Universidad Nacional Federico Villarreal

VRIN | VICERRECTORADO DE INVESTIGACIÓN

**FACULTAD DE INGENIERÍA ELECTRÓNICA E INFORMÁTICA**

# IMPLEMENTACIÓN DE INTERNET CON VPN IPSEC SOBRE TECNOLOGÍA STARLINK PARA DOS SEDES REMOTAS DE LA EMPRESA CR TECHNOLOGY

**Línea de investigación:**
**Sistemas eléctricos y electrónicos**

Trabajo de Suficiencia Profesional para optar el Título Profesional de Ingeniero de Telecomunicaciones


**Autor**

Reque Flores, Cristian Antony

**Asesor**

Cernaque Vera, Julio Cesar

ORCID: 0009-0005-0855-5152


**Jurado**

Solis Fonseca, Justo Pastor

Flores Masias, Edward Jose

Peña Carrillo, Cesar Serapio

**Lima - Perú**

**2026**

# IMPLEMENTACIÓN DE INTERNET CON VPN IPSEC SOBRE TECNOLOGÍA STARLINK PARA DOS SEDES REMOTAS DE LA EMPRESA CR TECNOLOGY

INFORME DE ORIGINALIDAD

| 4% | 4% | 0% | 0% |
|---|---|---|---|
| INDICE DE SIMILITUD | FUENTES DE INTERNET | PUBLICACIONES | TRABAJOS DEL ESTUDIANTE |

FUENTES PRIMARIAS

| | | |
|---|---|---|
| 1 | www.slideshare.net<br>Fuente de Internet | <1% |
| 2 | www.researchgate.net<br>Fuente de Internet | <1% |
| 3 | www.consumer.es<br>Fuente de Internet | <1% |
| 4 | 2022.jnic.es<br>Fuente de Internet | <1% |
| 5 | repositorio.utn.edu.ec<br>Fuente de Internet | <1% |
| 6 | chile.emc.com<br>Fuente de Internet | <1% |
| 7 | www.cverdad.org.pe<br>Fuente de Internet | <1% |
| 8 | doku.pub<br>Fuente de Internet | <1% |
| 9 | idoc.pub<br>Fuente de Internet | <1% |
| 10 | repository.unad.edu.co<br>Fuente de Internet | <1% |
| 11 | Submitted to Corporación Universitaria del Caribe<br>Trabajo del estudiante | <1% |
| 12 | repositorio.utm.edu.ec | |

FACULTAD DE INGENIERIA ELECTRONICA E INFORMATICA

# IMPLEMENTACIÓN DE INTERNET CON VPN IPSEC SOBRE TECNOLOGÍA STARLINK PARA DOS SEDES REMOTAS DE LA EMPRESA CR TECHNOLOGY

Línea de Investigación:
Sistemas eléctricos y electrónicos
Modalidad de Suficiencia Profesional para optar el Título Profesional de Ingeniero de Telecomunicaciones

Autor
Reque Flores, Cristian Antony

Asesor
Cernaque Vera, Julio Cesar
ORCID: 0009-0005-0855-5152

Jurado
Solis Fonseca, Justo Pastor
Flores Masias, Edward Jose
Peña Carrillo, Cesar Serapio

Lima – Perú
2026

# ÍNDICE

# ÍNDICE DE TABLAS

# ÍNDICE DE FIGURAS

## Resumen

**Objetivo**: El presente informe tuvo como finalidad describir la implementación una solución de Internet con VPN IPsec sobre tecnología Starlink para dos sedes remotas de la empresa CR Technology. Dichas sedes carecían de conectividad a Internet y presentaban limitaciones en el acceso a servicios de telecomunicaciones convencionales, por lo que la solución permitió su interconexión con la sede principal ubicada en Surco, la cual contaba de un servicio de Internet dedicado con seguridad perimetral on-premise. **Método**: El estudio fue de tipo descriptivo y aplicado. Se documentó la implementación física y lógica de la solución, así como las gestiones técnicas y operativas requeridas para su despliegue. **Resultado:** La solución permitió establecer una interconexión entre las sedes remotas y la sede principal, habilitando el acceso controlado a recursos corporativos y la navegación a Internet mediante el uso de la infraestructura de seguridad existente en Surco, aun cuando las sedes remotas operan bajo el esquema CGNAT del servicio Starlink, mediante la iniciación del túnel VPN desde dichas sedes hacia la sede principal. **Conclusiones:** Se concluyó que la implementación de Internet con VPN IPsec sobre tecnología Starlink permitió establecer una conectividad estable en sedes remotas de difícil acceso, garantizando la interconexión con la sede principal y la salida a Internet centralizada bajo un esquema de seguridad perimetral. La arquitectura propuesta demostró ser replicable en nuevas sedes remotas con características similares, optimizando el uso de la infraestructura existente y manteniendo un control unificado de la seguridad y del tráfico de red.

*Palabras clave:* Starlink, VPN IPsec, seguridad perimetral, CGNAT

## Abstract

**Objective**: This report aimed to describe the implementation of an IPsec VPN internet solution over Starlink technology for two remote sites of CR Technology. These sites lacked internet connectivity and had limited access to conventional telecommunications services, so the solution enabled their interconnection with the main office located in Surco, which had a dedicated internet service with on-premises perimeter security. **Method**: The study was descriptive and applied. The physical and logical implementation of the solution was documented, as well as the technical and operational steps required for its deployment. **Result**: The solution allowed for an interconnection between remote sites and the main headquarters, enabling controlled access to corporate resources and internet browsing through the use of the existing security infrastructure in Surco, even though the remote sites operate under the CGNAT scheme of the Starlink service, by initiating the VPN tunnel from these sites to the main headquarters. **Conclusions:** It was concluded that implementing IPsec VPN internet access over Starlink technology enabled stable connectivity in remote, hard-to-reach locations, guaranteeing interconnection with the main office and centralized internet access under a perimeter security scheme. The proposed architecture proved replicable in new remote locations with similar characteristics, optimizing the use of existing infrastructure and maintaining unified control over security and network traffic.


*Keywords:* Starlink, IPsec VPN IPsec, perimeter security,

# I. INTRODUCCIÓN

## 1.1. Trayectoria del autor

Profesional en las Telecomunicaciones, Redes y Ciberseguridad con nivel intermedio en el idioma inglés, con estudios, certificaciones internacionales y destreza en configuración, brindar soluciones, liderando proyectos Estado, en diferentes medios de transmisión y soluciones con protocolos avanzados. Cuento con experiencia comprobada en el sector de Telecomunicaciones en diferentes posiciones como Practicante, Operador e ingeniero NOC, especialista en Ciberseguridad e ingeniería realizando trabajo en equipo, basado en KPI y cumplimiento de SLA con diferentes Áreas.

## 1.2. Descripción de la Empresa / Institución

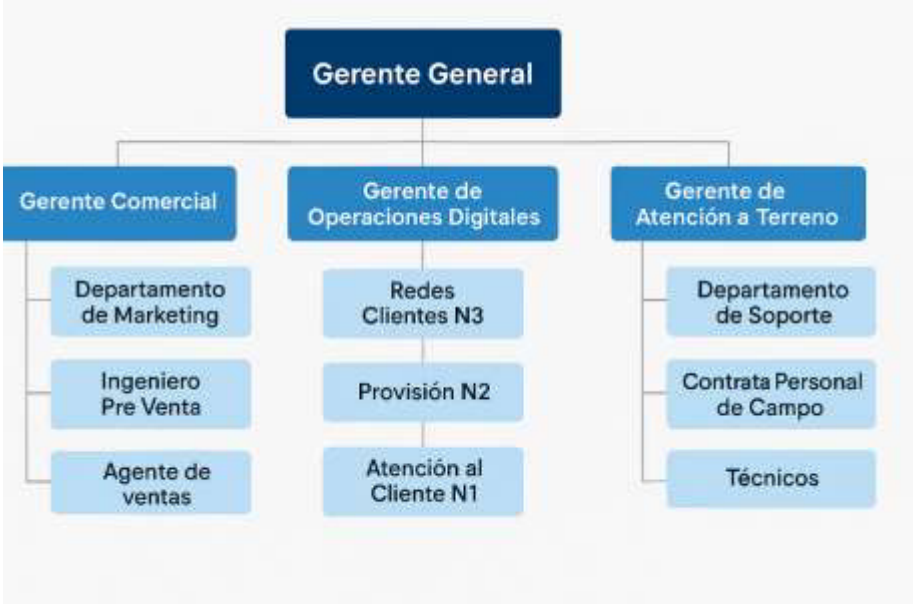
Entel Perú, es una empresa del grupo Entel Chile que inició operaciones en nuestro país en 2014, ofreciendo diversos servicios de telecomunicaciones. Los servicios que brinda son cloud, housing, hosting, red de datos, internet dedicado, seguridad perimetral, telefonía analógica y digital.

## 1.3. Organigrama de la Empresa

El organigrama del área Entel, dedicado a servicios para empresas es el siguiente:

**Figura 1**

*Organigrama de la empresa*




*Nota.* Elaboración propia (s.f.)

## 1.4. Áreas y funciones desempeñadas

A continuación, se detalla las funciones desempeñadas en el transcurso de mi vida profesional:

Practicante Profesional NOC (septiembre 2017 – febrero 2018): Fui responsable de las migraciones de servicios VOIP a nueva plataforma digital, brindando la mejora correspondiente a los clientes finales. Estuve a cargo de brindar soporte al personal de campo durante las migraciones

de equipamiento. Asimismo, fui responsable del levantamiento de información de los clientes según lo programado por el área supervisora.

Operador NOC (marzo 2018 – octubre 2020): Brindé atención de migraciones y solicitudes post – venta de los clientes de la red fija. Brindé soporte de segundo nivel a personal de instalaciones. También brindé atención de provisión, modificación y desinstalaciones de servicios relacionados a cliente de la red fija a través de sistema de órdenes de trabajo.

Ingeniero Residente Falabella (noviembre 2020 – noviembre 2021): Durante mi empleo como ingeniero residente realicé actividades como coordinación y soporte remoto con áreas de ingeniería e instalaciones para la resolución de averías en redes de datos y/o transmisión de clientes nivel diamante con soluciones especiales. También realicé diseño de proyectos de integración de clientes internos y externos en el backbone MPLS/IP. Además, realicé la investigación, priorización, diagnóstico, resolución y recuperación de los incidentes presentados en la red que afecten a clientes importantes. Realicé reporte de disponibilidad mensual al cliente Falabella y también fui el encargado de actualizar y revisar la documentación para el área TAC asociado a la atención de clientes.

Ingeniero SOC & VoIP (noviembre 2021 – febrero 2023): Durante mi labor como Ingeniero SOC & VoIP, desempeñé funciones de configuración, administración y troubleshooting de soluciones de seguridad y redes, utilizando tecnologías Fortinet, Sophos y firewalls Huawei USG. Especialista en soporte de soluciones de conectividad y seguridad a clientes Top y del Estado, asegurando la protección de la infraestructura frente a amenazas informáticas y garantizando la continuidad operativa de los servicios.

Llevé a cabo el control y seguimiento de incidencias relacionadas con los clientes, proponiendo mejoras y soluciones complejas en la red. Participé en reuniones técnicas y conferencias con proveedores y clientes de alto valor, así como en la elaboración de reportes mensuales del área. También realicé tareas de administración de servidores HP ProLiant DL360, levantamiento y operación de centrales VoIP en la nube, y gestión de soluciones de respaldo y almacenamiento de endpoints en la nube mediante Acronis.

Network & Cybersecurity Specialist (febrero 2023 – julio 2024): Durante mi desempeño como Network & Cybersecurity Specialist, realicé actividades de configuración, administración y troubleshooting de soluciones de seguridad y redes, utilizando tecnologías Fortinet (FortiGate, FortiAnalyzer, FortiAP, FortiSwitch y FortiManager), Sophos y firewalls Huawei USG. Fui responsable del diseño e implementación de soluciones de conectividad y ciberseguridad para clientes Top y del Estado, garantizando la protección de la información frente a amenazas como ataques cibernéticos, malware, ransomware y vulnerabilidades de seguridad tanto en entornos físicos como en la nube. Finalmente, estuve a cargo de la definición, organización y optimización del área de ciberseguridad, liderando un equipo de especialistas y manteniendo contacto directo con fabricantes como Fortinet, Sophos y Huawei. Fui responsable del análisis, desarrollo y ejecución de proyectos estratégicos de ciberseguridad para nuevos servicios dirigidos a clientes Top.

Ingeniero Líder de Preventa (agosto 2024 – noviembre 2025): Durante mi desempeño como Ingeniero Líder de Preventa en FIBERTEL PERÚ, fui responsable del diseño y desarrollo de soluciones tecnológicas integrales para el sector corporativo y empresarial, abarcando redes

LAN y Wireless LAN, seguridad perimetral, telefonía y servicios cloud. Participé en la preparación técnica de demostraciones y pruebas de concepto (PoC), así como en el desarrollo de proyectos de videovigilancia basados en tecnología GPON. Gestión de oportunidades comerciales y elaboré propuestas técnico-económicas para clientes de distintos sectores, incluyendo administración pública y entidades financieras, integrando soluciones de partners y fabricantes líderes como Fortinet, Palo Alto, Cisco, Huawei y Microsoft. Realicé el análisis y evaluación de Términos de Referencia (TDR) de proyectos gubernamentales, determinando su viabilidad técnica y estratégica.

# II. DESCRIPCIÓN DE UNA ACTIVIDAD ESPECÍFICA

## 2.1. Planteamiento del Problema

### *2.1.1. Determinación del problema*

Actualmente, uno de los principales retos que comparten la dependencia de la conectividad para el cumplimiento de sus objetivos organizacionales. Muchas de estas organizaciones tienen presencia en diversas ubicaciones geográficas, lo que genera la necesidad de mantener una conectividad permanente y confiable que permita el acceso a internet, así como el intercambio seguro y eficiente de información entre sus distintas sedes.

En este contexto, la implementación de una solución de conectividad basada en túneles VPN IPsec sobre tecnología de acceso a Internet satelital Starlink constituye una alternativa eficiente para empresas del sector retail ubicadas en zonas rurales o de difícil acceso a infraestructura de telecomunicaciones tradicionales. Esta solución permite brindar conectividad a sedes remotas mediante Internet satelital y, a su vez, centralizar la salida a Internet a través de la sede principal, donde se dispone de una dirección IP pública fija y de mecanismos de seguridad perimetral, garantizando un mejor control y gestión del tráfico de red.

Las sedes remotas de la empresa CR Technology se encuentran ubicadas en las siguientes direcciones:

- Sede remota 1: Distrito de Lurigancho, Chosica.
- Sede remota 2: Distrito de Ventanilla, provincia constitucional del Callao.

La empresa CR Technology dispuso de un servicio de Internet dedicado en alta disponibilidad en su sede principal ubicada en Surco, el cual cuenta con seguridad perimetral implementada mediante un equipo FortiGate 100F. Dicho servicio funciona como el único punto de salida a Internet para la sede principal y para algunas sedes remotas que ya cuentan con enlaces de datos dedicados. Todos los servicios de conectividad mencionados utilizaron infraestructura de transporte basada en fibra óptica.

Sin embargo, se identificó dificultades significativas en la conectividad de dos de sus sedes remotas, las cuales desde su apertura no contaba con ningún tipo de servicio de acceso a Internet y tampoco interconexión con la sede principal ubicada en Surco. Esta situación limitó el desarrollo adecuado de las operaciones, afectando la gestión centralizada de la información y de los recursos de la empresa.

Ambas sedes remotas requirieron conectividad permanente para el monitoreo de sus sistemas de videovigilancia, compuestos por tres cámaras por sede, los cuales deben ser supervisados desde la sede principal. La ausencia de conectividad impidió la visualización remota en tiempo real, reduciendo los niveles de control y seguridad de los almacenes. Asimismo, cada sede cuenta con dos usuarios, uno del área de seguridad y otro del área administrativa, que necesitaban acceso básico a Internet para el desempeño de sus funciones diarias, lo cual sin un servicio de conectividad no fue posible.

Las ubicaciones geográficas de estas sedes representan una dificultad adicional, ya que se encuentran en zonas rurales o de difícil acceso a infraestructura de telecomunicaciones. La disponibilidad de servicios tradicionales como fibra óptica o radioenlaces es limitada o inexistente,

y cuando están disponibles, los costos de implementación y operación resultaron ser elevados. Por otro lado, la cobertura de redes móviles LTE en estas zonas es inestable y no ofreció el ancho de banda ni la confiabilidad necesarios para soportar aplicaciones sensibles al retardo y a la pérdida de paquetes, como la transmisión de video.

Como consecuencia, la falta de una solución de conectividad adecuada generó riesgos operativos, limitó la supervisión remota, afectando la eficiencia administrativa y comprometiendo la continuidad operativa de la empresa en dichas sedes remotas.

### *2.1.2. Problema Principal*

¿Cómo se pudo implementar una solución de Internet mediante VPN IPSEC sobre tecnología Starlink para garantizar conectividad confiable en las dos sedes remotas de la empresa CR Technology?

### *2.1.3. Problemas secundarios*

¿De qué manera la implementación de Internet mediante VPN IPSEC sobre Starlink facilitó la interconexión de las dos sedes remotas con la sede principal de la empresa CR Technology?

¿Cuáles fueron los requerimientos técnicos y operativos para implementar Internet mediante VPN IPSEC sobre Starlink en las dos sedes remotas de CR Technology?

¿Cómo se pudo asegurar un desempeño óptimo y confiable en la implementación de Internet mediante VPN IPSEC sobre Starlink en las dos sedes remotas de CR Technology?

### *2.1.4. Objetivo principal*

Implementar una solución de Internet mediante VPN IPSEC sobre tecnología Starlink que permitiera garantizar conectividad confiable en las dos sedes remotas de la empresa CR Technology y asegurar su interconexión con la sede principal.

### *2.1.5. Objetivos secundarios*

Analizar y diseñar la interconexión de las dos sedes remotas con la sede principal mediante Internet con VPN IPSEC sobre tecnología Starlink, asegurando la transmisión confiable de datos.

Determinar los requerimientos técnicos y operativos necesarios para la implementación de Internet mediante VPN IPSEC sobre Starlink en las dos sedes remotas de CR Technology.

Realizar análisis y simulaciones que permitieran garantizar un desempeño óptimo de la conexión mediante VPN IPSEC sobre Starlink, donde se aseguró la continuidad operativa y la supervisión centralizada desde la sede principal.

### *2.1.6. Justificación*

**2.1.6.1. Justificación práctica.** En la actualidad, la conectividad a Internet se ha convertido en un elemento fundamental para la operación continua de las empresas, especialmente

aquellas que cuentan con sedes remotas ubicadas en zonas de difícil acceso a infraestructura de telecomunicaciones. En este contexto, la empresa CR Technology presentó la necesidad de tener una solución que garantizara acceso a Internet centralizado para sus dos sedes remotas, permitiendo la transmisión eficiente de datos y la supervisión de sus operaciones desde la sede principal.

**2.1.6.2. Justificación teórica.** En el presente estudio se examinaron las tecnologías utilizadas, las ventajas que ofrecen y el proceso de implementación de la solución propuesta, con el propósito de sustentar teóricamente la elección de la solución de conectividad basada en VPN IPsec sobre enlaces Starlink.

**2.1.6.3. Justificación metodológica.** El estudio realizado resultó viable, ya que permitió plantear una solución práctica a la falta de conectividad que presentaban las dos sedes remotas de la empresa CR Technology. A partir del análisis de la infraestructura existente, la identificación de requerimientos técnicos y operativos, y la implementación de una solución de Internet mediante VPN IPSEC sobre tecnología Starlink, fue posible establecer un procedimiento claro y replicable para entornos empresariales con limitaciones de acceso a servicios de telecomunicaciones tradicionales.

Asimismo, la metodología empleada en esta investigación puede servir como referencia para futuros proyectos de implementación de conectividad en sedes remotas, considerando aspectos como el diseño lógico y físico de la red, la configuración de túneles VPN IPSEC, la gestión centralizada de la seguridad perimetral y la validación del desempeño de la solución. De esta manera, el estudio aportó un enfoque metodológico que puede ser adaptado a empresas que

requieran garantizar acceso a Internet en ubicaciones rurales o de difícil acceso, utilizando tecnologías alternativas como Starlink.

### *2.1.7. Alcances y limitaciones*

**2.1.7.1. Alcances.** El presente trabajo de investigación se enfocó en la implementación de una solución de Internet mediante una VPN IPsec sobre tecnología Starlink, aplicada a dos sedes remotas de una empresa de CR Technology.

El alcance del estudio incluyó el diseño, la implementación y la validación de la solución propuesta, considerando tanto los aspectos lógicos como físicos de la infraestructura de red. También se describieron los procedimientos seguidos durante la implementación, la configuración de los dispositivos de red involucrados y los recursos tecnológicos utilizados.

El proyecto se limitó a evaluar la comunicación entre las dos sedes mencionadas, sin considerar su extensión a otras sucursales ni la optimización de servicios adicionales distintos al establecimiento del túnel VPN IPsec y su funcionamiento sobre la tecnología Starlink.

**2.1.7.2. Limitaciones.**

***A. Espacial.*** La implementación del proyecto se limitó a las dos sedes remotas de la empresa CR Technology, las cuales fueron consideradas como unidades de análisis para el desarrollo y validación de la solución propuesta. El estudio no contempló la implementación en otras sedes, ni a la ampliación de la solución hacia organizaciones o terceros ajenos al proyecto.

Por razones de confidencialidad y restricciones de información técnica, no se profundizó en la infraestructura interna del proveedor de servicios de conectividad ni en los detalles operativos externos a las instalaciones de la CR Technology.

***B. Temporal.*** El tiempo estimado para la ejecución del proyecto se dividieron en las siguientes etapas:

- Etapa de compra e importación de equipos: 14 días
- Etapa de planificación y diseño de la solución: 4 días
- Etapa de implementación física: Instalación de antenas y planta interna (4 días)
- Etapa de configuración lógica: 2 días

Debido a las limitaciones de tiempo para el desarrollo del proyecto, no se incluyeron posibles retrasos por factores externos como problemas de logística, cambios inesperados en la infraestructura o dificultades en la capacitación del personal.

***C. Social.*** La implementación del proyecto se realizó en colaboración con el personal de la empresa CR Technology, limitándose al conocimiento de los colaboradores asignados a la administración de la red interna. La recopilación de información sobre la segmentación de la red fue dependiente a la disponibilidad del personal y de la capacidad para acceder a la información necesaria.

No se consideraron factores sociales como la capacitación del personal a largo plazo ni la integración de nuevas tecnologías en áreas externas a la empresa.

## 2.2. Marco Teórico

### *2.2.1. Antecedentes bibliográficos*

Bilbao (2024) en su Trabajo de Fin de Máster titulado “Diseño, despliegue y análisis del sistema satelital Starlink como red de acceso”, analiza la viabilidad del sistema Starlink como una solución de conectividad a Internet para zonas rurales y de difícil acceso, donde las infraestructuras tradicionales como la fibra óptica o las redes móviles 4G y 5G resultan técnica o económicamente imposible. El estudio aborda las limitaciones históricas de las comunicaciones satelitales, tales como la alta latencia, las pérdidas de paquetes y los elevados costos de infraestructura, por lo que evalúa cómo el grupo de satélites de baja órbita (LEO) de Starlink permite superar este tipo de inconvenientes. Asimismo, se analizan las ventajas técnicas del sistema, destacando la mejora en velocidades de transmisión y la reducción significativa de la latencia en comparación con sistemas satelitales convencionales. Como resultado, el trabajo concluye que Starlink representa una alternativa innovadora y viable para que los proveedores de servicios de Internet (ISP) que puedan ofrecer conectividad de banda ancha confiable a usuarios ubicados en zonas remotas.

Lithman (2025), en su tesis titulada “Implementación de una red móvil 4G con Starlink y Zerotier para mejorar la conectividad en la comunidad Sensa – Cusco”, tuvo como objetivo implementar una solución de conectividad móvil de cuarta generación en una zona rural con limitada infraestructura de telecomunicaciones, donde únicamente existía la cobertura 2G. El estudio abarca la problemática de acceso restringido a servicios digitales esenciales debido a factores geográficos adversos y a la nula inversión en infraestructura tecnológica. Para ello, se propuso el uso del servicio satelital Starlink como medio de transporte de datos y la plataforma Zerotier como mecanismo de interconexión segura, permitiendo mejorar la calidad del servicio

móvil y fomentar la inclusión digital y financiera de la comunidad. La investigación se desarrolló bajo un enfoque cuantitativo experimental, estructurado en diversas fases que incluyeron la planificación, el diseño, la implementación y la optimización de la red. Los resultados evidenciaron mejoras significativas en los indicadores de velocidad, latencia y estabilidad, así como un incremento marcado en la satisfacción de los usuarios y en el uso de servicios digitales, concluyendo que la integración de tecnologías satelitales y redes privadas virtuales constituye una alternativa eficaz para reducir la brecha digital en zonas rurales de difícil acceso.

Conza (2009), en su tesis titulada “Diseño e implementación de un prototipo de DMZ y la interconexión segura mediante VPN utilizando el Firewall Fortigate 60”, desarrollada para optar el título de Tecnóloga en Análisis de Sistemas Informáticos, tuvo como objetivo general proteger la red interna de una organización mediante la separación de los servicios privados de la red pública y asegurar la transferencia de tráfico a través de una zona desmilitarizada (DMZ) y una red privada virtual (VPN). La investigación abordó el análisis de los métodos de ataque utilizados por intrusos y hackers, así como la evaluación de distintas herramientas de seguridad disponibles en el mercado para la protección de redes privadas y la transmisión segura de información sobre redes públicas. También, se analizaron alternativas de solución para la implementación de redes perimetrales seguras, se establecieron políticas de seguridad y se diseñó una solución funcional basado en un Firewall FortiGate 60. El estudio justificó la necesidad de contar con mecanismos de comunicación segura que permitan el acceso remoto a los usuarios y la interconexión entre una o múltiples redes LAN, destacando la importancia de la protección de los datos durante su transmisión. Los resultados demostraron que la implementación de DMZ y VPN constituye una solución efectiva

para fortalecer la seguridad perimetral y garantizar la confidencialidad, integridad y disponibilidad de la información.

Espinoza (2025), en su trabajo académico titulado “VPN IPsec con FortiGate: laboratorio de seguridad perimetral”, desarrollado en el marco de formación técnica en SENATI, tuvo como objetivo implementar túneles VPN IPsec orientados a fortalecer la seguridad perimetral de redes empresariales. El estudio se centró en la configuración de túneles IPsec de tipo site-to-site, la integración de políticas de firewall con el servicio de VPN IPsec y la implementación de enrutamiento estático para garantizar la correcta comunicación entre las redes remotas a través de una IP pública. En el desarrollo teó (Danny, 2025)rico, se abordaron los fundamentos de las redes privadas virtuales como mecanismo para establecer comunicaciones seguras sobre infraestructuras de WAN públicas, destacando el uso del protocolo IPsec como conjunto de estándares que aseguran la confidencialidad, integridad y autenticación de los datos transmitidos. El trabajo permitió validar, mediante un entorno de laboratorio, la eficacia del uso de firewalls FortiGate en la protección de las comunicaciones entre redes locales, evidenciando que la implementación de VPN IPsec constituye una solución confiable y ampliamente utilizada para la interconexión segura de redes en escenarios empresariales.

### *2.2.2. Bases Teóricas*

**2.2.2.1. ¿Qué es una red?** La progresión sigue en aumento y la variedad de dispositivos conectados es cada vez mayor. Sólo el tiempo nos dirá la manera en que la gran red se irá acomodando a las distintas expectativas (Liberatori, 2018).

Existen diversas maneras de analizar las redes de comunicación de datos. Las redes brindan las mismas funciones básicas para transferir un mensaje desde un emisor hasta un receptor. Estas redes pueden utilizar diversos hardware y software que al trabajar en conjunto logran cumplir con sus funciones (Fitzgerald, 2003).

Una manera de lograr el análisis de las redes es descomponiendo el conjunto completo de las funciones en capas las cuales se pueden definir por separado. Existen diversas maneras de diseñar las capas de la red y los modelos más conocidos son el Modelo de Referencia de Interconexión de Sistemas Abiertos (OSI) y el modelo de internet (Fitzgerald, 2003).

**2.2.2.2. Modelo OSI.** Con la finalidad de reducir la complejidad de su diseño, las redes están jerarquizadas en capas o niveles. El modelo OSI es definida como un marco de referencia basado en una propuesta desarrollada por la International Organization for Standardization (ISO) para la definición de arquitecturas de interconexión de sistemas de comunicaciones y fue revisada en el año 1995 (Tanenbaum & Wetherall, 2012). Este modelo el cual tiene el nombre de Modelo de Interconexión de Sistemas Abiertos posee siete capas. Cada capa cimenta su funcionalidad en la capa de nivel inferior. Las capas inferiores desarrollan competencias más primarias y los detalles de implementación no son visibles para las capas superiores. El presente modelo definió funciones principales a cada una de las 7 capas (Liberatori, 2018)**.**

Capa Física: En esta capa se especifica o define el medio de transmisión a utilizar, se determina la forma de adaptar los bits generados al propio medio. Esta capa tiene como funciónlas técnicas de codificación y señalización (banda pase o pasa-banda) como también de las

especificaciones de funcionamiento u operación de cables, conectores, transceptores, tarjeta de interfaz de red y de todo lo relacionado con la transmisión y recepción de los datos. Adicional a lo mencionado esta capa describe la topología dela red y el tipo de transmisión (Liberatori, 2018).

Capa de Enlace de Datos: su función es presentar a la capa de Red un enlace físico seguro, independiente de la Capa Física existente. En el modelo OSI esta capa se divide en dos: la subcapa de Control de Acceso al Medio (MAC) quien se encarga de definir la forma de adaptación para el acceso almedio específico que se encuentre por debajo y la subcapa de Control Lógico de Enlace (LLC) la cual se puede definir como una clase de interfaz entre la MAC y la Capa de Red, independiente del medio físico, esta subcapa provee servicios a la Capa 3 y a su vez oculta detalles de diferentes posibilidades a nivel de Capa 2 (Liberatori, 2018).

Capa de Red: Aquí se define como conectar redes entre sí. La capa de red se encarga de que se pueda realizar la comunicación entre dispositivos aun cuando se encuentren en distintas redes, a diferencia de la capa de Enlace que se encarga de la comunicación entre dispositivos de la misma red. Otra función primordial es el enrutamiento, el cual se puede definir como la posibilidad de manejar paquetes provenientes de diferentes fuentes, observar campos a nivel de Capa de Red y enviarlos hacia la red a la que deben llegarde manera consistente (Liberatori, 2018).

En la arquitectura del modelo OSI se tienen sistemas finales que corren aplicaciones y sistemas intermedios que tienen como función el enrutamiento. Cada sistema posee un identificador único en la red y se necesita una funcionalidad de red en todos por este motivo cada dispositivo lleva asociado una dirección lógica la cual nos permitirá la comunicación con

dispositivos fuera de la red local. Las unidades de datos de protocolo de este nivel se suelen conocer como paquetes (Liberatori, 2018).

Capa de Transporte: Es la primera capa end-to-end, en esta capa se brinda un control para el transporte de datos entre los sistemas finales de comunicación. La función principal de la capa de transporte es mantener un acceso continuo y uniforme a la red con el objetivo de proteger el nivel superior de los mecanismos de las redes subyacentes, debido a ello esta capa cuenta con las funcionalidades para manejo de errores, medición de retardo máximo permitido en una conexión, marcado de tráfico para brindar prioridad, control de fallas y control de flujo. La unidad de datos de protocolo de esta capa es conocido como segmentos (Liberatori, 2018).

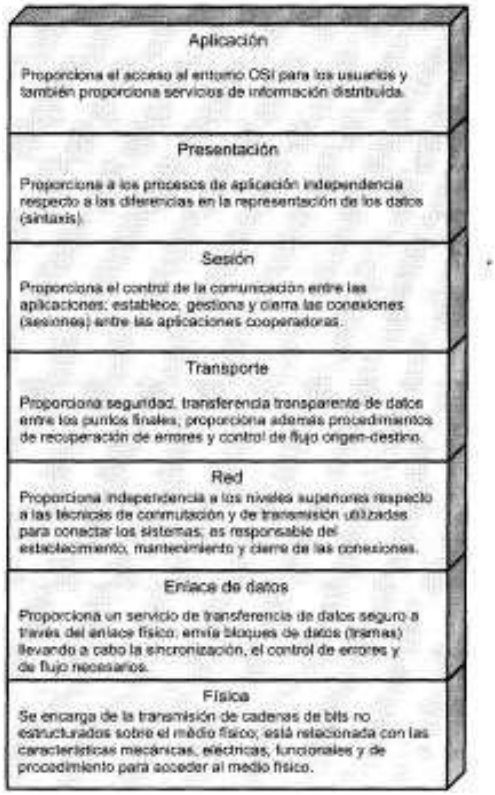
Capa de Sesión: El concepto de sesión se refiere al acceso remoto desde un terminal a un dispositivo como por ejemplo para la transferencia de archivos. La inclusión de una capa desesión ofrece a los usuarios el acceso a la red, previa codificación de datos que realiza la capa superior, permite el establecimiento y desconexión de una sesión. La función de esta capa es organizar, sincronizar y administrar el intercambio de información entre entidades del nivel superior. (Liberatori, 2018)

Capa de Presentación: La presente capa define el formato de los datos que se van a intercambiar entre aplicaciones para la resolución de diferencias sintácticas entre los sistemas. Algunas de estas representaciones son diferentes según el sistema operativo. Lo importante es la preservación de su significado entre ambos extremos de la comunicación (Liberatori, 2018).

Capa de Aplicación: Es la capa más cercana al entorno usuario. Esta capa lleva a cabo el procesamiento final del intercambio de información y es responsable de la semántica de la información intercambiada. La presente capa brinda servicios a los programas usuarios (Liberatori, 2018).

**Figura 2**

*Las capas de OSI*




*Nota.* Las capas de OSI. Tanenbaum y Wetherall, 2012.

Aun cuando el modelo OSI fue diseñado para proveer un modelo conceptual más no una guía de implementación, este esquema fue usado como la base de implementaciones tempranas de protocolos de red. Entre los protocolos asociados con el modelo OSI el más reconocido y usado

fue elprotocolo X.25. Desafortunadamente el modelo OSI es un desarrollo previo a Internet, no describe correctamente los protocolos de Internet y posee capas no usadas por losprotocolos TCP/IP (Perez & Higinio, 2017).

**2.2.2.3. Modelo TCP/IP.** La arquitectura TCP/IP consiste en una pila de protocolos. Cada protocolo lleva a cabo funciones fundamentales, las cuales trabajando en cooperación logran el objetivo que es implementar la comunicación en red (Liberatori, 2018)**.**

Realizando una comparación con el modelo OSI, IP desempeña la funcionalidad requerida por la Capa 3 o Capa de Red, y TCP corresponde con la Capa 4 o Capa de Transporte, cabe mencionar que la pila consta de más de un par de protocolos. Está también el Protocolo de Datagrama de Usuario(UDP). El modelo de referencia TCP/IP se definió por primera vez Cerf y Kahn (1974); después se refinó y definió como estándar en la comunidad de Internet (Branden, 1989). Clark (1988) describe la filosofía de diseño detrás de este modelo (Tanenbaum & Wetherall, 2012).

A continuación, se detalla los conceptos de cada nivel de la Arquitectura TCP/IP:

Aplicación: Es el nivel más alto de la arquitectura. La comunicación en este nivel tiene lugar entre procesos o aplicaciones que manejan datos de usuarios y se los comunican a otros procesos o aplicaciones en otro punto de la red. En este nivel operan protocolos como SMTP para transporte de mensajes de correo electrónico, FTP para transferencia de archivos, SSH para conexiones remotas seguras y HTTP para la navegación en la web (Liberatori, 2018).

Transporte: Este nivel de comunicación entre los equipos de red que forman parte de los extremos finales de la comunicación, estos equipos pueden hallarse en la misma red o en distintas redes conectadas a través de routers. Los protocolos del nivel de transporte TCP y UDP brindan al nivel superior una interfaz de acceso a la red de manera uniforme sin importar el tipo de conexión o red adyacente. A estos protocolos se les asocia funcionalidades como el control del error y control de flujo. Tanto TCP y UDP incluyen un esquema de direccionamiento para identificar aplicaciones. Se trata de campos de encabezado de 16 bits conocidos como números de puerto. TCP es un protocolo orientado a la conexión por lo que también permite manejar una conexión, es decir que TCP se encarga de brindar confiabilidad, abrir, mantener y cerrar conexiones solicitadas por protocolos de nivel superior por lo que tiene la capacidad de manejar datos desordenados, errados o duplicados y controlar la congestióny el manejo de paquetes perdidos. Los protocolos como HTTP apoyan su funcionalidad en el protocolo TCP. Por otra parte, el protocolo UDP brinda un servicio sin conexión para aplicaciones como DNS (Liberatori, 2018).

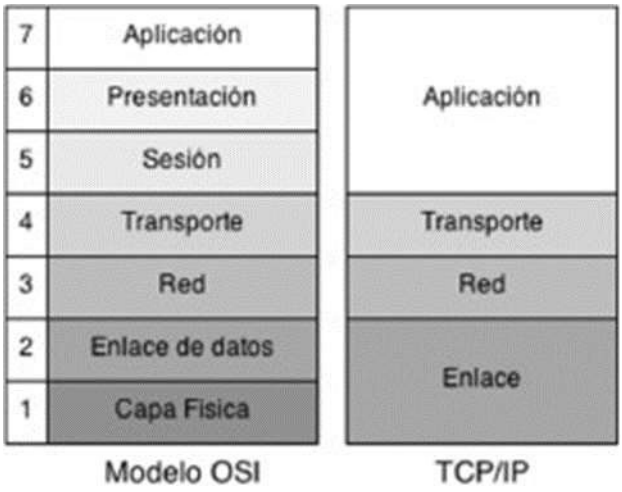
Red: En la presente capa existe un único protocolo cuya funcionalidad es lograr la interconexión de redes. IP es capaz de manejar datagramas o paquetes y enviarlos hacia el destino a través de diversas redes. El servicio de transmisión de paquetes IP es un servicio sin conexión no confiable pero que permite lograr una de las metas más importantes de manera sencilla que es la interconectividad. Su principal labores el ruteo, en la versión más antigua el protocolo IPv4 posee un esquema de direccionamiento de tipo jerárquico de 32 bits, conocido como esquema de direccionamiento IP. La versión más actual IPv6 tiene un esquema de direccionamiento más amplio que es de 128 bits, el servicio de ruteo es tipo salto a salto o hop-by-hop con comunicación

entre sistemas conectados directamente hasta llegar al router más cercano al destino final (Liberatori, 2018).

Enlace. En este nivel se atiende los asuntos relacionados conel tipo de red local sobre la cual se dirige la comunicación. En el presente nivel se manejan detalles del medio de comunicación sobre el que se transmitirán y recibirán los paquetes generados por IP entre dos diferentes equipos conectadas indirectamente o en el mismo enlace. La funcionalidad de los protocolos propios del nivel de enlace puede desarrollarse en hardware, como pueden ser las placas de red. Previo al envío de los paquetes sobre el medio físico estos deben estar acondicionados con un encabezado agregado generado por protocolos de este nivel, uno de los protocolos más antiguos que se llevan en este nivel es el Protocolo de Resolución de Direcciones (ARP) (Liberatori, 2018).

**Figura 3**

*Comparación Modelo OSI vs Arquitectura TCP/IP*

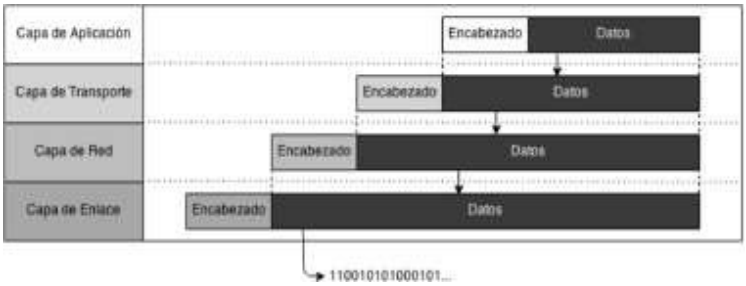



*Nota.* Comparación Modelo OSI vs Arquitectura TCP/IP, de Liberatori, 2018.

Como en el modelo OSI, la transmisión de mensaje atraviesa los protocolos hacia abajo agregando en cada capa información denominada encabezado como se puede visualizará en la Figura 3. En el lado del receptor el proceso es inverso (Liberatori, 2018).

**Figura 4**

*Encapsulado TCP/IP*




*Nota.* Encapsulado TCP/IP, de Liberatori, 2018.

Como sabemos Internet ha crecido velozmente y están siendo propuestos nuevos protocolos. La demanda no es sólo el crecimiento de las conexiones de red, también las nuevas tecnologías, el tráfico de la red, etc. Al no ser estáticos tanto Internet ni TCP/IP, se desarrollan nuevas aplicaciones y se usan nuevas tecnologías para la mejora de los mecanismos e infraestructuras. Por ejemplo, uno de los desarrollos más significativos involucra una revisión del Protocolo de Internet IP.La versión del Protocolo de Internet (IPv4) permaneció casi sin cambios desde que la establecieron a finales de los 70s, posterior a ello y debido a los notables cambios tecnológicos como la aparición de la tecnología inalámbrica y el aumento considerable de los enlaces de ancho de banda, la IETF (Internet Engineering Task Force) asignó a revisión la versión de IPv6 (Perez & Higinio, 2017).

**2.2.2.4. Clasificación de las redes.** En función de las dimensiones de red, los dispositivos que las conforman y las tecnologías que se utilizan, las redes se pueden clasificar en dos grupos: Redes de Área Amplia (WAN) y Redes de Área Local (LAN) (Liberatori, 2018). Cada tipo de red está diseñado para aplicaciones particulares, poseen estándares propios y tienen ventajas y restricciones diversas.

Asimismo, existen redes como las Redes de Área Personal (PAN) y las Redes de Área Metropolitana (MAN) (Perez & Higinio, 2017).

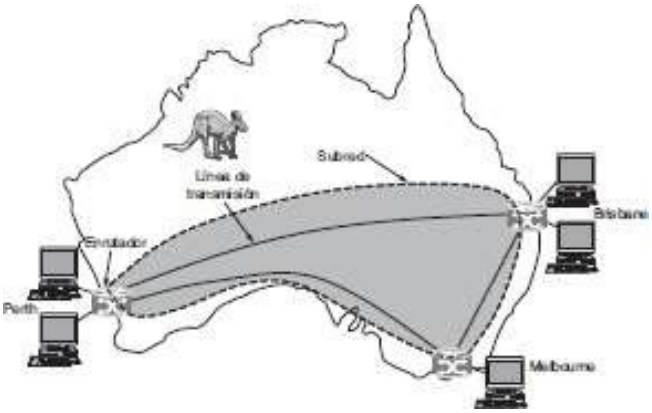
***A. Redes de Área Amplia (WAN).*** Las redes WAN se caracterizan por extenderse por grandes zonas geográficas, estas redes conectan redes más pequeñas. Las redes WAN pueden ser vistas como la integración de diversas redes LAN diversas. Las redes WAN emplean tecnologías de conmutación de circuitos y de paquetes y diversos esquemas de multiplexado. Los medios de transmisión comúnmente usados para interconectar las redes LAN son medios cableados y también se usan medios inalámbricos. Están compuestas por dispositivos denominados nodos conmutadores o dispositivos de encaminamiento (routers) (Perez & Higinio, 2017). El propósito principal de estas redes es el transporte de datos, debido a ello su funcionalidad primordial corresponde al área específica de enrutamiento, ofrecida como servicio de conmutación. Igualmente ofrecen servicios de conexión y acceso (Liberatori, 2018).

Estas redes están manejadas por los Proveedores de Servicio de Internet (ISP: compañía que brinda acceso a Internet). En la figura 4 se puede visualizar una red que conecta 3 oficinas en Australia, cada oficina contiene computadoras (hosts) cuya finalidad es desempeñar programas de

usuario. A la red que conecta estos hosts se les denomina subred. La labor de estas subredes es transportar mensajes de host a host (Tanenbaum & Wetherall, 2012).

**Figura 5**

*Red WAN que conecta sucursales en Australia*




*Nota.* Red WAN que conecta sucursales en Australia, de Tanenbaum & Wetherall, 2012.

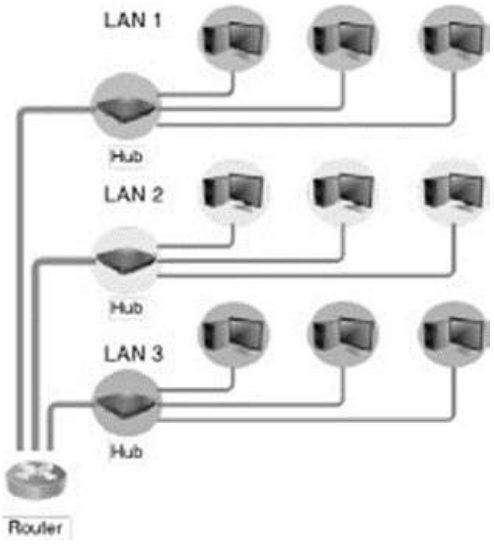
***B. Redes de Área Local (LAN).*** Las redes de área local son redes limitadas dentro de áreas geográficas pequeñas. Estas redes vincular dispositivos que se ubican en un espacio físico pequeño como una oficina o edificio. “Las redes LAN de mayor despliegue comercial son las conocidas con el nombre genérico de Ethernet” (Liberatori, 2018).

Habitualmente se tienen dos tipos de configuraciones: las LAN conmutadas o cableadas y las LAN inalámbricas o WLAN. Las redes LAN cableadas comúnmente usan el par trenzado y la fibra óptica. Los dispositivos activos frecuentemente utilizados son el conmutador Ethernet (Ethernet switch) para las LAN alámbricas y el Punto de Acceso Wi-Fi (AP Access Point) para las LAN inalámbricas (Perez & Higinio, 2017).

En la siguiente figura se puede visualizar una red LAN cableada, en la cual se encuentra computadoras, repetidores o hubs, switches y finalmente el router que comunica la red con la red WAN. Generalmente un router es el dispositivo de salida de una red LAN a una red WAN. Un hub es un dispositivo repetidor que se comporta como un bus, el cual reproduce por las salidas la información que recibe. Por otro lado, un switch es un elemento más compuesto que el hub, el switch reproduce la información entre sus puertos siguiendo un esquema determinado de direccionamiento especial propio de las LAN (Liberatori, 2018).

**Figura 6**

*Red LAN cableada*

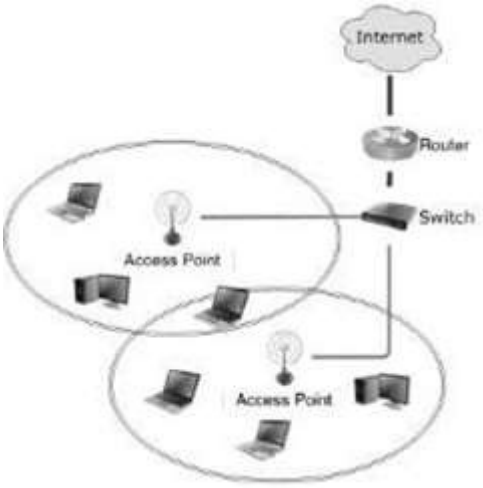



*Nota:* Red LAN cableada, de Liberatori, 2018.

En la figura 6 se presenta una red LAN inalámbrica con dispositivos inalámbricos como Access Point (AP) a través de este equipo pasan todas las comunicaciones (Liberatori, 2018).

**Figura 7**

*Dos redes LAN Wi-Fi conectadas a través de una LAN cableada*




*Nota*: Dos redes LAN wifi conectadas a través de una LAN cableada, de Liberatori, 2018.

**2.2.2.5. Ethernet.** La idea inicial de Ethernet se originó del problema de permitir que dos o más host utilizaran el mismo medio y evitar que las señales se interfieran entre sí. La mayor parte del tráfico en Internet se origina y culmina en conexiones de Ethernet. Desde sus inicios en los 70s Ethernet ha evolucionado para poder satisfacer el aumento de la demanda de LAN de alta velocidad. En 1985, el comité de estándares para Redes Metropolitanas y Locales del IEEE publicó los estándares para las LAN, estos estándares comienzan con el número 802. El estándar para Ethernet es el 802.3. El IEEE quería asegurar que sus estándares fueran compatibles con el Modelo OSI de la ISO. Por eso, el estándar IEEE 802.3 debía cubrir las necesidades de la Capa 1 y de las porciones inferiores de la Capa 2 del modelo OSI (Tanenbaum & Wetherall, 2012).

Al momento que aparece un nuevo medio, como lo fue la fibra óptica, Ethernet se adapta para sacar ventaja de un ancho de banda superior y de un menor índice de errores que la fibra óptica brinda. El éxito de Ethernet es debido a la sencillez y facilidad de mantenimiento, capacidad

para incorporar nuevas tecnologías, confiabilidad y bajo costo de instalación y de actualización (Tanenbaum & Wetherall, 2012).

Con el desarrollo de Gigabit Ethernet, lo que inició como tecnología LAN ahora se despliegan a distancias que hacen de Ethernet un estándar de Red de Área Metropolitana (MAN) y de Red de Área Extensa (WAN) (Tanenbaum & Wetherall, 2012).

**2.2.2.6. Medios de transmisión.** Los medios de transmisión utilizados para transferir información pueden clasificarse en medios guiados y no guiados. Los medios guiados proveen una vía o camino físico a través de la cual la señal se propaga, estos pueden ser el par trenzado, cable coaxial y la fibra óptica. Por otro lado, las tecnologías utilizadas en la transmisión no guiada son la difusión por radio, microondas y satélites (Stallings, 2000).

Para el diseño del sistema de transmisión se debe teneren cuenta factores relacionados con el medio de transmisión y con la señal que determinan la distancia y la velocidad de transmisión:

El ancho de banda: si los otros factores permanecen constantes, al aumentar el ancho de banda, la velocidad detransmisión se puede incrementar (Stallings, 2000).

Dificultades en la transmisión: las dificultades como la atenuación restringen la distancia. En medios guiados, el par trenzado sufre de mayores adversidades comparándolo con el cable coaxial, asimismo el cable coaxial vulnerable que la fibra óptica (Stallings, 2000).

Interferencias: Las interferencias en medios no guiados resultan de la presencia de señales en bandas de frecuencias próximas que pueden distorsionar la señal. En medios guiados, los múltiples cables de pares trenzados se repletan dentro de una misma cubierta, provocando interferencias, este problema puede reducirse utilizando un apantallamiento apropiado (Stallings, 2000).

Número de receptores: Un medio guiado puede usarse para enlaces compartidos mediante el uso de múltiples conectores. Estos conectores utilizados pueden atenuar la señal por lo que la distancia y velocidad de transmisión disminuirán (Stallings, 2000).

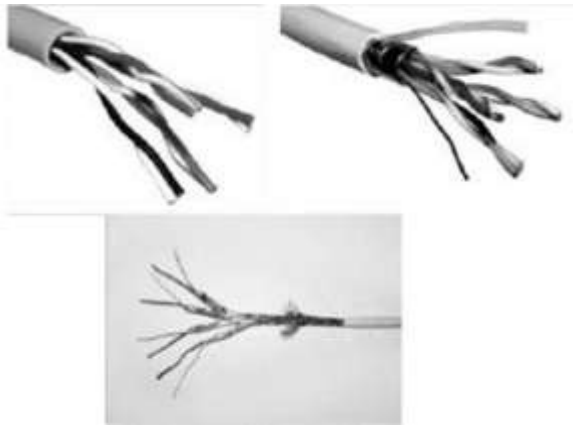
**2.2.2.7. Medios guiados**. Para el transporte de datos se pueden utilizar diversos medios físicos, cada medio tiene sus propias características como ancho de banda, retardo, facilidad de instalación, costo y mantenimiento (Liberatori, 2018).

Par trenzado: Es uno de los medios de transmisión más antiguos. Este medio consta de dos cables de cobre aislados generalmente de 1mm de grosor, estos cables están trenzados de manera helicoidal. El trenzado es debido a que dos cables paralelos constituyen una antena simple. Cuando estos cables setrenzan, las ondas de distintos trenzados se cancelan y el cable irradia menor efectividad. Esto proporciona una mejor inmunidad al ruido externo. Los pares trenzados se pueden usar para la transmisión analógica o digital, su ancho de banda depende del grosor del cable y del tramo que recorre. (Tanenbaum & Wetherall, 2012). Ejemplos de este medio de comunicación son el Par Trenzado no Apantallado (UTP) y el Par Trenzado Blindado (FTP) que al estar envuelta por una hoja de aluminio (la cual envuelve los 4 pares) brinda mayor protección frente a interferencia

electromagnética. Asimismo, se tiene el cable STP, la cual añade un blindaje independiente a cada par. El par trenzado es el cable de uso más extendido en redes de telefonía (ADSL) y de tipo LAN (para el tendido de distancias cortas). Es el menos costoso comparado con los medios de transmisión guiados, pero es el más limitado si nos referimos a la velocidad ydistancia (Liberatori, 2018).

**Figura 8**

*UTP, FTP y STP*

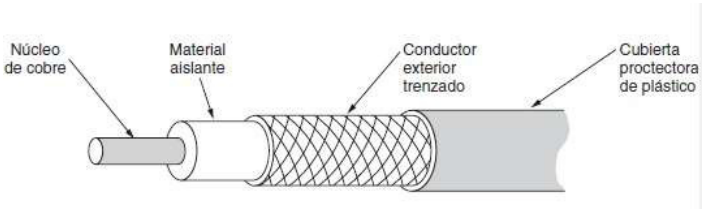


*Nota.* UTP, FTP y STP, por Liberatori, 2018.

Cable Coaxial: Consta de un conductor cilíndrico interno que se encuentra aislado de una malla externa por medio de un material dieléctrico. A diferencia del par trenzado, el cable coaxial posee un blindaje para protección conocido como apantallamiento, esto permite reducir la vulnerabilidad a interferencias, brinda mayor ancho de banda por lo que abarcan mayores distancias a velocidades más altas. El cable coaxial es un medio de transmisión común, utilizado para la distribución deseñales de televisión y conexión a internet en redes de TV por cable, pero actualmente está siendo reemplazado por la Fibra óptica (Liberatori, 2018).

**Figura 9**

*Cable Coaxial*

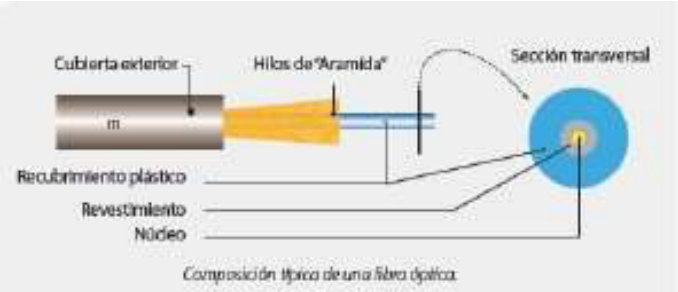



*Nota.* Cable Coaxial, por Tanenbaum y Wetherall, 2012.

Fibra óptica: La fibra óptica es un medio de transmisión que actualmente tiene gran aceptación en las telecomunicaciones. Posee forma cilíndrica y consta de 3 secciones concéntricas que vienen a ser el núcleo, el revestimiento y la cubierta. El núcleo es la sección más interna el cual está constituido por una o varias fibras de cristal o plástico y tiene un diámetro de 8 a 100 µm. Cada fibra está rodeada por su propio revestimiento y la capa más externa que envuelve a uno o varios revestimientos es la cubierta. La cubierta está hecha de plástico y otros materiales que brindan protección contra la humedad, aplastamientos y diversos peligros. Adicionalmente la protección básica de la fibra puede contar con una capa conocidacomo buffer la cual tiene como fin proteger la fibra durante la manipulación (Stallings, 2000).

**Figura 10**

*Composición típica de una fibra óptica*




*Nota.* Composición típica de una fibra óptica. Inictel (s.f.).

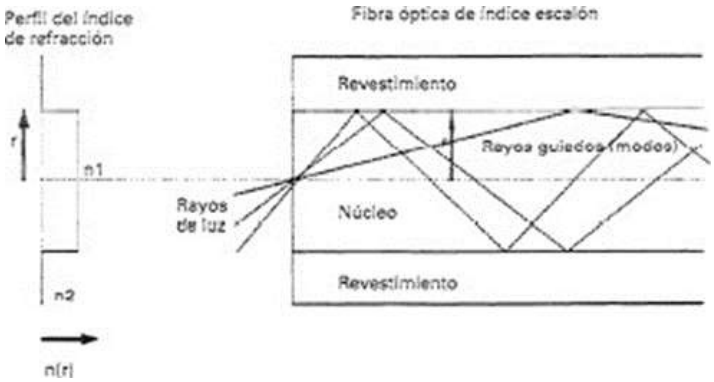
La ventaja de la fibra óptica que tiene al compararlo con los otros medios de comunicación guiados es que es inmune a las interferencias electromagnéticas, brinda mayor capacidad debido a que el ancho de banda de la fibra es enorme, posee menor peso y tamaño porque las fibras ópticas son apreciablemente más finas comparándolo con el cable coaxial y los pares trenzados, asimismo la atenuación de la fibra óptica es menor (Stallings, 2000).

La fibra óptica puede clasificarse según su tipo de propagación. Puede ser fibra multimodo y monomodo. La fibra multimodo es una fibra que puede propagar más de un modo de luz, es usada comúnmente en aplicaciones de distancia corta. Asimismo, este tipo de fibra multimodo se pueden dividir en fibra de índice de escalón y la fibra de índice gradual. La fibra óptica multimodo de índice escalón posee índices de refracción diferentes del núcleo y del revestimiento, pero no uniformes. Se presenta un cambio abrupto entre la frontera entre el núcleo y revestimiento. Los rayos de luz se reflejan en esta frontera y se propagan a lo largo de la fibra, estos rayos viajan por diferentes caminos en el núcleo, debido a que la distancia que viaja cada rayo debe diferenciarse y llegar al destino en diferentes tiempos. Esto origina que el pulso transmitido se ensanche con el

tiempo, este ensanchamiento restringe la velocidad de transmisión de información debido a que ésta es inversamente proporcional a la anchura del pulso (Chomycz, 2002).

**Figura 11**

*Propagación de la luz en una fibra óptica de índice escalón*

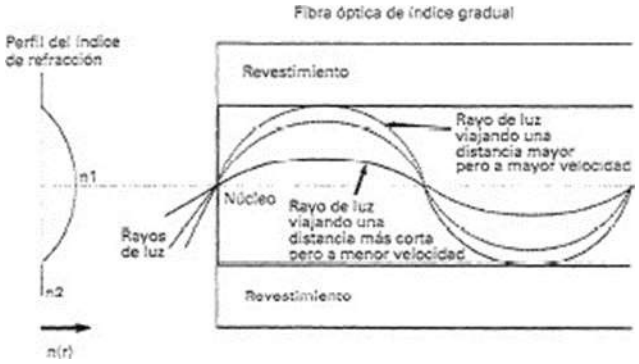



*Nota.* Propagación de la luz en una fibra óptica de índice escalón, por Chomycz, 2002.

En el caso de la fibra de índice gradual, el índice de refracción del núcleo decrece desde el centro al exterior. El índice de refracción del revestimiento es uniforme. El área exterior del núcleo posee un índice de refracción más bajo que el centro. La luz viaja a una velocidad mayor en un material con índice de refracción más bajo. Los rayos de luz de la región exterior del núcleo viajan a una distancia mayor y necesitan mayor tiempo para llegar al final de la fibra óptica, Sin embargo, debido a que la luz viaja a mayor velocidad en esta región, el mayor tiempo causado por la distancia es compensada parcialmente por una mayor velocidad del rayo. Esto reduce la cantidad de ensanchamiento del pulso entre los rayos del centro del núcleo y de la región externa, reduciendo así la dispersión modal, debido a ello este tipo de fibra posee un ancho de banda mayor que una fibra de índice escalón (Chomycz, 2002).

**Figura 12**

*Propagación de la luz en una fibra de índice gradual*

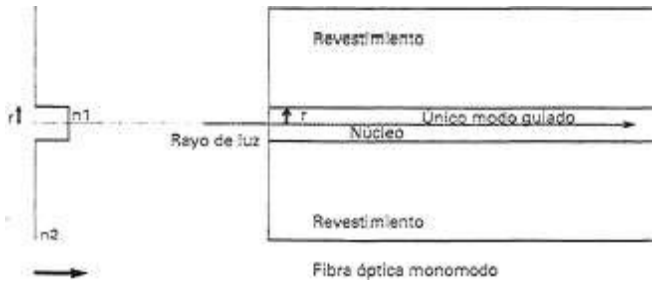



*Nota.* Propagación de la luz en una fibra de índice gradual, por Chomycz, 2002.

Por otro lado, la fibra monomodo solo propaga un modo de luz. El perfil del índice de refracción de una fibra monomodo se asemeja al de una fibra multimodo de índice escalón. Debido a que se propaga de un solo modo, se elimina el ensanchamiento del pulso debido a la dispersión modal, por lo que las velocidades de transmisión de información son mayores en distancias más largas (Chomycz, 2002).

**Figura 13**

*Propagación de la luz en una fibra monomodo*




*Nota.* Propagación de la luz en una fibra monomodo, por Chomycz, 2022.

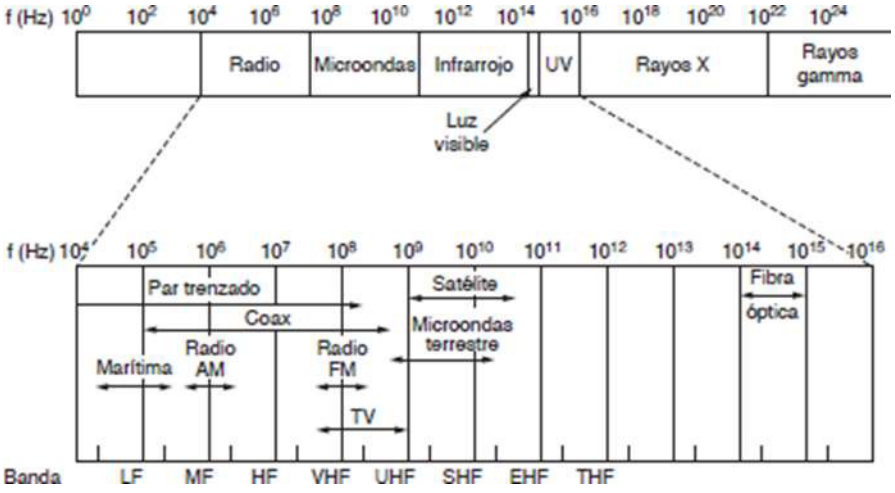
Las redes de fibra óptica constituyen una solución eficiente frente al desafío de la última milla, debido a las propiedades técnicas que ofrece este tipo de transmisión. Entre sus beneficios más destacados se encuentran: una capacidad de ancho de banda elevada y adaptable, que posibilita velocidades de transmisión de varios gigabits por segundo; una mayor fidelidad de la señal gracias a su resistencia a las interferencias electromagnéticas; una estructura liviana y de menor tamaño en cada filamento de fibra; además de su integración natural con sistemas digitales (Ojeda, 2009).

**2.2.2.8. Medios no guiados.** Cuando los electrones se mueven, generan ondas electromagnéticas, las cuales se pueden propagar por el espacio. En 1865 el físico inglés James Maxwell predijo estas ondas y en 1887 el físico alemán Heinrich Hertz observó estas ondas por primera vez. El número de oscilaciones por segundo de una onda electromagnética es conocido como frecuencia y se mide en Hz. Una longitud de onda viene a ser la distancia entre dos máximos (o mínimos) (Tanenbaum & Wetherall, 2012). En medios no guiados, la transmisión se realiza utilizando antenas. La antena radia ondas electromagnéticas al medio y son recepcionados por otra antena. Existen dos tipos de configuraciones: direccional y omnidireccional (Stallings, 2000).

Todas las ondas electromagnéticas viajan a igual velocidad en el vacío sin importar su frecuencia. La velocidad de la luz es el máximo límite de velocidad y su valor es aproximadamente $3x10^8$m/seg. En la siguiente imagen se muestra el espectro electromagnético. Las fracciones de radio, microondas, infrarrojo y luz visible del espectro se pueden utilizar para transmitir información mediante modulación de amplitud, fase de ondas o frecuencia. Las bandas nombradas al inferior dela imagen son los nombres de la ITU y están basadas en las longitudes de onda (Tanenbaum & Wetherall, 2012).

**Figura 14**

*El espectro electromagnético y sus usos para comunicaciones*




*Nota.* El espectro electromagnético y sus usos para comunicaciones, por Tanenbaum y Wetherall, 2012.

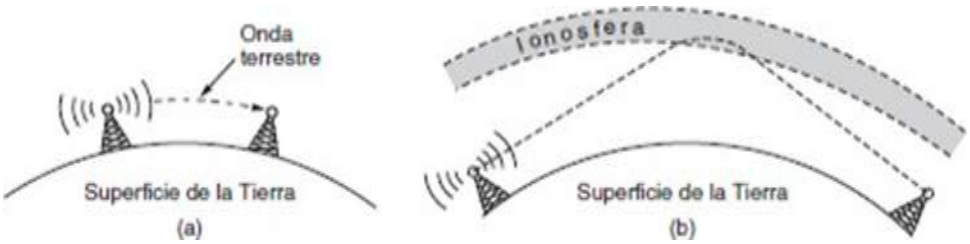
A continuación, describiremos cómo se utilizan las partes del espectro magnético:

Radiotransmisión: Son ondas de radiofrecuencia omnidireccionales, fáciles de generar, recorren largas distancias e introducirse a edificios fácilmente es por ello por lo que son muy utilizados en la comunicación. Sus propiedades dependen de la frecuencia, a bajas frecuencias las ondas atraviesan bien los obstáculos, pero su potencia disminuye drásticamente a medida que se aleja de la fuente. Esta atenuación es conocida como pérdida de trayectoria. Por otro lado, a altas frecuencias, las ondas de radio tienden a viajar en línea recta y rebotan en los obstáculos, la pérdida de trayectoria disminuye la potencia, asimismo estas ondas son absorbidas por la lluvia y demás obstáculos presentes en mayor grado que de las ondas de baja frecuencia. En las bandas VLF, LF y MF, las ondas de radio siguen la curvatura de la Tierra, estas ondas pueden ser detectadas a

1000km en frecuencias más bajas. En las bandas HF y VHF, las ondas suelen ser absorbidas por la Tierra, pero las ondas que llegan a la ionósfera se refractan y se envían de regreso a la Tierra (Stallings, Comunicaciones y Redes de Computadores 6ta Edición, 2000).

**Figura 15**

*(a) Bandas VLF, LF y MF. (b) Banda HF y VHF*




*Nota.* (a) Bandas VLF, LF y MF. (b) Banda HF y VHF, por Tanenbaum y Wetherall, 2012.

Transmisión por microondas: Este tipo de transmisión se puede subdividir en microondas terrestres y microondas por satélites. En las microondas terrestres, la antena más conocida es la del tipo parabólico. Para llevar a cabo comunicaciones a larga distancia, se utiliza encadenamiento de enlaces punto a punto situadas en torres continuas, estos enlaces deben estar perfectamente alineados. Es una alternativa al cable coaxial o a las fibras ópticas. Su uso es frecuente en la transmisión de televisión y de voz. Por otra parte, respecto a las microondas porsatélite, un satélite de comunicaciones es básicamente una estación que retransmite microondas. Es utilizado como enlace entre 2 o más receptores o transmisores terrestres, denominadasestaciones base. EL satélite recibe la señal en una banda de frecuencia (canal ascendente), lo amplifica o repite y luego lo retransmite en otra banda de frecuencia (canal descendente). Las aplicaciones vía satélite son usadas en la difusión de televisión, transmisión telefónica a larga distancia y redes privadas (Stallings, 2000).

Infrarrojos: Este tipo de comunicaciones son llevadas a cabo mediante transceivers que modulan la luz infrarroja no coherente. Los rayos infrarrojos difieren de las microondas debido a que los primeros no pueden atravesar paredes, no poseen problemas de seguridad y de asignación de frecuencias porque esta banda no requiere permisos (Stallings, 2000).

**2.2.2.9. Redes Privadas Virtuales (VPN).** Las Redes Privadas Virtuales (VPN, por sus siglas en inglés Virtual Private Network) conforman una tecnología que permite establecer comunicaciones seguras sobre una red pública, como Internet, simulando el comportamiento de una red privada. Una red privada virtual crea un túnel lógico cifrado que protege la confidencialidad, integridad y autenticidad de los datos transmitidos entre los extremos de la comunicación (Stallings, 2017).

El principio fundamental de una VPN es el encapsulamiento de los paquetes de datos originales dentro de otros paquetes que incorporan mecanismos de seguridad, permitiendo que la información se transmita de forma protegida a través de infraestructuras no confiables. Esta tecnología es ampliamente utilizada para la interconexión de sedes corporativas, acceso remoto seguro y transmisión de información sensible (Khan Academy, 2020).

Desde el nivel topológico, las VPN pueden clasificarse principalmente en VPN de acceso remoto y VPN sitio a sitio (*Site-to-Site*). Las VPN sitio a sitio permiten interconectar redes completas situadas en diferentes localizaciones geográficas, estableciendo una comunicación permanente y transparente para los usuarios finales (Tanenbaum & Wetherall, 2012).

**2.2.2.10. VPN Site-to-Site.** La VPN Site-to-Site es definida como una arquitectura de red que permite la interconexión segura de dos o más redes locales a través de Internet, utilizando dispositivos de seguridad perimetral como firewalls o routers con capacidades criptográficas. Este tipo de VPN no requiere intervención directa del usuario final, ya que el túnel se establece automáticamente entre los dispositivos de borde a diferencia de las VPN de acceso remoto (Stallings, 2017).

Este tipo de VPN es idóneo para empresas con sedes remotas, ya que permite compartir recursos, aplicaciones y servicios de red como si todas las ubicaciones de trabajo pertenecieran a una misma red local. Además, ofrece escalabilidad, reducción de costos frente a enlaces dedicados y compatibilidad con diferentes tecnologías de acceso a Internet, incluyendo enlaces satelitales (Perez & Higinio, 2017).

**2.2.2.11. Protocolo IPsec.** IPsec (Internet Protocol Security) es un conjunto de protocolos diseñado para garantizar las comunicaciones a nivel de la capa de red del modelo OSI. Proporciona mecanismos de autenticación, confidencialidad, integridad y protección contra ataques de repetición para los paquetes IP transmitidos a través de redes públicas (Kent & Seo, 2005).

IPsec opera mediante dos protocolos principales:

Authentication Header (AH), que proporciona autenticación e integridad de los datos.

Encapsulating Security Payload (ESP), que proporciona confidencialidad mediante cifrado, además de integridad y autenticación.

El establecimiento de un túnel IPsec se realiza a través del protocolo IKE (Internet Key Exchange), que se encarga de la negociación de parámetros de seguridad, intercambio de claves criptográficas y autenticación mutua entre los extremos (Stallings, 2017).

IPsec puede operar en dos modos:

Modo transporte, en el cual solo se protege la carga útil del paquete IP.

Modo túnel, donde se encapsula y protege el paquete IP completo, siendo este último el más utilizado en VPN Site-to-Site (Kent & Seo, 2005).

**2.2.2.12. Internet satelital de órbita baja (Starlink).** Starlink es un sistema de acceso a Internet satelital desarrollado por SpaceX, basado en una constelación de satélites de órbita terrestre baja (Low Earth Orbit – LEO) que se encuentran ubicados aproximadamente entre 340 y 550 km sobre la superficie terrestre. A diferencia de los sistemas satelitales geoestacionarios tradicionales, Starlink ofrece menores latencias y mayores velocidades de transmisión de datos (SpaceX, 2023).

La arquitectura LEO permite disminuir significativamente el retardo de propagación, alcanzando latencias promedio de entre 20 y 50 ms, lo cual hace factible la implementación de aplicaciones en tiempo real y tecnologías de seguridad como VPN IPsec (Handley, 2019).

Starlink es especialmente adecuado para zonas rurales o de difícil acceso donde las tecnologías de acceso convencionales no están disponibles tales como fibra óptica o los enlaces inalámbricos terrestres. Sin embargo, el uso de direcciones IP públicas dinámicas y la dependencia de enlaces inalámbricos hacen imprescindible la implementación de mecanismos de seguridad

adicionales para proteger la información transmitida, como el uso de VPN Site-to-Site con Ipsec (SpaceX, 2023).

### *2.2.3 Definición de términos básicos*

VPN Site to Site: (Red Privada Virtual de sitio a sitio) Es una conexión cifrada y permanente que interconecta de dos a más redes a través de internet, creando un túnel privado para que la comunicación entre hosts (Stallings, 2017).

Default Gateway: La puerta de enlace predeterminada es un término para un punto de hardware o nodo que brindará acceso saliente a paquetes de datos a un destino en otra red (Tanenbaum & Wetherall, 2012).

Enrutamiento estático: Es una forma o técnica de enrutamiento que permite al administrador configurar de manera específica redes en el enrutador, definiendo los caminos para la transferencia de paquetes (Perez & Higinio, 2017).

Starlink: Es un tipo de internet satelital de alta velocidad, que usa un grupo de satélites en órbita baja para llevar la conexión a internet desde cualquier lugar, especialmente en zonas rurales con falta de acceso de tecnologías convencionales (SpaceX, 2023).

DDNS (Dynamic DNS): Opción integrada en los dispositivos Fortigate que permite asociar un nombre de dominio a la dirección IP pública del Firewall, incluso cuando esta IP es dinámica y cambia periódicamente (Stallings, 2017).

Seguridad Perimetral: Es la primera línea de defensa de una infraestructura informática. Su función es establecer una barrera de protección entre la red privada y redes no confiables, como Internet, controlando y filtrando el tráfico que entra y sale. Comúnmente se utilizan dispositivos y soluciones como firewalls (Khan Academy, 2020).

Firmware: Es el software integrado directamente en el hardware de un dispositivo. Se encarga de controlar y permitir el correcto funcionamiento del hardware, además de hacer posible su actualización mediante nuevas versiones que corrigen errores, mejoran el rendimiento o agregan funcionalidades de acuerdo con el fabricante (Tanenbaum & Wetherall, 2012).

Sede remota: Se entiende por sede remota a una instalación de la empresa ubicada fuera de la sede principal, que requiere acceso a la red corporativa y a Internet para la operación de sus actividades. Estas sedes suelen interconectar con la sede principal a través de diferentes medios tecnológicos disponibles (Perez & Higinio, 2017).

IP pública dinámica: Una IP pública dinámica es una dirección IP asignada por el proveedor de Internet que puede cambiar con el tiempo, ya sea por reinicios del servicio o por condiciones propias de la red del proveedor. Este tipo de direccionamiento es común en servicios de Internet satelital, Internet residencial e Internet móvil (Stallings, 2017).

CGNAT (Carrier – Grade Nat): Es una técnica de red utilizada por los proveedores de internet (ISP) para compartir una única dirección IPv4 pública entre múltiples clientes, mitigando la escasez de direcciones IPv4. (SpaceX, 2023).

## 2.3 Propuesta de solución

### *2.3.1 Metodología de solución*

La metodología que se utilizó en el presente trabajo de investigación fue de tipo descriptiva y aplicada, ya que tuvo como propósito documentar el diseño, la implementación lógica y la implementación física de una solución de Internet mediante VPN IPsec sobre tecnología Starlink para la interconexión de dos sedes remotas de una empresa CR Technology.

Según su finalidad, la investigación se clasificó como aplicada, ya que se orientó al desarrollo e implementación de una solución tecnológica que permita atender la necesidad real previamente identificada, proponiendo una estrategia eficiente para la transmisión de datos entre sedes remotas.

Asimismo, la metodología se sustentó en el análisis del entorno actual de conectividad y seguridad, el diseño de la arquitectura de red, la configuración de los dispositivos involucrados y la validación del funcionamiento de la VPN IPsec, garantizando la disponibilidad de la información transmitida a través un servicio satelital Starlink.

La población de estudio de cada sede remota estuvo conformada por dos trabajadores y tres cámaras de videovigilancia. Al considerar ambas sedes remotas, se obtuvo un total de cuatro trabajadores y seis cámaras. La sede remota 1 se ubicó en distrito de Lurigancho–Chosica, mientras que la sede remota 2 se localizó en el distrito de Ventanilla, provincia constitucional del Callao.

Finalmente, el desarrollo del proyecto se ejecutó siguiendo los protocolos, especificaciones y normas técnicas propias de una implementación basada en VPN IPsec, documentando cada etapa del proceso para asegurar su reproducibilidad en entornos de características similares.

### *2.3.2 Justificación de la selección tecnológica*

La selección de la tecnología empleada en la presente propuesta de solución respondió a la necesidad de brindar a las sedes remotas de la empresa CR Technology una conectividad de rápida implementación, considerando su ubicación en zonas de difícil acceso a infraestructuras de telecomunicaciones convencionales, como enlaces de fibra óptica, radioenlaces terrestres o redes móviles de alta capacidad.

Para al acceso a Internet en las sedes remotas, se evaluaron distintas alternativas tecnológicas, incluyendo soluciones satelitales tradicionales, servicios de Internet móvil y diferentes modalidades del servicio Starlink. Las soluciones satelitales convencionales fueron descartadas debido a sus altos niveles de latencia y limitaciones de ancho de banda, de igual manera las soluciones móviles no garantizan cobertura ni estabilidad en las zonas donde se ubican las sedes remotas del proyecto.

Para el presente proyecto se optó por el uso del servicio Starlink empresarial, que ofrece características orientadas a entornos corporativos, como mayor estabilidad del servicio y planes de datos acordes a las necesidades requeridas para el proyecto. Otras modalidades, como Starlink residencial o Starlink itinerante, fueron descartadas debido a sus limitaciones en términos de gestión, estabilidad y enfoque no corporativo para el escenario propuesto. En cuanto al

equipamiento, se seleccionó la antena Starlink estándar, cuya capacidad técnica es suficiente para el volumen de tráfico requerido en las sedes remotas, permitiendo optimizar la inversión sin recurrir a hardware de gama superior que no resultaría necesario para el alcance del proyecto.

Para la implementación de los túneles VPN IPsec en las sedes remotas, se evaluaron distintos dispositivos de red capaces de establecer comunicaciones, como routers de propósito general y firewalls de diferentes fabricantes. Algunas soluciones de gama alta, orientadas a entornos empresariales de gran escala, fueron descartadas debido a los elevados costos de adquisición y licenciamiento superiores a los requeridos para el alcance del proyecto. Por otro lado, dispositivos de propósito general fueron considerados menos adecuados, ya que demandan una mayor carga de configuración y fortalecimiento de seguridad para cumplir con los estándares corporativos mínimos.

Bajo este enfoque, se seleccionaron equipos FortiGate modelo 40F debido a su capacidad para establecer túneles VPN IPsec de forma eficiente en entornos donde el acceso a Internet opera bajo esquemas de traducción de direcciones, como es el caso del servicio Starlink en las sedes remotas. Asimismo, la elección del FortiGate 40F respondió a criterios de compatibilidad con la infraestructura de seguridad perimetral existente en la sede principal de Surco, así como a la estandarización tecnológica y simplicidad operativa, considerando la experiencia previa de la empresa en la administración de soluciones del mismo fabricante, lo que contribuyó a reducir la complejidad de gestión, minimizar riesgos operativos y facilitar el soporte y mantenimiento de la solución implementada.

En cuanto al software del equipamiento seleccionado, se optó por utilizar una versión de firmware estable y alineada con la infraestructura existente en la sede principal. En particular, se empleó la versión 7.0.14, que se encontraba validada para entornos productivos al momento de la implementación y presentaba compatibilidad comprobada con las funcionalidades requeridas, tales como la configuración de túneles VPN IPsec y mecanismos de resolución dinámica de direcciones (DDNS). La estandarización de la versión de firmware entre los equipos de las sedes remotas y el firewall perimetral de la sede principal contribuyó a garantizar la compatibilidad, estabilidad del servicio y continuidad operativa de la solución implementada.

### *2.3.3 Factibilidad técnica – operativa*

La presente propuesta de solución fue evaluada desde un punto de vista técnico y operativo con la finalidad de determinar la viabilidad de implementación en las sedes remotas de la empresa CR Technology, considerando las condiciones del entorno, los recursos disponibles y la infraestructura existente en la sede principal.

**2.3.3.1. Factibilidad técnica.** la solución propuesta resultó técnicamente viable debido a la compatibilidad entre los componentes seleccionados y el modelo de operación definido. El servicio Starlink fue utilizado como medio de acceso en las sedes remotas y, bajo su configuración por defecto basada en CGNAT, permitió el uso de equipos FortiGate 40F para establecer túneles VPN IPsec iniciados desde las sedes remotas hacia la sede principal. Este esquema hizo posible la comunicación cifrada sin la necesidad de contar con direcciones IP públicas en los puntos remotos y facilitó la integración con la infraestructura perimetral existente en la sede principal de Surco, manteniendo centralizados los controles de seguridad y la salida a Internet.

Adicionalmente, la tecnología Starlink ofrece una conexión hacia internet con niveles de latencia y ancho de banda adecuados para el transporte de tráfico corporativo a través de los túneles VPN, lo que garantiza un acceso estable a los recursos internos y a los servicios externos. La compatibilidad entre los equipos FortiGate instalados en las sedes remotas y el firewall perimetral de Surco permitió implementar la solución sin requerir modificaciones significativas en la infraestructura existente.

Finalmente, la propuesta no necesitó enlaces redundantes ni equipamiento adicional en las sedes remotas, lo que permitió reducir la complejidad del diseño y facilitó su implementación. Además, la arquitectura definida permitió proyectar la incorporación futura de nuevas sedes mediante la creación de túneles VPN adicionales desde la sede principal, demostrando la escalabilidad de la solución.

**2.3.3.2. Factibilidad operativa.** Desde el punto de vista operativo, la solución resultó factible por la facilidad de instalación y administración de los dispositivos. La implementación de Starlink en las sedes remotas no necesitó infraestructura previa, lo que permite un despliegue rápido incluso en zonas de difícil acceso.

La gestión centralizada de la seguridad y de la salida a Internet desde la sede principal de Surco redujo la necesidad de intervenciones técnicas constantes en las sedes remotas, facilitando las labores de monitoreo, control y mantenimiento. Además, el uso de una plataforma de seguridad ya conocida por el personal técnico de la empresa ayudo a disminuir la curva de aprendizaje y agilizó los tiempos de respuesta ante incidencias.

Por otro lado, la solución propuesta minimizó la dependencia de personal especializado en campo, ya que las configuraciones críticas y los ajustes de seguridad se gestionaron de manera centralizada desde la sede principal de Surco. Esto resulta cómodo en entornos remotos, donde el acceso de personal técnico puede ser limitado o costoso.

En conjunto, el análisis de factibilidad operativa evidenció que la solución resultó viable, sostenible y adecuada para las condiciones de las sedes remotas de la empresa CR Technology, permitiendo cumplir los objetivos de conectividad, gestión centralizada y escalabilidad establecidos en el proyecto.

### *2.3.4 Desarrollo de la solución*

**2.3.4.1. Análisis del problema.** Las sedes remotas de la empresa CR Technology, nunca habían contado con un servicio de interconexión con la sede principal ubicada en Surco e internet de manera independiente. Esta carencia limitaba la comunicación entre las oficinas, lo que afectaba tanto las operaciones administrativas como el monitoreo de cámaras seguridad.

Actualmente, cada sede remota contaba con dos trabajadores y tres cámaras de videovigilancia. La necesidad de establecer conectividad surgió principalmente por la operación de estos trabajadores, quienes requerían acceso seguro a sistemas corporativos y recursos alojados en la sede principal, así como la supervisión en tiempo real de las cámaras de seguridad, que permitía garantizar la seguridad de las instalaciones.

La falta de un canal de comunicación cifrada genera varios problemas:

- Limitaciones en la transmisión de información, afectando la operación de los trabajadores remotos.
- Riesgos de seguridad, al no existir un enlace cifrado que proteja la información compartida entre sedes.
- Imposibilidad de monitoreo centralizado, lo que reduce la capacidad de supervisión de las instalaciones y equipos críticos.
- Dependencia de soluciones locales inadecuadas, como conexiones de Internet independientes, que no permiten centralizar ni controlar la navegación de manera eficiente.

**2.3.4.2. Evaluación de alternativas.** Identificado el problema y las necesidades de conectividad de las sedes remotas de la empresa CR Technology, se procedió a evaluar diversas alternativas tecnológicas que permitieran interconectar de manera segura las sedes con la oficina principal en Surco.

Para ello, se analizaron tres opciones principales: enlace de datos mediante radio enlace, fibra óptica y antenas Starlink con VPN Site-to-Site IPsec. Cada alternativa fue evaluada considerando criterios técnicos, económicos y operativos, para identificar la solución más adecuada a las características reales de las sedes remotas, donde trabajaban dos personas y se monitoreaban tres cámaras de videovigilancia por sede.

***A. Implementación de servicios de enlaces de datos mediante radioenlace.*** Esta alternativa consistía en la contratación de un servicio dedicado de transmisión de datos mediante radiofrecuencia, implementado y administrado por un proveedor de servicios de Internet (ISP), mediante el uso de antenas de radio enlace para la interconexión entre sedes.

Ventajas de esta alternativa:

- Servicio dedicado exclusivamente a la transmisión de datos, lo que garantiza estabilidad del enlace.
- Soporte técnico brindado por un proveedor certificado como ISP.
- Inclusión de un equipo router dentro del contrato del servicio.
- Mantenimiento preventivo trimestral, conforme a los estatutos establecidos por la empresa y exigidos al proveedor.
- Atención de averías dentro de los tiempos establecidos en el Acuerdo de Nivel de Servicio (SLA) definido por el ISP.

Desventajas de esta alternativa:

- Dependencia del proveedor ISP para la atención de incidencias y la ejecución de nuevas activaciones o modificaciones del servicio.
- Necesidad de contratar e implementar un enlace adicional en la sede principal de Surco, provisto por el mismo ISP, para permitir la interconexión con las sedes remotas.

- Mayor tiempo de implementación debido a la distancia considerable entre el nodo más cercano del proveedor y las sedes remotas, lo que implica la instalación de más de dos radios por cada sede.
- Costo inicial elevado, debido a la necesidad de instalar al menos tres radios por sede remota, incrementando significativamente el pago por concepto de instalación.

***B. Implementación de un servicio de fibra óptica.*** Esta alternativa contemplaba la implementación de un servicio de conectividad mediante fibra óptica, proporcionado por un operador de telecomunicaciones, con el fin de interconectar las sedes remotas con la sede principal de la empresa CR Techonology. La fibra óptica permitía una alta capacidad de transmisión de datos, baja latencia y mayor estabilidad en la comunicación.

Ventajas de esta alternativa:

- Alta velocidad de transmisión de datos y mayor ancho de banda en comparación con otras tecnologías.
- Baja latencia y alta confiabilidad del enlace, lo que garantiza un desempeño óptimo para aplicaciones críticas.
- Menor susceptibilidad a interferencias electromagnéticas y condiciones climáticas adversas.
- Servicio administrado y monitoreado por un operador de telecomunicaciones certificado.
- Posibilidad de escalabilidad en el ancho de banda según las necesidades futuras de la empresa.

Desventajas de esta alternativa:

- Limitada disponibilidad de infraestructura de fibra óptica en las zonas donde se ubican las sedes remotas.
- Alto costo de implementación inicial debido a la necesidad de realizar obras civiles para el tendido de fibra en tramos donde no existe cobertura.
- Dependencia del operador de telecomunicaciones para la atención de incidencias, ampliaciones o modificaciones del servicio.
- Tiempos prolongados de implementación asociados a permisos municipales, obras de canalización y despliegue de la infraestructura.
- Costos recurrentes elevados en comparación con otras alternativas de conectividad, lo que impacta en el presupuesto operativo de la empresa.

***C. Implementación de antenas Starlink con VPN Site to Site.*** Esta alternativa proponía la implementación de antenas satelitales Starlink en cada una de las sedes remotas, utilizando la infraestructura de Internet satelital de órbita baja (LEO), junto con equipos de red que permitieran la configuración de una VPN Site-to-Site basada en el protocolo IPsec para la interconexión con la sede principal de la empresa, ubicada en Surco.

La solución planteaba establecer un canal de comunicación cifrado a través de Internet, lo que garantizaba la confidencialidad, integridad y autenticidad de la información transmitida entre las sedes, independientemente del medio de acceso proporcionaba por Starlink.

Ventajas de esta alternativa:

- Amplia cobertura geográfica, lo que permite su implementación en zonas donde no existe disponibilidad de fibra óptica ni enlaces de radio.
- Menor tiempo de implementación, al no requerir obras civiles ni infraestructura terrestre adicional.
- Independencia de operadores ISP locales para la provisión del acceso a Internet.
- Alta disponibilidad y estabilidad del servicio gracias al uso de satélites de órbita baja.
- Posibilidad de implementar mecanismos de seguridad avanzados mediante VPN IPsec, asegurando la transmisión de datos entre sedes.
- Escalabilidad de la solución, permitiendo la incorporación de nuevas sedes remotas de manera sencilla.

Desventajas de esta alternativa:

- Latencia superior en comparación con enlaces terrestres como la fibra óptica, debido a la naturaleza satelital del servicio.
- Dependencia de condiciones climáticas extremas que podrían afectar la calidad del enlace en determinados escenarios.
- Necesidad de contar con equipos adicionales (firewalls o routers con capacidad IPsec) para la implementación de la VPN Site-to-Site.
- Costos recurrentes asociados al servicio de suscripción de Starlink.
- Requerimiento de conocimientos técnicos especializados para la configuración y mantenimiento de la VPN IPsec.

**Tabla 1**

*Comparación de alternativas tecnológicas*

| **Criterio** | **Radio Enlace** | **Fibra Óptica** | **Starlink + VPN IPsec** |
|---|---|---|---|
| Tipo de tecnología | Radiofrecuencia terrestre | Enlace terrestre por fibra óptica | Internet satelital LEO + VPN IPsec |
| Cobertura geográfica | Limitada a zonas con infraestructura del ISP | Limitada a zonas con despliegue de fibra | Amplia cobertura, ideal para zonas remotas |
| Tiempo de implementación | Alto | Alto | Bajo |
| Obras civiles requeridas | No | Sí | No |
| Dependencia de operador local | Alta | Alta | Baja |
| Ancho de banda | Medio | Alto | Medio–Alto |
| Latencia | Media | Baja | Media |
| Estabilidad del enlace | Media–Alta | Alta | Alta |
| Seguridad de la información | Media (según ISP) | Media (según ISP) | Alta (cifrado IPsec) |
| Escalabilidad | Media | Alta | Alta |
| Costo de implementación inicial | Alto | Alto | Medio |
| Costo operativo mensual | Alto | Alto | Medio |
| Flexibilidad de expansión | Limitada | Limitada | Alta |
| Adecuación a sedes remotas | Media | Baja | Alta |

*Nota.* Elaboración propia (s.f.)

Del análisis respecto al cuadro previo se observó que, si bien las alternativas basadas en radio enlace y fibra óptica ofrecían buen rendimiento, presentaban limitaciones significativas en términos de cobertura, tiempo de implementación y costos, especialmente en zonas remotas. Por

otro lado, la alternativa basada en tecnología Starlink con VPN Site-to-Site IPsec destacaba por su rápida implementación, la no dependencia de terceros, amplia cobertura y alto nivel de seguridad, lo que la convirtiera en la opción más adecuada para satisfacer los requerimientos de conectividad segura de la empresa CR Technology.

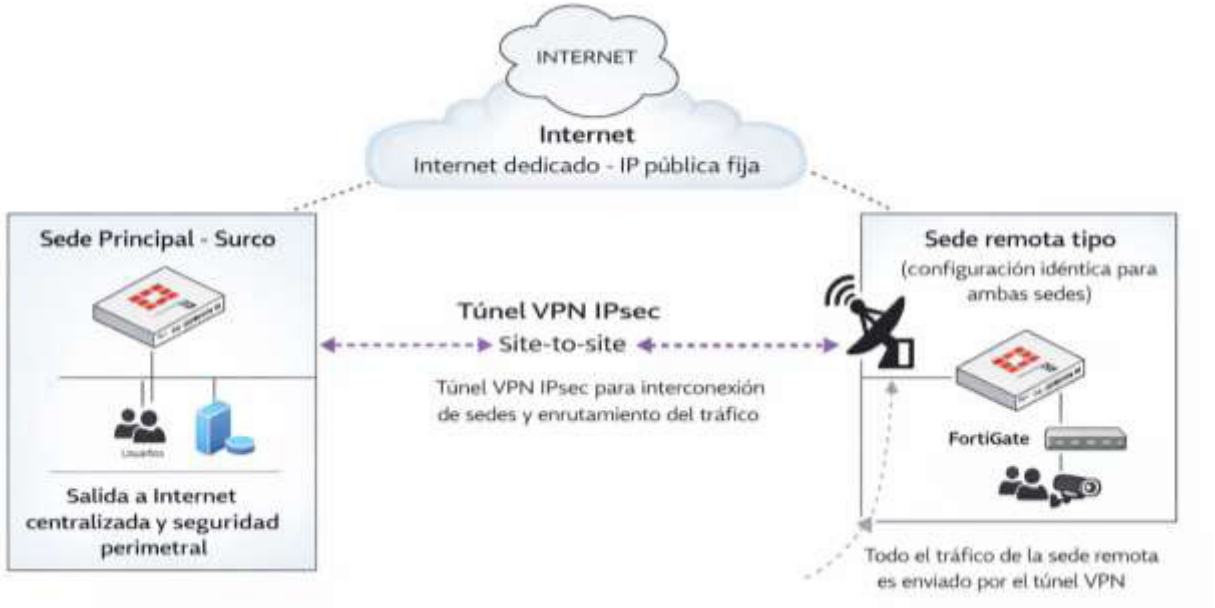
**2.3.4.3. Implementación de la solución Starlink + VPN.** Como resultado del análisis del problema y la evaluación de las alternativas, se seleccionó la implementación de Internet mediante tecnología Starlink, complementado con VPN Site-to-Site IPsec, como la opción más adecuada para interconectar las sedes remotas de la empresa con la sede principal en Surco.

Esta solución se justificó tanto por su rapidez de implementación, como por su cobertura en zonas remotas, su seguridad en la transmisión de información y su costo eficiente en relación con las necesidades reales de las sedes, que incluían únicamente dos trabajadores y tres cámaras de videovigilancia por sede.

***A. Arquitectura general de la solución.*** A continuación, se presenta la arquitectura general de la solución propuesta, la cual describía el diseño de interconexión de las sedes remotas con la sede principal de la empresa CR Technology, así como la centralización de la salida a Internet a través de la infraestructura de seguridad perimetral de la sede de Surco.

**Figura 16**

*Arquitectura general de la solución Starlink + VPN IPsec*




*Nota.* Elaboración propia (s.f.)

La arquitectura general de la solución propuesta se basaba en un esquema de conectividad Site-to-Site que permitía no solo la interconexión de las dos sedes remotas con la sede principal de la empresa CR Technology, ubicada en el distrito de Surco, sino también la centralización de la salida a Internet de dichas sedes a través de la infraestructura de seguridad perimetral existente en la sede principal.

Cada sede remota disponía de un enlace de Internet satelital Starlink, el cual brindaba conectividad mediante tecnología de satélites de órbita baja (LEO). Dicho enlace se conectaba a un dispositivo router encargado de la administración de los túneles VPN IPsec y del enrutamiento de tráfico hacia la sede principal, lo que garantiza la confidencialidad e integridad de la información transmitida a través de la red pública de Internet.

La sede principal de Surco contaba con un enlace de Internet dedicado de alta capacidad y un firewall perimetral, el cual actuaba como nodo central de la arquitectura, donde se concentraban los túneles VPN IPsec provenientes de las sedes remotas. A través de estos túneles se habilitó la comunicación cifrada hacia a los recursos corporativos de la empresa, así como la salida a Internet de las sedes remotas bajo un esquema de seguridad gestionada.

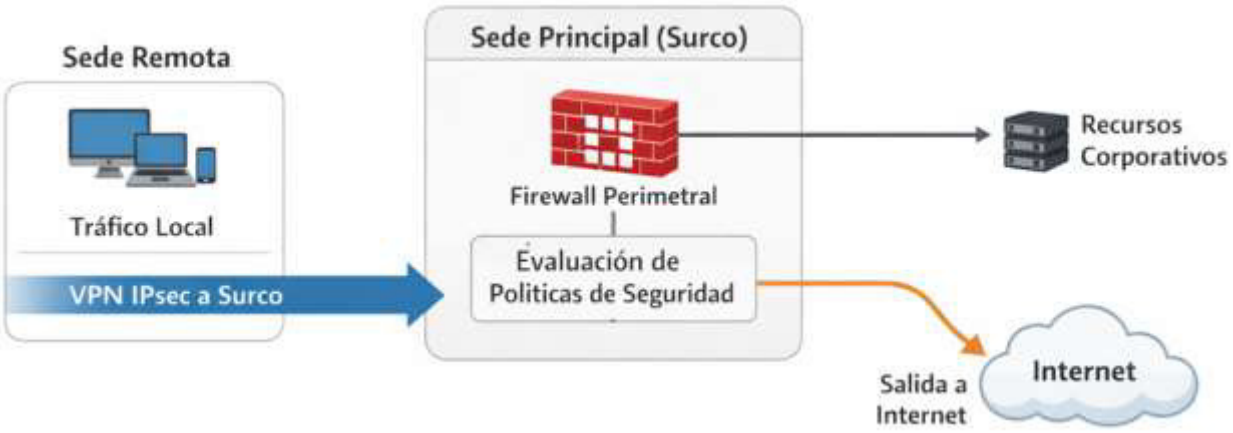
La arquitectura diseñada permitía la segmentación del tráfico, lo que diferenciaba el tráfico local, el tráfico corporativo y el tráfico de navegación hacia Internet. El diseño facilitó la aplicación de políticas de seguridad centralizadas, el monitoreo del tráfico y el cumplimiento de las políticas corporativas establecidas por la empresa.

Finalmente, la solución propuesta ofrecía escalabilidad, lo que permitía la incorporación de nuevas sedes remotas mediante el mismo esquema propuesto, sin requerir modificaciones significativas en la infraestructura existente.

***B. Flujo de tráfico y salida a internet centralizada.*** El flujo de tráfico de la solución propuesta fue diseñado para garantizar una comunicación segura y eficiente entre las sedes remotas y la sede principal de la empresa CR Technology, así como para centralizar el control de la salida a Internet bajo el esquema de seguridad gestionada.

**Figura 17**

*Flujo de tráfico y salida a internet centralizada*




*Nota.* Elaboración propia (s.f.)

En las sedes remotas, el tráfico generado por los usuarios y dispositivos locales era enviado hacia el dispositivo router encargado de la administración de los túneles VPN IPsec, no existía salida directa a Internet. Todo el tráfico destinado a recursos corporativos y a la navegación por Internet era enviado a través del túnel VPN hacia la sede principal de Surco, evitando la salida directa a Internet desde las sedes remotas.

Una vez que el tráfico llegaba a la sede principal, el firewall perimetral aplica las políticas de seguridad como control de acceso, inspección y monitoreo. Luego, el tráfico autorizado se dirigía al enlace de Internet dedicado, lo que garantizó una salida controlada y centralizada.

El tráfico destinado a los recursos internos se gestionó de forma independiente, lo que permitía el acceso a servidores y sistemas corporativos mediante túneles VPN IPsec, bajo el control de las políticas de seguridad perimetral de la sede principal.

El diseño del flujo de tráfico implementado permitió una administración unificada de la seguridad y facilitó la supervisión del uso de Internet por parte de las sedes remotas al concentrar los mecanismos en un único punto de control.

***C. Implementación de la solución en sedes remotas.*** La implementación de la solución propuesta se llevó a cabo en las dos sedes remotas de la empresa CR Technology, las cuales necesitaban conectividad y acceso a Internet gestionado de manera centralizada. El alcance del presente proyecto comprendió exclusivamente la implementación de los elementos de conectividad y comunicación en dichas sedes remotas, aprovechando la infraestructura de seguridad perimetral y el enlace de Internet dedicado preexistentes en la sede principal ubicada en Surco.

En cada sede remota se realizó la instalación de una antena satelital Starlink estándar, el cual constituye el medio de conectividad principal hacia la red pública de Internet. Este enlace actuó como punto de entrada y salida del tráfico, que posteriormente fue utilizado como un canal para los túneles VPN IPsec definidos en la solución. Dado que el servicio de Internet satelital Starlink elegido opera bajo un esquema CGNAT, la arquitectura fue diseñada con equipamiento y tecnología capaces de establecer y mantener túneles VPN IPsec sin depender de direcciones IP públicas fijas en uno de los extremos, específicamente en las sedes remotas.

Para la creación de los túneles VPN IPsec y el encaminamiento del tráfico hacia la sede principal, en cada sede remota se implementó un router FortiGate modelo 40F. Estos dispositivos fueron utilizados exclusivamente como equipos para la gestión de los túneles VPN IPsec y el

direccionamiento del tráfico, sin desempeñar funciones de seguridad perimetral local, las cuales se mantuvieron centralizadas en la sede principal de Surco.

La conexión física entre el sistema de acceso a Internet satelital Starlink y el router FortiGate 40F se realizó mediante cableado Ethernet, permitiendo el envío y recepción del tráfico del enlace satelital. Los equipos implementados fueron instalados en gabinetes de comunicaciones existentes en cada sede remota, lo que garantizó un entorno adecuado para su operación. Posteriormente, el tráfico fue distribuido hacia la red LAN a través de un switch no gestionable proporcionado por la empresa CR Technology, modelo TP-Link TL-SF1024, el cual permitió la conexión de los dispositivos finales, considerando la limitada cantidad de puertos Ethernet disponibles en el router Fortigate.

La comunicación entre las sedes remotas y la sede principal se estableció mediante túneles VPN IPsec de tipo Site-to-Site, permitiendo que tanto el tráfico da datos como el tráfico de navegación hacia Internet sean encapsulados, encriptados y transmitidos de forma segura hacia la sede central. De esta manera, se garantizó que la salida a Internet de las sedes remotas se realice bajo las políticas de seguridad definidas en el equipo perimetral de la sede principal.

El esquema de conectividad implementado permitió el uso de direccionamiento IP dinámico en enlaces satelitales, incorporando mecanismos de resolución dinámica que aseguraron la disponibilidad de los túneles VPN IPsec sin requerir configuraciones manuales recurrentes ante cambios de direccionamiento.

Finalmente, la solución implementada centralizó la gestión de conectividad y seguridad, asegurando una comunicación segura, confiable y escalable entre las sedes remotas y la sede principal.

***D. Evidencias de la implementación.*** Con la finalidad de respaldar la correcta ejecución de la solución propuesta, en el presente apartado se presentaron las evidencias correspondientes de la implementación realizada en las sedes remotas de la empresa CR Technology. Estas evidencias permitieron verificar la instalación física de los componentes, así como la integración de los elementos que conforman la solución de conectividad y salida a Internet centralizada.

Las evidencias correspondieron principalmente a la instalación del sistema de acceso a Internet satelital Starlink estándar, la implementación del firewall FortiGate 40F como dispositivo de borde para la terminación de los túneles VPN IPsec y la interconexión física entre los distintos componentes de la red LAN en cada sede remota.

**Figura 18**

*Instalación de la antena Starlink estándar en sede remota*

*Nota.* Elaboración propia (s.f.)

**Figura 19**

*Equipo FortiGate 40F instalado en gabinete de comunicaciones*

*Nota.* Elaboración propia (s.f.)

**Figura 20**

*Interconexión física de los equipos*


*Nota.* Elaboración propia (s.f.)

**Figura 21**

*Vista general del gabinete o área de comunicaciones*

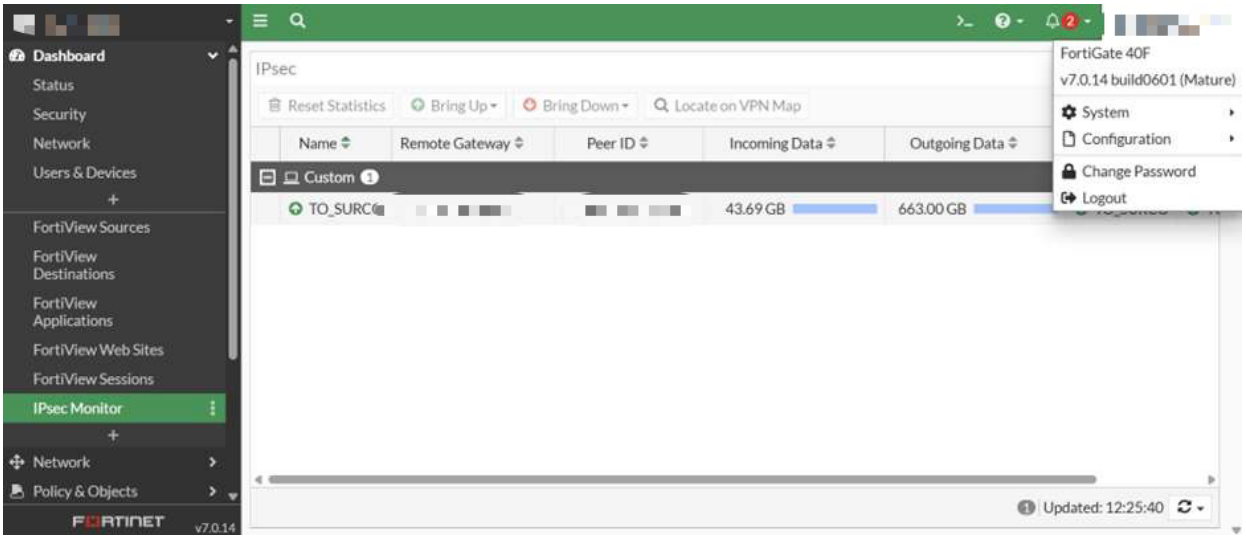
*Nota.* Elaboración propia (s.f.)

***E. Validación de la solución implementada.*** Con la finalidad de respaldar la correcta ejecución de la solución propuesta, en el presente apartado se presentó las evidencias correspondientes de la implementación realizada en las sedes remotas. Estas evidencias permitieron verificar la instalación física de los componentes, así como la integración de los elementos que conforman la solución de conectividad y salida a Internet centralizada.

En primer lugar, se verificó el establecimiento correcto de los túneles VPN IPsec entre cada una de las sedes remotas y la sede principal. Esta validación confirmó que los dispositivos FortiGate 40F instalados en las sedes remotas negociaron correctamente los parámetros de seguridad con el firewall perimetral de la sede principal, manteniendo los túneles en estado activo y estable, lo que garantizó la autenticación y encriptación de los datos transmitidos.

**Figura 22**

*Estado activo del túnel VPN IPsec entre sede remota y sede principal.*

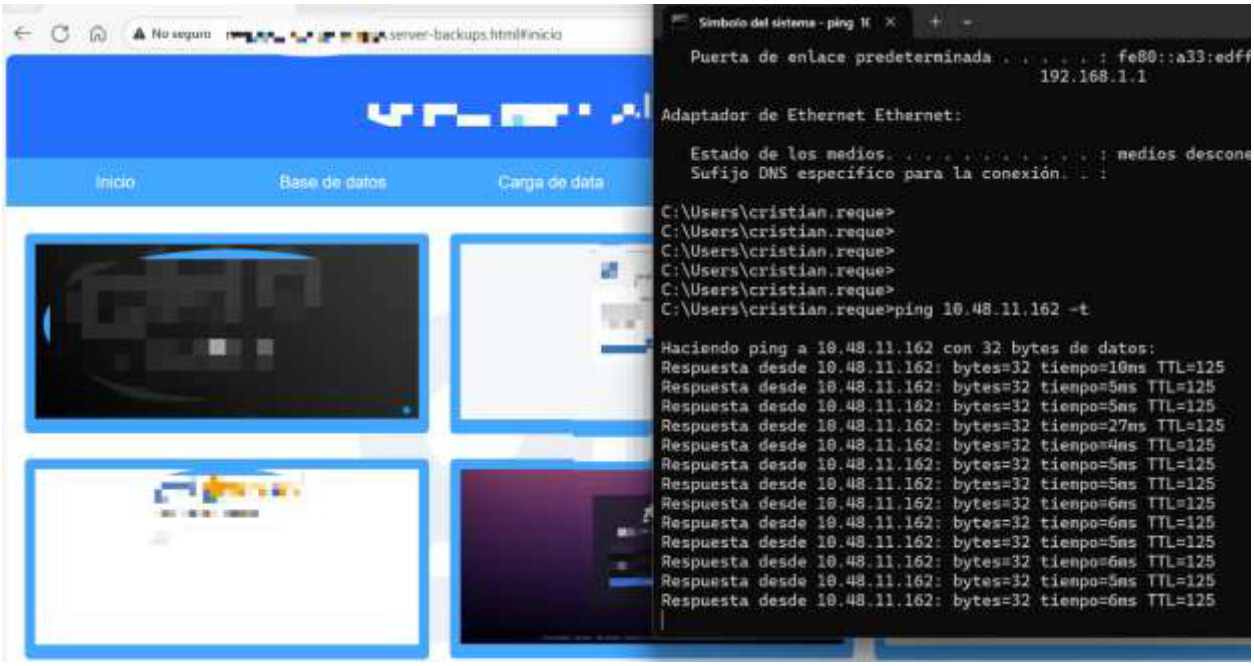



*Nota.* Elaboración propia (s.f.)

Posteriormente, se validó la conectividad hacia los recursos internos de la empresa alojados en la sede principal. Desde las sedes remotas se comprobó el acceso a sistemas y servicios corporativos, evidenciando que el tráfico fue transportado correctamente a través de los túneles VPN IPsec, lo que permitió que las redes involucradas se comuniquen como si formaran parte de una misma red LAN.

**Figura 23**

*Acceso desde sede remota a recurso interno alojado en la sede principal.*



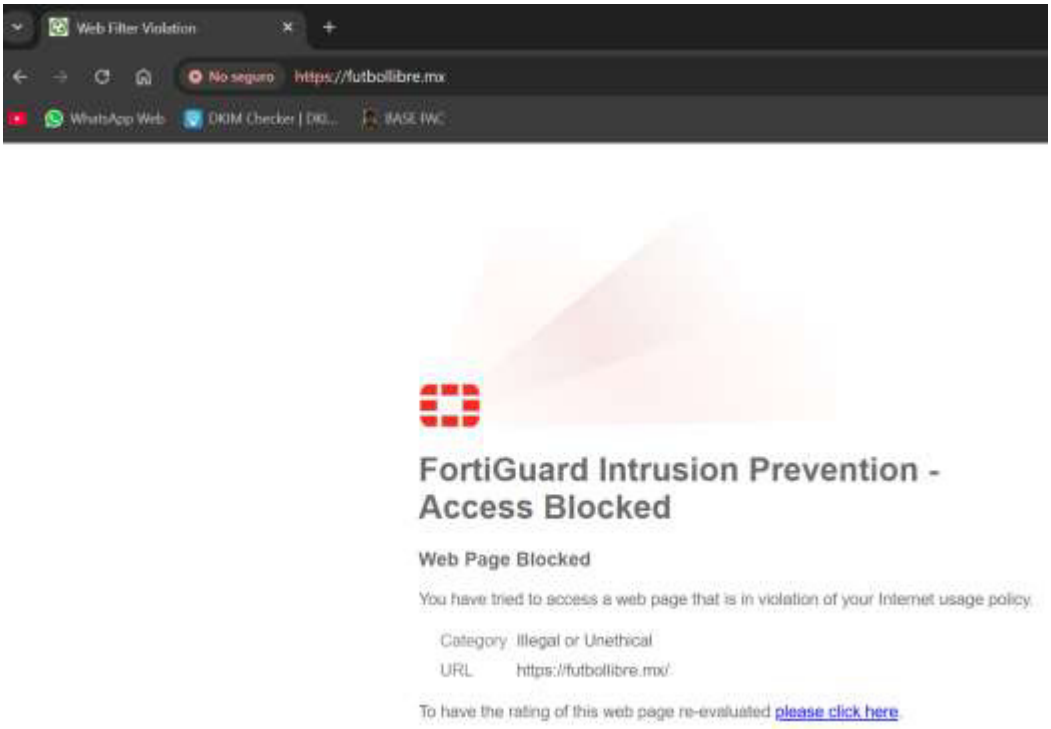

*Nota.* Elaboración propia (s.f.)

Como parte de las pruebas de salida a Internet centralizada, se verificó que el tráfico de navegación generado en las sedes remotas no realizará una salida de internet directa, sino que es enviado a través del túnel VPN hacia la sede principal. En este punto, el firewall perimetral aplicó las políticas de seguridad definidas por la empresa, incluyendo mecanismos de control y restricción de acceso a sitios web no autorizados.

Para validar este comportamiento, se realizó una prueba de acceso a un sitio web bloqueado por las políticas de seguridad perimetral, se comprobó que la restricción se ejecutó correctamente considerando que el acceso se origina desde una sede remota, lo que evidenció el control de navegación centralizado a través de la sede principal.

**Figura 24**

*Bloqueo de acceso a sitio web no autorizado desde sede remota mediante seguridad perimetral centralizada.*




*Nota.* Elaboración propia (s.f.)

Finalmente, los resultados obtenidos durante las pruebas realizadas demostraron que la solución implementada cumplió con los objetivos propuestos, lo que garantizó una conectividad estable desde las sedes remotas, una interconexión mediante túneles VPN IPsec y una salida a Internet controlada y gestionada desde la sede principal de Surco. Asimismo, la solución validada permitió una administración unificada de la seguridad y quedó como antecedente para nuevas sedes remotas de difícil acceso a infraestructuras de telecomunicaciones convencionales.

Las evidencias técnicas correspondientes a la configuración lógica de los equipos, la implementación de los túneles VPN IPsec y la validación del funcionamiento de la solución se

presentaron en la sección de anexos, a fin de complementar la información desarrollada en el presente capítulo.

## 2.4 Análisis económico de la solución

El presente apartado tuvo como objetivo presentar los costos asociados a la implementación de la solución propuesta, considerando la inversión inicial requerida y los costos operativos necesarios para la implementación en las sedes remotas de la empresa CR Technology.

### *2.4.1 Cuadro de inversión*

El cuadro de inversión presentó los costos asociados a la implementación de la solución de internet mediante VPN IPsec sobre tecnología Starlink en las dos sedes remotas con la empresa CR Technology. Para el análisis se consideraron los costos de inversión inicial (CAPEX), relacionados con la adquisición de equipamiento y la ejecución de la implementación, así como los costos operativos recurrentes (OPEX), correspondientes al servicio de conectividad.

No se incluyeron en este análisis los equipos ni la infraestructura preexistente, tales como el firewall perimetral FortiGate 100F de la sede de Surco y los gabinetes de comunicaciones de las sedes remotas, debido a que no forman parte del alcance del proyecto. El costo de la mano de obra incluyó las actividades de instalación física, interconexión de equipos y cableado necesario para la puesta en funcionamiento de la solución.

**Tabla 2**

*Costos de implementación (CAPEX)*

| Ítem | Descripción | Cantidad | Costo unitario | Costo total (S/) |
|---|---|---|---|---|
| 1 | Firewall FortiGate 40F | 2 | USD 250 | 1,780 |
| 2 | Kit Starlink estándar | 2 | S/ 1,449 | 2,898 |
| 3 | Envío y gestión Starlink | 2 | S/ 89 | 178 |
| 4 | Switch no gestionable TP-Link TL-SF1024 | 2 | S/ 259 | 518 |
| 5 | Mano de obra de implementación (2 días) | 1 | S/ 240 | 240 |
| | **Total CAPEX** | | | **S/ 5,614** |

*Nota.* Elaboración propia (s.f.)

Para la conversión de moneda se utilizó un tipo de cambio referencial de S/ 3.56 por dólar estadounidense, vigente durante el periodo de ejecución del proyecto. El costo de la mano de obra incluyó las actividades de instalación física, interconexión de equipos y cableado necesario para la puesta en funcionamiento de la solución.

**Tabla 3**

*Costos operativos (OPEX)*

| Ítem | Descripción | Cantidad | Costo mensual unitario | Costo mensual total |
|---|---|---|---|---|
| 1 | Servicio Starlink empresarial (500 GB) | 2 | S/ 370 | S/ 740 |

*Nota.* Elaboración propia (s.f.)

### *2.4.2 Costos de implementación (CAPEX)*

Los costos de implementación (CAPEX) correspondieron a la inversión inicial para la puesta en funcionamiento de la solución de Internet mediante VPN IPsec sobre tecnología Starlink en las sedes remotas de la empresa CR Technology. Estos costos estuvieron asociados principalmente a la adquisición de equipamiento de red y a las actividades de instalación requeridas para habilitar el servicio.

Dentro del CAPEX se contempló la adquisición e instalación de los kits Starlink estándar, que permitieron el acceso a Internet satelital en zonas de difícil cobertura, así como la compra de los routers FortiGate 40F, destinados al soporte de los túneles VPN IPsec en cada sede remota. Asimismo, se incluyó la adquisición de switches no gestionables, necesarios para la distribución del tráfico hacia la red LAN de cada sede.

Adicionalmente, el CAPEX contempló los costos de mano de obra correspondientes a las actividades de implementación física como la instalación de los equipos, la interconexión mediante cableado Ethernet y la puesta en operación de la infraestructura. No se incluyeron dentro de estos costos los equipos ni la infraestructura preexistente en la sede principal, dado que formaban parte de la plataforma operativa ya disponible en la empresa.

### *2.4.3 Costos operativos (OPEX)*

Los costos operativos (OPEX) correspondieron a los gastos recurrentes necesarios para mantener en funcionamiento la solución de Internet con VPN IPsec sobre tecnología Starlink una vez finalizada su implementación. Estos costos estuvieron asociados principalmente al servicio de

conectividad de Internet satelital y a la operación continua de la infraestructura instalada en las sedes remotas.

En el presente proyecto, el principal componente del OPEX estuvo representado por el servicio Starlink empresarial, que contempla un plan mensual de datos de 500 GB por sede remota. Este servicio permitió garantizar el acceso a Internet en ubicaciones donde no existe disponibilidad de infraestructura de telecomunicaciones convencional, asegurando la continuidad operativa de las sedes y la interconexión segura con la sede principal mediante túneles VPN IPsec.

No se consideraron dentro de los costos operativos gastos adicionales por licenciamiento de los equipos FortiGate 40F, dado que la funcionalidad de VPN IPsec utilizada formaba parte de las capacidades base del equipo. Asimismo, no se incluyeron costos asociados a mantenimiento preventivo, correctivo ni soporte técnico especializado externo, debido a que la administración, monitoreo y gestión de la solución fueron realizados por personal técnico interno de la empresa CR Technology como parte de sus funciones habituales.

De igual manera, el servicio Starlink empresarial incluyó dentro de su suscripción el soporte básico del enlace satelital, por lo que no se generaron costos adicionales relacionados con la operación de este servicio.

En consecuencia, el OPEX del proyecto se mantuvo controlado, limitándose esencialmente al pago mensual del servicio de conectividad satelital, lo que representó una ventaja frente a otras alternativas de acceso a Internet que implican mayores costos operativos, contratos de mantenimiento adicionales o dependencia de proveedores locales.

### *2.4.3 Análisis costo-beneficio de la solución*

El análisis costo–beneficio de la solución implementada permitió evaluar la relación entre la inversión realizada y los beneficios operativos obtenidos por la empresa CR Technology. La implementación de Internet con VPN IPsec sobre tecnología Starlink representó una inversión inicial moderada en comparación con alternativas tradicionales de conectividad en zonas de difícil acceso.

Uno de los principales beneficios de la solución fue la flexibilidad contractual del servicio Starlink empresarial, el cual no exigió contratos de permanencia por periodos prolongados. Esta característica permite que las empresas puedan cancelar el servicio en cualquier momento sin penalidades por terminación anticipada. A diferencia de los operadores convencionales de telecomunicaciones, esta flexibilidad redujo el riesgo financiero y la dependencia de contratos definidos.

Adicionalmente, el equipamiento adquirido para la implementación (kit Starlink y dispositivos modem) pasó a ser propiedad de la empresa, lo que elimina costos asociados a alquileres, devoluciones o penalidades contractuales. La solución también permitió una rápida implementación, disponibilidad inmediata del servicio y control centralizado de la seguridad, factores que contribuyeron a mejorar la eficiencia operativa de la empresa.

Se concluyó que la solución propuesta presentó una relación costo–beneficio favorable, al combinar flexibilidad contractual, rapidez de despliegue, control centralizado de la seguridad y costos operativos predecibles. Esta arquitectura permitió optimizar recursos disponibles al

aprovechar el enlace de Internet dedicado existente en la sede principal de Surco, evitando la contratación de nuevos servicios y reduciendo gastos recurrentes. Además, la interconexión segura entre las sedes remotas y la sede principal garantiza la protección de la información corporativa mediante políticas unificadas, lo que contribuye a mantener la integridad y disponibilidad de los datos. La solución también facilitó la administración y el monitoreo desde un punto central, disminuyendo la complejidad operativa y mejorando los tiempos de respuesta ante incidencias. Por estas razones, la propuesta se consideró adecuada y eficiente para sedes remotas ubicadas en zonas con limitada disponibilidad de infraestructura de telecomunicaciones.

Asimismo, se presentó el análisis de costo total a 3 años comparando la solución Starlink+VPN frente a alternativas tradicionales. Para este cálculo, se sumó CAPEX inicial más OPEX acumulado (36 meses).

**Tabla 4**

*Análisis comparativo de costos*

| Solución | CAPEX | OPEX mensual | OPEX 36m | Total 36m | Ahorro % |
|---|---|---|---|---|---|
| Starlink+VPN | S/ 5,614 | S/ 740 | S/ 26,640 | S/ 32,254 | BASE |
| Radioenlace | S/ 15,000 | S/ 800 | S/ 28,800 | S/ 43,800 | -36% |
| Fibra óptica | S/ 28,000 | S/ 1,200 | S/ 43,200 | S/ 71,200 | -121% |

*Nota.* Elaboración propia (s.f.)

La tabla evidencia que Starlink+VPN genera un ahorro del 36% versus radioenlace y 121% versus fibra óptica en 36 meses. El cálculo consideró CAPEX inicial S/5,614 más OPEX acumulado S/740 × 36 = S/26,640, resultando en un costo total de S/32,254. A partir del mes 8, la

alternativa Starlink + VPN presenta un menor costo acumulado que las soluciones de radioenlace y fibra óptica.

En consecuencia, se concluyó que la solución propuesta ofreció una relación costo-beneficio favorable, combinando flexibilidad contractual, rapidez de despliegue, control centralizado de la seguridad. La solución Starlink + VPN no genera ingresos adicionales, pero permite una reducción del costo total de conectividad respecto a otras alternativas. El análisis demuestra que Starlink + VPN representa la opción de menor costo total a 36 meses, generando ahorros de 36% frente a un radioenlace y del 121% frente a la fibra óptica.

## III. APORTES MÁS DESTACABLES A LA EMPRESA / INSTITUCIÓN

La aplicación de mis habilidades, fortalezas y competencias laborales en conjunto fueron clave para lograr los objetivos trazados por la empresa. Dentro de los aportes brindados a la empresa se destacaron las siguientes contribuciones:

La migración de la plataforma de la red de telefonía softswitch a Broadsoft. Las funciones desempeñadas fueron aprovisionamiento de líneas telefónicas en la nueva plataforma de telefonía IP (Broadsoft), brindando soporte a técnico en campo en momento de cambio de router Gaoke y la ejecución de la migración de plataforma softswitch a broadsoft.

Por otro lado, otro aporte brindado fue la migración masiva de la red LTE a la red LTE MMIMO y Ran Sharing proporcionando a los clientes un mejor servicio tanto en el ancho de banda como cobertura, validando gestión y conectividad a los equipos del cliente final sin tener afectación de este.

Finalmente, se conformó la formación e integrar el equipo que implementó la red de Falabella con Entel y ser el ingeniero residente del Grupo Falabella. Dentro de las labores realizadas fueron realizar la configuración y troubleshooting de los equipos Core de la red MPLS, Cisco, Huawei, Extreme, ZTE, GAOKE, Ericsson, Ubiquiti, Raisecom. Manejé tecnologías WiMAX E, WIMAX D, LTE, MMIMO, Radwin, Radioenlace, Fibra Óptica, GPON FIBERHOME, GPON HUAWEI, ADM, DSL, Telefonía IP, Voz IP. Por otro lado, también realicé la configuración y enrutamiento de protocolos BGP, OSPF, EIGRP & RIP; con redundancia HSRP

y VRRP, fui encargado de la Administración y configuración de seguridad perimetral a nivel core y de cara a los clientes (Firewall Fortigate, Firewall Fortinet), Creación de VPN IPSEC y SSL en firewall en soluciones especiales.

# IV. CONCLUSIONES

De acuerdo con el trabajo de investigación realizado, se llegó a las siguientes conclusiones:

**4.1.** La implementación de una solución de Internet con VPN IPsec sobre tecnología Starlink permitió resolver de manera efectiva la falta de conectividad en dos sedes remotas de la empresa CR Technology ubicadas en zonas de difícil acceso a infraestructura de telecomunicaciones convencional, garantizando el acceso a Internet y la interconexión cifrada con la sede principal.

**4.2.** El servicio Starlink empresarial con antena estándar permitió habilitar conectividad en sedes remotas ubicadas en zonas de difícil acceso a infraestructura de telecomunicaciones tradicional, actuando como medio de transporte hacia la red pública de Internet. Por lo que se concluyó que el aprovechamiento de este servicio dentro de un entorno corporativo requiere la integración de equipamiento adicional, como el equipo FortiGate 40F, que posibilitó la implementación de túneles VPN IPsec, la interconexión con la sede principal y la centralización de la salida a Internet bajo políticas de seguridad del equipo perimetral.

**4.3.** La implementación de los túneles VPN IPsec Site-to-Site garantizó una comunicación cifrada y segura entre las sedes remotas y la sede principal de Surco, garantizando la confidencialidad e integridad de la información transmitida. A partir de esta interconexión, y gracias a una adecuada definición de la arquitectura y a la selección de equipos con soporte corporativo para IPsec, fue posible centralizar la salida a Internet a través de la sede principal, aun cuando las sedes remotas operaban bajo el esquema CGNAT del servicio Starlink.

**4.4.** Las pruebas realizadas durante la etapa de validación demostraron que la solución implementada cumple con los objetivos planteados, garantizando conectividad en las sedes remotas, interconexión mediante túneles VPN IPsec y salida a Internet centralizada a través de la sede principal de Surco. La solución permitió una administración centralizada de la seguridad y del tráfico de red, aprovechando la infraestructura existente de la empresa. Finalmente, la arquitectura diseñada presentó un enfoque escalable y replicable, lo que permitiría su futura implementación en nuevas sedes remotas de características similares, especialmente en zonas de difícil acceso a infraestructura de telecomunicaciones convencional.

**4.5.** Desde el punto de vista económico, la solución que se implementó presentó una relación costo beneficio favorable, al aprovechar infraestructura preexistente, minimizar costos operativos recurrentes y evitar contratos rígidos con proveedores de telecomunicaciones tradicionales, lo que otorgó mayor flexibilidad y control de recursos a la empresa.

**4.6.** Finalmente, la solución implementada se estableció como un modelo ejemplo para futuras sedes remotas de la empresa CR Technology, constituyéndose en una alternativa para proyectos de conectividad en ubicaciones rurales o de difícil acceso, manteniendo niveles de seguridad, control y continuidad operativa.

# V. RECOMENDACIONES

A partir de los resultados obtenidos durante la implementación de Internet con VPN IPsec sobre tecnología Starlink para las sedes remotas de la empresa CR Technology, se proponen las siguientes recomendaciones orientadas a optimizar y ampliar la solución implementada en escenarios futuros.

**5.1.** Se recomienda considerar la arquitectura implementada como un modelo de ejemplo para futuras sedes de la empresa ubicadas en zonas rurales o de difícil acceso a infraestructura de telecomunicaciones convencionales. La solución basada en Starlink y VPN IPsec permite una rápida respuesta en operación sin necesidad de obras civiles complejas ni contratos de largo plazo con operadores ISP.

**5.2.** Se recomienda implementar mecanismos de monitoreo que permitan supervisar el estado de los túneles VPN IPsec, el uso del ancho de banda y la disponibilidad del enlace satelital. Esto facilitará la detección temprana de posibles incidentes y una respuesta oportuna ante eventuales degradaciones de los enlaces.

**5.3.** Se sugiere mantener y actualizar periódicamente las políticas de seguridad aplicadas en la sede principal, considerando la evolución de las amenazas y los requerimientos operativos de las sedes remotas. Esto incluye la revisión de reglas de acceso, control de navegación y segmentación del tráfico, aprovechando que la salida a internet esta centralizada.

**5.4.** Se recomienda elaborar y mantener actualizada la documentación técnica de la solución implementada, así como brindar capacitación básica al personal encargado de la administración de la red lan. Esto facilitará la operación, el mantenimiento y la resolución de incidentes, minimizando la dependencia de un soporte externo.

**5.5.** Para escenarios donde la continuidad del servicio es crítica, es conveniente evaluar la incorporación de enlaces de respaldo o soluciones de alta disponibilidad que complementen la solución actual, como enlaces móviles o una segunda conexión satelital, asegurando mayor resiliencia ante fallas del enlace primario en cada sede remota o sede nueva.

# VI. REFERENCIAS


Álvarez-Gayou, J. J. (2003). *Cómo hacer investigación cualitativa Fundamentos y metodología.* Ediciones Paidós Ibérica S. A.

Bilbao, I. (2024). *Diseño, despliegue y análisis del sistema satelital Starlink como red de acceso.* [Tesis de maestría, Universidad del País Vasco]. Repositorio Institucional UPV/EHU. https://addi.ehu.es/bitstream/handle/10810/68839/TFM%20BilbaoIratI.pdf?sequence=1&isAllowed=y

Chomycz, B. (2002). *Instalaciones de Fibra Óptica: Fundamentos, técnicas y aplicaciones.* Mc Graw Hill.

Conza, A. (2009). *Diseño e implementación de un prototipo de DMZ y la interconexión segura mediante VPN utilizando el Firewall Fortigate 60*. [Tesis de pregrado, Escuela Politécnica Nacional]. Repositorio Digital - EPN. https://bibdigital.epn.edu.ec/handle/15000/1868

Espinoza, J. (2025). *VPN IPsec con FortiGate: laboratorio de seguridad perimetral*. https://www.studocu.com/pe/document/servicio-nacional-de-adiestramiento-en-trabajo-industrial/fortigate/lab-vpn-ipsec-con-fortigate-senati/117655818

Fitzgerald, J. (2003). *Redes y comunicacion de datos en los Negocios.* Editorial Limusa S.A. De C.V.

Handley, M. (2019). Delay is not an option: Low latency routing in space. *Proceedings of the 17th ACM Workshop on Hot Topics in Networks*, (pp. 85–91). doi:https://doi.org/10.1145/3286062.3286075

Hernández Sampieri, R., Fernández Collado , C., & Baptista Lucio, P. (2014). *Metodología de la investigación* (6ª. ed.). Mc Graw Hill Education y Interamericana Editores S.A. de C.V.

Kent, S., & Seo, K. (2005). *Security architecture for the Internet Protocol (RFC 4301).* Internet Engineering Task Force. https://www.rfc-editor.org/rfc/rfc4301

Khan Academy. (2020). *Introducción a la seguridad informática*. https://es.khanacademy.org

Liberatori, M. C. (2018). *Redes de datos y sus protocolos.* Editorial de la Universidad Nacional de Mar del Plata.

Lithman, D. (2025). I*mplementación de una red móvil 4G con Starlink y Zerotier para mejorar la conectividad en la comunidad Sensa – Cusco*. [Tesis de pregrado, Universidad Tecnológica del Perú]. Repositorio UTP. https://hdl.handle.net/20.500.12867/13410

Ojeda Sotomayor, A. O. (2009). *Estudio y diseño de una red FTTH en un campus universitario y una vivienda residencial.* [Tesis de pregrado, Pontifica Universidad Católica del Perú]. Repositorio de Tesis PUCP. http://hdl.handle.net/20.500.12404/854

Perez, S., & Higinio, F. (2017). *Dispositivos y Protocolos y Redes LAN y WAN.* Mendoza: UTN Regional Mendoza.

SpaceX. (2023). *Starlink specifications*. Obtenido de https://www.starlink.com

Stallings, W. (2000). *Comunicaciones y Redes de Computadores* (6a. ed.). Pearson Educación.

Stallings, W. (2017). *Cryptography and network security: Principles and practice* (7a. ed.). Pearson.

Tanenbaum, A., & Wetherall, D. (2012). *Redes de Computadoras* (5ª ed.). Pearson Education.

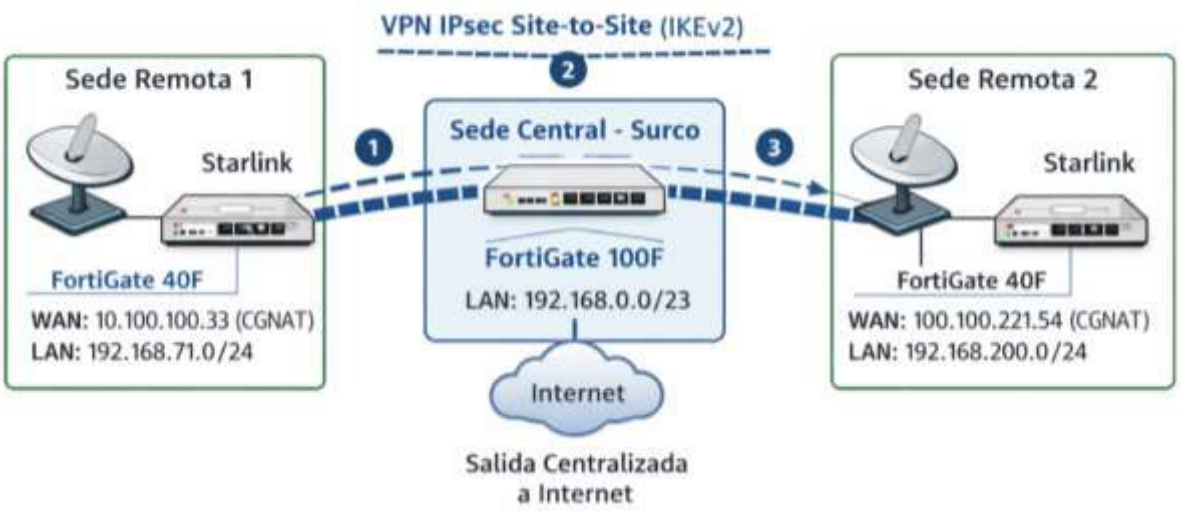
# VII. ANEXOS

## Anexo A – Arquitectura detallada de la solución

El presente anexo describe la arquitectura técnica implementada para brindar acceso a Internet a dos sedes remotas de la empresa CR Technology.

**Figura 25**

*Diagrama lógico de la solución implementada*




*Nota.* Elaboración propia (s.f.)

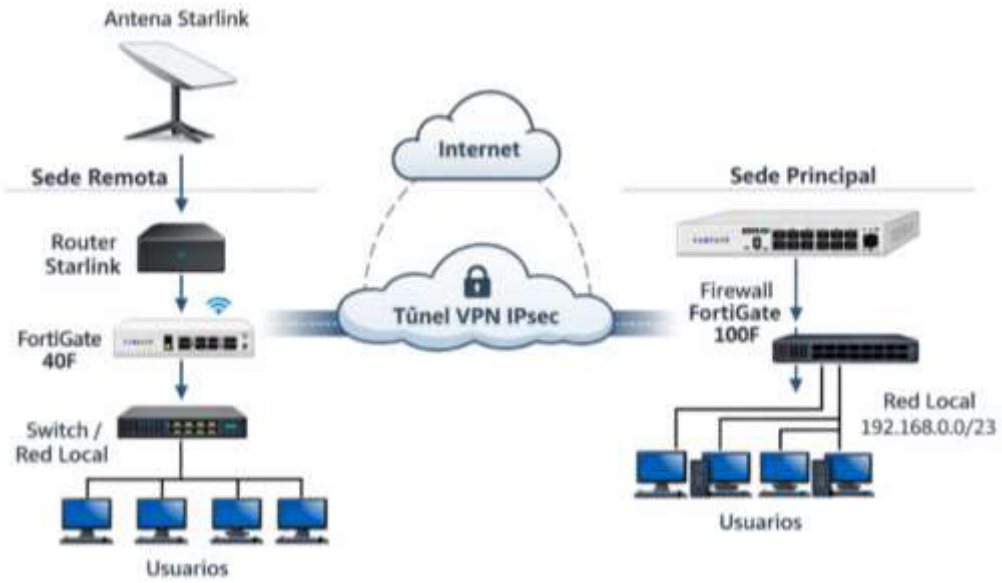
Tal como se muestra en la Figura 25, cada sede remota dispone de un equipo router FortiGate 40F se conecta a Internet a través del servicio Starlink, recibiendo una dirección IP dinámica asignada por el proveedor bajo un esquema de CGNAT. Debido a esta condición, los túneles VPN IPsec se establecieron desde las sedes remotas hacia la sede principal que cuenta con una dirección IP pública fija.

La sede principal, ubicada en el distrito de Surco, utilizó un firewall FortiGate 100F y actúa como punto central de salida a Internet para las sedes remotas. La red local de esta sede corresponde al segmento 192.168.0.0/23, desde donde se gestionan las políticas de seguridad, enrutamiento y traducción de direcciones de red (NAT), así como también los controles de acceso hacia destinos específicos.

Las sedes remotas implementan redes locales independientes, correspondientes a los segmentos 192.168.71.0/24 y 192.168.200.0/24 respectivamente, las cuales acceden a Internet de forma cifrada a través de los túneles VPN IPsec establecidos hacia la sede principal. Esta arquitectura permitió garantizar la confidencialidad del tráfico de red y una administración centralizada del acceso a Internet, evitando accesos no autorizados y contribuyendo a un uso correcto del ancho de banda disponible.

**Figura 26**

*Diagrama físico de la solución implementada*




*Nota.* Elaboración propia (s.f.)

El diagrama físico presentado en la Figura 26 muestra la disposición de los principales componentes de red involucrados en la solución implementada, incluyendo la antena Starlink, el equipo de acceso, los firewalls FortiGate en las sedes remotas y en la sede principal, así como su interconexión con las redes locales correspondientes.

El diagrama presentado en este anexo complementa la arquitectura general descrita en la sección 2.3.4.3.A del Capítulo II, proporcionando un mayor nivel de detalle técnico sobre los componentes de red y el direccionamiento IP utilizados en la solución implementada.

**Anexo B – Plan de direccionamiento IP de la solución**

El presente anexo detalla el esquema de direccionamiento IP utilizado en la implementación de la solución de Internet con VPN IPsec sobre tecnología Starlink para las dos sedes remotas de la empresa CR Technology.

**Direccionamiento IP de la sede principal**

La sede principal cuenta con un firewall FortiGate 100F y administra la red local correspondiente al segmento:

- Red LAN: 192.168.0.0/23
- Función: Concentración de salida a Internet de las sedes remotas, administración centralizada del tráfico y aplicación de políticas de seguridad perimetral.
- Segmentación interna (servidores locales, sistema central CCTV, usuarios de la empresa.

**Direccionamiento IP de las sedes remotas**

Cada sede remota implementa una red local independiente, administrada por un router FortiGate 40F, con el siguiente esquema:

**Tabla 5**

*Segmentación LAN de las sedes remotas*

| Sede | Segmento LAN | Máscara |
|---|---|---|
| Sede Remota 1 | 192.168.71.0 | 255.255.255.0 |
| Sede Remota 2 | 192.168.200.0 | 255.255.255.0 |

*Nota.* Elaboración propia (s.f.)

**Direccionamiento WAN en las sedes remotas**

Las interfaces WAN de los routers FortiGate 40F en las sedes remotas se conectaron al servicio Starlink, que asignó direcciones IP dinámicas bajo un esquema de CGNAT. Estas direcciones fueron utilizadas para el establecimiento de los túneles VPN IPsec hacia la sede principal.

**Consideraciones generales**

- Las direcciones IP públicas operan bajo un esquema CGNAT provisto por Starlink; por ello, no disponen de direcciones IPv4 públicas propias y dichas direcciones no forman parte del esquema de direccionamiento interno.
- El plan de direccionamiento permitió identificación de las redes locales y segmentación del tráfico entre sedes.

- La comunicación entre sedes remotas y sede principal se realizó a través de los túneles VPN IPsec, conforme a la arquitectura descrita en el Anexo A.

## Anexo C – Configuración de la VPN IPsec

El presente anexo se documentó los parámetros de configuración de los túneles VPN IPsec implementados que garantizó el acceso a Internet desde las sedes remotas de la empresa CR Technology a través del servicio Starlink.

### VPN IPsec – Sedes remotas hacia la sede principal

**Tabla 6**

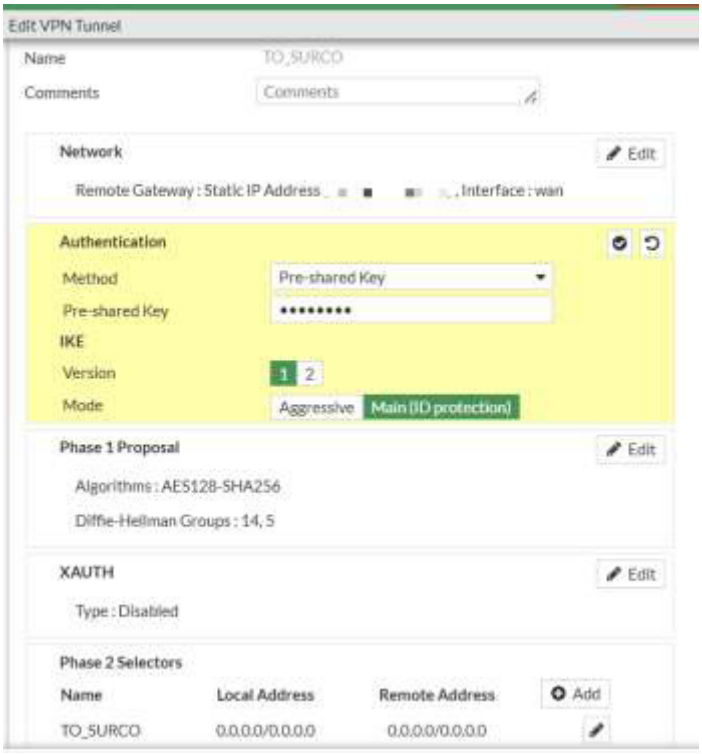
*Parámetros de la VPN IPsec, sede remota*

| Parámetro | Valor |
|---|---|
| Tipo de VPN | Site-to-Site |
| FortiGate sede remota | 40F |
| Modo IKE | IKEv1 |
| Remote Gateway | IP pública fija de la sede principal |
| Authentication | Pre-shared Key (PSK) |
| Encryption | AES128 |
| Hash | SHA256 |
| DH Group | 14, 5 |
| Local Subnet | 0.0.0.0/0 |
| Remote Subnet | 0.0.0.0/0 |
| NAT Traversal | Habilitado |

*Nota.* Elaboración propia (s.f.)

**Figura 27**

*Captura de la VPN Site to Site en Fortigate 40F*




*Nota.* Elaboración propia (s.f.)

**VPN IPsec – Sede principal hacia la sede remota**

**Tabla 7**

*Parámetros de la VPN IPsec, sede principal*

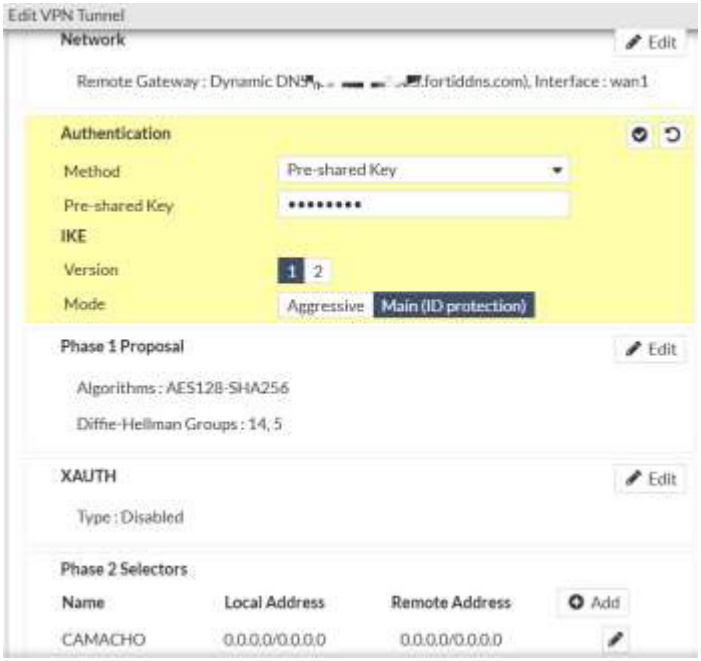
| **Parámetro** | **Valor** |
|---|---|
| Tipo de VPN | Site-to-Site |
| FortiGate sede Principal | 100F |
| Modo IKE | IKEv1 |
| Remote Gateway | DDNS: prueba.fortiddns.com |
| Authentication | Pre-shared Key (PSK) |
| Encryption | AES128 |
| Hash | SHA256 |

| | |
|---|---|
| DH Group | 14, 5 |
| Local Subnet | 0.0.0.0/0 |
| Remote Subnet | 0.0.0.0/0 |
| NAT Traversal | Habilitado |

*Nota.* Elaboración propia (s.f.)

**Figura 28**

*Captura de la VPN Site to Site en Fortigate 100F*




*Nota.* Elaboración propia (s.f.)

**Configuración del servicio DDNS en Fortigate 40F (sede remota)**

***Tabla 8***

*Parámetros de configuración DDNS del FortiGate de la sede remota*

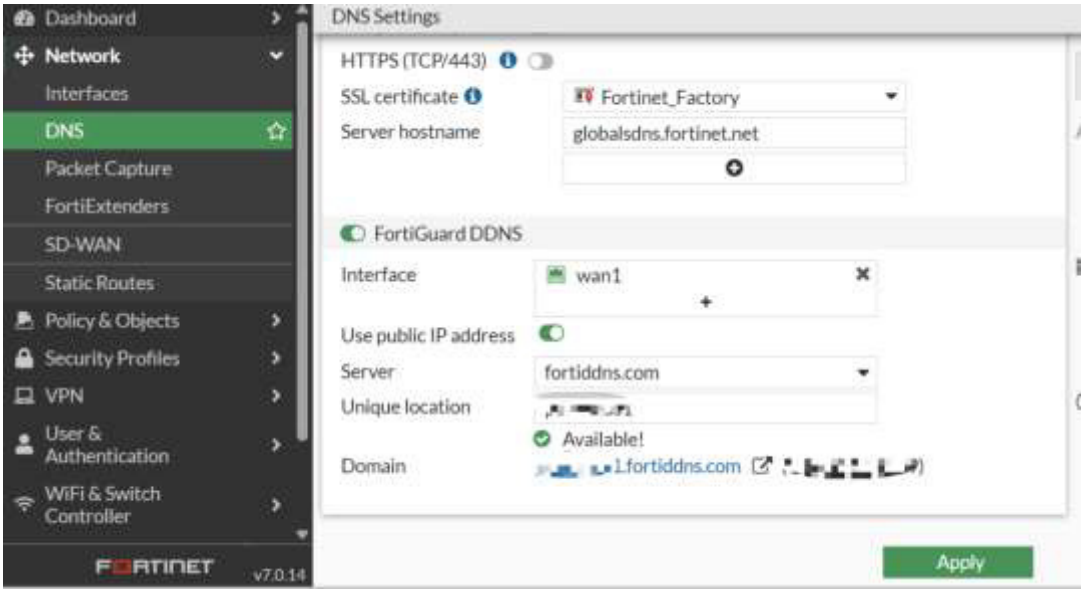
| **Parámetro** | **Valor** |
|---|---|
| Interfaz asociada | WAN (Starlink) |
| Servidor DDNS | fortiddns.com |

| | |
|---|---|
| Nombre Dominio | prueba.fortiddns.com |
| Use public IP address | Habilitado |

*Nota.* Elaboración propia (s.f.)

***Figura 29***

*Captura de la configuración DDNS*



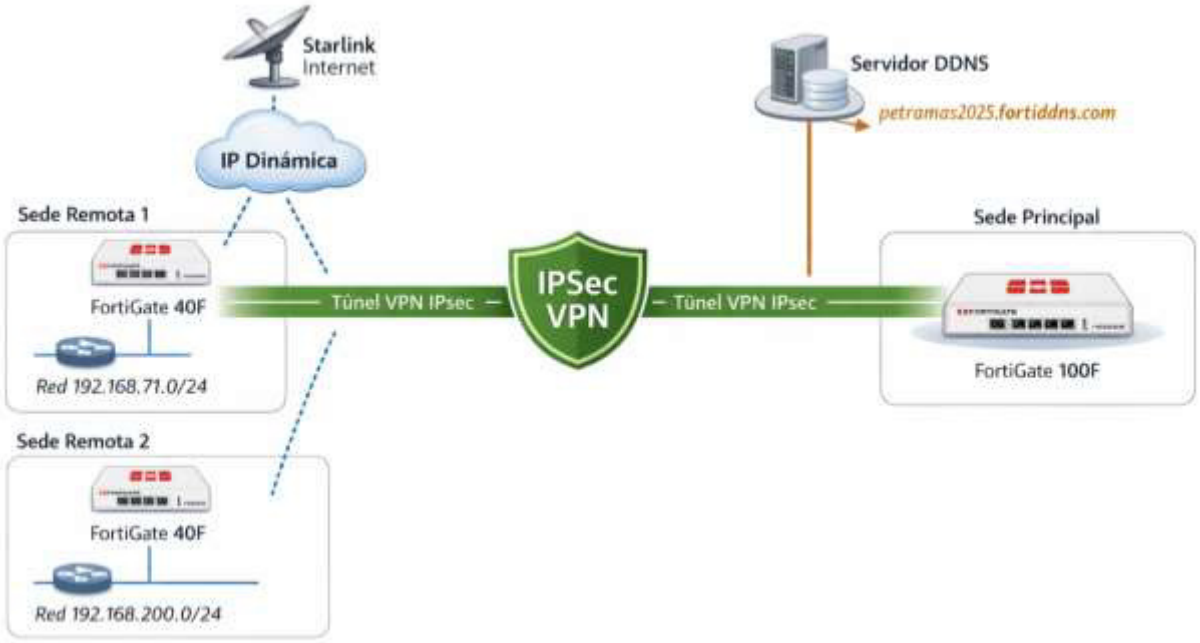

*Nota.* Elaboración propia (s.f.)

**Consideraciones generales**

- Todos los túneles VPN implementados utilizaron IPsec Site-to-Site y cifrado para garantizar confidencialidad del tráfico.
- La configuración DDNS es crítica para el funcionamiento de la VPN debido a que los servicios Starlink no brinda una IP publica dedicada a los FortiGate 40F.
- El esquema permitió la administración centralizada del tráfico y garantiza acceso a Internet desde las sedes remotas hacia la sede principal.

**Figura 30**

*Diagrama lógico del flujo de la VPN IPsec con DDNS*




*Nota.* Elaboración propia (s.f.)

La figura 30 muestra la implementación de los túneles VPN Site-to-Site entre la sede principal y las sedes remotas con la resolución automática de IP mediante DDNS. Con esto se garantizó que el tráfico entre sedes se mantenga disponible, complementando la información presentada en las tablas y capturas de pantalla de este anexo.