# Diseño De Una Red Privada Virtual (VPN) Que Garantice La Interconexión De Servicios Internos En Los Diferentes Centros De Atención Universitaria De Colombia Para La Universidad Santo Tomás

Juan Camilo Cuervo López

Trabajo de Grado para Optar por el Título de Especialización En Gestión De Nuevas Tecnologías En Telecomunicaciones

Director

Ing. William Fabián Chaparro Becerra

Facultad de Ingeniería Electrónica

División de arquitectura e Ingenierías

Especialización en Gestión de las Nuevas Tecnologías de las Telecomunicaciones

Universidad Santo Tomás

Seccional Tunja

Bogotá, Colombia

2025

**Contenido**

## Índice de tablas

## Índice de Figuras

**Resumen**

El proyecto garantizó la conectividad segura y eficiente en la Universidad Santo Tomás mediante el diseño de una Red Privada Virtual (VPN) autogestionada, que permitió conectar servicios internos en sus Centros de Atención Universitaria (CAU) a nivel nacional. La necesidad de unificar procesos y mejorar la accesibilidad a recursos tecnológicos internos dio como iniciativa poder comunicarse hacia recursos propios que están de manera interna como lo es software académico y servicios de comunicación de voz, los cuales presentan inestabilidad de acceso y una administración descentralizada. la puesta en marcha de esta VPN permitió centralizar la administración y configuración de recursos, se busca reducir costos operativos asociados a servicios tercerizados por proveedores y mejorar la calidad del servicio ofrecido a la comunidad universitaria, siguiendo la Estrategia Institucional 2024-2028 ECOS 5 de la universidad, que busca ser un ecosistema educativo multicampus incluyente e innovador.

Dentro del desarrollo general del proyecto incluye el diagnóstico de la red actual para identificar necesidades específicas, por medio del diseño se definieron topologías, equipos y protocolos de seguridad (como IKEv2/IPsec), la implementación piloto es fundamental en uno de los CAU para validar el funcionamiento, y un posterior despliegue y escalamiento a nivel nacional. El desarrollo logró una reducción significativa en los costos operativos, un aumento en el uso remoto de recursos por parte de estudiantes y personal administrativo, y una mejora en la atención oportuna de los usuarios gracias a la proactividad ante incidentes que puedan surgir.

## Introducción

La interconexión de forma segura entre diferentes sitios es, actualmente, uno de los puntos más relevantes de las organizaciones. La necesidad de que muchas instituciones educativas puedan interconectar sus recursos tecnológicos es un gran desafío, y más cuando se trata de poder interconectar recursos a nivel nacional, donde se dificultan la administración e integración de servicios. Con la puesta en marcha de una red privada (VPN) se garantizó la conexión segura entre diferentes sedes, así como el acceso a recursos tecnológicos internos de la institución, como software académico. También se contó con una administración centralizada de todo dispositivo tecnológico en las diferentes sedes o centros de atención universitaria, como lo es la Universidad Santo Tomás.

Una solución tecnológica que garantice interconexión y seguridad ofrecerá que las actividades académicas y administrativas se realicen de forma centralizada. Poder interactuar con diferente recurso interno propio de la universidad es de gran ayuda para toda la parte académica, administrativa y financiera de la institución, con lo cual se busca reducir costos operativos y mejorar la entrega de servicio al usuario final. Diversos estudios demuestran impactos positivos en la implementación de VPNs en instituciones de educación superior.

# Capítulo 1

## Objetivos

### Objetivo General

Diseñar una solución de una Red Privada Virtual (VPN) con la cual se tenga una autogestión que permita ser segura y escalable, donde se pueda centralizar la conectividad entre los diferentes Centros de Atención Universitaria (CAUS) de la Universidad que se encuentran ubicados a nivel nacional, garantizando la interconexión eficiente de los servicios académicos y administrativos, permitiendo también la reducción de costos operativos y la mejora de la calidad del servicio que se presta a los usuarios.

### Objetivos específicos

Diagnosticar el estado actual de la red a nivel de infraestructura, donde se puedan evaluar las necesidades específicas de conectividad a recursos tecnológicos (software, servicios internos de telefonía, impresoras) que permitan la administración centralizada de los diferentes recursos para los diferentes CAU de la Universidad Santo Tomás.

Diseñar un esquema de red para la solución VPN en los Centros de Atención Universitaria (CAU), seleccionando topologías, equipos a usar, protocolos de seguridad (IKEv2/Ipsec) que sean más adecuados para garantizar la seguridad, confidencialidad, integridad, escalabilidad y calidad del servicio.

Implementar en uno de los CAU el diseño planteado con el fin de validar el funcionamiento, realizando configuraciones en los equipos y enlaces para así realizar pruebas iniciales de conectividad y luego poder desplegar a nivel nacional la solución planteada.

Evaluar el funcionamiento de conectividad de la red en cuanto a rendimiento y seguridad para así validar los impactos operativos a nivel de costos y satisfacción del usuario que usa el servicio.

# Capítulo 2

## Cuerpo Del Trabajo

### Marco Referencia

#### *Revisión Literaria*

La evolución tecnológica constante que se presenta en el mundo ha llevado a traer el concepto y origen de las VPNs, Redes Privadas Virtuales. (Palo Alto Networks, s.f.) señala que estas surgen en la década de 1990 con la introducción del protocolo HTTP, lo cual dio origen a lo que se conoce como (WWW) World Wide Web, donde comunicarse de forma segura se ha convertido en una necesidad, lo que impulsó al desarrollo del cifrado a nivel de capa IP, con lo cual se dio origen a lo que se conoce como (VPN).

Las VPN, en la actualidad, tienen un uso fundamental en cuanto al ámbito educativo y administrativo para algunas organizaciones. Hoy en día, no solo se usan para generar una conexión remotamente, sino para consumir diversos recursos de forma eficaz y rápida.

De acuerdo con (Stallings 2020), la red privada virtual (VPN) ofrece una solución atractiva para los administradores de red, pero el administrador se enfrenta a un requisito fundamental, que es la seguridad, (Stallings 2020) nos menciona que, gracias a mecanismos de seguridad de cifrado como lo es IPsec, tiene la capacidad de generar túneles seguros, con lo cual adoptar esta práctica proporciona una adopción segura en diferentes organizaciones (p. 485).

El propósito de una VPN es garantizar la privacidad, integridad y confidencialidad de la información que se transmite. De esta forma, se logra que personas externas realicen alguna conexión accediendo a recursos críticos donde se pudiera alterar la información. Según (Kagan 1998), muchas empresas, al pensar en la seguridad, se preocupan por los proveedores de servicios externos, los cuales permiten el tráfico por sus redes públicas; pero las redes privadas virtuales con enrutamiento IP permiten

a las empresas mantener el control del tráfico, así la comunicación se enrute por redes públicas, lo que garantiza que la calidad del servicio y el rendimiento de la red sea óptimo y seguro.

***Sistematización comparativa con los casos de referencia***

**Tabla 1**

*Comparación con casos de éxito*

| Característica | Universidad Nacional de Loja (Ecuador) | Universidad Distrital (Colombia) | Investigación a Entornos Universitarios (Tay et al., 2024) |
|---|---|---|---|
| Institución/Tipo | Universidad | Universidad | Investigación |
| Objetivo Principal | "Solucionar el acceso remoto a bases de datos científicas interna." [a] | "Permitir el acceso a recursos locales (carpetas, aplicaciones) y de otras entidades." [b] | "Implementar una VPN segura y de buen rendimiento para diversos usuarios." [c] |
| Tipo de Conexión/Solución | "VPN diseñada internamente." [a] | "Conexión Sitio a Sitio a través de su red UDNET." [b] | "VPN implementada mediante un dispositivo MikroTik." [c] |
| Metodología Utilizada | "4 fases: Análisis, Diseño, Creación de escenario de prueba, Evaluación." [a] | "Procedimientos en la gestión de usuarios y control de acceso." [b] | "PPDIOO (Prepare, Plan, Design, Implement, Operate, Optimize)." [c] |
| Tecnologías/Protocolos Clave | "Herramientas Open Source para el diseño de VPN." [a] | "Red UDNET (no se especifican protocolos VPN)." [b] | "Dispositivo MikroTik, protocolo de seguridad IKEv2." [c] |
| Resultado Destacado | "Solución óptima y viable para conexiones remotas con fines académicos." [a] | "Acceso controlado y seguro a recursos; guías de soporte para la instalación de sus VPN." [b] | "Solución segura, de buen rendimiento, y compatible con múltiples plataformas (Android, iOS, Windows)." [c] |
| Alcance/Contexto | "Caso de éxito internacional, contexto latinoamericano." [a] | "Caso de éxito nacional (Colombia)." [b] | "Propuesta como alternativa moderna para diferentes universidades." [c] |

*Nota*. [a] (Andrés 2016). [b] (Distrital, 2021). [c] (Tay et al., 2024)

Usar Redes Privadas Virtuales (VPN) permite contar con varias capacidades claves, las cuales se muestran en estudios de investigación y casos de éxito. Al contar con Interconexión Segura entre Sitios (Site-to-Site) se busca no solo conectar usuarios individuales, sino también redes enteras. La Universidad Distrital (Distrital, 2021) implementó una conexión Sitio a Sitio, lo cual permitió interconectar diferentes campus. Se busca un acceso Seguro a Recursos Internos. La Universidad Nacional de Loja (Andrés, 2016) implementó una VPN para dar acceso remoto a sus bases de datos científicas, lo cual facilitó las actividades académicas. De igual forma, lo hizo la Universidad Distrital (Distrital, 2021), donde utilizó su VPN para que el personal lograra acceder a recursos locales de la institución. En cuanto a los controles de acceso y seguridad, se utilizaron protocolos actualizados y robustos como IKEv2, donde solo con autorización de acceso se puede tener alcance a recursos digitales (Distrital, 2021; Tay et al., 2024). Una solución VPN busca tener Flexibilidad Multiplataforma y Modernización. La investigación de Tay et al. (2024) demostró una implementación de VPN accesible desde plataformas como Android, iOS y Windows.

**Desafíos Identificados e innovación**

Entre los diferentes retos se encuentra poder extender diversos programas, académicos para estudiantes en los diferentes CAU, sin necesidad de trámites presenciales en la universidad o tener que realizar diferentes solicitudes para poder acceder a un recurso. Se busca garantizar que los estudiantes puedan acceder en línea a los servicios necesarios para alcanzar sus objetivos académicos. Para la Estrategia Institucional 2024–2028 ECOS 5, se promueve un modelo educativo multicampus, incluyente, sostenible e innovador, estructurado en cinco ejes estratégicos: (Dirección de Comunicaciones, 2024).

Se busca fortalecer las estrategias de la universidad por medio de 5 megas, las cuales son:

- M1 Ecosistema Multicampus
- M2 Ecosistema Sostenible y Sustentable
- M3 Ecosistema para el Buen Vivir

- M4 Ecosistema de Disrupción Educativa
- M5 Ecosistema para Todos.

**Articulación de la Propuesta de VPN con las Estrategias Institucionales de la Universidad Santo Tomás**

La Universidad Santo Tomás, en su Plan General de Desarrollo, ha definido cinco megas estratégicas bajo el proyecto ECOS-5, cuyo propósito superior es: "Ser un ecosistema educativo multicampus incluyente con proyección latinoamericana que se fundamenta en prácticas sostenibles e innovadoras en lo académico y administrativo, para impulsar el crecimiento individual, institucional y de los territorios, con una formación integral que no solo promueva el intelecto, sino que también conecte con el entorno y la felicidad". (Universidad Santo Tomás, 2024).

La implementación de una red privada virtual (VPN) institucional se alinea con este propósito al proporcionar una infraestructura tecnológica que facilita el acceso seguro y eficiente a los recursos académicos y administrativos, fortaleciendo así la conectividad entre las diferentes sedes y centros de atención universitaria (CAUs), y promoviendo la inclusión y equidad en el acceso a la educación.

**Modelos de acceso granular**

Un ISP puede ofrecer servicios de VPN y colocarlos en funcionamiento conectando diferentes redes, pero lo que se busca no es solo generar una conexión, sino que la universidad implemente:

- Una gestión centralizada de múltiples sedes como los Centros de Atención Universitaria (CAU), y por medio de lo anterior lograr mantener los estándares para una nueva acreditación.
- Escalabilidad dinámica para eventos académicos masivos, donde se integren estudiantes a nivel nacional a participar de eventos que realice la universidad.
- Mejorar la calidad del servicio que se presta por medio de QoS, priorizando las videoconferencias y todo tipo de material educativo.

- Contar con auditorías periódicas cumpliendo estándares como ISO/IEC 27032.
- Poder certificar la universidad en ISO 27001 versión 2022, o cumplir con los requisitos que esta exija para su debida certificación.
- Tener acceso a salas de cómputo de forma remota en horarios que el estudiante desee, con el fin de acceder a recursos de software académico necesario para el desarrollo de clases, investigaciones o proyectos de grado, entre otros.
- Transmitir servicios de voz, videos y datos para que usuarios de los centros de atención universitaria (CAUs) tengan comunicación de forma rápida con la sede principal de la universidad, permitiendo de esta forma cumplir con actividades administrativas y dar un servicio óptimo al estudiante.
- Al contar con un control y personalización de los servicios, la institución podrá tener control total sobre la infraestructura y seguridad de las VPN, lo que facilitará que se pueda adaptar a necesidades que se soliciten, lo cual es de gran importancia en la operación diaria para no depender de un ISP cuando realiza configuraciones estándar.
- Para solucionar el tema de latencia, retardos y acceso a infraestructuras del ISP, se tiene actualmente contratado un servicio de SOC (Centro de Operaciones de Seguridad), al cual se agregará solo la supervisión de los canales de internet. Además, se cuenta con recurso humano desde la universidad, que estará encargado de forma continua del servicio de VPN y, en conjunto, llegado el caso de no tener servicio, la idea es actuar proactivamente. Por otra parte, los canales actuales se ampliarán a 100 Mbps, esto debido a que actualmente existen unos de 20 y 50 Mbps; de esta forma se soluciona el tema de latencia.
- La universidad contará con un aplicativo para reportar casos en caso de caída del servicio de internet, debido a que este servicio sí depende de un proveedor externo y, por tal motivo, es imposible poder gestionar el servicio de internet internamente, debido a que la universidad no es

un proveedor de ISP. Por lo cual se cuenta con tiempos de respuesta y atención 24/7 para solucionar caídas en la mayor brevedad.

- A diferencia de un ISP comercial, la universidad está orientada a cumplir con estándares de calidad y estrategias, como lo es la Estrategia Institucional 2024–2028 ECOS-5, la cual busca "Ser un ecosistema educativo multicampus incluyente con proyección latinoamericana que se fundamenta en prácticas sostenibles e innovadoras en lo académico y administrativo, para impulsar el crecimiento individual, institucional y de los territorios, con una formación integral que no solo promueva el intelecto, sino que también conecte con el entorno y la felicidad" (Dirección de Comunicaciones, 2024).

**Sostenibilidad económica**

Uno de los principales desafíos para la universidad es lograr un equilibrio entre costo y beneficio, especialmente en la mejora de sus servicios. Se busca evitar el pago a un proveedor externo (ISP) por el servicio de VPN, optando, en su lugar, por una implementación propia mediante dispositivos como MikroTik. Estos equipos permiten establecer conexiones seguras y confiables, lo que representa una solución más económica y eficiente. De esta manera, se eliminan costos asociados al mantenimiento de servicios y dispositivos innecesarios, generando así beneficios directos para la universidad.

## Criterios de selección de tecnologías (IKEv2, IPsec)

IKEv2 es el protocolo más reciente de claves criptográficas para la configuración de VPN, se caracteriza por:

- Conexiones móviles estables: Al cambiar de red sin interrumpir la conexión, permite establecer una VPN activa así se cambie de IP lo cual es ideal para los usuarios para que puedan mantener sus conexiones
- Seguridad: Utiliza cifrados avanzados (AES, SHA-2) y certificados X.509 para autenticación y cifrado seguro.

- Amplia compatibilidad: Funciona en sistemas operativos (Windows, macOS, iOS) entre otros.
- Eficiencia de recursos: El consumo de ancho de banda es mínimo al igual que recursos del dispositivo, lo que representa ventajas para conexiones limitadas.

IPsec también es un protocolo que proporciona seguridad a nivel de red, cifrado y autenticación, se caracteriza por:

- Protocolo estándar y valido: al ser un estándar internacional se puede garantizar su confiabilidad.
- Túneles seguros: Se establecen túneles seguros que garantizan la confidencialidad e integridad de la información
- Flexibilidad operativa: Tiene la capacidad de operar en modo transporte o túnel.
- Compatibilidad: Tiene la capacidad de funcionar con IKEc2 lo cual es ideal para gestionar eficiente claves y protección de datos integral.

## Inclusión de Normativas Actuales de Ciberseguridad Educativa

### *NIST*

La estructura del marco de Ciberseguridad del NIST 2.0 permite enfocar e integrar la seguridad de las Redes Privadas virtuales (VPNs) en la educación superior (Coro, 2024).

Esta guía orienta a la gestión de riesgo en la ciberseguridad donde se busca reducir riesgos y ayudar a proteger las redes y datos, para lo cual existen seis pilares funcionales (Gobernar, Identificar, Proteger, Detectar, Responder, Recuperar) (National Institute of Standards and Technology, 2024).

**Tabla 2**

*Análisis NIST*

| Pilar del NIST 2.0 | Descripción y Aplicación a VPNs en Educación Superior |
|---|---|
| Gobernar | El liderazgo institucional debe definir la estrategia de ciberseguridad.<br>Es necesario asignar responsabilidades y crear políticas claras.<br>La seguridad de VPNs debe ser organizacional. |
| Identificar | Determinar qué usuarios necesitan acceso VPN y qué datos manejan.<br>Realizar análisis de activos y riesgos para diseñar una infraestructura segura. |
| Proteger | Implementar autenticación fuerte (como MFA).<br>Utilizar cifrado en tránsito y controles de acceso.<br>Establecer políticas de control de acceso según el rol. |
| Detectar | Identificar accesos no autorizados o tráfico anómalo.<br>Utilizar monitoreo continuo para detectar actividades sospechosas en la red VPN. |
| Responder | Desarrollar un plan de respuesta a incidentes orientado a VPNs.<br>El plan debe incluir contención, análisis, mitigación y comunicación ante incidentes. |
| Recuperar | Diseñar planes de resiliencia para asegurar la continuidad operativa.<br>Establecer procedimientos de respaldo y restauración de la infraestructura VPN. |

*Nota*. Aplicación de los pilares del NIST 2.0 a las VPNs en Educación Superior

Por medio de documentos como SP 800-77 se guía sobre las mejores prácticas en la puesta en marcha de VPNs seguras, al igual que el uso de mecanismos criptográficos (NIST SP 800-171) son primordiales. (Barker et al., 2020; Ross & Pillitteri, 2024)

**ISO/IEC 27032**

La ISO/IEC 27032 es un marco el cual proporciona directrices con el fin de mejorar la ciberseguridad. Su objetivo principal es la seguridad de internet, para lo cual es importante tener en

cuenta el diseño de la seguridad y la implementación de las VPNs en instituciones de educación superior (AENOR, 2023).

***Seguridad en internet***

La norma indica que la comunicación por medio de VPNs es importante para asegurar la comunicación por internet, especialmente en entornos de acceso remoto. La norma también sitúa las VPNs en el contexto global de amenazas en Internet (PMG SSI, 2023).

**Evaluación y tratamiento de riesgos**

La norma enfoca la gestión del riesgo basada en:

- Identificación de amenazas y vulnerabilidades en las VPNs
- Gestionar riesgos como lo es software desactualizado, métodos de autenticación poco robustos
- Hay que asegurar que se cuente con monitoreo continúo, implementado controles de seguridad adecuados (PMG SSI, 2023).

***Colaboración interinstitucional segura***

La importancia del teletrabajo colaborativo seguro es algo importante dentro de la norma, donde se resalta la importancia que las VPNs deben permiten el intercambio seguro de información entre diferentes proveedores de la academia, buscando de esta forma un trabajo colaborativo y el intercambio de información seguro (PMG SSI, 2023).

**Controles técnicos y buenas prácticas**

La norma puede guiar para que en instituciones de educación superior se pueda tener una implementación de codificación segura donde se busca un monitoreo constante al tráfico VPN, controlando o administrando niveles de acceso a recursos como servidores VPN, donde se busca que los usuarios finales puedan comprender sobre el uso seguro de VPNs y que les permita comprender ataques como el phishing (Arévalo, 2020/2025).

**Análisis de Riesgos Asociados a la Autogestión de VPNs**

***Brechas de seguridad***

Algunas brechas de seguridad que podrían surgir al tener el servicio autogestionado son:

- Riesgo: Se pueden presentar malas prácticas como configuraciones incorrectas por no conocer adecuadamente el producto, algunas actualizaciones para el firewall no pueden ser las más adecuadas
- Mitigación: Implementar auditorias constantes a nivel de configuración, contar con procedimientos de implementación y documentación del proyecto.

***Administración de credenciales***

- Los riesgos presentados en la administración de credenciales pueden estar asociados a perdida de las credenciales, manejo inadecuado de credenciales facilitando el acceso a terceros
- Mitigación: Actualizar servidor de contraseñas donde solo se tiene acceso a personal autorizado utilizando clave de acceso con doble factor de autenticación (2FA).

***Continuidad del servicio***

- Riesgo: Falla en el servicio de internet por parte del ISP en los dispositivos que son propiedad del proveedor o malas configuraciones que puedan afectar el servicio.
- Mitigación: Actualmente se cuenta con un SOC donde se cuenta con el monitoreo contante del servicio de internet, ante cualquier falla esta se estará informando vía correo o teléfono, también se cuenta con servicio de infraestructura UPS, en caso de cortes de energía esta entrará en funcionamiento también se tendrá un monitoreo constante desde la sede central.

## Articulación de la Propuesta con los ODS de la Agenda 2030

### *ODS 4: Educación de Calidad*

El Objetivo de Desarrollo Sostenible 4 consiste en garantizar una educación inclusiva, equitativa y de calidad, y promover oportunidades de aprendizaje durante toda la vida para todos (Naciones Unidas, s.f.).

### *ODS 4: Metas*

#### Meta 4.3: Acceso equitativo a educación de calidad

El acceso a plataformas virtuales (Moodle, software institucional) garantiza seguridad y equidad (Naciones Unidas, s.f.).

#### Meta 4.4: Aumentar las competencias técnicas y profesionales

Por medio del aprendizaje a distancia se fortalecerá competencias mediante tecnologías seguras y accesibles.

#### Meta 4.a: Instalaciones con entornos de aprendizaje seguros

Establecer entornos de aprendizaje mediados por tecnologías segura que permitan ayudar a personas con discapacidad y las diferencias de género. (Naciones Unidas, s.f.).

El Objetivo de Desarrollo Sostenible 9 consiste en construir infraestructuras resilientes, promover la industrialización sostenible y fomentar la innovación (Naciones Unidas, s.f.).

### *ODS 9: Industria, Innovación e Infraestructura*

#### Meta 9.4. Recursos Sostenibles Mediante Tecnologías Limpias y Sostenibles

El uso de soluciones VPN modernas y sostenibles ayudará a reducir costos y dependencia de terceros. (Naciones Unidas, s.f.).

**Meta 9.b y 9.c: Apoyar La Innovación Local y Mejorar El Acceso a TIC**

Fortalecer la infraestructura tecnológica universitaria para impulsar la transformación digital. (Naciones Unidas, s.f.).

**Análisis Comparativo con otras tecnologías**

**Tabla 3**

*Análisis con otras tecnologías*

| Tecnología | Seguridad | Rendimiento | Costo | Escalabilidad | Ideal para |
|---|---|---|---|---|---|
| **VPN** | Media | Variable | Bajo | Media | Acceso remoto |
| **MPLS** | Alta | Alta | Alto | Media | Sedes críticas, QoS garantizada |
| **SD-WAN** | Alta | Alta | Medio | Alta | Redes híbridas, multinube, sedes dispersas |
| **ZTNA** | Muy alta | Alta | Variable | Alta | Acceso seguro a apps específicas |
| **SASE** | Muy alta | Alta | Variable | Muy alta | Transformación digital, seguridad cloud-native |
| **Leased Line** | Alta | Muy alta | Muy alto | Baja | Comunicación directa, tiempo real crítico |
| **Metro Ethernet** | Alta | Alta | Medio | Alta | Sedes urbanas/interconectadas regionalmente |

*Nota.* Comparación de tecnologías de conectividad en redes empresariales

**Tabla 4**

*Análisis comparativo VPN vs MPLS*

| Parámetro | VPN | MPLS |
|---|---|---|
| **Costo** | Menores costos de implementación y operación; aprovecha la infraestructura de internet existente. | Mayores costos de implementación y operación; requiere líneas arrendadas dedicadas y hardware especializado. |
| **Seguridad** | Fuertes protocolos de cifrado (p. ej., IPsec, OpenVPN); la seguridad depende de la solidez del cifrado y la confianza en el proveedor. | Privacidad inherente debido a la infraestructura de red privada; sin cifrado predeterminado; requiere seguridad física. |
| **Rendimiento** | El rendimiento depende de la conexión a internet subyacente; potencial de latencia y jitter. | Rendimiento predecible y fiable; baja latencia y jitter para tráfico prioritario; sólido soporte QoS. |
| **Flexibilidad/Escalabilidad** | Altamente flexible y escalable; se adapta fácilmente a usuarios remotos y cambios en el tamaño de la red. | Flexibilidad y escalabilidad limitadas; agregar nuevos sitios o aumentar el ancho de banda puede ser costoso y llevar mucho tiempo. |
| **Gestión/Implementación** | Relativamente fácil de implementar y gestionar, especialmente con clientes basados en software y gestión centralizada. | Implementación y gestión complejas; a menudo requiere experiencia especializada de proveedores de servicios. |

*Nota.* Comparación detallada entre VPN y MPLS.

La propuesta de una solución de conectividad VPN, en comparación con otras tecnologías se debe a:

***Rentabilidad Superior***

Reducir en gran escala costos frente a tecnologías como MPLS y SD-WAN, al eliminar la necesidad de líneas arrendadas o dedicadas (Ramírez Páez, 2018, p. 22).

Contar con infraestructura existente como firewall, sin requerir licencias o hardware adicionales (Ramírez Páez, 2018, pp. 56, 77).

Existen algunos costos asociados por certificados, pero son inferiores a los de soluciones dedicadas (Ramírez Páez, 2018, p. 51).

MPLS presenta altos costos de conectividad y operación (Moreno Alayón, 2021, pp. 31-32). La VPN es más accesible también frente a Metro Ethernet (Arévalo Méndez et al., 2015).

La VPN se adecúa a la Universidad esto debido al presupuesto limitado (Sheldon, 2022; SolveForce, s.f.).

***Mayor Control y Simplicidad de Gestión***

Con las VPN se puede contar con gestión directa, a diferencia de MPLS, que requiere administración externa. La implementación de las VPN es más sencilla comparada con SD-WAN, ZTNA o SASE, que pueden resultar algo complejos o excesivos para ciertos proyectos (Mavroudis, 2024; Monroy **Zabala, 2024)**. También, no se requieren configuraciones sofisticadas y se permite un despliegue rápido (Proxyium, s.f.; Sheldon, 2022).

***Seguridad Adecuada y Confiable***

Las VPN cuentan con control mediante cifrado como AES y funciones hash como SHA, lo cual garantiza la confidencialidad, integridad y autenticación (Ramírez Páez, 2018, pp. 18-19, 22, 27). Por otra parte, se emplean IPsec/SSL, mecanismos criptográficos robustos incluso en redes públicas (Forero Ortiz, 2014, pp. 16, 25; Cato Networks, 2023; Tech-Latest, 2023). El protocolo IKE facilita la autenticación de pares IPsec y el intercambio seguro de claves (Ramírez Páez, 2018, p. 23).

***Flexibilidad y Escalabilidad***

Las VPN pueden interconectar todas las sedes, incluyendo los CAU (Universidad Santo Tomás, s.f.)**.** Soportando acceso remoto seguro y expansión a nuevas ubicaciones sin necesidad de infraestructura costosa (Forero Ortiz, 2014; Ramírez Páez, 2018; NordLayer, 2024), para entornos de trabajo remoto o híbrido (Hexatronic Data Center, s.f.; Sheldon, 2022).

**Adecuación Específica al Proyecto**

El proyecto se adecúa al uso de VPN, debido a que se busca generar interconexión para los CAUS no cubiertos por MPLS y reducir costos. La posibilidad de control interno y su robusta seguridad lo hace una solución simple y no sofisticada que no requiere mayor complejidad, lo que permite una implementación sencilla frente a las alternativas mencionadas.

# Capítulo 3

## Planteamiento del Problema de Investigación

La Universidad Santo Tomás, buscando la unificación de sus procesos por medio de un ecosistema educativo multicampus (Estrategia Institucional 2024-2028 ECOS 5), cuenta actualmente con diferentes Centros de Atención Universitaria (CAU) a nivel nacional, donde se atienden solicitudes académicas y administrativas. En vista de mejoras en la prestación de servicios internos para la comunidad académica y administrativa, se ha dificultado el acceso en la interconexión de servicios internos como software académico, servicios internos como comunicación de voz, entre otros, los cuales son de vital importancia para el funcionamiento y apoyo de la comunidad universitaria. Adicionalmente, no hay una administración centralizada de los recursos actuales, lo cual está ocasionando malestar en los usuarios cuando intentan comunicarse a la sede principal en Bogotá. Por otra parte, se están generando algunos sobrecostos en los servicios de internet, los cuales se buscan reducir por dependencia de terceros. Esto limita actualmente a la Universidad en poder dar una atención de respuesta rápida y efectiva.

En consecuencia, de lo anterior, se ha visto afectada la cobertura a nivel nacional de los CAU, ya que no todos disponen de los mismos niveles de conectividad. La administración descentralizada provoca que dispositivos como impresoras, teléfonos IP y puntos de acceso no puedan ser configurados, actualizados ni monitoreados adecuadamente. Por otra parte, el incremento de costos operativos derivados de soluciones de un proveedor de servicios de internet (ISP) y de soluciones tercerizadas está dificultando la prestación de soporte oportuno. Finalmente, el desconocimiento sobre el estado actual de la seguridad impide tener claridad sobre las configuraciones activas en los túneles creados.

### *Antecedentes de la Temática*

Las referencias indican que las VPN se utilizan para poder interconectar de manera segura una red privada de cierta organización a usuarios que se encuentran remotamente o en sitios distantes (Andrés, 2016; Distrital, 2021), con el fin de aplicar controles de acceso y mejorar la seguridad de los datos mediante protocolos actualizados (Distrital, 2021; Tay et al., 2024), para ofrecer soluciones de conectividad flexibles y eficientes en entornos multiplataforma (Tay et al., 2024). Una VPN tiene como fin:

- Facilitar el trabajo y estudio remoto
- Proteger la información sensible
- Interconectar redes de forma segura
- Proporcionar una solución de acceso universal
- Implementar soluciones costo beneficios

### *Justificación y Contribución*

Con el diseño del proyecto de una VPN a nivel educativo se solucionará problemas actuales como:

Garantizar la comunicación entre CAUs hacia el campus principal en Bogotá; de esta forma se garantizará tener túneles cifrados en diferentes sitios, con el fin de fortalecer la experiencia académica y administrativa.

Otra de las grandes contribuciones es poder tener de forma centralizada y controlado los diferentes dispositivos y servicios, lo cual permitirá realizar configuraciones y actualizaciones estando virtualmente, lo cual servirá para presentar auditorías y crear políticas de seguridad unificadas en el campus principal, donde se tendrán controles de seguridad que están enfocados a tener una gestión de accesos más precisa y un monitoreo constante. Por otra parte, no depender de un proveedor inicialmente

generará una optimización de costos y la gestión en la operación será mucho más rápida, lo que ayudará en gran medida a dar un buen servicio cuando surjan requerimientos o solicitudes en los diferentes CAUs.

También se busca fortalecer la Estrategia Institucional (ECOS-5), donde por medio de las megas estratégicas Ecosistema Multicampus (M1), Ecosistema Sostenible y Sustentable (M2) y Ecosistema de Disrupción Educativa (M4), se busca mejorar la interoperabilidad y apoyar la innovación educativa. La contribución más importante, y por la que muchas empresas suelen presentar dificultades, es la documentación. En general, es importante dejar todo documentado desde el inicio hasta el final, con el fin de que, para futuras implementaciones, se cuente con una base sobre cómo empezar y se disponga de un caso de éxito que funcione como una guía práctica. Esta guía debe brindar soluciones que no solo sean escalables, sino también adaptables a diferentes escenarios de conectividad.

# Capítulo 4

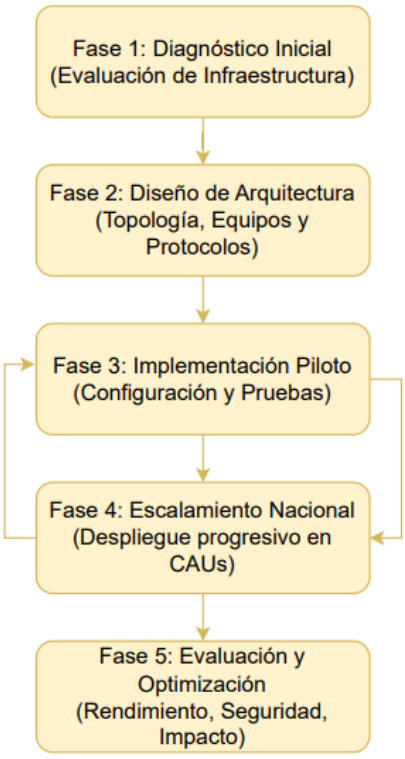
## Justificación de la Propuesta e Identificación y Descripción del Conocimiento que Generará el Proyecto de Investigación

Con el diseño de una red privada virtual (VPN) autogestionada para la Universidad Santo Tomás, se presenta una solución original en cuanto al enfoque de necesidades específicas de la institución a nivel nacional en comparación con soluciones tercerizadas o comerciales. El proyecto busca fortalecer a la Universidad mediante infraestructura propia, segura y escalable, que permita administrar de forma centralizada los servicios académicos y administrativos, permitiendo que la experiencia de estudiantes, docentes y personal sea mucho más amigable y fácil de usar. La propuesta está acorde con la estrategia institucional ECOS-5, donde se aporta directamente a la sostenibilidad, inclusión y transformación digital, al mismo tiempo que responde a los desafíos actuales de conectividad, seguridad de la información y operatividad.

# Capítulo 5

**Figura 1**

*Framework General*




*Nota.* Este modelo permite retroalimentación constante entre etapas, lo cual es clave para mantener la red actualizada, segura y adaptada a nuevas necesidades.

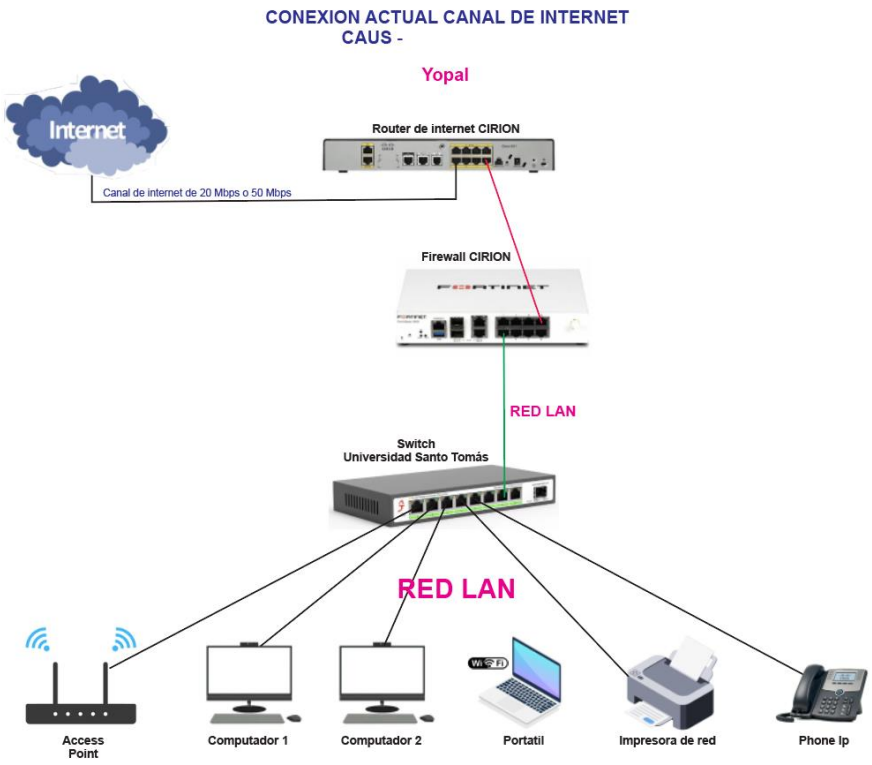
## Materiales y Métodos

### *Fase 1: Diagnóstico del estado actual de la red (Objetivo 1)*

Se realizaron visitas a los Centros de Atención Universitaria (CAU) seleccionados donde se realizarán actividades de diagnóstico actual de la infraestructura

**Figura 2**

*Conexión actual en los diferentes CAU*




*Nota.* El diagrama incluye información de la conexión de los diferentes CAU(https://app.diagrams.net)

La conexión actual en los CAUS está conformada por:

- Un canal de internet de 20 Mbps o 50 Mbps
- Un router de internet propiedad del proveedor Cirion
- Un Firewall Fortinet propiedad de Cirion
- Un switch para la conexión LAN propiedad de la Universidad

- Diferentes dispositivos que se conectan a la red LAN
- La configuración de los dispositivos es igual para todos los CAUS

***Fase 2: Diseño del esquema de red VPN (Objetivo 2)***

En esta fase se desarrolló un diseño lógico y físico de red, se definirán las topologías de red (Site-to-Site), protocolos de seguridad (IKEv2/IPsec).

**Dispositivos y materiales**

**Tabla 5**

*Análisis técnico de equipos*

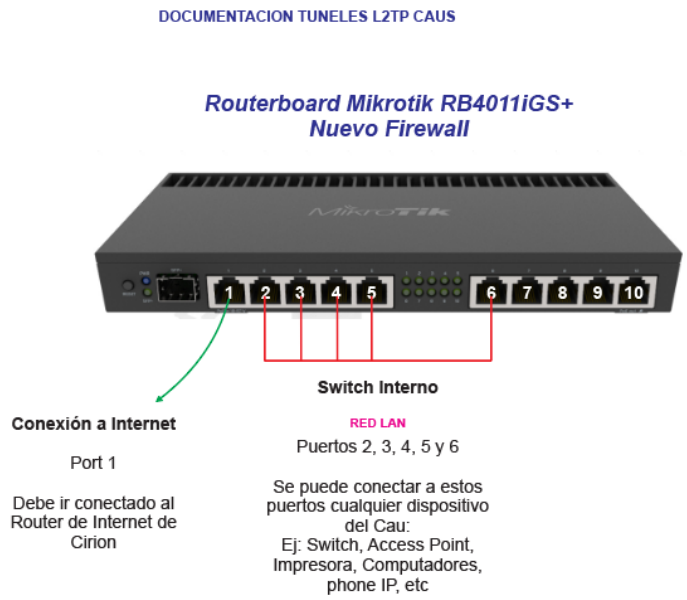
| Característica | MikroTik RB4011iGS+RM | MikroTik CCR2116-12G-4S+ | TP-Link SG3452P |
|---|---|---|---|
| **Tipo de dispositivo** | Router de alto rendimiento | Router central (Core) | Switch administrable con PoE |
| **Precio estimado** | USD $219.00 | USD $995.00 | Aproximadamente USD $600.00 |
| **CPU** | 4 núcleos, 1.4 GHz | 16 núcleos, 2.0 GHz | No aplica (switch) |
| **RAM** | 1 GB | 16 GB | No aplica |
| **Almacenamiento** | 512 MB | 128 MB | No aplica |
| **Puertos Ethernet** | 10 x 1 Gbps | 13 x 1 Gbps | 48 x 1 Gbps |
| **Puertos SFP+ (10G)** | 1 | 4 | 4 SFP |
| **PoE** | Salida PoE pasiva en 1 puerto | No | 48 puertos PoE+ |
| **Consumo máximo de energía** | 18 W | 60 W | 464 W |
| **Sistema Operativo** | RouterOS v7 (Licencia Nivel 5) | RouterOS v7 (Licencia Nivel 6) | Sistema operativo de TP-Link |
| **Enfriamiento** | Pasivo (sin ventiladores) | 4 ventiladores activos | Ventiladores activos |
| **Uso recomendado** | Sedes pequeñas | Centros de datos, diversas conexiones | Redes pequeñas con dispositivos PoE |

| Característica | MikroTik RB4011iGS+RM | MikroTik CCR2116-12G-4S+ | TP-Link SG3452P |
|---|---|---|---|
| **Relación costo-beneficio** | Alta: rendimiento optimo a bajo costo | Muy alta: rendimiento para empresas grandes a menor costo que marcas líderes | Alta: funciones avanzadas a precio competitivo |

*Nota.* Tabla donde se analiza las tecnologías a implementar (https://mikrotik.com/products)

**Figura 3**

*Modelo MIKROTIK RB4011IGS+*




*Nota.* La figura 2 representa el modelo de dispositivo a adquirir (https://mikrotik.com/product/rb4011igs_rm#fndtn-gallery)

Se usarán dispositivos MikroTik RB4011IGS+ los cuales tienen un costo beneficio, debido a su valor comercial y las funciones que trae integradas dentro de las cuales se encuentra las VPN Site to Site, C2S y firewall.

**Figura 4**

*Switch Tp-Link SG3452P*

*Nota.* La figura 3 representa el modelo de switch a implementar (https://www.tp-link.com/co/business-networking/omada-switch-access/tl-sg3452p/)

Se usarán dispositivos switch Tp-Link SG3452P, estos cuentan con alimentación POE para los teléfonos, son dispositivos de 48 puertos a 10/100/1000 Mbps y son administrables para realizar configuraciones en la red LAN, a los puertos se puede conectar Access Point, impresoras, computadores, teléfonos entre otros.

**Figura 5**

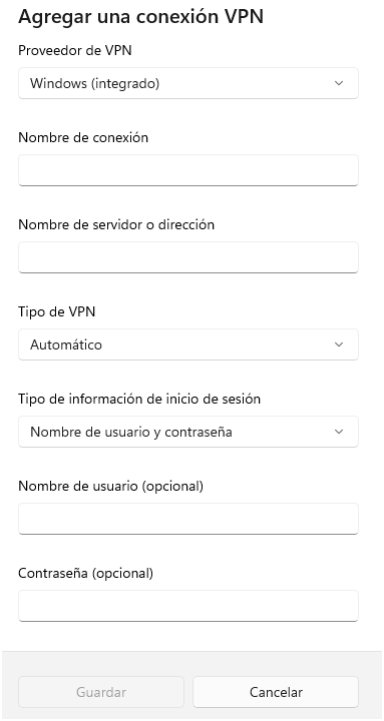
*Modelo MikroTik CCR2116-12G-4S+*

*Nota.* La figura 4 representa el modelo de MikroTik que interconectara todos los CAU https://mikrotik.com/product/ccr2116_12g_4splus#fndtn-gallery

Se tendrá un dispositivo MikroTik CCR2116-12G-4S+ en la sede principal Bogotá de la universidad la cual es la encargada de recibir todas las conexiones de las VPN de los diferentes CAU (Site to Site)

**Figura 6**

*Conexión VPN C2S*

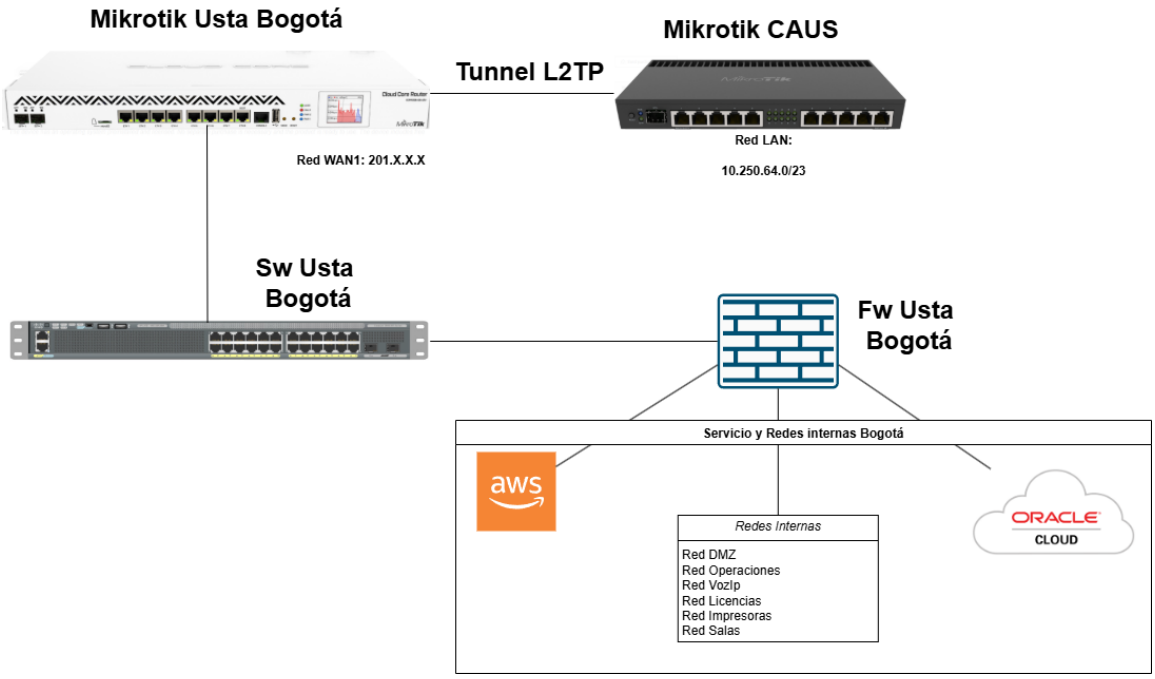



*Nota.* La figura 5 representa la forma de conectividad en dispositivos clientes (https://wiki.upv.es/confluence/display/MANUALES/Windows+-+VPN+con+Microsoft+Windows+11)

Los clientes VPN que se usaran se encuentra integrado dentro de las funciones que tiene Windows, para el caso se realizara la conexión en una computadora con Windows, pero podemos realizar conexiones con otras plataformas como Linux, IPhone, Android entre otras en caso de necesitarse la conexión.

**Figura 7**

*Diagrama de conectividad deseado*




*Nota.* El diagrama incluye información de la conexión de los diferentes CAU a implementar (https://app.diagrams.net)

El diseño anterior es la solución planteada de una VPN que interconectará servicios internos de la Universidad Santo Tomás, donde se podrá tener gestión de los dispositivos y de las diferentes redes que se interconectan, logrando tener una escalabilidad y seguridad al usar protocolos como L2TP-IPsec, tener en cuenta que para este estado los canales se ampliaron a 100 Mbps.

***Fase 3: Implementación piloto de la solución (Objetivo 3)***

**Configuración MikroTik CAU.**

Se seleccionó uno de los CAU para la implementación piloto. Se configurarán routers MikroTik para establecer túneles L2TP-IPsec, reglas de firewall y enrutamientos.

Para la configuración de las VPN se debe tener en cuenta las siguientes configuraciones a nivel de red:

**Tabla 6**

*Configuraciones iniciales*

| **Descripción** | Cantidades/características |
|---|---|
| **Cantidad** | 1 |
| **CAU** | Yopal |
| **ID Servicio** | 81-37ZGUOV |
| **Ip Router Internet** | 8.242.X.X |
| **Ip Fw MikroTik CAU** | 8.242.X.X |
| **Dirección de Red CAU** | 10.250.64.0/23 |
| **Host** | 10.250.64.1 - 10.250.65.254 |
| **Puerta de enlace** | 10.250.64.1 |
| **Total, Hosts** | 510 |

*Nota.* Tabla donde se puede ver la configuración que van a tener todos los CAU

**Tabla 7**

*Configuraciones iniciales*

| **Descripción** | Cantidades/Características |
|---|---|
| **Cantidad** | 1 |
| **CAU** | Yopal |
| **Gw Tunnel VPN L2TP CAU** | 10.52.152.5 |
| **Gw Tunnel VPN L2TP Sede Principal** | 10.52.152.1 |
| **Usuarios VPN de Soporte** | user_prueba |
| **Clave Compartida VPNs de soporte** | Pruebaxxx |
| **Pass VPNs de Soporte** | soporte_prueba |
| **Ip Usuario VPN** | 192.168.10.5/24 |

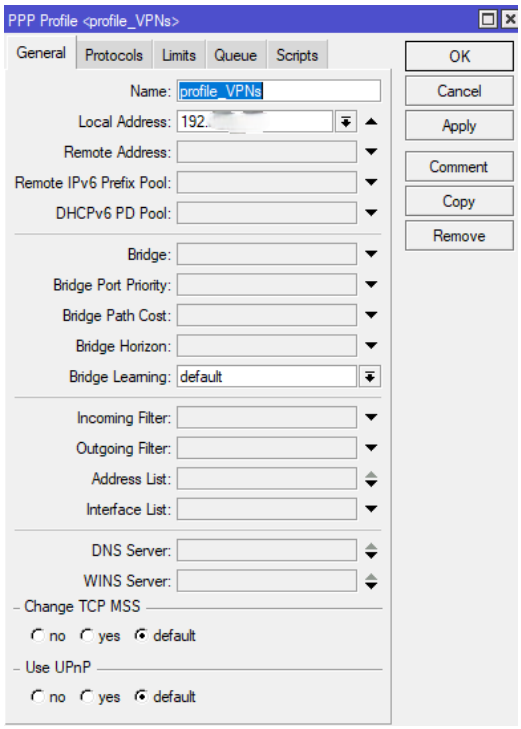
*Nota.* Tabla donde se muestran las configuraciones que va a tener usuarios y claves de conexión

Inicialmente se debe habilitar el servidor L2TP en la MikroTik y configurar algún perfil.

Se realiza la creación del perfil (profile_prueba), se debe establecer una dirección IP en local Address de una subred que no se esté usando en ninguno de los extremos las demás opciones se dejan por default.

**Figura 8**

*Creación de perfil*

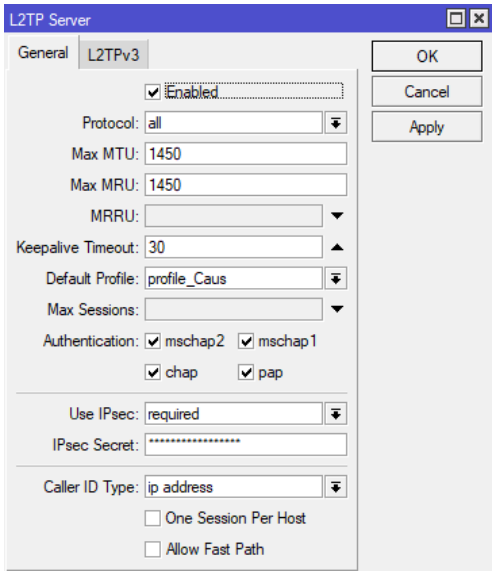



*Nota.* Fuente propia

Se procede habilitar el servidor L2TP, también la opción de usar IPsec y asignamos alguna contraseña las demás opciones la dejamos por default.

**Figura 9**

*Creación L2TP*

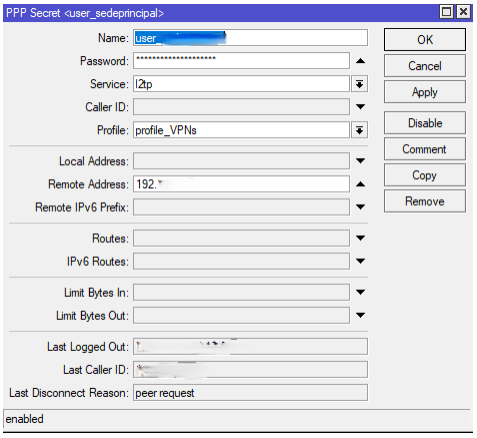



*Nota.* Fuente propia

Ahora se creará el usuario el cual será el encargado de poder conectarse a la MikroTik principal donde se recibirán todas las conexiones, el usuario creado es user_prueba y su contraseña Pruebaxxx a modo de pruebas, en service dejamos l2tp con su respectiva Remote Address donde se asignará una dirección IP del segmento previamente dado.

**Figura 10**

*Creación Usuario*




*Nota.* Fuente propia

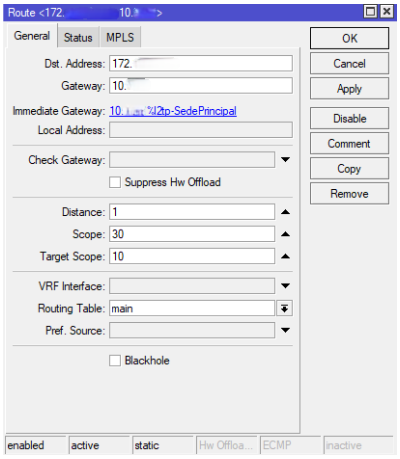
Se creará las rutas estáticas las cuales permitirá encontrar las redes internas que se encuentran en la sede Bogotá.

Se debe crear rutas para las redes:

Red DMZ – Red Operaciones – Red licencias – Red Salas – Red telefonía – Red Impresoras. Nuestro Gateway es el 10.52.152.1 y nuestros destinos son todas las redes internas.

**Figura 11**

*Creación de rutas*

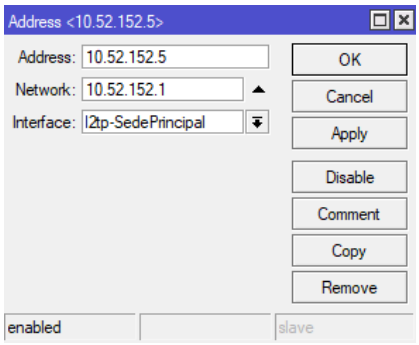



*Nota.* Fuente propia

Se debe proceder con la creación de la red que realizar la conexión contra Bogotá

**Figura 12**

*Creación de red*

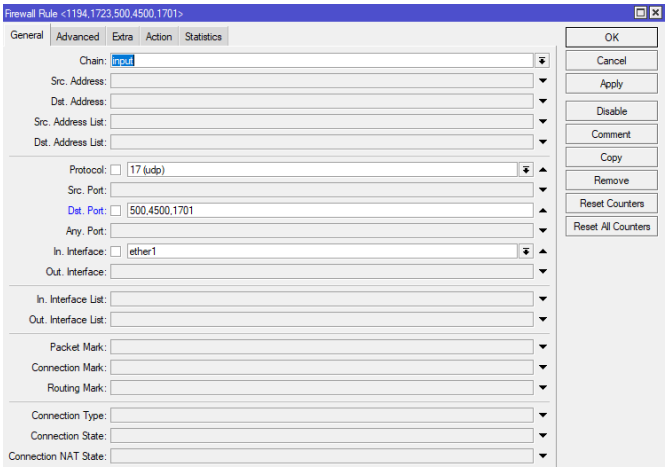



*Nota.* Fuente propia

Se procede con la configuración en el firewall, donde se habilitan los puertos 500, 1701, 4500, por protocolo udp para la conexión de las VPN, también se habilita el protocolo 50 IPsec para cifrar y proteger los paquetes IP en la capa de red.

**Figura 13**

*Creación reglas firewall*

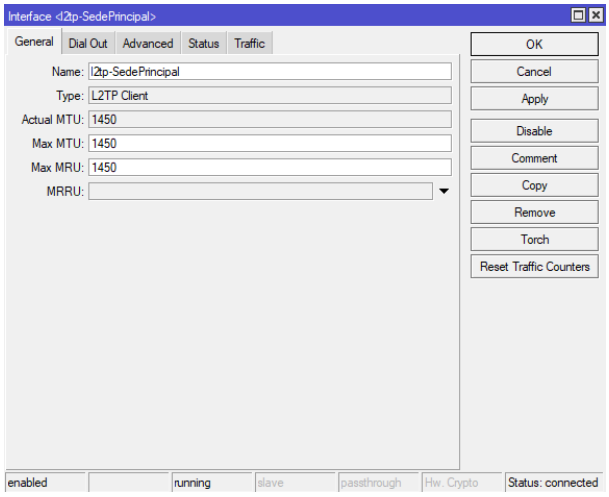



*Nota.* Fuente propia

Ahora se continua con la configuración de una interfaz la cual se conectará con la IP pública de la sede en Bogotá, se colocará el usuario creado en la MikroTik de Bogotá con su respectiva contraseña habilitamos usar IPsec y se colocará la Ipcec Secret. Hasta este punto se terminaría la configuración de la MikroTik de alguno de los CAU.

**Figura 14**

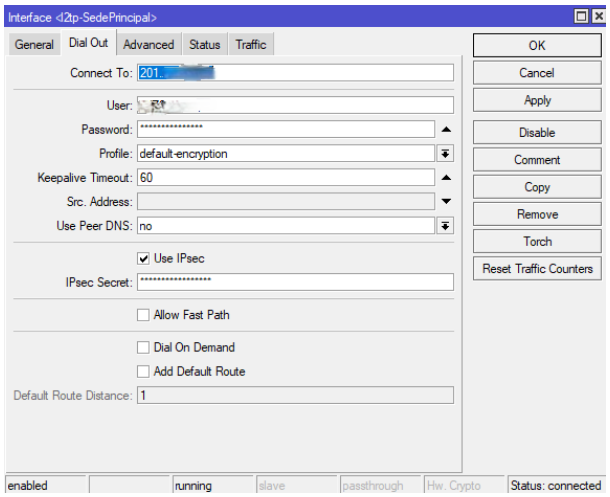
*Creación interfaz*



*Nota.* Fuente propia

**Figura 15**

*Creación interfaz Dial Out*



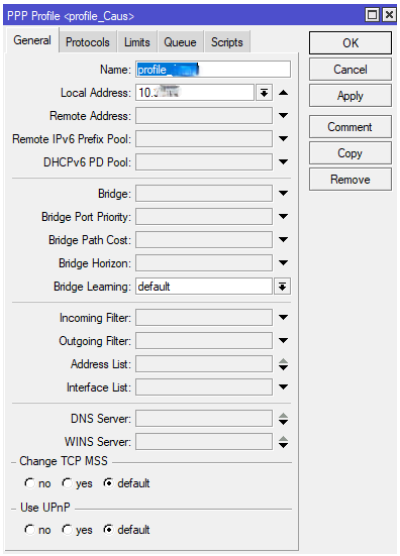

*Nota.* Fuente propia

**Configuración MikroTik Principal Bogotá**

Se procede a configurar el perfil (profile_prueba), se debe establecer una dirección IP en local Address la cual se dio previamente en la configuración que era 10.52.152.1 las demás opciones se dejan por default.

**Figura 16**

*Creación perfil*

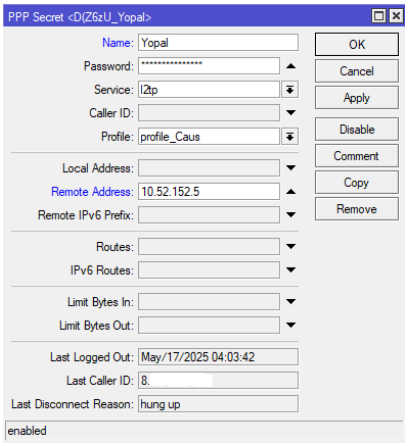



*Nota.* Fuente propia

Procedemos a crear el usuario secreto que se usara en la MikroTik de algún CAU, es importante definir un nombre en este caso es Yopal y su Remote Address 10.52.152.5

**Figura 17**

*Creación usuario secreto*

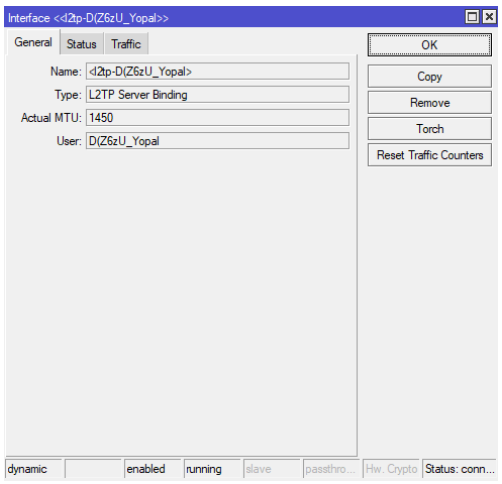



*Nota.* Fuente propia

Se realiza la creación del L2TP server Binding el cual usaremos para la creación de nuestra red de conexión.

**Figura 18**

*Creación L2TP*

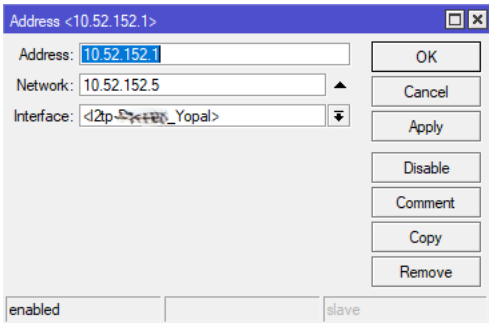



*Nota.* Fuente propia

Posteriormente se procede con la creación de la red en la MikroTik de Bogotá esta red es la que tendrá alcance y conexión hacia la MikroTik de Yopal, la interface a seleccionar es la previamente creada.

**Figura 19**

*Creación red*

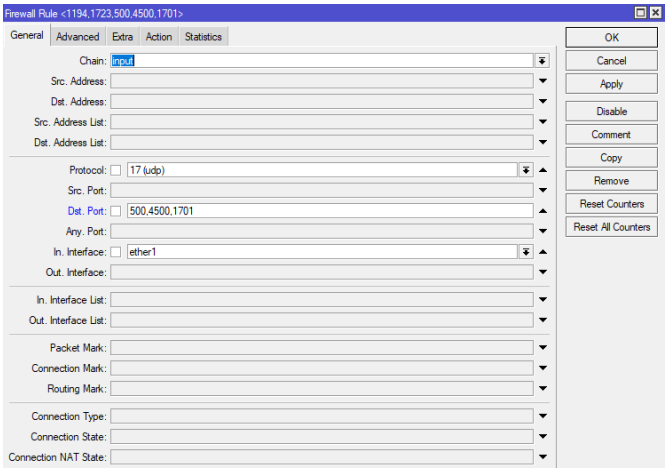



*Nota.* Fuente propia

Al igual que en la MikroTik anterior se procede a permitir los puertos y protocolos, donde se habilitan los puertos 500, 1701, 4500, por protocolo udp para la conexión de las VPN, también se habilita el protocolo 50 IPsec para cifrar y proteger los paquetes IP en la capa de red.

**Figura 20**

*Creación reglas firewall*

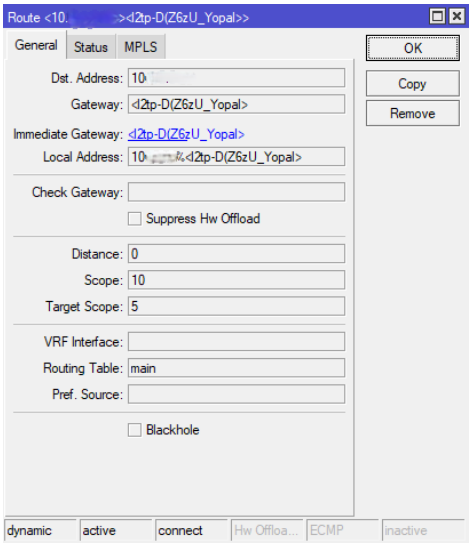



*Nota.* Fuente propia

Se procede a configurar nuestras rutas en la MikroTik de Bogotá, donde nuestro destino será la red de la MikroTik de algún CAU en este caso 10.52.152.5, el Gateway será el anteriormente configurado en L2TP server Binding y así poder generar la conexión hacia nuestro destino.

**Figura 21**

*Creación rutas*

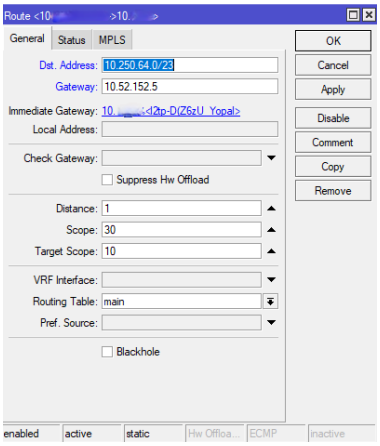



*Nota.* Fuente propia

Se alcanza también la red interna 10.250.64.0/23 para lo cual se crea otra ruta

**Figura 22**

*Creación de ruta*




*Nota.* Fuente propia

***Fase 4: Evaluación de rendimiento y análisis de impacto (Objetivo 4)***

Dentro del análisis y evaluación generada se puede evidenciar:

***Reducción de costos operativos***

Comparación de costos previos con ISP ($21.714.000) vs. costos estimados tras implementación propia (reducción estimada de al menos $13.770.000).

Se demuestra que la autogestión de la VPN permite reducir significativamente la dependencia de proveedores externos, validando un impacto económico positivo.

***Rendimiento de red y conectividad***

Se realizaron pruebas de latencia, pérdida de paquetes y disponibilidad del servicio, donde se evidencia que los enlaces presentan un rendimiento estable, que se ajustan a los servicios académicos, administrativos y videollamadas.

**Tabla 8**

*Pruebas de rendimiento*

| Métrica | Red Yopal VPN | Red Bogotá VPN | Red Interna Yopal |
|---|---|---|---|
| IP Destino | 10.252.152.5 | | 10.250.64.1 |
| Paquetes enviados | 14 | | 10 |
| Paquetes recibidos | 14 | | 10 |
| Paquetes Perdidos | 0% | | 0% |
| RTT Mínimo | 7.320 ms | | 7.392 ms |
| RTT máximo | 7.711 ms | 10.52.152.1 | 7.664 ms |
| RTT promedio | 7.467 ms | | 7.524 ms |
| Jitter estimado | 0.391 ms | | 0.272 ms |
| Estabilidad del enlace | Alta | | Alta |
| Observaciones | Sin pérdida, jitter leve | | Sin pérdida, jitter leve |

*Nota.* Tabla donde se muestra los resultados de pruebas realizadas desde la red de Bogotá

**Tabla 9**

*Pruebas de rendimiento*

| Métrica | Red Bogotá VPN | Red Interna Bogotá | Red Yopal |
|---|---|---|---|
| IP Destino | 10.52.152.1 | 10.4.1.3 | |
| Paquetes enviados | 20 | 21 | |
| Paquetes recibidos | 20 | 21 | |
| Paquetes Perdidos | 0% | 0% | |
| RTT Mínimo | 7.251 ms | 7.294 ms | |
| RTT máximo | 7.724 ms | 7.693 ms | 10.252.152.5 |
| RTT promedio | 7.433 ms | 7.507 ms | |
| Jitter estimado | 0.473 ms | 0.400 ms | |
| Estabilidad del enlace | Alta | Alta | |
| Observaciones | Sin pérdida, jitter moderado | Sin pérdida, jitter leve | |

*Nota.* Tabla donde se muestra los resultados de pruebas realizadas desde la red de Yopal

Se garantiza confidencialidad, integridad y autenticación robusta en las conexiones, alineando la solución con estándares internacionales de ciberseguridad por medio de protocolos seguro como IPsec – L2TP.

## Cronograma de Actividades

**Hoja de Ruta de Implementación**

**Tabla 10**

*Cronograma de actividades*

| Item | Actividades | Responsable | %Avance | Estado | Fecha I | Fecha F |
|---|---|---|---|---|---|---|
| **1** | **Diagnóstico y Levantamiento de Requerimientos** | | | | 1/06/2025 | 6/06/2025 |
| **2** | Inventario de sedes, mapeo de recursos tecnológicos | Infraestructura | 100% | Realizado | 1/01/2025 | 12/02/2025 |
| **3** | Definición de requerimientos técnicos y académicos | Infraestructura | 100% | Realizado | 21/03/2025 | 1/04/2025 |
| **4** | Establecimiento de presupuesto y recursos necesarios | Director de TI | 100% | Realizado | 2/04/2025 | 12/04/2025 |
| **5** | **Diseño de la Arquitectura de la Red** | | | | | |
| **6** | Definición de la topología | Infraestructura TI | 100% | Realizado | 21/04/2025 | 12/05/2025 |
| **7** | Selección de equipos | Infraestructura TI | 100% | Realizado | 13/05/2025 | 14/05/2025 |
| **8** | Configuración de protocolos y parámetros de seguridad | Infraestructura TI | 100% | Realizado | 15/05/2025 | 20/06/2025 |
| **9** | **Implementación Piloto** | | | | | |
| **10** | Despliegue en un Centros de Atención Universitaria (CAU) | Infraestructura TI | 100% | Realizado | 23/06/2025 | 27/06/2025 |
| **11** | Configuración de equipos y enlaces | Infraestructura TI | 100% | Pendiente | 24/06/2025 | 27/07/2025 |
| **12** | Pruebas iniciales de conectividad y seguridad | Infraestructura TI | 100% | Pendiente | 30/06/2025 | 04/07/2025 |
| **13** | **Despliegue y Escalamiento Nacional:** | | | | | |
| **14** | Extensión gradual por regiones | Infraestructura TI | 50% | Pendiente | 07/07/2025 | 21/09/2025 |

| Item | Actividades | Responsable | %Avance | Estado | Fecha I | Fecha F |
|---|---|---|---|---|---|---|
| **15** | integración con sistemas académicos existentes | Infraestructura TI | 0% | Pendiente | 07/09/2025 | 16/09/2025 |
| **16** | Capacitación de administradores locales | Infraestructura TI | 0% | Pendiente | 17/09/2025 | 17/06/2025 |
| **17** | **Evaluación, Optimización** | | | | | |
| **18** | Recolección de métricas | Infraestructura TI | 0% | Pendiente | 18/09/2025 | 19/09/2025 |
| **19** | análisis de retroalimentación | Infraestructura TI | 0% | Pendiente | 22/09/2025 | 26/09/2025 |
| **20** | Monitoreo de rendimiento | Infraestructura TI | 0% | Pendiente | 29/09/2025 | 1/10/2025 |

## Resultados

A continuación, se detallan los resultados directos, medibles y cuantificables que se obtendrán con el desarrollo del proyecto.

**Tabla 11**

*Resultados*

| Objetivo Específico | Resultado | Fecha Tentativa de Finalización | Nuevo Conocimiento Generado | Indicador Verificable |
|---|---|---|---|---|
| 1. Diagnosticar el estado actual de la red en los CAU. | Informe de diagnóstico de la infraestructura actual y necesidades de conectividad. | 1/07/2025 | Inventario, esquemas actuales y análisis de limitaciones. | Informe técnico aprobado con diagnóstico de mínimo 1 CAU. |
| 12. Diseñar un esquema de red para la solución VPN. | Diseño completo del esquema de red VPN con topología, equipos y protocolos L2TP/IPsec definidos. | 1/08/2025 | Documentación con diseño lógico/físico, análisis de tecnologías y recomendaciones de seguridad. | Documentación de diseño validado con al menos 90% de requerimientos cumplidos. |
| 3. Implementar en un CAU el diseño planteado. | Implementación inicial funcional con túneles IPsec activos y acceso remoto validado. | 1/09/2025 | Manual técnico de instalación y procedimientos de conexión VPN. | Pruebas funcionales con pérdida de paquetes igual o inferior al 0,5%, latencia igual o inferior a 10 ms, disponibilidad 100% durante la prueba. |
| 4. Evaluar el funcionamiento de la red implementada. | Estimación del impacto en rendimiento, seguridad, costos y satisfacción del usuario. | 1/10/2025 | Reporte de valoración con métricas cuantitativas y cualitativas. | Disminución de costos de $7.944.000, >80% de satisfacción en encuestas, > 10 pruebas funcionales documentadas. |

*Nota.* Tabla donde se muestra los resultados del proyecto

## Impactos

El desarrollo del proyecto “Diseño de una red privada virtual (VPN) que garantice la interconexión de servicios internos en los diferentes centros de atención universitaria de Colombia para la Universidad Santo Tomás” establece impactos en múltiples aspectos: tecnológico, operativo, académica y estratégica.

**Tabla 12**

*Impactos*

| Plazo | Impacto | Indicador Verificable | Forma de Medición / Seguimiento |
|---|---|---|---|
| **Corto (0–6 meses)** | Mejora en la conectividad entre CAU y sede principal | RTT igual o inferior a 10 ms, 0% pérdida de paquetes, jitter menor o igual 0.5 ms | Pruebas de red (ping, traceroute, test de conectividad) |
| | Reducción de incidencias técnicas | Disminución ≥ 30% en solicitudes relacionados con fallas de conectividad | Reporte mensual de mesa de ayuda |
| | Capacitación al personal técnico | Al menos 2 talleres formativos realizados con registros y evaluaciones | Actas de reuniones |
| **Mediano (6–12 meses)** | Reducción de costos por servicios tercerizados | Disminución de $7.944.000 frente a costos del ISP (base: $21.714.000) | Comparativo presupuestal y facturación |
| | Acceso remoto eficiente a servicios institucionales | > 80% de satisfacción en encuestas en CAU integrados | Encuestas a usuarios finales |
| | Documentación técnica generada | Manuales técnicos publicados para el área TI | Verificación documental y control de versiones |
| **Largo (1–3 años)** | Interconexión de todos los CAU a la VPN institucional | 100% de CAU conectados mediante túneles IPsec activos | Registro de conexiones activas y monitoreo MikroTik/CCR |
| | Contribución al cumplimiento del plan ECOS-5 | Inclusión de la solución VPN en informes de acreditación y calidad institucional | Reportes de gestión institucional y autoevaluación |

| Plazo | Impacto | Indicador Verificable | Forma de Medición / Seguimiento |
|---|---|---|---|
| | Mejora de ciberseguridad institucional | En camino hacia certificación ISO/IEC 27001:2022, cumplimiento de NIST | Auditorías internas y externas. |
| | Alta disponibilidad de servicios educativos remotos | > 90% de disponibilidad de servicios medidos semestralmente | Monitoreo de red y servicios de SOC |

*Nota*. Impactos en el tiempo a corto mediano y largo plazo

## Conclusiones

El desarrollo del presente proyecto permitió evidenciar que la implementación de una red privada virtual (VPN) autogestionada es una solución efectiva y pertinente para la interconexión de servicios internos entre los distintos Centros de Atención Universitaria (CAU) de la Universidad Santo Tomás. A partir del diagnóstico, diseño, implementación y evaluación de la solución propuesta, se estableció que es técnicamente viable, financieramente sostenible y alineada con las estrategias institucionales de transformación digital y sostenibilidad educativa.

Desde una perspectiva técnica, se logró demostrar que los protocolos seleccionados (IPsec) ofrecen niveles adecuados de seguridad, compatibilidad y rendimiento, permitiendo la confidencialidad e integridad de la información, así como la disponibilidad de los servicios críticos de la institución. El uso de equipos MikroTik y la configuración detallada en las pruebas piloto refuerzan la viabilidad operativa de una implementación a escala nacional.

A nivel institucional, la VPN autogestionada fortalece la capacidad de la Universidad para responder a las exigencias actuales de conectividad y gestión centralizada, al tiempo que reduce su dependencia de proveedores externos. Esta autonomía técnica se traduce en una mayor capacidad de respuesta ante incidentes, así como en la posibilidad de adaptar la infraestructura a las necesidades específicas de cada sede.

Estratégicamente, la solución se articula de manera clara con los lineamientos del plan ECOS-5, aportando al ecosistema educativo multicampus incluyente y al cumplimiento de los Objetivos de Desarrollo Sostenible (ODS), particularmente el ODS 4 (Educación de Calidad) y el ODS 9 (Industria, Innovación e Infraestructura).

## Análisis de Encuestas y Retroalimentación de Usuarios

Con el objetivo de evaluar la experiencia de uso de la red privada virtual (VPN) autogestionada implementada en el Centro de Atención Universitaria (CAU) seleccionado para la fase piloto, se diseñó y aplicó una encuesta dirigida a usuarios finales, incluyendo personal administrativo, docentes y estudiantes que hicieron uso del servicio durante un periodo de prueba de tres semanas.

### 1. Metodología

Se utilizó una encuesta anónima con preguntas cerradas de escala (1 a 5), así como una sección de observaciones abiertas. La muestra incluyó a 35 usuarios, con una tasa de respuesta del 85,7% (30 encuestas válidas).

### 2. Resultados Cuantitativos

**Tabla 13**

*Encuesta*

| Ítem Evaluado | Valor Promedio (1-5) |
|---|---|
| Facilidad de conexión a la VPN | 4.6 |
| Estabilidad del servicio (sin caídas o desconexiones) | 4.3 |
| Rapidez en el acceso a recursos internos (Moodle, software, etc.) | 4.4 |
| Nivel de satisfacción general con el servicio | 4.5 |
| Calidad de soporte técnico recibido en caso de dudas o errores | 4.7 |

Nota. Se considera satisfactoria una puntuación mayor o igual a 4.0.

### 3. Comentarios Representativos de los Usuarios

- *"La conexión fue estable durante jornada laboral. No noté interrupciones y accedí fácilmente a las herramientas para desarrollar actividades administrativas."* (Administrativo)
- *"Muy útil para acceder a la plataforma de software. Antes no se podía acceder de forma rápida."* (Docente)
- *"Sería ideal tener una app móvil para conectarse más fácilmente."* (Estudiante)

**Referencias**

Stallings, W. (2014). Data and computer communications (10th ed., International ed.). Pearson Education Limited.

R. S. Kagan, "Virtual private networks-new strategies for secure enterprise networking," Wescon/98. Conference Proceedings (Cat. No.98CH36265), Anaheim, CA, USA, 1998, pp. 267-272, doi: 10.1109/WESCON.1998.716461.

Andrés, P. J. M. (2016). Diseño de una VPN para el acceso a las bases de datos científicas de la Universidad Nacional de Loja.https://dspace.unl.edu.ec/jspui/handle/123456789/17159

Distrital, U. (2021). Acceso desde internet a la red interna de la universidad. Obtenido de VPN UD: https://ti.udistrital.edu.co/servicio/vpn

Tay, W. J., Lew, S. L., & Ooi, S. Y. (2024). An IKEv2-based approach for remote access VPN on MikroTik router. Journal of Information Science and Engineering, 40(5), 1093–1114. https://doi.org/10.6688/JISE.202409_40(5).0011

Naciones Unidas. (s.f.). Educación y desarrollo sostenible. https://www.un.org/sustainabledevelopment/es/education/

Dirección de Comunicaciones. (2024, 15 de marzo). Docentes y administrativos conocen ECOS - 5, la estrategia que nos llevará más allá de los límites. Tomás Noticias. https://tomasnoticias.usta.edu.co/docentes-y-administrativos-conocen-eco-5-la-estrategia-que-nos-llevar%C3%A1-m%C3%A1s-all%C3%A1-de-los-l%C3%ADmites

Universidad Santo Tomás. (s.f.). Sedes y seccionales. https://usantotomas.edu.co/sedesyseccionales

Ramírez Páez, L. E. (2018). Propuesta para la implementación de una VPN en RCN TV [Monografía]. Universidad Santo Tomás.

Forero Ortiz, A. C. (2014). Mejoras en el sistema de transmisión de información biométrica adquirida a partir de las terminales móviles del Fondo Nacional del Ahorro (FNA) mediante VPN [Monografía]. Universidad Santo Tomás.

Moreno Alayón, S. M. (2021). Comparación de aspectos operativos y económicos entre SD-WAN y MPLS para establecer la mejor opción de una empresa corporativa a nivel nacional e internacional [Trabajo opción de grado Pasantías en la Empresa ORANGE S.A., Universidad Santo Tomás de Aquino].

Sheldon. (2022, 8 de julio). VPN vs MPLS: ¿cuál es la diferencia? FS.com. https://www.fs.com/blog/vpn-vs-mpls-whats-the-difference-2020.html

Mavroudis, V. (2024). Zero-Trust Network Access (ZTNA). arXiv. https://doi.org/10.48550/arXiv.2410.20611.

Monroy Zabala, D. A. (2024). Mejora proceso de presentación de ofertas de Netskope Borderless WAN en la región de LATAM Trabajo de grado, Universidad Santo Tomás. Repositorio institucional Universidad Santo Tomás.

Arévalo Méndez, C. A., Arévalo Pérez, D. A., & Grisales Giraldo, J. A. (2015). Planificación para la migración de servicios FastEthernet de tecnología SDH a Metro Ethernet para un cliente específico Trabajo de grado, Universidad Santo Tomás.

SolveForce. (s.f.). MPLS vs. VPN: Which Is the Right Choice for Your Business?. Recuperado de https://solveforce.com/mpls-vs-vpn-which-is-the-right-choice-for-your-business/

Tech-Latest. (2023). Secure Your Network: VPN vs. MPLS - Which One Should You Choose?. Recuperado de https://tech-latest.com/vpn-vs-mpls/

NordLayer. (2024). VPN vs MPLS: Which one to choose?. Recuperado de https://nordlayer.com/blog/vpn-vs-mpls-which-one-to-choose/

Proxyium. (s.f.). Comparing MPLS and VPN: Which Is Right for Your Network?. Recuperado de https://proxyium.com/blog/comparing-mpls-and-vpn-which-is-right-for-your-network

Hexatronic Data Center. (s.f.). Comparing Different Methods of Data Center Connectivity: Direct Connect vs. VPN vs. MPLS. Recuperado de https://hexatronicdatacenter.com/en/knowledge/comparing-different methods-of-data-center-connectivity-direct-connect-vs.-vpn-vs.-mpls

Universidad Santo Tomás. (2024, 1 de noviembre). Acuerdo No. 46 de 2024: Aprobación del proyecto SANTOTO SUMMA a nivel multicampus, estrategia de educación continua de la Universidad Santo Tomás. https://secretariageneral.usta.edu.co/images/documentos/2024/Acuerdo-46-2024-Proyecto-Santoto-SUMMA.pdf

Barker, E., Dang, Q., Frankel, S., Scarfone, K., & Wouters, P. (2020). Guide to IPsec VPNs (NIST Special Publication 800-77 Revision 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-77r1

Ross, R., & Pillitteri, V. (2024). Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (NIST Special Publication 800-171 Revision 3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-171r3

National Institute of Standards and Technology. (2024). NIST Cybersecurity Framework 2.0: Resource & Overview Guide (NIST Special Publication 1299). https://doi.org/10.6028/NIST.SP.1299

Coro Cybersecurity. (2024, March 6). How NIST CSF 2.0 Can Help Schools. Recuperado de https://www.coro.net/blog/how-nist-csf-2-0-can-help-schools

AENOR. (2023, 13 de julio). Nueva ISO/IEC 27032:2023 para la seguridad en Internet. https://tienda.aenor.com/Paginas/Noticias/nueva-isoiec-270322023-para-la-seguridad-en-internet.aspx

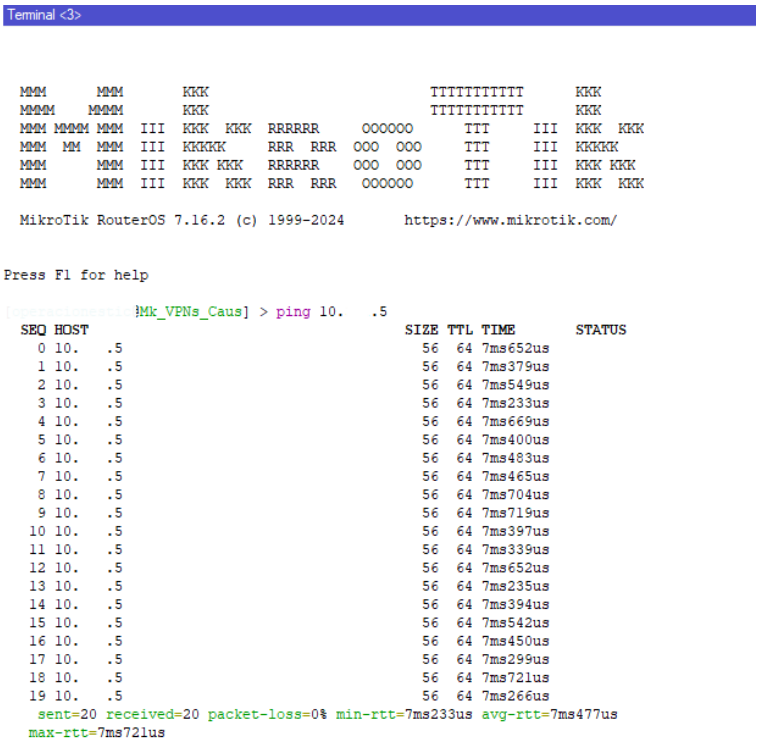
PMG SSI. (2023, 31 de agosto). ¿Qué es la norma ISO 27032? Una guía completa sobre ciberseguridad en la sociedad digital. https://www.pmg-ssi.com/2023/08/que-es-la-norma-iso-27032-una-guia-completa-sobre-ciberseguridad-en-la-sociedad-digital/

Arévalo, M. C. (2020, 5 de octubre; actualizado el 19 de febrero de 2025). ISO 27032, el estándar enfocado en ciberseguridad. Pirani. https://www.piranirisk.com/es/blog/iso-27032-el-estandar-enfocado-en-ciberseguridad

# Anexos

## Figura 23

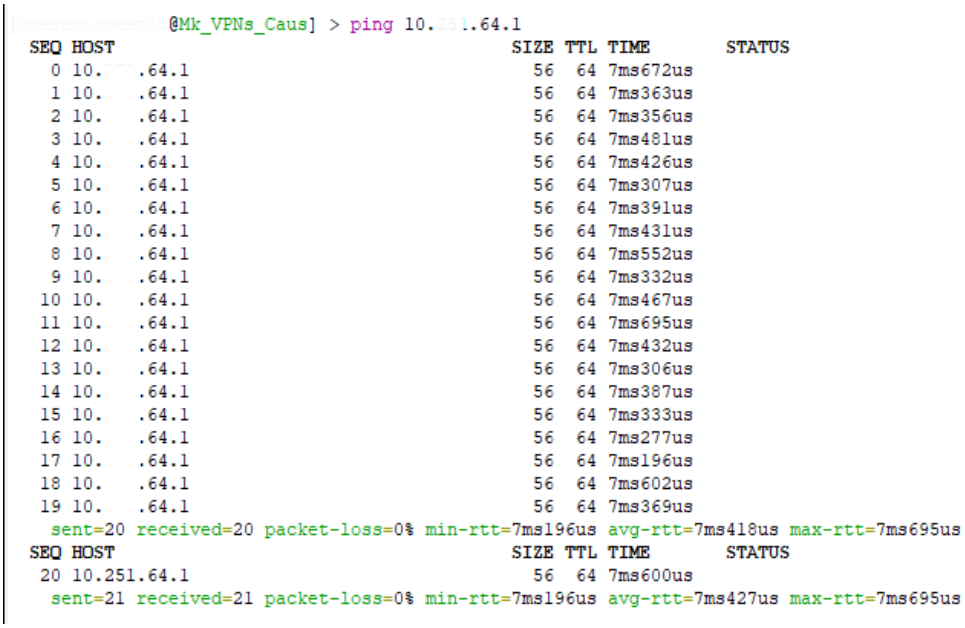
*Log MikroTik*




*Nota*. Evidencia de conectividad entre red VPN en Bogotá (10.X.X.X) y VPN CAU Yopal

**Figura 24**

Log MikroTik

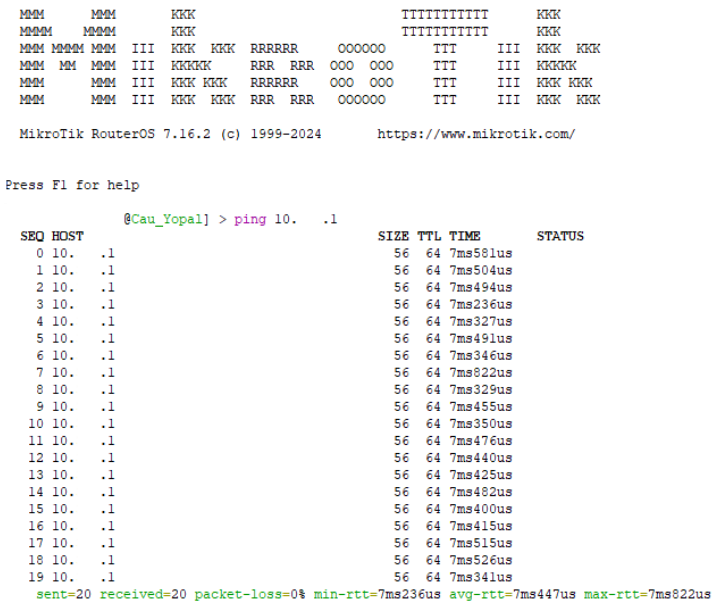


```
[Mk_VPNs_Caus] > ping 10.   .64.1
SEQ HOST                                     SIZE TTL TIME       STATUS
  0 10.    .64.1                             56  64 7ms672us
  1 10.    .64.1                             56  64 7ms363us
  2 10.    .64.1                             56  64 7ms356us
  3 10.    .64.1                             56  64 7ms481us
  4 10.    .64.1                             56  64 7ms426us
  5 10.    .64.1                             56  64 7ms307us
  6 10.    .64.1                             56  64 7ms391us
  7 10.    .64.1                             56  64 7ms431us
  8 10.    .64.1                             56  64 7ms552us
  9 10.    .64.1                             56  64 7ms332us
 10 10.    .64.1                             56  64 7ms467us
 11 10.    .64.1                             56  64 7ms695us
 12 10.    .64.1                             56  64 7ms432us
 13 10.    .64.1                             56  64 7ms306us
 14 10.    .64.1                             56  64 7ms387us
 15 10.    .64.1                             56  64 7ms333us
 16 10.    .64.1                             56  64 7ms277us
 17 10.    .64.1                             56  64 7ms196us
 18 10.    .64.1                             56  64 7ms602us
 19 10.    .64.1                             56  64 7ms369us
  sent=20 received=20 packet-loss=0% min-rtt=7ms196us avg-rtt=7ms418us max-rtt=7ms695us
SEQ HOST                                     SIZE TTL TIME       STATUS
 20 10.251.64.1                              56  64 7ms600us
  sent=21 received=21 packet-loss=0% min-rtt=7ms196us avg-rtt=7ms427us max-rtt=7ms695us
```

*Nota*. Log de conectividad entre red VPN en Bogotá (10.X.X.X) y Red local CAU Yopal 10.250.64.0/23

**Figura 25**

Log MikroTik

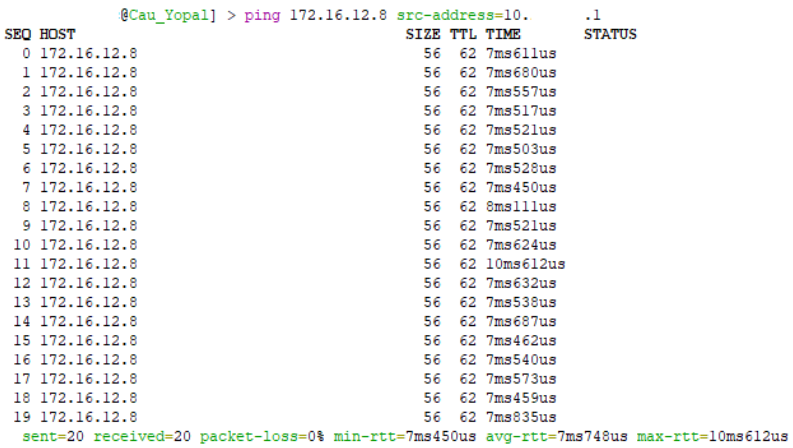


```
MMM      MMM       KKK                        TTTTTTTTTTT      KKK
MMMM    MMMM       KKK                        TTTTTTTTTTT      KKK
MMM MMMM MMM  III  KKK  KKK  RRRRRR     OOOOOO      TTT     III  KKK  KKK
MMM  MM  MMM  III  KKKKK     RRR  RRR  OOO  OOO     TTT     III  KKKKK
MMM      MMM  III  KKK KKK   RRRRRR    OOO  OOO     TTT     III  KKK KKK
MMM      MMM  III  KKK  KKK  RRR  RRR   OOOOOO      TTT     III  KKK  KKK

MikroTik RouterOS 7.16.2 (c) 1999-2024       https://www.mikrotik.com/

Press F1 for help

             [Cau_Yopal] > ping 10.   .1
 SEQ HOST                                     SIZE TTL TIME       STATUS
   0 10.   .1                                 56  64 7ms581us
   1 10.   .1                                 56  64 7ms504us
   2 10.   .1                                 56  64 7ms494us
   3 10.   .1                                 56  64 7ms236us
   4 10.   .1                                 56  64 7ms327us
   5 10.   .1                                 56  64 7ms491us
   6 10.   .1                                 56  64 7ms346us
   7 10.   .1                                 56  64 7ms822us
   8 10.   .1                                 56  64 7ms329us
   9 10.   .1                                 56  64 7ms455us
  10 10.   .1                                 56  64 7ms350us
  11 10.   .1                                 56  64 7ms476us
  12 10.   .1                                 56  64 7ms440us
  13 10.   .1                                 56  64 7ms425us
  14 10.   .1                                 56  64 7ms482us
  15 10.   .1                                 56  64 7ms400us
  16 10.   .1                                 56  64 7ms415us
  17 10.   .1                                 56  64 7ms515us
  18 10.   .1                                 56  64 7ms526us
  19 10.   .1                                 56  64 7ms341us
   sent=20 received=20 packet-loss=0% min-rtt=7ms236us avg-rtt=7ms447us max-rtt=7ms822us
```

*Nota*. Log de conectividad entre red VPN en Yopal (10.52.152.5) y Red VPN Bogotá 10.52.131.1

**Figura 26**

Log MikroTik



```
            @Cau_Yopal] > ping 172.16.12.8 src-address=10.      .1
SEQ HOST                                     SIZE TTL TIME       STATUS
  0 172.16.12.8                                56  62 7ms611us
  1 172.16.12.8                                56  62 7ms680us
  2 172.16.12.8                                56  62 7ms557us
  3 172.16.12.8                                56  62 7ms517us
  4 172.16.12.8                                56  62 7ms521us
  5 172.16.12.8                                56  62 7ms503us
  6 172.16.12.8                                56  62 7ms528us
  7 172.16.12.8                                56  62 7ms450us
  8 172.16.12.8                                56  62 8ms111us
  9 172.16.12.8                                56  62 7ms521us
 10 172.16.12.8                                56  62 7ms624us
 11 172.16.12.8                                56  62 10ms612us
 12 172.16.12.8                                56  62 7ms632us
 13 172.16.12.8                                56  62 7ms538us
 14 172.16.12.8                                56  62 7ms687us
 15 172.16.12.8                                56  62 7ms462us
 16 172.16.12.8                                56  62 7ms540us
 17 172.16.12.8                                56  62 7ms573us
 18 172.16.12.8                                56  62 7ms459us
 19 172.16.12.8                                56  62 7ms835us
  sent=20 received=20 packet-loss=0% min-rtt=7ms450us avg-rtt=7ms748us max-rtt=10ms612us
```

*Nota*. Log de conectividad entre red local en Yopal (10.250.64.1) y Red una red local de Bogotá (172.16.12.8)