este escenario se plantea la caída del enlace de internet de fibra óptica, debido a la configuración activo-activo todo el tráfico debe ser asumido por el enlace de datos.

Figura 18

Caída de enlace de internet.



Fuente: Elaboración propia.

Observaciones:

- Ante la caída del canal de internet de fibra óptica, se pierde la conectividad hacia internet de los equipos finales. Solo tendrán acceso a los recursos internos de la compañía y no el tráfico definido a ir hacia internet.
- La configuración SD-WAN realiza el monitoreo de salud de los enlaces (health check) haciendo uso del performance SLA y reglas configuradas. Tras la caída de la interfaz INET1-GFIBER, el tráfico hacia internet es enrutado hacia el túnel VPN sobre el enlace de

datos VPN-LIMA-TDP. El tráfico hacia los recursos internos de la entidad se mantiene sobre el túnel VPN-LIMA-TDP definido según orden de prioridad.

Figura 19

Interfaces del canal de datos activas por orden de prioridad.

SD-WAN Zones		SD-WAN Rules		Performance SLAs	
+ Create New		Edit	Clone	Delete	Search
ID	Name	Source	Destination	Members	
IPv4 2/3					
4	TO_OFFICE365_TRENDMICRO_TEAMS	all	Microsoft-Skype_Teams Microsoft-Teams.Published.Worldwide.Allow Microsoft-Teams.Published.Worldwide.Optimize Microsoft-DNS	INET1-GFIBER (INET1-GFIBER) VPN-LIMA-TDP INET2-STARLINK (INET2-STARLINK)	
2	TO_VPN_LIMA	all	all	VPN-LIMA-TDP VPN-GFIBER-LIMA CNX-TDP-LIMA	

Fuente: Informe interno de instalación de servicio.

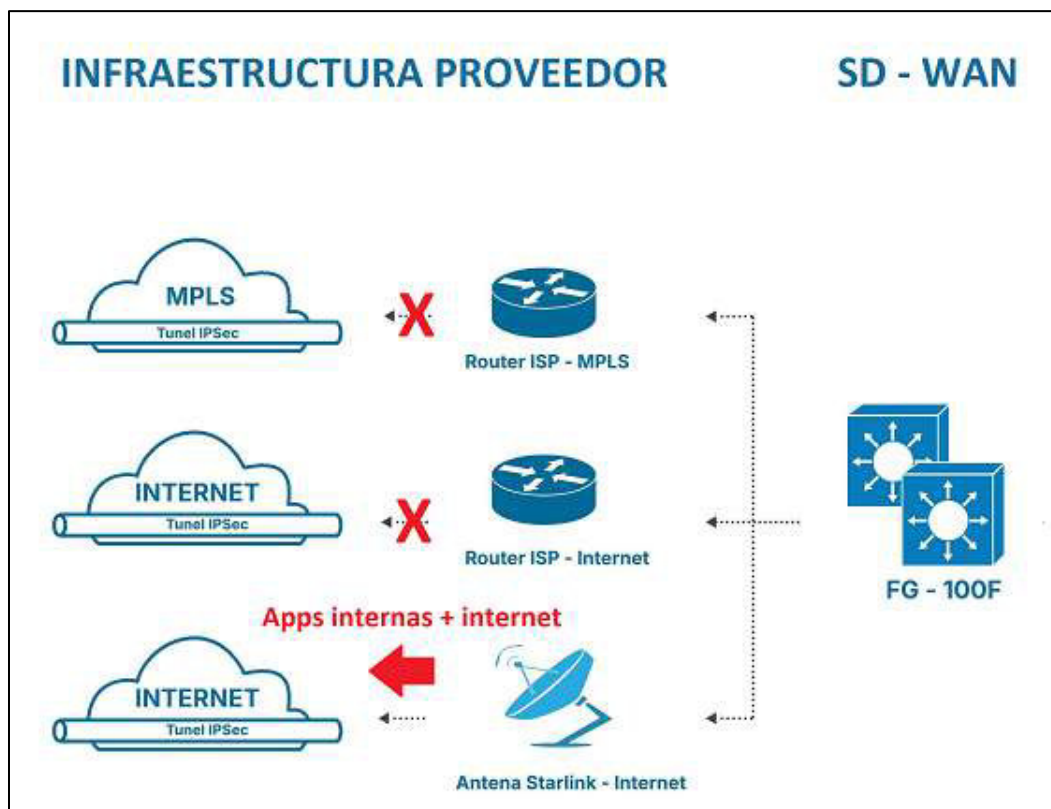
- SD-WAN determina que el tráfico de internet debe ir por el túnel VPN sobre el canal de datos VPN-LIMA-TDP para llegar a la salida de internet corporativo en el datacenter de Lima y así alcanzar los recursos de internet definidos en la regla demostrando la alta disponibilidad.
- Una vez superado el incidente del canal de internet, la configuración de performance SLA determina que el enlace se encuentra activo y realiza la actualización en la regla SD-WAN retornando al funcionamiento inicial.

3.6.3.3 Escenario 3: Caída de los enlaces de datos e internet

En este escenario se plantea la caída del enlace de fibra óptica de datos como el de internet, debido a la configuración en los equipos core Fortigate 100F el tráfico es asumido por el enlace satelital.

Figura 20

Caída de los enlaces de datos e internet.



Fuente: Elaboración propia.

Observaciones:

- Ante la caída de los canales de internet y datos de fibra óptica, se pierde la conectividad total hacia los recursos internos y hacia internet.
- La configuración SD-WAN realiza el monitoreo de salud de los enlaces (health check) haciendo uso del performance SLA y reglas configuradas. Tras la caída de la interfaz INET1-GFIBER, el tráfico hacia internet es enrutado hacia la interfaz de internet satelital INET2-STARLINK. El tráfico a los recursos internos de la entidad es enrutado hacia la VPN sobre en el enlace de internet satelital CNX-TDP-LIMA.

Figura 21

Interfaces de internet satelital activas por orden de prioridad.

SD-WAN Zones				
SD-WAN Rules				
Performance SLAs				
+ Create New Edit Clone Delete Search				
ID	Name	Source	Destination	Members
IPv4 2/5				
4	TO_OFFICE365_TRENDMICRO_TEAMS	all	Microsoft-Skype_Teams Microsoft_Teams.Published.Worldwide.Allow Microsoft_Teams.Published.Worldwide.Optimize Microsoft-DNS	INET1-GFIBER (INET1-GFIBER) VPN-LIMA-TDP INET2-STARLINK (INET2-STARLINK)
2	TO_VPN_LIMA	all	all	VPN-LIMA-TDP VPN-GFIBER-LIMA CNX-TDP-LIMA

Fuente: Informe interno de instalación de servicio.

- SD-WAN determina que el tráfico de internet y datos debe ir sobre los canales de internet satelital INET2-STARLINK y CNX-TDP-LIMA para alcanzar los recursos internos y destinos de internet definidos en las reglas demostrando la alta disponibilidad.
- Una vez superado el incidente del canal de datos e internet, la configuración de performance SLA determina que el enlace se encuentra activo y realiza la actualización en la regla SD-WAN retornando al funcionamiento inicial.

CAPITULO IV: DISCUSION DE RESULTADOS

4.1 Descripción de la implementación

En esta etapa se ha procedido a la evaluación de los tiempos de implementación y puesta en marcha haciendo uso de herramientas de gestión de proyectos, identificar los recursos necesarios para la implementación y ejecutar las configuraciones en la red de transporte para el curso del tráfico SD-WAN entre otros.

4.1.1 Formulación inicial del proyecto

El diseño e implementación de la nueva infraestructura de red en la sucursal se enmarca en un proyecto corporativo de mayor envergadura el cuál es la apertura de una nueva agencia bancaria. Este proceso involucra la colaboración y coordinación de las diversas gerencias dentro de la entidad. En este contexto, el presente trabajo se centra específicamente en las acciones lideradas por la Gerencia de Tecnología, orientadas a la planificación, diseño e implementación de la red que dará soporte a la operatividad tecnológica de la nueva agencia.

Como entregables iniciales del proyecto se elaboró un diagrama GANTT en el cual se detallan las actividades necesarias, responsabilidades y fechas de compromiso para la implementación de la nueva agencia. El diagrama se encuentra detallado en el Anexo D.

4.1.2 Implementación de los enlaces y equipos de fibra óptica – outdoor/indoor

En la implementación de fibra externa es necesario remarcar que pertenece al contrato con los proveedores de los enlaces de datos e internet respectivamente.

Los permisos y licencias para el uso de postes, cableado aéreo y uso de infraestructura del centro comercial es parte de la gestión del proveedor.

Las actividades ejecutadas por los proveedores son:

- Estudio y diseño de la red externa
- Despliegue de cable de fibra óptica
- Visita técnica de reconocimiento del lugar para el acceso de cable de fibra óptica
- Acceso de cable de fibra óptica
- Pruebas y validación del enlace de fibra óptica
- Pruebas y validación del servicio

Enlace de internet

Para el enlace de internet fue adjudicado a la empresa propietaria de la administración del centro comercial Mall Aventura Plaza Iquitos, Global Fiber, la cual ejecutó el tendido de fibra óptica externa desde su nodo más cercano al centro comercial hasta el gabinete ubicado en la sala datacenter de la nueva agencia. Se realizó la instalación del siguiente equipo como parte de la implementación del servicio de internet del proveedor:

- Cisco ISR4331 que cumple la función de router CPE.

Figura 22

Instalación de equipo Cisco ISR4221 en gabinete de sala DataCenter de la nueva sucursal.



Fuente: Informe de instalación Global Fiber.

- ZTE F601 que cumple la función de demarcador.

Figura 23

Instalación de equipo ZTE F601 en gabinete de sala DataCenter de la nueva sucursal.



Fuente: Informe de instalación Global Fiber.

Enlace de datos

Para el enlace de internet fue adjudicado a la empresa telefónica del Perú, la cual como se hace mención en puntos anteriores tiene una red MPLS desplegada para las agencias ya existentes de la entidad. De la

misma forma que para el enlace de internet, se hizo un tendido de fibra desde el nodo más cercano hasta la sala data center de la agencia.

Figura 24

Recorrido de la ruta fibra óptica de planta externa para el ingreso desde el nodo del proveedor hasta la sala de sistemas de la nueva agencia bancaria.



Fuente: Informe TSS de proveedor del servicio de datos.

Se realizó la instalación del siguiente equipo router como parte de la implementación del servicio de datos del proveedor:

- Cisco ISR4331 que cumple la función de router CPE

Figura 25

Instalación de equipo Cisco modelo ISR4331 en gabinete de sala Data Center de la nueva sucursal en la ciudad de Iquitos.



Fuente: Informe de instalación ISP datos.

4.1.3 Implementación de enlace satelital

La implementación del enlace satelital fue responsabilidad del proveedor de telecomunicaciones tercero el cuál procedió con el anclaje de la antena Starlink en la azotea del Mall Aventura Plaza Iquitos y el tendido de cable hasta la sala data center de la entidad.

Figura 26

Instalación y anclaje de la antena Starlink en la azotea del CC Mall Aventura Iquitos.



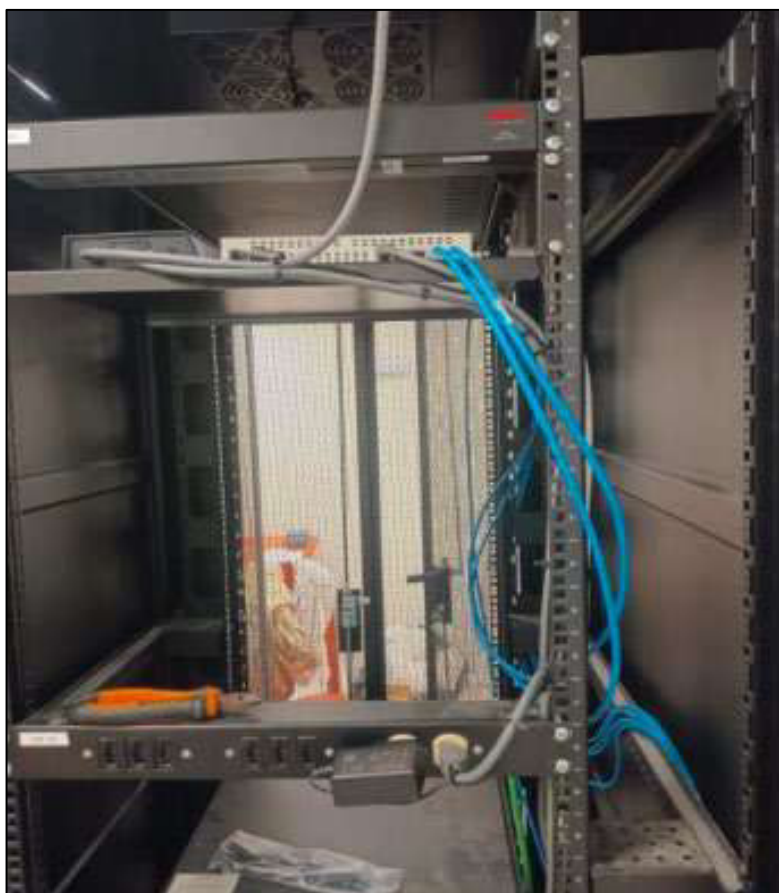
Fuente: Informe de instalación WIN Empresas.

Los equipos instalados por el proveedor son:

- Fortigate 40F como equipo router del servicio satelital y se usa para la asignación de una IP pública fija.

Figura 27

Instalación de equipo Fortigate 40F y power supply en sala Datacenter para enlace satelital Starlink.



Fuente: Informe de instalación proveedor satelital.

4.1.4 Implementación de cableado de red y equipos LAN

La implementación del cableado LAN e instalación del equipamiento estuvo a cargo de la contrata interna de la entidad, la cual tenía el siguiente listado de actividades requeridas para la puesta en marcha del servicio:

Figura 29

Instalación de equipos Fortigate y Cisco en gabinete de sala Datacenter.



Fuente: Informe interno de instalación de red.

4.1.5 Configuración de equipos networking

En esta etapa se establece la configuración de los equipos de networking pertenecientes a la red LAN y la configuración SD-WAN mediante los Fortinet 100F instalados en la sala data center de la agencia.

En primer lugar, se establece los equipos Fortigate 100F como equipos Core de la agencia que entre sus funciones deberá realizar:

- Enrutamiento hacia los segmentos de la red interna de la entidad.
- Puerta de enlace para los segmentos VLAN previamente definidos.
- Establecimiento del túnel SD-WAN hacia la cabecera ubicada en el data center principal en Lima.

- Balanceo de carga entre los enlaces de internet y datos haciendo uso de los performances SLA y reglas SD-WAN configuradas.
- Direcccionamiento del tráfico a la ruta activa (sea el caso de internet, datos o satelital) ante una caída de uno de los enlaces.

Por temas relacionados a confidencialidad se mostrará la configuración con segmentos IP referenciales y el túnel establecido en el enlace de datos. El resto de los túneles tienen la misma lógica de funcionamiento y procedimiento de configuración.

La configuración del túnel se detalla en el Anexo E.

En segundo lugar, se establece la configuración de los switches Cisco C9200 como accesos para la conectividad de los usuarios finales. Sus funciones son:

- Proporcionar conectividad a los usuarios finales en los puntos de red implementados.
- Segmentar la red mediante la propagación de las VLANs previamente definidas.

La configuración de los switches de acceso se detalla en el Anexo F.

4.2 Disponibilidad de la red

La disponibilidad de la red en la nueva agencia en la ciudad de Iquitos se definió en base a la solicitud de la gerencia de tecnología regional de la entidad, la cual establece un SLA de 99.98% mensual de disponibilidad para la infraestructura de red.

La red implementada alcanzó la disponibilidad mensual promedio esperada que equivale a un tiempo máximo de inactividad de aproximadamente 8.64 minutos por mes lo que evidencia una arquitectura de red sólida, con mecanismos de respaldo y recuperación ante fallos.

Adicionalmente, los registros del año siguiente a la implementación (2024) muestran que la red mantiene un comportamiento estable, sin incidencias mayores que impliquen pérdida de servicio total y cumpliendo los SLAs acordados.

Tabla 10

Resumen de incidentes en el periodo 2024 de la sucursal implementada.

TICKET	SUCURSAL	SERVICIO	FECHA	MOTIVO
TBR-234	Iquitos	MPLS	07/12/2023	Corte de fibra en red de proveedor
TBR-281	Iquitos	MPLS	06/01/2024	Masiva en Estación base (EBC) de proveedor
TBR-401	Iquitos	MPLS	13/01/2024	Intermitencia en la red del proveedor
TBR-460	Iquitos	Internet	21/03/2024	Caída de nodo del proveedor por evento de energía.
TBR-603	Iquitos	MPLS	05/05/2024	Masiva por corte de FO en San Juan y Punchana
TBR-662	Iquitos	Internet	19/06/2024	Inhibición de equipo de transmisión en nodo de proveedor
TBR-754	Iquitos	MPLS	02/08/2024	Perdida de comunicación por eventos climatológico.
TBR-897	Iquitos	MPLS	12/10/2024	Corte de energía en nodo Iquitos.
TBR-923	Iquitos	MPLS/Internet	23/11/2024	Corte de fibra en tramo Yurimaguas.
TBR-979	Iquitos	Internet	03/12/2024	Perdida de comunicación por eventos climatológico.

Fuente: Informe interno de indicadores de incidencias.

En la Tabla 10 se presentan los registros de incidentes asociados a los servicios de conectividad (Internet y MPLS) de la entidad. A pesar de los eventos de indisponibilidad en los enlaces principales, el nivel de servicio mensual de la sucursal no se vio afectado, manteniéndose en línea con el objetivo establecido de un 99.98 % de disponibilidad. El resultado obtenido es atribuido a la correcta implementación de la solución SD-WAN en la nueva agencia, la cual proporciona una red resiliente, con mecanismos de redundancia activa permitiendo la continuidad operativa aún durante fallas parciales.

La red implementada alcanzó la disponibilidad mensual promedio esperada que equivale a un tiempo máximo de inactividad de aproximadamente 8.64 minutos por mes lo que evidencia una arquitectura de red sólida, con mecanismos de respaldo y recuperación ante fallos.

4.3 Evaluación Económica

La importancia del desarrollo y la justificación de este proyecto tiene como origen la necesidad de implementar una red de alta disponibilidad para la nueva sucursal bancaria en la ciudad de Iquitos. Ante los desafíos presentes en la infraestructura de la ciudad, la entidad requiere que la red sea confiable y resiliente haciendo uso eficiente de los recursos. Es debido a esto que se diseñó un modelo con un 99.98% de disponibilidad mensual que emplee tecnologías de última generación en el mercado para hacer rentable la inversión realizada por la entidad. La implementación de este proyecto ha sido una solución estratégica para el crecimiento de la empresa en productividad con la captación de nuevos clientes que hacen uso de los diversos servicios bancarios como créditos, financiamientos, etc. y en lo económico debido al aseguramiento de la continuidad del servicio por la alta redundancia de la red.

En la siguiente tabla se hace el desglose de costos considerados como gastos CAPEX y OPEX en la implementación de la nueva sucursal.

Tabla 11

Resumen de gastos CAPEX del área de tecnología para la implementación de la nueva sucursal.

Nº	DESCRIPCION	QTY	COSTO UNIT	TOTAL (SIN IGV)	MONEDA	TIPO
1	Traslado y entrega en Iquitos	1	502.87	502.87	USD	CAPEX
2	Equipos Fortigate 100F	2	2981.16	5962.32	USD	CAPEX
3	Equipos Cisco C9200-24P	4	2981.16	11924.64	USD	CAPEX
4	Transceiver SFP-10G-SR-S	8	218.93	1751.44	USD	CAPEX

5	Transceiver FN-TRAN-SFP+SR	6	139.89	839.34	USD	CAPEX
6	Implementación de enlace de internet Iquitos 10MB	1	1190.20	1190.20	USD	CAPEX
7	Implementación de enlace satelital Starlink	1	3500.00	3500.00	USD	CAPEX
8	Implementación de enlace MPLS 10MB	1	3243.24	3243.24	USD	CAPEX
9	Personal técnico de campo (Cableado, instalación de equipos, etc...)	1	6312.43	6312.43	USD	CAPEX
				35226.48	USD	

Fuente: Elaboración propia de resumen de gastos internos

Tabla 12

Resumen de gastos OPEX del área de tecnología para la implementación de la nueva sucursal.

Nº	DESCRIPCION	QTY	COSTO UNIT	TOTAL (SIN IGV)	MONEDA	TIPO
1	Licencia Forticare Premium 1 año	2	663.22	1326.44	USD	OPEX
2	Cisco smartnet 1 año	4	230.47	921.88	USD	OPEX
3	Recurrente mensual servicio de Internet (1 año)	12	175.68	2108.16	USD	OPEX
4	Recurrente mensual servicio de Starlink (1 año)	12	750.00	9000.00	USD	OPEX
5	Recurrente mensual servicio de MPLS (1 año)	12	2702.70	32432.40	USD	OPEX
				45788.88	USD	

Fuente: Elaboración propia de resumen de gastos internos

CAPITULO V: CONCLUSIONES

- La identificación de los desafíos técnicos durante la fase de diseño es de suma importancia para la implementación de una arquitectura de red que garantice rendimiento, estabilidad y adaptabilidad frente a las limitaciones del entorno.
- Se logró diseñar e implementar una red de alta disponibilidad, que cumple con los requerimientos técnicos establecidos por la entidad. La solución desplegada garantiza un SLA mensual del 99.98% acorde a los niveles exigidos para una agencia remota del sector financiero.
- Se logró diseñar una topología de red resiliente y que hace uso eficiente de los recursos de red, teniendo en cuenta las limitaciones geográficas y técnicas propias de la ciudad de Iquitos. El diseño propuesto considera la limitada conectividad en la región, priorizando SD-WAN y Starlink como soluciones con alta disponibilidad y eficiencia. Esto permitió hacer más eficiente el rendimiento sin comprometer la viabilidad económica ni operativa del proyecto.
- Se identificaron y dimensionaron correctamente las tecnologías y equipos requeridos para la implementación del diseño de red planteado. La elección de marcas y modelos se fundamentó en criterios técnicos, escalabilidad y compatibilidad con la solución SD-WAN.
- La implementación de la infraestructura de red diseñada se realizó con éxito, incluyendo la configuración de la solución SD-WAN. Las pruebas de conectividad y rendimiento ejecutadas demostraron que la topología de red cumple con los parámetros de calidad, redundancia y disponibilidad esperados, validando la eficiencia del diseño y su correcta implementación.

- La nueva red proporciona una mejora significativa en comparación con la topología de red estándar de las agencias existentes. El balanceo de carga y la configuración activo-activo evita la saturación de servicios y hace eficiente el uso de los recursos de red.

CAPITULO VI: RECOMENDACIONES

De acuerdo con lo desarrollado en el diseño e implementación de la red en la nueva sucursal, se sugiere lo siguiente:

- Programar mantenimientos preventivos de red de manera anual del equipamiento instalado en la sede con la finalidad de asegurar el correcto funcionamiento del servicio.
- Programar con el proveedor del servicio Starlink el mantenimiento de la antena instalada en la azotea del centro comercial debido a las condiciones climáticas de la ciudad.
- Realizar pruebas de contingencia trimestralmente con la finalidad de asegurar el correcto funcionamiento de la configuración redundante.
- Añadir los equipos al sistema de monitoreo interno de la entidad a fin de asegurar la gestión de eventos/incidentes.
- Asegurar la actualización de los equipos de red a las versiones más actuales con la finalidad de fortalecer la seguridad ante alguna brecha de seguridad.

CAPITULO VII: BIBLIOGRAFÍA

Ahmed, M., & Basit, A. (2014, junio). *Implementation of Traffic Engineering and Addressing QoS in MPLS VPN based IP Backbone*. International Journal of Computer Science and Telecommunications, 5(6), 9-14.
https://www.ijcst.org/Volume5/Issue6/p2_5_6.pdf

Alvariño Herrera, N. (2024, mayo 29). Infraestructura de conexión en Iquitos Parte III: Internet. [Publicación en LinkedIn] <https://www.linkedin.com/pulse/infraestructura-de-conexi%C3%B3n-en-iquitos-parte-iii-internet-fri-esan-oxpnc/>

Campana Silverio, R. A. (2023). Implementación del servicio de internet satelital mediante la plataforma Starlink para la empresa Pluspetrol, 2023. <https://hdl.handle.net/20.500.14717/1353>

Cato Networks. (s. f.). What Is SD-WAN? <https://www.catonetworks.com/sd-wan/>

Cisco. (s.f.-a). What is MPLS – Multiprotocol Label Switching. <http://www.cisco.com/c/en/us/products/ios-nx-os-software/multiprotocol-label-switching-mpls/index.html>

Cisco. (s.f.-b). ¿Qué es un router?. https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/what-is-a-router.html

Cisco. (s.f.-c). Distintos tipos de switches Ethernet y de red. https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/what-is-a-router.html

center/networking/understanding-the-different-types-of-network-switches.html

Cisco. (s.f.-d). Cisco Catalyst 9200 series switches data sheet. <https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9200-series-switches/nb-06-cat9200-ser-data-sheet-cte-en.html>

Cisco Systems, Inc. (2024, julio 31). Cisco Catalyst 9200 Series Data Sheet. <https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9200-series-switches/nb-06-cat9200-ser-data-sheet-cte-en.html>

Cisneros Paladines, E. (2020). Diseño de una SD-WAN para las sucursales de una empresa de cadena de tiendas en Ecuador. <http://www.dspace.espol.edu.ec/handle/123456789/56385>

Cloudflare. (s.f.). ¿Qué es IPsec?. <https://www.cloudflare.com/es-es/learning/network-layer/what-is-ipsec/>

Condon, S. (2022, septiembre 25). What is Starlink? Everything you need to know about Elon Musk's satellite internet service. <https://www.zdnet.com/home-and-office/networking/starlink-satellite-internet-how-does-it-work-cost-features-speed/>

Fortinet. (s.f.-a). SD-WAN Defined and Explained. <https://www.fortinet.com/resources/cyberglossary/sd-wan-explained>

Fortinet. (s.f.-b) ¿Qué es un firewall? Definición y tipos de firewall. <https://www.fortinet.com/lat/resources/cyberglossary/firewall>

Fortinet. (s.f.-c). FortiGate 100F series. <https://www.fortinet.com/lat/resources/data-sheets/fortigate-100f-series>

Fortinet. (2025, abril 7). FortiGate 100F Series Data Sheet. <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-100f-series.pdf>

Gooley, J., Yanch, D., Schuemann, D., & Curran, J. (2021). Cisco Software-Defined Wide Area Networks: Designing, Deploying and Securing Your Next Generation WAN with Cisco SD-WAN.

Info@Citel (2010). Fibra Óptica. Obtenida desde: https://www.oas.org/es/citel/infocitel/2010/abril/ftth_e.asp

OSTEC. (2023). SD-WAN: Conceptos y funcionamiento. OSTEC Blog. <https://ostec.blog/es/seguridad-perimetral/sd-wan-conceptos-funcionamiento/>

Rak, J., Girão-Silva, R., Gomes, T., Ellinas, G., Kantarci, B., & Tornatore, M. (2021). Disaster resilience of optical networks: State of the art, challenges, and opportunities. *Optical Switching And Networking*, 42, 100619. <https://doi.org/10.1016/j.osn.2021.100619>

Ramirez, W., Masip-Bruin, X., Marin-Tordera, E., & Sánchez-López, S. (2015). Managing resilience in carrier grade networks: Survey, open issues and trends. *Computer Communications*, 61, 1-16. <https://doi.org/10.1016/j.comcom.2015.02.015>

Sergieieva, K. (2025). Tipos de satélites: sus órbitas y funciones. EOS Data Analytics. <https://eos.com/es/blog/tipos-de-satelites/>

SpaceX. (2024). Planes de servicio: Starlink para empresas. <https://www.starlink.com/pe/service-plans/business>

Starlink. (2024). Progress report 2024. <https://stories.starlink.com/>

Starlink. (s.f.). Technology. <https://www.starlink.com/technology>

Starlink. (s.f.). Especificaciones. <https://www.starlink.com/pe/specifications>

Telecomunicaciones Perú. (2020). Fibra óptica subfluvial Yurimaguas – Iquitos [Infografía]. <https://telecomunicaciones-peru.blogspot.com/2020/06/fibra-optica-subfluvial-yurimaguas.html>

Yang, Z., Cui, Y., Li, B., Liu, Y., & Xu, Y. (2019). Software-Defined Wide Area Network (SD-WAN): Architecture, advances and opportunities. En 2019 28th International Conference on Computer Communication and Networks (ICCCN) (pp. 1–9). IEEE. <https://doi.org/10.1109/ICCCN.2019.8847124>

CAPITULO IX: ANEXOS

Anexo A

Figura A1

Ficha técnica de Starlink

Antena	Matriz electrónica en fase	
Campo de visión	110°	
Orientación	Orientación manual asistida por software	
Peso	2.9 kg (6.4 lb) 3.2 kg (7 lb) con pie 3.8 kg (8.3 lb) con pie y cable de 15 m	
Clasificación ambiental	IP67 Tipo 4	
Temperatura de funcionamiento	-30 °C a 50 °C (-22 °F a 122 °F)	
Velocidad del viento	Funcionamiento: más de 96 km/h (más de 60 mph)	
Capacidad para derretir la nieve	Hasta 40 mm/hora (1.5 pulg./hora)	
Consumo de energía	Promedio: de 75 a 100 W	
Antena	Matriz electrónica en fase	
Campo de visión	110°	
Orientación	Orientación manual asistida por software	
Peso	2.9 kg (6.4 lb) 3.2 kg (7 lb) con pie 3.8 kg (8.3 lb) con pie y cable de 15 m	
Clasificación ambiental	IP67 Tipo 4	
Temperatura de funcionamiento	-30 °C a 50 °C (-22 °F a 122 °F)	
Velocidad del viento	Funcionamiento: más de 96 km/h (más de 60 mph)	
Capacidad para derretir la nieve	Hasta 40 mm/hora (1.5 pulg./hora)	
Consumo de energía	Promedio: de 75 a 100 W	

Nota. Adaptado de *Starlink Especificaciones* [Infografía], por Starlink, s.f.,
<https://www.starlink.com/pe/specifications>, CC BY 2.0

Anexo B

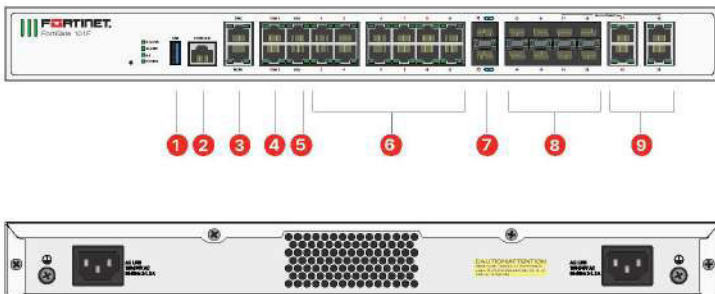
Figura B1

Ficha técnica Fortigate 100F – Página 7.

FortiGate 100F Series
Data Sheet

Hardware

FortiGate 100F Series



The diagram shows the front panel of the FortiGate 100F Series. It features a USB port (1), a console port (2), two GE RJ45 MGMT/DMZ ports (3), two GE RJ45 WAN ports (4), two GE RJ45 HA ports (5), 12 GE RJ45 ports (6), two 10 GE SFP+ FortiLink slots (7), four GE SFP slots (8), and four GE RJ45/SFP Shared Media Pairs (9). Below the main panel, there is a secondary panel with power and status indicators.

Interfaces

1. 1 x USB Port
2. 1 x Console Port
3. 2 x GE RJ45 MGMT/DMZ Ports
4. 2 x GE RJ45 WAN Ports
5. 2 x GE RJ45 HA Ports
6. 12 x GE RJ45 Ports
7. 2 x 10 GE SFP+ FortiLink Slots
8. 4 x GE SFP Slots
9. 4 x GE RJ45/ SFP Shared Media Pairs

Hardware Features

SP4
TRU
DUAL AC
480GB



Dual power supply

Power supply redundancy is essential in the operation of mission-critical networks. The FortiGate 100F series offers dual built-in non-hot swappable power supplies.



Access layer security

FortiLink protocol enables you to converge security and network access by integrating the FortiSwitch into the FortiGate as a logical extension of the firewall. These FortiLink-enabled ports can be reconfigured as regular ports as needed.


7

Nota. Adaptado de *FortiGate 100F series data sheet* [Infrografía], por Fortinet, 2025, <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-100f-series.pdf>, CC BY 2.0

Figura B2

Ficha técnica Fortigate 100F – Página 8.

FortiGate 100F Series		Data Sheet
Specifications		
	FORTIGATE 100F	FORTIGATE 101F
Interfaces and Modules		
Hardware Accelerated GE RJ45 Ports	12	
Hardware Accelerated GE RJ45 Management/ HA/ DMZ Ports	1 / 2 / 1	
Hardware Accelerated GE SFP Slots	4	
Hardware Accelerated 10 GE SFP+ FortiLink Slots (default)	2	
GE RJ45 WAN Ports	2	
GE RJ45 or SFP Shared Ports *	4	
USB Port	1	
Console Port	1	
Onboard Storage	0	1x 480 GB SSD
Trusted Platform Module (TPM)	—	—
Bluetooth Low Energy (BLE)	—	—
Signed Firmware Hardware Switch	—	—
Included Transceivers	0	
System Performance — Enterprise Traffic Mix		
IPS Throughput ²	2.6 Gbps	
NGFW Throughput ^{2,4}	1.6 Gbps	
Threat Protection Throughput ^{2,5}	1 Gbps	
System Performance and Capacity		
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	20 / 18 / 10 Gbps	
Firewall Latency (64 byte, UDP)	4.97 µs	
Firewall Throughput (Packet per Second)	15 Mpps	
Concurrent Sessions (TCP)	1.5 Million	
New Sessions/Second (TCP)	55 000	
Firewall Policies	10 000	
IPsec VPN Throughput (512 byte) ¹	11.5 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	2000	
Client-to-Gateway IPsec VPN Tunnels	16 000	
SSL-VPN Throughput	1 Gbps	
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	500	
SSL Inspection Throughput (IPS, avg. HTTPS) ¹	1 Gbps	
SSL Inspection CPS (IPS, avg. HTTPS) ¹	1800	
SSL Inspection Concurrent Session (IPS, avg. HTTPS) ¹	135 000	
Application Control Throughput (HTTP 64K) ²	2.2 Gbps	
CAPWAP Throughput (HTTP 64K)	15 Gbps	
Virtual Domains (Default / Maximum)	10 / 10	
Maximum Number of FortiSwitches Supported	32	
Maximum Number of FortiAPs (Total / Tunnel)	128 / 64	
Maximum Number of FortiTokens	5000	
High Availability Configurations	Active-Active, Active-Passive, Clustering	
Dimensions and Power		
Height x Width x Length (inches)	1.73 x 17 x 10	
Height x Width x Length (mm)	44 x 432 x 254	
Weight	7.25 lbs (3.29 kg)	7.56 lbs (3.43 kg)
Form Factor (supports EIA/non-EIA standards)	Rack Mount, 1 RU	
AC Power Supply	100-240V AC, 50/60 Hz	
Power Consumption (Average / Maximum)	26.5 W / 29.5 W	35.3 W / 39.1 W
Current (Maximum)	100V / 1A, 240V / 0.5A	
Heat Dissipation	100.6 BTU/h	121.3 BTU/h
Redundant Power Supplies	Yes (Default dual non-swappable AC PSU for 1+1 Redundancy)	
Power Supply Efficiency Rating	80 Plus Compliant	
Operating Environment and Certifications		
Operating Temperature	32°F to 104°F (0°C to 40°C)	
Storage Temperature	-31°F to 158°F (-35°C to 70°C)	
Humidity	10% to 90% non-condensing	
Noise Level	40.4 dBA	
Forced Airflow	Side to Back	
Operating Altitude	Up to 10 000 ft (3048 m)	
Compliance	FCC Part 15B, Class A, CE, RoHS, VCCI, UL/cUL, CB, BSMI	
Certifications	USGv6/IPv6	

¹ Latency based on Ultra Low Latency (ULL) ports

Note: All performance values are "up to" and vary depending on system configuration.

¹ IPsec VPN performance test uses AES256-SHA256.

² IPS (Enterprise Mix), Application Control, NGFW and Threat Protection are measured with Logging enabled.

³ SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.

⁴ NGFW performance is measured with Firewall, IPS and Application Control enabled.

⁵ Threat Protection performance is measured with Firewall, IPS, Application Control and Malware Protection enabled.

⁶ Uses RSA-2048 certificate.

Nota. Adaptado de FortiGate 100F series data sheet [Infrografía], por Fortinet, 2025, <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-100f-series.pdf>, CC BY 2.0

Figura B3

Ficha técnica Fortigate 100F – Página 9.

FortiGate 100F Series

Data Sheet

Subscriptions

Service Category	Service Offering	A-la-carte	Bundles		
			Enterprise Protection	Unified Threat Protection	Advanced Threat Protection
FortiGuard Security Services	IPS — IPS, Malicious/Botnet URLs	*	*	*	*
	Anti-Malware Protection (AMP)—AV, Botnet Domains, Mobile Malware, Virus Outbreak Protection, Content Disarm and Reconstruct ¹ , AI-based Heuristic AV, FortiGate Cloud Sandbox	*	*	*	*
	URL, DNS and Video Filtering — URL, DNS and Video ¹ Filtering, Malicious Certificate	*	*	*	
	Anti-Spam		*	*	
	AI-based Inline Malware Prevention ²	*	*		
	Data Loss Prevention (DLP) ¹	*	*		
	Attack Surface Security — IoT Device Detection, IoT Vulnerability Correlation and Virtual Patching, Security Rating, Outbreak Check	*	*		
	OT Security—OT Device Detection, OT vulnerability correlation and Virtual Patching, OT Application Control and IPS ¹	*			
	Application Control		-----Included with FortiCare Subscription-----		
	Inline CASB ²		-----Included with FortiCare Subscription-----		
SD-WAN and SASE Services	SD-WAN Underlay Bandwidth and Quality Monitoring	Models up to FG/FWF-60F series			
	SD-WAN Underlay and Application Monitoring Service	FG-70F series and above			
	SD-WAN Overlay-as-a-Service	*			
	SD-WAN Connector for FortiSASE Secure Private Access	*			
	SASE expansion for SD-WAN (SD-WAN SPA Connector license plus FortiSASE starter kit for n* users) ²	Selected models only ²			
	SASE connector for FortiSASE Secure Edge Management (with 10Mbps Bandwidth)	Desktop models only			
NOC and SOC Services	FortiConverter Service for one time configuration conversion	*	*		
	Managed FortiGate Service—available 24x7, with Fortinet NOC experts performing device setup, network, and policy change management	*			
	FortiGate Cloud—Management, Analysis, and One Year Log Retention	*			
	FortiManager Cloud	*			
	FortiAnalyzer Cloud	*			
	FortiGuard SOCaaS—24x7 cloud-based managed log monitoring, incident triage, and SOC escalation service	*			
Hardware and Software Support	FortiCare Essentials	Desktop models only			
	FortiCare Premium	*	*	*	*
	FortiCare Elite	*			
Base Services	Device/OS Detection, GeoIPs, Trusted CA Certificates, Internet Services and Botnet IPs, DDNS (v4/v6), Local Protection, PSIRT Check, Anti-Phishing		-----Included with FortiCare Subscription-----		

1. Full features available when running FortiOS 7.4.1.

2. See the FortiSASE Ordering Guide for supported models and their associated number of user licenses.

3. Not available for FortiGate/FortiWiFi 40F, 60E, 60F, 80E, and 90E series from 7.4.4 onwards. Not available for FortiGate/FortiWiFi 30G and 50G series in any OS build.

FortiGuard Bundles

FortiGuard AI-Powered Security Bundles provide a comprehensive and meticulously curated selection of security services to combat known, unknown, zero-day, and emerging AI-based threats. These services are designed to prevent malicious content from breaching your defenses, protect against web-based threats, secure devices throughout IT/OT/IoT environments, and ensure the safety of applications, users, and data. All bundles include FortiCare Premium Services featuring 24x7x365 availability, one-hour response for critical issues, and next-business-day response for noncritical matters.

9

Nota. Adaptado de *FortiGate 100F series data sheet* [Infrografía], por Fortinet, 2025, <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-100f-series.pdf>, CC BY 2.0

Figura B4*Ficha técnica Fortigate 100F – Página 10.*

FortiGate 100F Series		Data Sheet
Ordering Information		
Product	SKU	Description
FortiGate 100F	FG-100F	22x GE RJ45 ports (including 2x WAN ports, 1x DMZ port, 1x Mgmt port, 2x HA ports, 16x switch ports with 4 SFP port shared media), 4 SFP ports, 2x 10 GE SFP+ FortiLinks, dual power supplies redundancy.
FortiGate 100F	FG-100F-HA	22 x GE RJ45 ports (including 2 x WAN ports, 1 x DMZ port, 1 x Mgmt port, 2 x HA ports, 16 x switch ports with 4 SFP port shared media), 4 SFP ports, 2x 10G SFP+ FortiLinks, dual power supplies redundancy. FG-XX-HA SKUs must be bought in pairs and entitle HA pair to leverage single service contracts.
FortiGate 101F	FG-101F	22x GE RJ45 ports (including 2x WAN ports, 1x DMZ port, 1x Mgmt port, 2x HA ports, 16x switch ports with 4 SFP port shared media), 4 SFP ports, 2x 10 GE SFP+ FortiLinks, 480 GB onboard storage, dual power supplies redundancy.
FortiGate 101F	FG-101F-HA	22 x GE RJ45 ports (including 2 x WAN ports, 1 x DMZ port, 1 x Mgmt port, 2 x HA ports, 16 x switch ports with 4 SFP port shared media), 4 SFP ports, 2x 10G SFP+ FortiLinks, 480GB onboard storage, dual power supplies redundancy. FG-XX-HA SKUs must be bought in pairs and entitle HA pair to leverage single service contracts.
Transceivers		
1 GE SFP RJ45 Transceiver Module	FN-TRAN-GC	1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP SX Transceiver Module	FN-TRAN-SX	1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP LX Transceiver Module	FN-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.
10 GE SFP+ RJ45 Transceiver Module	FN-TRAN-SFP+GC	10 GE SFP+ RJ45 transceiver module for systems with SFP+ slots.
10 GE SFP+ Transceiver Module, Short Range	FN-TRAN-SFP+SR	10 GE SFP+ transceiver module, short range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Long Range	FN-TRAN-SFP+LR	10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Extended Range	FN-TRAN-SFP+ER	10 GE SFP+ transceiver module, extended range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, 80km Extreme Long Range	FN-TRAN-SFP+ZR	10 GE SFP+ transceiver module, 80km extreme long range, for systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, 30 km Long Range	FN-TRAN-SFP+BD27	10 GE SFP+ transceiver module, 30KM long range single BiDi for systems with SFP+ and SFP/SFP+ slots (connects to FN-TRAN-SFP+BD33, ordered separately).
10 GE SFP+ Transceiver Module, 30 km Long Range	FN-TRAN-SFP+BD33	10 GE SFP+ transceiver module, 30KM long range single BiDi for systems with SFP+ and SFP/SFP+ slots (connects to FN-TRAN-SFP+BD27, ordered separately).
Cables		
10 GE SFP+ Passive Direct Attach Cable 1m	FN-CABLE-SFP+1	10 GE SFP+ passive direct attach cable, 1m for systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Passive Direct Attach Cable 3m	FN-CABLE-SFP+3	10 GE SFP+ passive direct attach cable, 3m for systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Passive Direct Attach Cable 5m	FN-CABLE-SFP+5	10 GE SFP+ passive direct attach cable, 5m for systems with SFP+ and SFP/SFP+ slots.

Visit <https://www.fortinet.com/resources/ordering-guides> for related ordering guides.

Nota. Adaptado de *FortiGate 100F series data sheet* [Infrografía], por Fortinet, 2025, <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-100f-series.pdf>, CC BY 2.0

Anexo C

Figura C1

Ficha técnica Cisco C9200

C9200-24P-E Datasheet



Overview

C9200-24P-E is the Catalyst 9200 24-port PoE+ Switch, with Network Essentials software. Cisco® Catalyst® 9200 Series switches extend the power of intent-based networking and Catalyst 9000 hardware and software innovation to a broader set of deployments. With its family pedigree, Catalyst 9200 Series switches offer simplicity without compromise – it is secure, always on, and IT simplified.

Quick Spec

Table 1 shows the quick spec.

Model	C9200-24T-P
Downlinks total 10/100/1000 or PoE+ copper ports	24-port PoE+
Uplink configuration	Modular uplink options
Default primary AC power supply	PWR-C6 600WAC
Fans	FRU redundant
Software	Network Essentials
Stacking bandwidth	160 Gbps
DRAM	4 GB
Flash	4 GB
Switching capacity	128 Gbps
Forwarding rate	190.4 Mpps
Chassis Dimensions	1.73 x 17.5 x 13.8in 4.4 x 44.5 x 35.0 cm

Product Details

Catalyst 9200 series provides these highlights:

- Up to 48 ports of full Power over Ethernet Plus (PoE+) capability
- Resiliency with Field-Replaceable Units (FRU) and redundant power supply, fans, and modular uplinks
- Flexible downlink options with data or PoE+
- Operational efficiency with optional backplane stacking, supporting stacking bandwidth up to 160 Gbps
- UADP 2.0 Mini with integrated CPU offers customers optimized scale with better cost structure
- Enhanced security with AES-128 MACsec encryption, policy-based segmentation, and trustworthy systems
- Layer 3 capabilities, including OSPF, EIGRP, ISIS, RIP, and routed access
- Advanced network monitoring using Full Flexible NetFlow
- Cisco Software-Defined Access (SD-Access):
 - Simplified operations and deployment with policy-based automation from edge to cloud managed with Cisco Identity Services Engine (ISE)
 - Network assurance and improved resolution time through Cisco DNA Center™
- Plug and Play (PnP) enabled: A simple, secure, unified, and integrated offering to ease new branch or campus device rollouts or updates to an existing network
- Cisco IOS XE: A Common Licensing based operating system for the enterprise Cisco Catalyst 9000 product family with support for model-driven programmability and streaming telemetry
- ASIC with programmable pipeline and micro-engine capabilities, along with template-based, configurable allocation of Layer 2 and Layer 3 forwarding, Access Control Lists (ACLs), and Quality of Service (QoS) entries

Nota. Adaptado de *Cisco Catalyst 9200 series data sheet* [Infografía], por Cisco Systems, 2024,
<https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9200-series-switches/nb-06-cat9200-ser-data-sheet-cte-en.html>, CC BY 2.0

Figura C2

Ficha técnica Cisco C9200

Supported Products	
Table 2 shows the recommended supported products.	
Network modules	
Product number	Product description
C9200-NM-4G	Catalyst 9200 4 x 1GE Network Module
C9200-NM-4X	Catalyst 9200 4 x 10GE Network Module, spare
C9200-NM-BLANK	Catalyst 9200 BLANK Network Module
StackWise-80 and StackWise-160 Kit and cables	
Product number	Product description
C9200-STACK-KIT-	C9200 Stack Kit Spare
C9200L-STACK-KIT-	C9200L Stack Kit Spare
STACK-T4-50CM	50CM Type 3 Stacking Cable
STACK-T4-1M	1M Type 3 Stacking Cable
STACK-T4-3M	3M Type 3 Stacking Cable
Soft Licenses	
Product number	Product description
C9200-DNA-P-24	C9200 DNA Premier Term, 24-Port. Includes Term Licenses for DNA Advantage, 25 ISE Base & 25 ISE Plus Endpoints, 25 Stealthwatch Flows (including Virtual Flow Collector & Management Console). Requires separate purchase of ISE appliance/ISE VM and DNA Center appliance.
C9200-DNA-P-24-3Y	C9200 DNA Premier, 24-port, 3Y Term – DNA, 25 ISE PLS and ISE BASE, 25 SWITCH
C9200-DNA-P-24-5Y	C9200 DNA Premier, 24-port, 5Y Term – DNA, 25 ISE PLS and ISE BASE, 25 SWITCH
C9200-DNA-P-24-7Y	C9200 DNA Premier, 24-port, 7Y Term – DNA, 25 ISE PLS and ISE BASE, 25 SWITCH
Power supplies	
Product Number	Product Description
PWR-C6-600WAC	600WAC power supply spare
Compare to Similar Items	
Table 3 shows the comparison.	
Product number	Product description
C9200-24T-A	Catalyst 9200 24-port Data Switch, Network Advantage
C9200-24T-E	Catalyst 9200 24-port Data Switch, Network Essentials
C9200-24P-A	Catalyst 9200 24-port PoE+ Switch, Network Advantage
C9200-24P-E	Catalyst 9200 24-port PoE+ Switch, Network Essentials
Get More Information	
Do you have any question about the Cisco C9200-24P-E?	
Contact us now via Live Chat or sales@router-switch.com .	

Nota. Adaptado de *Cisco Catalyst 9200 series data sheet* [Infografía], por Cisco Systems, 2024,
<https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9200-series-switches/nb-06-cat9200-ser-data-sheet-cte-en.html>, CC BY 2.0

Figura C3**Ficha técnica Cisco C9200**

C9200-24P-E Specification	
Downlinks total 10/100/1000 or PoE+ copper ports	24 ports full PoE+
Uplink configuration	Modular uplink options
Default primary AC power supply	PWR-C6-600WAC
Fans	FRU redundant
Software	Network Essentials
Chassis Dimensions	1.73 x 17.5 x 13.8 in 4.4 x 44.5 x 35.0 cm
Virtual Networks	4
Stacking bandwidth	160 Gbps
Total number of MAC addresses	32,000
Total number of IPv4 routes (ARP plus learned routes)	14,000 (10,000 direct routes and 4,000 indirect routes)
IPv4 routing entries	4,000
IPv6 routing entries	2,000
Multicast routing scale	1,000
QoS scale entries	1,000
ACL scale entries	1,600
Packet buffer per SKU	6 MB buffers for 24- or 48-port Gigabit Ethernet models
Flexible NetFlow (FNF) entries	16,000 flows on 24- and 48-port Gigabit Ethernet models
DRAM	4 GB
Flash	4 GB
VLAN IDs	4096
Total Switched Virtual Interfaces (SVIs)	1000
Jumbo frames	9198 bytes
Wireless bandwidth per switch	Up to 48 Gbps on 24-port and 48-port Gigabit Ethernet model
Switching capacity	128 Gbps
Forwarding rate	190.4 Mpps
Mean time between failures (hours)	422,310

Nota. Adaptado de *Cisco Catalyst 9200 series data sheet* [Infografía], por Cisco Systems, 2024,
<https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9200-series-switches/nb-06-cat9200-ser-data-sheet-cte-en.html>, CC BY 2.0

Anexo D

Figura D1

Gantt de actividades de implementación

TÍTULO DEL PROYECTO		IMPLEMENTACIÓN AGENCIA IQUITOS - COMUNICACIONES TI		
STAKEHOLDERS		Comunicaciones, Proveedores terceros, StorePlanning		
FECHA INICIO		19 de Julio 2023		

TAREA ID	TAREA TÍTULO	TAREA RESPONSABLE	INICIO FECHA	VENCIMIENTO FECHA
1	INFRAESTRUCTURA MALL - COMUNICACIONES			
1.1	Implementación de ducterías Mall - Sala de sistema BR	StorePlanning	-	08/16/23
1.2	Implementación de tuberías para enlace satelital StarLink	StorePlanning	-	08/15/23
1.3	Entrega de puntos de red piso 1 BR	StorePlanning / Disec	-	08/21/23
2	SERVICIOS DE TELECOMUNICACIONES WAN			
2.1	Visita de campo proveedor enlace de Internet	Com/Optical Network	-	07/20/23
2.2	Visita de campo proveedor enlace MPLS	Com/TDP	-	07/20/23
2.3	Visita de campo proveedor enlace satelital	Com/Global Fiber	-	08/09/23
2.4	Implementación de enlace de FO internet	Optical Network	-	08/26/23
2.5	Implementación de enlace FO MPLS	TDP	-	08/26/23
2.6	Implementación de enlace satelital Starlink	Global Fiber	-	08/17/23
3	EQUIPAMIENTO DE RED LAN			
3.1	Coordinación de entrega de equipos LAN	Com / ADEXUS	-	08/16/23
3.2	Instalación de equipos LAN	Com / Disec	-	08/17/23
3.3	Configuración de equipos	Com / N2	-	08/21/23
4	SDWAN			
4.1	Instalación de FW en DC Lince	Comunicaciones	-	08/14/23
4.2	Instalación de FW en sala de equipos Iquitos	Disec	-	08/16/23
4.3	Configuración de FW en DC Lince	Com / N2	-	08/21/23
4.3	Configuración de FW en sala de equipos Iquitos	Com / N2	-	08/21/23
4.3	Validación de túnel Lince - Iquitos	Comunicaciones	-	08/21/23
5	PRUEBAS DE SERVICIO			
5.1	Pruebas de conectividad de red (Starlink)	Comunicaciones / Servicios TI	-	08/29/23
5.2	Pruebas de servicio/aplicaciones (Starlink)	Comunicaciones / Servicios TI	-	08/29/23
5.3	Pruebas de conectividad de red (FO + Starlink)	Comunicaciones / Servicios TI	-	08/30/23
5.4	Pruebas de servicios/aplicaciones (FO + Starlink)	Comunicaciones / Servicios TI	-	08/30/23

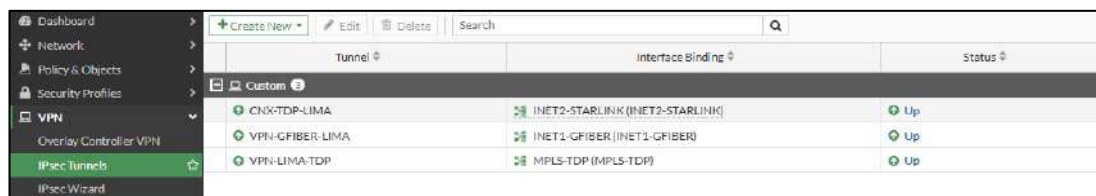
Fuente: Documentación interna del proyecto.

Anexo E

Configuración de equipos Fortigate 100F

Figura E1

Configuración de túneles en equipo core Iquitos.

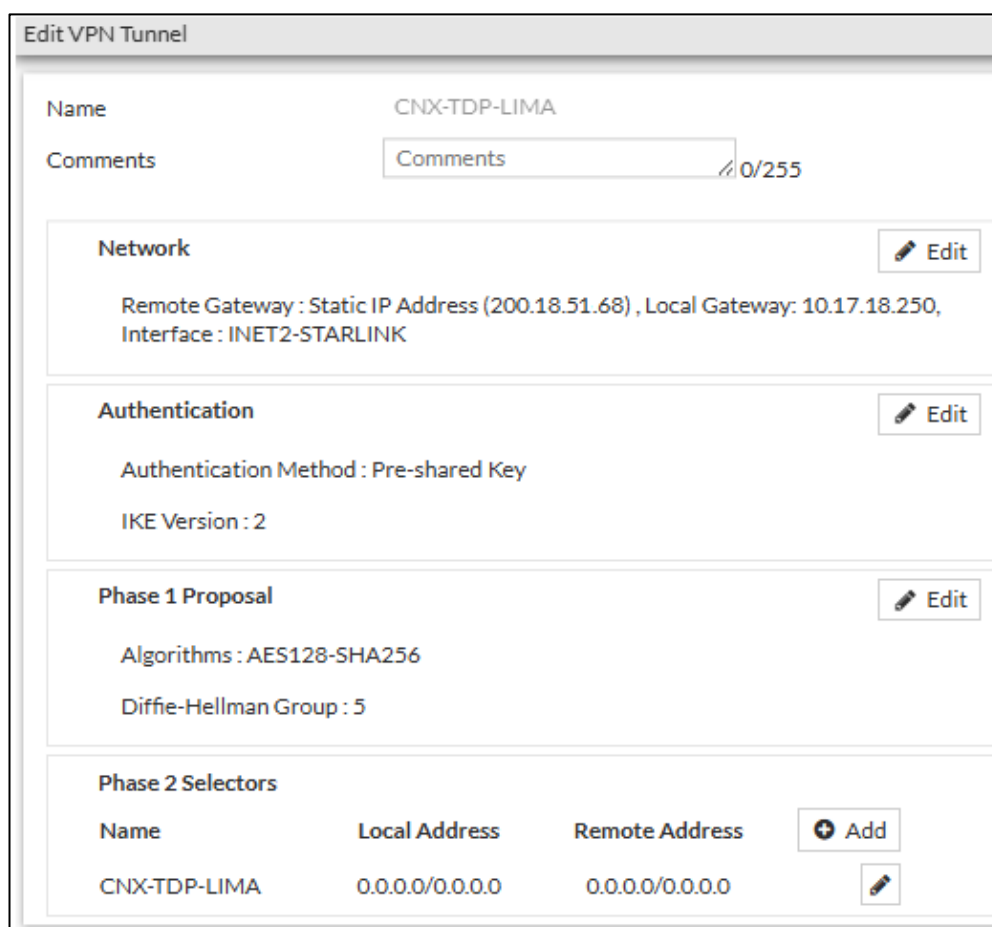


Tunnel	Interface Binding	Status
Custom		
CNX-TDP-LIMA	INET2-STARLINK (INET2-STARLINK)	Up
VPN-GFIBER-LIMA	INET1-GFIBER (INET1-GFIBER)	Up
VPN-LIMA-TDP	MPLS-TDP (MPLS-TDP)	Up

Fuente: Informe interno de implementación de servicio.

Figura E2

Configuración de túneles en equipo core Iquitos.



Edit VPN Tunnel

Name: CNX-TDP-LIMA

Comments: 0/255

Network Edit

Remote Gateway : Static IP Address (200.18.51.68) , Local Gateway: 10.17.18.250,
Interface : INET2-STARLINK

Authentication Edit

Authentication Method : Pre-shared Key

IKE Version : 2

Phase 1 Proposal Edit

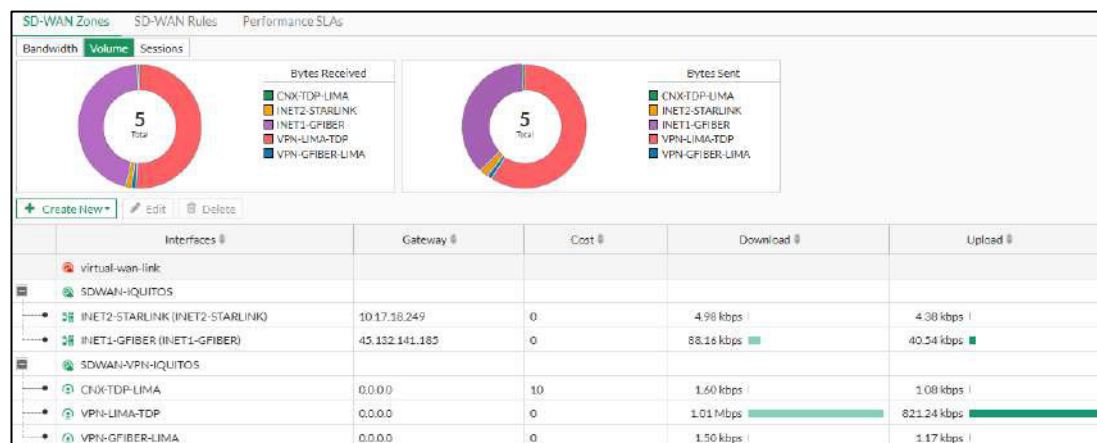
Algorithms : AES128-SHA256

Diffie-Hellman Group : 5

Phase 2 Selectors

Name	Local Address	Remote Address	
CNX-TDP-LIMA	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	Add Edit

Fuente: Informe interno de implementación de servicio.

Figura E3**Configuración de zonas SD-WAN**

Fuente: Informe interno de implementación de servicio.

Figura E4**Configuración de reglas SD-WAN**

ID	Name	Source	Destination	Criteria	Members	Hit Count
4	TO_OFFICE365_TRENDMICRO_TEAMS	all	Microsoft-Skype_Teams Microsoft-Teams.Published:Worldwide.Allow Microsoft-Teams.Published:Worldwide.Optimize Microsoft-DNS		INET1-GFIBER (INET1-GFIBER) VPN-LIMA-TDP INET2-STARLINK (INET2-STARLINK)	32,062,376
2	TO_VPN_LIMA	all	all		VPN-LIMA-TDP VPN-GFIBER-LIMA CNX-TDP-LIMA	221,792...

Fuente: Informe interno de implementación de servicio.

Figura E5**Configuración de políticas SD-WAN en equipo Core Fortinet**

Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Pro
DENY_IP_PRIVADAS	APP_MOVIL_BANCO (VLAN51)	SDWAN-VPN-IQUITOS	10.17.18.224/28	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	always	ALL	DENY		
TO-SLA-MONITOR	SDWAN-VPN-IQUITOS	SLA-MONITOR	all	all	always	ALL	ACCEPT	Disabled	no-its
ACCESS-SWITCH	SDWAN-IQUITOS	GESTION-BANCO	all	SWITCH SWITCH2 SWITCH3	always	ALL	ACCEPT	Disabled	no-its
INTERVLAN	GESTION-BANCO LED-MARK PC-BANCO POS-MC SEGURIDAD VOZ-BANCO Gestion_AP_banco (VLAN80)	GESTION-BANCO LED-MARK PC-BANCO POS-MC SEGURIDAD VOZ-BANCO Gestion_AP_banco (VLAN80)	all	all	always	ALL	ACCEPT	Disabled	no-its
SDWAN-IQUITOS	GESTION-BANCO LED-MARK PC-BANCO POS-MC SEGURIDAD VOZ-BANCO	SDWAN-IQUITOS	all	all	always	ALL	ACCEPT	Enabled	no-its
LAN_CNK-TDP	GESTION-BANCO LED-MARK	SDWAN-VPN-IQUITOS	all	all	always	ALL	ACCEPT	Disabled	no-its

Fuente: Informe interno de implementación de servicio.

Anexo F

Configuración de equipos networking LAN

Figura F1

Configuración de VLANs en switch LAN

```
IQUITOS-SUCURSAL#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Te1/1/3, Te1/1/4
20	PC	active	Gi1/0/4, Gi1/0/5, Gi1/0/6, Gi1/0/7, Gi1/0/8, Gi1/0/9, Gi1/0/10, Gi1/0/13, Gi1/0/14, Gi1/0/15, Gi1/0/16, Gi1/0/17, Gi1/0/19, Gi1/0/22, Gi1/0/23
25	SEGURIDAD	active	Gi1/0/18
50	POS-MC	active	
55	LEXMARK	active	Gi1/0/24
65	VOZ	active	Gi1/0/4, Gi1/0/5, Gi1/0/6, Gi1/0/7, Gi1/0/8, Gi1/0/9, Gi1/0/10, Gi1/0/13, Gi1/0/14, Gi1/0/15, Gi1/0/16, Gi1/0/17, Gi1/0/19, Gi1/0/22
70	GESTION	active	
80	AP-GESTION	active	
502	R-BCO-Internet	active	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

```
IQUITOS-SUCURSAL#
```

Fuente: Informe interno de implementación de servicio.

Figura F2

Configuración de interfaces de gestión de switches LAN

```
IQUITOS-SUCURSAL#show ip int br
```

vlan1	unassigned	YES NVRAM	up	down
vlan70	10.17.18.10	YES NVRAM	up	up
GigabitEthernet1/0/1	unassigned	YES unset	up	up
GigabitEthernet1/0/2	unassigned	YES unset	up	up
GigabitEthernet1/0/3	unassigned	YES unset	up	up
GigabitEthernet1/0/18	unassigned	YES unset	up	up
GigabitEthernet1/0/22	unassigned	YES unset	up	up
GigabitEthernet1/0/24	unassigned	YES unset	up	up
Te1/1/1	unassigned	YES unset	up	up
Te1/1/2	unassigned	YES unset	up	up

```
IQUITOS-SUCURSAL#
```

```
IQUITOS-SUCURSAL#show run int vlan 70
```

```
Building configuration...
```

```
Current configuration : 92 bytes
```

```
!
```

```
interface vlan70
```

```
description GESTION
```

```
ip address 10.17.18.10 255.255.255.224
```

```
end
```

```
IQUITOS-SUCURSAL#show run int Te1/1/1
```

```
Building configuration...
```

```
Current configuration : 116 bytes
```

```
!
```

```
interface TenGigabitEthernet1/1/1
```

```
switchport trunk allowed vlan 20,25,50,55,65,70,80
```

```
switchport mode trunk
```

```
end
```

Fuente: Informe interno de implementación de servicio.