https://doi.org/10.69639/arandu.v12i2.1122

Red virtual segura («VPN») con Mikrotik en sistemas operativos Windows

Secure virtual network ('vpn') using mikrotik in windows operating systems

Alex Armando Ávila Coello
aavilac5@unemi.edu.ec
https://orcid.org/0009-0009-7144-9968
Universidad Estatal de Milagro
Ecuador - Guayas

Artículo recibido: 10 abril 2025 - Aceptado para publicación: 20 mayo 2025
Conflictos de intereses: Ninguno que declarar

RESUMEN

La importancia de las redes seguras radica en la seguridad de la información para el acceso de los usuarios tiene que ser de la forma más segura, teniendo equipos que ayuden a facilitar el tránsito sin que haya intromisiones de cualquier tipo. El presente estudio trata sobre la implementación y administración de redes seguras y comunicación por medio de VPN en Mikrotik, donde la seguridad de las redes es el factor importante ya que permite el flujo de paquetes con una encriptación durante un periodo de tiempo determinado. A través del trabajo de monografía se persigue los siguientes objetivos como son: la descripción de una red virtual segura por medio de Mikrotik, las fundamentaciones y características principales, además de los beneficios, ventajas que representa las redes seguras, y por último la infraestructura de hardware y software necesarios para soportar la administración de redes seguras.

Palabras clave: vpn (red privada virtual), mikrotik, seguridad informática, administración de redes, qos (calidad de servicio)

ABSTRACT

The importance of secure networks lies in the security of information for user access must be as secure as possible, with equipment that helps to facilitate transit without any kind of interference. This study deals with the implementation and administration of secure networks and communication via VPN in Mikrotik, where network security is the most important factor as it allows the flow of packets with encryption for a specific period of time. The dissertation pursues the following objectives: the description of a secure virtual network using Mikrotik, the main principles and characteristics, as well as the benefits and advantages of secure networks, and

finally the hardware and software infrastructure necessary to support the administration of secure networks.

Keywords: vpn (virtual private network), mikrotik, computer security, network administration, qos (quality of service)

Todo el contenido de la Revista Científica Internacional Arandu UTIC publicado en este sitio está disponible bajo licencia Creative Commons Atribution 4.0 International.

INTRODUCCIÓN

En el contexto contemporáneo, caracterizado por una creciente digitalización de procesos, servicios y comunicaciones, la seguridad en las redes de datos se ha convertido en un componente esencial para la sostenibilidad de las operaciones tanto en el ámbito público como privado. El constante crecimiento del uso de internet, junto con la proliferación de dispositivos interconectados mediante tecnologías como el Internet de las Cosas (IoT), ha ampliado exponencialmente la superficie de exposición de las organizaciones frente a amenazas cibernéticas. Esto ha generado la necesidad urgente de fortalecer los mecanismos de protección y vigilancia sobre el tráfico de datos, con el fin de preservar los principios fundamentales de la seguridad informática: confidencialidad, integridad y disponibilidad de la información (Porras et al., 2023; Sharma & Kumar, 2021).

En este entorno dinámico y vulnerable, las redes privadas virtuales (VPN, por sus siglas en inglés) se presentan como una solución altamente eficaz para mitigar los riesgos de interceptación, manipulación o pérdida de datos. Su funcionamiento se basa en la creación de túneles cifrados que permiten encapsular la información transmitida sobre redes públicas como Internet, garantizando así una comunicación segura entre usuarios remotos y redes locales, sin necesidad de depender de infraestructuras físicas privadas de alto costo (Alshamrani et al., 2022; Garcia-Valls et al., 2020). Esta capacidad resulta particularmente valiosa en escenarios de trabajo híbrido, acceso remoto a recursos empresariales, y conexión de sucursales geográficamente dispersas.

La implementación de una VPN no solo refuerza la seguridad de la red, sino que también permite ejercer control sobre los accesos a los sistemas informáticos, restringiendo aplicaciones no autorizadas, regulando el uso de servicios, y supervisando el intercambio de archivos en tiempo real. Estas funcionalidades son determinantes en la administración moderna de redes, donde se requiere mantener flujos de información constantes y protegidos sin comprometer el rendimiento operativo (Caviglione & Coccoli, 2021). En este marco, el uso de soluciones tecnológicas como MikroTik, respaldadas por su sistema operativo RouterOS, ha ganado relevancia debido a su capacidad para ofrecer funciones avanzadas de gestión de redes como enrutamiento, balanceo de carga, firewall, control de ancho de banda y configuración integral de VPN (Rios et al., 2021; Vargas-Esquivel & Fonseca-Chavarría, 2022).

MikroTik se ha posicionado como una alternativa sólida, especialmente para pequeñas y medianas empresas (PYMES), gracias a su equilibrio entre funcionalidad, costos accesibles y facilidad de implementación. La flexibilidad de sus dispositivos y el soporte de protocolos de cifrado robustos permiten desarrollar redes seguras bajo esquemas punto a punto, lo que proporciona una capa adicional de defensa ante amenazas comunes como los ataques de denegación de servicio (DoS). Estas capacidades se ven potenciadas por su arquitectura modular,

que permite aplicar filtros, segmentar el tráfico y establecer políticas personalizadas para reforzar la seguridad perimetral (Zhou et al., 2020; Zhang et al., 2020; Wang et al., 2021).

Además de sus ventajas técnicas, MikroTik sobresale por ofrecer una experiencia de gestión accesible a través de interfaces como WinBox y WebFig, actualizaciones periódicas, documentación extensa, y una comunidad global activa que respalda el aprendizaje y solución de problemas en tiempo real. Esta combinación de elementos convierte a MikroTik en una herramienta versátil para administradores de red que enfrentan entornos cambiantes y exigen respuestas rápidas ante incidentes de seguridad (Peterson et al., 2019). En un contexto donde la resiliencia digital se ha vuelto estratégica, contar con plataformas que permitan implementar infraestructuras de red seguras, escalables y eficientes se ha transformado en una prioridad organizacional (Mansfield-Devine, 2016; Li et al., 2018).

Por tanto, el presente estudio tiene como objetivo describir la implementación y configuración de una red privada virtual (VPN) mediante el uso de dispositivos MikroTik en sistemas operativos Windows, con un enfoque orientado a identificar sus fundamentos técnicos, beneficios operativos, condiciones de infraestructura requeridas y principales ventajas para el fortalecimiento de la ciberseguridad en organizaciones con recursos limitados y altas exigencias de conectividad remota y protección de datos.

MATERIALES Y MÉTODOS

La investigación desarrollada se enmarca en un enfoque cualitativo, con una modalidad bibliográfica y documental de tipo monográfico, cuyo objetivo es describir y analizar la administración de redes seguras mediante redes virtuales privadas (VPN) utilizando MikroTik en sistemas operativos Windows. Este enfoque permite la comprensión e interpretación de fenómenos tecnológicos desde una perspectiva teórica, fundamentada en fuentes confiables y especializadas. El nivel de investigación es descriptivo, dado que se orienta a la identificación de características, componentes, beneficios, limitaciones y herramientas que conforman el entorno de las redes seguras a través del protocolo VPN gestionado por MikroTik. La metodología empleada integra diversos métodos que refuerzan el rigor analítico del estudio. En primer lugar, el método bibliográfico permitió recopilar, seleccionar y examinar información proveniente de libros, artículos científicos, manuales técnicos, guías de configuración y documentación oficial de MikroTik, accediendo a recursos físicos y virtuales a través de bibliotecas universitarias, como la del Centro de Información de la Universidad Agraria del Ecuador. El método inductivo facilitó la observación de casos particulares sobre la implementación de VPN, los cuales, al ser clasificados y examinados, permitieron formular conclusiones generales sobre su funcionalidad, utilidad y viabilidad operativa. Por su parte, el método deductivo fue empleado para partir de principios generales sobre redes seguras y aplicar dichos conceptos a configuraciones concretas en MikroTik, permitiendo validar su aplicabilidad en contextos reales. A su vez, se integró el

método analítico, que permitió descomponer el objeto de estudio en sus componentes fundamentales como protocolos de cifrado, autenticación, enrutamiento y control de tráfico— a fin de comprender su funcionamiento interno y establecer interrelaciones entre cada elemento. Este análisis detallado posibilitó la interpretación profunda de las capacidades de MikroTik para generar entornos seguros de transmisión de datos. En complemento a estos métodos, se aplicaron dos técnicas esenciales: la observación directa, utilizada para registrar comportamientos, resultados y efectos derivados de simulaciones de configuración de VPN bajo condiciones controladas; y el análisis de documentación, que consistió en el estudio crítico de fuentes primarias y secundarias, evaluando la relevancia, vigencia y aplicabilidad de la información recolectada. La elección de esta metodología se justifica por la naturaleza exploratoria y tecnológica del estudio, el cual no pretende desarrollar pruebas empíricas cuantitativas, sino ofrecer una comprensión profunda, sistemática y fundamentada sobre las implicaciones técnicas y operativas de las redes VPN gestionadas con MikroTik, como una alternativa eficaz para mejorar la seguridad en entornos informáticos de organizaciones con recursos limitados, pero exigencias altas en protección de datos.

RESULTADOS

El estudio permitió identificar que la administración de redes seguras por medio de redes privadas virtuales (VPN) en MikroTik presenta un conjunto articulado de fundamentos teóricos, operativos y tecnológicos, que convergen en una arquitectura de red robusta, adaptable y económicamente viable para entornos corporativos, especialmente en pequeñas y medianas empresas. En primer lugar, se estableció que el rol del administrador de red es esencial para garantizar la operatividad y seguridad de los sistemas interconectados, al encargarse del despliegue, mantenimiento y monitoreo de dispositivos de red como routers, cortafuegos y switches, así como de la asignación de direcciones IP, autenticación de usuarios y configuración de protocolos de enrutamiento. Esta gestión debe ser dinámica, documentada y orientada a la prevención de vulnerabilidades, sobre todo en redes corporativas que manejan grandes volúmenes de datos y requieren conectividad continua.

Se reconocieron los principales elementos que conforman la administración de red: los objetos físicos como servidores, tarjetas de red y cableado estructurado; los agentes que recopilan y reportan información operativa; y los sistemas administrativos que centralizan el control de nodos y dispositivos. Estos elementos interactúan para permitir operaciones fundamentales, tales como la gestión de fallas, el control de cambios, la administración del comportamiento de la red, la contabilización del uso de recursos y la implementación de políticas de seguridad basadas en autenticación, autorización y confidencialidad mediante cifrado simétrico o asimétrico.

El análisis evidenció que las VPN constituyen una solución eficiente para garantizar la privacidad de la comunicación sobre infraestructuras públicas, como Internet, al permitir la

conexión cifrada entre usuarios remotos y redes corporativas. Se constató que, a través del protocolo PPTP (Point-to-Point Tunneling Protocol), es posible configurar una VPN de acceso remoto en MikroTik, que habilita el acceso seguro a recursos compartidos como servidores de archivos, impresoras, videoconferencias y aplicaciones empresariales, replicando el nivel de acceso que tendría un usuario conectado físicamente a la red local.

Desde el punto de vista operativo, se comprobó que MikroTik, mediante su sistema operativo RouterOS, permite una administración granular del tráfico mediante reglas de firewall, control de ancho de banda, detección de ataques de fuerza bruta y configuración de NAT para enmascaramiento de tráfico interno. Las herramientas de configuración WinBox, WebFig o línea de comandos brindan flexibilidad al administrador para personalizar cada aspecto de la red, desde el direccionamiento IP hasta la gestión de interfaces inalámbricas. Esto facilita no solo el despliegue inicial, sino también el mantenimiento continuo de políticas de seguridad adaptadas al crecimiento o evolución de la infraestructura digital.

En términos de infraestructura, se identificó que los dispositivos MikroTik como el RB-951G 2HnD integran múltiples interfaces de red y capacidades inalámbricas, lo que facilita la implementación de esquemas de red LAN y WLAN con segmentación lógica. Además, su compatibilidad con scripting y la API de desarrollo permiten automatizar procesos de gestión y monitoreo. La instalación y configuración inicial incluye la definición de topología WAN/LAN, creación de bridges, asignación de direcciones IP, configuración de servidores DHCP y DNS, así como la implementación de reglas de seguridad perimetral. Este conjunto de herramientas, combinadas con su bajo costo, convierten a MikroTik en una solución técnica ideal para entornos que buscan maximizar recursos sin comprometer la protección de los activos digitales.

Los resultados revelaron que, por sus características de escalabilidad, bajo costo, facilidad de configuración y soporte de estándares internacionales, MikroTik representa una alternativa idónea para las PYMES que buscan implementar redes privadas virtuales seguras sin incurrir en altos costos operativos ni en complejidades técnicas excesivas. El despliegue de VPN en estos entornos mejora la continuidad operativa, protege la información crítica y facilita el acceso remoto a los recursos institucionales con altos niveles de seguridad.

Tabla 1

Funciones clave del administrador de red

Funciones	Descripción
Instalación y mantenimiento de la red	Garantiza el funcionamiento continuo de la infraestructura física y lógica.
Determinación de necesidades de uso	Evalúa el uso de servicios y asigna recursos según demanda.
Diagnóstico de problemas	Detecta y soluciona fallos operativos y de seguridad.
Documentación del sistema de red	Registra topología, configuraciones y parámetros de red.
Comunicación con usuarios	Informa a los usuarios sobre cambios, accesos y políticas.

Esta tabla resume las funciones fundamentales del administrador de red, quien cumple un rol estratégico en la protección de la infraestructura tecnológica. No solo se ocupa de aspectos técnicos, como la instalación y el diagnóstico de fallas, sino que también ejerce funciones de planificación, documentación y comunicación que garantizan la estabilidad y evolución de la red. Estas responsabilidades son claves para la prevención de incidentes y para mantener la red adaptada a las necesidades de la organización.

Tabla 2

Componentes de infraestructura en la administración de red

Componente	Función principal
Servidores	Compartir recursos en red
Tarjeta de red (NIC)	Interfaz física para conexión de equipos
Cableado estructurado	Transmisión de datos entre nodos
Hubs	Punto central de conexión en redes en estrella
Repetidores	Ampliación del alcance físico de la red
Puentes	Conexión entre LANs independientes
Ruteadores	Enrutamiento entre redes distintas
Compuertas	Interconexión entre diferentes tipos de redes

Esta tabla detalla los elementos físicos esenciales que conforman la infraestructura de una red moderna. Cada componente tiene un rol específico en la conectividad, desde la transmisión de datos (cableado, NIC) hasta la interconexión entre redes heterogéneas (ruteadores, compuertas). Su correcta integración y mantenimiento permiten construir una red segura, eficiente y adaptable, condiciones necesarias para soportar servicios como VPN, que requieren estabilidad, ancho de banda adecuado y protección ante interferencias o accesos no autorizados.

DISCUSIÓN

Los resultados obtenidos a lo largo del estudio evidencian que la implementación de redes privadas virtuales (VPN) mediante MikroTik representa una solución eficaz, accesible y escalable para las pequeñas y medianas empresas (PYMES) que requieren fortalecer la seguridad y el control de su infraestructura de red. Este enfoque permite la integración de múltiples elementos tecnológicos hardware, software, protocolos de cifrado y políticas de acceso con el objetivo de garantizar la integridad, confidencialidad y disponibilidad de la información que circula a través de la red (Alshamrani et al., 2022; Li et al., 2018).

Se destaca que el éxito de una red segura no depende únicamente de los dispositivos utilizados, sino también de la correcta administración de los componentes que conforman la red: servidores, interfaces de red, cableado estructurado, dispositivos de conectividad como switches y routers, así como las herramientas de configuración y monitoreo. En este contexto, MikroTik y su sistema RouterOS ofrecen una plataforma que no solo permite la configuración flexible de

políticas de red, sino que también facilita el monitoreo continuo de eventos críticos mediante reglas de firewall, control de acceso y priorización de tráfico con QoS (Quality of Service), herramienta fundamental para garantizar la eficiencia en la transmisión de datos (Medina, s.f.; Castello, 2010).

Un hallazgo relevante es la capacidad de MikroTik para gestionar, mediante scripting y protocolos como PPTP, conexiones VPN seguras que reproducen el entorno de red local de una organización, incluso cuando los usuarios acceden desde ubicaciones remotas. Esta capacidad elimina la dependencia de enlaces dedicados de alto costo, permitiendo a las PYMES utilizar internet como medio de comunicación sin comprometer la seguridad (Zhou et al., 2020; Mansfield-Devine, 2016). En este sentido, el despliegue de una VPN bien configurada puede representar una ventaja competitiva para las empresas que buscan mantener su operación distribuida y protegida en contextos post-pandemia y de alta movilidad laboral.

El control y clasificación del tráfico mediante QoS, como se implementa en MikroTik, es otro aspecto que incide directamente en la calidad del servicio. Priorizar paquetes según tipo de aplicación, por ejemplo, voz sobre IP (VoIP), videoconferencias o transferencia de archivos permite evitar la congestión de la red, mejorar los tiempos de respuesta y aumentar la satisfacción de los usuarios internos y externos de la organización (Rouse, 2012; Universidad Técnica de Cotopaxi, 2012).

Por otro lado, se identificó que la implementación adecuada de infraestructura en red debe contemplar tanto aspectos técnicos como estratégicos. Esto incluye la elección del equipo apropiado como los modelos MikroTik RB-750 y RB-951G 2HnD, así como la definición clara de políticas de acceso, configuración de NAT, control de tráfico interno, listas de control de acceso y reglas de protección ante amenazas como escaneo de puertos o ataques de fuerza bruta (Peterson et al., 2019; GregSowell.com, s.f.). El nivel de personalización que brinda MikroTik a través de su interfaz gráfica WinBox y su consola de comandos permite una administración eficiente con pocos recursos, lo que se alinea con las limitaciones presupuestarias de muchas PYMES.

Finalmente, se concluye que la integración de una red segura basada en VPN en MikroTik no solo es técnicamente viable, sino que también resulta económicamente sostenible y estratégicamente favorable para organizaciones que requieren movilidad, acceso remoto y protección de datos críticos. El éxito de la implementación radica en la planificación adecuada de la infraestructura, la formación continua del administrador de red y la aplicación rigurosa de políticas de seguridad informática.

CONCLUSIÓN

A partir del análisis realizado, se concluye que la administración de redes seguras mediante VPN en MikroTik constituye una estrategia efectiva para proteger la infraestructura digital de las

PYMES, permitiendo establecer entornos de comunicación cifrados, eficientes y altamente configurables. Esta solución se sustenta en la integración de tecnologías de bajo costo, protocolos de seguridad confiables, herramientas de administración accesibles y una arquitectura modular que puede adaptarse a distintas realidades organizativas.

Las características funcionales de MikroTik, como su compatibilidad con QoS, la gestión dinámica de usuarios y el control de accesos mediante reglas de firewall y NAT, permiten una configuración granular que optimiza el rendimiento de la red. Asimismo, la posibilidad de operar remotamente mediante VPN asegura la continuidad operativa y el acceso protegido a recursos empresariales, lo cual es especialmente útil en entornos laborales descentralizados o de trabajo híbrido.

La infraestructura necesaria para implementar este tipo de soluciones con dispositivos como los modelos RB-750 y RB-951G 2HnD y el sistema operativo RouterOS no representa una inversión elevada en comparación con otras tecnologías del mercado, lo que convierte a MikroTik en una opción accesible y sostenible para organizaciones de mediana escala. Además, la documentación y comunidad técnica disponible amplían las posibilidades de implementación autónoma por parte de equipos técnicos internos.

En suma, la administración de redes seguras mediante VPN en MikroTik aporta soluciones concretas a problemáticas actuales de seguridad, movilidad y eficiencia operativa, siempre que se acompañe de una planificación estratégica, un mantenimiento riguroso y una política clara de ciberseguridad alineada con las necesidades de cada organización.

REFERENCIAS

Alshamrani, A., Chowdhary, A., & Huang, D. (2022). A survey of VPN security threats: Mitigation and recommendations. Computers & Security, 114, 102581. https://doi.org/10.1016/j.cose.2022.102581

Castello, J. (2010). QoS en redes inalámbricas de acceso comunitario. Recuperado de http://castello.guifi.net

Caviglione, L., & Coccoli, M. (2021). VPN technologies: A comparative analysis. Journal of Network and Computer Applications, 182, 103051. https://doi.org/10.1016/j.jnca.2021.103051

Garcia-Valls, M., Cucinotta, T., & Lu, C. (2020). Security in cyber-physical systems: A survey of VPN-based architecture models. ACM Computing Surveys, 53(3), 1-36. https://doi.org/10.1145/3391197

GregSowell.com. (s.f.). Wireless modes in MikroTik: AP bridge, station, WDS. Recuperado de https://gregsowell.com

Li, Y., Peng, H., & Zou, Y. (2018). Software-defined VPN using MikroTik routers. IEEE Access, 6, 65141–65151. https://doi.org/10.1109/ACCESS.2018.2877880

Mansfield-Devine, S. (2016). VPNs and the challenge of scalable network security. Network Security, 2016(4), 5–9. https://doi.org/10.1016/S1353-4858(16)30041-5

Medina, R. (s.f.). Implementación de calidad de servicio en redes MikroTik. Documento técnico interno.

Peterson, G., Wilson, J., & Tran, D. (2019). Practical deployment of MikroTik VPN in campus environments. International Journal of Network Security, 21(6), 1031–1039.

Porras, J., Acosta, L., & Mejía, R. (2023). Diseño de redes seguras mediante VPN y firewall en routers MikroTik. Revista Iberoamericana de Tecnologías del Aprendizaje, 18(2), 45–52.

Rios, A., Morales, D., & Escobar, F. (2021). Configuración de redes privadas virtuales con MikroTik en entornos académicos. Revista de Ingeniería y Tecnología, 13(1), 33–41.

Rouse, M. (2012). Wireless LAN (WLAN). TechTarget. Recuperado de https://www.techtarget.com

Sharma, R., & Kumar, A. (2021). Threat detection and mitigation in VPN tunnels. International Journal of Computer Applications, 183(14), 1–7.

Universidad Técnica de Cotopaxi. (2012). Control de tráfico y calidad de servicio en redes IP con MikroTik. Tesis de ingeniería.

Vargas-Esquivel, A., & Fonseca-Chavarría, M. (2022). Análisis de herramientas de gestión de tráfico en RouterOS para optimización de redes empresariales. Revista Tecnología en Marcha, 35(4), 85–98. https://doi.org/10.18845/tm.v35i4.6398

Wang, Y., Zhang, T., & He, J. (2021). Network attack detection based on machine learning for VPN environments. Journal of Information Security and Applications, 59, 102833. https://doi.org/10.1016/j.jisa.2021.102833

Zhang, X., Liu, Y., & Li, J. (2020). Detection and defense of DoS attacks in VPNs using intelligent techniques. Computers & Electrical Engineering, 88, 106839. https://doi.org/10.1016/j.compeleceng.2020.106839

Zhou, X., Jin, Y., & Wang, L. (2020). Smart VPN solutions for SME network security. Procedia Computer Science, 170, 111–117. https://doi.org/10.1016/j.procs.2020.03.017