UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES

CARRERA DE COMPUTACIÓN

Tema: **"Redes privadas virtuales para campus universitario"**

Trabajo de Integración Curricular previo a la obtención del título de Ingeniero en Ciencias de la Computación

AUTOR: Pullugando Gualuntuña Steve Rodrigo
TUTOR: Ing. Del Hierro Mosquera Miltón Gabriel MSc.

Tulcán, 2026.

CERTIFICADO DEL TUTOR

Certifico que el estudiante Pullugando Gualuntuña Steve Rodrigo con el número de cédula 1753732740 respectivamente ha desarrollado el Trabajo de Integración Curricular: "Redes privadas virtuales para campus universitario"

Este trabajo se sujeta a las normas y metodología dispuesta en el Reglamento de la Unidad de Integración Curricular, Titulación e Incorporación de la UPEC, por lo tanto, autorizo la presentación de la sustentación para la calificación respectiva

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
MILTON GABRIEL DEL HIERRO MOSQUERA

_____

Ing. Del Hierro Mosquera Milton Gabriel MSc.

TUTOR

Tulcán, julio de 2026

AUTORÍA DE TRABAJO

El presente Trabajo de Integración Curricular constituye un requisito previo para la obtención del título de Ingeniero en la Carrera de computación de la Facultad de Industrias Agropecuarias y Ciencias Ambientales.

Yo, Pullugando Gualuntuña Steve Rodrigo con cédula de identidad número 1753732740 respectivamente declaro que la investigación es absolutamente original, auténtica, personal y los resultados y conclusiones a los que he llegado son de mi absoluta responsabilidad.

_____

Pullugando Gualuntuña Steve Rodrigo

AUTOR

Tulcán, julio de 2026

ACTA DE CESIÓN DE DERECHOS DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Yo Pullugando Gualuntuña Steve Rodrigo declaro ser autor de los criterios emitidos en el Trabajo de Integración Curricular: "Redes privadas virtuales para campus universitario" y eximo expresamente a la Universidad Politécnica Estatal del Carchi y a sus representantes de posibles reclamos o acciones legales.

_____

Pullugando Gualuntuña Steve Rodrigo

AUTOR

Tulcán, julio de 2026

AGRADECIMIENTO

El autor expresa su sincero agradecimiento a la Universidad Politécnica Estatal del Carchi, y en particular a la Carrera de Computación, por la formación académica y profesional recibida.

Al Ing. Milton Del Hierro, tutor del presente trabajo, por su acertada dirección, rigor académico y constante apoyo metodológico durante el desarrollo de la investigación.

Al Sr. Javier Torres, encargado de redes de TIC de la institución, por facilitar el acceso a la información técnica necesaria para el diagnóstico y diseño de la red.

Finalmente, a los compañeros y amigos de aula, por su compañía y apoyo a lo largo de la etapa universitaria.

DEDICATORIA

A Dios, por ser mi guía y fortaleza en cada etapa de este camino, por iluminar mis pasos en los momentos de duda y por darme la perseverancia necesaria para alcanzar esta meta.

A mis padres, por su amor incondicional y por cada sacrificio realizado en silencio para que yo pudiera llegar hasta aquí. Su apoyo constante, su confianza en mí y sus palabras de aliento fueron el motor que me impulsó a seguir adelante en los momentos más difíciles.

A mis abuelitos, por su sabiduría y sus consejos llenos de experiencia y amor. Por cada bendición que me han brindado a lo largo de la vida y por enseñarme.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

RESUMEN

La presente investigación tiene como objetivo determinar una solución de interconexión basada en redes privadas virtuales para los distintos campus de la Universidad Politécnica Estatal del Carchi, con la finalidad de fortalecer la conectividad institucional y garantizar la seguridad de la información transmitida entre sedes geográficamente distribuidas. La metodología aplicada corresponde a un enfoque cuantitativo, de tipo descriptivo y aplicado, desarrollada mediante la metodología PPDIOO, que permitió realizar el diagnóstico de la infraestructura de red existente, identificar los requerimientos de comunicación institucional y analizar diferentes alternativas tecnológicas relacionadas con protocolos de tunelización, topologías de red y mecanismos de seguridad para la interconexión de sedes. A partir del análisis realizado, se diseñó una arquitectura VPN Site-to-Site con topología Hub-and-Spoke basada en el protocolo IPsec e implementada sobre la plataforma pfSense, considerando criterios de escalabilidad, administración centralizada y protección de la información. Posteriormente, la propuesta fue validada mediante un entorno de emulación utilizando GNS3, donde se efectuaron pruebas orientadas a evaluar parámetros de conectividad, rendimiento y seguridad a través de métricas como latencia, jitter, pérdida de paquetes y throughput. Demostraron los resultados obtenidos que la arquitectura diseñada permite establecer túneles seguros entre campus, garantizando la confidencialidad e integridad de la información mediante mecanismos de cifrado y autenticación, además de mantener niveles de rendimiento adecuados para el funcionamiento de los servicios institucionales.
Como conclusión, se determina que la solución propuesta fortalece la interconectividad entre sedes y aporta un modelo de referencia para el diseño, evaluación y validación de arquitecturas VPN orientadas a entornos universitarios con infraestructura de red distribuida; en su conjunto, este resumen sintetiza el recorrido metodológico y los hallazgos centrales del estudio desarrollado.

Palabras clave: redes privadas virtuales, IPsec, pfSense, GNS3, seguridad de la información.

ABSTRACT

This research aims to determine a Virtual Private Network (VPN) based interconnection solution for the different campuses of the Universidad Politécnica Estatal del Carchi in order to strengthen institutional connectivity and ensure the security of information transmitted between geographically distributed sites. The study adopted a quantitative, descriptive, and applied research approach, supported by the PPDIOO methodology, which enabled the assessment of the existing network infrastructure, the identification of institutional communication requirements, and the analysis of different technological alternatives related to tunneling protocols, network topologies, and security mechanisms for campus interconnection. Based on the technical analysis conducted, a Site-to-Site VPN architecture with a Hub-and-Spoke topology was designed using the IPsec protocol and implemented on the pfSense platform, considering scalability, centralized management, and information protection requirements. The proposed solution was subsequently validated in an emulation environment using GNS3, where connectivity, performance, and security tests were carried out through metrics such as latency, jitter, packet loss, and throughput. The results demonstrated that the proposed architecture is capable of establishing secure tunnels between campuses, ensuring data confidentiality and integrity through encryption and authentication mechanisms while maintaining performance levels suitable for institutional services. It is concluded that the proposed solution enhances inter-campus connectivity and provides a reference framework for the design, evaluation, and validation of VPN architectures intended for distributed university network environments.

Keywords: Virtual Private Networks (VPNs), IPsec, pfSense, GNS3, information security.

INTRODUCCIÓN

En la actualidad, el entorno global atraviesa lo que múltiples especialistas denominan la "Cuarta Revolución Industrial", un período caracterizado por la convergencia entre lo físico y lo digital, que transforma radicalmente los modos de operación en todas las organizaciones. Frente a este contexto, el sistema de educación superior ecuatoriano se ha visto en la necesidad de adaptarse progresivamente a los nuevos paradigmas. Las universidades y escuelas politécnicas del país transitan hoy de manera ineludible hacia el modelo denominado "Educación 4.0", en el cual la tecnología deja de cumplir una función meramente instrumental para convertirse en el eje central de los procesos de enseñanza, aprendizaje e investigación. La transformación digital dejó de representar una opción innovadora para las instituciones académicas. Hoy constituye una condición indispensable para su vigencia y competitividad, según confirman investigaciones recientes sobre el aprendizaje en la educación superior: la integración de recursos tecnológicos resulta fundamental para garantizar una formación de calidad, alineada con las exigencias de un mercado laboral en constante proceso de tecnificación (Delgado et al., 2024).

La emergencia sanitaria mundial impulsó este proceso de cambio de forma abrupta. Las deficiencias estructurales de las antiguas plataformas informáticas institucionales quedaron expuestas sin margen de duda, forzando una migración acelerada hacia las modalidades virtual e híbrida que permitió sostener el desarrollo de las actividades académicas, aunque a costa de revelar desigualdades profundas en el acceso y limitaciones serias de conectividad. Para el caso ecuatoriano, diversas revisiones académicas recientes coinciden en que el desafío pospandemia central radica en reducir la brecha tecnológica y garantizar condiciones adecuadas de conectividad para toda la comunidad universitaria (Ocampo et al., 2024). Las instituciones de educación superior de carácter público concentran una proporción considerable de la matrícula nacional; de ahí que enfrenten, con presupuestos limitados, la urgencia

de modernizar sus infraestructuras de red, procurando equilibrar cobertura, innovación y sostenibilidad financiera.

Nuevos predios, extensiones, unidades administrativas y centros de investigación distribuidos en distintas zonas geográficas suelen incorporarse a medida que las instituciones de educación superior expanden su capacidad para atender la demanda académica creciente. Constituye, sin duda, un avance desde la perspectiva académica e institucional. No obstante, esa misma expansión genera una problemática técnica y logística de magnitud considerable: la fragmentación de la información. Cuando una institución matriz opera de manera simultánea con múltiples sedes, el desafío trasciende la simple provisión de acceso a internet en cada punto: integrar todos los nodos dentro de un sistema institucional unificado se convierte en la verdadera exigencia. Sin redes adecuadas, cada recinto queda convertido en una unidad aislada respecto a los sistemas centrales, con la consecuente duplicación innecesaria de registros, demoras en los procesos administrativos y dificultades adicionales tanto para docentes como para estudiantes.

A esta fragmentación territorial se suma un factor crítico que con frecuencia recibe atención insuficiente: la seguridad de la información institucional. Circulando a diario datos académicos, financieros y de carácter confidencial, los sistemas universitarios se han convertido en objetivos prioritarios para agentes malintencionados. Diversos reportes especializados en ciberseguridad aplicada al contexto ecuatoriano advierten que las instituciones educativas presentan actualmente una mayor vulnerabilidad frente a amenazas como el phishing y los ataques de tipo ransomware; dicha situación se atribuye principalmente a la ausencia de políticas de seguridad robustas y al uso persistente de redes abiertas para la transmisión de información sensible (Ibarra et al., 2025). Con la entrada en vigor de la Ley Orgánica de Protección de Datos Personales, además, las entidades académicas asumen una responsabilidad jurídica explícita de garantizar la privacidad e integridad de los datos que administran (Menéndez & Sánchez, 2025). La transmisión de información institucional a través de redes públicas sin mecanismos de seguridad apropiados no constituye, entonces, una simple deficiencia operativa: representa un riesgo jurídico e institucional de magnitud inaceptable para cualquier centro de educación superior del país.

Interconectar sedes geográficamente dispersas de forma confiable sin incurrir en los costos que implica el tendido de infraestructura física dedicada exige recurrir a soluciones lógicas de conectividad. Las Redes Privadas Virtuales adquieren, en este contexto, un papel de particular relevancia. Una VPN permite construir un canal cifrado y seguro sobre la infraestructura de internet público, emulando el comportamiento de una conexión física privada: un usuario ubicado en una sede remota puede así acceder directamente a los recursos de la sede central como si se encontrara físicamente en ella, con la garantía de que los datos transmitidos permanecen protegidos e inaccesibles para terceros no autorizados. Análisis técnicos realizados en el ámbito universitario ecuatoriano, como el desarrollado por la Universidad Técnica de Cotopaxi, han demostrado que la implementación de VPNs bajo estándares reconocidos como IPsec no solo resulta económicamente asequible para instituciones públicas, sino que fortalece considerablemente los niveles de seguridad y facilita la administración integral de los servicios de red (Andaluz & Guanolisa, 2022).

Es precisamente en este escenario donde se enmarca el caso de la Universidad Politécnica Estatal del Carchi. Al tratarse de una institución en proceso de crecimiento, la UPEC enfrenta el reto de unificar sus instalaciones y garantizar que la comunidad académica pueda acceder de manera equitativa y segura a las plataformas tecnológicas institucionales, independientemente de la sede desde la cual lo haga. Compromete actualmente el rendimiento de los sistemas digitales, además, la ausencia de una infraestructura de red unificada, que expone a la institución a las amenazas cibernéticas previamente descritas; de ahí la urgencia de una solución que conjugue eficiencia económica, alto nivel de protección y capacidad de proyección para acompañar la transformación institucional en curso.

El presente trabajo de investigación tiene como objetivo central, en respuesta a esta situación, diseñar y proponer una solución de conectividad basada en redes privadas virtuales, ajustada a los requerimientos específicos de la UPEC. No se limita el estudio a la configuración de dispositivos de red; aborda además un análisis detallado de los requerimientos de tráfico y seguridad al interior de la institución, con el propósito de determinar el modelo VPN más adecuado.

I. EL PROBLEMA

1.1. PLANTEAMIENTO DEL PROBLEMA

La transformación digital en la educación superior constituye, sin lugar a duda, uno de los fenómenos más relevantes de las últimas décadas a escala mundial, un proceso que ha reconfigurado por completo la manera en que las instituciones gestionan su información y sostienen sus procesos académicos. El tráfico de datos en redes universitarias ha crecido de forma sostenida. Plataformas de gestión académica, entornos virtuales de aprendizaje y servicios de videoconferencia se han masificado a un ritmo que las infraestructuras de red existentes no siempre logran acompañar, generando una presión creciente sobre su capacidad operativa. Documentan Rosario et al. (2021) que las instituciones de educación superior enfrentan una pronunciada brecha digital en la que las arquitecturas de conectividad tradicionales resultan insuficientes para sostener los requerimientos actuales de disponibilidad, velocidad y seguridad una insuficiencia que compromete tanto la continuidad de los procesos académicos como la equidad en el acceso a los recursos tecnológicos institucionales, y que termina convirtiendo la red, de un soporte transparente que debería pasar inadvertido, en un factor crítico y visible del desempeño universitario.

A esta presión se suma otra dimensión del problema, esta vez de naturaleza física: la expansión de las instituciones universitarias hacia múltiples sedes y extensiones. Cuando una institución opera con campus distribuidos geográficamente sin contar con una infraestructura de interconexión centralizada, cada sede tiende a comportarse como un nodo aislado respecto a los sistemas de información de la matriz, replicando procesos y generando inconsistencias que rara vez resultan evidentes hasta que afectan la operación diaria. De Jesús, Flores y Jalife (2022) advierten al respecto que más de 108 centros universitarios regionales en América Latina presentan deficiencias críticas de interconectividad. La dependencia exclusiva de la internet pública para la gestión de servicios institucionales evidencia, en consecuencia, fragmentación de datos, inconsistencia en los registros y exposición a amenazas de seguridad; sin una capa de red privada sobre la infraestructura

pública, la confidencialidad, la integridad y la disponibilidad en la transmisión de información sensible entre sedes simplemente no pueden garantizarse.

El caso ecuatoriano agrava este panorama con particularidades propias del contexto nacional. Tras la emergencia sanitaria, persisten en las universidades públicas del país dificultades para garantizar condiciones adecuadas de conectividad a su comunidad académica, un rezago que, lejos de resolverse, parece haberse instalado como condición estructural. Ocampo et al. (2024) señalan que las deficiencias de conectividad inciden directamente en la equidad académica y afectan de manera desproporcionada a los estudiantes de instituciones con múltiples sedes dispersas. Hay además una dimensión crítica de seguridad que se suma a la de acceso: la vigente Ley Orgánica de Protección de Datos Personales (LOPDP, 2021) impone a las entidades académicas la obligación legal de garantizar la privacidad e integridad de los datos que administran. Ibarra et al. (2025), sin embargo, documentan que diversas instituciones académicas ecuatorianas continúan transmitiendo información sensible registros académicos, datos financieros, credenciales institucionales a través de conexiones no cifradas, exponiéndose a ataques de tipo phishing y ransomware con consecuencias que pueden derivar en responsabilidades legales de consideración.

La Universidad Politécnica Estatal del Carchi reúne las condiciones descritas en los párrafos anteriores. Su proceso de crecimiento ha resultado en la incorporación de nuevas sedes y extensiones en la región norte del país, pero la infraestructura de red no ha evolucionado al mismo ritmo. Carece hoy la UPEC de un sistema de interconexión segura entre sus diferentes campus situación que ha confirmado institucionalmente el responsable del Departamento de Redes de la universidad, al señalar que el crecimiento institucional hace imperativa la implementación de una solución de conectividad que integre todas las sedes bajo una arquitectura unificada. Cada campus opera, como resultado de esta deficiencia, de forma independiente respecto a los servidores centrales, sin mecanismos que garanticen la confidencialidad ni la integridad de la información que se transmite entre ellos.

Concretas y cuantificables, las consecuencias operativas de esta situación se manifiestan en distintos planos de la gestión institucional. A nivel administrativo, el personal debe trasladarse físicamente entre sedes para acceder a registros centralizados, lo que incrementa los tiempos de respuesta y reduce la eficiencia operativa. Estudiantes y docentes ubicados fuera del campus principal enfrentan, en

el plano académico, restricciones de acceso a repositorios, sistemas de gestión académica y herramientas institucionales, generando condiciones de desigualdad frente a quienes sí cuentan con acceso directo. La transmisión de información institucional a través de conexiones públicas no cifradas, desde la perspectiva de la seguridad, expone a la institución a vulnerabilidades que pueden comprometer la confidencialidad de datos protegidos por la LOPDP, con las implicaciones jurídicas que ello conlleva. Este escenario, sostenido en el tiempo, constituye un obstáculo directo para el desarrollo de una gestión universitaria eficiente, equitativa y legalmente conforme.

Frente a la ausencia de una solución de interconexión segura que integre los campus de la UPEC, surge la necesidad de diseñar una arquitectura basada en redes privadas virtuales capaz de garantizar seguridad, disponibilidad y eficiencia en la comunicación entre sedes universitarias. La tecnología VPN, al permitir establecer canales cifrados sobre la infraestructura de internet existente sin requerir el tendido de infraestructura física dedicada, se presenta como una alternativa técnicamente viable y económicamente sostenible para instituciones públicas. Andaluz y Guanoluisa (2022), en un estudio desarrollado en la Universidad Técnica de Cotopaxi, han demostrado que la implementación de VPNs bajo estándares como IPsec mejora de forma significativa los niveles de seguridad y simplifica la administración centralizada de los servicios de red. No existe, sin embargo, un estudio que evalúe de manera sistemática la viabilidad, el rendimiento y la arquitectura óptima de esta solución para las condiciones específicas de la UPEC y es precisamente ese vacío el que la presente investigación busca atender.

1.2. FORMULACIÓN DEL PROBLEMA

De la expansión institucional de la Universidad Politécnica Estatal del Carchi ha derivado por la incorporación progresiva de sedes y extensiones que hoy operan desarticuladas de los sistemas centrales una condición operativa cuyas consecuencias, se manifiestan en múltiples capas. No se trata únicamente de deficiencias en la gestión administrativa y académica. Al transmitirse datos sensibles por canales no cifrados, la información institucional queda expuesta a riesgos de seguridad que la Ley Orgánica de Protección de Datos Personales tipifica con claridad, y que acarrean implicaciones jurídicas cuya gravedad escala con cada nuevo incidente. Carece hoy la UPEC de una infraestructura de interconexión segura que permita administrar centralizadamente los recursos tecnológicos; cada campus

persiste en un aislamiento funcional respecto a la matriz universitaria que, lejos de ser una limitación meramente logística, constituye una vulnerabilidad estructural difícil de sostener en el entorno normativo vigente.

1.3. JUSTIFICACIÓN

El avance sostenido de la transformación digital en la educación superior ha generado una dependencia creciente de plataformas de gestión académica, servicios administrativos en línea y sistemas de información institucional que requieren condiciones de conectividad segura, estable y continua; en este escenario, las instituciones universitarias que operan con campus distribuidos geográficamente enfrentarán dificultades operativas de consideración si no disponen de una infraestructura de red que garantice la interconexión de sus sedes bajo criterios de confidencialidad, integridad y disponibilidad, pues su expansión institucional ha generado una fragmentación tecnológica que compromete tanto la eficiencia de sus procesos internos como la protección de la información que administra.

Desde una perspectiva técnica, la adopción de una arquitectura VPN permitirá establecer canales de comunicación cifrados sobre la infraestructura de internet existente, eliminando la necesidad de transmitir datos sensibles a través de conexiones públicas no protegidas, con lo cual se reduce la exposición de la institución frente a amenazas como el acceso no autorizado y la interceptación de datos, en concordancia con las obligaciones que establece la Ley Orgánica de Protección de Datos Personales. La implementación de protocolos de cifrado reconocidos en el diseño de la arquitectura propuesta fortalecerá los mecanismos de seguridad institucional sin requerir inversión en infraestructura física dedicada, lo que representa una alternativa técnicamente sólida y económicamente viable para una institución pública.

En el plano institucional, la solución propuesta favorecerá la integración operativa de los campus universitarios bajo un sistema de red unificado. Esto permitirá que los procesos académicos y administrativos que actualmente dependen de la presencia física en la sede central puedan ejecutarse de manera remota con los mismos niveles de acceso y seguridad, proyectándose una reducción en los tiempos de respuesta de los trámites institucionales, una mayor continuidad en la prestación de servicios digitales y una administración más eficiente de los recursos tecnológicos disponibles.

Beneficios todos que contribuirán al fortalecimiento de la capacidad operativa de la UPEC en un contexto de crecimiento institucional sostenido.

Beneficiarios directos de esta investigación serán los estudiantes, docentes y personal administrativo de todos los campus de la universidad, quienes accederán en condiciones de mayor equidad y seguridad a los recursos y plataformas institucionales, independientemente de la sede desde la que operen. El Departamento de Tecnologías de la Información y Comunicación de la UPEC también se verá beneficiado, al contar con una arquitectura de referencia que facilitará la administración centralizada y el monitoreo de la red institucional. De manera indirecta, la investigación aportará elementos de utilidad para otras instituciones de educación superior que enfrenten problemáticas similares de interconexión entre sedes.

Desde el punto de vista metodológico, el estudio proporcionará un modelo estructurado de análisis de requerimientos, diseño y validación de arquitecturas VPN aplicable a entornos universitarios con infraestructura distribuida. La validación mediante herramientas de emulación de redes permitirá verificar el comportamiento técnico de la solución antes de cualquier implementación, generando evidencia técnica documentada que podrá servir como referencia para investigaciones posteriores en el campo de las redes institucionales y la ciberseguridad aplicada a la educación superior.

Justifica, en síntesis, la presente investigación la necesidad concreta de fortalecer la conectividad y la seguridad de la infraestructura de red de la Universidad Politécnica Estatal del Carchi, aportando una solución técnicamente fundamentada, económicamente sostenible y metodológicamente replicable que responda a los requerimientos actuales de la institución y contribuya a su desarrollo tecnológico en el mediano plazo.

1.4. OBJETIVOS Y PREGUNTAS DE INVESTIGACIÓN

1.4.1. Objetivo General

Determinar una solución de interconexión basada en redes privadas virtuales para los distintos campus de la Universidad Politécnica Estatal del Carchi.

1.4.2. Objetivos Específicos

- Diagnosticar la situación actual de la conectividad y los requerimientos de comunicación entre los campus de la UPEC.

- Comparar diferentes tipos y tecnologías de VPN para identificar la alternativa más adecuada a las necesidades de la universidad.
- Proponer un diseño de arquitectura de red mediante VPN adecuada para la interconexión entre campus universitarios mediante un entorno de emulación.
- Evaluar el rendimiento y la seguridad de la arquitectura propuesta mediante pruebas de conectividad y transmisión de datos.

1.4.3. Preguntas de Investigación

- ¿Cuáles son las necesidades de conectividad y seguridad presentes en la infraestructura de red de la UPEC?
- ¿Qué tecnologías VPN resultan más adecuadas para la interconexión segura de campus universitarios?
- ¿Cómo diseñar una arquitectura VPN orientada a la interconexión segura entre campus universitarios?
- ¿Cuál es el rendimiento de la arquitectura VPN propuesta respecto a conectividad, latencia y seguridad de transmisión?

II. FUNDAMENTACIÓN TEÓRICA

2.1. ANTECEDENTES DE LA INVESTIGACIÓN

En su investigación Quishpe Iza (2021), el análisis de los requisitos de la red y la estimación del volumen de usuarios activos llevó a diseñar una solución que, tras comparar distintas tecnologías sobre servidores Linux evaluando aspectos como la madurez del código, la facilidad de gestión y el rendimiento en entornos de recursos limitados, decantó la selección finalmente por OpenVPN, privilegiando su robustez en materia de cifrado y autenticación. Las pruebas de conectividad posteriores mostraron un funcionamiento estable y un costo de operación mínimo, circunstancia que otorga a este antecedente un valor significativo: ofrece una comparativa real, ejecutada en condiciones de laboratorio, entre herramientas de licencia libre, lo cual resulta de particular interés cuando se dispone de un presupuesto restringido.

Haro (2021) abordó el problema de conectar una oficina matriz con sus agencias remotas mediante túneles VPN basados en tecnología IPSec, articulados con una arquitectura SD-WAN que permitiera gestionar de forma inteligente los enlaces disponibles. Sus resultados evidenciaron que los denominados "túneles dinámicos" seleccionan automáticamente la ruta más expedita en cada momento, garantizando así la continuidad del servicio incluso ante fluctuaciones en la calidad de las conexiones de internet. De este trabajo se desprenden criterios técnicos de especial utilidad para configurar una red que mantenga la estabilidad entre sedes dispersas una condición crítica cuando se piensa en los campus universitarios y su necesidad de operar como una unidad funcional.

Desarrolló Chávez Paredes (2022) un modelo de infraestructura VPN expresamente concebido para organizaciones con despliegue multicampus, aplicando una topología LAN-to-LAN soportada sobre el protocolo IPSec. La evaluación de su propuesta, llevada a cabo mediante simulación en entornos virtuales que replicaban las condiciones de tráfico y latencia propias de redes institucionales, demostró que la transmisión de datos preservaba en todo momento los atributos de confidencialidad y consistencia, sin degradaciones apreciables en el rendimiento.

Centrado ya en el dominio educativo, el trabajo de Ataypoma Llanto (2023) se orientó a mejorar la comunicación entre las oficinas externas y el campus principal de la Universidad José Faustino Sánchez Carrión, para lo cual implementó una VPN con OpenVPN que dio acceso seguro a los sistemas administrativos y a los flujos de trámite documentario. Los resultados obtenidos apuntaron a una mejora sensible tanto en el nivel de seguridad perimetral como en la facilidad de acceso a la información, dos dimensiones que suelen entrar en tensión y que en esta experiencia lograron equilibrarse de manera satisfactoria.

Baque & Gómez (2023), por su parte, enfocaron la interconexión de sedes como un problema eminentemente de seguridad, y propusieron una VPN Site-to-Site con protocolo IPSec que permitiera extender la red local sin exponer puertos públicos a internet, logrando así que el acceso al servidor central se realizara a través de un túnel cifrado sin necesidad de abrir servicios sensibles al exterior. Este proyecto refuerza la convicción ampliamente compartida en el ámbito de la ciberseguridad de que las VPN constituyen, en escenarios de comunicación entre sitios, la alternativa más fiable para la protección de datos institucionales; un principio que, por su solidez técnica, actuará como eje vertebrador de la propuesta.

2.2. MARCO TEÓRICO

2.2.1. Modelos de referencia: OSI y TCP/IP

Para que dos dispositivos puedan intercambiar información sin importar quién los fabricó ni qué sistema operativo corren, las redes modernas recurren a arquitecturas organizadas por capas. La idea, tal como la describen Oviedo & Samaniego, (2018), es bastante práctica: si se divide el problema de la comunicación en partes más pequeñas y cada parte se resuelve por separado, un cambio en el hardware o en el software de un nivel no tiene por qué arrastrar consigo al resto del sistema.

2.2.1.1. El Modelo de Referencia OSI

La Organización Internacional de Normalización propuso el Modelo de Interconexión de Sistemas Abiertos como un esquema conceptual de siete capas. No es un protocolo en sí mismo, sino más bien un mapa que permite entender qué le pasa a la información mientras viaja desde la pantalla del usuario hasta convertirse en una señal física. Según Marcillo, (2024) lo describe de la siguiente manera:

Figura 1. Modelo de referencia OSI.

- **Capa 7:** Aquí es donde los programas se conectan a la red. Protocolos como HTTP, DNS o DHCP viven en este nivel.
- **Capa 6:** Su trabajo es que ambos lados hablen el mismo idioma: se ocupa del formato de los datos, la compresión.
- **Capa 5:** Mantiene la conversación entre dos terminales. Abre el canal, lo sostiene el tiempo necesario y lo cierra de forma ordenada cuando ya no se necesita.
- **Capa 4:** Divide los datos en fragmentos manejables y se asegura de que lleguen bien al otro extremo.
- **Capa 3:** Decide por dónde viaja cada paquete. El protocolo IP asigna las direcciones lógicas y los algoritmos de enrutamiento buscan el camino más conveniente en cada momento.
- **Capa 2:** Toma los paquetes y los empaqueta en tramas. También controla quién puede usar el medio en un momento dado y usa las direcciones MAC para identificar los equipos dentro de una misma red local.
- **Capa 1:** Es el nivel más concreto de todos: cables, voltajes, frecuencias de radio. Convierte los unos y ceros en algo que puede viajar físicamente de un punto a otro.

2.2.1.2. Modelo TCP/IP

El modelo OSI es útil para estudiar y analizar, pero Internet no funciona sobre él sino sobre TCP/IP. Barreto, (2025) señala que esta suite agrupa todo en cuatro capas, lo que la hace más sencilla de implementar y explica en buena medida por qué terminó

imponiéndose tanto en entornos de software libre como en redes corporativas de todo tamaño:

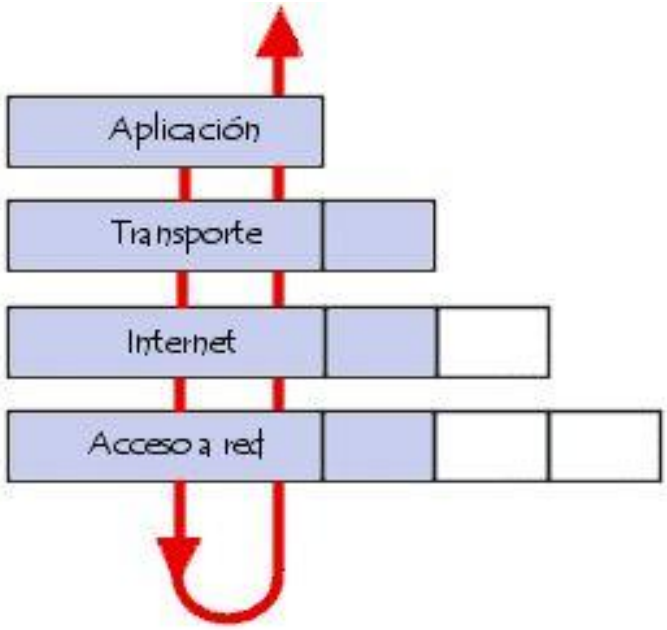

Figura 2. Modelo de referencia TCP/IP.

- **Capa de Aplicación:** Absorbe lo que en OSI serían tres capas distintas aplicación, presentación y sesión y las trata como una sola. Es donde operan los programas que el usuario final utiliza.
- **Capa de Transporte:** Cumple una función similar a su equivalente en OSI: gestiona la comunicación directa entre hosts.
- **Capa de Internet:** Se encarga de que los paquetes lleguen a su destino, aunque tengan que atravesar varias redes distintas. El protocolo IP y el direccionamiento lógico son su territorio.
- **Capa de Acceso a la Red:** Junta en un solo bloque lo que OSI separa en física y enlace de datos. En la práctica, es la capa que trata directamente con el cable, la fibra o la antena.

Tener conocimientos de cómo se organizan estas capas tiene un alto en la seguridad de las redes. Las guías de la Universidad Estatal de Milagro (UNEMI, 2022) indican que las soluciones de protección más sólidas actúan precisamente en la capa de Internet, porque desde ahí pueden interceptar y cifrar todo el tráfico que viene de los niveles superiores antes de que salga hacia redes públicas.

2.2.2. Direccionamiento IP y segmentación de redes

Que los datos encuentren su destino dentro de una red no ocurre por casualidad. Cada dispositivo conectado necesita un identificador numérico que lo diferencie de cualquier otro, y administrar esos identificadores de forma planificada es lo que sostiene, en las redes empresariales actuales, tanto la estabilidad del tráfico como la protección de la información institucional.

2.2.2.1. Estructura de la Identificación Lógica (IPv4)

Oviedo & Samaniego, (2018) describen el protocolo IPv4 como un esquema de 32 bits distribuidos en cuatro grupos numéricos. Sin embargo, una dirección por sí sola no dice mucho si no se sabe qué parte de ella identifica a la red y qué parte identifica al equipo concreto. Esa separación la realiza la máscara de red, que divide la dirección en dos secciones con roles distintos:

- Los bits de mayor peso conforman el Identificador de Red (NetID), que le indica a los enrutadores a qué segmento pertenece un paquete para poder enviarlo sin necesitar conocer la ubicación exacta de cada terminal.
- Los bits restantes forman el Identificador de Host (HostID), cuya función es distinguir cada interfaz, ya sea física o virtual, dentro de ese segmento particular.

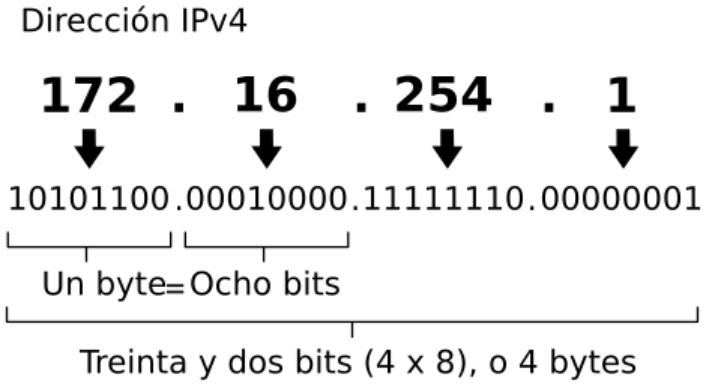

Figura 3. Detalle de una dirección IPv4.

2.2.2.2. Fundamentos y Necesidad de la Segmentación de Red

Una red plana, en la que todos los dispositivos conviven en el mismo espacio lógico, funciona bien cuando la infraestructura es pequeña. El problema aparece cuando esa infraestructura crece: el tráfico se vuelve inmanejable, la seguridad se debilita y

cualquier fallo tiene el potencial de afectar a toda la red. Frente a eso, dividir el espacio en subredes independientes aporta soluciones concretas que Paucar et al. (2025) recoge de la siguiente manera:

- **Mitigación de tormentas de difusión:** Al reducir el tamaño de los dominios de broadcast, los paquetes de difusión quedan contenidos dentro de su propio segmento y no llegan a saturar los canales ni a degradar el rendimiento de equipos ubicados en otras partes de la red.
- **Aislamiento de tráfico por criticidad:** Servicios como la telefonía IP, los sistemas de videovigilancia o las conexiones a bases de datos institucionales pueden operar en subredes separadas del tráfico general, lo que reduce considerablemente la exposición a interceptaciones internas.
- **Optimización de recursos perimetrales:** Conocer el tipo de tráfico que circula por cada segmento permite concentrar las reglas de inspección del cortafuegos justo donde se necesitan, sin que el motor de filtrado tenga que procesar tráfico que no representa riesgo.

2.2.2.3. Optimización Mediante Máscaras de Longitud Variable

Uno de los problemas más frecuentes en el diseño de redes es el desperdicio de direcciones IP: cuando se asigna el mismo tamaño de bloque a todos los segmentos sin importar cuántos equipos van a conectarse, el espacio disponible se agota más rápido de lo necesario. La técnica VLSM aborda ese problema de raíz. La UNEMI (2022) señala que este esquema permite subdividir el espacio de direccionamiento de manera recursiva y diferenciada, ajustando el prefijo de cada subred a la cantidad real de hosts que debe soportar.

2.2.3. Redes WAN

Una Red de Área Amplia es una infraestructura que permite interconectar equipos y redes locales situados a grandes distancias geográficas (Vera & Llambo, 2021). Desde el punto de vista funcional, una arquitectura WAN hace que la organización pierda el control sobre el perímetro físico e interno de su red, lo que la obliga a apoyarse en canales de transporte, conmutadores y pasarelas de comunicación que administran los Proveedores de Servicios de Internet. Son estos elementos externos los que hacen posible el tránsito y el enrutamiento de paquetes de datos a gran escala.

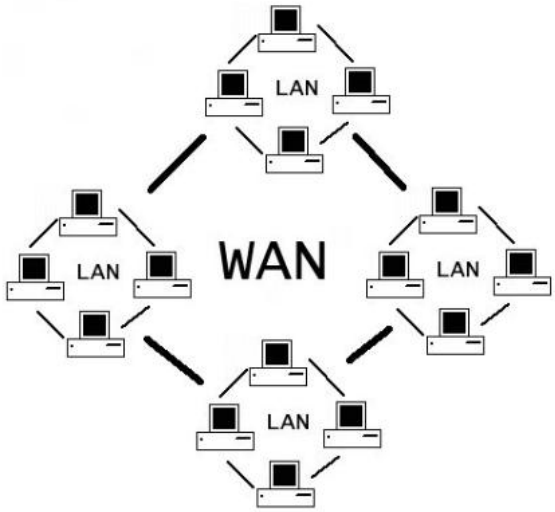

Figura 4. Representación de una red WAN.

2.2.3.1. Modelos de conectividad WAN

La forma en que se transmiten los datos en una red de área amplia depende del medio físico o lógico por el que viaja la información. Se distinguen, sobre todo, dos esquemas teóricos:

- **Enlaces dedicados:** Este modelo usa líneas físicas exclusivas que entregan los operadores de telecomunicaciones. Estas líneas garantizan un ancho de banda constante, parámetros predecibles y un aislamiento natural del tráfico. Sin embargo, los costos de operación elevados limitan bastante su adopción generalizada (Vera & Llambo, 2021).
- **Internet público:** Aquí se aprovechan los accesos comerciales comunes a la red mundial, lo que resulta una alternativa económica y de alta disponibilidad para establecer enlaces de datos (Borja, 2022).

2.2.3.2. El factor de latencia en los enlaces de larga distancia

El rendimiento de una arquitectura WAN está sujeto a restricciones geográficas inevitables. La distancia física que separa los extremos de la red genera una latencia base estructural que depende de la velocidad con que se propagan las señales en el medio físico y del número de conmutaciones en los enrutadores intermedios del proveedor de servicios. Este retardo geográfico acumulado representa el tiempo base que tarda la información en viajar y se mide de manera práctica mediante el Tiempo de Ida y Vuelta (Ponce, Yumber, & Herrera, 2023). Conocer esta latencia base sin procesar es indispensable en ingeniería de redes, ya que constituye el punto de

partida antes de que se sume el retraso computacional que introducen el procesamiento y el cifrado de los datos.

2.2.4. Seguridad de la información en infraestructura de red

La seguridad de la información en infraestructuras de red consiste en coordinar políticas, diseños lógicos y sistemas de cifrado para proteger los datos que se transmiten, ya sea por medios físicos o virtuales (Ponce, Yumber, & Herrera, 2023).

2.2.4.1. La Triada de la Seguridad (CIA)

En el diseño de redes de telecomunicaciones distribuidas para entornos académicos, la seguridad no se resuelve simplemente poniendo un firewall en cada campus y dando el tema por cerrado. Como señala Obregón, (2025) en su análisis sobre los desafíos de seguridad en plataformas digitales, toda infraestructura debe construirse sobre tres principios que no son negociables:

Figura 5. Triada de la seguridad (CIA).

- **Confidencialidad:** Garantiza que los flujos de datos y la información restringida que circulan por la red permanezcan accesibles únicamente para las entidades y los procesos autenticados y autorizados. Para preservarla se reduce el riesgo de divulgación no autorizada de paquetes mediante algoritmos criptográficos que convierten la información en ilegible para terceros.
- **Integridad:** Asegura que los datos enviados desde un nodo de origen no sufran alteraciones, modificaciones, inserciones o eliminaciones maliciosas o accidentales durante su recorrido por los canales de comunicación. En teoría,

esto se comprueba a través de funciones de dispersión criptográfica y códigos de autenticación de mensajes, que validan que el paquete recibido sea exactamente igual al que se envió.

- **Disponibilidad:** Establece que los recursos de red, el ancho de banda y los servicios de conectividad deben permanecer operativos y accesibles en el momento en que los usuarios legítimos los requieran. Esto exige que la infraestructura sea resistente frente a fallas o saturaciones intencionadas que busquen degradar o interrumpir el canal de comunicación.

2.2.4.2. Vulnerabilidades en el tránsito de datos

Cuando la información circula por canales que escapan del control físico del perímetro local, los datagramas quedan expuestos a distintos vectores de ataque orientados a interceptar o manipular el tráfico. Al respecto, Salazar et al. (2023) señalan que los principales vectores de ataque orientados a interceptar o manipular el tráfico en estos entornos son los siguientes:

- **Transmisión en texto plano:** Es la vulnerabilidad básica y aparece cuando los protocolos de aplicación transfieren la información sin codificación criptográfica previa. Cualquier nodo intermedio en la ruta de red puede leer sin restricciones los encabezados y la carga útil de los paquetes.
- **Sniffing:** Técnica de escucha pasiva en la que un agente no autorizado configura la interfaz de red en modo promiscuo dentro de un segmento compartido, con el fin de capturar y almacenar las tramas de datos en tránsito. Esta práctica compromete de manera directa la confidencialidad del canal.
- **Ataques Man-in-the-Middle:** Es un vector de ataque activo donde un elemento externo interfiere lógicamente en la ruta de comunicación entre dos extremos de la red y desvía el flujo de tráfico hacia su propia estación de forma transparente. Esto le permite no solo examinar el contenido de los paquetes, sino también modificar la información o suplantar la identidad de los extremos antes de retransmitirla, lo que rompe al mismo tiempo la confidencialidad y la integridad de la transmisión.

2.2.4.3. Criptografía Básica Aplicada

Para atacar de raíz esas vulnerabilidades del medio de transporte, las arquitecturas VPN se apoyan en criptografía aplicada, que básicamente convierte la información en algo completamente ilegible mediante funciones matemáticas. Whitman &

Mattord, (2022), en su investigación sobre estándares federales de procesamiento de información, explica que para garantizar confidencialidad en enlaces de alto rendimiento se usa criptografía simétrica, siendo AES el referente absoluto de la industria. AES trabaja aplicando sustituciones y permutaciones matemáticas sobre bloques de datos de tamaño fijo, con claves de 128 o 256 bits. Su diseño está pensado para ser eficiente en los procesadores especializados de los firewalls modernos, lo que le permite cifrar grandes volúmenes de tráfico sin introducir variaciones de retardo que afectarían servicios en tiempo real como la telefonía IP.

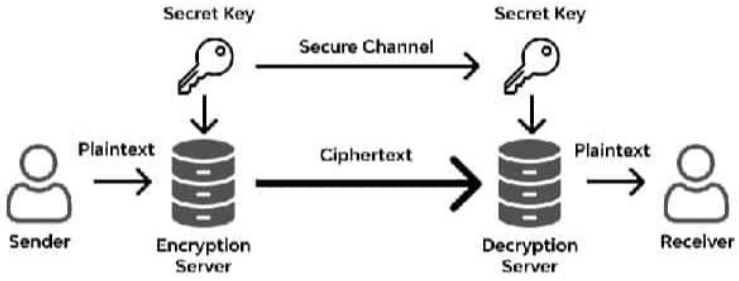

Figura 6. Modelo de funcionamiento de la encriptación AES.

Para la integridad, el mecanismo es diferente: no se cifra, sino que se usan funciones de hash criptográfico. Whitman & Mattord, (2022) explica que algoritmos como SHA-256 procesan el paquete completo y generan una cadena hexadecimal de 256 bits que es matemáticamente irreversible. Si durante el trayecto alguien modifica, aunque sea un solo bit del contenido, el hash que calcula el receptor no va a coincidir con el original, y el equipo descarta el paquete de inmediato para evitar que se inyecte código malicioso.

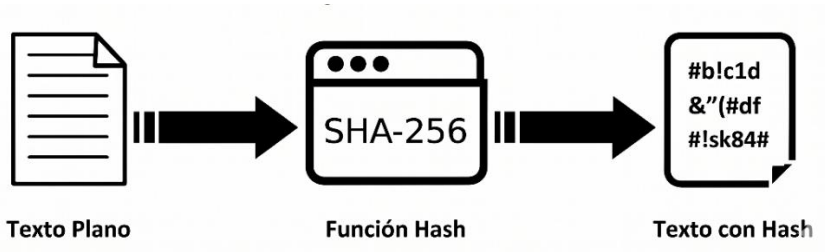

Figura 7. Modelo de funcionamiento del algoritmo Hash.

Cuando se combinan el cifrado AES y la validación SHA dentro de una estructura llamada HMAC, se obtiene un motor criptográfico robusto.

2.2.5. Redes Privadas Virtuales

Cuando se diseñan redes WAN para organizaciones, la Red Privada Virtual es la solución que permite proteger los datos que viajan por canales públicos donde no se tiene control del perímetro. Como explica Fortinet, (2026) la función de una VPN es ocultar la dirección IP del usuario y así crear un túnel privado incluso cuando la conexión se hace desde una red wifi pública. Por lo tanto, se ha convertido en una de las herramientas más eficaces para proteger la privacidad y el anonimato en Internet, ya que proporciona conexiones cifradas y seguras.

Figura 8. Funcionamiento de un túnel VPN.

2.2.5.1 Modelos de implementación

La forma en que se integran los canales virtuales protegidos depende de qué tan persistente sea el enlace y del perfil de los puntos finales que se conectan. Guerra (2023) agrupa estas implementaciones en dos modelos principales:

- **VPN sitio a sitio:** Se establece una interconexión permanente, fija y transparente entre dos o más redes locales separadas geográficamente, por ejemplo, la sede principal y los campus remotos. Todo el trabajo criptográfico queda a cargo de los firewalls o dispositivos de borde, de modo que las máquinas internas no necesitan ejecutar ningún software de seguridad adicional.

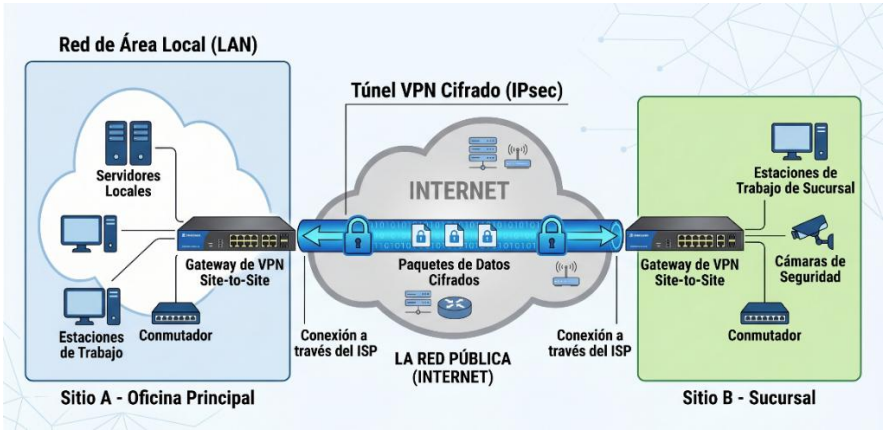

Figura 9. Modelo de conexión site to site.

- **VPN de acceso remoto:** Pensada para conexiones temporales y móviles de usuarios individuales. En este caso, la persona debe instalar un programa cliente en su equipo; ese cliente negocia de manera dinámica un túnel seguro temporal hacia el firewall central, y por lo general se apoya en autenticación multifactor.

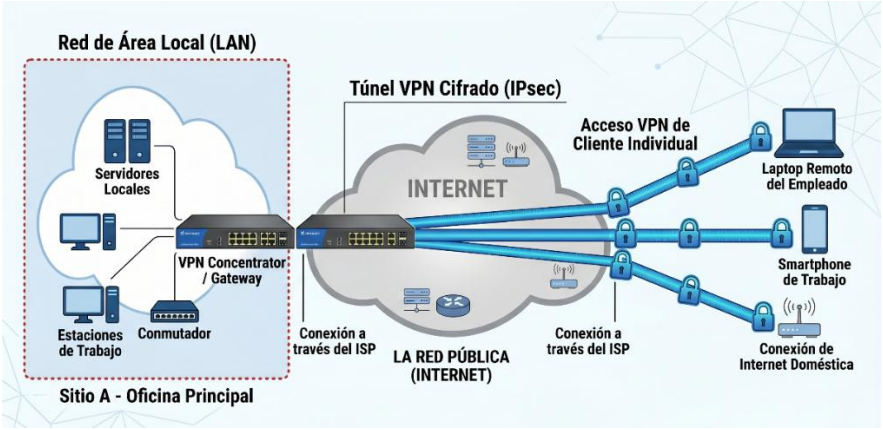

Figura 10. Modelo de conexión client to site.

2.2.5.2 Topologías VPN

La manera en que se organizan y conectan lógicamente los túneles repercute directamente en la latencia, la tolerancia a fallos y la carga de procesamiento de los equipos. Rios & López, (2024) explica que las infraestructuras WAN suelen adoptar dos configuraciones de red virtualizada:

- **Topología Hub-and-Spoke (estrella):** un concentrador central (Hub) reúne las políticas de seguridad y la conectividad, mientras que las sedes remotas (Spokes) levantan túneles exclusivos hacia él. Es el modelo más adecuado cuando los servicios están centralizados en una sola sede, porque evita

duplicar configuraciones lógicas, aunque introduce un único punto de fallo en el nodo central.

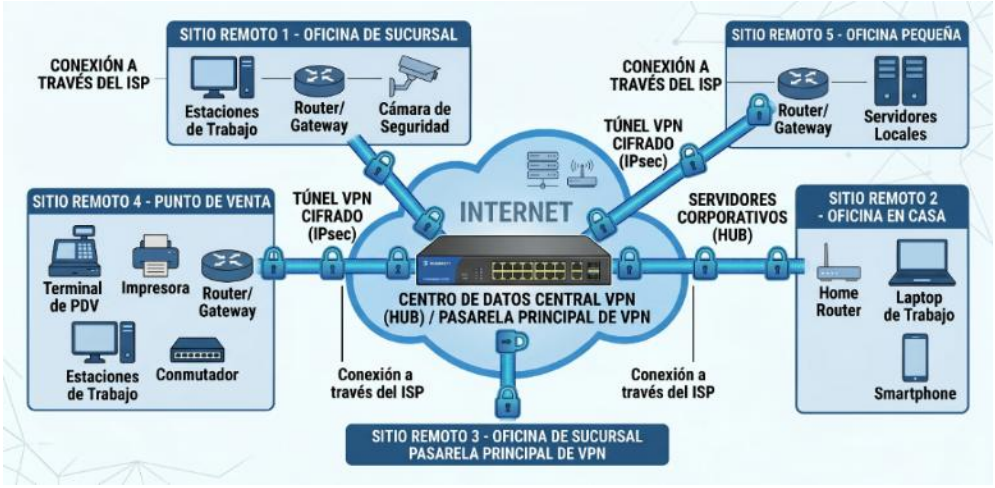

Figura 11. Topología Hub-and-Spoke o estrella.

- **Topología Full Mesh (malla completa):** en esta arquitectura, cada puerta de enlace perimetral mantiene un canal cifrado directo y simultáneo con todos los demás nodos de la red distribuida. La ventaja es que se reducen los retardos porque el tráfico viaja por rutas directas sin pasar por un intermediario. La desventaja es que el número de asociaciones de seguridad crece de forma exponencial (n(n−1)), lo que complica el procesamiento y limita bastante la escalabilidad en hardware convencional.

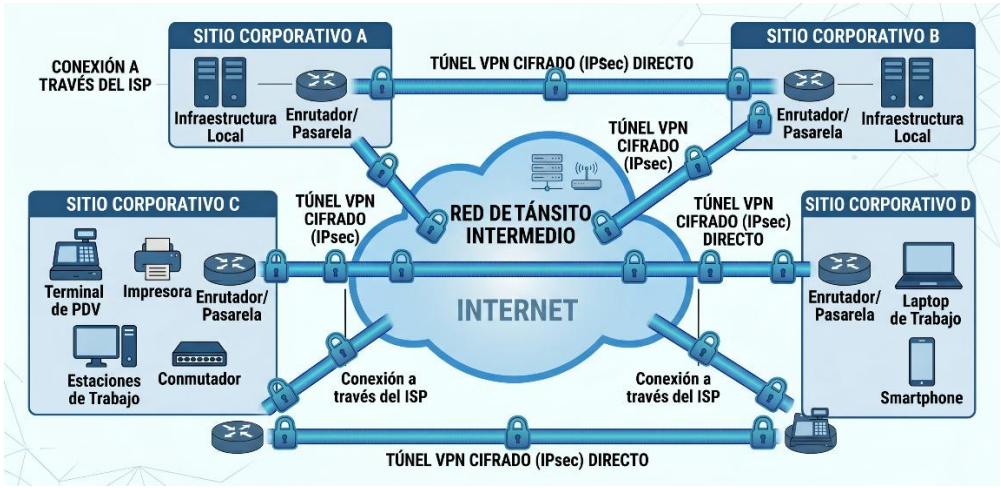

Figura 12. Topología de red malla completa.

2.2.5.3. Técnicas de Ruteo

El manejo del tráfico genérico hacia internet desde los nodos satélites o clientes remotos dicta la eficiencia del uso del ancho de banda de la red universitaria. En su análisis sobre la evolución de las arquitecturas SASE de red, Cloudflare, (2024) explica que existen los túneles se estructuran bajo los siguientes perfiles operativos:

- **Full Tunneling:** Secuestra a nivel del sistema operativo todo el espectro de tráfico IP originado por la máquina o subred remota. De este modo, sea una petición al servidor financiero local o un acceso genérico a un motor de búsqueda, todo viaja encriptado hasta el cortafuegos principal de la sede matriz. Aunque este diseño garantiza visibilidad analítica total y el cumplimiento de las políticas de filtrado corporativo, somete a la red al destructivo efecto hairpinning. Forzar tráfico de navegación pública por un túnel interurbano provoca la saturación severa de la fibra óptica de la sede matriz y multiplica por tres los tiempos de respuesta para el usuario final.

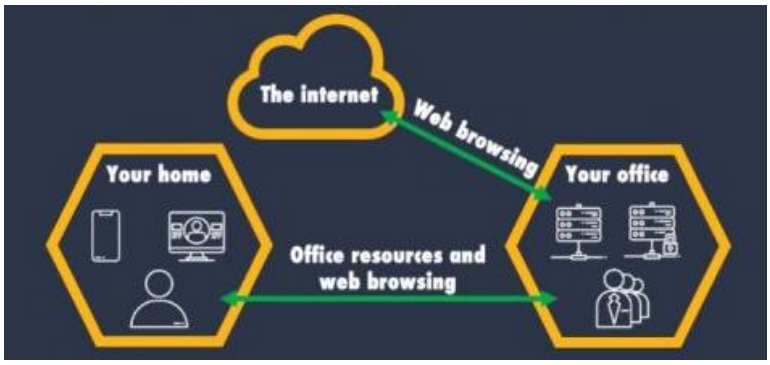

Figura 13. *Modelo de Full Tunneling.*

- **Split Tunneling:** Mediante esta técnica, el ingeniero de red inyecta políticas de enrutamiento condicional estáticas en el equipo de borde remoto. El cortafuegos local inspecciona el campo IP de destino en la cabecera IP de origen: si el paquete está destinado a una subred declarada como corporativa, la carga es encapsulada hacia el túnel VPN. Si el algoritmo detecta una IP genérica que no sea institucional, excluye el paquete de la capa criptográfica, le realiza la traducción de direcciones de red (NAT) y lo envía de inmediato a internet mediante el enlace de banda ancha de la sucursal remota. Este enrutamiento selectivo reduce de forma significativa la carga de procesamiento sobre la unidad central de la organización, lo que

optimiza la velocidad de transmisión y reserva el túnel cifrado exclusivamente para el tráfico que realmente lo requiere.

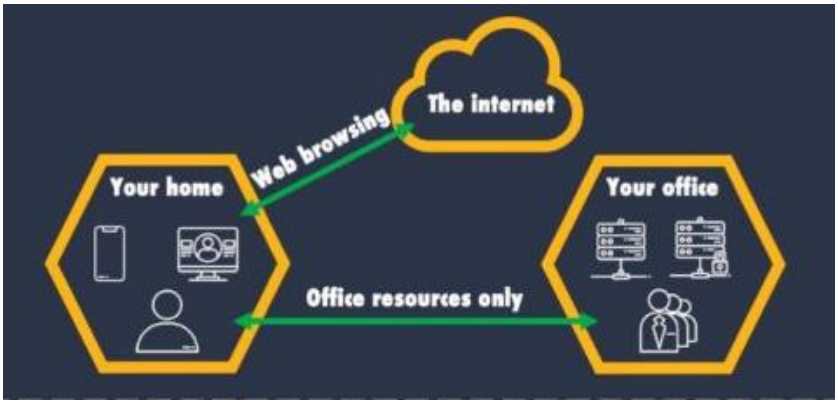

Figura 14. Modelo Split Tunneling.

2.2.5.4. Protocolos de Túneles VPN

Un protocolo VPN permite crear mediante procedimientos y reglas un túnel seguro y cifrado a través de una red pública como lo es internet, para que dispositivos remotos se puedan comunicar a una red privada. Coello, (2025) advierte que quedarse con el cifrado más fuerte como único criterio es un error: la arquitectura interna del protocolo, cómo gestiona sus cabeceras y cuántos recursos consume en los enrutadores bajo carga real son factores igual de críticos. Tres arquitecturas concentran hoy ese debate:

1. OpenVPN

Este protocolo posee una amplia trayectoria en el ámbito de las telecomunicaciones, lo cual se refleja tanto en su estabilidad operativa como en sus restricciones estructurales de diseño.

- **Arquitectura de memoria**. Perdigón & Madrigal, (2022) exponen que cada paquete que llega a la tarjeta de red se copia del núcleo del sistema a la memoria de usuario para cifrarlo, y después se copia otra vez al núcleo para poder enviarlo. Ese viaje de ida y vuelta se repite con todos los paquetes. En conexiones de un Gigabit, donde circulan millones de paquetes por segundo, el gasto de procesador que genera ese constante cambio de contexto es un problema grande.
- **División de canales:** El protocolo divide sus funciones en dos canales que operan de manera paralela. El canal de control emplea TLS con certificados

asimétricos para verificar la identidad de ambos extremos al iniciar una conexión. Una vez completada la autenticación se activa el canal de datos por donde el tráfico real circula protegido con algoritmos simétricos más eficientes (Carvajal, 2025).

- **Modos de operación:** OpenVPN puede funcionar en dos modos: a nivel de capa 2 por medio de interfaces TAP, lo cual resulta práctico cuando se necesita pasar tráfico de difusión como DHCP a través del túnel; o a nivel de capa 3 usando interfaces TUN, que es el modo habitual para el enrutamiento IP convencional entre redes.

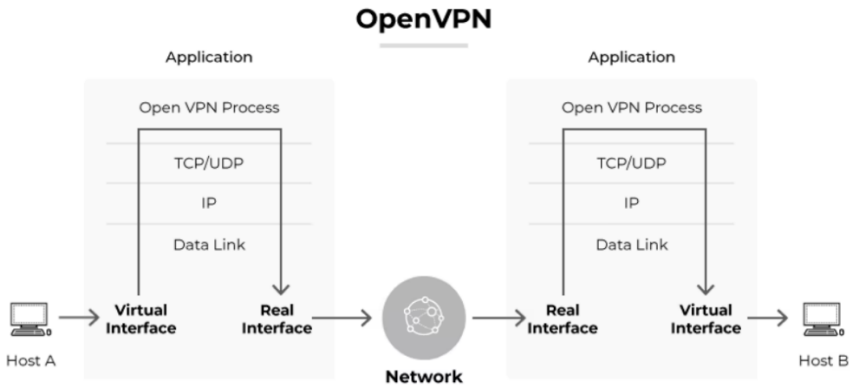

Figura 15. Flujo de datos en OpenVPN.

2. WireGuard

Este protocolo fue desarrollado con el objetivo de optimizar los entornos de conectividad segura frente a soluciones tradicionales como OpenVPN, mediante un rediseño integral de su arquitectura telemática.

- **Arquitectura monolítica:** Este protocolo se implementa como un módulo que corre directamente en el kernel de Linux. El código fuente ocupa alrededor de 4.000 líneas una cifra que a simple vista parece modesta, pero que cobra valor real cuando se la confronta con las extensiones propias de otros protocolos de propósito similar, donde la verbosidad suele ser la norma y no la excepción; y esa economía expresiva no es un mero dato anecdótico, porque con menos líneas la superficie expuesta a vulnerabilidades de día cero se reduce de forma considerable, y los paquetes, además, se cifran en la misma capa de memoria donde ocurre el enrutamiento físico, sin necesidad de copiarlos de un lado a otro (Berrones, 2025).

- **Primitivas criptográficas estáticas:** Carvajal (2025) señala que, a diferencia de OpenVPN e IPsec protocolos que permiten negociar qué algoritmos utilizar en cada sesión, ofreciendo un abanico de posibilidades que busca compatibilidad pero introduce complejidad, WireGuard simplemente impone un conjunto fijo: Curve25519 para el intercambio de claves elípticas, ChaCha20 para el cifrado del flujo de datos y Poly1305 para la autenticación de mensajes. No hay opciones, y esa rigidez, lejos de ser una limitación, elimina de raíz los ataques de degradación de cifrado, donde una atacante fuerza a los extremos a acordar un algoritmo más débil; justo el tipo de vulnerabilidad que, en entornos institucionales con múltiples dispositivos y versiones, suele explotarse con éxito cuando el protocolo ofrece demasiadas alternativas.
- **Enrutamiento por clave criptográfica:** tal como lo explica Berrones (2025), ata cada clave pública de un par a una lista específica de direcciones IP internas permitidas; de modo que si un paquete se descifra correctamente con la clave de un extremo, pero su IP de origen no figura en esa lista, el kernel lo descarta en silencio. Sin mensaje de error, sin respuesta. Previene eso la suplantación de identidad de una forma que otros protocolos no implementan tan limpiamente, precisamente porque la ausencia de retroalimentación elimina cualquier superficie de información que pudiera ser explotada por un atacante para inferir la existencia o estructura de las reglas internas.

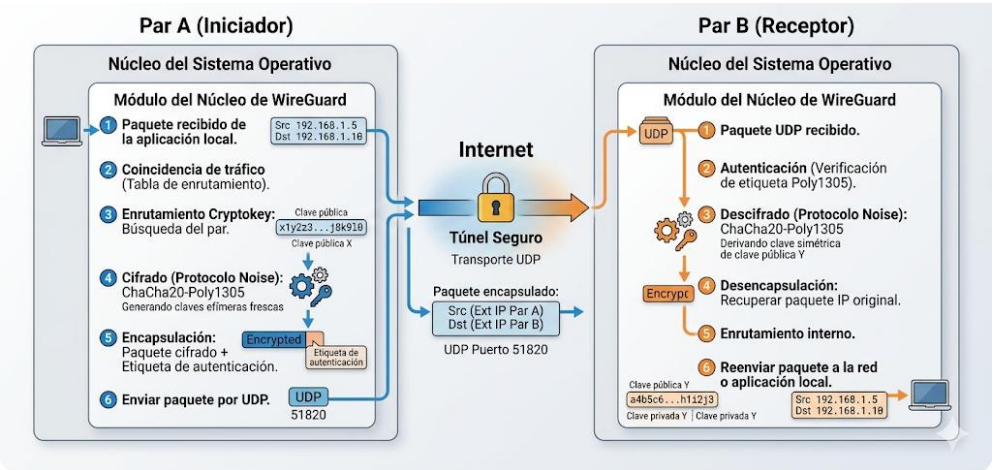

Figura 16. Funcionamiento de WireGuard.

3. Protocolo IPSec

IPsec no constituye un algoritmo de cifrado aislado, sino una suite de protocolos interconectados que operan de forma nativa en la capa de red (Capa 3) del modelo OSI.

- **Arquitectura Modular:** Lo que hace robusto a IPSec, señala Ojeda (2021), es precisamente su modularidad: permite configurar perfiles de seguridad específicos combinando dos protocolos independientes según lo que necesite cada escenario.
    1. **Autenticación Header (AH)**, cuya función es verificar que el paquete llegó sin modificaciones y que realmente proviene de quien dice provenir, usando para eso un código de autenticación basado en hash. Una limitación importante, no obstante, apunta Monterroso (2022): AH no cifra nada, el contenido del paquete viaja en texto plano, lo que lo deja expuesto a interceptaciones en redes públicas.
    2. **Encapsulating Security Payload (ESP)**, resuelve ese problema. Detalla Monterroso (2022) que ESP combina autenticación, verificación de integridad y cifrado simétrico directamente sobre la carga útil del paquete; para lograrlo, agrega una cabecera adicional y un campo de relleno al final del datagrama, lo que garantiza que el contenido sea completamente ilegible para cualquier herramienta de análisis de tráfico que intente interceptarlo en el camino.
- **Modos de Operación:** IPSec puede funcionar de dos maneras distintas, y la elección entre una y otra tiene consecuencias directas sobre el enrutamiento y el rendimiento de la red, aspecto que suele subestimarse en diseños iniciales pero que termina definiendo la viabilidad operativa de la solución en entornos con restricciones de ancho de banda o latencia variable.
    1. **Modo Transporte** está pensado para comunicaciones directas entre dos dispositivos finales. En este caso, ESP se inserta entre la cabecera IP original y la capa de transporte TCP/UDP, lo que resulta en una carga computacional menor. El problema es que las direcciones IP reales de los equipos que se comunican quedan visibles para el proveedor de internet, lo que lo hace poco adecuado cuando se necesita ocultar la topología interna de la red.

2. **Modo Túnel** es el estándar para conectar sedes geográficamente separadas. Ponce, Yumber, & Herrera, (2023) explican que en este modo el paquete IP original completo se cifra en su totalidad y se mete dentro de un nuevo paquete IP que solo muestra las direcciones públicas de los firewalls en cada extremo. La red interna queda completamente oculta para cualquier equipo intermedio.

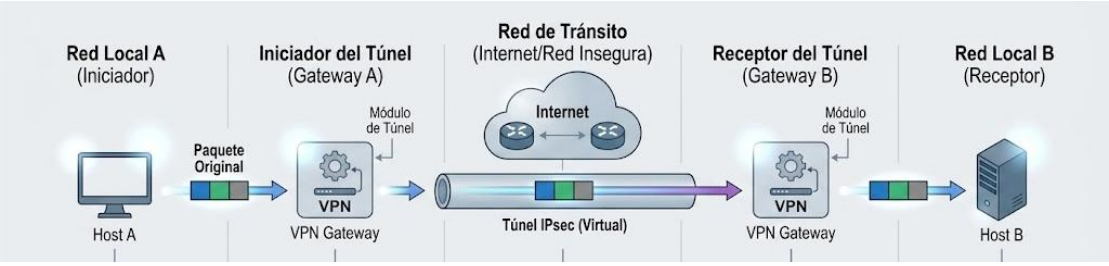

Figura 17. Mecanismo fundamental del túnel IPSec.

- **Negociación IKEv2:** Antes de que el túnel pueda funcionar, los equipos de ambos extremos necesitan ponerse de acuerdo sobre qué claves y algoritmos van a usar. Ese proceso lo gestiona el protocolo IKE. Ojeda, (2021) establece que IKEv2 es indispensable para que ESP funcione, y que opera en dos fases bien diferenciadas.

    1. **Fase 1**, los firewalls se autentican mutuamente usando certificados digitales o claves precompartidas. Durante esta etapa se ejecuta el algoritmo matemático de Diffie-Hellman, que Córdoba, (2022) describe como un mecanismo que permite a ambos equipos llegar a una clave maestra idéntica sin que esa clave viaje en ningún momento por el enlace. Al final de esta fase queda establecida la primera Asociación de Seguridad entre los extremos del túnel.
    2. **Fase 2**, también llamada Quick Mode, ya con el canal seguro establecido, se negocian los algoritmos criptográficos concretos que se van a aplicar al tráfico real de datos entre las sedes.

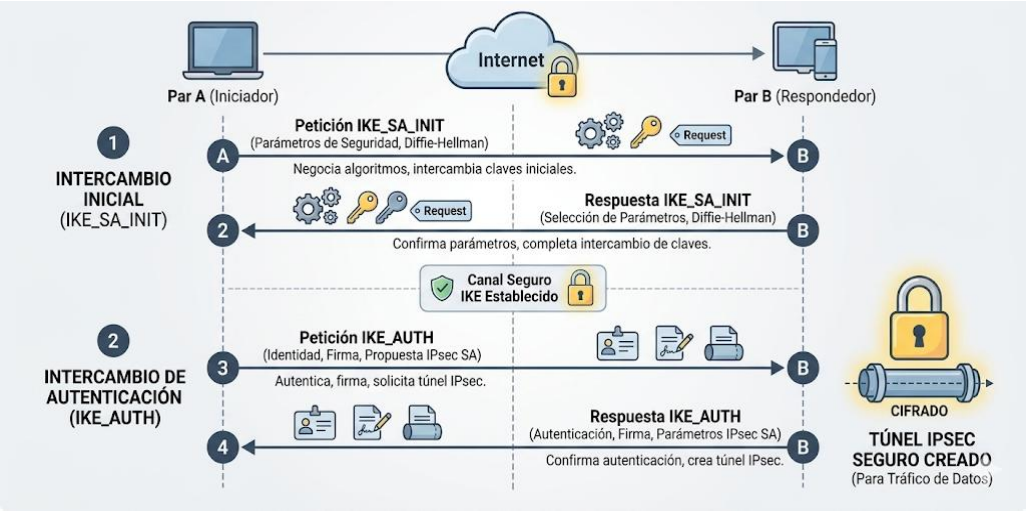

Figura 18. Negociación IKEv2.

Adicionalmente, para protegerse frente a ataques que graban tráfico cifrado con la esperanza de descifrarlo más adelante, se implementa el Secreto Perfecto hacia Adelante (PFS). Córdoba, (2022) explica que el PFS obliga a los equipos a ejecutar un intercambio Diffie-Hellman completamente nuevo e independiente para cada ciclo de renovación del túnel. El resultado es que, aunque un atacante lograra comprometer la clave principal de un dispositivo, no podría descifrar las sesiones anteriores, porque cada una fue cifrada con claves derivadas de forma completamente independiente entre sí.

2.2.6. Calidad de Servicio en redes con cifrado

En redes de alta velocidad, la Calidad de Servicio agrupa los mecanismos lógicos y de arquitectura que permiten asignar el ancho de banda de forma diferenciada y predecible sobre una infraestructura compartida. Según el estudio multicriterio de Ormachea et al. (2022), aplicar políticas de calidad de servicio se vuelve crítico cuando los flujos multimedia en tiempo real muy sensibles a las variaciones temporales, como la telefonía IP o los sistemas de videovigilancia CCTV centralizados tienen que convivir con tráfico de datos asíncrono en los enlaces WAN de una institución.

De acuerdo con la metodología de evaluación analítica expuesta por Romero, (2024), el comportamiento cualitativo y la eficiencia de los mecanismos de aprovisionamiento de tráfico se evalúan de forma cuantitativa continua mediante cuatro métricas elementales de rendimiento de capa 3 y capa 4:

- **Ancho de banda:** Tasa neta de bits efectivos transmitidos por unidad de tiempo a través del canal lógico.
- **Latencia:** Tiempo que transcurre desde que el nodo origen emite un datagrama hasta que el nodo destino lo recibe por completo. En entornos seguros, esta métrica incluye tanto el retardo de propagación del medio físico como el retardo de procesamiento que añade el hardware criptográfico de borde.
- **Fluctuación del retardo:** Se trata de la variación estadística en los tiempos de llegada de los paquetes que forman parte de un mismo flujo. Cuando el jitter es elevado, los búferes de recepción pierden sincronización, lo que perjudica de forma notable la calidad de las llamadas de voz sobre IP.
- **Tasa de pérdida de paquetes:** Es el porcentaje de paquetes que se pierden, ya sea porque las colas en las interfaces físicas se saturan o porque expira algún temporizador de espera antes de que puedan ser procesados.

Crece bastante la complejidad técnica cuando se introduce el encapsulamiento criptográfico. Cuando un protocolo como IPsec funciona en modo túnel con la cabecera ESP, explican Ormachea et al. (2022), la carga útil y las cabeceras originales de la capa de transporte quedan ocultas bajo una capa cifrada; al perderse esa visibilidad, los firewalls intermedios no pueden hacer inspección profunda de paquetes ni clasificar el tráfico por números de puerto. Configurar las políticas de QoS justo en el borde de la red, antes del cifrado, o copiar los bits del campo DSCP hacia la nueva cabecera IP externa para mantener las prioridades, se vuelve entonces obligatorio, lo que introduce un punto adicional de diseño que, si no se planifica con antelación, puede degradar el rendimiento de forma significativa en escenarios con volúmenes de tráfico elevados.

2.2.6.1 Límites de retardo para tráfico síncrono.

Al dimensionar los recursos en arquitecturas de borde para interconectar campus universitarios, hay que ceñirse a los umbrales de tolerancia que fijan los organismos internacionales. Define la Unión Internacional de Telecomunicaciones (UIT), mediante la recomendación ITU-T G.114 (2004), los límites de retardo unidireccional aceptables para conservar la fluidez de una conversación.

Cuando se diseñan túneles VPN intercampus, cumplir esa norma se vuelve un desafío directo debido al overhead de procesamiento y al retardo de serialización propios

del enrutamiento WAN. Si la infraestructura de transporte público ya introduce una latencia base alta por la distancia geográfica, los ciclos de reloj que el procesador del firewall consume para calcular algoritmos como AES-256 pueden empujar el tiempo de tránsito unidireccional más allá de la frontera crítica de 150 ms; el resultado son retardos asimétricos y pérdida de sincronía en las tramas de los servicios interactivos del perímetro, fenómenos que suelen manifestarse de forma más aguda en horas pico cuando la congestión de la red de transporte agrava los efectos del procesamiento criptográfico. En la Tabla 1 se observa el estándar que determina una categorización tridimensional para evaluar el impacto del retardo en aplicaciones interactivas:

Tabla 1. Límites de tolerancia de retardo unidireccional extremo a extremo.

Retardo Unidireccional (ms)	Clasificación de Impacto
0 a 150 ms	**Rango Aceptable:** Imperceptible resulta el retardo para el oído humano, constituyendo el objetivo de diseño indispensable para telefonía IP institucional de alta fidelidad.
150 a 400 ms	**Rango de Degradación Controlada:** Viable es aún la comunicación, aunque se introducen interrupciones notables y solapamiento conversacional; requiere, por tanto, sintonía fina de QoS para mantener la operatividad dentro de márgenes tolerables.
Mayor a 400 ms	**Rango Inaceptable:** La latencia base bloquea la interactividad en tiempo real; los búferes de descarte se saturan y el servicio pierde funcionalidad operativa, escenario que en la práctica suele traducirse en abandonos de llamada y reinicios de sesión que terminan afectando la percepción global del servicio más allá de lo que indican las métricas de red.

Nota: Adaptado de Recomendación UIT-T G.114: Objetivos de rendimiento de transmisión para el tiempo de transmisión unidireccional de extremo a extremo, por la Unión Internacional de Telecomunicaciones (UIT), 2004.

2.2.6.2 Mitigación de la fragmentación en túneles WAN

El encapsulamiento criptográfico agranda inevitablemente cada paquete, porque añade encabezados de seguridad, trailers y vectores de inicialización (IV). Esto hace que las VPN introduzcan un riesgo serio de degradación por fragmentación en la capa IP. Si un paquete TCP/IP común se acerca al tamaño estándar de la MTU de internet 1500 bytes, la sobrecarga de un túnel IPsec entre 50 y 70 bytes adicionales hace que la trama supere el límite físico que permiten los proveedores de servicio (ISP).

Según la documentación técnica de Cisco (2023), cuando un paquete supera la MTU del enlace de salida y tiene activo el bit Don't Fragment o DF en su cabecera IP, el enrutador de borde lo descarta y devuelve un mensaje ICMP tipo 3, código 4. Sin

embargo, como muchos firewalls perimetrales bloquean el tráfico ICMP por políticas de seguridad estrictas, este mensaje a menudo se pierde el llamado "agujero negro de PMTUD", lo que provoca que las sesiones colapsen sin razón aparente o sufran muchas retransmisiones.

Para resolver este problema sin debilitar el cifrado en el perímetro se emplea la técnica conocida como TCP MSS Clamping. Explica Cisco (2023) que se trata de una inspección activa: el firewall perimetral intercepta de forma transparente los paquetes de señalización TCP durante el establecimiento de la conexión, en concreto los que llevan los bits SYN o SYN-ACK activos.

Revisa el firewall el campo opcional TCP MSS donde los hosts declaran el tamaño máximo de carga útil que pueden recibir, normalmente 1460 bytes, y modifica ese valor a la baja. Al obligar a los hosts a generar segmentos más pequeños desde el origen, el paquete final, incluso con la sobrecarga de las cabeceras ESP e IPsec, nunca supera los 1500 bytes de la MTU WAN; se elimina así por completo la fragmentación en tránsito, se reduce la carga de CPU en el hardware perimetral y se evitan las pérdidas de rendimiento en la entrega de tráfico crítico intercampus, lo que convierte a esta técnica en un recurso casi indispensable cuando se opera con enlaces WAN de capacidad ajustada y se necesita garantizar la fluidez de aplicaciones sensibles a la latencia.

2.2.7. Ecosistema de Software Libre para Gestión Perimetral

El diseño de redes modernas ha experimentado una transformación progresiva, transitando de la dependencia exclusiva de hardware con Circuitos Integrados de Aplicación Específica propietarios, hacia la Virtualización de Funciones de Red soportada por sistemas operativos de código abierto. La relevancia del software de código abierto en las telecomunicaciones, sostiene Marín (2024) en su investigación sobre el fortalecimiento de la ciberseguridad en infraestructuras críticas, no se limita a la viabilidad económica derivada de la ausencia de licenciamiento, sino que se extiende hacia la transparencia estructural que ofrece frente a entornos tecnológicos cambiantes; una cualidad que, en el contexto de arquitecturas de borde para instituciones educativas con recursos limitados, resulta tan valiosa como el ahorro presupuestario, pues permite auditar el comportamiento del plano de datos sin depender de la caja negra que suelen imponer los fabricantes comerciales.

2.2.7.1 Análisis Comparativo de Distribuciones para Gestión Perimetral

Para la interconexión de ubicaciones geográficamente distribuidas, la selección del dispositivo de borde firewall o enrutador determina el límite superior del rendimiento de la red. A continuación, se presenta un análisis de las distribuciones más representativas del ecosistema de gestión perimetral de código abierto:

1. pfSense

   Constituye la distribución pfSense una de las plataformas de prevención perimetral de código abierto con mayor adopción en entornos institucionales. Establecen Camacho & Núñez (2021), en su estudio sobre plataformas de Gestión Unificada de Amenazas, que pfSense se fundamenta sobre el sistema operativo FreeBSD, del cual hereda el motor de filtrado de paquetes Packet Filter; este motor opera mediante inspección de estado, mecanismo mediante el cual el cortafuegos no evalúa únicamente direcciones IP o puertos de forma estática, sino que rastrea dinámicamente las banderas de sincronización y los números de secuencia del protocolo TCP, almacenándolos en memoria para validar la legitimidad de cada conexión entrante y saliente, lo que permite mitigar ataques de suplantación de identidad y denegación de servicio. Incorpora, además, pfSense integración nativa con el conjunto de instrucciones AES-NI de los procesadores modernos, lo que permite delegar las operaciones de cifrado simétrico como AES-256-GCM directamente al hardware físico; este mecanismo reduce la latencia computacional asociada al procesamiento criptográfico y minimiza la sobrecarga generada por la fragmentación de paquetes, contribuyendo a mantener un rendimiento cercano a la capacidad física del enlace de red, aspecto que en entornos con presupuestos ajustados resulta determinante para justificar la adopción de soluciones basadas en software frente a appliances comerciales de costo elevado.

2. OPNsense

   Surge OPNsense como una bifurcación del código fuente de pfSense, evolucionando hacia un modelo de desarrollo orientado a la seguridad a nivel de arquitectura de memoria y a la modernización de sus interfaces de programación. Establece Rios Monar & López Quezada (2024), en su evaluación de rendimiento de firewalls virtualizados, que OPNsense implementa modificaciones sustanciales respecto a su origen, entre las que se destacan ciclos de actualización

incrementales de mayor frecuencia. A nivel de sistema base, OPNsense utiliza HardenedBSD, una variante de FreeBSD que incorpora mecanismos de mitigación de vulnerabilidades como la Aleatorización del Diseño del Espacio de Direcciones, técnica que dificulta la predicción de las ubicaciones en memoria de las rutinas de los protocolos de red, reduciendo la superficie de ataque ante intentos de inyección de código malicioso. Destaca, además, que OPNsense incorpora un marco de trabajo de API RESTful que permite automatizar la gestión de reglas de enrutamiento mediante scripts externos, así como soporte para el marco de red Netmap; este último posibilita la integración de un Sistema de Prevención de Intrusos (IPS) en línea, con capacidad para interceptar y descartar flujos anómalos de paquetes a velocidades del orden de Gigabit, sin generar una carga excesiva sobre el procesador central del dispositivo, lo que resulta especialmente valioso cuando se opera con enlaces de alta capacidad y se requiere inspección en tiempo real sin degradar el rendimiento..

3. VyOS

Es VyOS un sistema operativo de red desarrollado sobre el núcleo Linux (Debian), concebido para emular el modelo operativo de enrutadores empresariales de uso extendido en la industria. Detalla Aspera (2025), en su análisis de arquitecturas virtualizadas y controladores de red, que VyOS centraliza los servicios perimetrales incluyendo el cifrado IPSec, la traducción de direcciones de red (NAT) y la tunelización de paquetes en una interfaz unificada de línea de comandos de tipo transaccional; este modelo de administración permite a los ingenieros preparar, revisar y confirmar cambios en las tablas de enrutamiento mediante operaciones de commit y rollback, reduciendo el riesgo de interrupciones accidentales en enlaces de producción.

Desde la perspectiva del rendimiento, Sentrium (2022) señala que la ausencia de una interfaz gráfica web elimina los procesos asociados a servidores HTTP y motores de bases de datos que consumen recursos del procesador en segundo plano, lo que se traduce en una eficiencia computacional elevada al procesar protocolos de enrutamiento dinámico como OSPF o BGP a través de su motor interno FRRouting. En entornos de red con múltiples sedes, esta característica lo posiciona como una opción adecuada para operar como reflector de rutas en el núcleo de la red, con capacidad para gestionar grandes volúmenes de rutas IP manteniendo valores de retardo estables; justo el perfil de carga que suele exigirse

en arquitecturas de campus distribuidos donde la estabilidad de la tabla de enrutamiento es tan crítica como la velocidad de convergencia.

2.2.8. Entornos de evaluación

Validar una arquitectura de red antes de llevarla a producción no es opcional; es una práctica metodológica consolidada en telecomunicaciones y ciberseguridad. El problema del hardware físico es su costo: adquirir equipos reales para un laboratorio de pruebas resulta inviable en la mayoría de los contextos académicos e investigativos. Por eso los entornos virtualizados se han convertido en la alternativa estándar (Gómez et al., 2023). Ahora bien, el mismo estudio advierte algo que con frecuencia se ignora: no todos los entornos virtualizados son equivalentes, y confundir simulación con emulación puede arruinar por completo la validez de los resultados obtenidos.

2.2.8.1. Simulación de Redes

Simular una red significa construir un modelo de software que replica, de forma aproximada, cómo se comporta un dispositivo y cómo transita el tráfico entre nodos. Son claros Asadi et al. (2024) al respecto: los simuladores no corren el sistema operativo real del equipo; funcionan con modelos matemáticos de eventos discretos, respondiendo solo a comandos que ya tienen programados. No hay kernel real, no hay acceso al hardware del anfitrión.

Eso los hace muy eficientes en recursos poca RAM, poco CPU, pero los vuelve inútiles para ciberseguridad seria. Plantea Galata et al. (2024) que, sin un núcleo operativo auténtico, el simulador no puede ejecutar rutinas criptográficas reales; cuando un túnel VPN "funciona" en un simulador, lo que ocurre no es un proceso de cifrado real sino una representación visual del mismo. Nada de eso es medible ni auditable.

2.2.8.2. Emulación de Redes

La emulación funciona diferente desde la base. No modela el comportamiento del dispositivo: recrea su hardware para que el sistema operativo de red corra exactamente igual que lo haría en un equipo físico de producción. Explican Flores et al. (2024) que esto se logra mediante virtualización asistida por hardware, donde los componentes virtuales interactúan directamente con la CPU física del servidor.

QEMU y KVM son las tecnologías que hacen posible esa interacción. Al asignar ciclos reales del procesador a cada nodo emulado y correr el firmware original del

fabricante sin modificaciones, la fidelidad del tráfico es total; en la práctica eso significa poder auditar paquetes cifrados mientras viajan, completar negociaciones IKEv1 e IKEv2 de principio a fin, y medir latencia y jitter con los mismos instrumentos que se usarían en producción, lo que convierte a la emulación en el único entorno de pruebas que puede ofrecer resultados directamente trasladables a escenarios reales sin necesidad de correcciones por factores de escala..

2.2.8.3. Análisis de Herramientas de Virtualización de Red

Tres plataformas concentran el uso en virtualización de red. Cada una responde a necesidades distintas y tiene limitaciones concretas que conviene entender antes de elegir.

- **Cisco Packet Tracer:** Es el simulador educativo de Cisco, ampliamente usado para aprender los fundamentos de Capa 2 y Capa 3 del modelo OSI. Asadi et al. (2024) confirman su utilidad pedagógica en ese nivel. El inconveniente es estructural: al ser un simulador de eventos discretos con núcleo cerrado, no acepta software externo ni distribuciones FreeBSD o Linux. Tampoco tiene motor de cifrado real, así que cualquier configuración de VPN que se haga es pura sintaxis, sin procesamiento criptográfico detrás.
- **EVE-NG:** El Emulated Virtual Environment Next Generation corre el kernel real de los sistemas operativos mediante QEMU, lo que lo convierte técnicamente en un emulador. Harahus et al. (2024) lo destacan por su interfaz web sin cliente y su compatibilidad con plataformas empresariales. Pero su modelo freemium es un problema real para investigación: la versión gratuita no permite modificar interfaces con los nodos activos, no integra Docker de forma fluida y bloquea la captura completa de tráfico con Wireshark.
- **GNS3:** El Graphical Network Simulator-3 es el emulador de código abierto con arquitectura cliente-servidor. Su integración con QEMU y KVM, señalan Galata et al. (2024), permite emular arquitecturas x86 y ARM sin ninguna restricción de licencia. Al ser libre, importa y ejecuta pfSense de forma directa y transparente. Corre el procesamiento matemático sobre el CPU del host, lo que habilita validar cualquier suite criptográfica y capturar el 100% del tráfico con Wireshark en tiempo real, sin límites ni pagos adicionales; una combinación de características que lo convierte en la herramienta de elección cuando se requiere fidelidad absoluta en la reproducción de comportamientos de red sin

incurrir en costos de licenciamiento que suelen hacer inviables los laboratorios de pruebas en entornos académicos.

2.2.8.4. Herramientas de Análisis y Evaluación de Rendimiento en Redes

Que una VPN conecte dos sedes no significa que funcione bien. La conectividad es el mínimo; lo que realmente importa es cuánto castiga el rendimiento de la red el hecho de cifrar y encapsular cada paquete. Medir eso exige herramientas específicas y variables concretas: ancho de banda real, variación del retardo y latencia, entre otras. Subraya Moreira (2022) que, sin esa medición estadística, cualquier validación de un entorno seguro es incompleta.

1. Ping y el Protocolo ICMP

   Ping es lo primero que se ejecuta y, bien interpretado, dice bastante. Trabaja en Capa 3 enviando paquetes ICMP de solicitud y respuesta de eco entre dos puntos. En el contexto de un túnel IPsec, Ponce, Yumber, & Herrera, (2023) precisa que Ping cumple dos funciones distintas: confirma que existe accesibilidad lógica bidireccional entre las sedes, y establece la métrica base de latencia mediante el RTT (Round Trip Time). Ese tiempo, medido en milisegundos, refleja directamente cuánto tarda el procesamiento criptográfico de los firewalls en despachar cada paquete. Es un número simple, pero es el primer síntoma de que algo va mal o bien.

2. iPerf3

   Esta herramienta dice qué tan transitado puede estar ese camino antes de colapsar. Funciona bajo un modelo cliente-servidor que genera flujos de datos activos tanto en TCP como en UDP. Lo identifican Torres et al. (2023) como el estándar de la industria para medir throughput real frente al ancho de banda contratado. En un escenario VPN, lo que hace iPerf3 es inyectar ráfagas controladas de datos y cuantificar exactamente cuánto de ese ancho de banda se pierde por las cabeceras ESP que IPsec añade a cada paquete; cuando se fuerza tráfico UDP, además calcula pérdida de paquetes y jitter, dos variables críticas para servicios como la Telefonía IP, donde la variación del retardo destruye la calidad de la llamada antes de que el usuario lo note.

3. Wireshark

Examina esta herramienta cada paquete individualmente y lo descompone capa por capa según el modelo OSI. Confirman Torres et al. (2023) su valor para observar el comportamiento dinámico del tráfico en tiempo real. En esta investigación su rol es probatorio: se usa para certificar que el cifrado del túnel funciona como debe. Wireshark no debe poder leer el contenido original de los paquetes; lo que aparecen son cabeceras ESP o tráfico enmascarado en el puerto UDP 4500 cuando hay NAT-T de por medio. Si eso es lo que muestra la captura, el túnel es criptográficamente sólido, y esa verificación visual –por elemental que parezca– constituye la evidencia más directa de que la confidencialidad prometida por el protocolo se está cumpliendo en la práctica.

2.2.9 Interoperabilidad y Estándares Internacionales

El ecosistema global de telecomunicaciones opera sobre una premisa fundamental de ingeniería la adopción de protocolos abiertos y tecnológicamente neutrales. En este contexto el MinTIC, 2021 dentro de su análisis normativo de arquitecturas de internet, señala que la fuerza de tareas de ingeniería de internet constituye la entidad encargada de diseñar, evaluar y publicar las especificaciones técnicas que rigen el tránsito de datos en redes de comunicación; estas especificaciones se materializan a través de documentos estandarizados denominados RFC.

La relevancia operativa de estos estándares reside en su capacidad para garantizar la interoperabilidad entre entornos tecnológicamente heterogéneos. Sostienen Wassef & Lee (2024), en su investigación sobre la optimización de seguridad en ecosistemas de red complejos, que la estandarización promovida por la IETF permite que protocolos criptográficos establezcan reglas universales de encapsulamiento, de modo que la carga útil transmitida desde un dispositivo emisor pueda ser interpretada, descifrada y enrutada correctamente por el receptor, independientemente de la arquitectura de hardware subyacente; esta característica elimina el fenómeno de dependencia de fabricante, permitiendo que las instituciones puedan integrar dispositivos de distintos fabricantes en una misma infraestructura de red sin comprometer la continuidad operativa del túnel VPN, aspecto que en entornos con presupuestos limitados y renovaciones tecnológicas escalonadas resulta tan determinante como el propio rendimiento criptográfico.

2.2.9.1 Viabilidad de Interconexión entre Sistemas Heterogéneos

El diseño de arquitecturas Site-to-Site que combinan equipos propietarios con software libre no es un escenario nuevo en redes institucionales, pero sí plantea preguntas técnicas concretas que vale la pena revisar con detenimiento. Plataformas como FortiGate y distribuciones como pfSense son quizás el ejemplo más representativo de esta convivencia híbrida.

El primer punto de contraste entre ambas está en cómo cada una resuelve el cifrado. Documenta Romero (2021) que los equipos FortiGate incorporan Circuitos Integrados de Aplicación Específica (ASIC) diseñados exclusivamente para asumir las operaciones criptográficas del protocolo IPSec; al sacar ese trabajo de la CPU principal, el dispositivo puede sostener flujos de múltiples gigabits con una afectación mínima sobre la latencia, algo que en redes de producción marca una diferencia práctica considerable.

pfSense resuelve el mismo problema, pero desde otro ángulo. Al correr sobre hardware convencional x86_64, no dispone de esos aceleradores. Lo que hace, según describen Rios & López (2024) en su evaluación de firewalls virtualizados, es apoyarse en las instrucciones AES-NI que traen integradas la mayoría de los procesadores Intel y AMD actuales; estas instrucciones permiten ejecutar el cifrado dentro de la propia unidad aritmética del procesador, sin necesidad de hardware adicional. El resultado en términos de jitter es aceptable para la mayoría de los entornos, aunque la capacidad máxima de procesamiento es naturalmente inferior a la de un ASIC dedicado.

Ahora bien, que ambos sistemas lleguen al cifrado por caminos distintos no impide que trabajen juntos. Lo señala Guerra (2023) con claridad en su estudio sobre redes Site-to-Site corporativas: la razón por la que esta interoperabilidad funciona es que los dos implementan IPSec siguiendo los mismos RFC de la IETF. Cuando se levanta el túnel, la Fase 1 del protocolo IKE pone a negociar a ambos dispositivos bajo Diffie-Hellman hasta que acuerdan los mismos parámetros; con eso resuelto, la Fase 2 establece el canal de datos mediante cabeceras ESP y el túnel queda operativo.

III. METODOLOGÍA

3.1. ENFOQUE METODOLÓGICO

3.1.1. Enfoque

La presente investigación posee un enfoque cuantitativo, debido a que se orienta al análisis y evaluación de variables relacionadas con el rendimiento y seguridad de una arquitectura VPN para la interconexión de campus universitarios. Este enfoque permitirá obtener datos medibles mediante pruebas de conectividad, latencia, transmisión de datos y comportamiento del tráfico de red dentro del entorno de emulación implementado.

3.1.2. Metodología

Para el desarrollo del presente trabajo de integración curricular, se adoptó la metodología PPDIOO, concebida originalmente por Cisco Systems. Esta metodología define el ciclo de vida continuo de las redes de telecomunicaciones y es reconocida como un estándar en la industria para garantizar que la infraestructura tecnológica cumpla con los requerimientos operativos, de seguridad y de escalabilidad de una institución (Cisco, 2006).

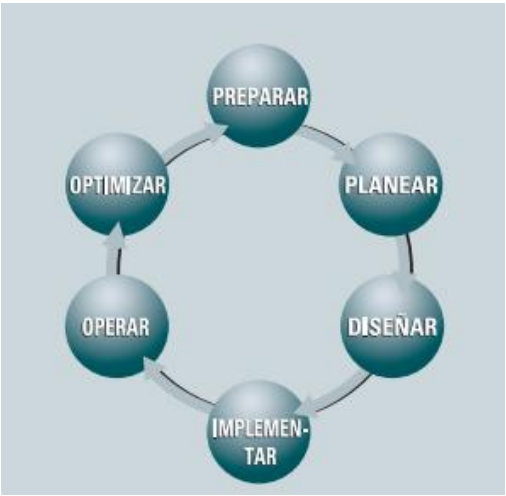

Figura 19. Metodología PPDIOO.

La elección de este marco metodológico se justifica por su enfoque estructurado, el cual permite transitar de manera ordenada desde la identificación de la

vulnerabilidad en las sedes remotas de la universidad hasta la emulación y validación del tráfico encriptado.

El uso de esta metodología se enfocará exclusivamente en el diseño de la solución, aplicando únicamente las tres primeras fases de la siguiente manera:

- **Fase de Preparación** donde se estudia la topología actual de la universidad, el esquema de direccionamiento IP existente y los requerimientos de acceso seguro hacia los servicios críticos
- **Fase de Planificación** en la cual se define la estructura arquitectónica de la red, la selección de protocolos de encriptación y el ecosistema de software firewall necesario.
- **Fase de Diseño** utiliza herramientas de virtualización de red para proyectar el comportamiento de los equipos, validar la negociación criptográfica y certificar el rendimiento de la propuesta en un entorno controlado.

Las fases de implementación en hardware y monitoreo operativo no forman parte de la investigación porque el alcance del estudio es únicamente proponer una solución técnica, sin ejecutar intervenciones en la infraestructura física de la universidad. Estos procesos se podrán realizar más adelante por parte de la institución si decide adoptar la propuesta; no se descartan, pero no son parte del alcance académico del presente documento.

3.1.3. Tipo de Investigación

La investigación es de tipo aplicada, debido a que se orienta a la propuesta de una solución tecnológica destinada a fortalecer la interconexión segura entre los campus universitarios de la Universidad Politécnica Estatal del Carchi. Como señala Bernal (2022), la investigación aplicada tiene como propósito "utilizar los conocimientos teóricos para resolver problemas prácticos que mejoren la calidad de vida o el entorno". Esto se refleja en la propuesta final, entregando a la institución un diseño estructural validado y listo para su consideración.

3.1.3.1. Investigación descriptiva

Posee un alcance descriptivo, ya que permite analizar las características, funcionamiento de distintas tecnologías VPN para la interconexión de redes institucionales.

3.1.3.2. Investigación experimental

Presenta el estudio también un componente experimental, debido a que la arquitectura propuesta será validada mediante entornos de emulación y pruebas controladas de conectividad, rendimiento y seguridad de red.

3.1.3.3. Investigación documental

El trabajo adopta una estrategia documental que se apoya en artículos científicos, tesis, cuerpos normativos y manuales técnicos centrados en redes privadas virtuales y seguridad informática.

3.2. IDEA A DEFENDER

La utilización de tecnologías VPN para la interconexión de los campus de la Universidad Politécnica Estatal del Carchi contribuirá al fortalecimiento de la seguridad, la disponibilidad y la eficiencia de la comunicación institucional, optimizando la gestión de los recursos tecnológicos y mejorando las condiciones de acceso a los servicios digitales para la comunidad universitaria.

3.3. DEFINICIÓN Y OPERACIONALIZACIÓN DE LAS VARIABLES

En este apartado se desagregan las variables de estudio, definidas con criterio técnico y en correspondencia directa con los objetivos específicos que orientan el diseño de la red VPN institución. Transformar nociones abstractas en componentes operables y mensurables a partir de pruebas de emulación constituye el núcleo del procedimiento.

3.3.1. Variable Dependiente

Pone el foco en el desempeño y la integridad del tráfico de datos una vez desplegada la arquitectura. Interesa comprobar si la infraestructura resultante es capaz de sostener un intercambio de información estable y resguardado.

Tabla 2. Variable Dependiente.

Variable	Definición	Dimensión	Indicador	Técnica	Instrumento
Interconectividad segura de campus universitarios	Capacidad de comunicación segura y estable entre redes institucionales mediante mecanismos de protección y disponibilidad.	Rendimiento, conectividad, disponibilidad	Latencia, throughput, pérdida de paquetes	Emulación de red. Pruebas de conectividad Monitoreo de tráfico de red Análisis de rendimiento de red	GNS3 Wireshark iPerf3 Ping

3.3.2. Variable Independiente

Esta variable comprende los elementos técnicos, protocolos y configuraciones de red que integran la propuesta de diseño para la institución. Su operacionalización permite estandarizar los parámetros de seguridad que serán aplicados sobre los dispositivos virtuales.

Tabla 3. Variable Independiente.

Variable	Definición	Dimensión	Indicador	Técnica	Instrumento
Arquitectura basada en tecnologías VPN	Conjunto de tecnologías y mecanismos utilizados para establecer conexiones seguras entre redes mediante túneles cifrados.	Protocolos VPN, cifrado, autenticación	Estabilidad del túnel, nivel de cifrado	Emulación de red Pruebas de conectividad Monitoreo de tráfico	GNS3 Wireshark iPerf3

3.4. MÉTODOS UTILIZADOS

Método analítico

Este método se aplicó al examen de las características técnicas y funcionales de las tecnologías VPN consideradas como alternativas de interconexión para los campus de la UPEC. Mediante su empleo resultó posible identificar los componentes, protocolos de tunelización y mecanismos de cifrado pertinentes para el diseño de la arquitectura propuesta; de ese análisis se derivó una base conceptual que orientó las decisiones técnicas posteriores.

Método comparativo

Con este método se evaluaron distintas tecnologías VPN atendiendo a criterios de seguridad, rendimiento, escalabilidad y viabilidad de implementación en entornos universitarios con infraestructura distribuida. Su aplicación facilitó identificar la alternativa técnicamente más adecuada para las condiciones particulares de la institución, sustentando así la selección tecnológica con evidencia analítica antes de proceder al diseño de la arquitectura.

Método experimental

Constituye el eje central del proceso de validación técnica: mediante el despliegue de una topología virtualizada se ejecutaron pruebas controladas orientadas a medir el comportamiento de la arquitectura VPN propuesta bajo condiciones de carga emulada. Latencia, jitter, porcentaje de pérdida de paquetes y estabilidad del

enlace cifrado fueron las variables evaluadas, cuyos resultados se procesarán mediante análisis estadístico descriptivo y se representarán a través de gráficos comparativos. Este enfoque hizo posible obtener evidencia cuantitativa del impacto del procesamiento criptográfico sobre el rendimiento de la red, sin intervenir sobre la infraestructura operativa de la institución.

Método documental

En la revisión sistemática de artículos científicos, tesis de grado, normativas vigentes y documentación técnica relacionada con redes privadas virtuales, seguridad de redes institucionales e interconectividad de campus universitarios se empleó el método documental. De dicha revisión se obtuvo el sustento teórico y referencial requerido para contextualizar la investigación y fundamentar las decisiones metodológicas adoptadas a lo largo del estudio.

3.4.1. Datos y variables de evaluación

Los datos obtenidos durante el proceso de validación se clasificarán en dos categorías. La primera corresponde a datos técnicos de rendimiento —integrados por valores numéricos de latencia, jitter y pérdida de paquetes, recolectados mediante inyección de tráfico controlado sobre la topología virtual—. Datos lógicos de infraestructura conforman la segunda categoría, referida al esquema de direccionamiento IP, la topología de red de las sedes institucionales y la verificación del encapsulamiento de paquetes en los túneles establecidos; en conjunto, ambas categorías posibilitan una lectura complementaria del desempeño técnico y de la coherencia lógica de la arquitectura desplegada.

3.4.2. Procedimiento metodológico

El desarrollo de la investigación se estructuró en tres fases secuenciales:

La primera fase correspondió a Preparar, en la cual se realizó el levantamiento de información sobre la infraestructura tecnológica institucional, identificando la estructura de red existente, los segmentos de direccionamiento utilizados en las diferentes sedes y los servicios críticos que requieren mecanismos de comunicación segura y disponibilidad permanente. Esta fase permitió establecer los requerimientos funcionales y técnicos necesarios para el desarrollo de la propuesta.

La segunda fase correspondió a Planear, donde se analizaron las alternativas de interconexión disponibles para entornos multisede, considerando criterios

relacionados con seguridad, escalabilidad, facilidad de administración y compatibilidad con la infraestructura institucional. A partir de este análisis se determinarán los elementos necesarios para la construcción de la propuesta tecnológica y se establecerán los criterios de evaluación que serán utilizados posteriormente.

La tercera fase correspondió a Diseñar, en la cual se desarrolló la arquitectura de red propuesta a partir de los requerimientos identificados y los criterios definidos en la fase anterior. Asimismo, se elaboró el entorno de validación que permitirá verificar el comportamiento de la solución mediante pruebas de conectividad, rendimiento y seguridad, cuyos resultados servirán para determinar el cumplimiento de los objetivos establecidos en la investigación.

3.5. ANÁLISIS ESTADÍSTICO

Dado el enfoque metodológico de la presente investigación, el tratamiento de los datos se realizó mediante estadística descriptiva básica orientada a caracterizar el comportamiento de las métricas de red obtenidas durante las pruebas experimentales. Este tipo de análisis resulta adecuado para estudios de prueba de concepto en entornos emulados, donde el objetivo no es generalizar resultados a una población, sino describir y comparar el comportamiento técnico de una arquitectura bajo condiciones controladas.

Para las métricas cuantitativas obtenidas mediante iPerf3 e ICMP latencia, jitter, throughput y pérdida de paquetes se emplearon los siguientes recursos estadísticos: valor registrado por prueba, comparación entre escenarios con y sin túnel VPN, y cálculo del margen de seguridad respecto a los umbrales normativos establecidos por la recomendación ITU-T G.114. Mediante tablas comparativas se representaron los resultados, lo que permite visualizar el impacto del procesamiento criptográfico sobre cada indicador evaluado.

Para el instrumento cualitativo, se aplicó una entrevista estructurada dirigida al responsable del Departamento de Redes y Telecomunicaciones de la UPEC, quien constituyó el informante clave del estudio, al tratarse del funcionario con conocimiento directo y autoridad técnica sobre la infraestructura de red institucional, su testimonio aportó los parámetros reales de configuración esquemas de direccionamiento, servicios críticos, equipamiento existente y requerimientos de

interconexión que sirvieron de base para el diseño de la arquitectura propuesta. cuantitativo obtenido a través de las pruebas de rendimiento.

IV. RESULTADOS Y DISCUSIÓN

4.1. RESULTADOS

Este capítulo expone los hallazgos técnicos obtenidos a lo largo de las fases de la metodología PPDIOO: se presenta el diagnóstico estructural de la red actual, continúa con la validación de la topología lógica propuesta mediante emulación en GNS3 y concluye con la discusión técnica del impacto de la solución sobre la infraestructura de la universidad.

En función de la evolución del perímetro de red de la UPEC se estructuran los resultados, transitando desde el levantamiento de información inicial hasta la recolección de métricas de rendimiento en el entorno emulado; de este recorrido se desprende una progresión coherente entre el estado inicial de la red y el desempeño verificado de la arquitectura propuesta.

4.1.1. Diagnóstico y Levantamiento de la Infraestructura Actual

A partir de la entrevista técnica estructurada realizada al departamento de TIC y la revisión de la situación perimetral, se consolidó el levantamiento de información de la Sede Matriz Tulcán y los campus remotos. Este diagnóstico establece la línea base sobre la cual opera actualmente la red universitaria. La Tabla 4 expone el inventario técnico actual recolectado durante la fase de planificación.

Tabla 4. Inventario técnico actual.

Componente Técnico	Estado Actual: Sede Matriz (Tulcán)	Estado Actual: Campus Remotos
Equipamiento de Borde	Fortigate 1100E.	Conexión hacia la red pública sin estandarización de pasarelas VPN corporativas.
Enlaces WAN	Enlaces de fibra óptica de 1 Gbps bajo un esquema de redundancia Dual ISP.	Conexión estándar a Internet para salida de tráfico.
Alojamiento de Servicios	Centralización total de servidores	No alojan servidores críticos. Consumen servicios de la matriz.
Planimetría y Topología	Cuenta con diagrama físico y documentación de equipos de borde.	Carecen de diagramas lógicos o físicos documentados en el departamento de redes.

Se determinó que la Universidad Politécnica Estatal del Carchi dispone de una infraestructura de seguridad perimetral centralizada en el campus principal, compuesta por un firewall Fortigate 1100E configurado con dos enlaces redundantes y una dirección IP pública virtual. Este equipo actúa como punto de control para la protección de los servicios institucionales y para la gestión de las conexiones VPN actualmente implementadas.

Asimismo, se identificó que la institución ya emplea redes privadas virtuales para casos específicos, tales como la interconexión con la infraestructura Cloud Oracle que aloja parte del portafolio institucional y el acceso remoto del personal de TIC hacia los servidores internos. Sin embargo, no existe una solución VPN que permita integrar de manera permanente y transparente los diferentes campus universitarios bajo un mismo esquema de comunicación segura.

El esquema de hardware perimetral actual de la sede central, levantado durante esta fase, se detalla en la Figura 20:

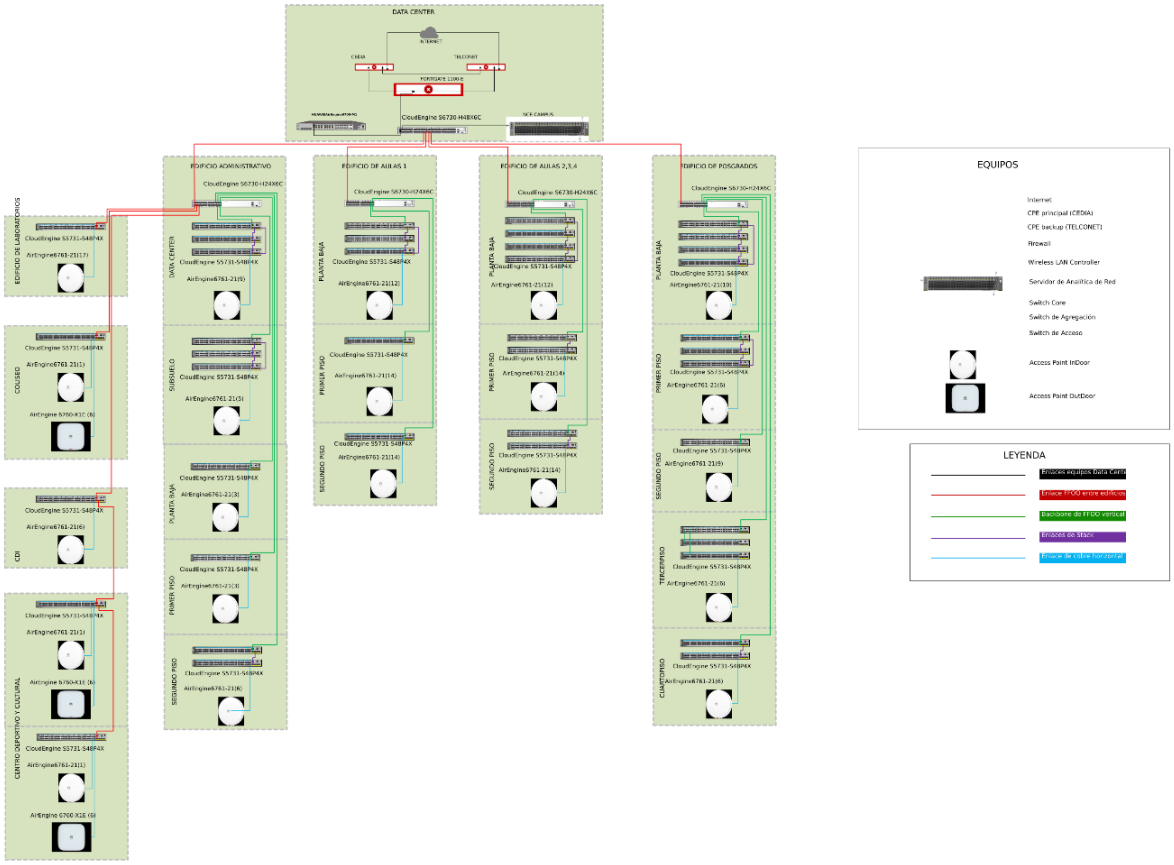

Figura 20. Topología física actual de la infraestructura perimetral en la Sede Matriz Tulcán.

4.1.1.1. Requerimientos de interconectividad entre campus

El levantamiento de requerimientos evidenció la necesidad de implementar una arquitectura de interconexión total entre los diferentes campus de la universidad, permitiendo que las sedes remotas accedan a los mismos servicios disponibles en el campus principal. De acuerdo con la Dirección TIC, la solución propuesta debe garantizar el intercambio seguro de información institucional y posibilitar el acceso transparente a los recursos tecnológicos estratégicos de la institución.

Se estableció, además, que cada campus mantiene esquemas de direccionamiento diferenciados para evitar conflictos entre segmentos de red condición que deberá considerarse dentro del diseño de la arquitectura VPN propuesta; la solución debe contemplar, en la misma línea, la escalabilidad necesaria para incorporar futuras sedes universitarias sin afectar la estructura lógica previamente definida.

4.1.1.2. Servicios institucionales críticos

Dentro de la Tabla 5 se identificaron, como resultado del levantamiento realizado, los servicios institucionales cuya disponibilidad y accesibilidad resultan prioritarias dentro del proceso de interconexión entre campus. Constituyen estos servicios elementos necesarios para la operación académica y administrativa de la universidad, de modo que la solución VPN propuesta deberá garantizar su acceso seguro y continuo desde las sedes interconectadas; en conjunto, definen el conjunto mínimo de disponibilidad que la arquitectura debe sostener una vez desplegada.

Tabla 5. Servicios institucionales prioritarios.

Servicio	Función
Cloud Oracle	Aloja el portafolio institucional y el sistema integrado universitario
Telefonía IP	Comunicación institucional entre dependencias
CCTV	Monitoreo y vigilancia de las instalaciones
Acceso administrativo	Gestión de recursos internos autorizados

4.1.1.3 Esquema de direccionamiento institucional

La Dirección TIC indicó que cada campus universitario utiliza un segmento de direccionamiento independiente basado en el espacio privado 172.0.0.0/16, con el propósito de evitar conflictos de direccionamiento y facilitar la administración de la red institucional. Este esquema constituye una referencia importante para el diseño de la solución propuesta, ya que permite establecer rutas específicas hacia cada sede interconectada.

Tabla 6. Segmentación IP institucional.

Sede	Interfaz LAN
Sede Matriz Tulcán	172.20.0.0/16
Campus Cayambe	172.21.0.0/16
Campus Huaca	172.22.0.0/16
Campus Santa Martha de Cuba	172.23.0.0/16
Futuras sedes	Incremento progresivo del segundo octeto

4.1.2. Análisis Multicriterio de Selección Tecnológica

Con el propósito de definir los componentes técnicos más adecuados para la arquitectura VPN propuesta, se realizó una evaluación comparativa de diferentes alternativas empleadas en entornos institucionales. Este proceso permitió seleccionar la topología de interconexión, el protocolo de comunicación segura, el mecanismo de tunelización que mejor se ajustaron a los requerimientos identificados durante la fase de diagnóstico.

4.1.2.1. Evaluación y Selección de la Topología VPN

La determinación de la estructura de interconexión entre la sede matriz y los campus dispersos geográficamente requirió contrastar los dos modelos principales de redes privadas virtuales aplicados a nivel corporativo.

Tabla 7. Comparación de topología VPN utilizados en redes institucionales.

Criterio de Evaluación	Topología Estrella (Hub-and-Spoke)	Topología de Malla Completa (Full Mesh)
Complejidad de Configuración	**Baja-Moderada:** Requiere únicamente el despliegue de N−1 túneles concurrentes centralizados en el nodo raíz.	**Elevada:** Exige la configuración manual de N(N−1) enlaces, complejizando la administración perimetral.
Consumo de Recursos (CPU/RAM)	**Eficiente:** El esfuerzo de procesamiento criptográfico se distribuye equitativamente en los extremos y se concentra en el Hub de forma controlada.	**Excesivo:** Cada nodo periférico debe mantener asociaciones de seguridad activas y simultáneas con todas las sedes.
Escalabilidad de Infraestructura	**Excelente:** La integración de un nuevo campus remoto solo requiere el aprovisionamiento de un túnel apuntando hacia el nodo central.	**Deficiente:** Añadir una nueva sucursal obliga a modificar las tablas de rutas y políticas de todos los firewalls preexistentes.
Idoneidad para Flujos Centralizados	**Óptima:** Diseñada específicamente para redes donde los centros de datos y servicios compartidos residen en un único punto focal.	**Innecesaria:** Diseñada para entornos descentralizados donde las sucursales intercambian datos masivos entre sí de forma directa.

Tras evaluar las métricas de la Tabla 7, se seleccionó la topología de tipo Estrella, definiendo al Campus Matriz Tulcán como el nodo central y a las sedes como los nodos remotos. Esta decisión se fundamenta en el diagnóstico de la infraestructura telemática de la UPEC obtenido en la fase de investigación, donde se constató que

el 100% de los servicios internos críticos se encuentran físicamente centralizados en el Data Center de la matriz. Implementar un modelo de malla completa habría provocado un desperdicio crítico de procesamiento y memoria RAM en los firewalls perimetrales de las sedes remotas, debido al overhead implicado en sostener túneles permanentes e inactivos hacia sedes con las que no existe comunicación real.

4.1.2.2. Evaluación y selección de protocolo criptográfico

Para salvaguardar la confidencialidad e integridad de la información en tránsito a través del enlace público de Internet, en la Tabla 8 se examinaron los tres protocolos de tunelización más estables.

Tabla 8. Análisis comparativo de protocolos VPN.

Criterio Técnico	Protocolo IPsec	Protocolo OpenVPN	Protocolo WireGuard
Capa de Operación	**Capa 3 (Red):** Opera de manera nativa en el kernel del sistema operativo, procesando directamente paquetes IP.	**Capa 4 (Transporte):** Se ejecuta en el espacio de usuario, encapsulando tráfico sobre TCP o UDP.	**Capa 3 (Red):** Implementado en el kernel, basado en el principio de enrutamiento criptográfico
Rendimiento Útil	**Alto:** Minimiza el retardo al evitar el intercambio de contextos de memoria y beneficiarse de la aceleración física por hardware.	**Moderado:** Sufre penalizaciones de velocidad bajo cargas de tráfico masivo debido a las colas en el espacio de usuario.	**Muy Alto:** Arquitectura de código extremadamente ligera optimizada para un procesamiento de alta velocidad.
Interoperabilidad Heterogénea	**Excelente:** Es un estándar abierto universal estandarizado por el IETF (RFC 4301), soportado por todos los fabricantes globales.	**Limitada:** Requiere la instalación de clientes o daemons específicos en plataformas de hardware propietario de red.	**Moderada:** Al ser una tecnología reciente, su integración nativa en plataformas *legacy* de gama corporativa es limitada.
Consumo de Canal	**Bajo-Moderado:** Añade una cabecera fija controlable mediante parámetros de segmentación lógica de paquetes.	**Elevado:** La sobrecarga introducida por el cifrado TLS/SSL expande significativamente el tamaño de la carga útil.	**Mínimo:** Cabecera altamente compacta que reduce al mínimo el consumo adicional de ancho de banda.

El análisis comparativo determinó la adopción del estándar universal IPsec operando en Modo Túnel. El factor determinante para esta selección radica en el cumplimiento del principio de interoperabilidad en entornos heterogéneos: el nodo principal de la universidad cuenta con una infraestructura perimetral consistente, basada en un equipo comercial de alta gama Fortigate 1100E. Al tratarse IPsec de un estándar abierto de la industria, faculta un acoplamiento transparente, seguro y nativo con plataformas de software libre, lo que garantiza la viabilidad de una futura integración con la infraestructura perimetral institucional basada en Fortigate; su ejecución

directa en la capa de red del kernel aprovecha de forma óptima la aceleración criptográfica de hardware, asegurando que el tráfico síncrono no experimente retrasos perjudiciales.

4.1.2.3. Evaluación y Selección del Modo de Tunelización

Dentro de la Tabla 9 se analizó el mecanismo de ruteo del tráfico perimetral para normar como se comportarán las peticiones de datos de los usuarios de las sedes remotas.

Tabla 9. Comparación de modos de tunelización VPN.

Aspecto Operativo	Túnel Completo	Túnel Dividido
Destino del Tráfico	Todo el tráfico, incluyendo navegación web, pasa por la sede central.	Solo el tráfico institucional entra al túnel; internet sale directamente desde cada sede.
Impacto en el Ancho de Banda Hub	**Ineficiente:** la sede central procesa también el tráfico web de las sedes remotas.	**Óptimo:** el canal central se reserva para servicios y datos institucionales.
Seguridad de los Endpoints	**Máxima:** todas las sedes quedan bajo las políticas del firewall principal.	**Descentralizada:** cada sede debe gestionar su propia seguridad de salida a internet.
Rendimiento de Servicios Síncronos	**Deficiente:** Introduce latencia adicional por el efecto de "trompeta" al triangular el tráfico web ordinario.	**Excelente:** Las llamadas de VoIP y flujos de CCTV intercampus viajan por rutas dedicadas sin competir con la navegación web común.

Para los requerimientos operativos de la UPEC, se definió la implementación de un Túnel Dividido implementado mediante enrutamiento estático de subredes corporativas. Esta configuración faculta el aislamiento y blindaje de las comunicaciones destinadas específicamente hacia las subredes de la universidad, delegando que las consultas ordinarias a Internet público solicitadas por docentes y estudiantes se resuelvan localmente por el ISP de cada sede.

4.1.2.4 Plataformas de Gestión Perimetral de Código Abierto

Para la implementación de la arquitectura propuesta se evaluaron tres plataformas de gestión perimetral de código abierto con soporte nativo para IPsec. El análisis consideró criterios técnicos, operativos y de viabilidad institucional, cuyos resultados se presentan en la Tabla 10.

Tabla 10. Comparación de plataformas de software libre para gestión perimetral VPN.

Criterio	pfSense	OPNsense	VyOS
Base del Sistema	FreeBSD	FreeBSD	Debian Linux
Interfaz de Gestión	Web (GUI completa)	Web (GUI moderna)	Línea de comandos
Soporte Ipsec/IKEVv2	Nativo, estable	Nativo, estable	Nativo, mediante CLI
Documentación	Extensa y consolidada	Buena, en crecimiento	Técnica, orientada a expertos
Comunidad de Soporte	Muy amplia	Moderada	Reducida
Interoperabilidad	Alta (Estándares RFC)	Alta (Estándares RFC)	Alta (Estándares RFC)
Perfil de uso	Institucional y empresarial	Institucional y empresarial	Operadoras y redes avanzadas

La selección de pfSense como plataforma de terminación VPN se sustenta en tres criterios. Su soporte nativo de IPsec con IKEv2 está, en primer lugar, ampliamente documentado y validado en entornos institucionales, lo que reduce la curva de aprendizaje para el equipo de TI de la UPEC. Facilita, en segundo término, su interfaz de administración web centralizada la gestión de las asociaciones de seguridad, las reglas de filtrado y el monitoreo del estado de los túneles sin requerir conocimiento avanzado de línea de comandos a diferencia de VyOS. La amplitud de su comunidad de soporte y la disponibilidad de documentación técnica consolidada representan, por último, una ventaja operativa concreta para una institución pública que debe mantener y escalar su infraestructura de forma autónoma. Si bien OPNsense comparte características técnicas similares, pfSense cuenta con mayor trayectoria de implementación en entornos universitarios; esto lo posiciona como la alternativa más adecuada para las condiciones particulares de la universidad dentro del alcance de esta investigación.

4.1.3. Diseño y Emulación de la Topología Lógica Propuesta

Para solventar la vulnerabilidad del tráfico inter-sedes y la falta de planimetría lógica descubierta en el diagnóstico, se diseñó una arquitectura de red privada virtual basada en el modelo Estrella. El Campus Matriz Tulcán asume, en este diseño estratégico, el rol de nodo central (Hub), encargado de concentrar y enrutar las peticiones seguras hacia los servicios críticos centralizados.

4.1.3.1. Emulación de la Arquitectura en GNS3

Con el propósito de validar experimentalmente la propuesta desarrollada, se implementó la arquitectura de red en el entorno de emulación GNS3. Reprodujo el escenario construido la estructura de interconexión institucional mediante una topología Hub-and-Spoke, donde el Campus Matriz Tulcán asumió el rol de nodo

central encargado de concentrar y distribuir el tráfico proveniente de las diferentes sedes remotas.

Para representar los dispositivos de seguridad perimetral utilizados por la institución, se desplegaron múltiples instancias virtuales del sistema operativo pfSense. Un firewall central asociado al Campus Tulcán y cuatro firewalls adicionales correspondientes a las sedes Cayambe, Huaca, Santa Marta de Cuba y una sede adicional destinada a evaluar la escalabilidad de la propuesta conformaron la infraestructura emulada. Se incorporaron, asimismo, switches virtuales para la segmentación de las redes LAN, un servidor institucional que representa los servicios centralizados y una nube NAT encargada de emular el tránsito del tráfico a través de Internet; en conjunto, este montaje reprodujo con fidelidad razonable las condiciones topológicas de la red institucional real.

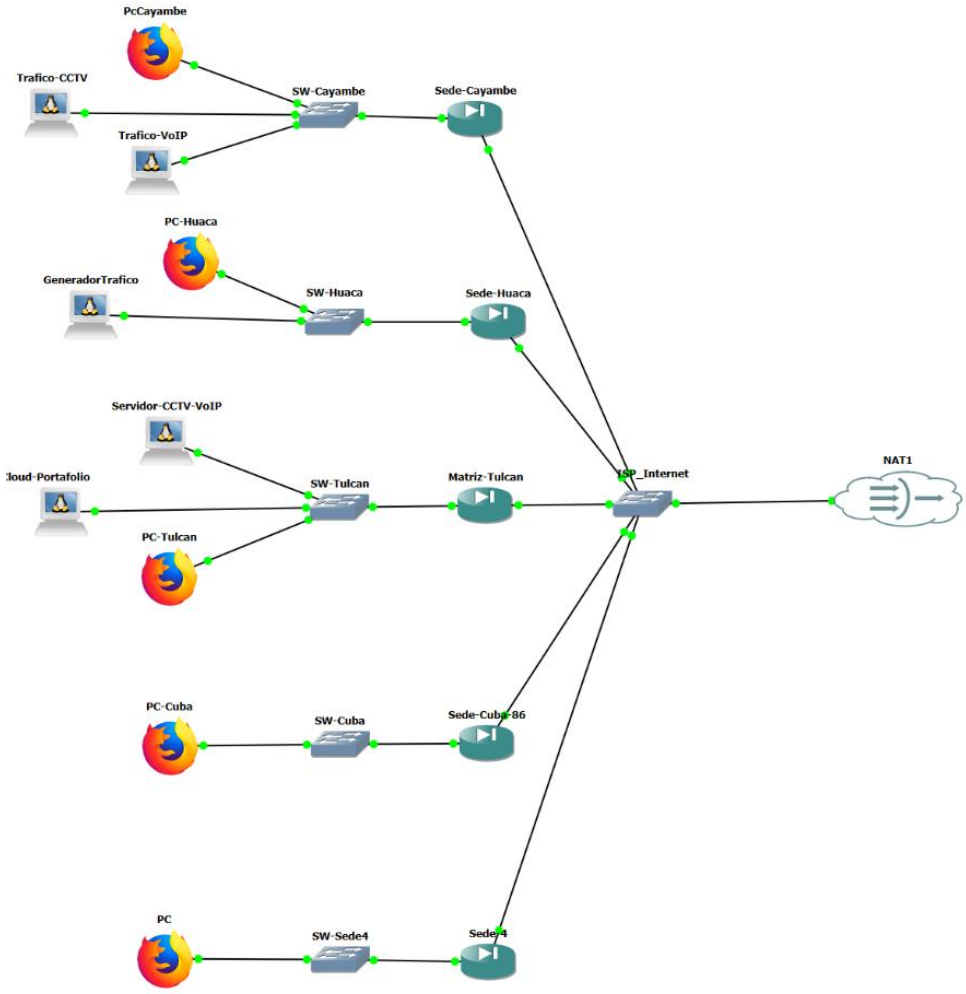

Figura 21. Topología física propuesta y emulada en la plataforma GNS3.

4.1.3.2. Topología lógica propuesta

Desde una perspectiva lógica, la arquitectura propuesta adopta un modelo Hub-and-Spoke basado en túneles VPN Site-to-Site. Opera en este esquema el Campus Matriz Tulcán como concentrador principal, estableciendo asociaciones seguras independientes con cada uno de los campus remotos; esta disposición facilita la administración centralizada de los recursos institucionales, reduce la complejidad operativa y favorece la incorporación de nuevas sedes sin alterar significativamente la estructura existente.

Esquemas de direccionamiento diferenciados mantienen las redes involucradas, lo que permite el intercambio seguro de información entre campus y el acceso a los servicios institucionales centralizados condición que sostiene, en conjunto, la coherencia lógica de la segmentación adoptada por la arquitectura propuesta.

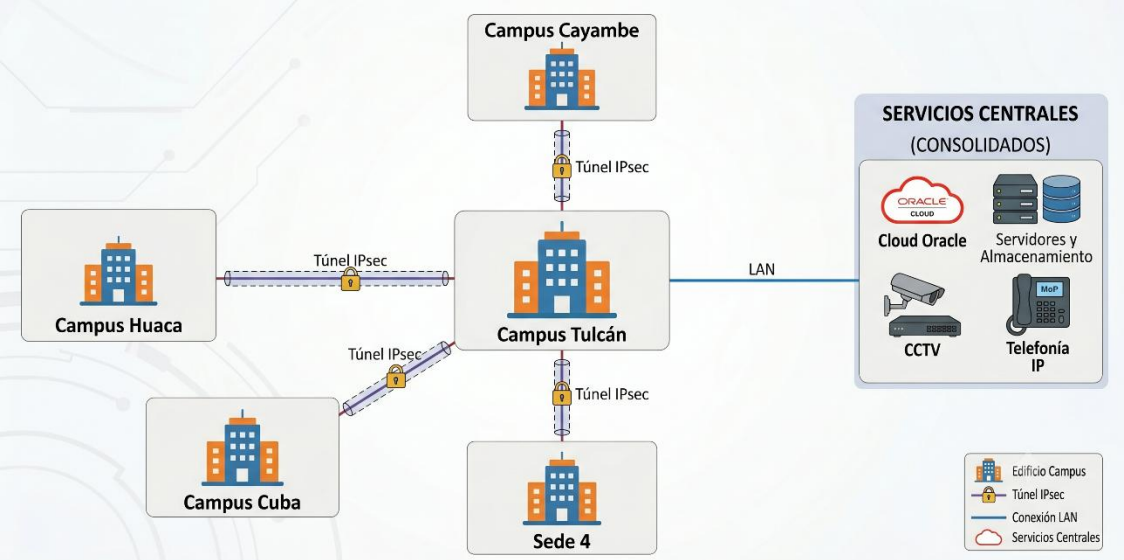

Figura 22. Topología lógica de la arquitectura VPN propuesta.

4.1.3.3. Funcionamiento técnico de la arquitectura VPN propuesta

El funcionamiento inicia cuando un usuario perteneciente a una de las sedes remotas genera tráfico destinado a un recurso alojado en la red institucional del Campus Tulcán. El firewall pfSense identifica que la dirección de destino corresponde a una red protegida por las políticas definidas para el túnel Ipsec, caso contrario envía el tráfico hacia el internet público.

Posteriormente, si las asociaciones de seguridad no se encuentran activas, se ejecuta el proceso de negociación IKEv2, mediante el cual ambos extremos autentican su identidad e intercambian los parámetros criptográficos previamente establecidos.

Una vez completada esta etapa, el tráfico original es encapsulado utilizando el protocolo ESP, aplicando cifrado AES-256 para garantizar la confidencialidad de la información y mecanismos de integridad basados en SHA-256 para detectar posibles modificaciones durante el tránsito.

Los paquetes cifrados son transmitidos a través del enlace WAN simulado que representa Internet y son recibidos por el firewall del extremo opuesto, donde se verifica su autenticidad, se descifran y finalmente son reenviados hacia la red LAN correspondiente. Este proceso permite que los usuarios accedan a los servicios institucionales como si pertenecieran a una misma infraestructura lógica, manteniendo protegida la información intercambiada entre sedes.

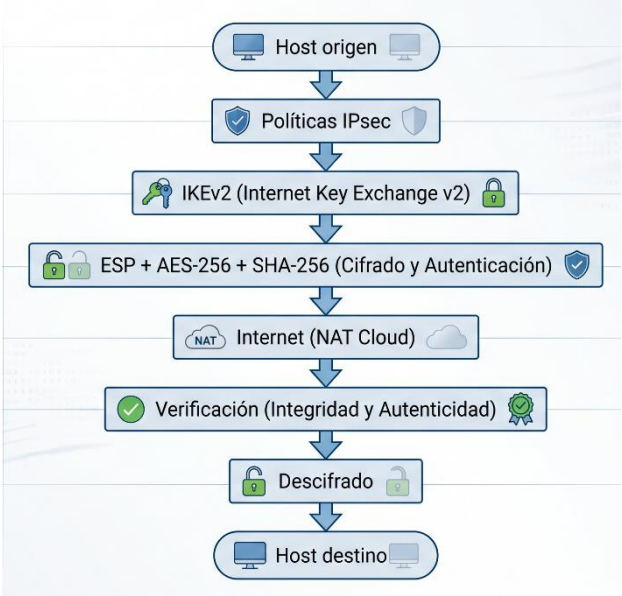

Figura 23. Flujo técnico del funcionamiento del túnel IPsec Site-to-Site.

4.1.3.4. Configuración del Túnel IPsec Site-to-Site

Una vez definida la arquitectura de interconexión y comprendido el funcionamiento técnico del protocolo IPsec, se procedió a la configuración de los túneles VPN Site-to-Site en cada uno de los dispositivos perimetrales pfSense. La implementación se realizó de manera homogénea en todos los nodos de la topología, considerando las dos etapas que conforman el establecimiento de asociaciones de seguridad bajo IPsec: la Fase 1, orientada a la negociación y autenticación de los extremos, y la Fase 2, encargada de proteger el tráfico de datos intercambiado entre las redes institucionales.

Fase 1 (IKEv2)

La Fase 1 tuvo como finalidad autenticar los dispositivos perimetrales participantes y establecer un canal seguro para la negociación de los parámetros criptográficos empleados durante la comunicación.

Tabla 11. Configuración fase 1 túnel IPsec.

Componente	Parámetro	Valor	Justificación
Fase 1 (IKEv2)	Método de autenticación	**Clave precompartida (PSK)**	Permite autenticar los dispositivos perimetrales de manera sencilla y eficiente dentro del entorno de emulación.
Fase 1 (IKEv2)	Protocolo de Intercambio	**IKEv2**	Mejora la estabilidad ante interrupciones WAN, soporta NAT-Trasversal y reduce los tiempos de reconexión del túnel.
Fase 1 (IKEv2)	Algoritmo de Cifrado	**AES-256**	Proporciona un elevado nivel de confidencialidad para proteger el canal de negociación entre los extremos.
Fase 1 (IKEv2)	Función de Hash	**SHA-256**	Garantiza la integridad de la negociación inicial y ofrece alta resistencia frente a ataques de colisión.
Fase 1 (IKEv2)	Grupo Diffie-Hellman	**Grupo 14** (2048 bits)	Permite el intercambio seguro de claves y mantiene un equilibrio adecuado entre seguridad y rendimiento computacional.

Fase 2 (ESP)

Posteriormente, la Fase 2 definió los mecanismos responsables de proteger el tráfico de datos intercambiado entre las redes institucionales, especificando los algoritmos de cifrado y las condiciones necesarias para garantizar la confidencialidad e integridad de la información transmitida.

Tabla 12. Configuración fase 2 túnel IPsec.

Componente	Parámetro	Valor	Justificación
Fase 2 (ESP)	Modo de operación	Tunnel	Permite encapsular completamente el paquete IP original, característica necesaria en conexiones Site-to-Site.
Fase 2 (ESP)	Protocolo de seguridad	ESP	Proporciona mecanismos de confidencialidad e integridad para el tráfico de datos intercambiado entre sedes.
Fase 2 (ESP)	Algoritmo de cifrado	AES-256	Garantiza la protección del contenido transmitido a través del túnel VPN.
Fase 2 (ESP)	Método de autenticación	SHA-256	Permite verificar la integridad y autenticidad del tráfico encapsulado.
Fase 2 (ESP)	Red remota	172.21.0.0/16	Define el segmento institucional accesible a través del túnel establecido.

Los mecanismos criptográficos implementados dentro de la arquitectura IPsec actúan de forma complementaria durante el establecimiento y operación del túnel VPN. Durante la negociación inicial mediante IKEv2, el algoritmo Diffie-Hellman Grupo 14 permite que los extremos generen material criptográfico compartido sin transmitir directamente las claves a través de la red pública. Este proceso se fundamenta matemáticamente en operaciones de exponenciación modular sobre números primos de gran tamaño, cuya complejidad computacional dificulta la obtención de las claves privadas por parte de terceros. Una vez establecidas las asociaciones de seguridad, AES-256 se utiliza para proporcionar confidencialidad a la información mediante un proceso de cifrado simétrico basado en múltiples rondas de sustitución, permutación y transformaciones algebraicas aplicadas sobre bloques de datos. De manera complementaria, la integridad de la comunicación queda resguardada por SHA-256, que genera resúmenes criptográficos de 256 bits a partir de operaciones hash; cualquier alteración de la información transmitida se vuelve detectable con este mecanismo. Integrados dentro del protocolo ESP, ambos resguardos protegen el tráfico institucional frente a accesos no autorizados, modificaciones o intentos de interceptación durante su tránsito por la red pública.

El panel de monitoreo del firewall central pfSense, mostrado en la Figura 24, confirmó la convergencia exitosa de la arquitectura segura propuesta. El estado operativo "Established" puso de manifiesto que las negociaciones correspondientes a IKEv2 y las asociaciones de seguridad ESP se completaron correctamente entre la sede matriz y los campus remotos, validando así la configuración apropiada de los túneles Site-to-Site dentro del entorno de emulación.

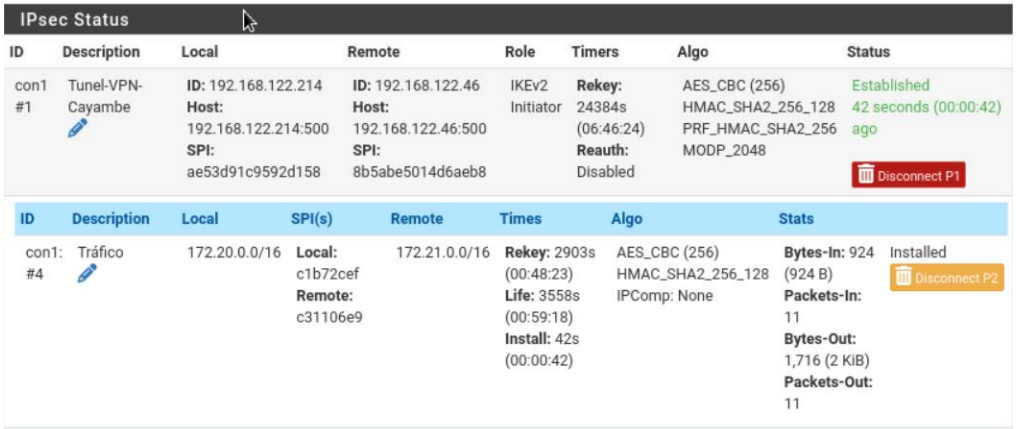

Figura 24. Estado operativo del túnel IPsec en pfSense.

4.1.3.5. Políticas de Cortafuegos y Acceso a Servicios Críticos

La operatividad de un túnel IPsec no solo depende de su fase criptográfica, sino de las políticas de control de acceso dictadas por el cortafuegos perimetral. Basándose en los requerimientos institucionales recolectados mediante las entrevistas al departamento de TI de la UPEC, se identificaron tres flujos de tráfico críticos que debían ser garantizados a través de las sedes: el acceso a los sistemas alojados en Cloud Oracle, el tránsito de Telefonía IP y la transmisión del sistema de videovigilancia.

Para dar cumplimiento a estos requerimientos, se procedió a configurar las reglas de filtrado en la interfaz lógica IPsec de los equipos pfSense. Como se ilustra en la Figura 25, se definieron reglas de cortafuegos que permiten explícitamente el tránsito bidireccional de los protocolos requeridos entre los segmentos LAN de la matriz y las sucursales.

Debido a que la presente investigación se desarrolló en un entorno experimental orientado a validar la conectividad, seguridad y rendimiento de la arquitectura propuesta, las reglas de filtrado fueron configuradas de manera permisiva para evitar que restricciones adicionales afectaran los resultados obtenidos durante las pruebas. Esta decisión permitió evaluar de forma objetiva el comportamiento del túnel VPN Site-to-Site y garantizar la comunicación entre las redes participantes.

Una vez que el tráfico ha sido desencapsulado y validado por la Fase 2 del túnel, el cortafuegos interno autoriza las peticiones hacia los servidores específicos; así, un usuario en el Campus Huaca o Cayambe puede consumir los recursos centralizados de la matriz Tulcán o acceder a los aplicativos en la nube sin interrupciones, manteniendo las normativas de seguridad perimetral de la institución. En una implementación en producción, estas medidas deberían complementarse con políticas de acceso más restrictivas basadas en el principio de mínimo privilegio, de modo que cada sede únicamente alcance los servicios estrictamente necesarios. La configuración descrita resuelve la conectividad, pero acotar los permisos reduce la superficie de exposición ante movimientos laterales no deseados dentro de la red institucional.

Figura 25. Reglas de filtrado aplicadas sobre la interfaz IPsec.

4.1.4. Validación experimental de conectividad y rendimiento

Una vez implementado y configurado el túnel VPN IPsec Site-to-Site, se ejecutaron pruebas experimentales para examinar el comportamiento de la arquitectura propuesta en escenarios con y sin encapsulación criptográfica; posibilitaron herramientas como Ping, iPerf3 y Wireshark la evaluación de latencia, jitter, throughput, pérdida de paquetes y el perfil del tráfico en tránsito.

4.1.4.1. Validación del comportamiento del tráfico cifrado

Desplegar una red privada virtual en la Universidad Politécnica Estatal del Carchi se justifica, ante todo, por la exigencia de resguardar la confidencialidad e integridad de la información institucional cuando esta atraviesa redes públicas. Constituye un cifrado correctamente negociado y aplicado al canal, por tanto, la condición mínima para que la arquitectura satisfaga el propósito que motivó su diseño sobre esta base se sustenta la evaluación experimental descrita a continuación. Para evidenciar el cumplimiento de este requerimiento, se procedió a realizar un análisis de tráfico en la capa de red utilizando el analizador de protocolos Wireshark.

La metodología de comprobación consistió en inyectar tráfico continuo mediante el protocolo ICMP desde la red LAN de la Matriz Tulcán hacia la red LAN del Campus Cayambe, mientras simultáneamente se realizaba una captura de paquetes directamente en el enlace WAN perimetral.

Como se evidencia en la Figura 26, los resultados de la captura demuestran que el tráfico original es invisible en el medio de transporte. El analizador de protocolos no registra peticiones con origen en texto plano; únicamente identifica tramas etiquetadas bajo el protocolo ESP, correspondiente a la capa de seguridad de IPsec. Que toda la carga útil y el direccionamiento IP interno de la universidad viajen encapsulados y cifrados queda así corroborado, y el diseño propuesto protege de manera efectiva los activos de información frente a ataques de intercepción. La traza

capturada confirma que el túnel no deja expuesta ninguna cabecera interna durante el tránsito por la red pública.

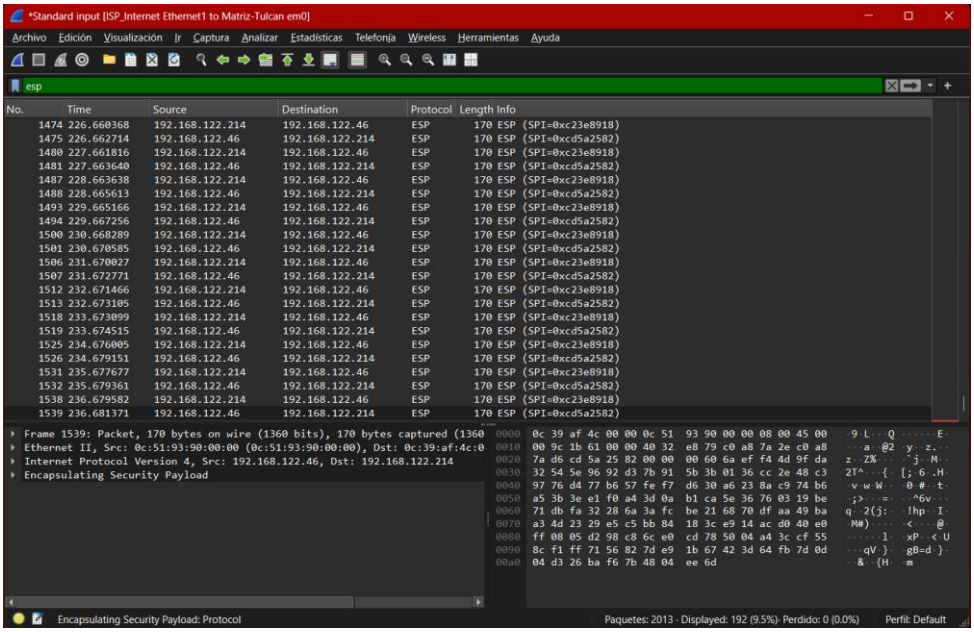

Figura 26. Captura de tráfico ESP en el túnel IPsec mediante Wireshark.

4.1.4.2. Validación experimental del túnel VPN IPsec

Para evaluar el comportamiento del túnel IPsec bajo condiciones de carga realistas, las pruebas de conectividad básica fueron reemplazadas por la generación de tráfico sintético mediante herramientas de diagnóstico de red.

La ejecución de la métrica requirió configurar un nodo en la Matriz Tulcán operando en modo servidor de escucha multipuerto, mientras que en el Campus Cayambe se dispuso un nodo en modo cliente. Esta distribución replicó, dentro del entorno de emulación, el flujo asimétrico característico de una arquitectura Hub-and-Spoke con servicios concentrados en la sede central.

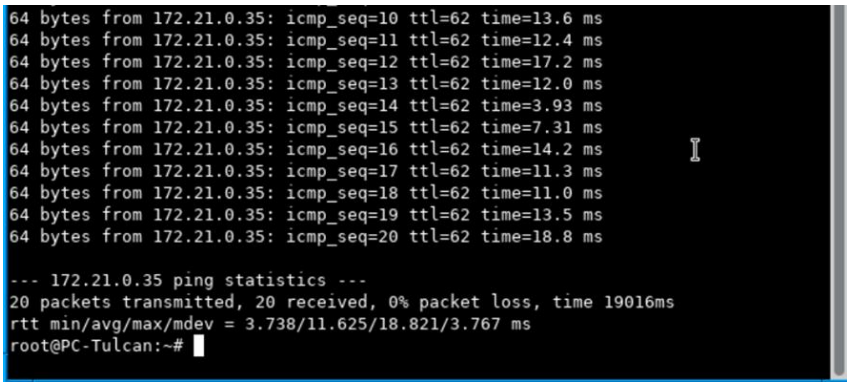

Figura 27. Reporte de rendimiento mediante ICMP

La Figura 27 presenta el comportamiento del transporte de datos mediante el protocolo ICMP hacia el nodo remoto correspondiente al Campus Cayambe. Durante la prueba se aplicó una transferencia de 20 paquetes, observándose estabilidad en la tasa de transferencia. En relación con la calidad del enlace, la métrica de latencia registró un valor promedio de 11.62 ms. Asimismo, no se evidenció pérdida de paquetes durante la transmisión, lo que refleja estabilidad en el comportamiento del túnel VPN bajo las condiciones evaluadas. Con el propósito de evaluar el comportamiento de la arquitectura propuesta bajo condiciones concurrentes, se ejecutó una prueba simultánea de tráfico durante un periodo de 30 segundos. Para ello, se emuló un flujo de 100 Kbps asociado a un servicio de telefonía IP y, de manera paralela, un flujo de 1 Mbps correspondiente a una transmisión de videovigilancia CCTV con compresión H.264.

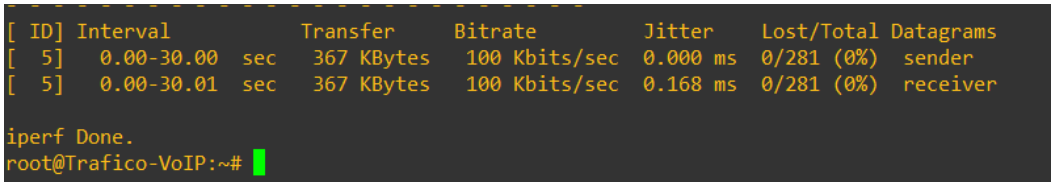

Figura 28. Prueba de rendimiento VoIP mediante iPerf3.

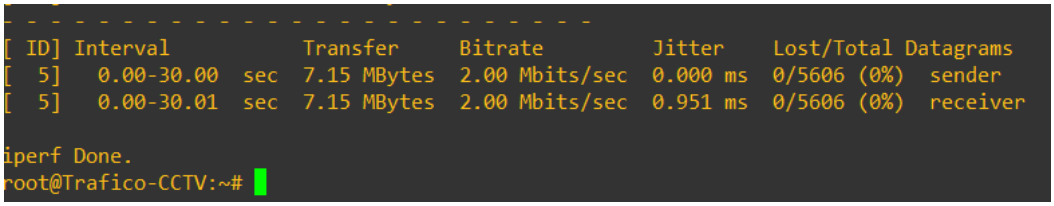

Figura 29. Prueba de rendimiento CCTV mediante iPerf3.

Como se observa en las Figuras 28 y 29, las métricas obtenidas evidenciaron estabilidad en el procesamiento del tráfico cifrado a través del túnel IPsec implementado en pfSense. Los valores de jitter registrados fueron de 0.168 ms para el tráfico VoIP y 0.951 ms para el flujo de video, manteniéndose dentro de rangos adecuados para aplicaciones de comunicación en tiempo real. Del mismo modo, no se registró pérdida de paquetes durante las pruebas realizadas, permitiendo validar el funcionamiento de la arquitectura propuesta bajo las condiciones del entorno experimental.

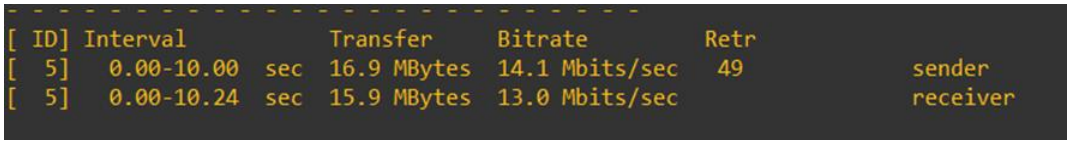

Figura 30. Prueba de rendimiento mediante iPerf3 THROUGHPUT.

La Figura 30 presenta las métricas de rendimiento obtenidas mediante la herramienta iPerf3, utilizando un flujo continuo de tráfico TCP entre los segmentos lógicos correspondientes a la Matriz Tulcán y el Campus Cayambe.

A continuación, se presentan las Tablas 13 y 14 resumen de las métricas de rendimiento obtenidas durante la fase de validación del túnel IPSec en el entorno virtualizado GNS3. Los valores reflejan el comportamiento del sistema bajo carga concurrente de los servicios críticos identificados por la UPEC.

Tabla 13. Métricas de rendimiento obtenidas en el túnel IPsec.

Servicio evaluado	Protocolo	Carga simulada	Jitter obtenido	Pérdida paquetes	Calidad del Enlace
Telefonía IP (VoIP)	UDP / RTP	100 Kbps	0.168 ms	0 %	✓ **Aprobado**
Video vigilancia (CCTV)	UDP / H.264	1 Mbps	0.951 ms	0 %	✓ **Aprobado**
Carga concurrente	UDP mixto	1.1 Mbps	< 1 ms	0 %	✓ **Aprobado**
Conectividad base	ICMP / Ping	—	Estable	0 %	✓ **Verificado**
Cifrado en tránsito	ESP / AES-256	Sniffing	—	0 % expuesto	✓ **Encriptado**

Bajo carga simultánea de tráfico VoIP y CCTV durante 30 segundos, el túnel IPSec con cifrado AES-256 + SHA-256 procesó el 100% de los paquetes sin registrar pérdidas en ninguno de los dos canales, y los valores de jitter obtenidos se situaron por debajo de 1 ms. La integridad del flujo, incluso con streams concurrentes de distinta naturaleza, quedó respaldada por la combinación de cifrado simétrico y autenticación robusta que opera sobre ESP.

Tabla 14. Comparación de métricas de red con estándares ITU-T G.114.

Indicador	Valor obtenido	Umbral aceptable	Margen de seguridad	Resultado
Jitter VoIP	0.168 ms	≤ 30 ms	178× por debajo del límite	✓ **Cumple**
Jitter CCTV	0.951 ms	≤ 30 ms	31× por debajo del límite	✓ **Cumple**
Pérdida de paquetes VoIP	0 %	≤ 1 %	Margen total (100 %)	✓ **Cumple**
Pérdida de paquetes CCTV	0 %	≤ 1 %	Margen total (100 %)	✓ **Cumple**
Confidencialidad en WAN	100 % ESP	ESP visible	Sin texto plano expuesto	✓ **Cumple**

Los márgenes cuantificados resultan relevantes para proyectar el comportamiento en producción: el jitter VoIP de 0.168 ms se sitúa por debajo del umbral máximo tolerable, en tanto que el jitter CCTV de 0.951 ms obtiene resultados favorables. Sugieren estos márgenes que la arquitectura dispone de capacidad suficiente para absorber la degradación adicional que introduce el internet público en condiciones

reales, aunque su verificación definitiva dependerá de pruebas sobre infraestructura física con usuarios concurrentes.

4.1.4.3. Optimización de Tránsito y Resolución de Fragmentación

Uno de los desafíos técnicos inherentes a la implementación de túneles IPsec es el incremento de la sobrecarga en las cabeceras de los paquetes debido a los procesos de encapsulamiento y cifrado. En la topología desplegada para la Universidad Politécnica Estatal del Carchi, se detectó que el envío de cargas útiles de tamaño máximo sufría procesos de fragmentación lo que derivaba en descartes de paquetes y un rendimiento subóptimo en la red, un escenario inaceptable para la transmisión de bases de datos o sistemas de CCTV institucionales.

Se procedió, para resolver esta anomalía de rendimiento, a intervenir en la negociación de la capa de transporte, aplicando la técnica de MSS Clamping en las interfaces correspondientes a los túneles VPN de los equipos pfSense. Como se evidencia en la Figura 31, se ajustó el valor del parámetro MSS a 1350 bytes.

Fuerza esta configuración a los equipos cliente a negociar segmentos de datos más pequeños durante el saludo inicial TCP; al limitar el MSS a 1350 bytes, se deja el margen exacto necesario para que pfSense añada las cabeceras criptográficas de IPsec sin superar el límite de transmisión del enlace físico. Los resultados de esta optimización fueron inmediatos: se eliminó la fragmentación, se estabilizó el túnel de extremo a extremo y se garantizó un flujo de datos constante para los servicios críticos de la sede central y sus sucursales; en conjunto, este ajuste puntual resolvió una limitación estructural que habría comprometido el desempeño de los servicios más sensibles a la pérdida de paquetes.

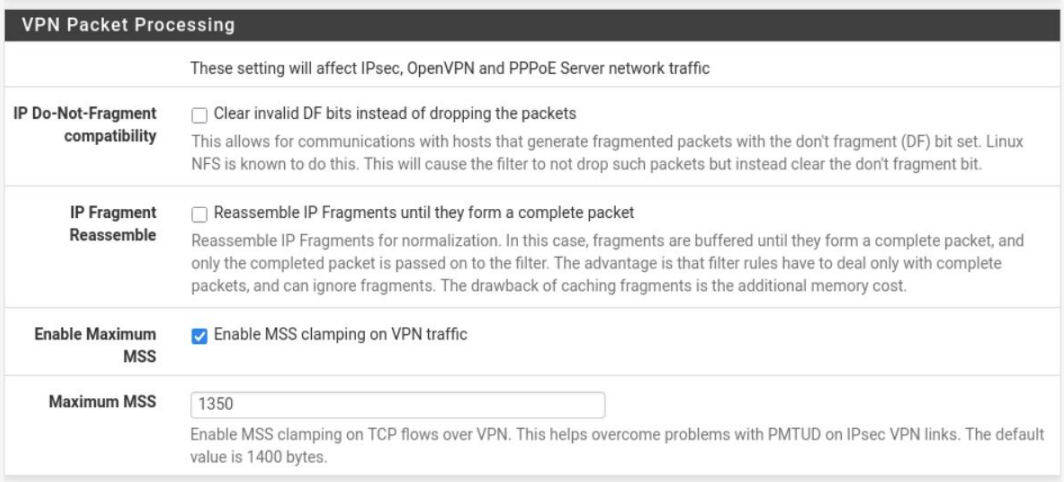

Figura 31. Configuración MSS Clamping en pfSense.

Los resultados obtenidos evidenciaron que la implementación del túnel IPsec permitió mantener niveles adecuados de rendimiento y estabilidad para el tráfico institucional evaluado. Introdujo el procesamiento criptográfico, si bien, una ligera sobrecarga respecto al escenario sin VPN; las métricas registradas permanecieron, no obstante, dentro de los umbrales recomendados para aplicaciones sensibles al retardo, garantizando de forma simultánea la confidencialidad e integridad de la información transmitida entre las sedes universitarias.

4.1.4.4. Validación experimental del sin túnel VPN

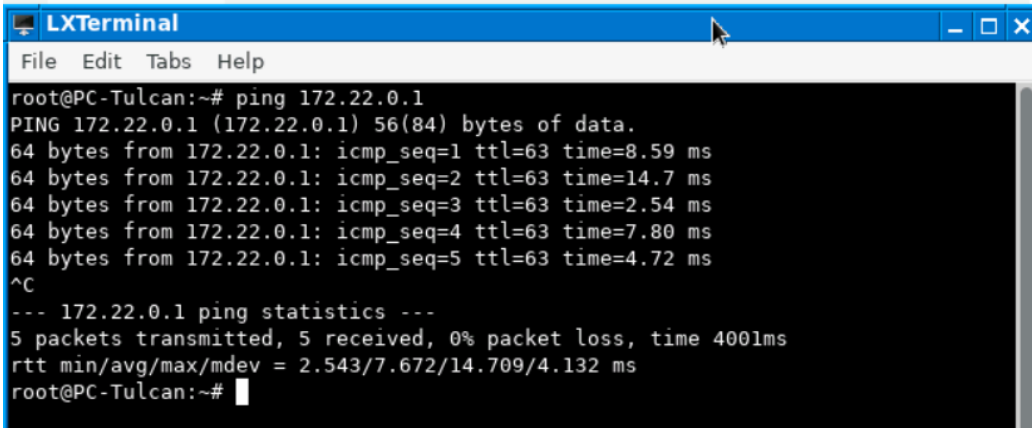

Figura 32. Reporte de rendimiento mediante ICMP sin VPN.

En la Figura 32 se evidencia que no se registró pérdida de paquetes mostrando estabilidad en la comunicación dentro del entorno emulado empleado para la investigación.

La latencia, se mantuvo en valores bajos durante las pruebas de conectividad. La ausencia de paquetes descartados y la contención del RTT en un entorno donde las

interfaces WAN introducen el primer salto de enrutamiento confirman que la capa de transporte virtualizada no agregó inestabilidad ajena al diseño previsto. Este comportamiento corresponde a un escenario de transmisión sin encapsulación criptográfica, en el cual el tráfico es procesado directamente mediante enrutamiento convencional de Capa 3. Los resultados obtenidos sirven como referencia comparativa para evaluar posteriormente el impacto del túnel VPN IPsec sobre el rendimiento de la red.

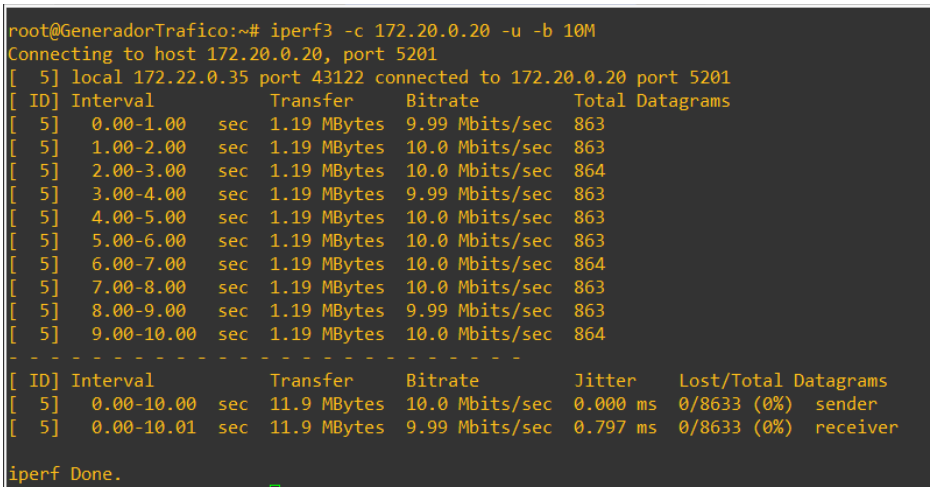

Figura 33. Prueba de rendimiento mediante iPerf3 sin VPN.

Tabla 15. Métricas de rendimiento e integridad obtenidas mediante iPerf3.

Parámetro Evaluado	Valor Registrado	Condición
Protocolo de Transporte	UDP	Correcto
Ancho de Banda Inyectado	10.0 Mbps	Parámetro de carga nominal
Rendimiento Real	9.99 Mbps	Línea de transmisión saturada al 100%
Fluctuación del Retardo	0.797 ms	Óptimo / Despreciable
Pérdida de Paquetes	0%	Integridad total del flujo

Los resultados obtenidos y resumidos en la Tabla 15, junto con la evidencia mostrada en la Figura 33, reflejan estabilidad en la transmisión de tráfico UDP dentro del entorno evaluado. El throughput alcanzó valores cercanos a los 10.0 Mbits/s configurados durante la prueba, manteniéndose un comportamiento constante en la transferencia de datos.

Registró la fluctuación del retardo, en cuanto a la calidad del enlace, un promedio de 0.797 ms, dentro de rangos adecuados para aplicaciones sensibles al retardo, como Voz sobre IP y servicios multimedia; tampoco se evidenció, durante las pruebas realizadas, pérdida de paquetes, lo que permite establecer una línea base de rendimiento previa a la implementación del túnel IPsec y al procesamiento criptográfico asociado.

```
root@GeneradorTrafico:~# iperf3 -c 172.20.0.20
Connecting to host 172.20.0.20, port 5201
[  5] local 172.22.0.35 port 41020 connected to 172.20.0.20 port 5201
[ ID] Interval           Transfer     Bitrate         Retr  Cwnd
[  5]   0.00-1.00   sec  3.77 MBytes  31.6 Mbits/sec    0    209 KBytes
[  5]   1.00-2.00   sec  4.04 MBytes  33.9 Mbits/sec    0    376 KBytes
[  5]   2.00-3.00   sec  4.60 MBytes  38.6 Mbits/sec    0    550 KBytes
[  5]   3.00-4.00   sec  3.60 MBytes  30.2 Mbits/sec    0    720 KBytes
[  5]   4.00-5.00   sec  2.50 MBytes  21.0 Mbits/sec    0    880 KBytes
[  5]   5.00-6.00   sec  3.75 MBytes  31.5 Mbits/sec    0   1.02 MBytes
[  5]   6.00-7.00   sec  2.50 MBytes  21.0 Mbits/sec    0   1.18 MBytes
[  5]   7.00-8.00   sec  2.50 MBytes  21.0 Mbits/sec    0   1.30 MBytes
[  5]   8.00-9.00   sec  3.75 MBytes  31.5 Mbits/sec    0   1.48 MBytes
[  5]   9.00-10.00  sec  2.50 MBytes  21.0 Mbits/sec    0   1.62 MBytes
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate         Retr
[  5]   0.00-10.00  sec  33.5 MBytes  28.1 Mbits/sec    0             sender
[  5]   0.00-10.67  sec  32.8 MBytes  25.8 Mbits/sec                  receiver
```

Figura 34. Prueba de rendimiento mediante iPerf3 THROUGHPUT sin VPN.

Tabla 16. Throughput y flujo TCP sin sobrecarga criptográfica.

Parámetro Evaluado	Valor Registrado
Protocolo de Transporte	TCP
Duración de la prueba	10 s
Datos Transferidos	32.8 MB
Ancho de Banda Máximo	25.8 MB/sec
Retransmisiones	0
Ventana de Congestión	1.62 MB

Los resultados de la Figura 34 y reflejados en la Tabla 16 muestran un comportamiento estable en la transmisión de tráfico TCP. El throughput obtenido alcanzó valores sostenidos cercanos al límite configurado durante las pruebas, lo que indica un funcionamiento continuo de la comunicación entre los segmentos evaluados.

No se registraron retransmisiones durante la transferencia de datos lo que indica la ausencia de congestión o pérdida de paquetes en el entorno experimental utilizado. Estos resultados permiten establecer una referencia comparativa para analizar posteriormente el impacto del procesamiento criptográfico que introduce la activación del túnel VPN IPsec.

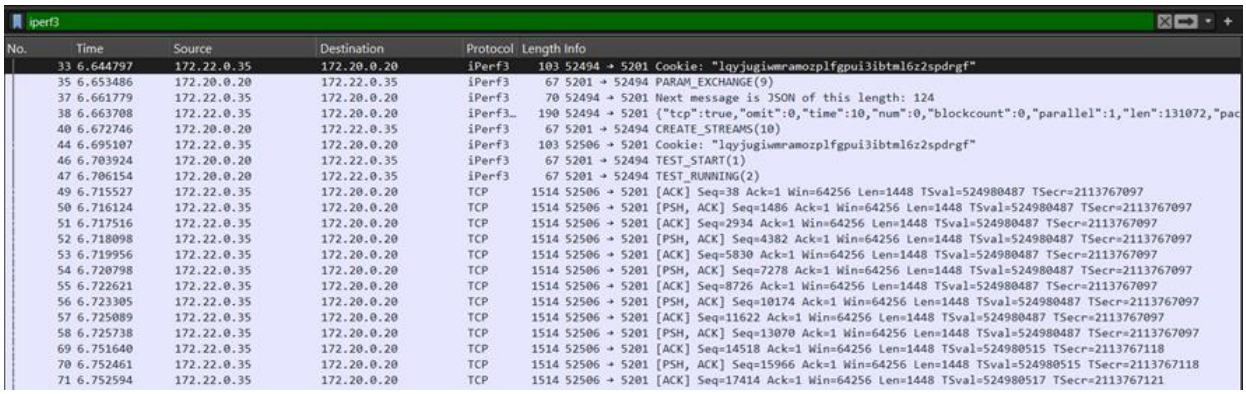

Figura 35. Captura de tráfico sin VPN mediante Wireshark.

El análisis del tráfico capturado mediante Wireshark, mostrado en la Figura 35, permitió observar que la información transmitida entre las sedes circulaba sin encapsulación criptográfica. Fue posible identificar, durante la inspección de paquetes, las direcciones IP internas utilizadas en la comunicación, así como información correspondiente a la capa de transporte y los puertos empleados durante las pruebas de conectividad.

Esta visibilidad del tráfico evidencia que el escenario evaluado carece de mecanismos de cifrado y protección de la información en tránsito, lo que permite que los datos puedan ser inspeccionados desde la red WAN; en este contexto, la implementación de túneles VPN IPsec representa una alternativa orientada a mejorar la confidencialidad y protección del tráfico entre las sedes universitarias evaluadas en la investigación.

4.1.5. Análisis Comparativo Métricas de conectividad y seguridad intercampus

El contraste de los resultados obtenidos evidencia en la Tabla 17 que la implementación del túnel VPN IPsec introduce un incremento moderado en las métricas de latencia, jitter y throughput, asociado al procesamiento criptográfico requerido para la encapsulación y protección del tráfico; permanecieron, no obstante, los valores registrados durante las pruebas dentro de rangos adecuados para aplicaciones sensibles al retardo.

En relación con el rendimiento de la red, la reducción observada en el throughput TCP representa el impacto operativo asociado al uso de mecanismos de cifrado y autenticación implementados mediante el protocolo ESP. A diferencia del escenario sin VPN, el escenario con IPsec permitió encapsular y proteger la información transmitida entre las sedes evaluadas; el contraste entre ambos escenarios ilustra, en definitiva, el compromiso entre rendimiento y seguridad inherente a la adopción de túneles cifrados.

Tabla 17. Cuadro comparativo de rendimiento, métricas de conectividad y seguridad.

Métrica	Escenario 1: Sin Túnel VPN	Escenario 2: Con Túnel VPN IPsec	Impacto Técnico
Latencia Promedio (RTT)	7.67 ms	11.62 ms	Penalización temporal por procesamiento
Jitter Promedio (UDP)	0.797 ms	0.951	Variabilidad por colas simétricas
Throughput Máximo TCP	25.8 Mbps	13 Mbps	Degradación por *Overhead* y MSS

Visibilidad del Direccionamiento LAN	Totalmente Visible	Completamente Oculto	Ocultación de Topología
Estado del Payload	Texto Plano	Cifrado Simétrico	Confidencialidad Absoluta

Los resultados obtenidos permiten considerar que la arquitectura implementada sobre pfSense y emulada en GNS3 constituye una alternativa viable para la interconexión segura entre campus universitarios.

4.2. DISCUSIÓN

4.2.1. Análisis del Rendimiento Criptográfico frente a Métricas de Conectividad.

Las pruebas de emulación ejecutadas sobre la arquitectura propuesta arrojaron un jitter de 0.168 ms para tráfico VoIP y de 0.951 ms para transmisiones de CCTV, con 0% de pérdida de paquetes en ambos canales. Estos valores —obtenidos bajo carga concurrente en entorno virtualizado GNS3— permiten establecer una línea base técnica que respalda la viabilidad de la comunicación cifrada entre la matriz Tulcán y las sedes remotas de la UPEC. Conviene tener presente que el entorno de emulación trabajó con volúmenes de tráfico controlados; por tanto, los resultados deben interpretarse como referencia de diseño lógico y no como proyección directa de producción.

Lo relevante de estos datos no radica únicamente en que los valores sean bajos, sino en lo que implican: ni la encapsulación IPsec ni el cifrado AES-256 con mecanismos de integridad basados en SHA-256 introdujeron una sobrecarga capaz de comprometer la calidad de los servicios evaluados. Los valores obtenidos se mantuvieron muy por debajo de los umbrales comúnmente aceptados para aplicaciones de voz en tiempo real. Haber quedado a una fracción de milisegundo de ese límite indica que el diseño del túnel maneja adecuadamente el overhead criptográfico sin afectar la experiencia de los usuarios institucionales.

Este análisis permite distinguir lo que corresponde al protocolo de lo que depende del hardware. En un despliegue real con mayor número de usuarios simultáneos, las limitaciones que eventualmente surjan estarán asociadas a la capacidad de procesamiento de los equipos de borde, no a deficiencias en el diseño lógico de la VPN. En ese sentido, la investigación entrega a la UPEC un modelo técnico validado a partir del cual puede proyectar el despliegue físico de su red intersedes con un riesgo de diseño significativamente reducido.

4.2.2. Viabilidad del Software Libre en Infraestructuras Críticas

Uno de los hallazgos que merece interpretación específica es el desempeño demostrado por pfSense como nodo de terminación VPN. En instituciones públicas como la UPEC suele asumirse que una seguridad perimetral robusta va de la mano con soluciones comerciales de licenciamiento anual. Los resultados obtenidos en este estudio cuestionan dicha equivalencia: una distribución basada en FreeBSD, de código abierto, mostró un comportamiento estable dentro del entorno de emulación evaluado, al menos bajo las condiciones allí reproducidas.

En términos técnicos, pfSense sostuvo sin degradación el intercambio de claves y la negociación de las fases IKE y ESP del protocolo IPSec. La adopción de estándares IETF favorece, además, la interoperabilidad entre fabricantes, lo cual reviste importancia porque trabajar sobre estándares abiertos permite integrar equipos de distintos fabricantes sin dependencia de un proveedor específico. Esto tiene implicaciones directas para la capacidad de la universidad de escalar su infraestructura de manera modular y autónoma, sin incurrir en los costos y restricciones del vendor lock-in.

Desde una perspectiva económica, la adopción de este modelo libera recursos de presupuesto que habitualmente se destinan a licenciamiento; dichos fondos podrían redirigirse hacia mejoras en hardware físico o en capacidad de ancho de banda. Este resultado no implica que pfSense sea la solución adecuada para cualquier institución, sino que, bajo las condiciones específicas de la UPEC y en el contexto evaluado, constituye una alternativa técnicamente fundamentada y económicamente viable. La validación con tráfico concurrente de voz y video en un esquema Hub-and-Spoke sugiere que el umbral de exigencia superado no fue trivial, y que el software libre, correctamente configurado, puede equiparar las prestaciones de plataformas propietarias en escenarios de complejidad intermedia.

4.2.3. Impacto de la Criptografía y Validación de Seguridad Perimetral

La captura de tráfico realizada mediante Wireshark sobre el enlace WAN emulado entre la matriz Tulcán y las sedes remotas mostró que la carga útil de los paquetes transmitidos aparece completamente ilegible, resultado directo de la acción del protocolo ESP con cifrado AES-256. Constituye este hallazgo la verificación empírica de que el cifrado de extremo a extremo opera correctamente en la arquitectura

diseñada, lo cual responde de manera directa al objetivo de garantizar la confidencialidad de la información institucional en tránsito.

La relevancia de este resultado se comprende mejor al contrastarlo con la situación previa a la propuesta: la ausencia de un mecanismo de interconexión cifrada entre sedes incrementaba el riesgo potencial de exposición de información durante el tránsito a través de redes públicas, y bajo esa condición un actor externo con acceso al canal de comunicación del proveedor de internet habría podido capturar información en texto plano. Elimina la arquitectura propuesta ese vector de ataque dentro del alcance del entorno validado.

Lo que este resultado demuestra va más allá de la configuración técnica: confirma que la integración correcta de las fases IKE y el encapsulamiento ESP no solo resuelve la interconexión geográfica entre sedes, sino que establece condiciones de confidencialidad, integridad y autenticidad para las comunicaciones institucionales, alineando la infraestructura de red con los requerimientos de la Ley Orgánica de Protección de Datos Personales y con los estándares vigentes de ciberseguridad institucional; en conjunto, este hallazgo cierra el ciclo de validación técnica planteado para la arquitectura propuesta.

4.2.4. Comparación con Estudios Previos y Contraste de Resultados

Quishpe Iza (2021) documentó que las arquitecturas VPN permiten establecer interconexiones estables con bajo costo operativo en entornos universitarios ecuatorianos. Son consistentes los resultados del presente estudio con esa conclusión, y agregan un elemento que ese trabajo no desarrolló con la misma profundidad: la estabilidad del túnel no depende únicamente del protocolo de encapsulamiento, sino también de cómo la arquitectura gestiona los servicios con requerimientos de tiempo real como VoIP y CCTV. Los valores de jitter registrados en este estudio resultaron inferiores a los reportados en investigaciones con OpenVPN diferencia que se relaciona con la mayor carga de procesamiento que ese protocolo impone al operar en espacio de usuario, frente a la eficiencia que ofrece IPsec al trabajar en la capa de red.

La selección de IPsec sobre alternativas basadas en SSL/TLS respondió a criterios técnicos concretos. Documenta la literatura el uso frecuente de SSL/TLS para acceso remoto móvil, donde la flexibilidad prima sobre el rendimiento; en el escenario de interconexión fija entre sedes evaluado en esta investigación, en cambio, IPsec

presentó ventajas al evitar el reprocesamiento de cabeceras que ocurre cuando el cifrado se aplica en capas superiores de la pila de protocolos. Esto se reflejó en los valores de latencia obtenidos, que contrastan con los cuellos de botella documentados en tesis que emplearon protocolos con mayor overhead.

En cuanto a la interoperabilidad entre equipos de distintos fabricantes, algunos estudios la identifican como un factor de riesgo en la negociación del túnel. En las pruebas realizadas con la infraestructura de la UPEC, la negociación IKE y el encapsulamiento ESP operaron sin inconvenientes entre dispositivos heterogéneos, lo que sugiere que el cumplimiento de los estándares IETF mitiga ese riesgo de manera efectiva. Es coherente esta observación con los hallazgos de Baque Pinargote y Gómez Guerra (2023), quienes también reportaron interoperabilidad adecuada en arquitecturas IPsec Site-to-Site con equipos de diferentes proveedores; no obstante, esta conclusión debe entenderse dentro del alcance del entorno emulado y no como una generalización extensible a cualquier combinación de hardware, por lo que su validez queda circunscrita a las condiciones específicas del estudio realizado.

4.2.5. Limitaciones del Entorno de Emulación y Transparencia Metodológica

Toda investigación empírica en ingeniería de redes debe delimitar con precisión las condiciones bajo las cuales se obtuvieron sus resultados. La principal restricción de este estudio radica en que las pruebas se desarrollaron sobre un entorno virtualizado en GNS3, donde el transporte de área amplia fue abstraído mediante un nodo NAT compartido; no incorporan las métricas obtenidas las latencias propias del ruteo en internet público, la congestión de los proveedores de servicio ni las variaciones en los enlaces físicos reales.

Esta abstracción del medio de transporte, sin embargo, no compromete la validez de los hallazgos criptográficos ni lógicos del estudio. Ejecuta GNS3 los núcleos reales de las distribuciones basadas en FreeBSD, de modo que los procesos de encapsulamiento, la negociación de asociaciones de seguridad y la aplicación del algoritmo AES-256 se ejecutaron con precisión algorítmica. Al aislar la topología de las variables incontrolables del internet público, fue posible medir de forma específica el rendimiento del túnel IPsec y la eficacia del cifrado de la carga útil, sin interferencia de factores externos; configuran los datos obtenidos, por tanto, una validación de línea base del diseño lógico propuesto.

Estas consideraciones metodológicas definen el punto de partida para las etapas de implementación en la UPEC. Haber verificado que la arquitectura de túneles Site-to-Site con pfSense opera de manera estable, segura e interoperable para tráfico crítico reduce el riesgo técnico asociado al despliegue físico. En un escenario real con mayor número de usuarios concurrentes, los equipos de borde experimentarán niveles de exigencia de CPU y memoria superiores a los del entorno virtualizado; los protocolos y estándares sobre los que se sustenta la arquitectura, con todo, demostraron dentro del alcance de esta investigación estar correctamente dimensionados para las condiciones evaluadas, lo que confirma la coherencia entre el diseño lógico validado y los requerimientos técnicos de la institución.

V. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

El diagnóstico de la situación actual de la infraestructura de red de la Universidad Politécnica Estatal del Carchi permitió identificar la necesidad de disponer de un mecanismo de interconexión seguro entre sus diferentes campus. Evidenció el análisis que la separación geográfica de las sedes representa un desafío para el acceso eficiente a recursos y servicios institucionales compartidos, así como para la gestión centralizada de la información.

La comparación realizada entre las principales tecnologías de redes privadas virtuales permitió establecer que IPsec constituye la alternativa más adecuada para el contexto de interconexión entre campus universitarios. Su operación en la capa de red y su amplia adopción en entornos empresariales e institucionales respaldan, asimismo, su utilización como una solución confiable y alineada con las necesidades de seguridad y escalabilidad identificadas en la UPEC.

Como resultado del proceso de diseño, se desarrolló una arquitectura de interconexión basada en una VPN Site-to-Site utilizando el protocolo IPsec e implementada mediante dispositivos pfSense dentro de un entorno de emulación. Permitió la propuesta integrar lógicamente las diferentes redes institucionales conservando la segmentación establecida para cada sede y definiendo mecanismos de comunicación seguros entre ellas; incluyó el diseño la estructuración de la topología lógica, la asignación del direccionamiento correspondiente y la configuración del enrutamiento necesario para garantizar el intercambio de información entre campus. De esta manera, se obtuvo una propuesta técnicamente fundamentada que puede servir como referencia para futuras implementaciones reales en entornos universitarios con características similares.

La evaluación de la arquitectura propuesta mediante pruebas de conectividad y transmisión de datos demostró la viabilidad técnica de la solución diseñada dentro del entorno de emulación. Los resultados obtenidos evidenciaron que el túnel VPN permitió mantener una comunicación estable entre las redes interconectadas,

posibilitando el intercambio de información sin afectar significativamente el funcionamiento general del sistema. En conjunto, las pruebas realizadas permitieron validar que la propuesta cumple con los requerimientos definidos inicialmente en términos de conectividad segura y operatividad entre sedes.

En términos generales, la presente investigación permitió determinar que una solución basada en VPN Site-to-Site con IPsec representa una alternativa técnicamente factible para fortalecer la interconectividad entre los campus de la Universidad Politécnica Estatal del Carchi. Responde la propuesta desarrollada a las necesidades identificadas durante el diagnóstico inicial, integra mecanismos de seguridad acordes con las exigencias actuales de protección de la información y demuestra, mediante un entorno de emulación, su potencial para facilitar el acceso seguro a los recursos institucionales.

5.2. RECOMENDACIONES

Con base en los resultados obtenidos durante la fase de validación, se recomienda llevar el diseño propuesto a producción de forma escalonada, integrando primero la Matriz Tulcán con el campus de mayor carga administrativa antes de extender la solución a las sedes restantes. Este enfoque permitirá al equipo de TI institucional registrar el comportamiento real de los túneles bajo las variables propias del internet público y construir una línea base de producción que complemente los datos de emulación generados en esta investigación.

Los resultados de las pruebas de carga evidenciaron que el rendimiento de la arquitectura en producción dependerá, en parte, de las características del hardware físico utilizado como nodo de terminación VPN. Se recomienda dimensionar los equipos de borde considerando el volumen de usuarios concurrentes por sede, el ancho de banda disponible y la carga computacional del cifrado AES-256. En particular, se sugiere evaluar hardware con soporte para el conjunto de instrucciones AES-NI, lo que permite delegar las operaciones criptográficas al procesador y liberar recursos para las tareas de enrutamiento y filtrado.

Para campus con cargas administrativas moderadas, podrían emplearse appliances compatibles con pfSense o equipos de propósito general con procesadores Intel Core i3 o equivalentes, un mínimo de 8 GB de memoria RAM y almacenamiento SSD, especificaciones suficientes para soportar túneles IPsec Site-to-Site, aplicar políticas

de cortafuegos y gestionar servicios institucionales sin comprometer el rendimiento de la red.

Dado que las pruebas se ejecutaron en un entorno controlado sin congestión de red pública, se recomienda incorporar políticas de Calidad de Servicio en los equipos de borde para el despliegue en producción. La configuración de colas de prioridad mediante los planificadores HFSC o PRIQ disponibles en pfSense permitirá asignar mayor peso al tráfico UDP asociado a VoIP y a los flujos de videovigilancia, de modo que los servicios críticos identificados mantengan condiciones de transmisión adecuadas en escenarios de mayor congestión del enlace WAN.

Durante la fase de diseño se aplicó MSS Clamping como mecanismo de mitigación de fragmentación en los túneles WAN, configuración que demostró ser necesaria para garantizar la entrega continua de tráfico sin retransmisiones innecesarias. Se recomienda conservar y documentar esta configuración como parte de los procedimientos operativos estándar del Departamento de Redes, verificando su ajuste ante cualquier cambio en el proveedor de internet o en el equipamiento de borde, ya que modificaciones en la MTU del enlace pueden reactivar el problema de fragmentación en producción.

Se recomienda implementar un sistema de monitoreo activo de los túneles VPN mediante herramientas de código abierto compatibles con pfSense, como Zabbix o Grafana con exportadores de métricas de red. El sistema deberá registrar de forma continua indicadores como el estado de las asociaciones de seguridad IKE/ESP, la latencia inter-sede, el jitter y el porcentaje de utilización del ancho de banda por túnel.

Como línea de trabajo futuro derivada de las limitaciones del entorno de emulación, se recomienda explorar la implementación de esquemas de alta disponibilidad mediante la configuración de enlaces de respaldo en cada sede. La conmutación automática ante la interrupción del enlace primario, aprovechando las capacidades de balanceo y rutas flotantes de pfSense, elevaría los niveles de disponibilidad de la red hacia estándares de continuidad operativa más exigentes.

VI. REFERENCIAS BIBLIOGRÁFICAS

Andaluz, A., & Guanolisa, J. (2022). Implementación de una Red VPN "Virtual Private Network para la mejora de la seguridad dentro de la red local inalámbrica de la Empresa de distribución de material de Construcción y Ferretero "Distribuidora Gómez, mediante el uso de protocolos Ipsec y Tcp/. Obtenido de http://repositorio.utc.edu.ec/handle/27000/9740

Asadi, S., Jordan, A., Madhu, K., & Mehrbakhsh, N. (2024). Simulation-Based Learning for Computer and Networking Teaching: A Systematic Literature Review and Bibliometric Analysis. Education and Information Technologies. doi:10.1007/s10639-024-12476-7

Aspera, G. (2025). Red GPON experimental virtualizada (NFV) mediante gestión definida por software (SDN). Obtenido de https://accedacris.ulpgc.es/bitstream/10553/142607/1/TFG%20LaresAsperaGabrielErnesto.pdf

Ataypoma Llanto, J. (2023). Como la implementación de una red privada virtual (VPN) mejora la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión. Universidad Nacional José Faustino Sánchez Carrión. Obtenido de http://hdl.handle.net/20.500.14067/7655

Baque Pinargote, O., & Gómez Guerra, W. (2023). Implementación de una VPN site-to-site bajo el protocolo de cifrado IPSec para el control y seguridad administrativa de la empresa privada Inter&Solutions. Universidad Estatal de Jipijapa (UNESUM). Obtenido de https://repositorio.unesum.edu.ec/handle/53000/5927

Barreto, G. (2025). Sistema de comunicación para la transmisión de datos y tratamiento de la información bajo la norma ANSI/TIA 568B en las aulas de la clase del bloque 1 de la carrera de la tecnologías de la información. Obtenido de https://repositorio.unesum.edu.ec/bitstream/53000/8183/1/BARRETO%20GARCÍA%20GENESIS%20NATHALY.pdf

Berrones, M. (2025). Evaluación de la efectividad de VPN OPEN SOURCE en estrategias de ciberseguridad: Un estudio integral sobre implementación, desafíos y mejores prácticas. Obtenido de https://repositorio.utn.edu.ec/handle/123456789/17338

Borja, B. (2022). Análisis de rendimiento de puertas de enlace VPN mediante una arquitectura de red para la comunicación segura sitio a sitio entre las PYMES. Obtenido de https://repositorio.puce.edu.ec/items/9a73f61e-a3d9-4a1b-abae-2f04c8f78124

Camacho, C., & Nuñez, D. (2021). Análisis comparativo de Gestión Unificada de Amenazas (UTM) de código abierto para fortalecer la seguridad de la información en las PYMES.

Carvajal, J. (2025). Capacidades técnicas, tácticas y de respuesta para equipos red team y blue team. Obtenido de https://repository.unad.edu.co/jspui/bitstream/10596/78853/3/jjcarvajalv.pdf

Chávez Paredes, L. (2022). Modelo de infraestructura de red VPN para interconexión segura de organizaciones, usando IPSec con Linux, bajo un entorno virtualizado de clientes y servidores. Universidad Nacional del Altiplano. Obtenido de https://repositorio.unap.edu.pe/handle/20.500.14082/18361

Cisco. (2006). Nuevas tecnologías simplificadas. Obtenido de https://www.cisco.com/c/dam/global/es_mx/products/servicios/docs/LCS_Brochure_Enterprise_Spanish_062006.pdf

Cisco. (2023). Resolver fragmentación de IPv4 y problemas de MTU, MSS y PMTUD con GRE e IPSEC. Obtenido de https://www.cisco.com/c/es_mx/support/docs/ip/generic-routing-encapsulation-gre/25885-pmtud-ipfrag.html

Cloudflare. (2024). Overview of Internet-Native SASE Architecture. Obtenido de https://assets.ctfassets.net/slt3lc6tev37/6zdZWTjDukemlpiZJ3CZbF/e5db0f65a3ffd45daa3e8133d931c5ca/Overview_of_Internet_Native_SASE_Architecture_-_Whitepaper.pdf

Coello, A. A. (2025). Redes privadas virtuales y ciberseguridad: revisión bibliométrica y sistemática de las tendencias de investigación, los protocolos y las aplicaciones (2004-2024). Obtenido de https://orcid.org/0009-0009-7144-9968

Córdoba, D. (2022). Criptografía Post-Cuántica Aplicada a Entornos de Producción Open Source. Obtenido de https://um.edu.ar/wp-content/uploads/UM-FI-MTI_Cordoba.pdf

de Jesús, C., Flores, C., & Jalife, S. (2022). *Infraestructura y conectividad como eje para la transformación universitaria.* Obtenido de https://cudi.edu.mx/sites/default/files/2022-11/Entregable_Infraestructura_conectividad_como-eje_transformacion_educacion_opt_0.pdf

Delgado, V., Añazco, A., Gonzáles, D., & Romero, S. (2024). Transformación digital en los procesos de aprendizaje de la educación superior. Obtenido de https://revistas.utb.edu.ec/index.php/magazine/article/view/3060

Flores, J., Arellano, C., & Urbieta, A. (2024). Gotham Testbed: A Reproducible IoT Testbed for Security Experiments and Dataset Generation. doi:10.1109/TDSC.2023.3247166

Fortinet. (2026). ¿Qué es una VPN? ¿Cómo funciona una red privada virtual? Obtenido de https://www.fortinet.com/lat/resources/cyberglossary/what-is-a-vpn

Galata, L., Korniyenko, B., & Yudin, A. (2024). Effectiveness of Application Software in the Simulation Boundary for Critical Data Protection. Journal of Information Security Research. Obtenido de https://doi.org/10.6025/jisr/2024/15/3/89-102

Guerra, J. (2023). Implementación de una VPN Site to Site bajo el protocolo de cifrado IPSEC para el control y la seguridad administrativa de la empresa privada Inter&Solutions. Obtenido de https://repositorio.unesum.edu.ec/bitstream/53000/5927/1/GOMEZ%20GUERRA%20WALTHER%20JOSUE.pdf

Harahus, M., Čavojský, M., Bugar, G., & Pleva, M. (2024). Interactive Network Learning: An Assessment of EVE-NG Platform in Educational Settings. doi:10.2478/aei-2023-0011

Haro, . (2021). Software defined wide area networking (SD-WAN) como mencanismo de seguridad en accesos WAN. Pontificia Universidad Católica del Ecuador. Obtenido de https://repositorio.puce.edu.ec/server/api/core/bitstreams/a4457ad9-ae71-40cb-919c-4f6d5bfa7690/content

Hernández-Sampieri, R., & Mendoza, C. (2018). Metodología de la investigación. Las rutas cuantitativa, cualitativa y mixta. Obtenido de https://doi.org/10.22201/fesc.20072236e.2019.10.18.6

Ibarra, C., Tapia, C., Tene, A., Toapanta, R., & Ormaza, G. (2025). Análisis de los Ataques de Ingeniería Social en Ecuador. Obtenido de https://ciencialatina.org/index.php/cienciala/article/view/9777

ITU-T G.114. (2004). Tiempo de transmisión en un sentido. Obtenido de https://www.itu.int/rec/dologin_pub.asp?lang=s&id=T-REC-G.114-200305-I!!PDF-S&type=items

LOPDP. (2021). personales., Ley Orgánica de protección de datos. Obtenido de https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Marcillo, X. (2024). Guía general de redes y comunicación de datos. Obtenido de https://itq.edu.ec/wp-content/uploads/2025/02/ITQ-24-GP1-DS-04-Guia-general-de-redes-y-comunicacion-de-datos.pdf

Menendez, C., & Sáchez, W. (2025). Seguridad y privacidad de los datos en la era de la información en el Ecuador. Obtenido de https://revistasojs.utn.edu.ec/index.php/ideas/article/view/1287

MinTic. (2021). Guía para el Aseguramiento del Protocolo IPv6. Obtenido de https://www.mintic.gov.co/portal/715/articles-162301_guia_aseguramiento_ipv6.pdf

Monterroso, J. R. (2022). Estudio de pre-factibilidad para la implementación de ciberseguridad aplicada a subestaciones eléctricas de transmisión del Sistema Nacional Interconectado con base en las normas IEEE C37.240 e IEEE 1686. Obtenido de http://www.repositorio.usac.edu.gt/17978/1/José%20René%20Gallardo%20Monterroso.pdf

Obregón, M. A. (2025). Desafíos éticos en la gestión del aprendizaje mediado por TIC. Privacidad, seguridad y equidad. Ecuador. Obtenido de http://dspace.unach.edu.ec/bitstream/51000/14929/1/Villacrés%20Obregón%20Mayra%20A%20%282025%29Desafios%20eticos%20en%20la%20Gestión%20del%20Aprendizaje%20mediado%20por%20Tic..pdf

Ocampo, K., Guapulema, P., Castillo, M., & Camacho, K. (2024). La brecha digital en la educación ecuatoriana: Desafíos post pandemia: The digital divide in ecuadorian education: post-pandemic challenges. Obtenido de https://latam.redilat.org/index.php/lt/article/view/2907

Ormacheda, M., Almidón, C., Vicente, W., & Pacheco, L. (2022). Gestión del tráfico de red en la calidad de servicio "QoS" WAN en Tambopata-Perú 2021. Obtenido de https://www.redalyc.org/journal/280/28070565020/28070565020.pdf

Oviedo, B., & Samaniego, E. (2018). Libro de Fundamentos de REDES. Obtenido de https://www.researchgate.net/publication/358105030_Libro_de_Fundamentos_de_REDES

Paucar, J., Prado, X., & Calero, A. (2025). Redes y Comunicación de Datos: fundamentos, diseño y gestión. doi:10.64973/edu.2025.2515

Perdigón Llanes, R., & Madrigal Leiva, I. (2022). Solución basada en herramientas de software libre para la implementación del teletrabajo online en empresas cubanas. Obtenido de https://www.redalyc.org/journal/3783/378370413007/html/

Ponce, Y., & Herrera, J. (3 de Octubre de 2023). Evaluación del Rendimiento de una red IPv6 utilizando IPSec en Modo Túnel. doi:https://doi.org/10.33936/isrtic.v7i2.5710

Quishpe Iza, L. (2021). Estudio para la implementación de una red privada virtual (VPN) utilizando herramientas de software libre. Caso de estudio "Comisión Fulbright del Ecuador". (P. Quito, Ed.) Obtenido de https://repositorio.puce.edu.ec/handle/123456789/27881

Rios Monar, S., & López Quezada, S. (2024). Herramientas virtualizadas para evaluación y gestión de redes ópticas pasivas INGE-2744. Obtenido de

https://www.dspace.espol.edu.ec/bitstream/123456789/66063/1/T-115333%20INGE-2744%20RIOS-LOPEZ.pdf

Romero, D. (2021). Suministro para el equipamiento destinado a la seguridad perimetral y el acceso a Internet seguro en varios segmentos de red. Obtenido de https://innovacion.dip-caceres.es/wp-content/uploads/sites/12/2023/11/MemoriaTecnica_Ariadnex.pdf

Romero, R. (2024). Dimensionamiento de los recursos de red existentes en la empresa SITEC S.A. a través de la metodología Kanban para un correcto rendimiento en el acceso a los servicios locales. Obtenido de https://repositorio.utn.edu.ec/handle/123456789/15548

Salazar, A., Barahona, D., Delgado, J., & Suárez, J. (2023). Seguridad en Redes WIFI. Obtenido de https://repositorio.uide.edu.ec/handle/37000/6106

Torres , J., Ruelas, A., & Herrera, J. (2023). Rendimiento para la interoperabilidad entre Raspberry pi, ESP8266 y PLC con Node-RED para el IIoT. Obtenido de ttps://doi.org/10.17163/ings.n29.2023.08

UNEMI. (2022). Fundamentos y arquitectura de red (OSI y TCP/IP). Obtenido de https://sga.unemi.edu.ec/media/archivologo/2022/02/16/archivologocompendio_202221611629.pdf

Vera, E., & Llambo, O. (2021). Diseño e implementación de un banco de pruebas virtualizado con tecnología de redes definidas por software para redes de área amplia (SD-WAN) en el laboratorio de telecomunicaciones para la Universidad Politécnica Salesiana sede Guayaquil. Obteni
do de http://dspace.ups.edu.ec/handle/123456789/20114

Wassef, M., & Lee, J. (2024). Navigating Network Security: Optimizing TCP/IP and IPsec for Satellites. Obtenido de https://sites.wp.odu.edu/markwassef/wp-content/uploads/sites/37243/2024/09/Navigating-Network-Security_-Optimizing-TCP_IP-and-IPsec-for-Satellites.pdf

Whitman, M., & Mattord, H. (2022). Criptografía. Obtenido de https://wcruzy.pe/sdli/09criptografia.pdf

VII. ANEXOS

Anexo 1. Certificado del abstract por parte de idiomas

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI- FOREIGN AND NATIVE LANGUAGES CENTER

Informe sobre el Abstract de Artículo Científico o Investigación.

Autor Steve Rodrigo Pullugando Gualuntuña
Fecha de entrega del informe: July 10th 2026

El presente informe validará la traducción del idioma español al inglés si alcanza un porcentaje de: 9 – 10 Excelente.

Si la traducción no está dentro de los parámetros de 9 – 10, el autor deberá realizar las observaciones presentadas en el ABSTRACT, para su posterior presentación y aprobación.

Observaciones:

Después de realizar la revisión del presente abstract, éste presenta una apropiada traducción sobre el tema planteado en el idioma inglés. Según la rúbrica de evaluación de la traducción en inglés, ésta alcanza un valor de 9; por lo cual se valida dicho trabajo.

Atentamente

JAIRO MAURICIO GUEVARA ROSERO

MSc. Jairo Guevara
Director de Centro Académicos y de Formación Complementaria

Anexo 2. Entrevista

Redes privadas virtuales para campus universitario

Fecha: ____ / ____ / 2026

Entrevistado: _____

Cargo / Área: _____

Objetivo de la entrevista: Recopilar parámetros técnicos, de infraestructura y de tráfico necesarios para levantar y configurar el entorno de simulación de la red.

Nota para el entrevistado: Las respuestas pueden ser datos exactos o estimaciones operativas. El enfoque es obtener la base técnica para la configuración del simulador.

1. ¿Tiene la universidad una VPN?

Actualmente la U tiene configurado varias VPNs, dependiendo los servicios. Como interconectar nuestro campus hacia el cloud de servicios Oracle donde tenemos nuestro portafolio institucional. Asi también VPNs para la conexión remota de los compañeros de TIC hacia nuestros servidores.

2. ¿Cómo funciona la VPN de la universidad?

Se configura las VPN en nuestro equipo perimetral, donde todos los clientes VPN se conectan con la IP Pública Virtual de la red, y a la cual deben apuntar todas las VPNs.

3. ¿El nuevo túnel VPN que estamos planteando debe interconectarse o enrutar tráfico hacia la VPN actual de la universidad en la sede principal?

[X] Sí, interconexión total.

[ ] Sí, pero solo para ciertos servicios.

[ ] No, será una red local independiente.

Detalle: Se debe tener interconexión entre los campus de la Universidad con el campus principal, donde tendrá acceso a todos los servicios.

4. ¿Qué marca o sistema operativo de red utilizan los equipos de borde en este campus para levantar la VPN?

Como UPEC tenemos el equipo Fortigate 1100E, el cual actúa como Firewall con dos enlaces redundantes y una IP pública Virtual.

5. En caso de integración con la sede principal, ¿CEDIA impone algún protocolo de enrutamiento dinámico específico que debamos replicar en el simulador?

Respuesta: Como dirección de TIC, no se tiene injerencia en los equipos de CEDIA, pero ellos manejan XXXXXX en la interconexión de los equipos de red propios de ellos.

6. ¿Qué segmento de red se tiene previsto asignar al pool de usuarios remotos para evitar conflictos con el direccionamiento local y el de CEDIA?

Rango IP / Máscara: Para cada uno de los campus y sedes de la Universidad se utilizan diferentes pools de dirección:

- Campus Tulcán: 172.20.0.0/16
- Campus Cayambe: 172.21.0.0/16
- Campus Huaca 172.22.0.0/16
- Campus Santa Marta de Cuba: 172.23.0.0/16

El resto de campus a crearse deberán incrementar el segundo octedo dentro de la red de Ip privada 172.x.x.x

7. ¿Cuánto ancho de banda del enlace actual del campus se estima destinar o limitar para soportar el tráfico de esta nueva VPN?

Respuesta: El AB del campus principal es de 2.2Gbps, y para los enlaces VPN, estarán ligados a la capacidad que brinden los equipos de borde, donde se configurarán las VPN S2S

8. En un escenario de alta demanda, ¿cuántos usuarios concurrentes estiman que se conectarán simultáneamente a través de este nuevo túnel?

Este valor es incierto, ya que depende de la cantidad de usuarios que existan en cada campus, y a los servicios que vayan a acceder. Al no tener VPNs implementadas no podemos determinar el número de usuarios simultáneos.

9. ¿Qué tecnología o protocolo de túnel VPN prefieren implementar para este acceso?

Para este proceso es necesario la implementación de Túneles Ipsec Site to Site, debido a que cada campus tendrá su equipo de seguridad perimetral

10. Para la autenticación de los usuarios que se conecten, ¿se utilizará un directorio local del router, o se integrará con un servidor existente?

No es necesario la implementación de autenticación, debido a que los túneles serán Site to Site, y los equipos perimetrales de seguridad son los encargados de realizar dicha autenticación.

11. ¿Cuáles son los 2 o 3 sistemas o servidores internos críticos a los que el túnel VPN debe garantizar acceso prioritario?

Los servicios son:

- Cloud Oracle, donde se encuentra el portafolio institucional y sistema integrado
- Telefonía IP
- CCTV

12. ¿Cuáles son las políticas de restricción de acceso más importantes que debemos programar en el firewall/router para los usuarios que entren por esta VPN?

Las políticas son implementadas en cada uno de los firewalls, dependiendo de los servicios a acceder. Estas configuraciones se las realiza con el Administrador de Redes y Telecomunicaciones.