



Universidad Nacional Mayor de San Marcos
Universidad del Perú. Decana de América
Facultad de Ingeniería Electrónica y Eléctrica
Escuela Profesional de Ingeniería de Telecomunicaciones

**Diseño e implementación de solución satelital Starlink
para mejorar conectividad y seguridad de navegación
en una entidad rural de Loreto**

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de Ingeniera de
Telecomunicaciones

AUTOR

Diana Fiorela LLANTOY PARRA

ASESOR

Mg. Ana Milagros CORONEL CHAMORRO

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

Llantoy, D. (2026). *Diseño e implementación de solución satelital Starlink para mejorar conectividad y seguridad de navegación en una entidad rural de Loreto*. [Trabajo de suficiencia profesional de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería Electrónica y Eléctrica, Escuela Profesional de Ingeniería de Telecomunicaciones]. Repositorio institucional Cybertesis UNMSM.

Metadatos complementarios

Datos de autor	
Nombres y apellidos	Diana Fiorela Llantoy Parra
Tipo de documento de identidad	DNI
Número de documento de identidad	71224319
URL de ORCID	No Aplica
Datos de asesor	
Nombres y apellidos	Ana Milagros Coronel Chamorro
Tipo de documento de identidad	DNI
Número de documento de identidad	09752919
URL de ORCID	https://orcid.org/0000-0003-2165-0742
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Teresa Esther Nuñez Zuñiga
Tipo de documento	DNI
Número de documento de identidad	08006778
Miembro del jurado 1	
Nombres y apellidos	Wilbert Chavez Irazabal
Tipo de documento	DNI
Número de documento de identidad	08121733
Miembro del jurado 2	
Nombres y apellidos	Jean Carlos Malca Fernández
Tipo de documento	DNI
Número de documento de identidad	45535181
Datos de investigación	
Línea de investigación	C.03.10 – Redes de datos
Grupo de investigación	No Aplica
Agencia de financiamiento	No Aplica

Ubicación geográfica de la investigación	Edificio: Centro Empresarial Juan de Arona País: Perú Departamento: Lima Provincia: Lima Distrito: San Isidro Dirección: Avenida Juan de Arona 151, San Isidro Latitud: -12.096701319699593 Longitud: -77.03210059150015
Año o rango de años en que se realizó la investigación	2024-2025
URL de disciplinas OCDE	Telecomunicaciones https://purl.org/pe-repo/ocde/ford#2.02.05 Ingeniería de sistemas y comunicaciones https://purl.org/pe-repo/ocde/ford#2.02.04 Ingeniería eléctrica, Ingeniería electrónica https://purl.org/pe-repo/ocde/ford#2.02.01



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°41/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 19 de Junio del 2026, como presidente de Jurado la **DRA. TERESA ESTHER NUÑEZ ZUÑIGA**, integrado por el Miembro de Jurado el **MG. WILBERT CHAVEZ IRAZABAL**, el Miembro de Jurado el **MG. JEAN CARLOS MALCA FERNÁNDEZ** y Miembro Asesor la **MG. ANA MILAGROS CORONEL CHAMORRO**.

Después de escuchar la Sustentación Presencial del Trabajo de Suficiencia Profesional de la Bachiller **DIANA FIORELA LLANTOY PARRA** con código 16190024 que para optar el Título Profesional de Ingeniera de Telecomunicaciones sustentó el Trabajo de Suficiencia Profesional titulado **DISEÑO E IMPLEMENTACIÓN DE SOLUCIÓN SATELITAL STARLINK PARA MEJORAR CONECTIVIDAD Y SEGURIDAD DE NAVEGACIÓN EN UNA ENTIDAD RURAL DE LORETO**.

El jurado examinador procedió a formular las preguntas reglamentarias y, luego de una deliberación en privado, decidió otorgarle el calificativo de 17 Diecisiete.

Ciudad Universitaria, 19 de junio del 2026

DRA. TERESA ESTHER NUÑEZ ZUÑIGA
Presidente Jurado

MG. WILBERT CHAVEZ IRAZABAL
Miembro Jurado

MG. JEAN CARLOS MALCA FERNÁNDEZ
Miembro Jurado

MG. ANA MILAGROS CORONEL CHAMORRO
Miembro Asesor



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

CERTIFICADO DE SIMILITUD

Yo, **ANA MILAGROS CORONEL CHAMORRO** en mi condición de asesor acreditado con el Dictamen N°43/FIEE-PPP/2026 del Trabajo de Suficiencia Profesional titulado **DISEÑO E IMPLEMENTACIÓN DE SOLUCIÓN SATELITAL STARLINK PARA MEJORAR CONECTIVIDAD Y SEGURIDAD DE NAVEGACIÓN EN UNA ENTIDAD RURAL DE LORETO**, presentado por la bachiller **DIANA FIORELA LLANTOY PARRA**, para optar el título profesional de Ingeniera de Telecomunicaciones. 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 7% 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 profesional de Ingeniera de Telecomunicaciones.

Lima, 19 de Junio del 2026

Firma del Asesor

DNI: 097529107

Nombres y apellidos del asesor:

ANA MILAGROS CORONEL CHAMORRO

DEDICATORIA

Este trabajo está dedicado a mis padres, por su amor incondicional, su apoyo constante y por haber sido el pilar fundamental en cada etapa de mi formación personal y profesional. A ellos, que con esfuerzo y sacrificio me enseñaron el valor de la perseverancia y la responsabilidad, guiándome siempre con ejemplo, dedicación y fortaleza.

AGRADECIMIENTOS

Expreso mi sincero agradecimiento a la empresa por brindarme la oportunidad de desarrollar este trabajo y facilitar los recursos necesarios para su ejecución. Asimismo, agradezco a los profesionales y colaboradores que aportaron orientación durante el proceso, y a mi asesora de tesis por su valiosa guía y acompañamiento.

RESUMEN

El presente trabajo de suficiencia profesional desarrolla el diseño e implementación de una solución satelital Starlink, para mejorar la conectividad y seguridad de navegación en una entidad rural de la Loreto.

La metodología se estructura en cuatro etapas: análisis de requerimientos, diseño de la red, implementación del servicio y validación y puesta en operación. Durante la fase de análisis, se determina que las soluciones tradicionales, como la fibra óptica y los radioenlaces, no resultan viables debido a limitaciones geográficas y técnicas propias del entorno. En consecuencia, se opta por una solución satelital de órbita baja (LEO), que permite reducir la latencia y mejorar la estabilidad del servicio.

Como resultado, se implementa una infraestructura de comunicaciones que garantiza conectividad estable, baja latencia y un entorno seguro mediante la integración de un mecanismo de seguridad basado en software virtualizado. Las pruebas posteriores a la implementación evidencian mejoras relevantes en el desempeño del servicio, cumpliendo con los requerimientos de ancho de banda, latencia y disponibilidad establecidos por la entidad.

Palabras clave: Internet Satelital, Starlink, Seguridad de red, conectividad, latencia.

ABSTRACT

This professional proficiency work presents the design and implementation of a secure satellite internet solution based on Starlink technology, aimed at improving connectivity and browsing security in a rural entity located in Loreto.

The methodology is structured into four stages: requirements analysis, network design, service implementation, and validation and deployment. During the analysis phase, it was determined that traditional solutions such as fiber optics and radio links were not feasible due to geographical and technical constraints of the environment. Therefore, a Low Earth Orbit (LEO) satellite solution was selected, enabling reduced latency and improved service stability.

As a result, a communications infrastructure was implemented to ensure stable connectivity, low latency, and a secure environment through the integration of a virtualized software-based security mechanism. Post-implementation tests demonstrated significant improvements in service performance, meeting the bandwidth, latency, and availability requirements established by the organization.

Keywords: Satellite Internet, Starlink, Network Security, Connectivity, Latency.

INDICE GENERAL

RESUMEN	IV
ABSTRACT	V
INDICE GENERAL	VI
LISTA DE FIGURAS	VIII
LISTA DE TABLAS	X
CAPITULO I: INTRODUCCIÓN	11
CAPITULO II: INFORMACIÓN DEL LUGAR DONDE SE DESARROLLÓ LA ACTIVIDAD	13
2.1 INSTITUCIÓN – ACTIVIDAD QUE DESARROLLA	13
2.2 PERIODO DE DURACIÓN DE LA ACTIVIDAD	13
2.3 FINALIDAD Y OBJETIVOS DE LA ENTIDAD	13
2.4 RAZÓN SOCIAL	14
2.5 DIRECCIÓN POSTAL	14
2.6 NOMBRE Y CORREO ELECTRÓNICO DEL PROFESIONAL A CARGO	14
CAPITULO III: DESCRIPCIÓN DE LA ACTIVIDAD	15
3.1 ORGANIZACIÓN DE LA ACTIVIDAD	15
3.2 FINALIDAD Y OBJETIVOS DE LA ACTIVIDAD	16
3.2.1 <i>Finalidad</i>	17
3.2.2 <i>Objetivos</i>	17
3.3 PROBLEMÁTICA	17
3.3.1 <i>Problema General</i>	19
3.3.2 <i>Problemas Específicos</i>	19
3.3.3 <i>Justificación e importancia de la investigación</i>	19
3.4 METODOLOGÍA	21

3.4.1	<i>Bases teóricas</i>	21
3.4.2	<i>Marco conceptual</i>	26
3.5	PROCEDIMIENTO	36
3.5.1	<i>Etapa 1: Análisis del requerimiento</i>	37
3.5.2	<i>Etapa 2: Diseño de la red</i>	53
3.5.3	<i>Etapa 3: Implementación del servicio</i>	62
3.5.4	<i>Etapa 4: Validación y puesta en operación</i>	78
3.6	RESULTADO DE LA ACTIVIDAD	82
3.6.1	<i>Resultado de la evaluación del medio de transmisión de datos</i>	82
3.6.2	<i>Resultado de la evaluación de la mejor tecnología</i>	85
3.6.3	<i>Resultado de la evaluación del equipamiento</i>	87
3.6.4	<i>Resultado de la solución diseñada e implementada</i>	90
CAPITULO IV: DISCUSION DE RESULTADOS		93
4.1	DESCRIPCIÓN DE LA IMPLEMENTACIÓN	93
4.2	EVALUACIÓN ECONÓMICA	94
4.2.1	<i>CÁLCULO DEL VAN</i>	97
4.2.2	<i>CÁLCULO DEL TIR</i>	98
CAPITULO V: CONCLUSIONES		100
CAPITULO VI: RECOMENDACIONES		102
CAPITULO VII: REFERENCIAS BIBLIOGRÁFICAS		104
CAPITULO VIII: ANEXOS		109
ANEXO A		109
ANEXO B		111

LISTA DE FIGURAS

Figura 1 Organigrama de ON EMPRESAS.	15
Figura 2 Flujograma de las etapas del procedimiento.	37
Figura 3 Recorrido del tendido de fibra óptica para la sede Abelardo.	40
Figura 4 Recorrido del tendido de la fibra óptica para la sede Napo.	41
Figura 5 Recorrido del tendido de fibra óptica para la sede Abelardo.	41
Figura 6 Recorrido del radioenlace para la sede Abelardo.	43
Figura 7 Recorrido del radioenlace para la sede Napo.	43
Figura 8 Recorrido de fibra óptica para la sede Echenique.	44
Figura 9 Visibilidad al cielo para la sede Abelardo.	45
Figura 10 Visibilidad al cielo para la sede Napo	45
Figura 11 Visibilidad al cielo para la sede Echenique.	46
Figura 12 Evaluación del equipamiento router.	55
Figura 13 Características de las antenas satelitales Starlink.	56
Figura 14 Topología de red y sistema de seguridad para cada sede.	61
Figura 15 Configuración de las interfaces físicas de red.	67
Figura 16 Configuración de las interfaces lógicas de loopback.	68
Figura 17 Configuración de las interfaces lógicas de red.	68
Figura 18 Configuración de objetos de las redes internas.	69
Figura 19 Configuración de grupo de objetos.	70
Figura 20 Configuración de seguridad: Antivirus.	70
Figura 21 Configuración de seguridad: Protección vulnerabilidades	71
Figura 22 Configuración de seguridad: Filtrado web.	72
Figura 23 Configuración de seguridad: Wildfire Analysis.	72
Figura 24 Configuración de las políticas de acceso.	73
Figura 25 Configuración de la regla SNAT.	74
Figura 26 Componentes del Kit Satelital.	74
Figura 27 Instalación de la antena satelital.	75

Figura 28 Conexión del Kit Satelital.	76
Figura 29 Inicio de credenciales en el aplicativo de Starlink.	77
Figura 30 Conexión del Kit Satelital hacia el router.	77
Figura 31 Validación de conexión a internet.	79
Figura 32 Validación del software de seguridad.	79
Figura 33 Validación de los requerimientos de la sede Abelardo.	80
Figura 34 Validación de los requerimientos de la sede Napo.	81
Figura 35 Validación de los requerimientos de la sede Echenique.	81
Figura 36 Evidencia de carga y descarga de la sede Abelardo.	83
Figura 37 Evidencia de carga y descarga de la sede Napo.	84
Figura 38 Evidencia de carga y descarga de la sede Echenique.	84
Figura 39 Evidencia de latencia de la sede Abelardo.	85
Figura 40 Evidencia de latencia de la sede Napo.	86
Figura 41 Evidencia de latencia de la sede Echenique.	86
Figura 42. Evidencia mediante el reporte de seguridad.	90

LISTA DE TABLAS

Tabla 1. Población de 12 y más años de edad que usa internet.	20
Tabla 2. Requerimiento del cliente.	38
Tabla 3. Costos por sede y total mediante el medio de transmisión de fibra óptica	42
Tabla 4 Costos por sede y total mediante el medio de transmisión satelital.	46
Tabla 5 Costos por sede mediante el medio de transmisión fibra óptica	47
Tabla 6 Características del servicio actual y el servicio propuesto	50
Tabla 7. Características de las antenas que ofrece Starlink	55
Tabla 8. Características del servicio: Servidor + Software de seguridad	57
Tabla 9. Características del software de seguridad Palo Alto	58
Tabla 10. Configuración del router Cisco	66
Tabla 11 Disponibilidad mediante un determinado tiempo.	92
Tabla 12. Evaluación económica por las 3 sedes	96
Tabla 13 Costos de Operación y Mantenimiento (Opex) Anual	96
Tabla 14 Flujo de Caja a 3 años	97

CAPITULO I: INTRODUCCIÓN

En la actualidad, el acceso a internet constituye un elemento fundamental para el desarrollo económico y social del país, especialmente en aquellas zonas donde la brecha digital es significativa. En el Perú, si bien la conectividad ha mostrado un crecimiento sostenido en los últimos años, aún persisten importantes desigualdades entre áreas urbanas y rurales. De acuerdo con el Instituto Nacional de Estadística e Informática (INEI), aproximadamente el 79% de la población peruana utilizó internet en 2025 (INEI, 2025), evidenciando avances en inclusión digital; sin embargo, en las zonas rurales el acceso continúa siendo limitado y desigual.

Asimismo, según el Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL), más del 92% de los hogares peruanos cuenta con algún tipo de acceso a internet fijo o móvil (OSIPTEL, 2025). No obstante, en las áreas rurales solo alrededor del 21.7% de los hogares dispone de internet fijo (COMEXPERU, 2025), lo que refleja una brecha significativa respecto a las zonas urbanas. Adicionalmente la calidad del servicio en estas zonas suele ser inferior, con velocidades de conexión considerablemente menores, lo que restringe el acceso a servicios digitales esenciales como educación, salud y gestión pública.

En este contexto, la persistencia de la brecha digital en regiones rurales y amazónicas evidencia la necesidad de implementar soluciones tecnológicas innovadoras que permitan garantizar un acceso equitativo, continuo y de calidad a los servicios de internet. En regiones como Loreto, la conectividad presenta serias limitaciones debido a la escasa infraestructura, así como a condiciones geográficas y climáticas adversas, las cuales dificultan la

implementación de tecnologías tradicionales como la fibra óptica y los radioenlaces.

En respuesta a esta problemática, el presente trabajo propone el diseño e implementación de una solución de internet satelital Starlink, la cual utiliza satélites de órbita baja (LEO) para ofrecer menores niveles de latencia y mayor estabilidad en la conexión. Asimismo, se incorporan mecanismos de seguridad basados en la nube que permiten proteger la navegación de los usuarios frente a diversas amenazas informáticas.

El desarrollo del trabajo comprende las etapas de análisis de requerimientos, diseño de la red, implementación del servicio, así como la validación y puesta en operación. Los resultados obtenidos evidencian que la solución propuesta es técnicamente viable, eficiente y adecuada para mejorar tanto la conectividad como la seguridad en zonas rurales.

CAPITULO II: INFORMACIÓN DEL LUGAR DONDE SE DESARROLLÓ LA ACTIVIDAD

2.1 Institución – Actividad que desarrolla

El presente Trabajo de Suficiencia Profesional (TSP) se desarrolla en la compañía de ON EMPRESAS, organización especializada en la provisión de soluciones de conectividad, servicios gestionados, interconexión entre sedes y servicios de centro de datos, entre otros. En este contexto, el servicio se orienta a atender los requerimientos de una entidad que demanda conectividad con navegación segura.

2.2 Periodo de duración de la actividad

El periodo de ejecución del presente trabajo fue desde abril del año 2024 hasta setiembre del año 2024.

Dicho intervalo comprende desde la identificación y análisis de la problemática planteada por la entidad hasta la implementación completa de la solución en todas sus sedes.

2.3 Finalidad y objetivos de la entidad

ON Empresas es una organización del sector de Telecomunicaciones y Tecnologías de la Información cuya finalidad y objetivo es desafiar lo convencional para acelerar la evolución digital de las empresas, sumando creatividad e innovación para asegurar un servicio con una propuesta de valor distinta, eficiente, sostenible y competitiva, adaptada a las necesidades del mercado actual.

2.4 Razón social

ON EMPRESAS S.A.C: 20552504641

2.5 Dirección postal

Dirección: Av. José Gálvez Barrenechea 645, Lima 15036, Lima – San Borja.

2.6 Nombre y correo electrónico del profesional a cargo

- Nombre: Rudy, Carlos Ostoa
- Profesional: Gerente de Ingeniería Preventa

CAPITULO III: DESCRIPCIÓN DE LA ACTIVIDAD

3.1 Organización de la actividad

En la Figura 1 se muestra las áreas de la empresa que participaron en el desarrollo de la actividad, cuyo contorno de cuadros se encuentran de color verde.

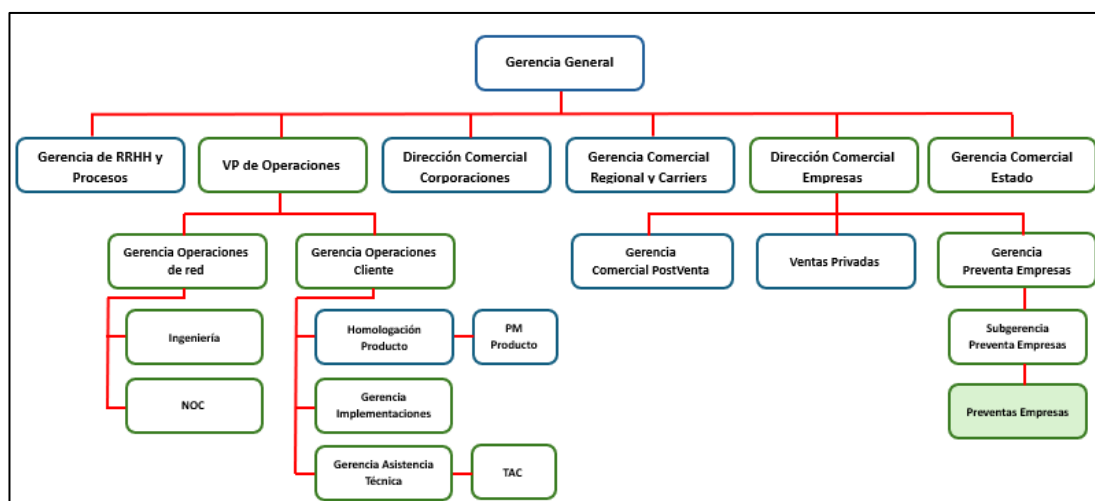


Figura 1 Organigrama de ON EMPRESAS. Fuente: Elaboración propia a partir de la plataforma de ON EMPRESAS.

Nota: El Organigrama representa las áreas de la empresa ON EMPRESAS y su división mediante jefaturas y gerencias.

La organización y participación de cada área (en contorno verde) en el desarrollo de la actividad se detallan a continuación:

- ❖ VP de Operaciones: Es la responsable de supervisar tanto la red de ON EMPRESAS como la red del cliente, garantizando la continuidad operativa y la calidad del servicio.
 - Gerencia de Operaciones de red: Encargada de la gestión y supervisión de la infraestructura de red.

- Área de Ingeniería: Se encarga del diseño y la planificación de soluciones que aseguren la correcta operación y eficiencia de la red de la empresa y del cliente.
- Área del NOC: Supervisa el funcionamiento de la red del cliente en tiempo real, detectando y gestionando incidentes o alarmas operativas.
- Gerencia Operaciones Cliente: Se encarga de coordinar la atención y soporte brindado al cliente.
 - Gerencia Implementaciones: Se encarga de la ejecución de nuevos proyectos solicitadas por el cliente.
 - Gerencia de Asistencia Técnica: Se encarga de proporcionar soporte especializado ante incidencias o requerimientos técnicos del cliente.
- ❖ Dirección Comercial Empresas: Se encarga de la gestión de las actividades comerciales, incluyendo al equipo comercial y preventa, quienes son responsables de ofrecer nuevos servicios y soluciones que contribuyan a la mejora de la red del cliente.
 - Gerencia Preventa Empresas: Se encarga de supervisar los requerimientos que ingresan al área de preventa, de acuerdo con las solicitudes del cliente derivadas por el equipo comercial.
 - Área de Preventa Empresas: Desarrolla soluciones técnicas y diseña propuestas a medida para satisfacer los requerimientos de los clientes.
- ❖ Gerencia Comercial Estado: Se encarga de la gestión comercial de los servicios orientados a entidades del sector público.

3.2 Finalidad y objetivos de la Actividad

En el presente trabajo de suficiencia profesional se propone el diseño e implementación de una solución de acceso satelital seguro en una entidad ubicada en la zona rural de Loreto.

3.2.1 Finalidad

Diseñar e implementar una solución satelital Starlink para mejorar la conectividad y seguridad de navegación en una entidad rural de Loreto.

3.2.2 Objetivos

- a. Determinar el medio de transmisión de datos más adecuado para mejorar la conectividad y seguridad de navegación en una entidad rural de Loreto.
- b. Determinar la mejor tecnología de servicio de internet satelital para mejorar la conectividad y seguridad de navegación en una entidad rural de Loreto.
- c. Determinar el tipo de equipamiento adecuado para un servicio de internet satelital con tecnología Starlink para mejorar la conectividad y seguridad de navegación en una entidad rural de Loreto.
- d. Determinar como la solución diseñada e implementada mejoró la conectividad y seguridad de navegación en una entidad rural de Loreto.

3.3 Problemática

En la actualidad, la conectividad a internet se encuentra entre las necesidades básicas del ser humano ya que proporciona un apoyo fundamental manteniendo la comunicación, la adquisición de conocimientos y la gestión de negocios. Hoy en día, las personas son dependientes del internet para desarrollar un trabajo eficiente y competente, principalmente en el ámbito social, salud, educación y corporativo; así mismo, los proveedores de servicios buscan cubrir las áreas urbanas y rurales mediante servicios de internet de fibra óptica y radioenlace. Sin embargo, en su mayoría enfrentan desafíos geográficos en el despliegue de los servicios de conectividad en las zonas rurales, debido a que la existencia de red de fibra óptica es escasa y no hay línea de vista entre antenas para un servicio de radioenlace a diferencia de un servicio de internet satelital. Del mismo modo, para las empresas localizadas en una zona rural, la conectividad es primordial, ya que una conexión inestable puede perjudicarlas significativamente. La mayoría de

ellas dependen de plataformas web y realizan reuniones virtuales, las cuales no serían eficientes sin un buen servicio de internet, afectando directamente su productividad, generando retrasos y malestar tanto interno como en sus clientes.

Para un servicio de internet, es importante considerar el nivel de latencia, ya que un tiempo de respuesta inmediata permite una conectividad óptima y eficiente. Una latencia elevada puede generar lentitud en la red, lo que afectaría negativamente el desempeño y haría que el servicio no sea la mejor opción. En el caso de las empresas o entidades ubicadas en zonas rurales, como en el departamento de Loreto, es indispensable contar con una conexión estable, ya que una alta latencia puede provocar demoras en la carga de plataformas web, lo cual ralentiza el trabajo de los colaboradores y retrasa el cumplimiento de sus tareas asignadas, perjudicando la productividad. Por ese motivo, una solución de internet satelital es la más adecuada. Las tecnologías satelitales disponibles son Starlink y VSAT, entre las cuales se debe optar por aquella que proporcione una baja latencia, con el fin de garantizar conectividad en todo momento y por tanto mejorar la productividad de las empresas. Así mismo, este medio de transmisión utiliza diversos equipamientos, los cuales poseen características que se diferencian entre sí según el uso específico que cada cliente requiera para adaptar su servicio de internet satelital seguro.

Por otro lado, la navegación en internet no es muy segura debido a que existen distintas amenazas que pueden ocasionar el robo de datos causando daños a la red interna, esto también es un desafío, por lo cual, los proveedores ofrecen soluciones de seguridad para brindar protección de la red. Del mismo modo, existen distintas entidades y empresas que se encuentran en zonas rurales y requieren proteger su información ante las amenazas que hay en la navegación. Resulta relevante considerar, que al adquirir un servicio de Internet se debe proporcionar la seguridad en la navegación para prevenir pérdidas de datos y las interrupciones de operaciones dentro de una entidad.

Las entidades y empresas ubicadas en zonas rurales, como en el departamento de Loreto aún desconocen la alternativa que representa el medio de transmisión satelital. Por ello, es necesario investigar esta problemática, con el objetivo de analizar cómo el servicio satelital Starlink, puede reducir las amenazas de seguridad, a la vez mejorar la conectividad, considerando factores geográficos y de rendimiento como la latencia y el equipamiento requerido. Esto fortalece la navegación segura y mejora la conectividad en entornos donde otras tecnologías resultan limitadas.

3.3.1 Problema General

¿Cómo realizar el diseño e implementación de una solución satelital Starlink para mejorar la conectividad y seguridad de navegación en una entidad rural de Loreto?

3.3.2 Problemas Específicos

- a) ¿Cómo determinar el medio de transmisión de datos más adecuado para mejorar la conectividad y seguridad de navegación en una entidad rural de Loreto?
- b) ¿Cómo determinar la mejor tecnología de servicio de internet satelital para mejorar la conectividad y seguridad de navegación en una entidad rural de Loreto?
- c) ¿Cómo determinar el tipo de equipamiento adecuado de un servicio de internet satelital con tecnología Starlink para mejorar la conectividad y seguridad de navegación en una entidad rural de Loreto?
- d) ¿Cómo la solución diseñada e implementada mejoró la conectividad y seguridad de navegación en una entidad rural de Loreto?

3.3.3 Justificación e importancia de la investigación

- a) Justificación Teórica: La zona rural de Loreto, la cual se encuentra ubicada en la región de la Selva, en los últimos años presentan un crecimiento en

el uso del servicio de internet. Según la última encuesta del Instituto Nacional de Estadística e Informática, que se muestra en la Tabla 1, se visualiza que en la región rural de la selva para el año 2024 y se evidencia una evolución positiva respecto del 2021 (INEI, 2024).

Tabla 1. Población de 12 y más años de edad que usa internet.

Región (Área Rural)	Año				Variación Porcentual (2024-2023)
	2021	2022	2023	2024	
Total	42%	47%	53.2%	58.4%	5.2%
Costa	58.6	65.4	70.2	73.6	3.4
Sierra	39.7	44.6	51.4	56.4	5
Selva	40.9	45.3	50.2	56.9	6.7

Fuente. Adaptado de Encuesta Nacional de Programas Presupuestales (p.36) por (INEI, 2024).

Nota: La tabla representa la variación del uso del internet en zona rural.

Bajo este contexto de crecimiento del uso de internet, y debido a la geografía del lugar que no permite desplegar fibra óptica o equipos radioenlaces para la conectividad, se implementa el servicio de internet en la zona rural de Loreto mediante transmisión satelital con el propósito de atender las necesidades y la creciente demanda de este servicio en las diversas sedes de la entidad ubicada en la región de la Selva.

El internet satelital permite garantizar una conexión estable y segura, asegurando que la entidad disponga de las herramientas necesarias para fortalecer su gestión y mejorar los servicios brindados a la población. Así mismo, facilita la atención de consultas a través de portales web, como el Sistema Integrado de Información del Comercio Exterior, que les proporciona información de rutas de exportación y agiliza el proceso de atención para el registro de los negocios.

- b) Justificación Práctica: Las personas que utilizan el internet se encuentran expuestos a diversos riesgos como el robo de información. Para la entidad, es primordial brindar un servicio seguro que garantice la protección de datos confidenciales que se obtiene durante el registro de los negocios y otras interacciones con sus clientes. Por este motivo se integra el servicio

de seguridad en la navegación, para resguardar la información privada de la entidad. Así mismo, se tiene un mejor control sobre el acceso a la navegación, restringiendo el acceso a páginas indebidas, distractoras, maliciosas, entre otras; por parte de los colaboradores de la entidad.

Según la Ley N°29733, Ley de Protección de Datos Personales, indica que se debe resguardar los datos personales y confidenciales contenidos o que se vayan a contener en bancos de datos públicos o privados referente a personas naturales y jurídicas. Por ello, el implementar este servicio en la entidad, que administra información privada de los negocios exportadores a través de sus servicios de Intranet, asegura la protección de la información de los usuarios y el cumplimiento de la ley.

Justificación Social: Es importante el uso de la tecnología en la entidad, debido a los siguientes factores: El primer factor es la mejora de la eficiencia operativa, la cual permite la optimización del acceso a Internet reduciendo los costos e incrementando la productividad. El segundo factor es fomentar la innovación, esta permite desarrollar nuevos productos analizando datos y tendencias de los clientes. El tercer factor es la mejora en la comunicación y colaboración, permitiendo una buena comunicación interna y externa y un ambiente colaborativo. El cuarto factor es la toma de decisiones informadas a partir de la base de datos que se obtiene debido a la digitalización (González & Octavio, 2024).

Así mismo, el acceso de Internet seguro en la entidad, además de optimizar sus procesos, permite compartir videos instructivos para los negocios exportadores, y realizar reuniones virtuales.

3.4 Metodología

3.4.1 Bases teóricas

3.4.1.1 Nacionales

(Juárez & Terrones, 2021), resaltan la importancia de evaluar alternativas satelitales desde una perspectiva técnica, considerando el ancho de banda

requerido por las diversas entidades. La implementación de esta tecnología permite ofrecer servicios de Internet en zonas de difícil acceso geográfico, en comunidades dispersas y áreas no atendidas por las redes existentes. Presentan como justificación tecnológica el análisis de las tecnologías de sistemas satelitales en el Perú, ya que el despliegue de acceso a Internet no se ha adecuado a ciertas zonas del territorio geográfico del Perú. Es por ese motivo que se debe brindar un servicio de internet satelital en las zonas de difícil acceso para así facilitar el acceso a información y servicios esenciales, y fortalecer las actividades productivas y administrativas que dependen de la conectividad.

(Alcócer, 2018), presenta como problemática el limitado acceso a los servicios de Telecomunicaciones debido a su ubicación geográfica, ya que se encuentra en zonas de difícil acceso por la altitud de las cordilleras de los Andes y las lejanas profundidades de la selva, a la cual solo se accede vía fluvial. Así mismo, el despliegue de redes en zonas rurales alejadas y dispersas de la sierra y selva es reducido por el alto costo de la inversión. Es por ese motivo que la conectividad mediante el servicio Satelital es la alternativa más adecuada para las zonas rurales de difícil acceso, ya que permite brindar una conectividad viable y continua.

Así mismo, en el documento menciona la importancia del desarrollo de una plataforma satelital para atender a la población ubicada en zonas rurales que no pueden ser beneficiada mediante una red de fibra óptica. Estos centros poblados poseen un gran potencial debido a la riqueza de su cultura, así como de sus productos, los cuales tienen mucha demanda en los mercados nacionales e internacionales tales como quinua, maíz amarillo duro, los tubérculos y diversas plantas medicinales. Para impulsar el desarrollo de estos mercados, se requiere que los productores dispongan de información actualizada y canales de comunicación que permita realizar transacciones comerciales. Por tal motivo, el servicio de Internet Satelital en zonas rurales es indispensable para fortalecer los negocios orientados a la exportación de productos, para mejorar su competitividad y promover el mercado mediante el turismo.

(Loyaga, 2024), realizó entrevistas a expertos militares de la comunidad fronteriza de Cantagallo respecto al empleo de la tecnología Satelital. Como resultado, los entrevistados coinciden en que dicha tecnología constituye un componente fundamental para la conectividad y la comunicación a nivel global; destacando la capacidad de brindar esta solución a pesar de la lejanía del lugar; así mismo consideran que la tecnología satelital brinda una visión de transformación económico y social. Por esa razón, es importante considerar un servicio de Internet Satelital para asegurar una conectividad continua en zonas rurales. Así mismo, la población ubicada en zonas alejadas viene adaptándose progresivamente a este servicio y lo considera primordial para mantenerse conectados y acceder a la información digital.

(Franco & Bejarano, 2025), presenta como problemática los ataques informáticos sufridos por una empresa, las cuales generan interrupciones operativas, pérdida de datos y disminución de la productividad. Estos incidentes comprometen la seguridad de la información confidencial y la integridad de los sistemas de la empresa, por ello, la ausencia de un sistema de seguridad perimetral expone a la empresa a diversas vulnerabilidades permitiendo que los atacantes accedan a la red interna y provoquen daños significativos. La empresa que analiza presenta las siguientes vulnerabilidades: ataques cibernéticos dirigidos al robo de datos e información, interrupciones operativas provocando la caída de los sistemas y servicios esenciales de la empresa, exposición de la información confidencial y la ausencia de un sistema de seguridad perimetral. Los autores proponen un sistema integral de Seguridad Perimetral basado en un equipo firewall que inspecciona el tráfico para bloquear amenazas, así como de un control de acceso seguro para los usuarios remotos, garantizando que solo los usuarios autorizados accedan a los recursos y datos necesarios de la red empresarial. Por estos motivos, es esencial incorporar un servicio de seguridad que garantice una conectividad segura, proteja la red evitando pérdida de datos y permitiendo la detección y el bloqueo de amenazas. Eso asegura una red confiable que fortalece la fiabilidad a sus usuarios. Así mismo, demuestra que contar con un servicio de internet seguro mejora la productividad, la eficiencia

y la eficacia; por lo tanto, es importante considerar este servicio en la implementación de una solución de conectividad.

3.4.1.2 Internacionales

(Cabrera, 2025), aborda los problemas de conectividad en áreas rurales y plantea como alternativa la implementación de una red satelital Starlink comparándola con la infraestructura de red inalámbrica para mejorar la conectividad. El autor realiza un análisis de las ventajas y desventajas de ambas tecnologías, destacando que la red Satelital Starlink resulta más accesible debido a su capacidad de proporcionar una cobertura global lo que convierte en una solución factible para zonas con infraestructura limitada; en cambio, la red inalámbrica depende de una infraestructura preexistente para poder implementarse. Así mismo, se señala que Starlink utiliza satélites de baja órbita, lo que facilita una conectividad estable y velocidades de transmisión más altas. El autor también recalca que Starlink depende de la visibilidad hacia cielo y de las condiciones atmosféricas. Por otra parte, la red inalámbrica convencional requiere una línea de vista terrestre entre antenas, por lo que la presencia de obstáculos puede impedir el alineamiento del enlace. Otro punto analizado es el equipamiento, donde se indica que la antena Starlink tiene un diseño compacto y resistente a condiciones climáticas adversas, permitiendo una instalación rápida y sencilla y, además, se instala en un ambiente despejado para garantizar su correcto funcionamiento. Los resultados obtenidos mediante la implementación de ambos tipos de redes evidencian que Starlink ofrece ventajas en términos de estabilidad, latencia y facilidad de implementación, gracias a su arquitectura. En contraste a la red inalámbrica, si bien es una solución válida y funcional, presenta mayores desafíos operativos, derivados de su sensibilidad a las condiciones físicas del entorno y la necesidad de mantener una línea de vista clara. El autor concluyó que Starlink es la mejor opción para áreas sin infraestructura, mientras que la red inalámbrica solo es viable donde ya existan torres y soporte técnico, debido a su mantenimiento exigente. Por tal motivo, es viable la adopción de una red satelital Starlink ya que constituye una alternativa altamente eficiente

para ampliar la conectividad en zonas rurales, reduciendo las limitaciones propias de la infraestructura tradicional y garantiza un servicio más estable, confiable y de rápida implementación.

(Slotte, 2025), tiene como objetivo investigar las amenazas de ciberseguridad que afectan a los sistemas satelitales, validar su impacto y analizar los tipos de medidas que puede emplearse para mitigar las vulnerabilidades. Esta investigación presenta como resultado los tipos de amenazas, vulnerabilidades, riesgos y ataques que pueden comprometer a un sistema satelital. Entre las vulnerabilidades, riesgos y amenazas identificadas se encuentran: malware y virus, intrusos y ataques, falta de planificación de la seguridad, sistema de detección de intrusos débiles, entre otros. Así mismo, el impacto asociado a estas vulnerabilidades incluye interrupciones operativas y de servicio como el internet, riesgos para la privacidad y seguridad de los datos, incremento de amenazas y daños a nivel organizacional. Las medidas de mitigación propuestas incluyen: implementación de una arquitectura de seguridad, adecuada configuración de sistemas y equipos como el firewall, desarrollo de estrategias para fortalecer la seguridad, combate de amenazas y fomentar la concienciación en seguridad dentro de las organizaciones. El autor concluye resaltando la importancia de la ciberseguridad en los sistemas satelitales y la existencia de métodos para mitigar las amenazas y vulnerabilidades según el impacto que se puede generar si no se abordan adecuadamente. Por tal motivo, es fundamental ofrecer un servicio de internet satelital seguro ya que la conectividad presenta vulnerabilidades y se debe proteger la navegación de internet para brindar mayor confiabilidad a los usuarios.

(Abdelraheem A, 2025), realiza una comparación detallada entre las soluciones de comunicación satelital VSAT y STARLINK. El estudio evidencia que STARLINK ofrece menores niveles de latencia y un mayor ancho de banda a comparación de la solución VSAT.

Así mismo, el autor destaca las diferencias en los costos de inversión asociados a cada solución, considerando tanto la infraestructura como la

operación del servicio. El autor concluye que las tecnologías satelitales han evolucionado significativamente, posicionando a las constelaciones LEO como una solución altamente competitiva para mejorar la conectividad en infraestructuras críticas, debido a su baja latencia, alta capacidad y menor costo.

3.4.2 Marco conceptual

Se definirá de manera precisa la nomenclatura, los términos técnicos y los conceptos fundamentales empleados a lo largo del presente trabajo de suficiencia profesional, con el fin de asegurar una comprensión coherente de los contenidos desarrollados.

STARLINK

Starlink es un sistema de conectividad a internet desarrollado por SpaceX, basado en una constelación de satélites en órbita terrestre baja (LEO). Su finalidad es proporcionar acceso a internet de alta velocidad y baja latencia en regiones rurales, remotas o con infraestructura limitada. La red opera mediante miles de satélites que trabajan en conjunto con estaciones terrestres y antenas de usuario, permitiendo una cobertura global progresiva (Starlink, 2025).

ZONA RURAL

La UNESCO-UIS (UNESCO, 2025) señala que una zona rural puede entenderse como “una región geográfica fuera de la aglomeración urbana”

Y según la National Geographic Society (Society, 2024), una zona rural es una extensión de tierra abierta donde existen pocas viviendas o edificaciones y donde la cantidad de habitantes es reducida, presentando una densidad poblacional muy baja.

Este tipo de territorio se ubica fuera de centros urbanos y se caracteriza por su amplitud geográfica y menor concentración de infraestructura, diferenciándose claramente de las áreas urbanizadas.

ROUTER

Según Cisco (CISCO, 2024), un router es un dispositivo de red que recibe y envía datos dentro de redes informáticas, y tiene la capacidad de conectar varias redes a la vez.

Además, el router dirige los datos mediante paquetes que contienen la dirección IP destino, analiza esa información y elige la mejor ruta para la transmisión, actuando como un despachador de datos.

Así, gracias a los routers es posible conectar múltiples equipos locales entre sí y con Internet, garantizando que los datos lleguen correctamente a su destino.

INTERNET

Según el RFC 1462 del IETF (IETF, 1993) , el Internet constituye un recurso de alcance mundial que interconecta a una enorme cantidad de usuarios. Lo conforman múltiples redes conectadas entre sí, dando lugar a un sistema que no es una única red, sino varias redes interconectadas. Las redes operan mediante un conjunto de protocolos estandarizados, que posibilitan la interoperabilidad entre ellas aun cuando utilicen tecnologías antiguas o distintos tipos de protocolos.

INTERNET SATELITAL

Según el artículo de revista científica publicado en Heliyon (Chen, Ma, & Wu, 2024), el Internet satelital consiste en un sistema de comunicación de alta velocidad, robusto y de amplia cobertura que opera mediante satélites. Esta infraestructura de red es creada a partir del despliegue de múltiples satélites que forma una red a gran escala, así mismo, utiliza dichos satélites como enlace para conectarse con estaciones y dispositivos terrestres. Su propósito es complementar y optimizar el desempeño de las redes terrestres.

INTERNET SATELITAL Y ÓRBITA

Según el artículo de revista científica publicado en Heliyon (Chen, Ma, & Wu, 2024), se precisa que los satélites se pueden clasificarse en tres grupos principales según la altura de su órbita: los de órbita baja (LEO), los de órbita

media (MEO) y los geoestacionarios (GEO). En el caso de los satélites MEO, su área de cobertura resulta más limitada que los satélites GEO y presentan una latencia mayor que los satélites LEO. No obstante, su despliegue y operación implica costos elevados debido a la necesidad de tecnologías avanzadas que permitan conservar la estabilidad de la órbita.

El internet satelital basado en satélites LEO se fundamenta en una constelación de satélites situados con una altitud orbital inferior a 2000 km. Las redes LEO emplean satélites de menor tamaño y su infraestructura implica costos más reducidos.

A diferencia de los sistemas satelitales GEO y MEO, la comunicación por satélite LEO aprovecha una órbita baja que permite conectar gran cantidad de usuarios en tierra con tiempo de respuesta baja y ofrece servicios de transformación de datos de alta velocidad. Asimismo, los costos de fabricación y lanzamiento de los satélites LEO son relativamente bajos, lo que aumenta la probabilidad de que logren cobertura global.

Según el artículo publicado en la IEEE (Kodheli, Maturo, Shankar, Merlano, & Chatzinotas, 2020), se señala que un elemento clave en las constelaciones de satélites es la altura de su órbita, ya que influye de manera directa en la latencia, la pérdida de señal y el alcance de la cobertura.

Existen tres tipos principales de órbitas: LEO, MEO y GEO. Sus altitudes típicas van de 500 a 900 km en LEO, de 5000 a 25 000 km en MEO y alrededor de 36 000 km en GEO. Un satélite ubicado en la órbita GEO puede cubrir aproximadamente un tercio de la tierra, esta cobertura abarca más del 99% de la población.

En cambio, las órbitas LEO y MEO requieren más satélites para lograr la cobertura global. La desventaja principal de los satélites GEO es su gran distancia respecto a la Tierra, lo que produce trayectorias más largas hacia las estaciones terrestres, mientras que los sistemas LEO ofrecen enlaces más cortos, similares a los de las redes terrestres. Como las señales viajan a la velocidad de la luz, una mayor distancia se traduce en un incremento del retardo de propagación afectando el rendimiento de aplicaciones en tiempo real.

NAVEGACION POR INTERNET

Según el artículo (Bielecki, y otros, 2010), indica que la navegación por internet la navegación por Internet es el proceso de desplazarse entre páginas web siguiendo enlaces para acceder a información o servicios. Desde un enfoque más técnico, el artículo expone que este proceso no se limita a una simple acción del usuario, sino que constituye un mecanismo organizado, donde el navegador funciona como un sistema que realiza operaciones secuenciales sobre la estructura interconectada de la web.

De este modo, navegar se interpreta como una interacción estructurada con un entorno digital que ordena y facilita el acceso a contenidos distribuidos.

DATOS

En el marco de las normas de International Organization for Standardization (ISO, 2015), los datos se entienden como forma de representación numérica, textual, visual o simbólica. Describe hechos, conceptos o instrucciones que puede ser almacenada, transmitida o procesada por sistemas informáticos.

Desde la perspectiva de NIST (NIST, 2019), los datos son un conjunto de valores, mediciones o registros obtenidos por un sistema, los cuales pueden organizarse o interpretarse para producir información útil.

TRANSMISIÓN DE DATOS

Según el libro “Data Transmission and networking media” (Binti & Binti, 2024), la transmisión de datos se refiere al proceso de enviar datos digitales o analógicos a través de un canal de comunicación desde un dispositivo hacia otro. Es un concepto fundamental en las tecnologías actuales ya que permite el intercambio de información entre computadoras, servidores y diversos dispositivos.

MEDIOS DE COMUNICACIÓN

Según el libro “Data Transmission and networking media” (Binti & Binti, 2024), los medios de comunicación en red se refieren a las diversas vías o canales físicos que permiten transferir datos entre dispositivos en una red. El tipo de

medio seleccionado influye directamente en la velocidad de transmisión, distancia y confiabilidad.

ANCHO DE BANDA

Según el libro “Data Transmission and networking media” (Binti & Binti, 2024), el ancho de banda representa la velocidad máxima con la que es posible enviar datos por un canal o vía de red. Generalmente se expresa en bits por segundo (bps), o en múltiplos como kilobits por segundo (Kbps), megabits por segundo (Mbps) y gigabits por segundo (Gbps).

SERVIDOR

De acuerdo con el IEEE (IEEE, 1990), un servidor es un sistema o programa que proporciona servicios, recursos o funcionalidades a otros sistemas denominados clientes, generalmente a través de una arquitectura distribuida o una red.

RED

De acuerdo a los estándares de la IEEE (IEEE, Standard Glossary of Computer Networking Terminology, 1995), una red es un conjunto de computadores, dispositivos o sistemas conectados entre sí mediante canales de comunicación, que permiten el intercambio de datos, la compartición de recursos y la coordinación de servicios dentro de una arquitectura de comunicación.

AMENAZAS

Según la norma ISO/IEC 27000 (ISO, 2018) , una amenaza se entiende como cualquier situación, condición o elemento que pueda originar un incidente no deseado y generar algún tipo de daño o impacto negativo en los activos de información, los procesos o la organización.

Según el NIST (NIST, Threat – Glossary, 2025), una amenaza es cualquier evento, condición o agente con la capacidad de causar un impacto negativo

sobre un sistema, red, organización o individuo, comprometiendo su funcionamiento, seguridad o integridad.

VULNERABILIDAD

De acuerdo con el NIST (NIST, Vulnerability – Glossary, 2024), una vulnerabilidad es una debilidad, falla o deficiencia presente en un sistema, red, proceso, software o control de seguridad, que puede ser aprovechada por una amenaza para causar un impacto negativo, comprometer la confidencialidad, integridad o disponibilidad, o afectar el funcionamiento normal de un entorno tecnológico.

Según la RFC 4949 (Shirey, 2007), una vulnerabilidad es una debilidad, error o característica deficiente en un sistema, protocolo, diseño, implementación o configuración, que puede ser aprovechada por un atacante o una amenaza para violar una política de seguridad o afectar el funcionamiento normal de la red o del sistema.

COBERTURA

Según la RFC 4949 (Shirey, 2007), la cobertura en el contexto de redes y comunicación se refiere al alcance geográfico o funcional de una red, determinado por su capacidad para ofrecer conectividad y servicios a los usuarios dentro de un área o dominio específico.

Este término incluye la accesibilidad y disponibilidad del servicio, lo cual es esencial para asegurar la cobertura completa de un sistema o red de comunicación.

FIBRA ÓPTICA

De acuerdo con la ITU-T (ITU-T, 2024), la fibra óptica es un medio de transmisión físico compuesto por un filamento dieléctrico, generalmente de vidrio o plástico, diseñado para guiar señales luminosas a lo largo de su estructura, permitiendo la transmisión de información a altas velocidades, con bajas pérdidas y mínima interferencia, siendo ampliamente utilizada en redes de telecomunicaciones y de acceso a Internet.

RADIOENLACE

Según el diccionario de la lengua española (Española, 2024), el radioenlace es una conexión entre dos puntos mediante ondas radioeléctricas.

(Gonzales, 2018), indica que la comunicación por radioenlace se determina como la interconexión entre terminales de telecomunicaciones que se realiza mediante ondas electromagnéticas a través de un medio no guiado, conocidas también como STL (Studio Transmitter Link o Enlace Estudio-Transmisor). Estas ondas operan en el rango de las microondas, correspondiente al espectro de altas frecuencias, que abarca desde 300 MHz hasta 300 GHz, con longitudes de onda comprendidas entre 1 m y 1 mm. No obstante, es más habitual el empleo de frecuencias súper altas (SHF, *Super High Frequency*), superiores a los 3 GHz. A partir de estas características se establecen dos frecuencias para el proceso de comunicación: una destinada a la portadora modulada de transmisión y otra a la portadora de recepción. Este esquema corresponde a una comunicación de tipo dúplex, en la cual las frecuencias de envío y recepción conforman el radiocanal.

LINEA DE VISTA

Según el artículo de la IEEE (Liu, Zhang, & Song, 2018) , la línea de vista (Line of Sight, LOS) describe un escenario de propagación en el que el transmisor y el receptor se encuentran unidos por un camino libre de obstáculos, lo que permite que la onda electromagnética se propague sin interferencias causadas por reflexiones, difracciones o dispersión del entorno. La existencia de línea de vista resulta un factor clave en los sistemas de comunicaciones inalámbricas, ya que tiene un impacto directo en el desempeño del enlace, las pérdidas de propagación y la exactitud de aplicaciones de posicionamiento y localización.

ANTENA

De acuerdo al libro “Antenna Theory” (Balanis, 2005) , una antena es un dispositivo que actúa como interfaz entre un sistema de transmisión guiada y el espacio libre, permitiendo convertir señales eléctricas en ondas

electromagnéticas que se propagan en el medio, y de manera inversa, captar ondas electromagnéticas para transformarlas nuevamente en señales eléctricas utilizables por los sistemas de comunicación. Este elemento es esencial en las redes inalámbricas y en los sistemas de transmisión de datos.

CONECTIVIDAD

Según la página web DevX (Staff, 2024) , la conectividad de red se refiere al proceso mediante el cual diversos dispositivos, sistemas o nodos se enlazan entre sí para permitir el intercambio fluido de datos e información. Esta conectividad puede establecerse tanto por medios cableados como inalámbricos (por ejemplo, cables Ethernet, Wi-Fi o redes celulares), y su propósito principal es garantizar que la comunicación y la transferencia de recursos entre los distintos componentes de la red se realicen de manera eficiente y confiable.

(Calderon, 2009), indica que la conectividad satelital se entiende como la capacidad de un sistema de comunicaciones para establecer y mantener enlaces de transmisión de datos mediante el uso de satélites artificiales, permitiendo la interconexión entre estaciones terrenas, usuarios finales y redes terrestres. Este tipo de conectividad resulta fundamental en escenarios donde la infraestructura física es limitada o inexistente, ya que el satélite actúa como un nodo intermedio que posibilita la comunicación a grandes distancias mediante enlaces ascendentes y descendentes.

DISPONIBILIDAD

Según la página web TechTarget (TechTarget, 2025) , la disponibilidad de red se refiere al grado en que una red o sistema de comunicaciones se mantiene operativo y accesible durante un período determinado de tiempo. Esta métrica expresa la capacidad de la infraestructura de red para ofrecer sus servicios de manera continua y confiable, y suele representarse como un porcentaje que indica el tiempo en que la red funciona correctamente en relación con el tiempo total evaluado. Una alta disponibilidad implica interrupciones mínimas

del servicio y es un indicador clave del desempeño y la confiabilidad de una red.

- **Fórmula de disponibilidad como indicador**

En ingeniería de redes y telecomunicaciones, la disponibilidad como indicador cuantitativo se expresa comúnmente en dos formas equivalentes:

$$\text{Disponibilidad (\%)} = \left(\frac{\text{Tiempo de operación}}{\text{Tiempo de operación} + \text{Tiempo de inactividad}} \right) \times 100$$

Esto mide qué fracción del tiempo total un sistema está operando.

LATENCIA

Según CETIS (CETIS, 2025), la latencia de red describe el retraso que ocurre en la comunicación entre dos puntos dentro de una red informática. Este término se refiere al tiempo que tardan los datos en desplazarse desde el origen hasta el destino a través de la red.

En redes con mayor latencia, los tiempos de respuesta son más lentos, mientras que una latencia baja se asocia con respuestas más rápidas y un mejor rendimiento. Mantener una latencia reducida es importante para optimizar la eficiencia y la experiencia de los sistemas y aplicaciones que dependen de la transmisión de datos en tiempo real.

SEGURIDAD

Según Fortinet (Fortinet, 2025), la seguridad de red es un conjunto integral de tecnologías, políticas, procedimientos y personas, diseñados para proteger la infraestructura de comunicaciones frente a ataques cibernéticos, accesos no autorizados y pérdida de datos.

Esto abarca no solo la red en sí, sino también el tráfico y los activos accesibles desde la red, tanto en su borde como dentro de su perímetro, con el objetivo de salvaguardar la confidencialidad, integridad y disponibilidad de la información, garantizando una operación segura, continua y robusta ante amenazas.

❖ Cómo funciona la seguridad de red

La seguridad de red opera mediante la implementación de múltiples mecanismos defensivos que protegen la red en diferentes niveles. A medida que las organizaciones adoptan tecnologías digitales, la superficie de ataque se amplía, incluyendo redes locales, WAN, IoT y servicios en la nube, lo que crea nuevas vulnerabilidades. Los componentes de seguridad trabajan en conjunto para reducir los riesgos, proteger la privacidad de los datos, garantizar la continuidad del negocio y preservar el rendimiento de la red al impedir que actores maliciosos interrumpen su funcionamiento.

❖ Tipos de soluciones de seguridad de red

Fortinet describe varias categorías de soluciones que fortalecen la protección de la red:

- Firewalls: Analizan y controlan el tráfico de red según políticas definidas para permitir o bloquear paquetes de datos.
- Sistemas de prevención de intrusiones (IPS): Detectan y bloquean amenazas antes de que comprometan la red.
- VPN de acceso remoto: Crean conexiones cifradas para permitir acceso seguro desde ubicaciones remotas.
- Control de acceso: Garantiza que solo dispositivos autorizados y conformes obtengan acceso.
- Otras soluciones, como herramientas de gestión de la superficie de ataque, que identifican activos y vulnerabilidades, y mecanismos avanzados como las VPN y soluciones para redes híbridas de seguridad integradas.

Así mismo, Paloalto (Networks, 2025), considera temas adicionales descritos por Fortinet enfatizando que la seguridad de red debe ser capaz de detectar comportamientos anómalos dentro de la infraestructura, lo que permite identificar actividades sospechosas que podrían no corresponder a ataques

tradicionales. Esta capacidad fortalece la postura de seguridad al anticipar y responder a amenazas emergentes.

Finalmente, Palo Alto Networks destaca como componentes esenciales de la seguridad las herramientas de monitoreo continuo y la gestión centralizada de políticas de seguridad. Estas permiten un control más preciso del tráfico, mayor visibilidad de la red y una administración unificada de las medidas de protección, lo que fortalece la continuidad operativa frente a amenazas internas y externas.

SEGURIDAD EN REDES SATELITALES

Según la RFC 4949 (Shirey, 2007), la seguridad en redes satelitales puede entenderse como el conjunto de medidas técnicas y organizativas destinadas a proteger los recursos de Internet que se transmiten a través de enlaces satelitales frente a accesos no autorizados, uso indebido, divulgación, interrupción, modificación o destrucción de la información, garantizando así la confidencialidad, integridad, autenticación y disponibilidad de los servicios de red.

3.5 Procedimiento

Para el diseño e implementación de la solución satelital Starlink, es necesaria la coordinación de actividades entre varias áreas involucradas en el proyecto, con el fin de garantizar que los requerimientos técnicos, operativos y comerciales se ejecuten de manera ordenada y conforme a los objetivos establecidos. A continuación, se visualiza el desarrollo de cada etapa del proyecto mediante el siguiente flujo:

El proyecto consiste en el desarrollo del diseño e implementación de una solución satelital Starlink, a través de las siguientes etapas:

- Etapa 1: Análisis del requerimiento
- Etapa 2: Diseño de la red
- Etapa 3: Implementación
- Etapa 4: Validación y puesta en marcha

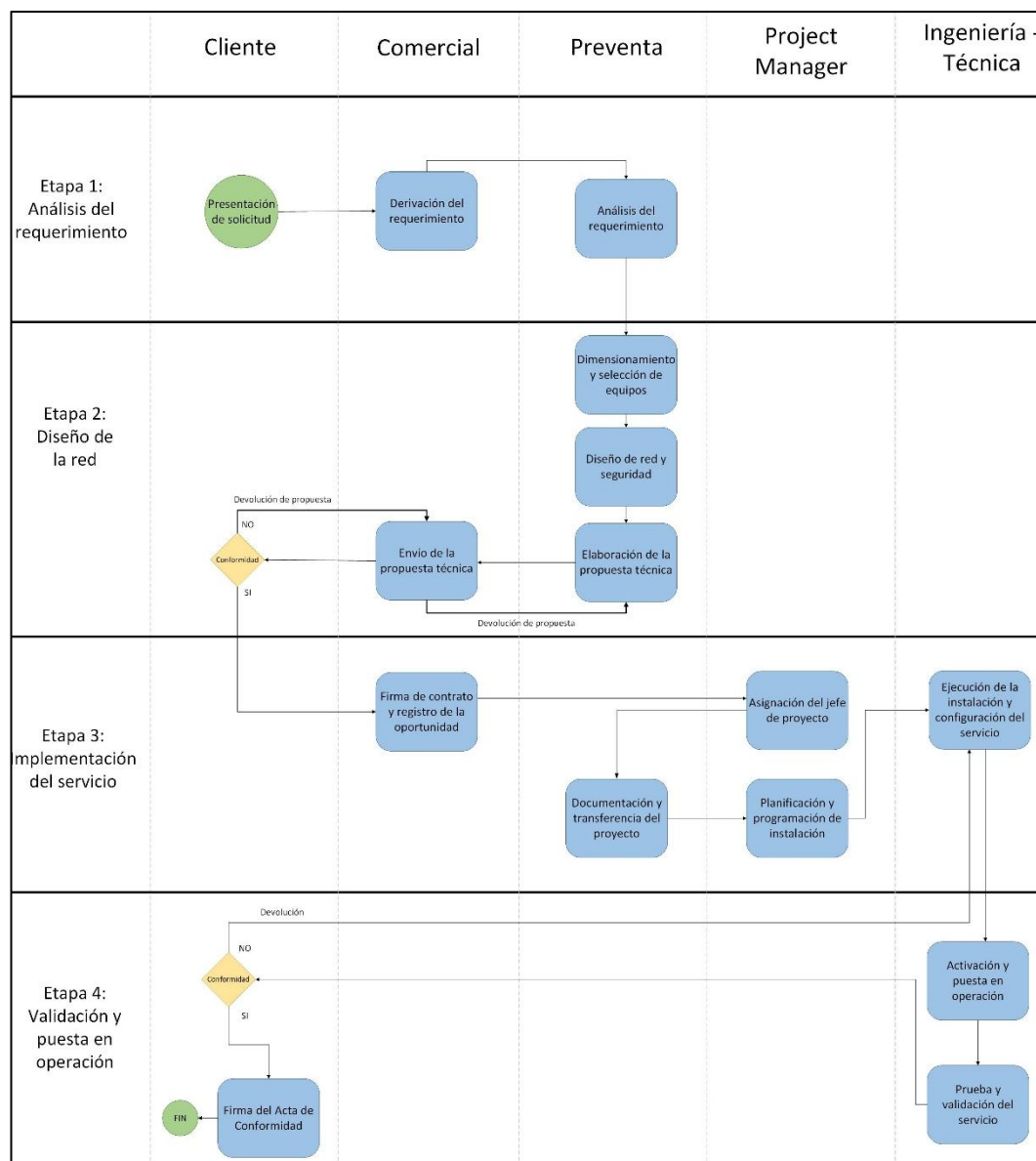


Figura 2 Flujograma de las etapas del procedimiento. Fuente: Elaboración propia a partir de los datos del área de Operaciones.

Nota: El Flujograma describe de manera ordenada y secuencial las etapas que conforman el procedimiento.

3.5.1 Etapa 1: Análisis del requerimiento

En esta etapa interviene el cliente, el área comercial y el área de preventa quienes coordinan para el adecuado levantamiento de información según el requerimiento del cliente. Las actividades desarrolladas en esta etapa son las siguientes:

- a) Presentación de la solicitud del cliente
- b) Derivación del requerimiento

- c) Análisis del requerimiento
- d) Análisis del nivel de seguridad

3.5.1.1 *Presentación de la solicitud del cliente*

La actividad inicia con la presentación de la solicitud por parte del cliente, la cual es canalizada a través del área comercial. En dicha solicitud, que incluye el documento denominado “Bases del concurso”, se expone la necesidad de contar con un servicio de conectividad que permita garantizar la continuidad del servicio considerando las características del entorno donde se requiere su implementación. Para ello, el cliente proporciona información de la ubicación geográfica de sus sedes y el nivel de criticidad del servicio para la continuidad de sus procesos.

Adicionalmente, el cliente detalla la problemática actual asociada a su servicio de conectividad y se identifica los aspectos que requieren mejora, tales como la capacidad de transmisión de datos requerida, los niveles de disponibilidad esperados y los parámetros de latencia requeridos para la conectividad solicitada. Esta información es importante para el análisis posterior del requerimiento, permitiendo establecer una evaluación de las necesidades del cliente.

En la tabla 2 se muestra las principales características técnicas del requerimiento solicitado por el cliente:

Tabla 2. Requerimiento del cliente.

Sede	Requerimiento del cliente			
	Cantidad de dispositivos	Ancho de banda mínimo	Medio de transmisión	Disponibilidad
Sede Abelardo	3	Internet simétrico de 5 Mbps	Fibra óptica aérea y/o subterránea canalizada, microondas o satelital (mínimo garantizado 70%)	98.3% para las sedes de provincia
Sede Napo	4	Internet simétrico de 5 Mbps	Fibra óptica aérea y/o subterránea canalizada, microondas o satelital (mínimo garantizado 70%)	98.3% para las sedes de provincia

Sede Echenique	4	Internet simétrico de 5 Mbps	Fibra óptica aérea y/o subterránea canalizada, microondas o satelital (mínimo garantizado 70%)	98.3% para las sedes de provincia
----------------	---	------------------------------------	--	---

Fuente. Elaboración propia a partir de las bases proporcionada por el cliente.

Nota: Se visualiza el requerimiento del cliente solicitado por cada sede ubicada en la zona rural de Loreto. Elaboración propia a partir de las bases proporcionada por el cliente.

3.5.1.2 Derivación del requerimiento

Una vez recibida la solicitud del cliente, el área comercial coordina y procede a la derivación del requerimiento al área de preventa, al equipo encargado de los pedidos del Estado, adjuntando la información recopilada durante la etapa inicial, como los datos generales del cliente, las características del sitio de implementación y los requerimientos del servicio solicitado. Esta derivación tiene como finalidad asegurar la correcta transferencia del requerimiento hacia el área responsable del análisis, permitiendo la continuidad del proceso de evaluación bajo un enfoque estructurado y ordenado.

3.5.1.3 Análisis del requerimiento

Tiene como propósito identificar y analizar la necesidad del cliente, la cual consiste en disponer de un servicio de acceso a internet confiable y de alta disponibilidad.

En esta actividad se presentan 4 subactividades:

- ❖ Análisis del medio de transmisión.
- ❖ Análisis del ancho de banda requerido.
- ❖ Análisis del rendimiento.
- ❖ Análisis del nivel de seguridad.

3.5.1.3.1 Análisis del medio de transmisión

Actualmente, el cliente cuenta con un servicio de internet satelital tradicional de alta latencia y baja velocidad, y necesita mejorar su servicio. Para atender esta solicitud, se realiza una evaluación técnica de la factibilidad de los principales medios de transmisión (fibra óptica, radioenlace y satelital), de acuerdo a la ubicación geográfica del cliente.

❖ Factibilidad mediante fibra óptica

Primero, se evalúa la factibilidad de implementar el servicio de acceso a internet mediante fibra óptica, dado que este medio de transmisión se caracteriza por ofrecer alta estabilidad, baja latencia y elevados niveles de disponibilidad. No obstante, es necesario considerar que, de las 36 sedes del cliente, 3 sedes se encuentran ubicadas en la región Loreto, que es una zona geográfica de difícil acceso, las cuales presentan limitaciones en infraestructura de telecomunicaciones.

- Sede Abelardo:

La sede Abelardo se encuentra ubicada en el centro poblado San Juan Bautista, Iquitos, Maynas Loreto; a una distancia aproximada de 94.8Km desde el nodo de la red de ON Empresas, siendo necesario esta cantidad de metraje de tendido de fibra óptica. En la Figura 3, se ilustra el recorrido de la fibra óptica desde el nodo hasta la sede del cliente.

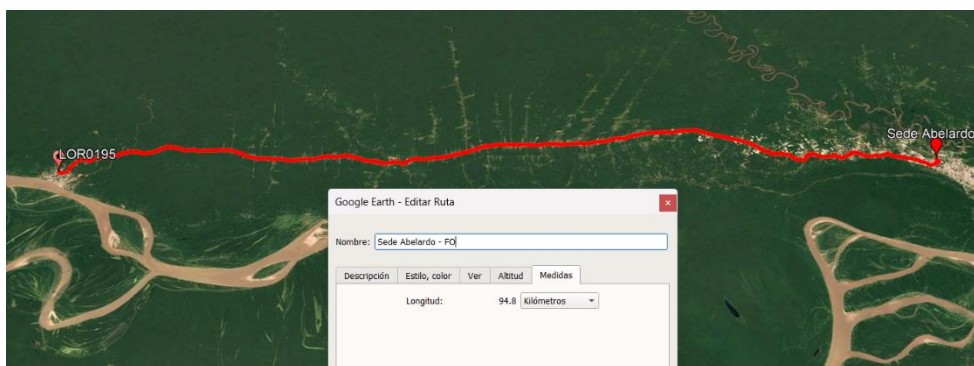


Figura 3 Recorrido del tendido de fibra óptica para la sede Abelardo. Fuente: Elaboración propia a partir de los datos proporcionados por Ingeniería Técnica y el cliente.

Nota: Representación del recorrido del tendido de la fibra óptica.

- Sede Napo:

La sede Napo se encuentra ubicada en el centro poblado 16002, Iquitos, Maynas Loreto; a una distancia aproximada de 103Km desde el nodo de la red de ON Empresas, siendo necesario esta cantidad de metraje de tendido de fibra óptica. En la Figura 4, se ilustra el recorrido de la fibra óptica desde el nodo hasta la sede del cliente.

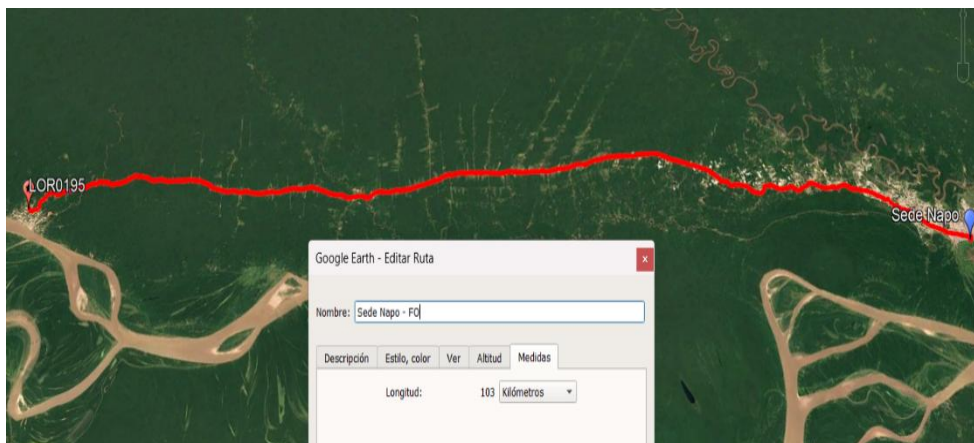


Figura 4 Recorrido del tendido de la fibra óptica para la sede Napo. Fuente: Elaboración propia a partir de los datos proporcionados por Ingeniería Técnica y el cliente.

Nota: Representación del recorrido del tendido de la fibra óptica.

- Sede Echenique:

La sede Echenique se encuentra ubicada en Iquitos, Maynas Loreto; a una distancia aproximada de 103Km desde el nodo de la red de ON Empresas, siendo necesario esta cantidad de metraje de tendido de fibra óptica. En la Figura 5, se ilustra el recorrido de la fibra óptica desde el nodo hasta la sede del cliente.

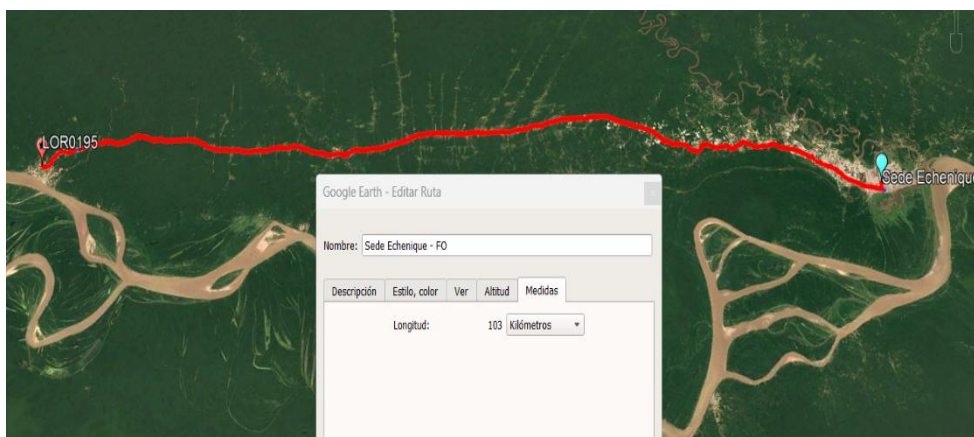


Figura 5 Recorrido del tendido de fibra óptica para la sede Abelardo. Fuente: Elaboración propia a partir de los datos proporcionados por Ingeniería Técnica y el cliente.

Nota: Representación del recorrido del tendido de la fibra óptica.

De acuerdo al análisis de las 3 sedes, se tiene los siguientes costos estimados de implementación, considerando los materiales, servicios y recursos necesarios para su ejecución:

Tabla 3. Costos por sede y total mediante el medio de transmisión de fibra óptica

Item	Material o servicio	Costos en Sede:		
		Abelardo	Napo	Echenique
1	Fibra óptica	\$40,764.00	\$44,290.00	\$44,290.00
2	Suspensores, muffa, cruceta,	\$38,750.00	\$42,102.00	\$42,102.00
3	Mano de obra del tendido	\$80,580.00	\$87,550.00	\$87,550.00
Total por sede		\$160,094.00	\$173,942.00	\$173,942.00
Total		\$507,978.00		

Fuente. Elaboración propia a partir de los datos proporcionados por Ingeniería Técnica.

Nota: Se visualiza el costo por sede orientado al tendido de fibra óptica.

Resultado:

La ubicación geográfica, la distancia del nodo hacia las sedes y la limitada cobertura de redes de fibra óptica en dichas zonas hacen que el despliegue de este medio de transmisión no resulte económicamente viable.

Por tanto, se descarta la fibra óptica como alternativa de conectividad para las sedes evaluadas, procediéndose a analizar otros medios de transmisión que se ajusten a las condiciones geográficas y operativas del entorno más económicas.

❖ Factibilidad mediante radioenlace

Se evalúa la factibilidad de implementar el servicio de acceso a internet mediante radioenlace, como una alternativa inalámbrica al tendido de fibra óptica.

Esta tecnología requiere la existencia de línea de vista directa entre los puntos de transmisión y recepción, así como condiciones climáticas favorables para garantizar la estabilidad y disponibilidad del enlace.

- Sede Abelardo:

La sede Abelardo se encuentra ubicada en el centro poblado San Juan Bautista, Iquitos, Maynas Loreto a una distancia aproximada de 86.6 Km desde el nodo de la red de ON Empresas.

En la Figura 6, se visualiza que no hay línea de vista desde el nodo hasta la sede del cliente.



Figura 6 Recorrido del radioenlace para la sede Abelardo. Fuente: Elaboración propia a partir de los datos proporcionados por Ingeniería Técnica y el cliente.

Nota: Representación del recorrido del radioenlace, donde se observa la ausencia de línea de vista. Fuente: Elaboración propia a partir de los datos proporcionados por Ingeniería Técnica y el cliente.

- Sede Napo:

La sede Napo se encuentra ubicada en el centro poblado 16002, Iquitos, Maynas Loreto a una distancia aproximada de 92.8 Km desde el nodo de la red de ON Empresas. En la Figura 7, se visualiza que no hay línea de vista desde el nodo hasta la sede del cliente.

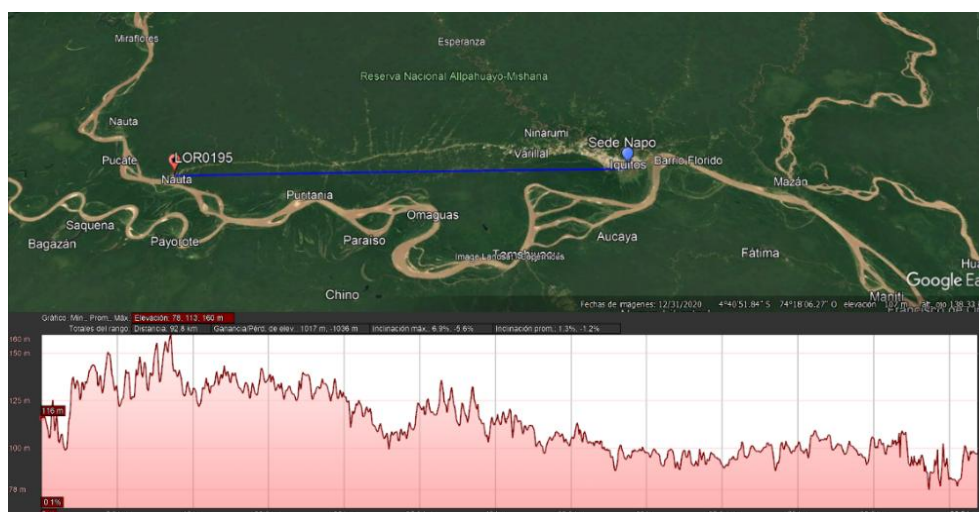


Figura 7 Recorrido del radioenlace para la sede Napo. Fuente: Elaboración propia a partir de los datos proporcionados por Ingeniería Técnica y el cliente.

Nota: Representación del recorrido del radioenlace, donde se observa la ausencia de línea de vista.

- Sede Echenique:

La sede Echenique se encuentra ubicada en Iquitos, Maynas Loreto a una distancia aproximada de 103 Km desde el nodo de la red de ON Empresas. En la Figura 8, se visualiza que no hay línea de vista desde el nodo hasta la sede del cliente.

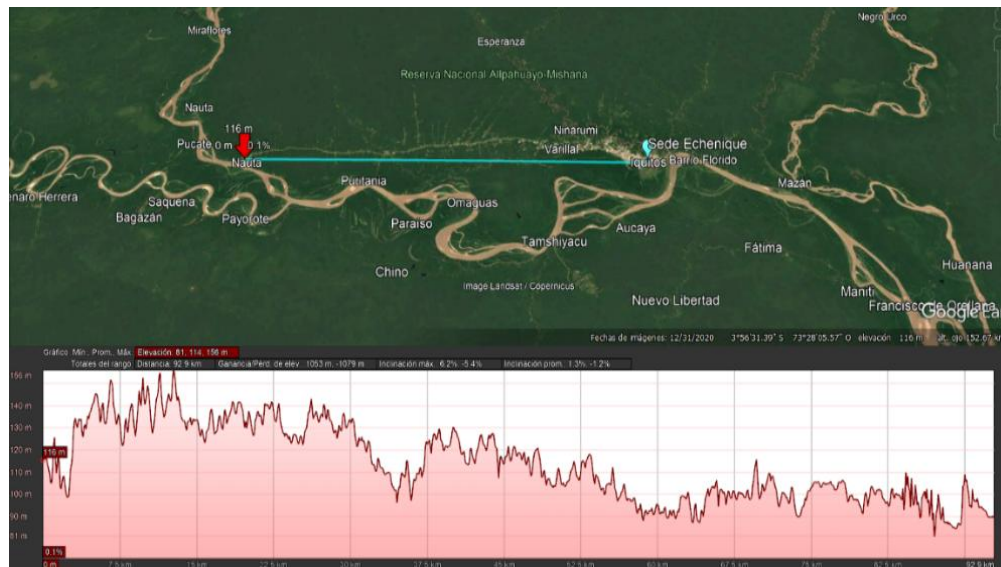


Figura 8 Recorrido de fibra óptica para la sede Echenique. Fuente: Elaboración propia a partir de los datos proporcionados por Ingeniería Técnica y el cliente.

Nota: Representación del recorrido del radioenlace, donde se observa la ausencia de línea de vista.

Resultado:

La alternativa de radioenlace es descartada al no cumplir con el requisito de línea de vista (LOS) entre los puntos de transmisión (nodo) y recepción (sedes), que es condición indispensable para garantizar la estabilidad y el desempeño del enlace.

❖ Factibilidad mediante satelital

Se evalúa la factibilidad de implementar el servicio de acceso a internet mediante tecnología satelital, considerando una alternativa a las soluciones de fibra óptica y radioenlace. La instalación requiere una ubicación con visión despejada al cielo para asegurar la estabilidad y disponibilidad del servicio, minimizando interferencias y optimizando el desempeño de la conectividad.

- Sede Abelardo

En la Figura 9 se visualiza que la sede Abelardo tiene una visión despejada al cielo, requisito fundamental para garantizar la factibilidad de la instalación del servicio satelital.



Figura 9 Visibilidad al cielo para la sede Abelardo. Fuente: Elaboración propia a partir de los datos del cliente.

Nota: Representación de la visibilidad al cielo para la implementación del servicio satelital.

- Sede Napo:

En la Figura 10 se visualiza que la sede Napo tiene una visión despejada al cielo, requisito fundamental para garantizar la factibilidad de la instalación del servicio satelital.

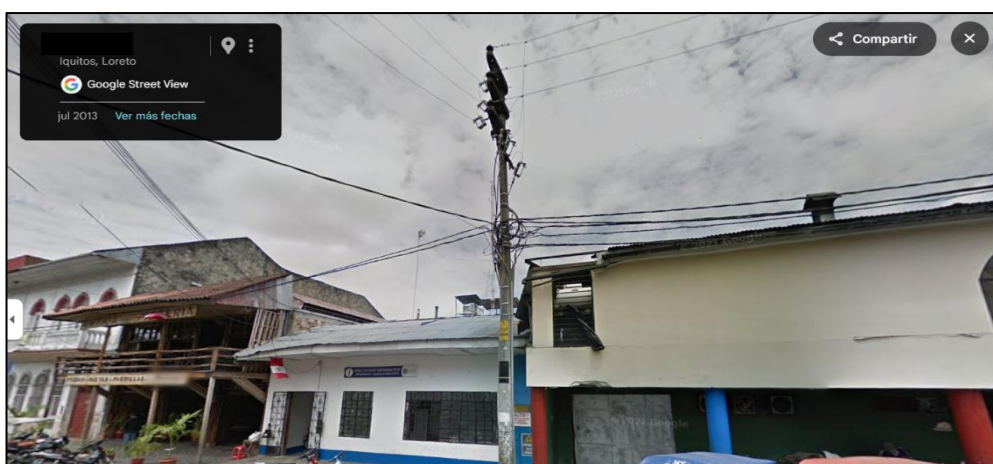


Figura 10 Visibilidad al cielo para la sede Napo. Fuente: Elaboración propia a partir de los datos del cliente.

Nota: Representación de la visibilidad al cielo para la implementación del servicio satelital. Fuente: Elaboración propia a partir de los datos del cliente.

- Sede Echenique:

En la Figura 11 se visualiza que la sede Echenique tiene una visión despejada al cielo, requisito fundamental para garantizar la factibilidad de la instalación del servicio satelital.

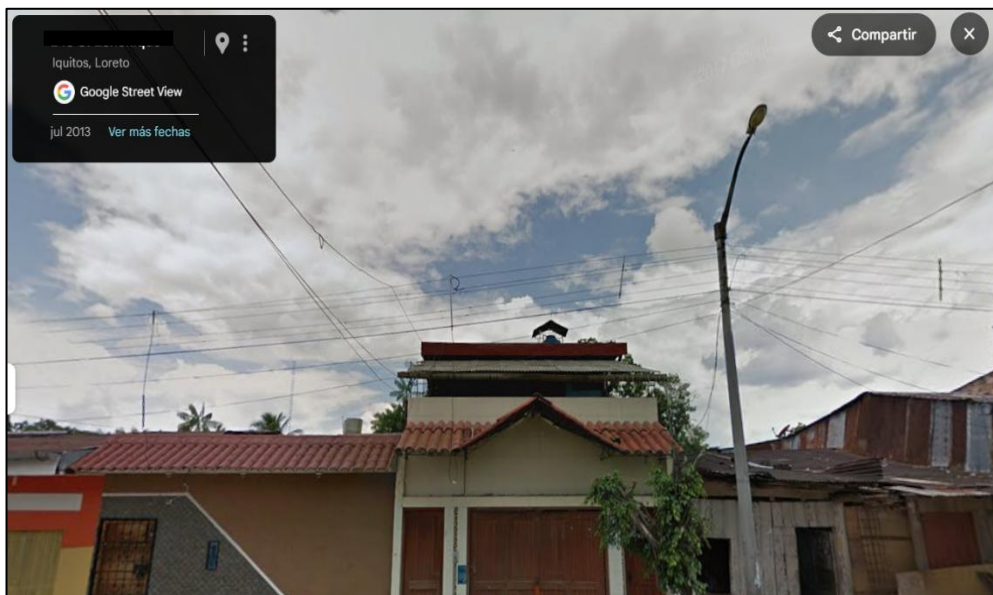


Figura 11 Visibilidad al cielo para la sede Echenique. Fuente: Elaboración propia a partir de los datos del cliente.

Nota: Representación de la visibilidad al cielo para la implementación del servicio satelital.

De acuerdo al análisis de las 3 sedes, se tiene los siguientes costos estimados de implementación:

Tabla 4 Costos por sede y total mediante el medio de transmisión satelital.

Item	Material o servicio	Costos en Sede:		
		Abelardo	Napo	Echenique
1	Kit Satelital	\$2,150.00	\$2,150.00	\$2,150.00
3	Activación del kit	\$20.00	\$20.00	\$20.00
4	Instalación y configuración del kit satelital	\$1,050.00	\$1,050.00	\$1,050.00
5	Router	\$120.00	\$120.00	\$120.00
Total por sede		\$3,340.00	\$3,340.00	\$3,340.00
Total		\$10,020.00		

Fuente. Elaboración propia a partir de los datos proporcionados por Ingeniería Técnica.

Nota: Se visualiza el costo por sede orientado a la implementación de un servicio satelital.

Resultado:

De acuerdo al análisis realizado mediante el medio de transmisión satelital resulta viable la atención de la solicitud del cliente debido a que en los 3 casos se tiene visión despejado al cielo.

A continuación, en la tabla 5, se muestra la comparación de los 3 medios de transmisión evaluados:

Tabla 5 Costos por sede mediante el medio de transmisión fibra óptica

Medio de transmisión	Ventajas	Desventajas	Evaluación según el caso analizado
Fibra óptica	-Alta estabilidad y confiabilidad del servicio. -Alta velocidad de transmisión. -Alta disponibilidad cuando existe infraestructura.	-Costos de implementación elevados. -Requiere tendido físico extenso de fibra óptica. -Dependencia de infraestructura existente. -Mayor despliegue en zonas de difícil acceso geográfico.	No viable económicamente. Las sedes se encuentran a distancias superiores a 90 km del nodo de red y en zonas con limitada cobertura de fibra óptica, lo que incrementa significativamente los costos de materiales y mano de obra
Radioenlace	-No requiere tendido físico de cableado. -Implementación relativamente rápida.	-Requiere estrictamente línea de vista (LOS). -Sensible a condiciones climáticas. -Limitaciones de estabilidad en largas distancias.	No viable técnicamente. Las sedes evaluadas no cumplen con el requisito de línea de vista directa entre el nodo y los puntos de recepción, condición indispensable para este tipo de tecnología.
Satelital	-Independiente de la infraestructura terrestre. -Cobertura en zonas rurales y de difícil acceso. -Implementación rápida. -No requiere línea de vista terrestre, solo visión despejada al cielo.	-Latencia mayor frente a fibra óptica. -Velocidad menor en tecnologías satelitales tradicionales.	Es el medio de transmisión más viable y recomendado. Las sedes evaluadas cuentan con visión despejada al cielo, cumpliendo el requisito fundamental para la instalación del servicio satelital, lo que permite atender la necesidad del cliente de forma viable.

Fuente. Elaboración propia a partir de los datos proporcionados por Ingeniería Técnica

Nota: Dado la evaluación comparativa de los medios de transmisión disponibles, se determina que la solución más adecuada es la implementación de un servicio de Internet satelital.

El análisis realizado evidencia que la implementación de un servicio mediante fibra óptica no resulta viable debido a la gran extensión de tendido requerida y al elevado costo de inversión asociado. Asimismo, la alternativa de

radioenlace es descartada al no cumplir con el requisito de línea de vista, condición indispensable para garantizar la estabilidad y el adecuado desempeño del enlace. Se decide por la implementación del servicio por satélite por el menor costo y la facilidad de implementación.

3.5.1.3.2 Análisis del ancho de banda requerido

Esta actividad tiene como propósito identificar y analizar la necesidad de ancho de banda del cliente. Actualmente, en la zona de Loreto, la entidad tiene un servicio de internet satelital tradicional, sin embargo, requiere mejorar la conectividad garantizando un internet estable y continuo para los colaboradores de cada sede.

Dado que la solución propuesta se basa en el medio de transmisión satelital, de acuerdo al análisis del punto anterior, se debe determinar el ancho de banda necesario en función al número de colaboradores por sede.

Para calcular el ancho de banda requerido en cada sede, se debe considerar los siguientes parámetros:

- Consumo mínimo por PC: El consumo mínimo es de 1Mbps, considerando para trabajos de oficina como navegación web, plataformas y correo electrónico.
- Consumo mínimo por videoconferencia (Teams, zoom): El consumo mínimo es de 1Mbps, considerando para reuniones virtuales.
- Consumo mínimo para video por PC: El consumo mínimo es de 4Mbps, para aplicaciones como streaming de video (Netflix) o subida de archivos grandes.

❖ Ancho de banda para la sede Abelardo

La sede Abelardo cuenta con 3 colaboradores. Para este caso, las PCs realizan trabajo de oficina, lo cual se puede dimensionar de la siguiente manera:

$$\text{Ancho de banda} = (\#PCs) \times (\text{consumo por PC})$$

$$\text{Ancho de banda} = (3) \times (1 \text{ Mbps} + 1 \text{ Mbps})$$

$$\text{Ancho de banda} = 6 \text{ Mbps}$$

❖ Ancho de banda para la sede Napo

La sede Napo cuenta con 4 colaboradores. Para este caso, las PCs realizan trabajo de oficina, lo cual se puede dimensionar de la siguiente manera:

$$\text{Ancho de banda} = (\#PCs) \times (\text{consumo por PC})$$

$$\text{Ancho de banda} = (4) \times (1 \text{ Mbps} + 1 \text{ Mbps})$$

$$\text{Ancho de banda} = 8 \text{ Mbps}$$

❖ Ancho de banda para la sede Echenique

La sede Echenique cuenta con 4 colaboradores. Para este caso, las PCs realizan trabajo de oficina, lo cual se puede dimensionar de la siguiente manera:

$$\text{Ancho de banda} = (\#PCs) \times (\text{consumo por PC})$$

$$\text{Ancho de banda} = (4) \times (1 \text{ Mbps} + 1 \text{ Mbps})$$

$$\text{Ancho de banda} = 8 \text{ Mbps}$$

Luego del análisis de las 3 sedes, se concluye que el ancho de banda mínimo requerido es de 8 Mbps (subida y bajada), que se elige de la sede con mayor necesidad de ancho de banda (sede Abelardo). Este ancho de banda asegura que las actividades de oficina como la navegación web, gestión de correos electrónicos y el uso de aplicaciones corporativas se puedan realizar de manera eficiente. También garantiza la estabilidad del servicio de internet, cumpliendo con los requisitos y favoreciendo el correcto desempeño de las tareas asignadas a cada colaborador.

3.5.1.3.3 Análisis del rendimiento

Esta actividad tiene como propósito identificar y analizar la necesidad de rendimiento del servicio solicitado. Para ello, se evaluará el nivel de latencia y disponibilidad del servicio propuesto. Actualmente, la entidad dispone de un servicio de internet satelital tradicional (VSAT) con una disponibilidad del 97.8% de acuerdo con el último requerimiento solicitado por la entidad.

Se realiza una comparativa, con el fin de identificar las ventajas y desventajas del servicio actual frente al servicio propuesto.

❖ Característica del servicio

En la tabla 6, se realiza una comparativa entre el servicio actual y el servicio propuesto, permitiendo evidenciar las limitaciones y las mejoras del servicio propuesto.

Tabla 6 Características del servicio actual y el servicio propuesto

Características	Internet Satelital VSAT (GEO) - Actual	Internet Satelital Starlink (LEO) - Propuesto
Latencia	Alta (500-700ms)	Baja (20-60ms)
Cobertura	Ubicación específica	Global
Interferencia atmosférica	Menor	Menor
Disponibilidad de satélites	Fijo (dependiendo de ubicación GEO)	Mayor (constelación)
Órbita de los satélites	Órbita GEO (35,786 Km)	Órbita LEO (1,500 Km)
Conectividad y señal	Satélites fijos, en el mismo punto de la órbita	Satélites en movimiento constante
Tamaño de la antena	Grande (antena parabólica)	Pequeña
Velocidad de instalación	Media	Baja
Ancho de banda	Dedicado, según requerimiento	Variable: Subida: 8 – 25 Mbps Bajada: 40 – 220 Mbps
Disponibilidad del servicio	97.8%	98.3%
Costo del servicio para 5 Mbps	Instalación: \$4,800.00 Mensual: \$3,250.00	Instalación: \$3,340.00 Mensual: \$1,110.00

Fuente. Elaboración propia a partir de los datos proporcionados por Ingeniería Técnica.

Nota: La tabla representa las características del servicio actual y del servicio propuesto, evidenciando las mejoras obtenidas.

De la comparación se puede evidenciar que la latencia y disponibilidad son mucho más favorables con la solución satelital Starlink. También importante que esta tecnología tiene cobertura global (incluso en movimiento) y utiliza antenas más pequeñas.

Respecto a los costos asociados a la solución de internet satelital, se evidencia que Starlink representa una alternativa económicamente más eficiente en comparación con la tecnología VSAT.

En términos de costos de instalación, Starlink presenta una reducción aproximada del 30.42% respecto a VSAT, mientras que en el costo mensual del servicio la diferencia es aún más significativa, siendo Starlink aproximadamente 66.85% más económico. Estos resultados reflejan una mejor optimización considerable en los costos de implementación y operación del servicio de conectividad para el cliente.

Esto coincide con los resultados del análisis según (Abdelraheem A, 2025), que concluye que starlink ofrece menores niveles de latencia y un mayor ancho de banda, y que los costos de inversión y operación son menores para esta tecnología.

❖ Disponibilidad

Actualmente, la entidad tiene una disponibilidad del servicio de internet satelital VSAT del 97.8%. Se propone un servicio con mayor disponibilidad asegurando un servicio eficiente y brindando mejoras.

- Servicio actual

La disponibilidad del servicio actual se calcula de la siguiente manera:

$$\text{Disponibilidad (\%)} = \left(\frac{\text{Tiempo de operación}}{\text{Tiempo de operación} + \text{Tiempo de inactividad}} \right) \times 100$$

$$\text{Disponibilidad (\%)} = \left(\frac{720}{720+16} \right) \times 100$$

$$\text{Disponibilidad (\%)} = \left(\frac{720}{736} \right) \times 100$$

$$\text{Disponibilidad (\%)} = (0.978260) \times 100$$

$$\text{Disponibilidad (\%)} = 97.8 \%$$

$$\text{Tiempo de indisponibilidad} = 16 \text{ horas al mes}$$

- Servicio propuesto

Para el servicio propuesto, La disponibilidad se calcula de la siguiente manera:

$$\text{Disponibilidad (\%)} = \left(\frac{\text{Tiempo de operación}}{\text{Tiempo de operación} + \text{Tiempo de inactividad}} \right) \times 100$$

$$\text{Disponibilidad (\%)} = \left(\frac{720}{720+12.45} \right) \times 100$$

$$\text{Disponibilidad (\%)} = \left(\frac{720}{732} \right) \times 100$$

$$\text{Disponibilidad (\%)} = (0.9830) \times 100$$

$$\text{Disponibilidad (\%)} = 98.30 \%$$

$$\text{Tiempo de indisponibilidad} = 12.45 \text{ horas al mes}$$

Del análisis realizado, sobre la disponibilidad mínima que ofrece cada tecnología, se identifica que para una disponibilidad del 97.8% el máximo

tiempo de inactividad será de 16 horas al mes y para una disponibilidad de 98.3% el máximo tiempo de inactividad será de 12.45 horas al mes.

No se tiene el dato de la disponibilidad del cliente usando VSAT, pero sí usando Starlink, con lo cual se puede determinar si se está cumpliendo con la disponibilidad propuesta.

3.5.1.3.4 Análisis del nivel de seguridad

Esta actividad tiene como propósito identificar y analizar la necesidad del cliente basado en el nivel de seguridad. Actualmente, la entidad no cuenta con una solución de seguridad que proteja el tráfico de navegación de sus colaboradores, lo que expone su red a posibles amenazas y riesgos informáticos. Se propone la implementación de seguridad en la navegación permitiendo a los colaboradores navegar de forma segura, controlada y confiable. La solución propuesta brinda una conexión segura y privada mediante una VPN IPSec, respaldada por la infraestructura de seguridad en nube de Palo Alto Networks, la cual se encuentra ubicada en el DataCenter de ON EMPRESAS. La solución cuenta con las siguientes características:

- Habilitación de una instancia virtual de seguridad en nube: Dedicada exclusivamente para la entidad.
- Firewall virtual de última generación: Integra funciones de red y seguridad sobre una infraestructura escalable y diseñada en un entorno cloud.
- Creación de perfiles de seguridad: Filtros web (*Web Filtering*), control de aplicaciones e IPS con protección antivirus.
- Prevención de amenazas (*Threat Prevention*): Permite bloquear vulnerabilidades de acceso (*exploits*) y software malicioso (*malware*), reduciendo ataques cibernéticos.
- Gestión de seguridad de red: Proporciona visibilidad del tráfico y administración a través de una consola gestionada por ON EMPRESAS.
- Asignación de una IP pública fija de ON EMPRESAS: Permite una navegación a internet segura y controlada mediante la infraestructura de seguridad cloud.

La solución propuesta con Starlink representa una mejora significativa en el perfil de seguridad en comparación con un servicio VSAT sin mecanismos de protección implementados.

Esta solución permite al cliente navegar de manera segura, ya que incorpora mecanismos avanzados de seguridad para la gestión del tráfico y la navegación en internet, fortaleciendo la protección de la red de la entidad. Asimismo, contribuye a la mitigación de amenazas de malware y a la reducción del riesgo de ataques frente a posibles incidentes de seguridad informática.

3.5.2 Etapa 2: Diseño de la red

En esta etapa interviene el cliente, el área comercial y el área de preventa quienes coordinan para el adecuado diseño de la red según la información y análisis del requerimiento. Las actividades desarrolladas en esta etapa son las siguientes:

- a) Dimensionamiento y selección de equipos
- b) Diseño de red y seguridad
- c) Elaboración de la propuesta técnica
- d) Envío de la propuesta técnica

3.5.2.1 Dimensionamiento y selección de equipos

Tiene como propósito el dimensionamiento y la selección del equipamiento en función de la tecnología ya definida en la “Etapa 1: Análisis del requerimiento”, de cual se definió a Starlink como la tecnología más adecuada para los requisitos y ubicación del cliente.

Se procede al dimensionamiento y selección del equipamiento necesario de acuerdo con la tecnología Starlink, considerando los siguientes equipamientos:

- ❖ Equipamiento router
- ❖ Equipamiento de antena satelital
- ❖ Equipamiento de seguridad en nube

3.5.2.1.1 Equipamiento router

Capacidad de tráfico:

Para realizar el dimensionamiento del equipamiento router se considera las velocidades máximas ofrecidas por el servicio satelital Starlink:

- Velocidad de subida: 8 – 25 Mbps
- Velocidad de bajada: 40 – 220 Mbps

En consecuencia, el router seleccionado debe ser capaz de manejar un tráfico mínimo de hasta 220 Mbps.

Configuración de VPN y conectividad en la nube:

Así mismo, se requiere realizar la configuración de una VPN del tipo site to site utilizando el protocolo IPsec, con el fin de garantizar la confidencialidad, integridad y autenticación de la información. Esta configuración es necesaria tanto para la interconexión con la infraestructura de seguridad en nube como para la gestión del equipamiento. El router debe soportar esta configuración de manera eficiente y sin inconvenientes.

Confiabilidad empresarial:

Para servicios empresariales, el equipamiento router preferido es de la marca Cisco debido a su reconocida reputación y percepción de confianza por parte de los clientes. Cisco se considera una opción atractiva para organizaciones que priorizan la reducción del riesgo tecnológico y la protección de la información, lo cual se evidencia en el cuadro de Gartner.

De acuerdo con el Cuadrante Mágico de Gartner 2024 (Fortinet, We're a Leader: 2024 Magic Quadrant™ for Enterprise Wired and Wireless LAN Infrastructure by Gartner®, 2024) para infraestructura LAN empresarial cableada e inalámbrica, Cisco se posiciona dentro del cuadrante de líderes, lo que evidencia su alta capacidad de ejecución y una sólida visión estratégica en el mercado de redes empresariales. Esta ubicación respalda la confiabilidad consolidándola como una de las principales opciones para la implementación de infraestructuras de red en entornos corporativos en comparación con soluciones de marcas como MikroTik y H3C. Considerando todos los criterios evaluados se tiene la oferta de 3 tipos de router los cuales

se indica en la Figura 12. Se selecciona el router Cisco C1121-4P, el cual cumple con los 4 requisitos necesarios para el servicio.

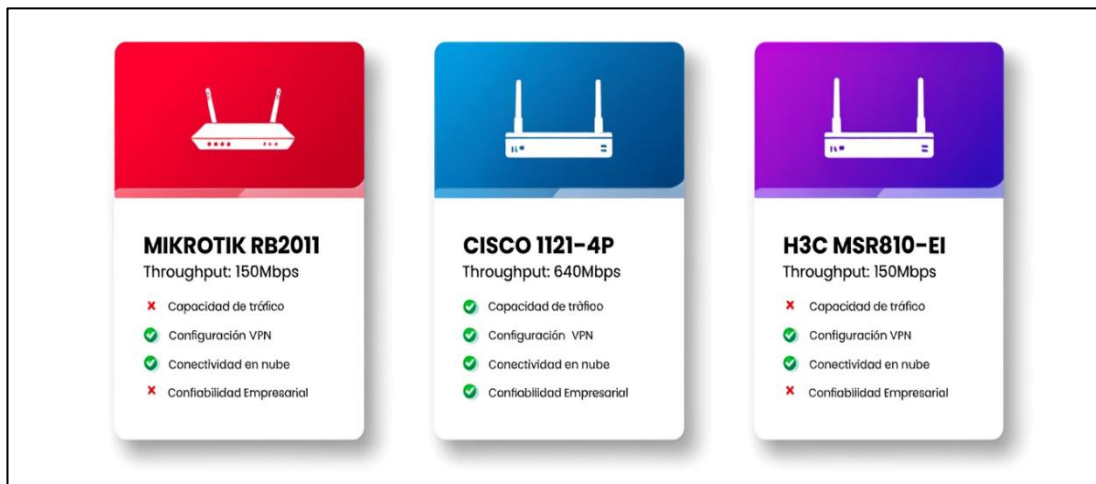


Figura 12 Evaluación del equipamiento router. Fuente: Elaboración propia a partir de los datos proporcionados por Ingeniería Técnica

Nota: Representación gráfica comparativa de las características principales de cada tipo de router.

3.5.2.1.2 Equipamiento de antena satelital

Se dimensiona una antena satelital adecuada para soportar tanto la cantidad de usuarios como las condiciones climáticas.

Para ello, Starlink ofrece distintos modelos de antenas según los requerimientos de los clientes. En la Tabla 7 se visualiza las principales características de cada modelo de antena.

Tabla 7. Características de las antenas que ofrece Starlink

Características	Antenas Starlink		
	Flat Hig Performance	Estandar Residencial	Mini
Tamaño del cable	Cable PoE de 25 metros	Cable PoE de 15 metros	Cable PoE de 15 metros
Latencia	20 – 60 ms	20 – 60 ms	40 – 90 ms
Clasificación ambiental	IP56 Tipo 4	IP54	IP67 Tipo 4
Campo de visión	140°	100°	110°
Consumo de energía	110 – 150 W	75 – 100 W	25 – 40 W
Usuarios	40	10	2

Fuente. Elaboración propia a partir de los datos proporcionados por Ingeniería Técnica.

Nota: La tabla representa las características de las antenas que se ofrece con la tecnología Starlink.

Considerando la ubicación geográfica en Loreto, se selecciona la antena Flat High Performance como la opción más adecuada. Esta elección se fundamenta en que, a pesar de que otros modelos como el Estandar Residencial y el Mini presentan ventajas específicas, la Flat High Performance ofrece un campo de visión más amplio de 140°, lo que favorece la estabilidad y cobertura de la señal en entornos con posibles obstáculos. Además, su clasificación ambiental IP56 Tipo 4 garantiza resistencia a las condiciones climáticas propias de la región amazónica.

Asimismo, la capacidad de usuarios permite cubrir holgadamente (40 usuarios) el requerimiento del cliente (3 a 4 usuarios), asegurando un servicio de alto desempeño para los usuarios previstos.

Por estas razones, la antena Flat High Performance se define como la opción más adecuada dentro de la oferta de Starlink, que cumple los requisitos necesarios para atender al cliente, tal como se puede identificar en la Figura 13.



Figura 13 Características de las antenas satelitales Starlink. Fuente: Elaboración propia a partir de los datos proporcionados por Ingeniería Técnica.

Nota: Comparación de las características de las antenas Starlink, observándose que solo Flat High Performance ofrecer campo de visión de 140°.

3.5.2.1.3 Sistema de seguridad en la nube

Se dimensiona un sistema de seguridad en la nube, el cual se encuentra ubicado en el Data Center de ON EMPRESAS y se integra a la solución mediante una conexión de VPN IPsec permitiendo garantizar una navegación segura y confiable.

El sistema de seguridad en la nube se implementa con la instalación del software de seguridad Palo Alto en un servidor del Data Center de ON EMPRESAS, el cual debe contar como mínimo con las características técnicas que se indican en la Tabla 8 de acuerdo al requerimiento del software de seguridad Palo Alto.

Es importante considerar estas características mínimas con el fin de asegurar que el servidor pueda alojar y ejecutar el software de Palo Alto de manera óptima, sin afectar el desempeño del servicio. Cabe resaltar que la velocidad máxima del servicio de internet seguro que ofrece Starlink es de 220 Mbps por cada sede, cumpliendo adecuadamente con los requerimientos del cliente y el plan de servicio propuesto.

El software Palo Alto presenta 2 paquetes de servicio cumpliendo estas características, como se puede observar en la Tabla 8.

Tabla 8. Características del servicio: Servidor + Software de seguridad

Características	Software Palo Alto (por sede)	Software Palo Alto (por las 3 sedes)
vCPU	2	2
RAM	4.5 GB	6.5 GB
Storage	60 GB	60 GB
Ancho de banda	300 Mbps	800 Mbps
Costo de instalación y configuración del servicio de seguridad	\$1,666.00	\$2,266.00

Fuente. Elaboración propia a partir de los datos proporcionados por Ingeniería Técnica.

Nota: Se visualiza las características del servidor requerido por el software Palo Alto.

Realizando el análisis de las 2 opciones del servicio, indicados en la Tabla 8, que ofrece el software Palo Alto es más conveniente implementar un software que permita soportar de manera conjunta la capacidad requerida por las tres

sedes, ya que esta alternativa resulta más eficiente desde el punto de vista económico y optimiza el uso de recursos de la máquina virtual.

Asimismo, el software de Palo Alto presenta 2 opciones de servicio cuyas características se muestra en la Tabla 9, cada una con funcionalidades orientadas a fortalecer el nivel de seguridad de la conectividad y la navegación por internet.

Tabla 9. Características del software de seguridad Palo Alto

Características	Software Palo Alto VM: 300Mbps	Software Palo Alto VM:800Mbps
Número de usuarios	250	2,000
Threat Prevention – Throughput	1.5 GB	1.5 GB
Conexión por Segundo	3,000	15,000
Max Sesiones	25,000	100,000
VPN site-to-site	4	25
VPN site-to-client	200	500
Funcionalidades de seguridad	VM NFGW: NAT, Dynamic Routing, VPN, Web Filtering Threat prevention: Antivirus	VM NFGW: NAT, Dynamic Routing, VPN, Web Filtering Threat prevention: Antivirus

Fuente. Elaboración propia a partir de los datos proporcionados por Ingeniería Técnica.

Nota: Se muestran las características de las 2 opciones del software Palo Alto instalado en el servidor de ON EMPRESAS.

De acuerdo con la Tabla 9, el software Palo Alto VM:800Mbps, opción empaquetada para las 3 sedes, presenta características adecuadas para la solución propuesta:

- El ancho de banda soportado de 800 Mbps supera la velocidad máxima del servicio de internet seguro (220 Mbps por sede), garantizando que el procesamiento del tráfico no se convierta en un cuello de botella para la red.
- La capacidad de hasta 2,000 usuarios, en caso de que el cliente requiera incrementar su personal en las 3 sedes, no presentará ninguna limitación en términos de seguridad, garantizando la protección de la navegación.
- El throughput de Threat Prevention de 1.5 Gbps demuestra que el sistema puede ejecutar funciones de seguridad avanzadas, como antivirus y

prevención de amenazas, sin afectar significativamente el rendimiento del servicio.

- El soporte de hasta 100,000 sesiones simultáneas y 15,000 conexiones por segundo garantiza una operación estable incluso ante picos de tráfico.
- La capacidad de implementar VPNs de tipo Site-to-Site y Site-to-Client permite una comunicación segura, fortaleciendo la arquitectura de seguridad de la solución.
- Las funcionalidades integradas de Next-Generation Firewall (NGFW), tales como NAT, enrutamiento dinámico, filtrado web y prevención de amenazas, permiten centralizar la seguridad de la red en una sola plataforma.

En conjunto, estas características demuestran que el software Palo Alto cumple con los requerimientos técnicos y de seguridad de la solución propuesta.

3.5.2.2 Diseño de red y seguridad

Tiene como propósito desarrollar el diseño de la red y seguridad del cliente en función de los resultados de la actividad de “Dimensionamiento y selección de equipos”. Para ello, se diseña un tipo de topología de red que luego es replicada para cada sede del cliente.

El diseño de la topología de red considera los siguientes elementos:

- Los equipos de acceso en el lado del cliente
- El medio de transmisión
- El sistema de seguridad.
- El servicio de Internet

Los equipos de acceso en el lado del cliente

En cada sede del cliente se implementa el router Cisco 1121-4P, el cual permite realizar las configuraciones necesarias para la interconexión con el **sistema de seguridad** mediante la configuración Site-to-site.

Adicionalmente, se realiza la configuración Site-to-site correspondiente para la **gestión y monitoreo del equipamiento**, garantizando la correcta operación del servicio y el cumplimiento del soporte 24x7 establecido.

El medio de transmisión

El medio de transmisión considerado para cada sede es de tipo satelital. Tras el análisis de los requerimientos se determinó que la solución basada en antenas de Starlink resulta la alternativa más adecuada para la solución de internet en la provincia de Loreto.

Esta tecnología opera mediante satélites en órbita baja terrestre (LEO), lo que permite ofrecer menores niveles de latencia y un desempeño más estable en comparación con sistemas satelitales tradicionales.

El sistema de seguridad

Como valor añadido del servicio, se brinda una solución de seguridad que se integra directamente con la conectividad a Internet, brindando protección avanzada a la red del cliente. Esta solución está basada en tecnología de Palo Alto Networks, la cual ofrece funcionalidades orientadas a la protección, control y gestión del tráfico. Entre sus principales capacidades se incluyen la prevención y detección de amenazas, control de aplicaciones y filtrado de páginas web, la cual permite restringir el acceso a sitios no autorizados optimizando el uso del ancho de banda y la reducción de los riesgos de seguridad.

El servicio de Internet

El servicio brindado en cada sede es el Internet, este servicio es primordial para acceder a las plataformas corporativas y sistema en nube, facilitando el desempeño eficiente.

El servicio de Internet es esencial para la operatividad y productividad de los colaboradores de la empresa. Por ello, se brinda un servicio estable y confiable en cada una de las 3 sedes, todas ubicadas en la provincia de Loreto.

En la Figura 14 se presenta la topología de red y seguridad correspondiente a una sede del cliente considerando los 4 elementos descritos previamente. En esta topología el funcionamiento es el siguiente: La conectividad de Internet se realiza mediante la antena Starlink en el lado del cliente, la cual se enlaza a una constelación de satélites de baja órbita (LEO), permitiendo el

acceso a la red pública de Internet. Desde la antena Starlink, el tráfico IP es transmitido hacia el router Cisco, ubicado en la sede del cliente, el cual establece un túnel VPN Site-to-Site IPsec sobre Internet directamente hacia el Data Center de ON Empresas, garantizando la confidencialidad e integridad de la información transmitida.

En el Data Center de ON Empresas, el tráfico es recibido por una máquina virtual con el software Palo Alto instalado, la cual actúa como control de seguridad perimetral, donde se aplican políticas de filtrado, enrutamiento y control de acceso, permitiendo que las comunicaciones del cliente sean gestionadas de manera segura para el acceso hacia Internet.

La gestión, monitoreo y soporte del router Cisco se realizan a través de otra VPN hacia el concentrador de gestión outbound de ON Empresas, el cual permite la supervisión 24x7 y la atención de incidencias.

Topología de red y sistema de seguridad para cada sede

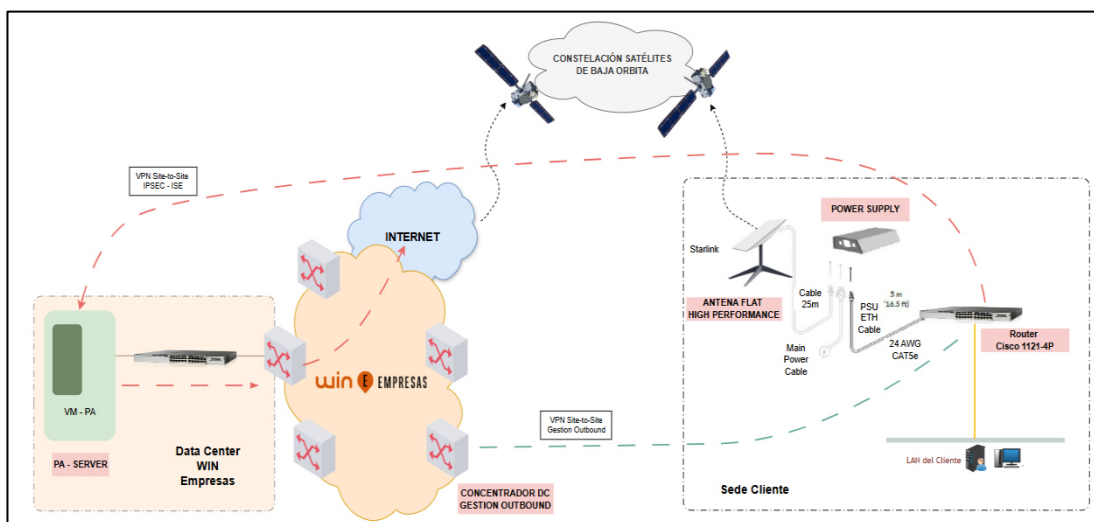


Figura 14 Topología de red y sistema de seguridad para cada sede.
Fuente: Elaboración propia a partir de los datos proporcionados por Ingeniería Técnica.

Nota: Esta topología es replicada para cada sede del cliente.

3.5.2.3 Elaboración de la propuesta técnica

Una vez definido el servicio, la tecnología y el equipamiento a implementar, se procede con la elaboración de la propuesta técnica en la cual se detalla el servicio diseñado de acuerdo con los requerimientos del cliente.

La propuesta técnica se estructura en tres secciones principales:

- ❖ En la primera sección se presenta a ON EMPRESAS como proveedor del servicio, describiendo sus características generales y las soluciones que ofrece como operador de telecomunicaciones.
- ❖ En la segunda sección se desarrolla la solución propuesta, la cual se encuentra diseñada de acuerdo con los requerimientos del cliente. En esta parte se detallan las funcionalidades del servicio, el plan ofertado, el equipamiento dimensionado, así como las consideraciones, exclusiones y condiciones asociadas a la prestación del servicio.
- ❖ En la tercera sección se describen las actividades del Centro de Atención de Ayuda (TAC), en donde incluye el flujo de atención y los canales de contacto establecidos para la gestión de incidencias, consultas o eventualidades relacionadas con el servicio.

3.5.2.4 Envío de la propuesta técnica

Realizado la propuesta técnica por el área de preventa, el área comercial deriva el documento al cliente para su evaluación correspondiente. Este documento es revisado por el área técnica y administrativa del cliente, con la finalidad de validar el alcance, las condiciones y la viabilidad de la solución propuesta. Tras culminar el proceso de revisión, se encuentra a la espera de la conformidad del cliente que permitirá dar inicio a la etapa de implementación.

En caso el cliente no otorgue su conformidad y formule observaciones a la propuesta técnica, el documento es derivado nuevamente al área de preventa con el fin de realizar las correcciones, ajustes técnicos y gestionar una nueva revisión y conformidad del cliente.

3.5.3 Etapa 3: Implementación del servicio

En esta etapa interviene el área comercial, el área preventa, el Project Manager y el área de Ingeniería, quienes coordinan para una adecuada implementación. Las actividades desarrolladas en esta etapa son las siguientes:

- a) Firma de contrato y registro de oportunidad.
- b) Asignación del Jefe de Proyecto.

- c) Documentación y transferencia del proyecto.
- d) Planificación y programación de la instalación.
- e) Ejecución de la instalación y configuración del servicio.

3.5.3.1 Firma de contrato y registro de la oportunidad

Esta actividad tiene como finalidad efectuar el registro de la información del cliente, los servicios a implementar, el equipamiento a utilizar y todo lo requerido para la instalación en cada una de las sedes. Este registro se efectúa una vez que el cliente ha otorgado su conformidad y se haya efectuado la firma del contrato.

El registro es el primer proceso para la recopilación de los datos del cliente, que permite la correcta gestión, seguimiento y soporte del servicio.

3.5.3.2 Asignación del jefe de Proyecto

Contando con la información del cliente y del servicio a implementar se procede a la asignación del jefe de proyecto.

El jefe de proyecto es el responsable de liderar la implementación de los servicios en cada sede, de coordinar y supervisar las actividades, asegurando el cumplimiento de los plazos de ejecución establecidos por el cliente.

Una de sus principales funciones es realizar las coordinaciones con el área Ingeniería-Técnica para las siguientes actividades:

- ✓ Programación y ejecución: Gestión de las visitas técnicas de cada sede del cliente para la instalación del equipamiento.
- ✓ Gestión de configuraciones: Gestionar las configuraciones de los equipos posterior a la instalación del equipamiento. Garantizando su correcto funcionamiento y desempeño con los requerimientos establecidos.

Así mismo, para una adecuada organización y seguimiento de las actividades, elabora un Plan de Trabajo.

3.5.3.3 Documentación y transferencia del proyecto

En esta actividad, el área de preventa realiza la consolidación y transferencia de la información correspondiente del cliente y los servicios a implementar al

jefe de proyecto. Esta documentación incluye los datos generales del cliente, el servicio, las sedes involucradas, el equipamiento a instalar y las consideraciones técnicas necesarias para la correcta implementación. Como resultado de esta actividad, el área de preventa elabora el documento denominado Acta de Conformidad del Proyecto (ACP), el cual formaliza la información del proyecto y constituye el documento base para el inicio de la instalación y configuración del servicio.

La información recopilada se transfiere mediante una reunión entre el área comercial, preventa y el jefe de proyecto, quedando registrada esta información en la plataforma Intranet de ON Empresas. Una vez realizada la transferencia, el jefe de proyecto asume la responsabilidad de revisar, validar y gestionar toda la documentación e información recibida. Posteriormente, el jefe de proyecto organiza y coordina la planificación y ejecución del servicio, garantizando que todos los requisitos técnicos sean correctamente aplicados.

3.5.3.4 Planificación y programación de instalación

Esta actividad, tiene como finalidad establecer la planificación y programación de la instalación del servicio para cada sede de acuerdo con los requerimientos solicitados por el cliente. Para ello, se elabora un documento denominado “Plan de Trabajo”, en el cual se detalla los plazos de ejecución y tareas que se desarrollarán de manera diaria durante el proceso de instalación.

El Plan de trabajo permite una coordinación eficiente y asegura el cumplimiento de los plazos establecidos. Así mismo, este documento brinda al cliente visibilidad sobre las labores a realizar en cada etapa y los tiempos estimados de ejecución.

Adicionalmente, se comunica al cliente el estado del avance del Plan de Trabajo, indicando la tarea en la que se encuentra el proceso de instalación, con la finalidad de mantenerlo informado y advertir oportunamente sobre posibles incidencias que puedan presentarse.

El Plan de Trabajo se encuentra detallado en el Anexo A1, el cual sirve para el seguimiento y monitoreo del proceso de instalación.

3.5.3.5 Ejecución de la instalación y configuración del servicio

Esta actividad tiene como propósito la instalación y configuración del servicio encargado por el Jefe de Proyecto.

Se realiza la coordinación y gestión de los permisos internos correspondientes en cada sede del cliente, con la finalidad de garantizar el acceso y la correcta ejecución de las actividades programadas. Asimismo, se efectúa el aprovisionamiento del equipamiento requerido para la implementación del Kit Satelital. Posteriormente, se lleva a cabo el traslado del equipamiento hacia cada sede del cliente, asegurando el proceso de instalación e implementación del servicio.

Siguiendo con las tareas descritas en el Plan de Trabajo, se procede a realizar las siguientes configuraciones:

- Configuración del equipo router
- Configuración de la máquina virtual
- Activación de la antena Satelital

3.5.3.5.1 Configuración del router

La configuración del router Cisco permite garantizar disponibilidad, seguridad y segmentación lógica del tráfico. Contempla los parámetros de administración segura, establecimiento de políticas y provisión de servicios de conectividad para la red LAN del cliente.

La configuración se divide en dos funcionalidades:

Gestión: Encargado de asegurar la administración remota del equipo mediante mecanismos de autenticación y cifrado.

Datos: responsable del encaminamiento del tráfico, traducción de direcciones (NAT) y asignación dinámica de parámetros de red (DHCP).

A continuación, se visualiza en la Tabla 10 los comandos para la configuración de equipamiento router.

Tabla 10. Configuración del router Cisco

N°	Configuración	Comandos principales	Funcionalidad	Objetivo
1	Activación de la licencia	license boot securityk9	Habilita funciones avanzadas de seguridad (IPSec)	Permitir la creación del túnel VPN de gestión
2	Configuración Básica del Sistema	hostname, clock timezone, no ip http server, service password-encryption	Parámetros iniciales del equipo	Identificación del router y fortalecimiento básico de seguridad
3	Seguridad de Acceso	crypto key generate rsa, ip ssh version 2, username, enable secret	Protección del acceso administrativo	Evitar accesos no autorizados
4	VPN IPSec de Gestión	crypto isakmp policy, crypto map, transform-set, keyring	Establece túnel cifrado hacia concentrador	Permitir gestión remota segura
5	Configuración de Interfaces	interface g0/0/0, loopback0, g0/0/1	Asignación de direcciones IP y roles (WAN/LAN/Gestión)	Separar tráfico de servicio y tráfico administrativo
6	AAA y TACACS+	aaa new-model, tacacs-server host, aaa authentication	Autenticación, autorización y auditoría centralizada	Control y registro de accesos administrativos
7	Listas de Control de Acceso (ACL)	ip access-list, access-list 25, SSH/Telnet, VPN	Filtrado de tráfico según origen/destino	Restringir accesos y definir tráfico cifrado
8	Monitoreo (IP SLA y SNMP)	ip sla, snmp-server community	Supervisión de disponibilidad y rendimiento	Detectar fallas y permitir monitoreo remoto
9	NAT	ip nat inside source list	Traducción de direcciones privadas a pública	Permitir salida a Internet de la red LAN
10	DHCP	ip dhcp pool, network, default-router	Asignación automática de IP a usuarios	Automatizar configuración de equipos cliente

Fuente. Elaboración propia a partir de los datos proporcionados por Ingeniería Técnica.

Nota: Se visualiza los comandos principales que se configura en cada router.

La configuración detallada se visualiza en el Anexo B1

3.5.3.5.2 Configuración de la máquina virtual

Primero se dispone de un servidor físico destinado a la creación de una máquina virtual que cumpla con los requisitos técnicos necesarios para el alojamiento e implementación del software de seguridad de Palo Alto, como se indicó en la Tabla 8. Luego, se procede con la instalación del software de seguridad dentro del entorno virtualizado.

Posteriormente, se realiza la configuración de los parámetros y funcionalidades principales de seguridad, orientadas a garantizar una navegación segura en internet para los usuarios finales. Así mismo, se

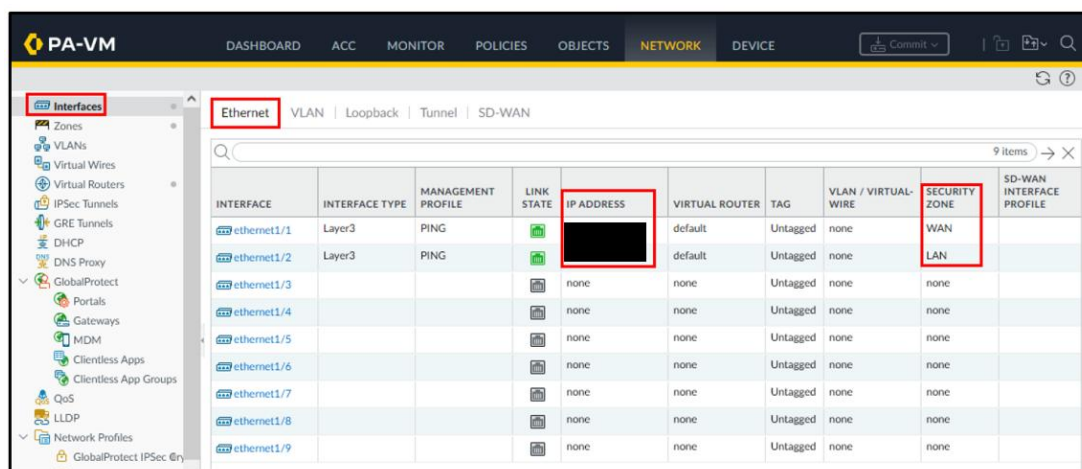
implementa los mecanismos de protección necesarios asegurando el adecuado control, monitoreo y filtrado del tráfico de red.

A continuación, se detalla la configuración de los parámetros y funcionalidades principales:

❖ Configuración de interfaces físicas

Ruta: Network >> Interfaces >> Ethernet

En la Figura 15 se muestra la configuración de las interfaces físicas Ethernet en el firewall PA-VM. Las interfaces ethernet1/1 y ethernet1/2 están configuradas como Layer 3, con direcciones IP asignadas y asociadas al virtual router default. Además, cada interfaz está vinculada a una zona de seguridad, donde ethernet1/1 corresponde a la WAN y ethernet1/2 a la LAN, permitiendo gestionar el tráfico entre la red externa e interna.



INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIRTUAL-WIRE	SECURITY ZONE	SD-WAN INTERFACE PROFILE
ethernet1/1	Layer3	PING		[Redacted]	default	Untagged	none	WAN	
ethernet1/2	Layer3	PING		[Redacted]	default	Untagged	none	LAN	
ethernet1/3				none	none	Untagged	none	none	
ethernet1/4				none	none	Untagged	none	none	
ethernet1/5				none	none	Untagged	none	none	
ethernet1/6				none	none	Untagged	none	none	
ethernet1/7				none	none	Untagged	none	none	
ethernet1/8				none	none	Untagged	none	none	
ethernet1/9				none	none	Untagged	none	none	

Figura 15 Configuración de las interfaces físicas de red. Fuente: Elaboración propia a partir de los datos proporcionados por Ingeniería Técnica.

Nota: Se configura las interfaces de red WAN y LAN en el software de seguridad de Palo Alto.

❖ Configuración de interfaces lógicas de Loopback

Ruta: Network >> Interfaces >> Loopback

En la Figura 16 se muestra la configuración de la interfaz lógica loopback donde se asigna una dirección IP y se habilita el perfil de gestión. Una

loopback es una interfaz virtual que se configura para identificación del equipo, servicios de red y pruebas de conectividad.

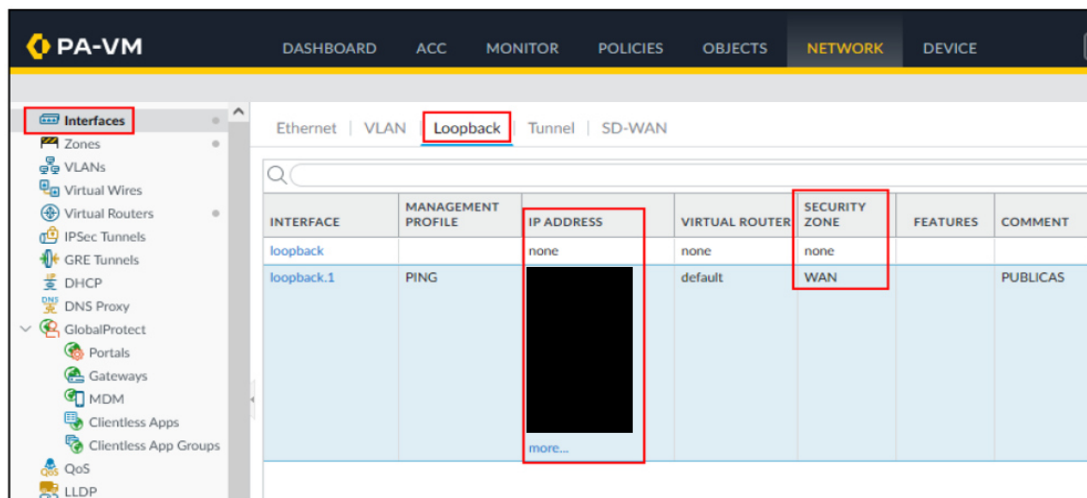


Figura 16 Configuración de las interfaces lógicas de loopback. Fuente: Elaboración propia a partir de los datos proporcionados por Ingeniería Técnica.

Nota: Se realiza la configuración de las loopback en el software de seguridad de Palo Alto.

❖ Configuración de interfaces lógicas de red

Ruta: Network >> Virtual Routes >> default

En la Figura 17 se muestra la configuración de rutas estáticas. Se ha definido varias rutas estáticas, la ruta por defecto y rutas específicas hacia las redes RED-LAN-A, RED-LAN-B y RED-LAN-C, indicando para cada una el destino y la dirección IP del siguiente salto (Next Hop). Esta configuración permite que el firewall determine por dónde debe enviar el tráfico hacia diferentes redes, facilitando el enrutamiento entre la red interna y otras redes conectadas.

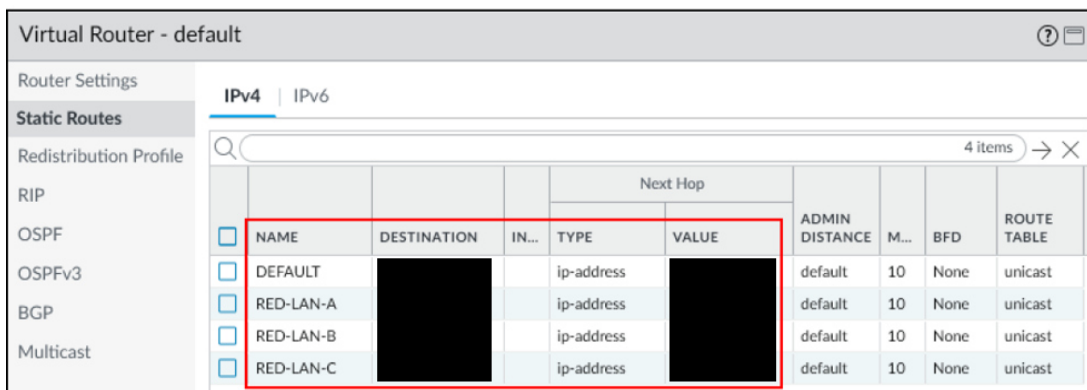


Figura 17 Configuración de las interfaces lógicas de red. Fuente: Elaboración propia a partir de los datos proporcionados por Ingeniería Técnica.

Nota: Se realiza la configuración de las interfaces lógicas de la red LAN en el software de seguridad de Palo Alto.

❖ Creación de objetos para redes internas

Ruta: Objects >> Address

En la Figura 18 se muestra la creación de objetos de direcciones en el firewall PA-VM. Se define varios objetos de tipo IP Netmask, donde se asigna un nombre identificador y una dirección IP o red específica correspondiente a las redes internas. Estos objetos permiten organizar y referenciar fácilmente las direcciones dentro de las políticas de seguridad, reglas de NAT o configuraciones de red, facilitando la administración y gestión del tráfico dentro del firewall.

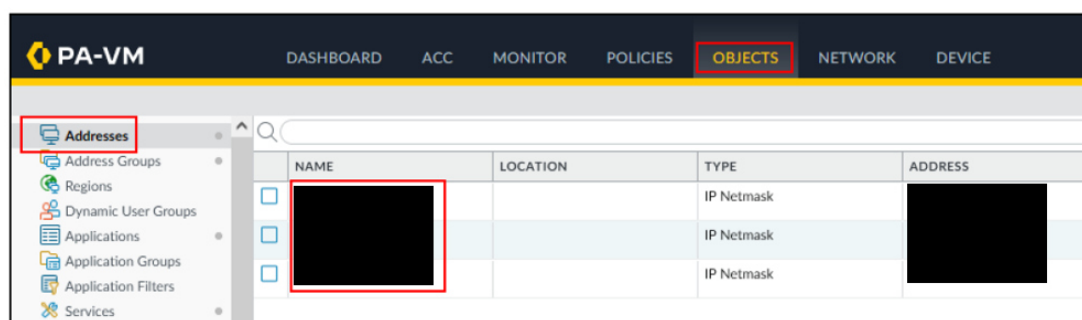


Figura 18 Configuración de objetos de las redes internas. Fuente: Elaboración propia a partir de los datos proporcionados por Ingeniería Técnica.

Nota: Se configura los objetos de la red interna. La configuración se realiza en el software de Palo Alto.

❖ Creación de grupo de objetos de redes internas

Ruta: Objects >> Address Groups

En la Figura 19 se muestra la creación de un grupo de direcciones en el firewall PA-VM. En esta configuración se define el grupo LAN-SUBNETS, el cual agrupa tres objetos de direcciones previamente creados que representan subredes de la red interna. La creación de este grupo permite organizar varias redes bajo un solo objeto lógico, facilitando su uso en políticas de seguridad, reglas de NAT o configuraciones de red, facilitando la administración y gestión del firewall.

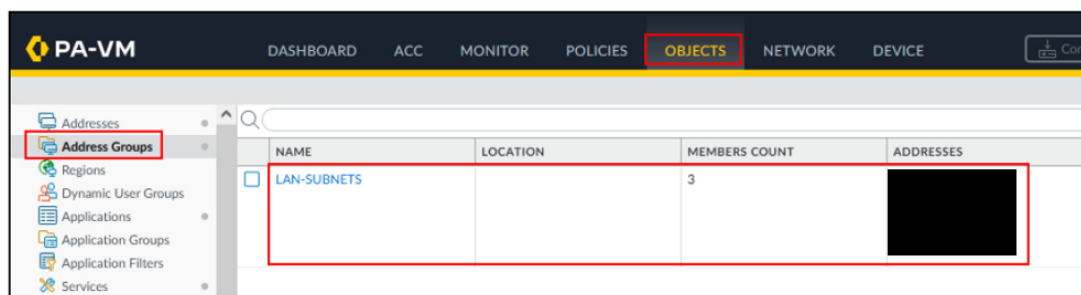


Figura 19 Configuración de grupo de objetos. Fuente: Elaboración propia a partir de los datos proporcionados por Ingeniería Técnica.

Nota: Se configura grupo de objetos en la que se encuentran los segmentos de la red privada. La configuración se realiza en el software de Palo Alto.

- ❖ Creación de perfil de antivirus para protección de malware sobre http, smtp, pop3, imap, ftp, smb.

Ruta: Objects >> Security Profiles >> Antivirus

En la Figura 20 se muestra la creación de un perfil de seguridad Antivirus en el firewall PA-VM. Se crea el perfil ANTIVIRUS, el cual permite inspeccionar y bloquear archivos maliciosos o malware que puedan transmitirse a través de distintos protocolos de red como HTTP, SMTP, POP3, IMAP, FTP y SMB. Alerta ante la detección de amenazas, contribuyendo a la protección del tráfico y la prevención de infecciones por malware dentro de la red.

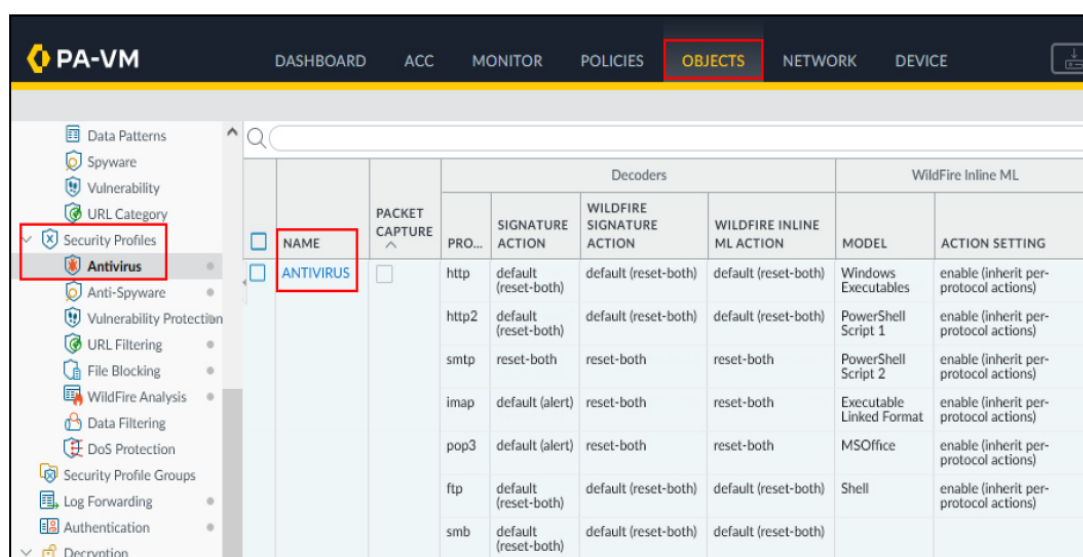


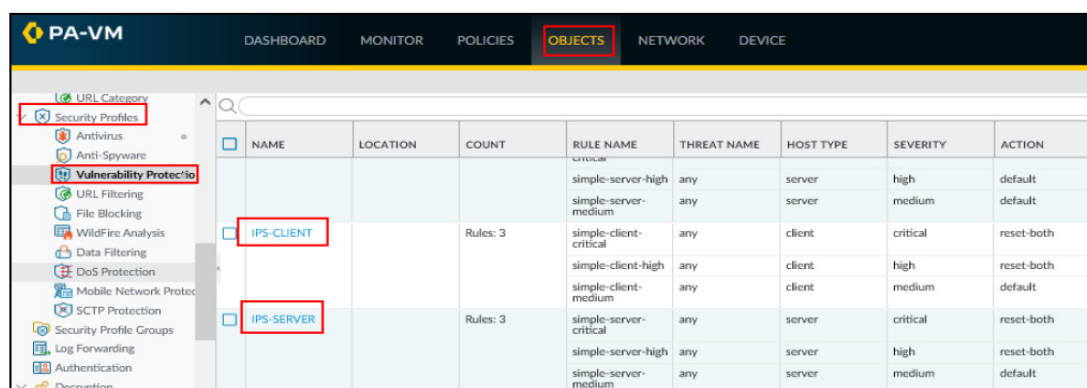
Figura 20 Configuración de seguridad: Antivirus. Fuente: Elaboración propia a partir de los datos proporcionados por Ingeniería Técnica

Nota: Se configura la funcionalidad de antivirus para la seguridad en la navegación. La configuración se realiza en el software de Palo Alto

- ❖ Creación de perfil de vulnerability protection (IPS) para protección de amenazas para clientes y servidores

Ruta: Objects >> Security Profiles >> Vulnerability Protection

En la Figura 21 se muestra la creación de perfiles de protección contra vulnerabilidades (IPS) en el firewall PA-VM. Se define dos perfiles: IPS-CLIENT y IPS-SERVER, cada uno con reglas orientadas a proteger respectivamente a clientes y servidores frente a intentos de explotación de vulnerabilidades. Estos perfiles analizan el tráfico y generan alertas cuando se detectan amenazas clasificadas por niveles de severidad (crítica, alta o media), permitiendo así prevenir ataques y fortalecer la seguridad de la red.



NAME	LOCATION	COUNT	RULE NAME	THREAT NAME	HOST TYPE	SEVERITY	ACTION
IPS-CLIENT		Rules: 3	simple-server-high	any	server	high	default
			simple-server-medium	any	server	medium	default
			simple-client-critical	any	client	critical	reset-both
IPS-SERVER		Rules: 3	simple-client-critical	any	client	critical	reset-both
			simple-client-high	any	client	high	reset-both
			simple-client-medium	any	client	medium	default
			simple-server-critical	any	server	critical	reset-both
			simple-server-high	any	server	high	reset-both
			simple-server-medium	any	server	medium	default

Figura 21 Configuración de seguridad: Protección de vulnerabilidades.
Fuente: Elaboración propia a partir de los datos proporcionados por Ingeniería Técnica.

Nota: Se configura la funcionalidad de protección de vulnerabilidades para la seguridad en la navegación. La configuración se realiza en el software de Palo Alto.

- ❖ Creación de perfil URL Filtering, para bloqueo de categorías maliciosas y de alto riesgo.

Ruta: Objects >> Security Profiles >> URL Filtering

En la Figura 22 se muestra la creación del perfil de seguridad URL Filtering en el firewall PA-VM. Se crea el perfil WEBFILTER, el cual permite controlar y filtrar el acceso a sitios web según categorías, bloqueando aquellas consideradas maliciosas o de alto riesgo. Este perfil permite alertar o bloquear

categorías específicas, reduciendo riesgos de malware, phishing o acceso a contenido no seguro dentro de la red.

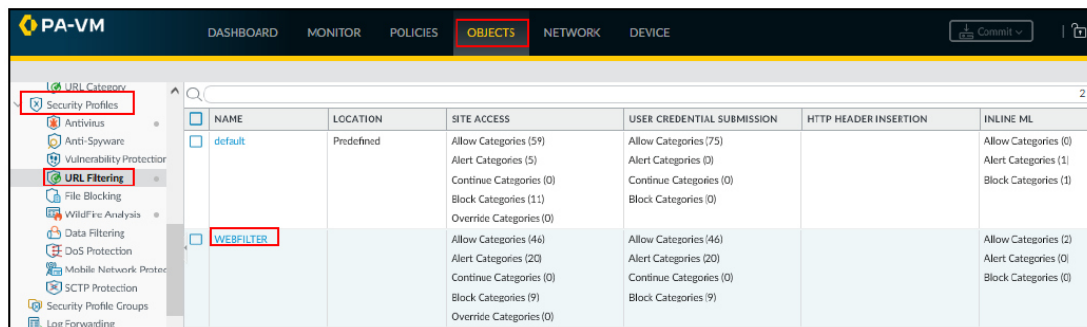


Figura 22 Configuración de seguridad: Filtrado web. Fuente: Elaboración propia a partir de los datos proporcionados por Ingeniería Técnica

Nota: Se configura la funcionalidad de filtrado web para la seguridad en la navegación. La configuración se realiza en el software de Palo Alto.

Categorías bloqueadas: abused-drugs, adult, command-and-control, extremism, grayware, high-risk, malware, phishing, ransomware.

- ❖ Creación de perfil de Wildfire para envío de archivos sospechosos para análisis de sandboxing y actualización de firmas.

Ruta: Objects >> Security Profiles >> Wildfire Analysis

En la Figura 23 se muestra la creación del perfil de seguridad WildFire Analysis en el firewall PA-VM. Se crea el perfil WILDFIRE, el cual permite enviar archivos sospechosos detectados en el tráfico de red hacia el servicio de análisis en sandbox de WildFire. Este proceso analiza el comportamiento de los archivos para identificar posibles amenazas desconocidas o malware, y posteriormente actualiza automáticamente las firmas de seguridad, fortaleciendo la protección de la red frente a nuevas amenazas.

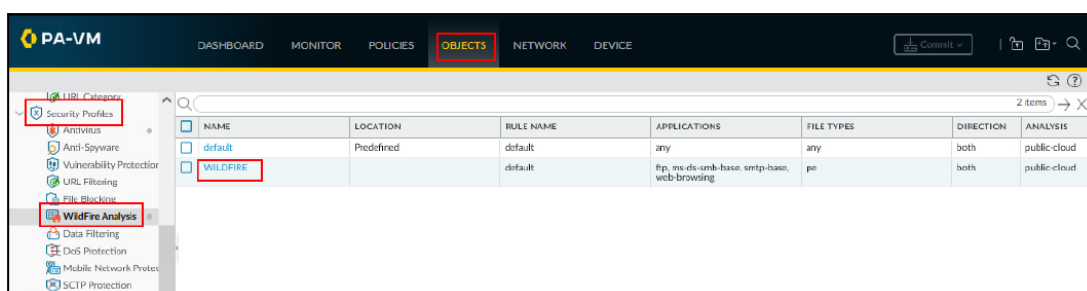


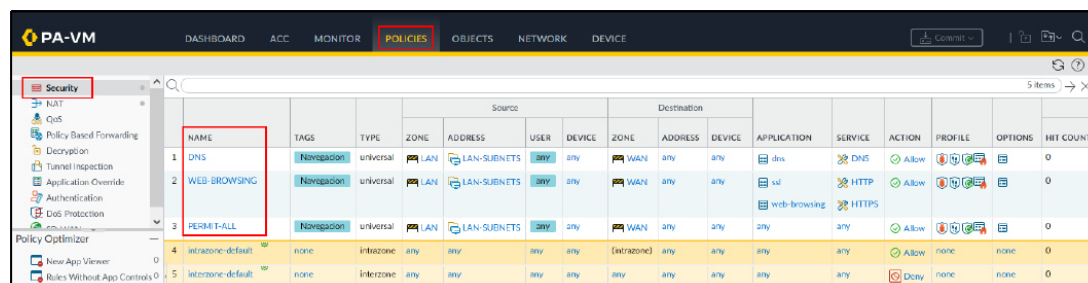
Figura 23 Configuración de seguridad: Wildfire Analysis. Fuente: Elaboración propia a partir de los datos proporcionados por Ingeniería Técnica.

Nota: Se configura la funcionalidad de wildfire analysis para la seguridad en la navegación. La configuración se realiza en el software de Palo Alto.

- ❖ Creación de políticas de acceso para DNS, Navegación Web y tráfico general. Las políticas cuentan con perfiles de protección de amenazas básicas de los servicios de Antivirus, Advanced URL Filtering, Threat Prevention y Wildfire

Ruta: Políticas >> Security

En la Figura 24 se muestra la configuración de políticas de seguridad en el firewall PA-VM. Se crean reglas de acceso para DNS, navegación web (HTTP/HTTPS) y tráfico general, permitiendo la comunicación desde la zona LAN hacia la zona WAN. Cada política aplica perfiles de seguridad como Antivirus, Advanced URL Filtering, Threat Prevention y WildFire, los cuales inspeccionan el tráfico para detectar malware, bloquear sitios maliciosos, prevenir ataques de vulnerabilidades y analizar archivos sospechosos, fortaleciendo así la protección de la red frente a amenazas externas.



NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS	HIT COUNT
1 DNS	Navegacion	universal	LAN	LAN-SUBNETS	any	any	WAN	any	any	dns	DNS	Allow	Antivirus, URL Filtering, Threat Prevention, Wildfire		0
2 WEB BROWSING	Navegacion	universal	LAN	LAN-SUBNETS	any	any	WAN	any	any	web-browsing	HTTP, HTTPS	Allow	Antivirus, URL Filtering, Threat Prevention, Wildfire		0
3 PERMIT-ALL	Navegacion	universal	LAN	LAN-SUBNETS	any	any	WAN	any	any	any	any	Allow	Antivirus, URL Filtering, Threat Prevention, Wildfire		0
4 intrazone-default		none	intrazone	any	any	any	intrazone	any	any	any	any	Allow	none	none	0
5 interzone-default		none	interzone	any	any	any	any	any	any	any	any	Deny	none	none	0

Figura 24 Configuración de las políticas de acceso. Fuente: Elaboración propia a partir de los datos proporcionados por Ingeniería Técnica.

Nota: Se configura la funcionalidad de políticas de acceso para la seguridad en la navegación. La configuración se realiza en el software de Palo Alto.

- ❖ Creación de regla de SNAT (overload) para permitir el acceso de las redes internas a internet usando la primera IP Publica disponible del pool asignado.

Ruta: Políticas >> NAT

En la Figura 25 se muestra la configuración de una regla de NAT de tipo SNAT (overload) en el firewall PA-VM. La regla SNAT-LAN permite que el tráfico

proveniente de las redes internas (LAN-SUBNETS) con destino a Internet (zona WAN) sea traducido mediante Source NAT dinámico, utilizando la primera dirección IP pública disponible del pool asignado. Esta configuración permite que múltiples dispositivos de la red interna compartan una misma IP pública para acceder a Internet, optimizando el uso de direcciones públicas y manteniendo la conectividad externa de la red.

PA-VM

DASHBOARDACCMONITORPOLICIESOBJECTSNETWORKDEVICE

Commit

Security

NAT

QoS

Policy Based Forwarding

Decryption

Tunnel Inspection

Application Override

Authentication

DoS Protection

Figura 25 Configuración de la regla SNAT. Fuente: Elaboración propia a partir de los datos proporcionados por Ingeniería Técnica.

Nota: Se realiza la configuración de SNAT para permitir accesos a las redes internas. La configuración se realiza en el software de Palo Alto.

3.5.3.5.3 Activación de la antena Satelital

El procedimiento de instalación comprende una fase física y una fase lógica de activación.

El kit satelital se encuentra conformado por los siguientes componentes: antena satelital, montaje, *Power Supply*, Modem AP, cables de interconexión y cables de energía. Estos componentes se muestran en la Figura 26.

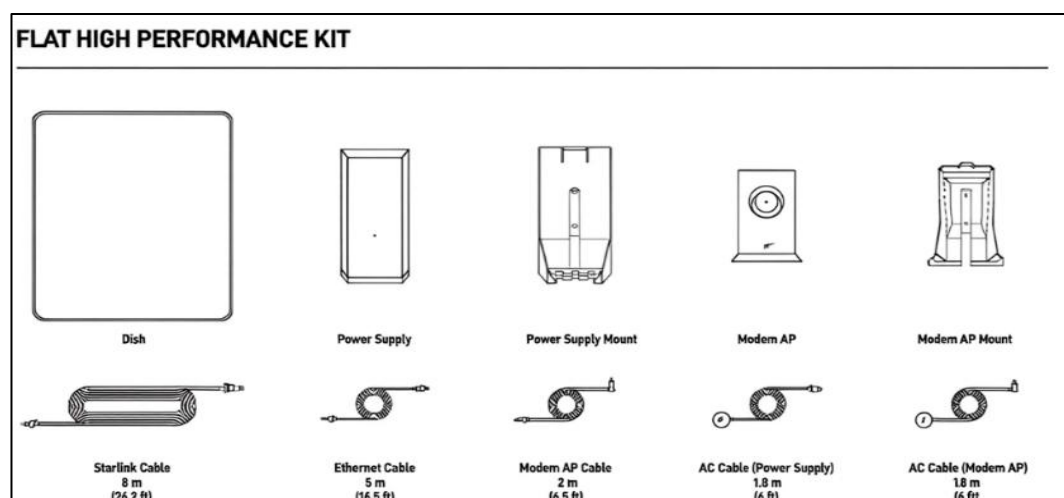


Figura 26 Componentes del Kit Satelital. Fuente: Starlink

Nota: Se visualiza los componentes correspondientes al kit satelital.

Posteriormente, la antena satelital debe instalarse firmemente en su base y colocarse en una zona elevada, estable y completamente despejada, garantizando una vista directa del cielo sin interferencias de árboles, edificios u otras estructuras que puedan generar obstrucciones en la línea de visión hacia los satélites. En la Figura 27 se muestra la antena satelital instalada en cada una de las sedes del cliente.



Figura 27 Instalación de la antena satelital. Fuente: Elaboración propia a partir de los datos proporcionados por Ingeniería Técnica.

Nota: Se visualiza cielo despejado para la instalación de la antena satelital en las 3 sedes.

Una vez definida la ubicación, se procede con la conexión física: el cable principal de 8 metros debe conectarse desde la antena satelital hasta el Power Supply, asegurando que el conector quede correctamente insertado y sin forzar el puerto.

Luego, el *Power Supply* se energiza mediante su cable AC correspondiente; posteriormente, se conecta el cable AC de 1.8 metros hacia el Modem AP, el cual también debe energizarse para completar la cadena de alimentación eléctrica. Esta conexión física se muestra en la Figura 28.

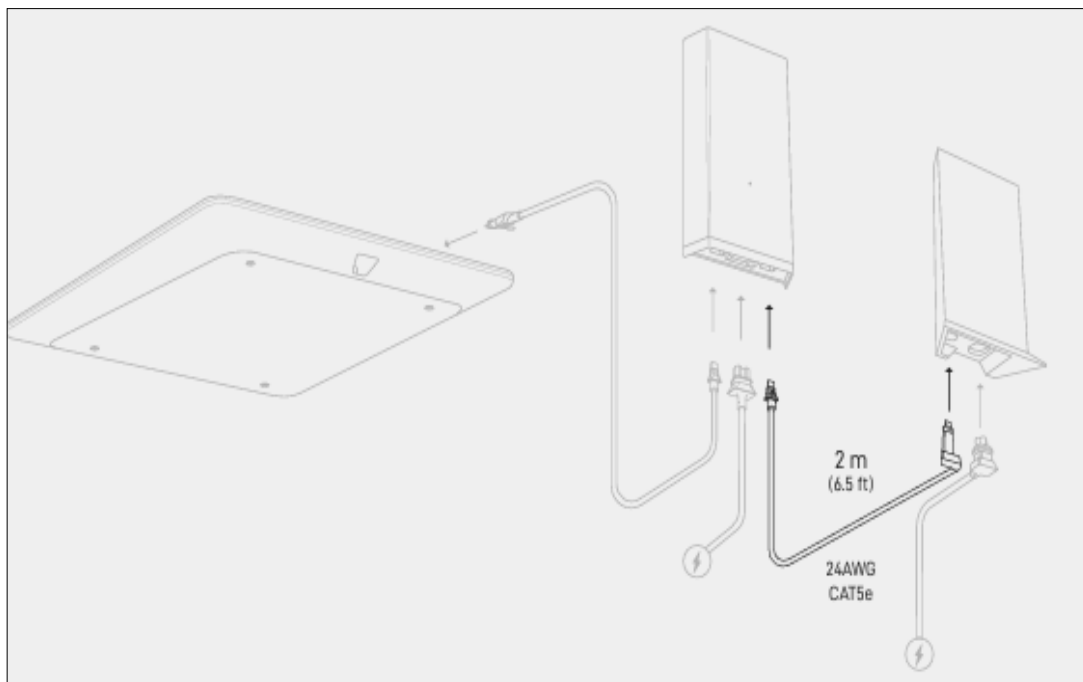


Figura 28 Conexión del Kit Satelital. Fuente: Starlink

Nota: Se visualiza la conexión correspondiente al kit satelital hacia el Access Point.

Con el equipamiento operativo se continúa con la fase de activación lógica mediante la descarga e instalación de la aplicación móvil Starlink. En la Figura 29 se muestra el inicio de credenciales para el acceso a la aplicación móvil. Desde la aplicación se inicia el proceso de configuración, seleccionando el modelo correspondiente del equipo instalado y confirmando la opción adecuada.

La aplicación solicita realizar una validación de ubicación utilizando la cámara del dispositivo móvil para escanear el cielo y comprobar posibles obstrucciones, garantizando que la antena tenga un campo de visión óptimo para mantener conexión constante con la constelación satelital. Posteriormente, el usuario debe conectarse a la red inalámbrica por defecto identificada como “Starlink” (SSID inicial), lo que permitirá continuar con la configuración.

En esta etapa se solicita la creación de un nuevo nombre de red (SSID personalizado) y una contraseña segura, lo cual formaliza la activación del servicio y habilita la conexión definitiva. Una vez configurado el SSID, el sistema inicia el proceso de sincronización con los satélites hasta mostrar el estado “En línea”, indicando que el servicio se encuentra operativo.

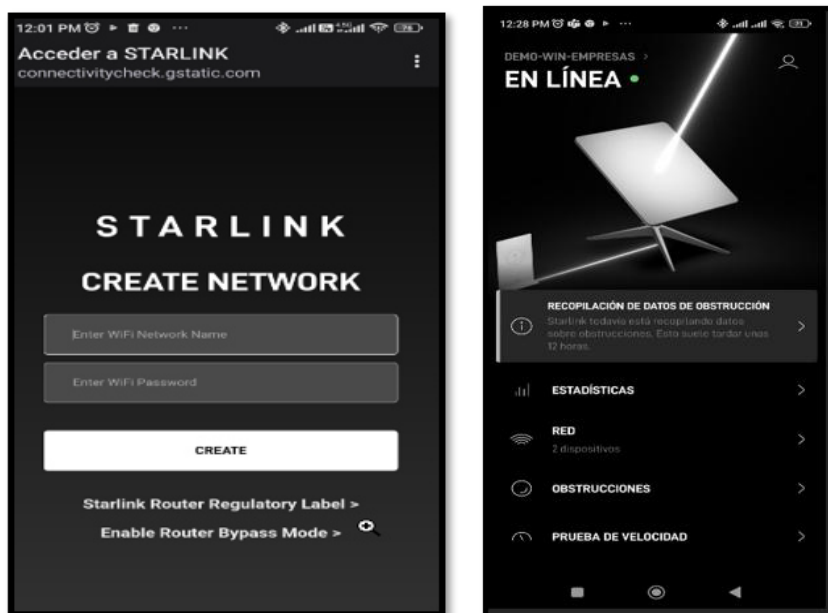


Figura 29 Inicio de credenciales en el aplicativo de Starlink. Fuente: Starlink

Nota: Se visualiza el inicio de las credenciales y la conexión a internet mediante el aplicativo de Starlink.

Finalmente, el modem debe ser reemplazado por el equipamiento router. La conexión del *Power Supply* al router es mediante un cable Ethernet RJ45. Dicho router soporta DHCP en la interfaz WAN para la asignación dinámica de IP privada y configurarse con NAT overload para la salida a Internet. En la Figura 30 se muestra la conexión de la antena Starlink hacia el router.

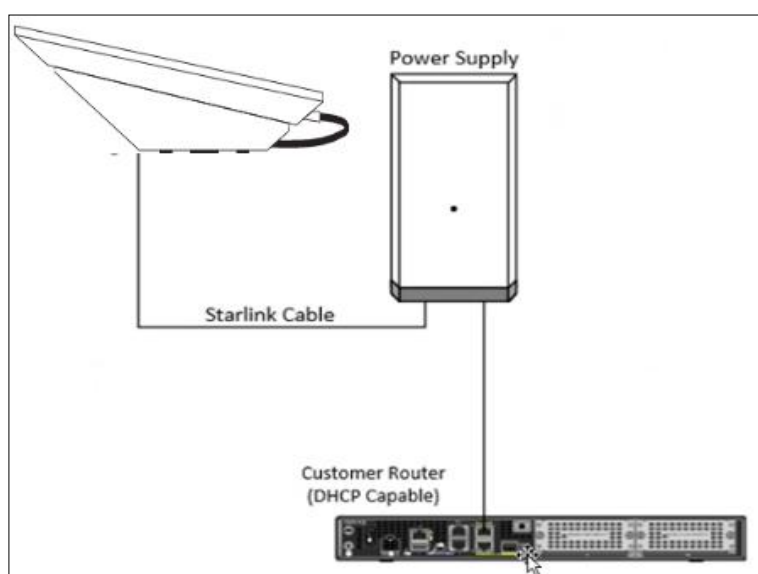


Figura 30 Conexión del Kit Satelital hacia el router. Fuente: Starlink

Nota: Se visualiza la conexión correspondiente al kit satelital hacia el router.

3.5.4 Etapa 4: Validación y puesta en operación

En esta etapa interviene el área de Ingeniería Técnica, la cual toma como referencia el documento ACP (Acta de Conformidad del Proyecto) elaborada en la “Etapa 3-Documentación y transferencia del proyecto”. A partir de esta información se procede a realizar la validación y puesta en marcha del servicio verificando el correcto funcionamiento y el cumplimiento de las especificaciones técnicas establecidas por el cliente. Las actividades desarrolladas en esta etapa son las siguientes:

- a) Prueba y validación del servicio
- b) Firma del Acta de Conformidad
- c) Activación y puesta en operación del servicio

3.5.4.1 Activación y puesta en operación

El área de Ingeniería Técnica en coordinación con el Project Manager procede con la activación y puesta en marcha del servicio implementado en las sedes del cliente ubicadas en la región Loreto. En esta actividad se realiza la habilitación operativa del servicio asegurando el correcto funcionamiento con el usuario.

3.5.4.2 Prueba y validación del servicio

Esta actividad tiene como finalidad realizar las pruebas y validaciones del servicio de internet, del servicio de seguridad y del requerimiento del cliente.

❖ Prueba y validación del servicio de internet

Una vez instalado el kit satelital, se procede a validar la correcta interconexión entre los componentes conformados por el kit satelital y el router. Para ello se realiza pruebas de conectividad como el envío de mensajes ICMP hacia los DNS públicos 8.8.8.8. Mediante esta prueba se valida la correcta asignación de la dirección IP y la estabilidad del enlace satelital.

En la Figura 31 se muestra el comando “ping” hacia el DNS público 8.8.8.8 para comprobar la conectividad a internet en las 3 sedes del cliente.

```

FG5H0E5819907888 # execute ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=116 time=30.6 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=30.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=30.6 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=30.6 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=116 time=30.6 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss

```

Figura 31 Validación de conexión a internet. Fuente: Router del cliente.
Nota: Se visualiza la validación mediante un ping de la conexión hacia internet.

❖ Prueba y validación del servicio de Seguridad

En la Figura 32 se muestra la verificación del estado de los dispositivos gestionados desde la plataforma Panorama de Palo Alto. Se visualiza el listado de los firewalls registrados en el sistema de administración centralizada y se identifican parámetros relevantes como el hostname del dispositivo, la dirección IP de gestión, el modelo del equipo, el número de serie, la versión de software instalada y el estado de conexión. En el caso mostrado, el firewall seleccionado presenta estado “Connected”, lo que indica que el software se encuentra correctamente integrado, permitiendo así la administración centralizada, monitoreo del estado operativo y despliegue de configuraciones y políticas de seguridad desde la consola de gestión.

DEVICE NAME	MODEL	SERIAL NUMBER	IP Address	HA	Status	LAST MERGED DIFF	SOFTWARE VERSION	APPS AND THREAT
VM2-ISEDEMO2	PA-VM	0079510003509...		cluster-unknown	Connected		10.2.3	8674-7847
VM3-ISE94960	PA-VM	0079510003509...		cluster-unknown	Connected		10.2.3	8674-7847
VM3-ISE76650	PA-VM	0079510003517...	10.1.1.4.14	cluster-unknown	Connected		10.2.3	8674-7847
VM3-ISE23460	PA-VM	0079510003530...		cluster-unknown	Connected		10.2.3	8674-7847
VM3-ISE17694	PA-VM	0079510003512...		cluster-unknown	Connected		10.2.3	8674-7847
VM3-ISE65060	PA-VM	0079510003517...		cluster-unknown	Connected		10.2.3	8674-7847

Figura 32 Validación del software de seguridad. Fuente: Elaboración propia a partir de los datos proporcionados por Ingeniería Técnica.

Nota: Se visualiza la validación y correcto funcionamiento del software de seguridad de Palo Alto.

❖ Prueba y validación del requerimiento del cliente

Se valida el requerimiento del cliente mediante una prueba de rendimiento de red, con el objetivo de evaluar el desempeño de la conexión a internet del enlace instalado.

Durante esta prueba se miden indicadores clave de desempeño como la velocidad de descarga (download), velocidad de carga (upload) y latencia, los cuales permiten verificar el comportamiento del servicio de conectividad.

Este tipo de medición forma parte del proceso de validación técnica del servicio, permitiendo comprobar que los parámetros de conectividad se encuentran dentro de los requerimientos establecidos por el cliente.

En la Figura 33 se observa 44.11 Mbps en descarga, 32.81 Mbps en carga y una latencia promedio de 33.70 ms, evidenciando el nivel de rendimiento del enlace, el cual cumple con el requerimiento del cliente de 8Mbps en carga y descarga y la latencia está dentro del rango que ofrece el equipo, de 20 a 60 ms.

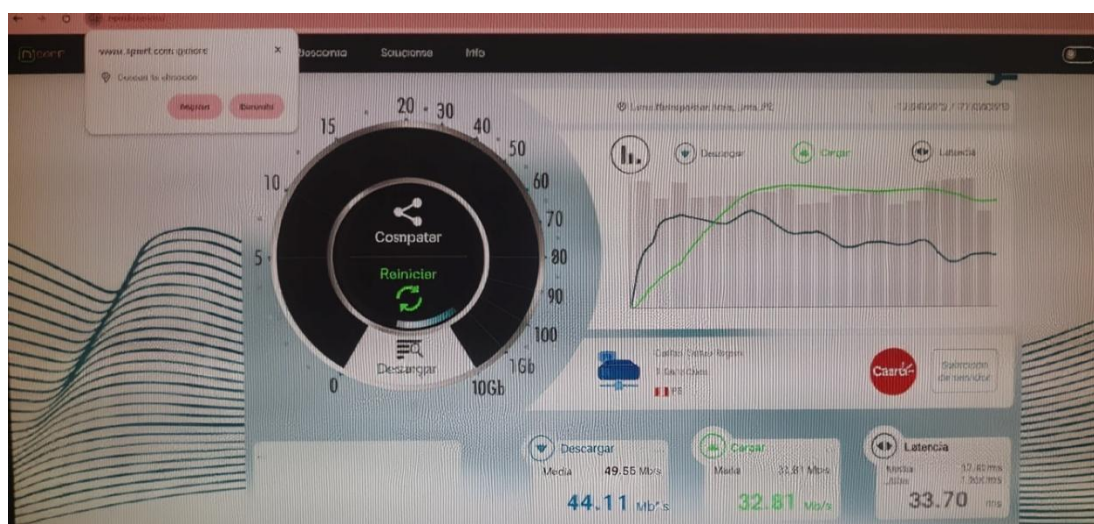


Figura 33 Validación de los requerimientos de la sede Abelardo. Fuente: Elaboración propia a partir de los datos proporcionados por Ingeniería Técnica.

Nota: Se visualiza la validación del ancho de banda y latencia.

En la Figura 34 se observa 96.01 Mbps en descarga, 18.48 Mbps en carga y una latencia promedio de 43.40 ms, evidenciando el nivel de rendimiento del

enlace, evidenciando el nivel de rendimiento del enlace, el cual cumple con el requerimiento del cliente de 8Mbps en carga y descarga y la latencia está dentro del rango que ofrece el equipo, de 20 a 60 ms.

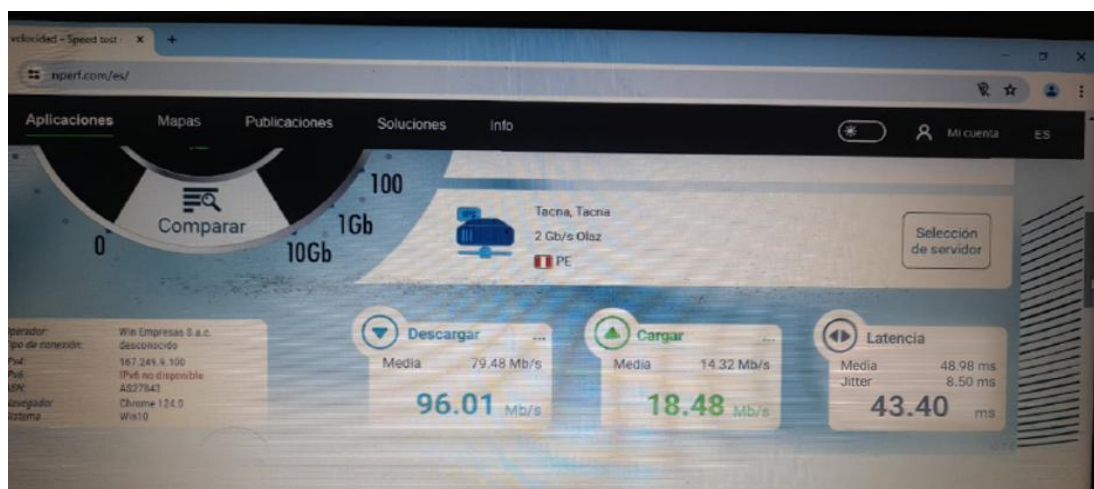


Figura 34 Validación de los requerimientos de la sede Napo. Fuente: Elaboración propia a partir de los datos proporcionados por Ingeniería Técnica.

Nota: Se visualiza la validación del ancho de banda y latencia.

En la Figura 35 se observa 50.10 Mbps en descarga, 25.64 Mbps en carga y una latencia promedio de 21.30 ms, evidenciando el nivel de rendimiento del enlace, el cual cumple con el requerimiento del cliente de 8Mbps en carga y descarga y la latencia está dentro del rango que ofrece el equipo, de 20 a 60 ms.

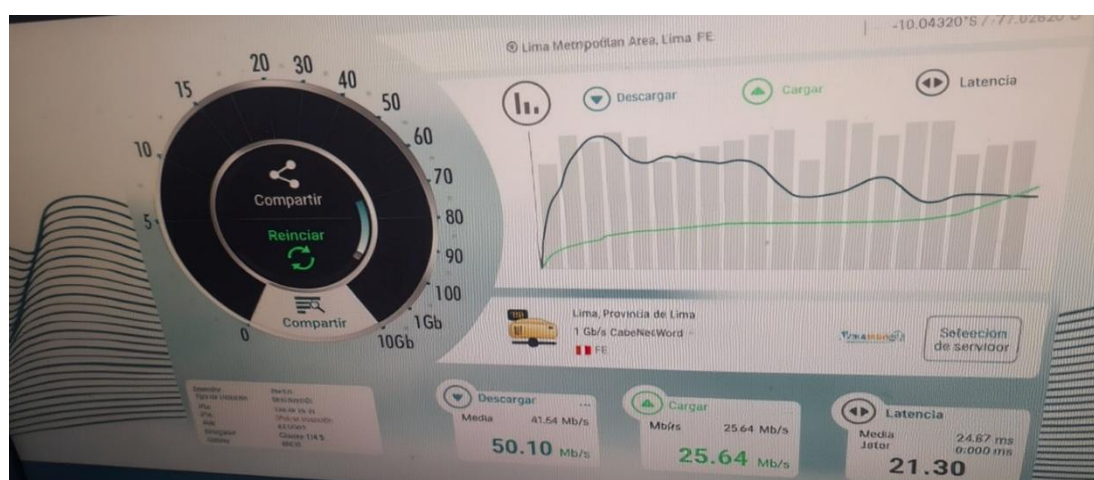


Figura 35 Validación de los requerimientos de la sede Echenique. Fuente: Elaboración propia a partir de los datos proporcionados por Ingeniería Técnica.

Nota: Se visualiza la validación del ancho de banda y latencia.

3.5.4.3 Firma del Acta de Conformidad

En esta actividad, el Project Manager elabora y firma el Acta de Conformidad de Implementación, en la cual se certifica que se realizó la instalación del kit satelital, el equipamiento router y la configuración de los servicios de seguridad conforme a los parámetros técnicos establecidos en el diseño de la solución y que se efectuó las pruebas de funcionamiento y validación de desempeño, mostrando los indicadores como la latencia y capacidad de ancho de banda, verificando que estos cumplen con los requerimientos técnicos definidos por el cliente.

Finalmente, el documento es revisado y firmado por el cliente, dejando constancia formal de su conformidad con la correcta instalación, configuración, validación y la puesta en marcha de los servicios solicitados.

3.6 Resultado de la actividad

Como resultado de las actividades realizadas, el servicio se encuentra activo en cada una de las sedes del cliente. Asimismo, se verifica que la solución implementada cumple con los objetivos planteados en el presente trabajo de suficiencia profesional, garantizando la disponibilidad del servicio y el correcto desempeño de la infraestructura de comunicaciones instalada.

3.6.1 Resultado de la evaluación del medio de transmisión de datos

En la “Etapa 1-Análisis del requerimiento” se evalúan las alternativas del medio de transmisión más adecuada para las sedes ubicadas en la zona rural de Loreto.

Se descarta la implementación mediante fibra óptica debido al elevado costo de inversión asociado al despliegue en zonas geográficamente alejadas. Asimismo, la alternativa de radioenlace no resulta viable al no cumplir con la línea de vista necesaria para garantizar la conectividad.

Por ese motivo, se determina que el medio de transmisión satelital es la alternativa más factible debido a su menor costo de implementación y su capacidad de brindar conectividad en zonas rurales.

Posteriormente, se realiza la evaluación del consumo real de ancho de banda, con el objetivo de verificar si cumple con una buena conectividad. Los resultados evidencian que el medio de transmisión satelital implementado mediante la tecnología Starlink satisface la demanda de tráfico generado por los usuarios, cumpliendo con el ancho de banda proporcionado por el plan Starlink contratado.

En la Figura 36 se evidencia el comportamiento del tráfico de carga y descarga correspondiente a la sede Abelardo. Durante el mes de enero se registró una velocidad máxima de carga de 0.16 Mbps y una velocidad máxima de descarga 1.11 Mbps, valores que se encuentran dentro de los parámetros de capacidad del servicio solicitado.

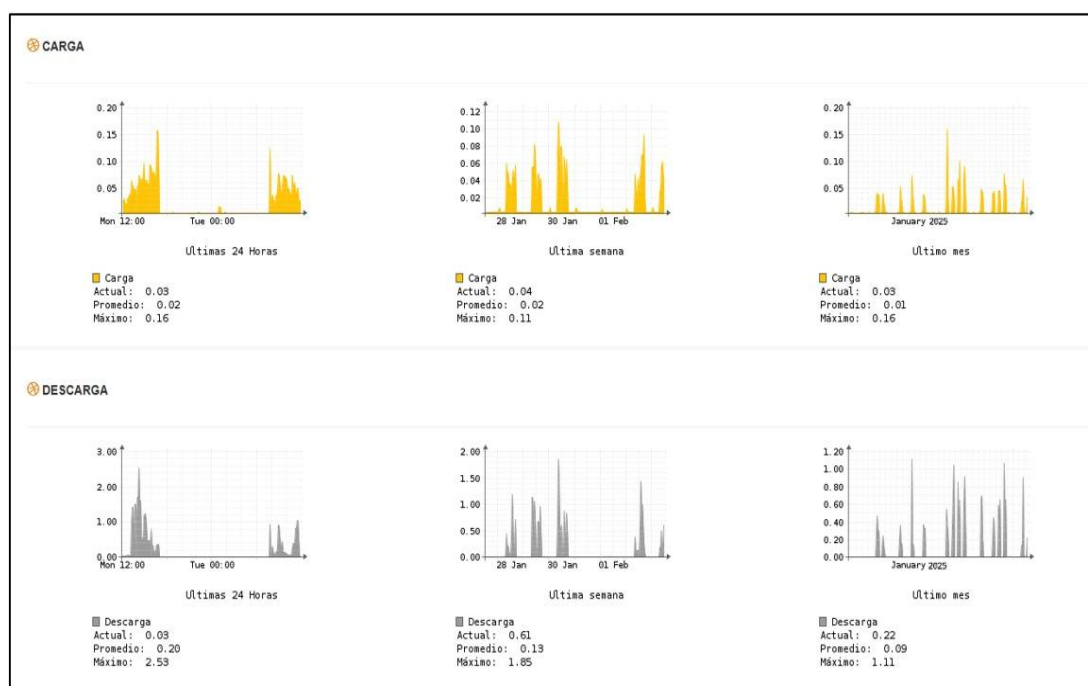


Figura 36 Evidencia de carga y descarga de la sede Abelardo. Fuente: Elaboración propia a partir de los datos del gestor de monitoreo.

Nota: Se visualiza el comportamiento del tráfico de carga y descarga.

En la Figura 37 se evidencia el comportamiento del tráfico de carga y descarga correspondiente a la sede Napo. Durante el mes de enero se registró una velocidad máxima de carga de 0.81 Mbps y una velocidad máxima de descarga 3.13 Mbps, valores que se encuentran dentro de los parámetros de capacidad del servicio solicitado.

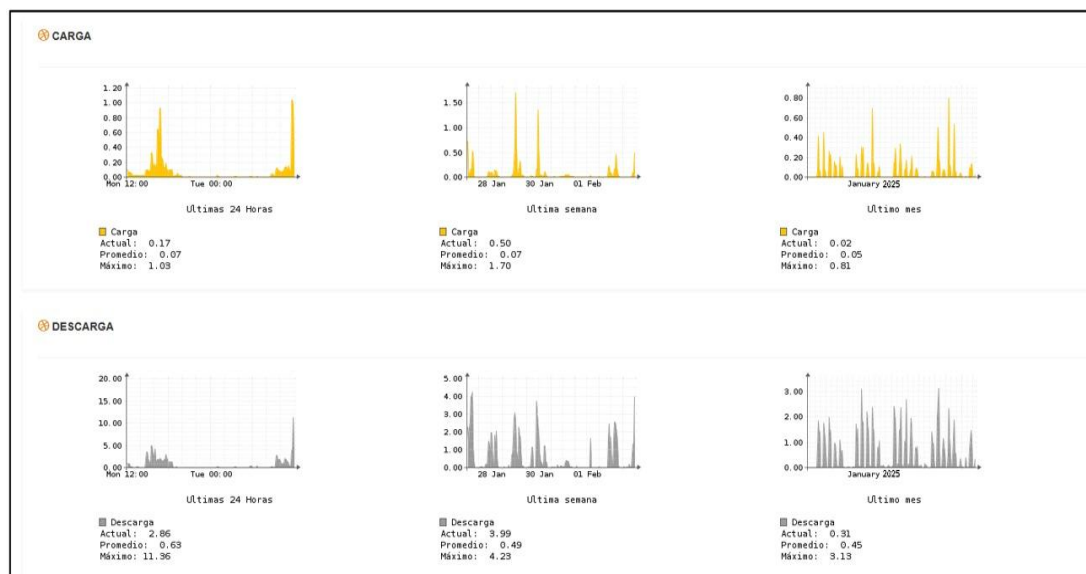


Figura 37 Evidencia de carga y descarga de la sede Napo. Fuente: Elaboración propia a partir de los datos del gestor de monitoreo.
Nota: Se visualiza el comportamiento del tráfico de carga y descarga.

En la Figura 38 se evidencia el comportamiento del tráfico de carga y descarga correspondiente a la sede Echenique. Durante el mes de enero se registró una velocidad máxima de carga de 2.73 Mbps y una velocidad máxima de descarga 8.97 Mbps, valores que se encuentran dentro de los parámetros de capacidad del servicio solicitado.

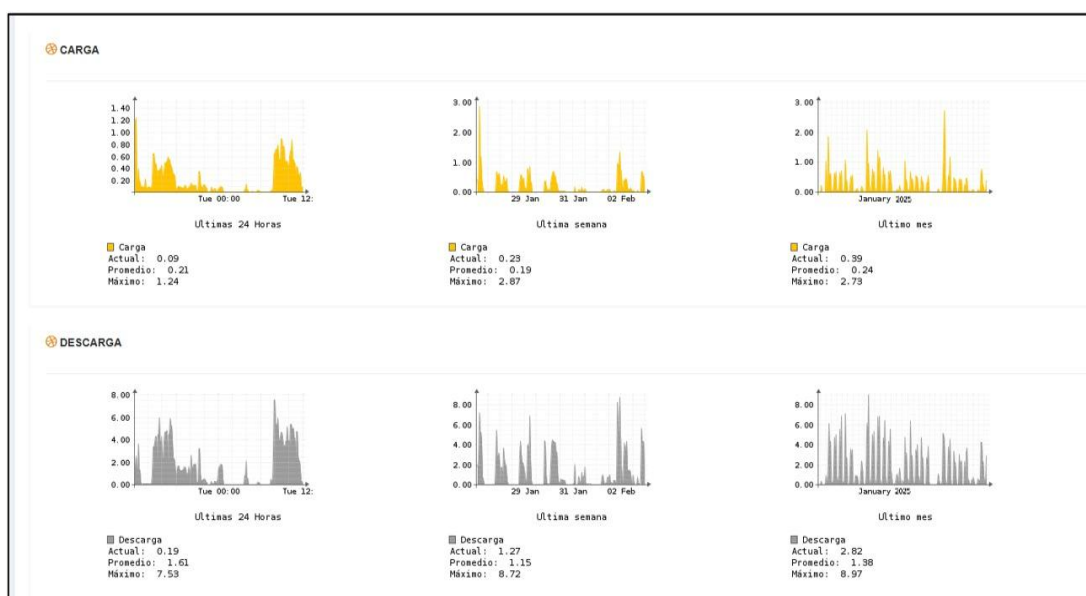


Figura 38 Evidencia de carga y descarga de la sede Echenique. Fuente: Elaboración propia a partir de los datos del gestor de monitoreo.
Nota: Se visualiza el comportamiento del tráfico de carga y descarga.

3.6.2 Resultado de la evaluación de la mejor tecnología

En la “Etapa 1-Análisis del requerimiento” se realiza la evaluación comparativa entre la tecnología actual del cliente y la tecnología propuesta. En el análisis se consideraron indicadores de desempeño orientados a la calidad de la conectividad, tales como el parámetro de latencia. La tecnología inicial del cliente es basada en enlaces satelitales VSAT la cual presenta teóricamente valores de latencia que oscilan entre 500 ms y 700 ms, mientras que la tecnología propuesta de STARLINK ofrece valores de latencia que oscilan entre 20 ms y 60 ms. Debido a esta mejora en la latencia se determina implementar el servicio mediante la tecnología STARLINK con el objetivo de mejorar la calidad de conectividad y navegación.

Posteriormente, se realiza la evaluación del comportamiento real de la latencia con el propósito de verificar si la tecnología implementada cumple con los niveles de desempeño esperados. Los resultados obtenidos evidencian una reducción significativa, lo cual contribuye a mejorar la conectividad y eficiencia en la transmisión de datos.

En la Figura 39 se evidencia el comportamiento de la latencia correspondiente a la sede Abelardo. Durante los últimos 4 meses se registra una latencia máxima de 34.42 ms, valor que se encuentran dentro de los parámetros brindados por la tecnología STARLINK lo que evidencia una mejora en comparación a la tecnología utilizada por el cliente.

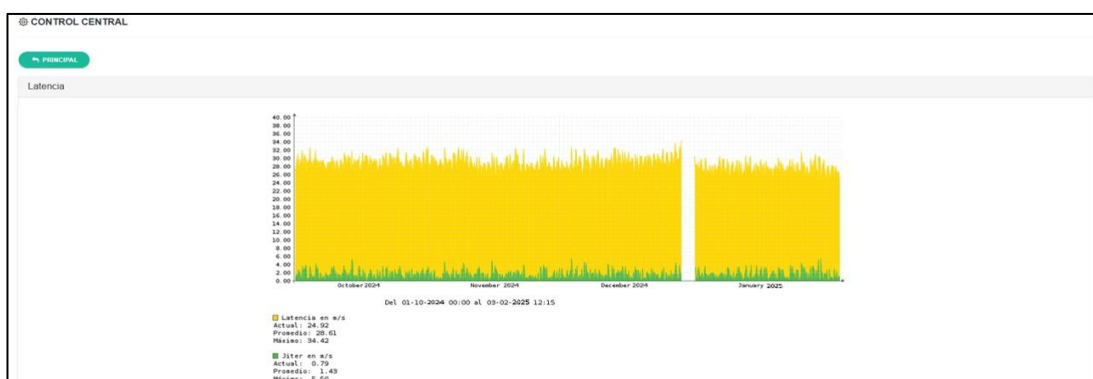


Figura 39 Evidencia de latencia de la sede Abelardo. Fuente: Elaboración propia a partir de los datos del gestor de monitoreo.

Nota: Se visualiza el comportamiento de la latencia registrada en los últimos meses. Fuente: Elaboración propia a partir de los datos del gestor de monitoreo.

En la Figura 40 se evidencia el comportamiento de la latencia correspondiente a la sede Napo. Durante los últimos 4 meses se registró una latencia máxima de 34.84 ms, valor que se encuentran dentro de los parámetros brindados por la tecnología STARLINK lo que evidencia una mejora en comparación a la tecnología utilizada por el cliente.

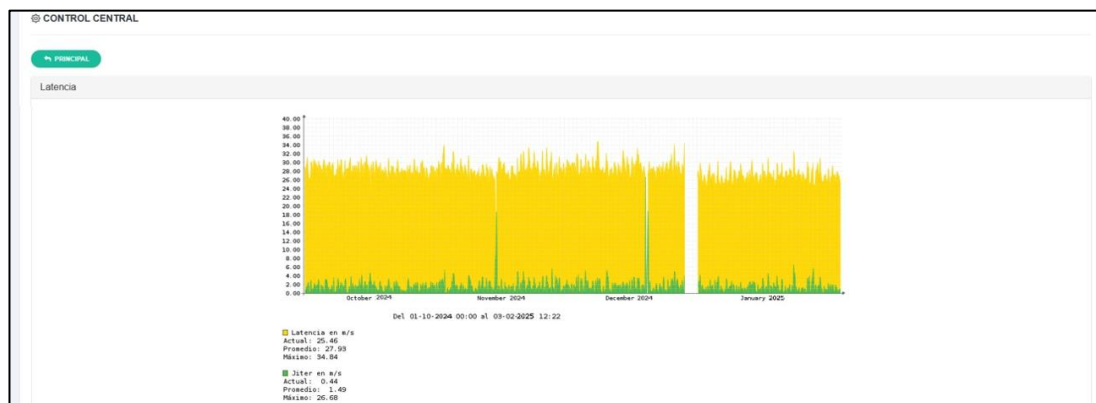


Figura 40 Evidencia de latencia de la sede Napo. Fuente: Elaboración propia a partir de los datos del gestor de monitoreo.

Nota: Se visualiza el comportamiento de la latencia registrada en los últimos meses.

En la Figura 41 se evidencia el comportamiento de la latencia correspondiente a la sede Echenique. Durante los últimos 4 meses se registró una latencia máxima de 36.73 ms, valor que se encuentran dentro de los parámetros brindados por la tecnología STARLINK lo que evidencia una mejora en comparación a la tecnología utilizada por el cliente

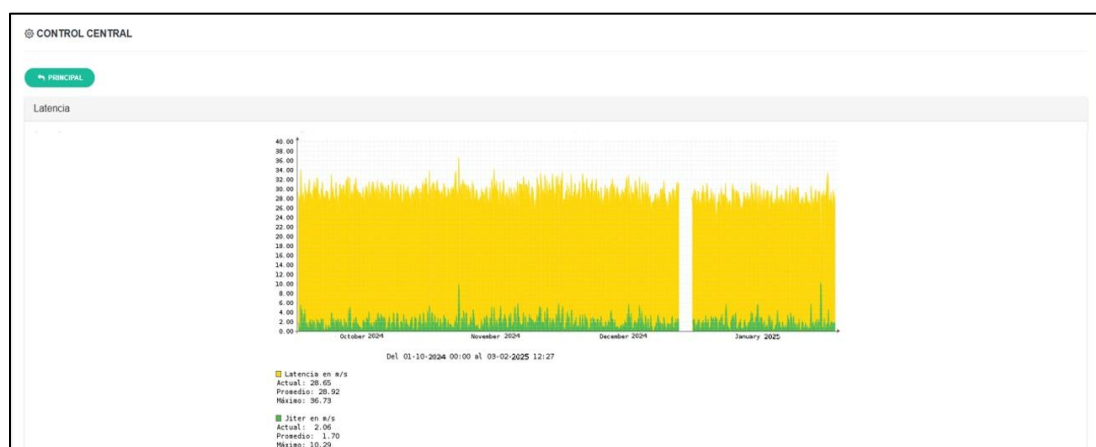


Figura 41 Evidencia de latencia de la sede Echenique. Fuente: Elaboración propia a partir de los datos del gestor de monitoreo.

Nota: Se visualiza el comportamiento de la latencia registrada en los últimos meses.

3.6.3 Resultado de la evaluación del equipamiento

En la “Etapa 1-Análisis del requerimiento” se identifica que el cliente no cuenta con mecanismos de seguridad para la navegación en internet lo cual expone su red a posibles amenazas y riesgos informáticos. Por ese motivo, se propone la implementación de un sistema de seguridad que permita garantizar una navegación segura y confiable para los colaboradores.

Se implementa un sistema de seguridad basada en tecnología Palo Alto, el cual proporciona diversas funcionalidades orientadas a la protección del tráfico de red, control de aplicaciones y la inspección del tráfico hacia internet.

Posteriormente, se realiza una evaluación del funcionamiento del sistema de seguridad con el fin de verificar el correcto desempeño. Como resultado se evidencia el adecuado funcionamiento del sistema mediante un reporte de seguridad que muestra los eventos de seguridad detectados durante un periodo determinado. A través de diversos indicadores y métricas, el reporte brinda información como los tipos de amenazas detectadas, vulnerabilidades identificadas y aplicaciones utilizadas por los usuarios.

Esta información permite obtener una visión integral del estado de seguridad de la infraestructura de red, facilitando la identificación de posibles riesgos, patrones de ataque y comportamientos anómalos del tráfico.

En la Figura 42 se muestra el reporte del sistema de seguridad, donde se evidencian los principales eventos y métricas de seguridad obtenidos como resultado de la implementación de la solución:

❖ Top 5 Users:

El reporte identifica los cinco usuarios o direcciones IP con mayor volumen de sesiones y tráfico generado en la red. Esta información permite identificar los principales generadores de tráfico dentro del entorno monitoreado, facilitando el análisis de patrones de uso de red y la detección de posibles comportamientos anómalos o excesivos en el consumo de recursos.

❖ Top 5 Attacker Sources:

El reporte identifica las direcciones IP de origen que generan la mayor cantidad de intentos de ataque o tráfico malicioso detectado por el sistema de seguridad como:

- ✓ Ataques de disponibilidad: DoS / DDoS
- ✓ Ataques de reconocimiento: Scanners
- ✓ Ataques de intrusión: Explotación de vulnerabilidades
- ✓ Ataques de malware: spyware
- ✓ Ataques de navegación web: Dominios maliciosos

Este análisis permite identificar los principales puntos de origen de amenazas externas, facilitando la implementación de políticas de bloqueo o filtrado en el firewall. La dirección IP 103.134.26.60, que ocupa el primer lugar en el listado analizado, registra un total de 1,400 eventos correspondientes a intentos de ataque.

❖ Top 5 Attacker Destinations:

El reporte identifica las direcciones IP de destino dentro de la infraestructura que han recibido la mayor cantidad de intentos de ataque. Esta información permite identificar recursos críticos potencialmente expuestos o más atacados, contribuyendo al fortalecimiento de controles de seguridad y monitoreo en dichos activos. La dirección IP 168.121.237.98, que ocupa el primer lugar en el listado, registra un total de 1,571 eventos asociados a intentos de ataque recibidos.

❖ Top 5 Attacks:

El reporte muestra los principales tipos de ataques detectados por el sistema de seguridad. Estos ataques corresponden principalmente a técnicas de denegación de servicio (DoS) utilizadas para saturar recursos de red o servidores mediante tráfico amplificado.

El tipo de amenaza que encabeza la lista es Proxy Domain, con un total de 2,800 eventos registrados.

❖ Top 5 Spyware:

El reporte identifica dominios o indicadores asociados a actividades de software espía o comportamiento malicioso, donde el evento más frecuente corresponde a Proxy Domain con 2,800 registros. Esta información permite detectar posibles comunicaciones con infraestructura de comando y control o dominios sospechosos.

❖ Top 5 Applications:

El reporte también presenta las aplicaciones más utilizadas dentro de la red, destacando ssl, dns-base, ms-office365-base, google-base y ping, lo que refleja el predominio de servicios de navegación web, resolución DNS y comunicaciones seguras. Este análisis permite comprender el comportamiento del tráfico de red y los servicios más utilizados por los usuarios.

❖ Top 5 Application Categories:

El análisis por categoría muestra que el 75.00% del tráfico corresponde a aplicaciones de networking, seguido por general-internet, unknown, business-systems y collaboration, lo que evidencia que la mayor parte del tráfico corresponde a protocolos de red y servicios básicos de conectividad.

Top 5 Users

User	Sessions	Bytes
170.82.97.6	18,500	145 MB
170.231.82.169	15,200	118 MB
190.187.201.137	12,800	96 MB
190.117.19.167	10,400	78 MB
170.231.170.134	8,900	65 MB

Top 5 Attacker Sources

Source	Count
103.134.26.60	1,400
103.49.115.220	1,050
38.25.36.44	980
139.99.40.25	480
38.25.36.212	160

Top 5 Attacker Destinations

Destination	Count
168.121.237.98	1,571
168.121.237.102	1,029
168.121.237.100	902
170.82.97.22	428
170.82.97.14	117

Top 5 Attacks

Threat	Count
Proxy Domain	2,800
Trojan.revetrat: winmicrosoft.sytes.net	1,950
XMRig Miner Command and Control Traffic	1,600
generic:wvdbzpf.comU	1,350
generic:kbz0pwxmv.com	1,100

Top 5 Spyware

Spyware	Count
Proxy Domain	2,800
Trojan.revetrat:winmicrosoft.sytes.net	1,600
XMRig Miner Command and Control	1,350
Malicious NRD Domain	1,100
generic:donate.v2.xmrig.com	600

Top 5 Applications

Application	Sessions	Bytes
ssl	150,000	9.4 G
dns-base	150,000	80M
ms-office365-base	30,000	830M
google-base	25,000	200M
ping	20,000	6 M

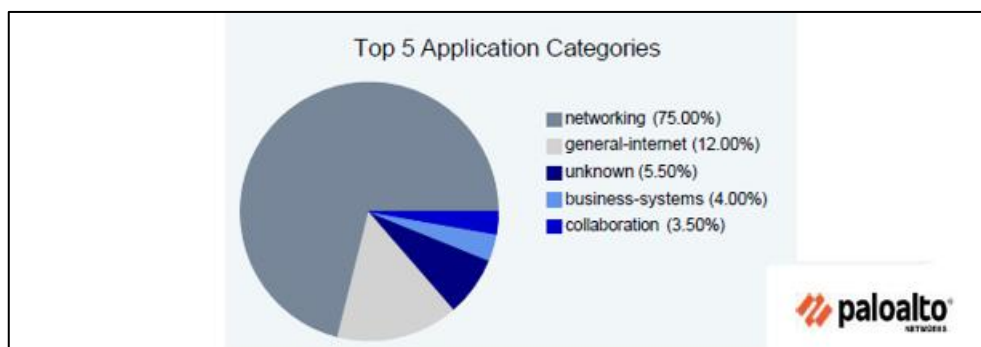


Figura 42. Evidencia mediante el reporte de seguridad. Fuente: Elaboración propia a partir de los datos del gestor de monitoreo.

Nota: Se visualiza el comportamiento del sistema de seguridad mediante un reporte.

3.6.4 Resultado de la solución diseñada e implementada

En la “Etapa 1-Análisis del requerimiento” se evalúa la disponibilidad del servicio satelital VSAT previamente utilizado por el cliente, el cual ofrecía una disponibilidad de 97.80%, equivalente aproximadamente a 16 horas de tiempo de inactividad mensual. En cambio, la solución implementada mediante la tecnología STARLINK presenta disponibilidad de 98.30% lo que corresponde a un tiempo máximo de inactividad de 12.45 horas al mes, representando una mejora en la continuidad del servicio. También se analiza el ancho de banda mínimo necesario por sede, cumpliendo en brindar un mínimo de 8 Mbps simétrico, garantizando así un servicio eficiente. Así mismo se evalúa el desempeño de la navegación mediante el nivel de latencia donde la solución VSAT tiene 500-700 ms y STARLINK de 20-60 ms.

En la evaluación de otras alternativas de medio de transmisión como la fibra óptica y radioenlace, se descarta la fibra óptica por ser económicamente costosa y al radioenlace por no tener línea de vista bajo el contexto del servicio solicitado.

En la “Etapa 2-Diseño de red” se realiza el dimensionamiento y la selección de los equipos necesarios para implementar la solución basada en tecnología STARLINK. Como resultado, se define una arquitectura compuesta por un router Cisco 1121-4P, una antena satelital Starlink Flat High Performance y un sistema de seguridad en la nube basado en el software Palo Alto en cada sede del cliente. Asimismo, se diseña una topología de red que integra estos

componentes mediante la configuración VPN Site-to-Site con protocolo IPsec. Este diseño asegura que el servicio de Internet satelital pueda operar de manera estable para las tres sedes del cliente en la provincia de Loreto. Luego de tener dimensionado y la realización del diseño de red, se elabora y se remite la propuesta técnica y económica al cliente, detallando la arquitectura planteada, los equipos seleccionados, los costos asociados y los alcances de la solución propuesta para su evaluación y aprobación.

En la “Etapa 3-Implementación del servicio” se lleva a cabo la instalación y configuración de la solución diseñada. Esta etapa se inicia a partir de la firma del contrato entre el cliente y el proveedor, formalizando los alcances y condiciones del servicio especificados en la propuesta técnica. Para ello, se asigna un jefe de proyecto responsable de planificar y supervisar la ejecución mediante un plan de trabajo que permite organizar las actividades de instalación en cada sede. Durante la implementación se efectúa el aprovisionamiento del equipamiento, la instalación del kit satelital Starlink, la configuración del router Cisco y la implementación del sistema de seguridad mediante la tecnología Palo Alto. Como resultado, el servicio de conectividad satelital es implementado de manera satisfactoria en las tres sedes del cliente, permitiendo conectividad segura y confiable.

En la “Etapa 4-Validación y puesta en marcha” se realiza las pruebas técnicas y la verificación del correcto funcionamiento de la solución implementada en las sedes del cliente. Entre las pruebas a realizar está la verificación de conectividad mediante pruebas ICMP hacia servidores públicos, validación del estado operativo del sistema de seguridad Palo Alto y las pruebas de rendimiento de la red para medir indicadores como velocidad de descarga, velocidad de carga y latencia, dando como resultado que los valores cumplen con los requerimientos solicitados por el cliente. Tras la validación satisfactoria del servicio, se procede con la firma del Acta de Conformidad, formalizando la aceptación de la solución implementada y su correcta puesta en marcha. Con el objetivo de verificar el desempeño de la solución implementada, se realiza el análisis de disponibilidad correspondiente a los últimos seis meses

de operación. Los resultados evidencian que la disponibilidad real del servicio alcanzó el 100%, ya que durante este periodo no se registraron interrupciones asociadas al servicio implementado. En la Tabla 11, se visualiza el detalle del análisis de disponibilidad del servicio durante el periodo evaluado.

Tabla 11 Disponibilidad mediante un determinado tiempo.

Sede	Solicitud del cliente	Disponibilidad					
		Ene-2025	Feb-2025	Mar-2025	Abr-2025	May-2025	Jun-2025
Abelardo	98.30%	100%	100%	100%	100%	100%	100%
Napo	98.30%	100%	100%	100%	100%	100%	100%
Echenique	98.30%	100%	100%	100%	100%	100%	100%

Nota: Se visualiza la disponibilidad del servicio en cada sede del cliente.

Fuente: Elaboración propia a partir de los datos del área de Operaciones.

CAPITULO IV: DISCUSION DE RESULTADOS

4.1 Descripción de la implementación

El operador anterior del cliente brindaba el servicio de internet mediante el medio de transmisión VSAT con ancho de banda 5Mbps, latencia de 500 a 700 ms y no presentaba un servicio de seguridad para la navegación de sus usuarios. Para cumplir con los requerimientos de la entidad, se plantea la implementación de una solución de conectividad que permita garantizar un ancho de banda mínimo de 5 Mbps, una latencia máxima de 60 ms y una disponibilidad mínima del 98.30%. Asimismo, la solución considera la incorporación de seguridad que permita mejorar la conectividad y la seguridad de navegación en las tres sedes de la entidad ubicadas en la zona rural de Loreto.

En cuanto al primer objetivo, relacionado con la elección del medio de transmisión más adecuado, se realiza el análisis de diferentes alternativas tecnológicas disponibles para brindar conectividad en zonas rurales, descartando la implementación mediante fibra óptica debido a los elevados costos asociados a su despliegue en zonas geográficamente alejadas y la alternativa de radioenlace debido a la falta de línea de vista entre las sedes. En consecuencia, se determina que el medio de transmisión satelital representa la alternativa más viable para garantizar la conectividad en las sedes del cliente, asegurando disponibilidad, cobertura y continuidad operativa del servicio

En cuanto al segundo objetivo, relacionado a la elección de la mejor tecnología de servicio de internet satelital, se realiza un análisis comparativo entre la tecnología satelital VSAT, solución inicialmente implementada por su anterior

operador, y la tecnología Starlink propuesta. Como resultado teórico del análisis, se evidencia que la tecnología VSAT presenta valores de latencia que oscilan entre 500 ms y 700 ms, mientras que la tecnología Starlink ofrece latencias aproximadas entre 20 ms y 60 ms. Luego se realiza pruebas de latencia observándose que la tecnología Starlink cumple con la latencia establecida, brindando una mejora en la conectividad por cada sede. Como resultado de la implementación, la latencia por sede está dentro de los parámetros ofrecidos por STARLINK. Las sedes Abelardo, Napo y Echenique tienen como latencia 34.42 ms, 38.72 ms y 36.73 ms, respectivamente, que cumplen con los requisitos solicitados por el cliente.

En cuanto al tercer objetivo, relacionado con la elección del equipamiento adecuado para un servicio de internet satelital seguro, se identifica que la infraestructura inicial del cliente no contaba con mecanismos de protección para la navegación hacia internet. Por este motivo, se implementa un sistema de seguridad basado en tecnología Palo Alto, el cual permite realizar inspección del tráfico, control de aplicaciones y detección de amenazas, garantizando una navegación segura y confiable para los usuarios de la red.

En relación con el cuarto objetivo, orientado a evaluar la mejora en la conectividad y seguridad de navegación a partir de la solución implementada, se realiza pruebas de disponibilidad del servicio. Los resultados obtenidos evidencian que la solución implementada cumple con los requerimientos establecidos por la entidad, alcanzando una disponibilidad del 100% durante los últimos seis meses de operación y garantizando una conectividad estable y segura en las tres sedes del cliente.

4.2 Evaluación Económica

En la evaluación económica se considera el análisis de inversión (CAPEX), costo de operación y mantenimiento del servicio (OPEX) e ingresos por la mensualidad del servicio, identificándose los siguientes componentes para la viabilidad del proyecto:

- CAPEX: Corresponde a la inversión inicial necesaria para la adquisición de equipos para el cliente, instalación y configuración de los equipos y software de seguridad.
- OPEX: Corresponde a los gastos recurrentes relacionados con la operación y mantenimiento, siendo estos el soporte técnico y el plan del servicio.
- Renta Mensual: Corresponde al pago mensual por el servicio que paga el cliente, generando ingreso a la empresa.

Para evaluar la rentabilidad, se emplean los indicadores financieros VAN y TIR, considerando las siguientes definiciones:

1. Valor Actual Neto (VAN): Indicador financiero que permite evaluar la rentabilidad de un proyecto, considerando el valor del dinero en el tiempo. El VAN se obtiene como la diferencia entre el valor actual de los ingresos y la inversión inicial. Su interpretación es la siguiente:

$VAN > 0$, el proyecto es rentable.

$VAN < 0$, el proyecto no es rentable.

$VAN = 0$, el proyecto solo recupera la inversión

2. Tasa Interna de Retorno (TIR): Indicador financiero que permite medir la rentabilidad de un proyecto. El TIR indica el porcentaje de ganancia que genera un proyecto a lo largo del tiempo. Su interpretación es la siguiente:

Si la $TIR >$ tasa de descuento, el proyecto es rentable.

Si la $TIR <$ tasa de descuento, el proyecto no es rentable.

$TIR =$ tasa de descuento, el proyecto es indiferente.

Se realiza el cálculo de forma integral por las 3 sedes. Así mismo, es importante tener en cuenta que los equipos utilizados en la solución son proporcionados bajo un esquema de arrendamiento, por lo que su costo se encuentra incorporado dentro del pago mensual del servicio, evitando que el cliente realice una inversión inicial significativa.

Finalmente, la evaluación económica permite establecer una base sólida para la toma de decisiones, asegurando que la solución propuesta no solo sea técnicamente viable, sino también financieramente sostenible en el tiempo.

Inversión (CAPEX) y costo de operación y mantenimiento (OPEX)

A continuación, en la Tabla 12, se detalla los gastos de capital (CAPEX) y gastos operativos (OPEX) para la implementación del proyecto

Tabla 12. Evaluación económica por las 3 sedes

Características	Capex	Opex (3 años)	Ingresos (3 años)
Costo de inversión inicial:			
Kit Satelital	\$6,450.00	-	
Activación del kit	\$60.00	-	
Instalación y configuración del servicio	\$3,150.00	-	
Router	\$360.00	-	
Instalación y configuración del servicio de seguridad	\$2,266.00		
Total	\$12,286.00	-	-
Costos de Operación y mantenimiento:			
Costo de Venta (Soporte del servicio, Plan del Servicio, Canon)	-	\$52,296.00	
Gasto de Venta	-	\$19,935.00	
Gasto Administrativo	-	\$4,794.00	
Impuestos	-	\$9,021.00	
Total	-	\$86,046.00	-
Ingresos			
Arrendamiento de equipos	-	-	\$39,780.00
Plan del Servicio	-	-	\$47,700.00
Servicio de Seguridad	-	-	\$32,400.00
Total	-	-	\$119,880.00

Fuente: Elaboración propia a partir de los datos del área de Operaciones.

Nota: Se visualiza la inversión y el servicio del proyecto.

Tabla 13 Costos de Operación y Mantenimiento (Opex) Anual

Características	Opex Año 1	Opex Año 2	Opex Año 3
Costos de Operación y mantenimiento:			
Costo de Venta (Soporte del servicio, Plan del Servicio, Canon)	\$17,432.00	\$17,432.00	\$17,432.00

Gasto de Venta	\$10,345.00	\$4,795.00	\$4,795.00
Gasto Administrativo	\$1,598.00	\$1,598.00	\$1,598.00
Impuestos	\$2,010.00	\$3,533.00	\$3,478.00
Total	\$31,385.00	\$27,358.00	\$27,303.00

Fuente: Elaboración propia a partir de los datos del área de Operaciones.

Nota: Se visualiza la inversión y el servicio del proyecto.

Tabla 14 Flujo de Caja a 3 años

Concepto	Año 0	Año 1	Año 2	Año 3
INGRESOS				
Ingresos por servicios	0	39,960	39,960	39,960
Total Ingresos	0	39,960	39,960	39,960
EGRESOS				
Inversión inicial (CAPEX)	-12,286	0	0	0
Costos de operación (OPEX)	0	-31,385	-27,358	-27,303
Total Egresos	-12,286	-31,385	-27,358	-27,303
FLUJO NETO	-12,286	8,575	12,602	12,657
FLUJO ACUMULADO	-12,286	-3,711	8,891	21,548

Fuente: Elaboración propia a partir de los datos del área de Operaciones.

4.2.1 Cálculo del VAN

El VAN positivo indica que el proyecto no solo recupera la inversión inicial, sino que genera valor adicional, siendo económicamente rentable

- Inversión inicial (CAPEX) I_0 : \$12,286.00
- Ingreso anual: \$39,960.00
- Gasto anual (OPEX) – Año 1: \$31,385.00
- Gasto anual (OPEX) – Año 2: \$27,358.00
- Gasto anual (OPEX) – Año 3: \$27,303.00
- Tasa de descuento: 16%

Por tanto, el flujo neto anuales:

$$\begin{aligned}
 f_{\text{neto-Año } X} &= \text{Ingresos}_{\text{Año } x} - \text{OPEX}_{\text{Año } x} \\
 f_{\text{neto-Año } 1} &= 39,960 - 31,385 = 8,575 \\
 f_{\text{neto-Año } 2} &= 39,960 - 27,358 = 12,602 \\
 f_{\text{neto-Año } 3} &= 39,960 - 27,303 = 12,657
 \end{aligned}$$

Luego para 3 años

$$VAN = \sum_{t=1}^3 \frac{F_{neto}}{(1 + \text{tasa de descuento})^t} - Inversion\ Inicial$$

$$VAN = \sum_{t=1}^3 \frac{F_{neto}}{(1 + 0.16)^t} - 12,286$$

Reemplazando

$$VAN = \frac{8,575}{(1.16)^1} + \frac{12,602}{(1.16)^2} + \frac{12,657}{(1.16)^3} - 12,286$$

El resultado es aproximadamente:

$$VAN \approx 12,580.38$$

Por lo tanto, el VAN es positivo, lo que indica que el proyecto es rentable y recupera ampliamente la inversión.

4.2.2 Cálculo del TIR

La TIR se obtiene encontrando la tasa que hace que el VAN sea igual a cero:

$$0 = \sum_{t=1}^3 \frac{F_t}{(1 + TIR)^t} - Inversión$$

Se obtiene la información mensual

$$0 = \frac{8,575}{(1 + TIR)^1} + \frac{12,602}{(1 + TIR)^2} + \frac{12,657}{(1 + TIR)^3} - 12,286$$

Probar con 50%

$$VAN = \frac{8,575}{(1.50)^1} + \frac{12,602}{(1.50)^2} + \frac{12,657}{(1.50)^3} - 12,286$$

$$VAN = 2,781.78$$

Probar con 70%

$$VAN = \frac{8,575}{(1.70)^1} + \frac{12,602}{(1.70)^2} + \frac{12,657}{(1.70)^3} - 12,286$$

$$VAN = -305.10$$

Al aplicar la interpolación

$$TIR = i_1 + \left(\frac{VAN_1}{VAN_1 - VAN_2} \right) (i_2 - i_1)$$

Resolviendo la ecuación se obtiene:

$$TIR = 50\% + \left(\frac{2,781.78}{2,781.78 - -305.10} \right) (70\% - 50\%)$$

$$TIR = 50\% + \left(\frac{2,781.78}{2,781.78 + 305.10} \right) (20\%)$$

$$TIR = 50\% + \left(\frac{2,781.78}{3,086.88} \right) (20\%)$$

$$TIR = 50\% + (0.901161572)(20\%)$$

$$TIR = 50\% + 18.02\%$$

$$TIR \approx 68.02\%$$

El proyecto presenta un Valor Actual Neto (VAN) de 12,580.38 y una Tasa Interna de Retorno (TIR) aproximada de 68.02%, lo cual evidencia su viabilidad económica. A pesar de los costos operativos variables, el proyecto genera flujos suficientes para recuperar la inversión inicial en el segundo año y obtener beneficios superiores al costo de oportunidad del capital (16%).

CAPITULO V: CONCLUSIONES

1. En general: Se concluye que el diseño e implementación de una solución de internet satelital Starlink permitió mejorar de manera integral la conectividad y la seguridad de navegación en la entidad ubicada en la zona rural de Loreto. La solución implementada integra adecuadamente el medio de transmisión, la tecnología de servicio y el equipamiento seleccionado, logrando una infraestructura de comunicaciones estable, con baja latencia y mecanismos de seguridad que garantizan la protección del tráfico de red. En consecuencia, se evidencia el cumplimiento del objetivo general del presente trabajo.
2. Medio de transmisión de datos: Se determina que el medio de transmisión de datos más adecuado para mejorar la conectividad y la seguridad de navegación en la entidad ubicada en la zona rural de Loreto es la tecnología satelital. Esta decisión se sustenta en la evaluación comparativa de alternativas como fibra óptica y radioenlaces, las cuales fueron descartadas debido a limitaciones técnicas, económicas y geográficas propias del entorno. En consecuencia, la solución satelital se consolida como la alternativa más viable, al garantizar conectividad estable, baja latencia y el cumplimiento de los requerimientos de ancho de banda y seguridad establecidos.
3. Tecnología de servicio satelital: Se determina que la tecnología de servicio de internet satelital más adecuada corresponde a la basada en satélites de órbita baja (LEO), específicamente mediante la tecnología Starlink. Esta selección se sustenta en la evaluación comparativa frente a soluciones satelitales tradicionales, evidenciándose un mejor

desempeño en términos de latencia, estabilidad y transmisión de datos. En consecuencia, la tecnología LEO se establece como la opción más adecuada para el entorno evaluado, al cumplir con los requerimientos de conectividad y seguridad definidos.

4. Equipamiento: Se determina que el equipamiento más adecuado para la implementación del servicio de internet satelital seguro con tecnología Starlink está conformado por un kit satelital Flat High Performance (antena, router y accesorios), complementado con un sistema de seguridad de red. Esta selección responde a la necesidad de cubrir tanto los requerimientos de conectividad como la implementación de mecanismos de seguridad, inexistentes en el equipamiento actual. En consecuencia, la integración de estos componentes permite garantizar la protección de la información, el control del tráfico de red y la aplicación de políticas de seguridad, optimizando el desempeño del servicio.
5. Solución implementada: Se determina que la solución diseñada e implementada mejora la conectividad y la seguridad de navegación en la entidad ubicada en la zona rural de Loreto. Este resultado se evidencia en las pruebas realizadas, donde se verificó una mejora en la disponibilidad del servicio, asegurando un acceso continuo a internet y mayor estabilidad en la conexión. Asimismo, se evidenció una optimización en las condiciones de navegación, fortaleciendo la seguridad del tráfico de datos. En consecuencia, la solución implementada mejora el acceso a internet en entornos rurales, incrementando la disponibilidad del servicio y fortaleciendo la continuidad operativa de la entidad.

CAPITULO VI: RECOMENDACIONES

1. En General: Se recomienda replicar la solución satelital Starlink en otras entidades ubicadas cerca de las zonas del proyecto o en otras zonas rurales con condiciones geográficas similares, considerando un enfoque integral que contemple el medio de transmisión, la tecnología de servicio y el equipamiento de seguridad.
2. Medio de transmisión de datos: Se recomienda priorizar la implementación de soluciones de conectividad satelital basadas en tecnología LEO, como Starlink, en entornos rurales con limitaciones geográficas, debido a su mayor viabilidad técnica y económica frente a alternativas como fibra óptica y radioenlaces, tal como se evidenció en el análisis comparativo del proyecto.
3. Tecnología de servicio satelital: Se recomienda evaluar de manera periódica la evolución de las tecnologías satelitales disponibles, considerando factores como latencia, disponibilidad, costos operativos y escalabilidad, con el fin de garantizar que la solución implementada continúe siendo la más eficiente y competitiva en el tiempo.
4. Equipamiento: Se recomienda seleccionar equipamiento de red complementándola con mecanismos avanzados de seguridad considerando escalabilidad y gestión centralizada con el fin de garantizar una navegación segura y proteger la información de la organización y así fidelizar al cliente.

5. Solución implementada: Se recomienda evaluar periódicamente indicadores clave como disponibilidad, latencia y desempeño de la red, con el fin de garantizar que las mejoras obtenidas en conectividad y seguridad se mantengan en el tiempo. Asimismo, es importante realizar mantenimientos preventivos y actualizaciones de las configuraciones de seguridad, asegurando la protección del tráfico de datos y la continuidad operativa de la entidad frente a posibles incidentes o degradaciones del servicio.

CAPITULO VII: REFERENCIAS BIBLIOGRÁFICAS

Abdelraheem A, M. (2025). *Satellite Communication Technologies for Smart Grid Applications: A Comprehensive Review of GEO VSAT and LEO Constellations*. Obtenido de ResearchGate: https://www.academia.edu/download/125361774/Satellite_Communication_Technologies_for_Smart_Grid_Application.pdf

Alcócer, A. (2018). Obtenido de <http://hdl.handle.net/20.500.12404/13790>

Balanis, C. (2005). *Antenna Theory*. John Wiley & Sons, Inc.

Bielecki, M., Hidders, J., Paredaens, J., Spielmann, M., Tyszkiewicz, J., & Bussche, J. V. (2010). The Navigational Power of Web Browsers. En *Theory of Computing Systems* (págs. 213-240). SPRINGER.

Binti, N., & Binti, N. (2024). *Data Transmission and Networking media*. Politeknik Tuanku Syed Sirajuddin.

Cabrera, A. (2025). Obtenido de <https://repositorio.utn.edu.ec/handle/123456789/17873>

Calderon, E. (2009). Obtenido de <https://bibdigital.epn.edu.ec/bitstream/15000/4193/1/CD-2563.pdf>

Cardenas, C., & Arteaga, K. (2016). Obtenido de <https://www.dspace.espol.edu.ec/bitstream/123456789/39080/1/T-106172%20CARDENAS-ARTEAGA.pdf>

CETIS. (2025). Obtenido de <https://www.cetis109.com/2025/6/latencia2.pdf>

Chen, Y., Ma, X., & Wu, C. (2024). The concept, technical architecture, applications and impacts of satellite internet: A systematic literature review. *Heliyon*.

CISCO. (2024). Obtenido de https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/what-is-a-router.html

COMEXPERU. (2025). Obtenido de <https://www.comexperu.org.pe/articulo/cierre-de-brechas-digitales-para-potenciar-la-productividad-peruana>

Española, D. d. (2024). *radioenlace | Definición | Diccionario de la lengua española*. Obtenido de Diccionario de la lengua española (DLE): <https://dle.rae.es/radioenlace?>

Fortinet. (2024). Obtenido de We're a Leader: 2024 Magic Quadrant™ for Enterprise Wired and Wireless LAN Infrastructure by Gartner®: <https://www.fortinet.com/blog/business-and-technology/leader-for-magic-quadrant-for-enterprise-wired-and-wireless-lan-infrastructure>

Fortinet. (2025). *What Is Network Security? Definition and Types*. Obtenido de Fortinet – CyberGlossary: <https://www.fortinet.com/lat/resources/cyberglossary/what-is-network-security>

Franco, J., & Bejarano, R. (2025). Obtenido de <https://hdl.handle.net/20.500.12952/10673>

Gonzáles, A., & Octavio, L. (2024). Obtenido de <https://doi.org/10.56712/latam.v5i5.2933>

Gonzales, G. (2018). Obtenido de <https://openaccess.uoc.edu/server/api/core/bitstreams/e9422e4a-cebf-4245-8f23-fc44b62c0008/content>

- Goodwin, M. (2025). *What Is Latency?* Obtenido de IBM Think: <https://www.ibm.com/think/topics/latency>
- IEEE. (1990). Glosario estándar IEEE de terminología de ingeniería de software. *IEEE*.
- IEEE. (1995). Standard Glossary of Computer Networking Terminology. *IEEE*.
- IETF. (1993). *FYI on "What is the Internet?"*. Obtenido de IETF Datatracker: <https://datatracker.ietf.org/doc/html/rfc1462>
- INEI. (2024). *INEI*. Obtenido de <https://www.gob.pe/institucion/inei/informes-publicaciones/6918505-encuesta-nacional-de-programas-presupuestales-2024>
- INEI. (2025). *INEI*. Obtenido de <https://www.gob.pe/institucion/inei/noticias/1195629-inei-58-9-de-los-hogares-del-pais-tiene-acceso-a-internet-en-el-primer-trimestre-de-2025>
- ISO. (2015). *Information technology-Vocabulary*. Obtenido de ISO: <https://www.iso.org/standard/63598.html>
- ISO. (2018). Obtenido de ISO/IEC 27000:2018: <https://www.iso.org/standard/73906.html>
- ITU-T. (2024). *G.652 – Characteristics of a single-mode optical fibre and cable*. Obtenido de ITU-T: <https://www.itu.int/rec/T-REC-G.652>
- Juárez, J., & Terrones, B. (2021). Obtenido de <https://repositorio.urp.edu.pe/handle/20.500.14138/4550>
- Kodheli, O., Maturo, N., Shankar, B., Merlano, J., & Chatzinotas, S. (2020). Satellite Communications in the New Space Era: A Survey and Future Challenges. *IEEE*.
- Liu, R., Zhang, C., & Song, J. (2018). *IEEE*. Obtenido de Line of Sight Component Identification and Positioning in Single Frequency

Networks Under Multipath Propagation:
<https://ieeexplore.ieee.org/abstract/document/8421080>

Loyaga, J. (2024). Obtenido de
<https://repositorio.esge.edu.pe/items/962ae7ea-8a9f-4751-9df0-664be5630d38>

Networks, P. (2025). *What Is Network Security?* Obtenido de Palo Alto Networks:
<https://www.paloaltonetworks.es/cyberpedia/what-is-network-security>

NIST. (2019). *Glossary of Key Information Security Terms*. Obtenido de NIST:
<https://csrc.nist.gov/glossary/term/data>

NIST. (2024). *Vulnerability – Glossary*. Obtenido de NIST:
<https://csrc.nist.gov/glossary/term/vulnerability>

NIST. (2025). *Threat – Glossary*. Obtenido de Computer Security Resource Center:
<https://csrc.nist.gov/glossary/term/threat>

OPSIPTTEL. (2025). Obtenido de <https://www.osiptel.gob.pe/portal-del-usuario/noticias/erestel-el-92-6-de-hogares-peruanos-tiene-acceso-a-internet-fijo-y-movil>

Shirey, R. (2007). *RFC 4949*. Obtenido de Internet Security Glossary, Version 2:
<https://www.rfc-editor.org/rfc/rfc4949>

Shirey, R. (2007). *RFC 4949 – Internet Security Glossary, Version 2*. Obtenido de RFC:
<https://www.rfc-editor.org/rfc/rfc4949>

Slotte, M. (2025). Obtenido de
https://lutpub.lut.fi/bitstream/10024/169233/1/bachelorsthesis_slotte_mattias.pdf

Society, N. G. (2024). Obtenido de
<https://education.nationalgeographic.org/resource/rural-area/>

Staff, E. (2024). *Network Connectivity – Glossary (o Network Connectivity)*.
Obtenido de DevX (DevX Technology Glossary):
<https://www.devx.com/terms/network-connectivity/>

Starlink. (2025). Obtenido de <https://www.starlink.com>

TechTarget. (2025). Obtenido de
<https://www.techtarget.com/searchnetworking/definition/network-availability>

UNESCO. (2025). Obtenido de
<https://databrowser.uis.unesco.org/resources/glossary/2385>

CAPITULO VIII: ANEXOS

ANEXO A

Plan de Trabajo

PLAN DE TRABAJO DE LA IMPLEMENTACION DEL SERVICIO SATELITAL	Duración (Días)	Comienzo	Fín
PROYECTO DE INTERNET SATELITAL SEGURO - LORETO (Sede Abelardo, Echenique y Napo)	63 Días	Día 0	Día 63
Fase de inicio			
Firma de contrato y registro de la oportunidad	1 Día	Día 0	Día 1
Fase de Planeación			
Documentación y transferencia del proyecto	2 Días	Día 2	Día 3
Planificación y elaboración del Plan de Trabajo	5 Días	Día 4	Día 8
Cliente revisa el Plan de Trabajo	3 Días	Día 9	Día 11
Cliente acepta el Plan de Trabajo	1 Días	Día 11	Día 11
Plan de Configuración de Router - (Sede Abelardo, Echenique y Napo)			
WIN revisa información de los requerimientos para la configuración del Satelital	11 Días	Día 4	Día 14
WIN enviará los resultados de la revisión realizada	1 Días	Día 15	Día 15
Cliente revisa los resultados y responde a WIN	7 Días	Día 16	Día 22
WIN completa el Plan de configuracion de Routers	11 Días	Día 23	Día 33
Plan de configuración completado	1 Días	Día 33	Día 33
Plan de Configuración del Kit Satelital - (Sede Abelardo, Echenique y Napo)			
WIN revisa información de los requerimientos para la configuración del Kit Satelital	11 Días	Día 4	Día 14
WIN enviará los resultados de la revisión realizada	1 Días	Día 15	Día 15
Cliente revisa los resultados y responde a WIN	7 Días	Día 16	Día 22
WIN completa el Plan de configuracion del Kit Satelital	11 Días	Día 23	Día 33
Plan de configuración completado	1 Días	Día 33	Día 33
Plan de Configuración del software de seguridad - (Sede Abelardo, Echenique y Napo)			
WIN revisa información de los requerimientos para la configuración del software de seguridad	11 Días	Día 4	Día 14
WIN enviará los resultados de la revisión realizada	1 Días	Día 15	Día 15
Cliente revisa los resultados y responde a WIN	7 Días	Día 16	Día 22
WIN completa el Plan de configuracion del software de seguridad	11 Días	Día 23	Día 33
Plan de configuración completado	1 Días	Día 33	Día 33
Fase de Aprovisionamiento, Instalación y Pruebas			
Instalación del Kit Satelital - Sede Abelardo			
Coordinación y gestión de los permisos internos de la sede del cliente	5 Días	Día 23	Día 27
Aprovisionamiento de equipamiento para instalación del Kit Satelital	11 Días	Día 23	Día 33
Traslado de equipamiento a las sedes del cliente	11 Días	Día 34	Día 44
Instalación, configuración y activación del Kit Satelital	1 Días	Día 45	Día 45
Firma del acta de instalación	1 Días	Día 45	Día 45
Instalación del Kit Satelital - Sede Echenique			
Coordinación y gestión de los permisos internos de la sede del cliente	5 Días	Día 23	Día 27
Aprovisionamiento de equipamiento para instalación del Kit Satelital	11 Días	Día 23	Día 33
Traslado de equipamiento a las sedes del cliente	11 Días	Día 34	Día 44
Instalación, configuración y activación del Kit Satelital	1 Días	Día 46	Día 46
Firma del acta de instalación	1 Días	Día 46	Día 46
Instalación del Kit Satelital - Sede Napo			
Coordinación y gestión de los permisos internos de la sede del cliente	5 Días	Día 23	Día 27
Aprovisionamiento de equipamiento para instalación del Kit Satelital	11 Días	Día 23	Día 33
Traslado de equipamiento a las sedes del cliente	11 Días	Día 34	Día 44
Instalación, configuración y activación del Kit Satelital	1 Días	Día 47	Día 47
Firma del acta de instalación	1 Días	Día 47	Día 47

Instalacion de Router - Sede Abelardo			
Aprovisionamiento de equipamiento para instalación del router	11 Días	Día 23	Día 33
Traslado de equipamiento a las sedes del cliente	11 Días	Día 34	Día 44
Instalación y configuración del equipo en la sede del cliente	1 Días	Día 45	Día 45
Configuración de Herramienta de Monitoreo	1 Días	Día 45	Día 45
Pruebas de funcionamiento de Herramienta de Monitoreo	1 Días	Día 45	Día 45
Firma del acta de instalación	1 Días	Día 45	Día 45
Instalacion de Router - Sede Echenique			
Aprovisionamiento de equipamiento para instalación del router	11 Días	Día 23	Día 33
Traslado de equipamiento a las sedes del cliente	11 Días	Día 34	Día 44
Instalación y configuración del equipo en la sede del cliente	1 Días	Día 46	Día 46
Configuración de Herramienta de Monitoreo	1 Días	Día 46	Día 46
Pruebas de funcionamiento de Herramienta de Monitoreo	1 Días	Día 46	Día 46
Firma del acta de instalación	1 Días	Día 46	Día 46
Instalacion de Router - Sede Napo			
Aprovisionamiento de equipamiento para instalación del router	11 Días	Día 23	Día 33
Traslado de equipamiento a las sedes del cliente	11 Días	Día 34	Día 44
Instalación y configuración del equipo en la sede del cliente	1 Días	Día 47	Día 47
Configuración de Herramienta de Monitoreo	1 Días	Día 47	Día 47
Pruebas de funcionamiento de Herramienta de Monitoreo	1 Días	Día 47	Día 47
Firma del acta de instalación	1 Días	Día 47	Día 47
Implementación del entorno virtual - Sede Abelardo, Echenique y Napo)			
Aprovisionamiento del entorno virtual	11 Días	Día 23	Día 33
Instalación y configuración del software de seguridad para el entorno virtual	11 Días	Día 34	Día 44
Instalacion del software de seguridad - Sede Abelardo			
Integración del software de seguridad hacia las sedes del cliente	1 Días	Día 45	Día 45
Pruebas de funcionamiento del software de seguridad	1 Días	Día 45	Día 45
Firma del acta de instalación	1 Días	Día 45	Día 45
Instalacion del software de seguridad - Sede Echenique			
Integración del software de seguridad hacia las sedes del cliente	1 Días	Día 46	Día 46
Pruebas de funcionamiento del software de seguridad	1 Días	Día 46	Día 46
Firma del acta de instalación	1 Días	Día 46	Día 46
Instalacion del software de seguridad - Sede Napo			
Integración del software de seguridad hacia las sedes del cliente	1 Días	Día 47	Día 47
Pruebas de funcionamiento del software de seguridad	1 Días	Día 47	Día 47
Firma del acta de instalación	1 Días	Día 47	Día 47
Fase de Cierre			
Pruebas de aceptación	9 Días	Día 48	Día 56
Documentación	4 Días	Día 56	Día 59
Fase Ejecución del Servicio y Puesta en Servicio			
Firma de Acta de Inicio de Servicio	4 Días	Día 60	Día 63

Figura A1 Plan de Trabajo de Implementación. Fuente: Elaboración propia a partir de los datos proporcionados por las áreas involucradas.

Nota: Se visualiza el plan de trabajo y la estimación de tiempo de acuerdo a los requerimientos de la solución propuesta, así como la participación del área Comercial, Preventa, Project Manager e Ingeniería-Técnica.

ANEXO B

Configuraciones de dispositivos

```

1  ##### GESTION #####
2  ACTIVACIÓN DE LA LICENCIA SECURITYK9
3  #Para tener gestión del equipo se levanta un túnel VPN IPSec, se deberá activar la licencia.
4  #La licencia es permanente
5  configure terminal
6  license boot securityk9
7  write
8  reload
9
10 #####
11 configure terminal
12 hostname CID-12345678
13 clock timezone pt -5 0
14 service password-encryption
15 !
16 no ip http server
17 no ip http secure-server
18 no ip bootp server
19 no cdp run
20 ip subnet-zero
21 ip classless
22 no ip source-route
23 no ip finger
24 !
25 ip name-server 190.12.72.XXX
26 ip name-server 190.12.72.XXX
27 ip domain name optical.com.pe
28 no ip domain lookup
29 no service dhcp
30 no service pad
31 !
32 service top-keepsalives-in
33 service top-keepsalives-out
34 service timestamps debug datetime msec
35 service timestamps log datetime msec localtime show-timezone
36 !
37 logging buffered 4096 informational
38 logging 190.12.64.XXX
39 logging console critical
40 logging trap notifications
41 ntp server 190.12.64.XXX
42 !
43 crypto key generate rsa general-keys modulus 1024
44 ip ssh version 2
45 ip ssh authentication-retries 3
46 ip ssh time-out 60
47 ip ssh port 2222 rotary 1
48 username operator privilege 15 secret soport30opticallyp # ingresar acceso local
49 enable secret soport30opticallyn3t
50 !
51 security passwords min-length 8
52 login block-for 180 attempts 3 within 60
53 security authentication failure rate 3 log
54 login quiet-mode access-class Gestion
55 login delay 4
56 login on-failure
57 !
58 crypto keyring KEYR1 # se crea un repositorio de claves
59 pre-shared-key address 191.98.136.XXX key CIR-12345678
60 #se apunta a una IP pública que apunta al concentrador para gestionar el equipo
61 crypto isakmp policy 10
62   encryption aes
63   hash sha256
64   authentication pre-share
65   group 5
66   exit
67   !
68 crypto isakmp key CIR-12345678 address 191.98.136.XXX #IP PUBLICA DEL CONCENTRADOR
69 crypto isakmp keepalive 10
70 crypto isakmp profile GESTION
71   keyring KEYR1
72   self-identity fqdn CIR-12345678
73   match identity user-fqdn CIR-12345678
74   initiate mode aggressive
75   exit
76   !
77 crypto ipsec transform-set Myset esp-aes esp-sha256-hmac
78   mode tunnel
79   exit
80   !

```

```

81 crypto map mymap 10 ipsec-isakmp
82 set peer 191.98.136.XXX #IP PUBLICA DEL CONCENTRADOR
83 set transform-set myset
84 set pfs group5
85 set isakmp-profile GESTION
86 match address VPN
87 exit
88 !
89 password encryption aes # aa para encriptar las contraseñas
90 key config-key password encrypt
91 CIR-12345678
92 CIR-12345678
93 !
94 interface GigabitEthernet0/0/0
95 description WAN-INTERNET
96 ip address dhcp
97 crypto map mymap
98 no shutdown
99 exit
100 !
101 interface Loopback0
102 ip address 10.45.0.XXX 255.255.255.XXX
103 description Gestion
104 exit
105 !
106 tacacs-server host 172.30.254.XXX
107 tacacs-server timeout 10
108 tacacs-server directed-request
109 tacacs-server key ? XXXXXXXXXXXXXXXX
110 ip tacacs source-interface loopback0
111 !
112 aaa new-model
113 aaa authentication fail-message # "Authentication Fails. Please try again, only 3
114 options" #
115 aaa authentication login default group tacacs+ local
116 aaa authentication login CONSOLE group tacacs+ local
117 aaa authentication login AUXILIAR group tacacs+ local
118 aaa authentication login VIRTUAL_TERMINAL group tacacs+ local
119 aaa authentication enable default group tacacs+ enable
120 aaa authorization exec default group tacacs+ if-authenticated
121 aaa authorization commands 1 default group tacacs+ none
122 aaa authorization commands 15 default group tacacs+ none
123 aaa accounting exec default start-stop group tacacs+
124 aaa accounting commands 1 default start-stop group tacacs+
125 aaa accounting commands 15 default start-stop group tacacs+
126 !
127 line vty 0 4
128 access-class SSH/Telnet in
129 login authentication VIRTUAL_TERMINAL
130 rotary 1
131 transport input telnet ssh
132 exit
133 !
134 access-list 25 permit 10.31.7.X 0.0.0.XXX
135 access-list 25 permit 190.12.72.XXX 0.0.0.X
136 access-list 25 deny any log
137 snmp-server ifindex persist
138 snmp-server community M0n1t0rC1i.0pt R0 25
139 !
140 ip access-list extended SSH/Telnet
141 permit tcp host 190.12.64.XX any eq 2222
142 permit tcp host 109.12.64.XXX any eq 2222
143 permit tcp 190.12.72.XXX 0.0.0.X any eq 2222
144 permit tcp host 10.3 any eq 2222
145 deny tcp any any eq 22
146 exit
147 !
148 ip access-list standard Gestion
149 permit 190.12.64.XXX
150 permit 190.12.64.XX
151 exit
152 !
153 ip access-list extended INTERNET
154 5 deny ip host 10.45.0.XXX host 190.12.64.XXX
155 5 deny ip host 10.45.0.XXX 10.32.1.XX 0.0.0.X
156 7 deny ip host 10.45.0.XXX 172.30.254.XX 0.0.0.XX
157 20 permit ip host 10.45.0.XXX any
158 !
159 ip access-list extended VPN
160 10 permit ip host 10.45.0.XXX 10.32.1.XX 0.0.0.X
161 20 permit ip host 10.45.0.XXX 172.30.254.XX 0.0.0.XX
162 30 permit ip host 10.45.0.XXX host 190.12.64.XXX
163 !

```

```

164 ip sla 1
165 icmp-echo 190.12.64.XXX source-ip 10.45.0.XXX
166 request-data-size 32
167 frequency 5
168 exit
169 ip sla schedule 1 life forever start-time now
170 !
171 ip sla 2
172 icmp-echo 172.30.254.X source-ip 10.45.0.XXX
173 request-data-size 32
174 frequency 5
175 exit
176 ip sla schedule 2 life forever start-time now
177 !
178 ip sla 3
179 icmp-echo 10.32.1.XX source-ip 10.45.0.XXX
180 request-data-size 32
181 frequency 5
182 exit
183 ip sla schedule 3 life forever start-time now
184 !
185 banner login #
186 TACACS - CLIENTE
187 *****
188 * NOTICE: This is a private network device. If you are not authorized *
189 * to connect or configure this device. disconnect at once! Actual *
190 * or attempted use, access, examination, or configuration change by *
191 * an unauthorized person will result in criminal and civil prosecution *
192 * to the full extent of the law. *
193 *****
194 #
195 line console 0
196 login authentication console
197 logging synchronous
198 !
199 banner exec
200
201
202
203
204
205
206
207
208
209 CLIENTE: NOMBRE DEL CLIENTE - CIRCUITO: 12345
210 !
211 interface VLAN1
212 no ip address
213 shutdown
214 and
215 write
216 *****SERVICIO*****
217 configure terminal
218 interface GigabitEthernet0/0/1
219 ip address 192.168.1.X 255.255.255.X
220 ip nat inside
221 no shutdown
222 description LAN
223 exit
224 !
225 interface GigabitEthernet0/0/0
226 ip nat outside
227 exit
228 !
229 ip access-list extended INTERNET
230 10 permit ip 192.168.1.X 0.0.0.XXX any
231 exit
232 !
233 ip nat inside source list INTERNET interface GigabitEthernet0/0/0 overload
234 !
235 ip dhcp pool DHCP-pool
236 default-router 192.168.1.X
237 dns-server 8.8.8.8 8.8.4.4
238 network 192.168.1.X 255.255.255.X
239 exit
240 !
241 ip dhcp excluded-address 192.168.4.X 192.168.55.XX
242 service dhcp
243 exit
244 !
245 write
246

```

```

247 #####CONFIGURACION VPN IPSEC CISCO#####
248 #CONFIGURACIONES###
249 #1 Configuración del repositorio de claves
250 crypto keyring KEVR2
251   pre-shared-key address 170.233.147.XXX key CIR-12345678
252 exit
253 !
254 #2 Configuración de la fase 1
255 crypto isakmp policy 20
256   encryption 3des
257   hash sha256
258   authentication pre-share
259   group 5
260 exit
261 !
262 crypto isakmp key CIR-12345678 address 170.233.147.XXX
263 #3 Configuración del perfil ISAKMP
264 crypto isakmp profile ISE-SAT
265   keyring KEVR2
266   self-identity fqdn CIR-12345678
267   match identity user-fqdn CIR-12345678
268   initiate mode aggressive
269 exit
270 !
271 #4 Configuración de la fase 2
272 crypto ipsec transform-set VPN-ISE esp-3des esp-sha256-hmac
273 mode tunnel
274 exit
275 !
276 #5 Configurar el mapa criptográfico con el mismo valor de la política previamente configurado en la fase 1
277 crypto map mymap 20 ipsec-isakmp
278   set peer 170.233.147.XXX
279   set transform-set VPN-ISE
280   set pfa group5
281   set isakmp-profile ISE-SAT
282   match address VPN-TO-ISE
283 exit
284 !
285 #6 Configuración de una lista de acceso
286 ip access-list extended VPN-TO-ISE
287   10 permit ip 192.168.XXX.0 0.0.0.XXX any
288 exit
289 !
290 #7 Consideración
291 #En la lista de acceso "INTERNET" debe retirarse la red LAN del CLIENTE
292 ip access-list extended INTERNET
293   5 deny ip host 10.45.0.XXX host 190.12.64.XXX
294   6 deny ip host 10.45.0.XXX 10.32.1.XX 0.0.0.X
295   7 deny ip host 10.45.0.XXX 172.30.254.XX 0.0.0.XX
296   20 permit ip host 10.45.0.XXX any
297
298 #Configuración de IP SLA
299 #Destino: IP PUBLICA DEL FIREWALL / ORIGEN: LAN DEL CLIENTE
300
301 ip sla 4
302   icmp-echo 190.102.144.XXX source-ip 192.168.5.X
303   request-data-size 32
304   frequency 5
305   ip sla schedule 4 life forever start-time now
306
307 #DESTINO: DNS de GOOGLE 8.8.8.8 / ORIGEN: LAN DEL CLIENTE
308
309 ip sla 5
310   icmp-echo 8.8.8.8 source-ip 192.168.5.X
311   request-data-size 32
312   frequency 5
313   ip sla schedule 5 life forever start-time now
314
315 #Configuración a nivel LAN
316 interface GigabitEthernet0/0/1
317   ip address 192.168.1.XX 255.255.255.X
318   description LAN
319 exit
320 !
321 ip dhcp pool DHCP-pool
322   default-router 192.168.1.X
323   dns-server 8.8.8.8 8.8.4.4
324   network 192.168.1.X 255.255.255.X
325 exit
326 !
327 ip dhcp excluded-address 192.168.1.XX 192.168.1.XX
328 service dhcp
329 exit
330 !
331 write
332

```

Figura B1 Configuración CPE Router Cisco. Fuente: Elaboración propia a partir de los datos proporcionados por el área de Ingeniería-Técnica.

Nota: Se visualiza la configuración de gestión, configuración de servicio y la configuración VPN IPSEC del equipamiento CPE Router Cisco de acuerdo a los requerimientos de la solución propuesta.