Revista Científica Multidisciplinar G-ner@ndo ISSN: 2806-5905

Redes privadas virtuales y ciberseguridad: revisión bibliométrica y sistemática de las tendencias de investigación, los protocolos y las aplicaciones (2004-2024)

Virtual private networks and cybersecurity: bibliometric and systematic review of research trends, protocols, and applications (2004–2024)

Alex Armando Ávila Coello

PUNTO CIENCIA.

Julio - diciembre, V°6 - N°2; 2025

Recibido: 06-11-2025
Aceptado: 07-11-2025
Publicado: 30-12-2025

PAIS

- Ecuador, Guayas

INSTITUCION

- Universidad Estatal de Milagro.

CORREO:

✉ aavilac5@unemi.edu.ec

ORCID:

https://orcid.org/0009-0009-7144-9968

FORMATO DE CITA APA.

Ávila, A. (2025). Redes privadas virtuales y ciberseguridad: revisión bibliométrica y sistemática de las tendencias de investigación, los protocolos y las aplicaciones (2004-2024). *Revista G-ner@ndo, V°6 (N°2). Pág. 2637 – 2673.*

Resumen

El estudio analiza la evolución de la investigación sobre redes privadas virtuales (VPN) y ciberseguridad en 2004–2024 mediante una revisión bibliométrica y sistemática. La muestra integra Scopus y Web of Science y, tras depuración por DOI y similitud de títulos, reúne 2.200 artículos únicos. El análisis con ScientoPy, VOSviewer y Bibliometrix describe un crecimiento sostenido desde 2010 y una intensificación en 2020–2024. Predomina la producción en conferencias, con aportes relevantes de Estados Unidos, China, Reino Unido, Alemania y Japón. Los focos temáticos se concentran en seguridad de red, criptografía, calidad de servicio y clasificación de tráfico. En cuanto a protocolos, la literatura consolida IPSec y SSL/TLS, mantiene interés en OpenVPN y reporta una presencia incipiente de WireGuard. Las aplicaciones más visibles abarcan teletrabajo, nube e IoT, con extensiones hacia SD-WAN y aproximaciones Zero Trust. La síntesis cualitativa de trabajos influyentes muestra avances en desempeño, autenticación, políticas de seguridad y detección de tráfico cifrado. Persisten brechas en evaluaciones comparativas de WireGuard, en escenarios IoT y 5G/6G, en soluciones de bajo costo como Mikrotik y en la integración de aprendizaje automático para defensa proactiva. El artículo propone una agenda que prioriza métricas comparables, repositorios abiertos y estudios experimentales de capa de datos y control en entornos heterogéneos.

Palabras clave: VPN; ciberseguridad; IPSec; WireGuard; IoT; SD-WAN.

Abstract

The study analyzes the evolution of research on virtual private networks (VPNs) and cybersecurity in 2004–2024 through a bibliometric and systematic review. The sample includes Scopus and Web of Science and, after filtering by DOI and title similarity, comprises 2,200 unique articles. The analysis with ScientoPy, VOSviewer, and Bibliometrix describes sustained growth since 2010 and an intensification in 2020–2024. Conference production predominates, with relevant contributions from the United States, China, the United Kingdom, Germany, and Japan. The thematic focus is on network security, cryptography, quality of service, and traffic classification. In terms of protocols, the literature consolidates IPSec and SSL/TLS, maintains interest in OpenVPN, and reports an incipient presence of WireGuard. The most visible applications cover teleworking, cloud, and IoT, with extensions to SD-WAN and Zero Trust approaches. The qualitative synthesis of influential works shows advances in performance, authentication, security policies, and encrypted traffic detection. Gaps remain in comparative evaluations of WireGuard, in IoT and 5G/6G scenarios, in low-cost solutions such as Mikrotik, and in the integration of machine learning for proactive defense. The article proposes an agenda that prioritizes comparable metrics, open repositories, and experimental studies of data and control layers in heterogeneous environments.

Keywords: VPN; cybersecurity; IPSec; WireGuard; IoT; SD-WAN.

Introducción

La transformación digital y la expansión del trabajo remoto instalaron la ciberseguridad como prioridad estratégica en organizaciones públicas y privadas. En ese marco, las redes privadas virtuales (VPN) aportan confidencialidad, integridad y autenticación sobre infraestructuras abiertas, y sostienen escenarios de acceso remoto seguro en banca, educación y administración pública, así como en campus y entornos móviles con requisitos de control y auditoría (Deshmukh & Iyer, 2017; Yu, Chen, & Tan, 2009).

La evolución tecnológica de las VPN avanzó desde protocolos iniciales hacia familias consolidadas como IPSec y SSL/TLS, con desarrollos abiertos de amplia adopción como OpenVPN y propuestas más recientes centradas en simplicidad y solidez criptográfica como WireGuard. Los estudios comparativos y las pruebas formales sobre estas alternativas describen alcances, ventajas y límites de seguridad, escalabilidad y facilidad de despliegue (Mao, Zhu, & Qin, 2012; Skendzic & Kovacic, 2017; Lipp, Blanchet, & Bhargavan, 2019).

La literatura reportó condicionantes de desempeño y costos de operación. Las pasarelas SSL VPN basadas en navegador reducen el rendimiento en transferencias de gran tamaño y saturan CPU bajo ciertas condiciones; optimizaciones de captura a alta velocidad elevaron el rendimiento en túneles SSL; y la negociación TLS introdujo retardos sensibles en sistemas de control industrial y aplicaciones críticas (Mache & Likarish, 2005; Wu KeHe, Zhao, Cui WenChao, Zhang XianKang, & Cui AJun, 2019; Rybin, Piliugina, & Piliugin, 2018).

La convergencia con arquitecturas programables impulsó nuevas trayectorias. En SDN/SD-WAN emergieron propuestas de SD-VPN y de IPsec sobre planos de datos programables P4, con despliegues y prototipos que demuestran control en tiempo real, orquestación automática y viabilidad de túneles de sitio a sitio y de host a sitio; incluso

se documentó un túnel IPsec quantum-safe con QKD a 10 Gbps en fibra metropolitana (Fu, Wang, Liu, & Wang, 2024; Hauser, Haeberle, Schmidt, & Menth, 2020; Alia et al., 2024).

Las áreas emergentes exigen respuestas técnicas específicas. La integración de IoT y 5G/6G plantea requisitos de latencia, fiabilidad y acuerdos de servicio; el reconocimiento de tráfico cifrado demandas técnicas de aprendizaje profundo con tasas de precisión elevadas; y los entornos organizacionales valoran diseños que combinen control, trazabilidad y costos contenidos (Xian, 2021; Cheng & Zhou, 2022; Jung, Han, & Lee, 2011).

A pesar del volumen de trabajos, predomina una literatura fragmentada por protocolo, caso de uso o plataforma, sin una síntesis bibliométrica y sistemática que cubra de forma integral el periodo 2004–2024. Este estudio propone un mapa global que identifica tendencias, protocolos más investigados, dominios de aplicación y brechas, y que enlaza resultados cuantitativos con una revisión cualitativa de contribuciones citadas y recientes (Mao et al., 2012; Lipp et al., 2019; Fu et al., 2024). El objetivo general consiste en analizar la evolución de la producción científica sobre VPN y seguridad de redes en 2004–2024 e identificar tendencias, protocolos, áreas de aplicación, vacíos y perspectivas. Las preguntas de investigación abordan la evolución del campo, la atención relativa a IPSec, OpenVPN, WireGuard, QoS y soluciones de bajo costo, las aplicaciones en teletrabajo, IoT, cloud, PYMES y educación, los países, instituciones y autores líderes, y las brechas persistentes.

Analizar la evolución de la producción científica sobre VPN y seguridad de redes en el período 2004–2024, identificando tendencias, protocolos más investigados, principales áreas de aplicación, brechas de investigación y perspectivas futuras.

Preguntas de investigación

- ¿Cómo ha evolucionado la investigación sobre VPN en los últimos 20 años?
- ¿Qué protocolos y tecnologías (IPSec, OpenVPN, WireGuard, QoS, Mikrotik) han recibido mayor atención?
- ¿Cuáles son las áreas de aplicación más investigadas (teletrabajo, IoT, cloud, PYMES, educación)?
- ¿Qué países, instituciones y autores lideran la investigación?
- ¿Qué brechas de conocimiento persisten en torno a VPN y seguridad de redes?

Revisión de literatura

La literatura técnica sobre SSL-VPN y IPSec describe comparaciones de alcance, seguridad y escalabilidad, y propone criterios de selección según escenarios de despliegue empresarial y remoto (Mao, Zhu, & Qin, 2012; Deshmukh & Iyer, 2017). Evaluaciones de rendimiento en pasarelas SSL basadas en navegador reportan reducción notable de throughput bajo cargas altas y aumento del uso de CPU, con implicaciones directas sobre transferencias de archivos y acceso a aplicaciones (Mache & Likarish, 2005).

El diseño de infraestructuras de prueba con máquinas virtuales ofrece un medio eficaz para validar subsistemas híbridos SSL-VPN, detectar errores de configuración y ajustar parámetros antes del despliegue en producción, con mejoras en reconfiguración y escalabilidad (Chen & Lin, 2013). En entornos de simulación distribuida con requisitos de multiclase de seguridad, la combinación de virtualización y VPN permite segmentación de datos, control de accesos y mantenimiento de integridad sin imponer plataformas físicas duplicadas (Stytz & Banks, 2007).

La integración de VPN con redes móviles y BWN exige atención a registro y autenticación de usuarios en acceso remoto, con propuestas que sustituyen mecanismos “dial-in” por combinaciones L2TP/IPSec para robustecer el establecimiento del túnel en escenarios de alta movilidad (Elkeelany, Matalgah, & Qaddour, 2004). En Mobile IPv6, la introducción de IKEv2 Configuration Payload reduce señalización y conserva el nivel de seguridad durante el acceso de nodos móviles a pasarelas IPsec-VPN (Lee, Nah, & Jung, 2005).

El uso de TLS/DTLS como base de VPN amplía el espectro de aplicaciones cuando existe multiplexación a nivel de sesión, con propuestas de extensión compatibles hacia tráfico sobre transporte fiable y no fiable que resuelven limitaciones de encapsulación exclusiva en HTTP (Badra & Hajjeh, 2006). La verificación de políticas de seguridad IPsec/VPN entre dominios administrativos exige definiciones formales de requisitos y criterios de corrección, con arquitecturas que generan políticas consistentes y gestionan cambios de forma automática (Yang, Martel, Fu, & Wu, 2006).

Los costes operativos y la dependencia de terceros motivan estudios de sustitución de servicios MPLS por IPSec propio, con evidencias de reducción de costos y control de seguridad en escenarios universitarios, aunque con impactos medibles en latencia y jitter que requieren dimensionamiento adecuado (Hashiyana, Haiduwa, Suresh, Bratha, & Ouma, 2020). En entornos corporativos, OpenVPN como opción open-source ofrece beneficios económicos y técnicos, con capacidades de autenticación flexibles y operación detrás de NAT (Skendzic & Kovacic, 2017).

El rendimiento de protocolos PPTP, IPSec y SSL depende de la elección de algoritmos y tamaños de ventana, con variaciones de 40 a 90 Mbps en Windows Server 2003 y efectos directos sobre la utilización de CPU, lo que refuerza la necesidad de pruebas comparativas antes del despliegue definitivo (Narayan, Kolahi, Brooking, & de Vere, 2008). En redes WLAN, combinaciones EAP-TLS con IPSec fortalecen

autenticación y cifrado en estaciones, puntos de acceso y servidores RADIUS, con guías de configuración y consideraciones de seguridad específicas (Zhou, Tan, & Gao, 2010).

Los trabajos sobre QoS en VPN destacan el control de flujos con garantías mínimas por flujo y la necesidad de mecanismos justos intra-VPN e inter-VPN; modelos y simulaciones con NS-2 muestran maximización de uso de ancho de banda con mantenimiento de garantías de servicio (Sabrina & Rogers, 2007). En redes ópticas Gigabit Ethernet, la técnica Virtual Private LAN Service demuestra provisión de QoS en tramos metro/core con establecimiento rápido de servicios en plataformas GMPLS (Rea et al., 2008).

Las extensiones de QoS hacia MPLS/MP-BGP en entornos de operador validan arquitecturas con DiffServ, WFQ y WRED, con mejoras medibles en retardo, jitter, pérdida y utilización de tráfico para clientes con SLA, lo que respalda estrategias de ingeniería de tráfico en VPN de proveedor (Beyene & Argaw, 2019). Procedimientos de seguridad en MPLS/VPN requieren auditoría de políticas y análisis inverso de configuraciones, con algoritmos y complejidades detalladas para calificar perímetros y priorizar mitigaciones (Llorens & Serhrouchni, 2007).

La convergencia con edge/fog computing introduce demandas de conectividad privada y programable entre nubes y bordes; EdgeVPN.io ejemplifica una red virtual programable que integra Kubernetes sobre nodos con NAT heterogéneo y direcciones privadas, y que simplifica la orquestación de aplicaciones TCP/IP en clústeres virtuales distribuidos (Figueiredo & Subratie, 2020). En SDN, comparaciones entre FlowVisor y OpenVirtex para VPN de sitio a sitio resaltan facilidad de implementación frente a soluciones tradicionales, aunque con limitaciones de confiabilidad para producción a gran escala (Nurkahfi, Mitayani, Mardiana, & Dinata, 2019).

El impacto de VPN en rendimiento de red aparece como variable de doble cara: algoritmos, hardware y software afectan desempeño mientras la propia VPN incide en

throughput y delay; simulaciones en NS-2 cuantifican efectos más marcados sobre TCP que sobre UDP, con una expresión analítica para modelado del impacto (Nawej & Du, 2018). En videoconferencia sobre DMVPN, los resultados en simulación muestran sensibilidad al número de sitios, participantes y protocolos de enrutamiento, con métricas de retardo, pérdidas y convergencia que permiten dimensionamiento y selección de protocolos (Bahnasse et al., 2019).

Los casos de uso sectoriales muestran aplicaciones directas. En logística, la combinación de VPN y GPS establece comunicación eficaz con flotas y control de almacenes, con mejoras en eficiencia operativa y reducción de tiempos de soporte (Alhadidi, Baniata, Baniata, Al-Ali, & Althwaini, 2012). En nube y big data, la integración de VPN y firewall mejora seguridad con afectación ligera de rendimiento, con resultados sobre throughput, pérdidas y retardo en escenarios densos (Shah, ud Din, Abizar, ud Din, & Khan, 2020).

La transición hacia Zero Trust mantiene vigentes equipos heredados como firewalls y VPN, lo que abre vectores de amenaza dentro de sistemas ZTNA; experimentos y análisis identifican riesgos y contramedidas para minimizar exposiciones en entornos públicos e institucionales (Kim & Sohn, 2024). En IoT-MANET, la configuración de VPN mitiga la interferencia de jammers y mejora retardo, rendimiento y pérdidas bajo diferentes potencias, cantidades de interferentes y cargas de tráfico, según evidencia de simulación en OPNET (Nourildean, 2024).

Las líneas metodológicas también abarcan optimización criptográfica y de políticas. Propuestas de reducción de políticas IPSec mejoran tiempos de actualización sin sacrificar requisitos de seguridad (Sadeghi, Ali, Pedram, Deghan, & Sabaei, 2009). Técnicas de optimización de logs de recursos SSL-VPN con Bloom Filter reducen redundancia y consumo asociado a auditoría, con impacto directo en eficiencia operacional (Song, Li, Cheng, Xiang, & Cai, 2016). En el plano de implementación,

ajustes de SSL-VPN de alta concurrencia elevan desempeño del servidor con mejoras en estructuras de E/S, temporizadores y notificación de disponibilidad (Chu, 2013).

El sector bananero del Ecuador ha sido considerado como un referente a nivel del mundo, y que a su vez los ha convertido en uno de los principales pilares de la economía del país debido a la generación de fuentes de empleo de manera directa e indirecta, y el aporte a la seguridad alimentaria del país (Jadán et al., 2024). De acuerdo con el reporte de la Encuesta de Superficie y Producción Agropecuaria Continua ([ESPAC], 2024), la superficie cosechada de banano fue de 175.181 hectáreas, la misma que registró un crecimiento de 4,6% en comparación con los resultados alcanzados durante el 2023, convirtiendo a la costa como el mayor referente dentro de este sector con el 89,0% de la superficie nacional cosechada de banano.

Métodos y Materiales

El estudio adoptó un diseño bibliométrico con una revisión exploratoria sistemática. El objetivo era describir la evolución, los actores y los temas de investigación relacionados con las VPN y la ciberseguridad, y sintetizar las pruebas cualitativas recientes y más citadas.

Fuentes y estrategia de búsqueda

Se consultaron Scopus y Web of Science Core Collection (WoS). La búsqueda se realizó en el intervalo 2004-2024, con especial énfasis en los protocolos, el rendimiento y las aplicaciones de las VPN.

Ecuación de Scopus (TITLE-ABS-KEY):

TITLE-ABS-KEY ("virtual private network" OR VPN* OR (VPN W/3 network*)) AND TITLE-ABS-KEY (security OR cybersecurity OR IPsec OR "SSL" OR "TLS" OR "SSL/TLS" OR "SSL VPN" OR "TLS VPN" OR "OpenVPN" OR "WireGuard" OR "L2TP"

OR "PPTP" OR "OpenConnect" OR "SoftEther" OR "remote access" OR "site-to-site" OR "site to site" OR "quality of service" OR QoS OR latency OR throughput OR jitter OR "packet loss" OR performance OR IoT OR "internet of things" OR "edge computing" OR "5G" OR "6G" OR "zero trust" OR ZTNA OR "SD-WAN") AND PUBYEAR > 2003 AND PUBYEAR < 2025 AND (LIMIT-TO (DOCTYPE , "ar") OR LIMIT-TO (DOCTYPE , "cp"))

Ecuación WoS (Tema = TS):

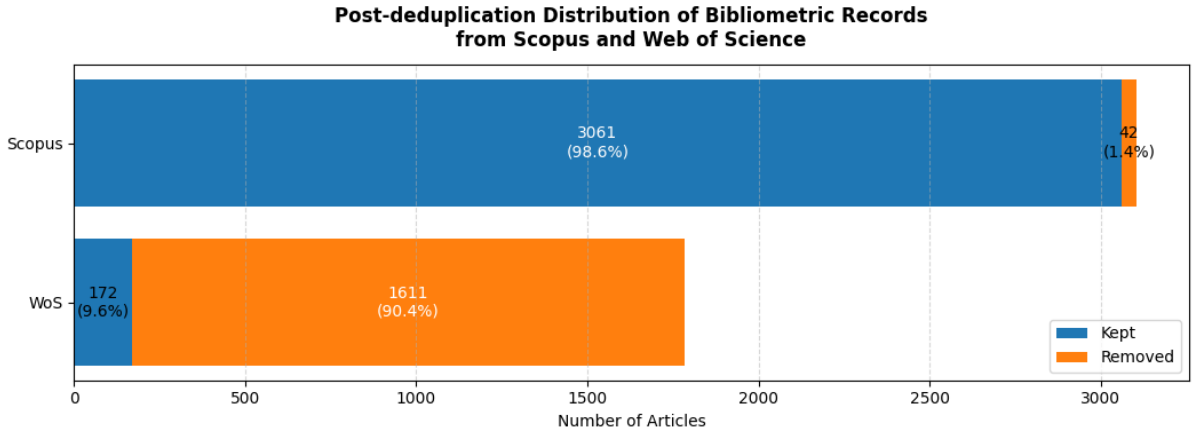
TS=("virtual private network" OR VPN* OR (VPN NEAR/3 network*)) AND TS=(security OR cybersecurity OR IPsec OR "SSL" OR "TLS" OR "SSL/TLS" OR "SSL VPN" OR "TLS VPN" OR "OpenVPN" OR "WireGuard" OR "L2TP" OR "PPTP" OR "OpenConnect" OR "SoftEther" OR "remote access" OR "site-to-site" OR "site to site" OR "quality of service" OR QoS OR latency OR throughput OR jitter OR "packet loss" OR performance OR IoT OR "internet of things" OR "edge computing" OR "5G" OR "6G" OR "zero trust" OR ZTNA OR "SD-WAN") AND PY=(2004-2024) AND DT=(ARTICLE OR PROCEEDINGS PAPER)

Criterios de inclusión y exclusión

Se incluyeron artículos y actas de conferencias que trataban sobre VPN y ciberseguridad en el periodo 2004-2024. Se excluyeron editoriales, notas técnicas, duplicados y registros sin metadatos mínimos (título, año, fuente), ver figura 1.

Extracción y limpieza de datos

Figura 1. *Depuración de datos finales*



Fuente: Elaboración Propia

La descarga inicial arrojó 4886 registros: 3103 de Scopus (63,5 %) y 1783 de WoS (36,5 %).

Se detectaron duplicados internos antes de la fusión: 42 en Scopus y 21 en WoS.

Tras combinar las bases de datos, la detección de duplicados entre bases de datos identificó 1600 documentos repetidos: 932 por DOI y 668 por título similar.

El conjunto final constaba de 2200 artículos únicos. Los títulos repetidos se guardaron en wos_scopus_repeatedstitles.csv.

Detalles técnicos de la limpieza

- Preprocesamiento de títulos con normalización de texto, eliminación de signos de puntuación, lematización en inglés y palabras vacías.
- Armonización de tipos de documentos (unificación de Proceedings Paper a Conference paper).
- Normalización de DOI a minúsculas sin prefijos.

- Asignación de ISSNatítulo canónico con SCImago; resolución por ISSN y coincidencia difusa cuando es necesario.

- Reparación y normalización de afiliaciones; consolidación de países con reglas de sustitución (por ejemplo, EE. UU. a Estados Unidos).

Corrección de palabras clave con un script de sustitución controlada:

- Recuento de palabras clave de autor: 17 577 a 17 365 únicas después de la limpieza.

- Recuento de palabras clave del índice: 14 955 a 14 758 únicas después de la limpieza.

- Protección explícita de «VPN» para evitar sustituciones erróneas; normalización de variantes como IPsec, SSL/TLS, WireGuard, QoS y SD-WAN.

Detección de duplicados y parámetros

El proceso adoptó un esquema de dos etapas:

1. Coincidencia exacta por DOI.

2. Coincidencia difusa por título con RapidFuzz (WRatio) y umbral=88. En caso de conflicto, se conservó la versión con los metadatos más completos y el mayor número de citas.

Variables y ventanas temporales

Se presentaron análisis descriptivos y series anuales para 2010-2024 debido a la disponibilidad y la coherencia tras la limpieza, aunque la estrategia de búsqueda abarcaba 2004-2024.

Indicadores y software

- Producción y citas: series anuales, ratio artículos/conferencias, crecimiento reciente.
- Redes: coautoría, coocurrencia de palabras clave y cocitación.
- Herramientas: Python (pandas, RapidFuzz, spaCy, matplotlib), ScientoPy para los indicadores, VOSviewer para las redes.
- Informe: diagrama PRISMA 2020 con recuentos de identificación, selección, elegibilidad e inclusión.

Síntesis cualitativa

Se seleccionó un subconjunto para su revisión cualitativa utilizando dos criterios concurrentes:

a) Mayor impacto (citas principales normalizadas por año) y b) Actualidad (≥ 2020) con diversidad temática y geográfica.

La extracción recopiló el contexto, los protocolos evaluados, las métricas de rendimiento (latencia, rendimiento, fluctuación, pérdida de paquetes, uso de CPU/RAM), los resultados y las limitaciones.

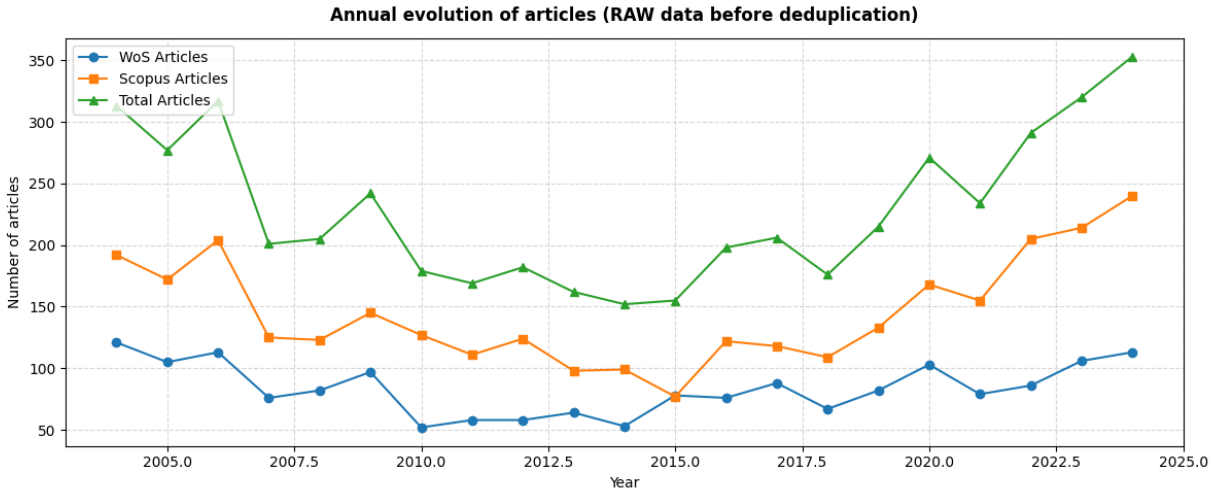
Análisis de resultados

Reproducibilidad

Los scripts para la limpieza, deduplicación y generación de figuras se documentaron con las versiones de la biblioteca, los parámetros y las rutas de salida. El archivo consolidado se guardó como datawos_scopus.csv y los duplicados como wos_scopus_repeatedstitles.csv.

Producción Científica Anual

Figura 2. *Producción científica*



Fuente: Elaboración Propia

La Figura 2, titulada Evolución anual de publicaciones sobre VPN y ciberseguridad (2004–2024), muestra un patrón de crecimiento irregular hasta 2015, seguido de un incremento sostenido en la producción científica durante la última década. En los primeros años del período analizado, la producción total combinada se mantuvo por debajo de 200 publicaciones anuales, mientras que a partir de 2016 se observó una tendencia ascendente que culminó con 353 documentos en 2024, el valor más alto de toda la serie. Este comportamiento refleja el creciente interés académico y tecnológico por la seguridad de redes, el trabajo remoto y la expansión de infraestructuras IoT y 5G.

En términos de fuentes, Scopus concentró la mayor proporción de artículos, con un promedio superior al 60 % del total anual, mientras que Web of Science mantuvo un aporte constante en torno al 35 %. Los años 2020 y 2023 constituyen puntos de inflexión, con un aumento simultáneo de ambas bases debido al auge de investigaciones relacionadas con el teletrabajo y las políticas de acceso remoto seguro durante la pandemia de COVID-19.

El análisis de citas acumuladas confirma esta tendencia ascendente: a partir de 2016, la cantidad de citas experimentó un incremento sostenido que alcanzó su punto máximo en 2023, con más de 5 000 citas registradas entre ambas bases. Este comportamiento sugiere una consolidación temática y la madurez del campo en torno a nuevos protocolos como WireGuard, la integración de inteligencia artificial en seguridad de red, y la adopción de arquitecturas zero trust y SD-WAN.

Respecto al tipo de documento, la categoría artículo científico representó la mayor proporción del total, seguida de los artículos de conferencia, lo que confirma la importancia de los congresos especializados en la difusión de avances técnicos dentro del ámbito de las redes y la ciberseguridad. No se identificó una presencia significativa de capítulos de libro o documentos retractados, lo cual refuerza la fiabilidad del corpus analizado.

En conjunto, la evolución cuantitativa de la literatura demuestra un cambio estructural en el interés académico y profesional por las VPN, especialmente en su vínculo con la seguridad de entornos distribuidos, la eficiencia del tráfico cifrado y las implementaciones en sectores productivos y educativos. El incremento sostenido observado desde 2018 indica que la temática continúa en expansión y que la investigación futura tenderá a consolidar enfoques híbridos basados en inteligencia artificial, virtualización y seguridad predictiva.

Autores más relevantes

El análisis de coautoría permitió identificar a los investigadores y grupos que han ejercido mayor influencia en el desarrollo del campo de las redes privadas virtuales y la ciberseguridad entre 2004 y 2024. El conjunto de datos reveló seis clústeres principales de colaboración científica, conformados por más de cincuenta autores con vínculos de cooperación sostenida y productividad significativa.

El Clúster 1 concentró a autores del ámbito europeo, principalmente asociados a instituciones italianas y españolas. Dentro de este grupo se destacan Antonio A. Pastor, Fulvio Valenza, Cataldo Basile y Guido Marchetto, quienes abordaron aspectos relacionados con la arquitectura segura de redes, los mecanismos de autenticación y la integración de VPN con entornos de nube. Este clúster se caracteriza por una fuerte densidad de enlaces, lo que evidencia una red de colaboración estable y productiva en estudios aplicados de seguridad en redes empresariales y gubernamentales.

El Clúster 2 estuvo conformado mayoritariamente por investigadores asiáticos vinculados a universidades japonesas, como Masahiko Emoto, Hideya Nakanishi, Masayuki Yoshikawa y Masaki Ohsuna. Este grupo concentró su producción en la evaluación de protocolos de comunicación, el desempeño de VPN en entornos de alto tráfico y la implementación de soluciones seguras para infraestructuras críticas. Su alta cohesión sugiere la existencia de laboratorios especializados en redes seguras y virtualización, con aportes relevantes a la investigación aplicada y experimental.

El Clúster 3, también de predominio japonés, reunió a autores como Shunji Abe, Kensuke Fukuda, Michihiro Koibuchi y Kenjiro Yamanaka, quienes centraron su atención en la optimización del rendimiento de VPN, el control de tráfico y los mecanismos de calidad de servicio (QoS). Sus contribuciones se orientaron hacia la eficiencia de los protocolos y la detección de anomalías en redes cifradas, aspectos fundamentales para el desarrollo de infraestructuras seguras en la era digital.

El Clúster 4 agrupó a investigadores europeos vinculados a proyectos colaborativos transnacionales. Destacaron Dimitri Papadimitriou, Ricard Vilalta, Lluis Gifre Renom y Thomas Zinner, quienes impulsaron estudios sobre virtualización de funciones de red (NFV) y redes definidas por software (SDN) aplicadas a entornos VPN. Este grupo constituye un puente entre los enfoques de seguridad clásica y las nuevas arquitecturas orientadas a servicios en la nube y redes de quinta generación.

El Clúster 5, de menor tamaño, reunió a Thomas Lorünser, Andreas Neppach y Christian Pfaffel-Janser, vinculados a líneas de investigación centradas en criptografía avanzada, privacidad de datos y autenticación distribuida. Su especialización ha contribuido a reforzar la dimensión criptográfica del estudio de las VPN, en especial en aplicaciones gubernamentales y bancarias.

Finalmente, el Clúster 6, encabezado por Shigeo Urushidani, integró a investigadores como Ichiro Inoue, Michihiro Aoki y Ryuichi Matsuzaki, con aportes en el diseño de arquitecturas de red resilientes y la medición del desempeño de túneles cifrados. Este grupo presenta alta centralidad dentro del mapa, lo que evidencia su papel articulador entre distintas comunidades científicas.

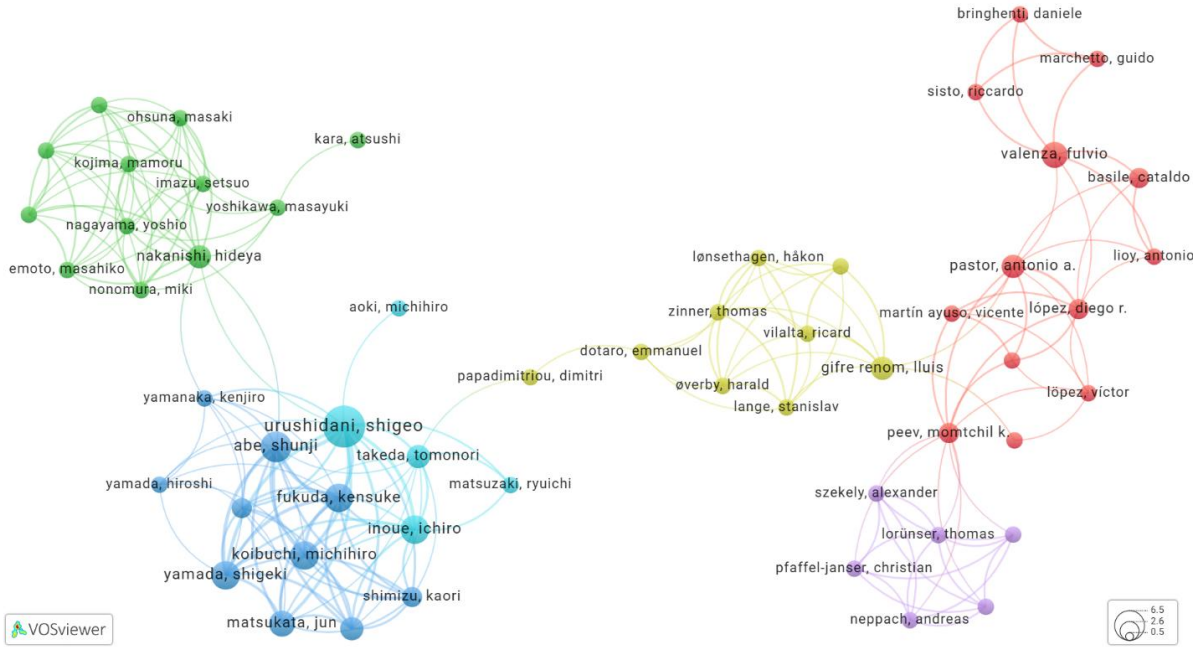
En términos de productividad individual, el análisis identificó a Renato J. Figueiredo como el autor con mayor número de publicaciones (19 documentos y 164 citas), seguido de Dan Ionescu (18 documentos y 78 citas) y Shigeo Urushidani (13 documentos y 94 citas). Asimismo, Madhusanka Liyanage destacó por su alto impacto relativo, con 296 citas en 11 trabajos, lo que refleja la pertinencia de sus investigaciones en VPN para entornos 5G y seguridad en IoT. Otros autores influyentes fueron Andrei V. Gurtov, Alexander V. Uskov, Hussein T. Mouftah y Xenakis Christos K., quienes abordaron temáticas relacionadas con la autenticación, la gestión del tráfico cifrado y la integración de VPN con sistemas de inteligencia artificial.

La distribución de autores refleja la presencia de dos polos geográficos dominantes: Asia (principalmente Japón y China) y Europa (especialmente Italia, España y Alemania). Estos polos concentran las principales redes de colaboración y producción conjunta, lo que sugiere una internacionalización moderada del campo, todavía centrada en comunidades regionales consolidadas.

En síntesis, el análisis de coautoría pone de manifiesto la existencia de comunidades científicas interconectadas que han impulsado el progreso del

conocimiento sobre redes privadas virtuales. Las alianzas entre universidades europeas y asiáticas han permitido generar una base sólida de investigación aplicada, con proyección hacia la implementación de entornos seguros y de alta disponibilidad en la nueva generación de infraestructuras digitales, ver figura 3.

Figura 3. *Red de coautoría de investigadores en VPN y ciberseguridad (2004–2024).*



Fuente: Elaboración Propia

Revistas y fuentes más relevantes

El análisis de las fuentes de publicación permitió identificar los canales de difusión más representativos de la producción científica sobre redes privadas virtuales y ciberseguridad durante el período 2004–2024. Los resultados evidencian una fuerte concentración de artículos en congresos especializados y series editoriales de alto impacto, lo que confirma el carácter eminentemente técnico y aplicado del campo.

La Figura 3, titulada Fuentes de publicación más relevantes en VPN y ciberseguridad (2004–2024), muestra que la ACM International Conference Proceeding

Series y la Lecture Notes in Computer Science constituyen las principales plataformas de divulgación, ambas con 40 documentos indexados. Estas fuentes mantienen una orientación hacia la ingeniería de redes, la seguridad de protocolos y la evaluación de rendimiento en entornos de virtualización. Aunque el crecimiento reciente en la ACM se ha mantenido estable, la colección Lecture Notes in Computer Science presentó una renovación temática significativa, con el 20 % de sus publicaciones concentradas en el bienio 2023–2024, lo que refleja su adaptabilidad a los nuevos escenarios tecnológicos.

La revista IEEE Access ocupa el tercer lugar con 33 publicaciones y un índice h de 15, evidenciando su papel como principal medio abierto de difusión de investigaciones recientes. Destaca su tasa de crecimiento relativa de 27,3 % en los dos últimos años, impulsada por estudios sobre Zero Trust Network Access (ZTNA), SD-WAN y la integración de inteligencia artificial en la gestión de tráfico cifrado.

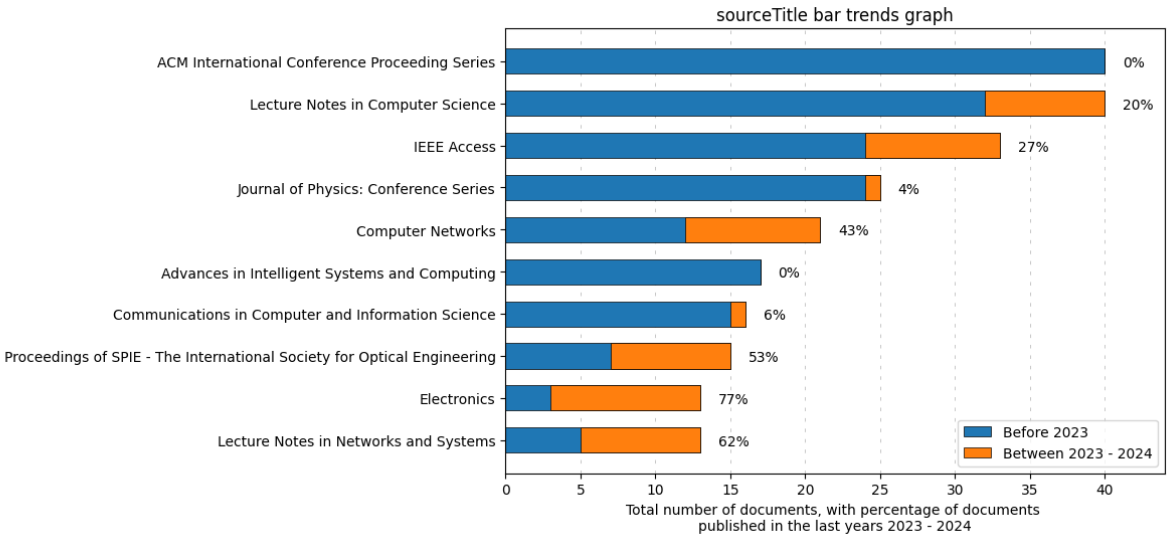
En cuarto lugar, se ubica el Journal of Physics: Conference Series con 25 contribuciones, que, aunque de orientación generalista, ha servido como espacio para la presentación de trabajos sobre modelado de redes y simulaciones de rendimiento. Le sigue Computer Networks, revista con 21 artículos y un crecimiento reciente del 42,9 %, consolidada como una de las publicaciones más influyentes en el ámbito de la ingeniería de comunicaciones y seguridad en redes distribuidas.

Otras fuentes relevantes incluyen Advances in Intelligent Systems and Computing, Communications in Computer and Information Science y los Proceedings of SPIE, cada una con entre 15 y 17 publicaciones. Estas series concentran investigaciones orientadas a la computación distribuida, la seguridad en IoT y la encriptación óptica. Particularmente, los Proceedings of SPIE presentaron un incremento del 53,3 % en los últimos años, impulsado por aplicaciones experimentales de ciberseguridad en entornos industriales.

En el segmento de revistas de acceso abierto, Electronics y Lecture Notes in Networks and Systems se destacan por su crecimiento reciente. Ambas presentan más del 60 % de sus artículos publicados entre 2023 y 2024, lo que refleja su rápida consolidación como fuentes emergentes en el estudio de redes definidas por software, optimización del tráfico y seguridad en infraestructuras de próxima generación.

En síntesis, el patrón de publicación confirma que el campo de las redes privadas virtuales se desarrolla en un entorno de alta rotación tecnológica y colaboración interdisciplinaria, donde los congresos internacionales y las series editoriales especializadas actúan como los principales canales de difusión científica. La tendencia hacia revistas de acceso abierto y de alcance multidisciplinario anticipa una expansión del área en los próximos años, impulsada por la integración de tecnologías 5G, inteligencia artificial y soluciones de bajo costo para entornos empresariales y educativos, ver figura 4.

Figura 4. *Fuentes de publicación más relevantes en VPN y ciberseguridad (2004–2024).*



Fuente: Elaboración Propia

Palabras clave y áreas temáticas emergentes

El análisis de co-ocurrencia de palabras clave permitió identificar los principales ejes temáticos y las líneas de investigación que han estructurado la producción científica sobre redes privadas virtuales y ciberseguridad durante el período 2004–2024. La red generada por VOSviewer (Figura 4) muestra una organización semántica compuesta por seis clústeres interconectados, con predominio de términos asociados a virtual private network, network security y cryptography, que conforman el núcleo conceptual del campo.

El término “virtual private network” presentó la mayor frecuencia de aparición con 1 436 ocurrencias, lo que confirma su rol central en la estructura del conocimiento. En torno a él se agrupan expresiones vinculadas a la arquitectura y funcionamiento de redes seguras, tales como network protocol (310), internet protocol suite (424), quality of service (399), security of data (285), van (638) y cryptography (450). Estos nodos principales reflejan el interés sostenido por la mejora de la seguridad, la estabilidad y el rendimiento de las conexiones virtuales en entornos distribuidos.

El Clúster 1 agrupa términos relacionados con la gestión del rendimiento y la infraestructura de red, como network management, router, packet loss, bandwidth, multi-protocol label switching y quality of service. Estos conceptos evidencian un enfoque técnico orientado a la optimización del tráfico cifrado, la reducción de latencia y la confiabilidad de las comunicaciones seguras.

El Clúster 2 reúne palabras vinculadas con la seguridad informática y la detección de amenazas, destacándose network security (812), data privacy (96), encryption (48), firewall (50), intrusion detection (95), malware (54) y machine learning (84). La aparición conjunta de deep learning (100) y traffic classification (93) evidencia una tendencia hacia el uso de inteligencia artificial para la clasificación y detección de

tráfico cifrado, una línea de investigación en expansión que fortalece la seguridad en entornos VPN.

El Clúster 3 está dominado por los términos internet protocol security (84), internet key exchange (38), secure socket layer (58) y security protocol (34), vinculados con los mecanismos de autenticación y cifrado. Este conjunto evidencia la continuidad de estudios dedicados a protocolos como IPSec, SSL/TLS, OpenVPN y WireGuard, que constituyen la base tecnológica de las implementaciones actuales de VPN en contextos empresariales y educativos.

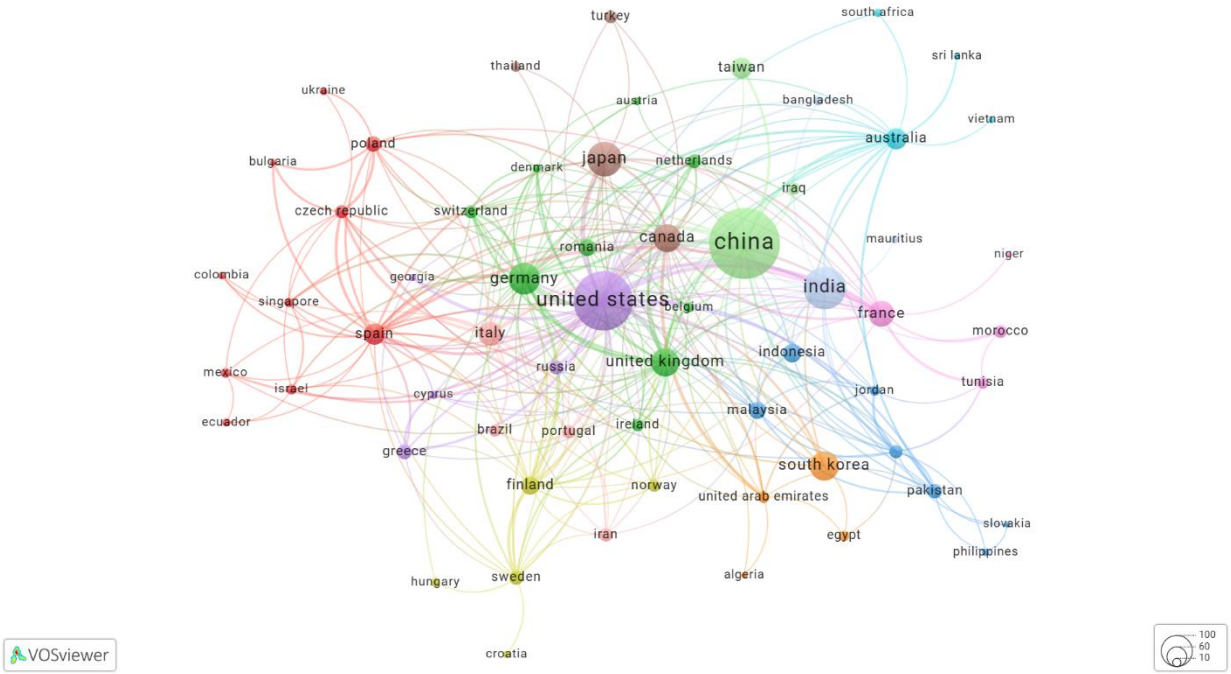
El Clúster 4 agrupa conceptos emergentes asociados con la virtualización y el cómputo en la nube, tales como cloud computing (105), software defined networking (78), virtual network (31) y virtual machine (26). Estos términos reflejan la integración progresiva de las VPN en infraestructuras virtuales, entornos de edge computing y redes 5G, impulsando configuraciones más dinámicas y seguras.

El Clúster 5 conecta los ámbitos de autenticación, inteligencia artificial y sistemas de información, con términos como authentication (233), artificial intelligence (56), automation (58) y information technology (94). Este grupo evidencia un giro hacia modelos predictivos de seguridad y sistemas automatizados de detección de intrusiones, fundamentales para la administración de redes privadas virtuales de nueva generación.

La convergencia de estos clústeres refleja una evolución temática desde los estudios tradicionales de protocolos y desempeño hacia enfoques híbridos basados en IA, virtualización y seguridad de datos. Además, el crecimiento reciente de términos como internet of things (151) y fifth generation mobile network (60) confirma la ampliación del campo hacia aplicaciones en IoT y 5G, donde las VPN se consolidan como elementos esenciales para la protección de dispositivos conectados y la gestión segura del tráfico distribuido.

En conjunto, los resultados confirman que la investigación sobre redes privadas virtuales transita de un paradigma centrado en la conexión segura hacia un modelo inteligente, automatizado y adaptativo, en el que la privacidad, la velocidad y la resiliencia del sistema constituyen ejes estratégicos de desarrollo científico y tecnológico, ver figura 5.

Figura 5. *Mapa de co-ocurrencia de palabras clave en estudios sobre VPN y ciberseguridad (2004–2024).*



Fuente: Elaboración Propia

Instituciones líderes y redes de colaboración académica

El análisis institucional permitió identificar las universidades y centros de investigación que han desempeñado un papel central en la producción científica sobre redes privadas virtuales y ciberseguridad entre 2004 y 2024. Los resultados muestran una estructura de colaboración global compuesta por dieciséis clústeres, en la que prevalece la concentración de instituciones asiáticas, seguidas por universidades de Norteamérica y Europa.

El Clúster 1, dominado por instituciones japonesas, agrupa al Institute of Science Tokyo, Kyushu University, Nara Institute of Science and Technology y The University of Tokyo, junto con la University of Technology Sydney (Australia) y la Ruhr-Universität Bochum (Alemania). Este grupo mantiene una fuerte cooperación en áreas de protocolos de comunicación segura, cifrado y evaluación del rendimiento de redes VPN, reflejando la tradición japonesa en ingeniería de telecomunicaciones y criptografía aplicada.

El Clúster 2 reúne a universidades de alto impacto global, entre ellas la University of California, Tsinghua University, University of Michigan y Johns Hopkins University. Estas instituciones constituyen el núcleo de la investigación de frontera en ciberseguridad, inteligencia artificial aplicada a redes, y sistemas de autenticación basados en criptografía avanzada. La University of California destaca por su productividad (25 artículos y 895 citas), mientras que Tsinghua University lidera en Asia continental con 25 publicaciones y 360 citas, consolidando su posición como referente en desarrollo de arquitecturas seguras y protocolos emergentes como WireGuard y SD-WAN.

El Clúster 3, conformado por universidades norteamericanas como Carnegie Mellon University, Princeton University y Yale University, se especializa en la modelización de seguridad en redes distribuidas y en la integración de aprendizaje automático en la detección de amenazas en VPN cifradas. Sus contribuciones se asocian con proyectos experimentales en entornos académicos y corporativos, y presentan altos índices de citación, con promedios superiores a las 150 citas por institución.

El Clúster 4 incluye a universidades chinas como Beihang University, Jilin University, Xi'an Jiaotong University y Wuhan University of Technology, caracterizadas por su producción sostenida y cooperación interna. Estas instituciones concentran

estudios sobre optimización de redes 5G, computación en la nube y virtualización de funciones de red, componentes clave de las VPN de nueva generación.

El Clúster 5, liderado por instituciones de India como Vellore Institute of Technology, SRM Institute of Science and Technology y Chitkara University, refleja un avance significativo de la investigación india en seguridad de redes empresariales, edge computing y entornos educativos digitales. Aunque su volumen de citación es moderado, este grupo ha contribuido a la expansión del conocimiento aplicado en soluciones de bajo costo y de amplia adopción regional.

En el contexto de Corea del Sur, el Clúster 6 está compuesto por la Korea University, la Kyungpook National University y la Sungkyunkwan University, junto al Electronics and Telecommunications Research Institute (ETRI), uno de los principales centros tecnológicos de Asia. Estas instituciones destacan por sus investigaciones sobre seguridad en redes móviles, IoT y comunicaciones 5G, aportando avances técnicos orientados a la eficiencia energética y al cifrado de tráfico en tiempo real.

El Clúster 7, de predominio chino, agrupa a la Shanghai Jiao Tong University, la South China University of Technology y la University of Science and Technology of China, esta última con 902 citas, una de las cifras más altas del conjunto. Este grupo representa una red de excelencia en cifrado cuántico, autenticación y redes definidas por software, con alto grado de internacionalización.

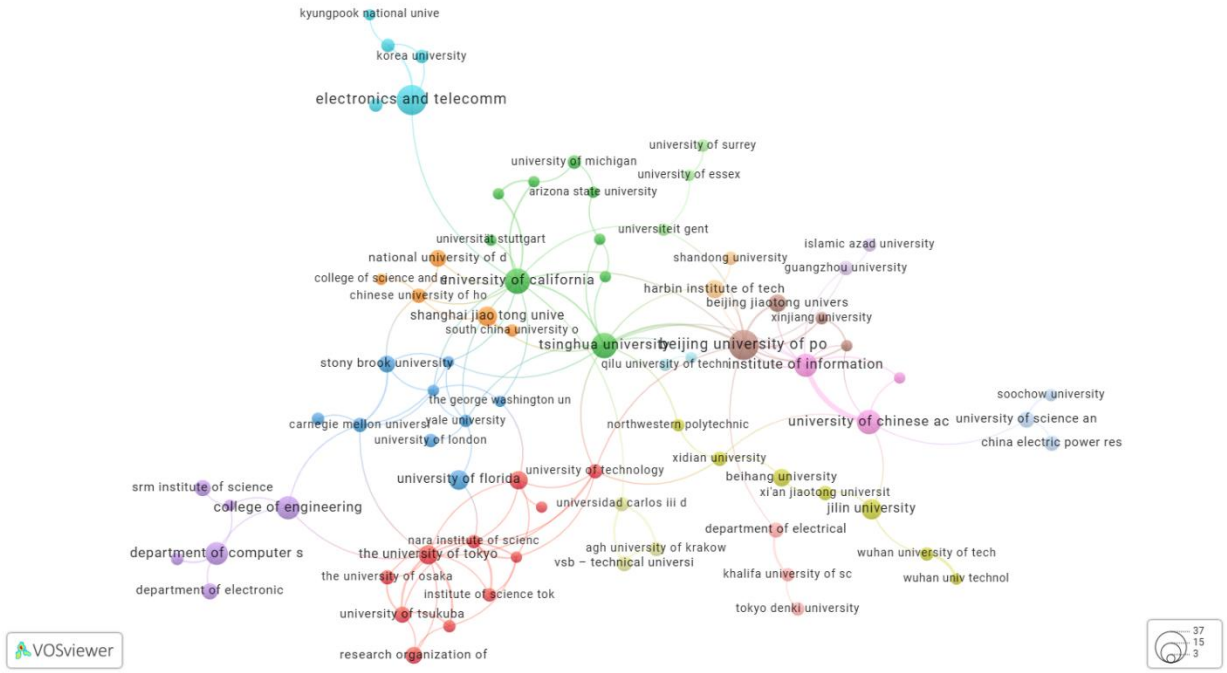
Otros clústeres, como el Clúster 8 (Beijing Jiaotong University, Beijing University of Posts and Telecommunications, Beijing University of Technology) y el Clúster 9 (Beijing Institute of Technology, Institute of Information Engineering, University of Chinese Academy of Sciences), consolidan el liderazgo chino en investigación aplicada y desarrollo de infraestructura nacional de ciberseguridad. Destaca el Institute of Information Engineering con 474 citas, que sobresale por sus contribuciones en detección de intrusiones y cifrado en redes gubernamentales.

En Europa, la Universidad Carlos III de Madrid (España) y la AGH University of Krakow (Polonia), agrupadas en el Clúster 13, representan los principales nodos regionales, con investigaciones orientadas a la seguridad en sistemas de información y evaluación del tráfico cifrado. Asimismo, la Universiteit Gent (Bélgica) y la University of Surrey (Reino Unido), integradas en el Clúster 11, destacan por su alta visibilidad internacional, con más de 800 citas combinadas, en temas de virtualización y privacidad de datos.

De manera general, el panorama institucional confirma un ecosistema global de investigación altamente diversificado, con predominio de universidades asiáticas y norteamericanas que articulan redes de colaboración intercontinental. Las instituciones europeas, aunque con menor volumen de publicaciones, mantienen altos índices de impacto y se posicionan como intermediarias entre los polos científicos de Asia y América del Norte.

En conjunto, las universidades y centros identificados configuran una red de excelencia académica que impulsa el avance de la ciberseguridad, la criptografía aplicada y la ingeniería de redes privadas virtuales. La tendencia hacia colaboraciones internacionales, la adopción de tecnologías emergentes y la orientación hacia el código abierto refuerzan la convergencia entre el ámbito académico y la innovación tecnológica global, ver figura 6.

Figura 6. *Red institucional de colaboración en estudios sobre VPN y ciberseguridad (2004–2024).*



Fuente: Elaboración Propia

Países e instituciones líderes

El análisis de la producción científica por país revela una clara concentración geográfica de la investigación sobre redes privadas virtuales y ciberseguridad entre 2004 y 2024. La red de colaboración internacional (Figura 5) muestra una estructura global en la que predominan los aportes de Asia, América del Norte y Europa, con una participación creciente de países emergentes de América Latina y Medio Oriente.

El liderazgo científico corresponde a China y a los Estados Unidos, que concentran conjuntamente más del 55 % de la producción total. China ocupa la primera posición con 741 publicaciones y 5 781 citas, seguida por los Estados Unidos con 519 artículos y 7 379 citas. Ambos países conforman el eje central del mapa de cooperación, caracterizado por una alta interconexión con Europa y Oceanía. La preeminencia de estas dos naciones se asocia con su inversión sostenida en investigación aplicada sobre

ciberseguridad, criptografía y redes 5G, así como con la consolidación de instituciones como la Tsinghua University, la Chinese Academy of Sciences, la University of California y el Massachusetts Institute of Technology.

En el contexto asiático, Japón (178 documentos, 1 135 citas) y India (267 documentos, 1 498 citas) ocupan posiciones destacadas, impulsadas por universidades con fuerte orientación tecnológica. Japón mantiene una tradición consolidada en la optimización de protocolos y arquitecturas seguras, mientras que India ha diversificado su investigación hacia la integración de machine learning y detección de intrusiones en entornos VPN. Corea del Sur, con 125 documentos y 492 citas, refuerza este bloque regional con aportes en seguridad de redes móviles y sistemas IoT.

En Europa, los países más productivos son Alemania (147 publicaciones, 1 935 citas), Reino Unido (116 publicaciones, 2 169 citas), Francia (98 publicaciones, 1 145 citas) e Italia (85 publicaciones, 1 034 citas). Alemania y el Reino Unido destacan por su liderazgo en proyectos colaborativos sobre redes definidas por software (SDN), virtualización de funciones de red (NFV) y Zero Trust Network Access (ZTNA). Por su parte, España presenta 66 publicaciones y 698 citas, consolidándose como el principal referente del ámbito hispanohablante y el nodo europeo con mayor interacción con América Latina.

Dentro de América Latina, los países más activos son Brasil (22 documentos, 106 citas), México (14 documentos, 42 citas), Colombia (8 documentos, 94 citas) y Ecuador (10 documentos, 70 citas). Estos resultados reflejan un interés incipiente, aunque en expansión, en temas relacionados con el teletrabajo seguro, la infraestructura educativa digital y la protección de datos en entornos institucionales. España actúa como puente de cooperación principal para los países latinoamericanos, según la densidad de enlaces mostrada en el mapa.

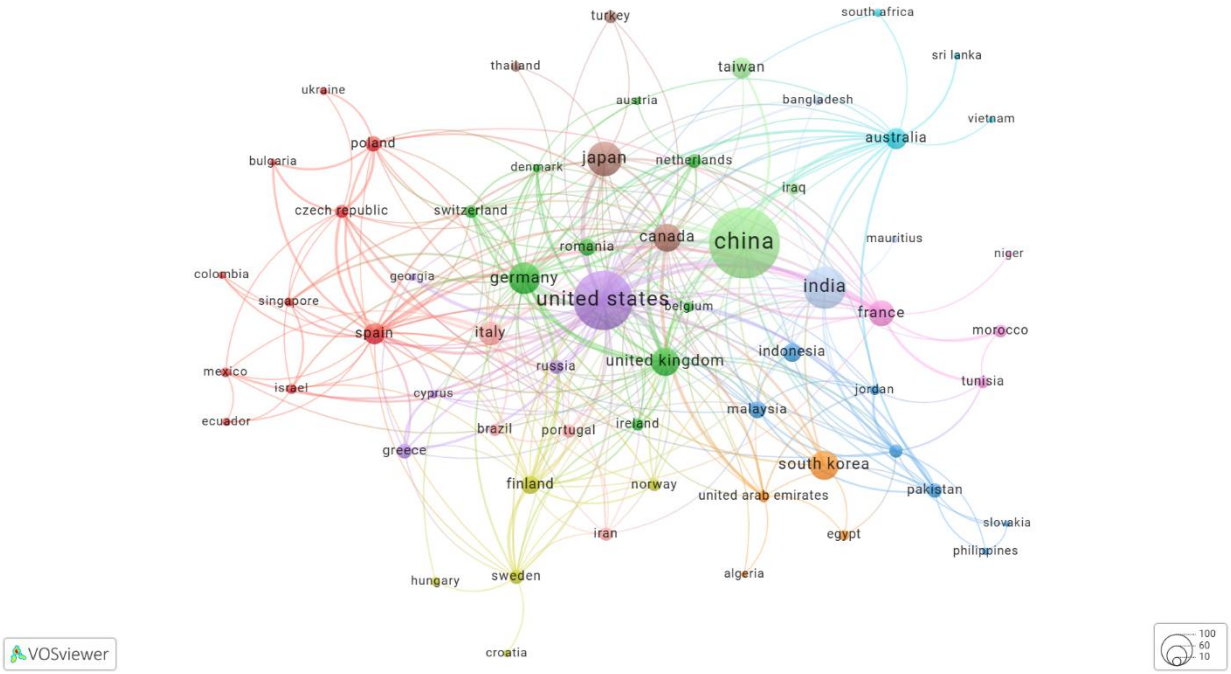
El análisis de los clústeres de colaboración evidencia doce comunidades geográficas interrelacionadas. El Clúster 1, liderado por España, agrupa a varios países de Europa del Este y América Latina (México, Colombia, Ecuador, Polonia y República Checa), lo que revela una red de cooperación Sur–Europa orientada a la aplicación práctica de tecnologías VPN en sectores públicos y educativos. El Clúster 2, integrado por Alemania, Reino Unido, Países Bajos, Irlanda, Bélgica y Suiza, representa la comunidad europea más consolidada, con alta productividad y citación media elevada. En Asia, el Clúster 3 reúne a Malasia, Indonesia, Pakistán y Filipinas, centrados en la seguridad de datos y las implementaciones de VPN en redes inalámbricas.

Por su parte, el Clúster 5, encabezado por los Estados Unidos, agrupa a Rusia, Grecia y Chipre, configurando una red transatlántica caracterizada por proyectos de simulación, criptografía avanzada y gestión de tráfico cifrado. Asimismo, el Clúster 8, compuesto por Canadá, Japón, Turquía y Tailandia, evidencia la diversificación de colaboraciones intercontinentales en entornos de telecomunicaciones y seguridad móvil.

De manera general, la cooperación internacional ha aumentado de forma progresiva en la última década, reflejando la necesidad de compartir conocimiento técnico y estándares de seguridad. Sin embargo, persisten brechas regionales, especialmente en África y América del Sur, donde la producción científica continúa limitada por factores estructurales y tecnológicos.

En síntesis, la distribución geográfica confirma un patrón de investigación altamente concentrado y asimétrico, dominado por potencias tecnológicas y con redes de colaboración cada vez más globalizadas. No obstante, el crecimiento de publicaciones en países emergentes sugiere una tendencia hacia la descentralización del conocimiento, **impulsada** por la expansión del acceso a infraestructuras digitales, la adopción de políticas de ciberseguridad y la consolidación de programas universitarios especializados en redes seguras, ver figura 7.

Figura 7. *Red de colaboración internacional en estudios sobre VPN y ciberseguridad (2004–2024).*



Fuente: Elaboración Propia

Discusión

La comparación entre familias de protocolos confirma un patrón dual: IPSec ofrece madurez, granularidad de políticas y amplia interoperabilidad, mientras SSL/TLS simplifica accesos remotos y compatibilidad con aplicaciones, aunque con costes de rendimiento bajo cargas elevadas. Los resultados sostienen decisiones por caso de uso, con énfasis en requisitos de desempeño y de control criptográfico en capas de red y transporte (Mao, Zhu, & Qin, 2012; Narayan, Kolahi, Brooking, & de Vere, 2008).

Los cuellos de botella de SSL-VPN en pasarelas comerciales aparecen documentados en pruebas con tráfico de gran tamaño y altas tasas de uso de CPU. Optimizaciones de captura de paquetes con PF_RING incrementan el rendimiento y reducen la latencia en túneles SSL, lo que sugiere una línea de mejora basada en I/O y

fast path de usuario cuando el cifrado no representa el único límite (Mache & Likarish, 2005; Wu KeHe, Zhao, Cui WenChao, Zhang XianKang, & Cui AJun, 2019).

El efecto de la negociación TLS sobre APCS y sistemas críticos depende del hardware y de versiones de protocolo, con incidencias sobre el tiempo de establecimiento de sesiones seguras. Dicho hallazgo exige perfiles de riesgo distintos para control industrial y para acceso corporativo general, y valida estrategias de offloading y de reducción de handshakes en segmentos sensibles al retardo (Rybin, Piliugina, & Piliugin, 2018).

La convergencia con SDN/SD-WAN reconfigura el papel de la VPN. SD-VPN muestra control en tiempo real y orquestación automática, mientras P4-IPsec traslada funciones de túnel a planos de datos programables. Ambos enfoques apuntan a cadenas de servicio más flexibles y a una reducción de complejidad en IKE cuando el controlador asume tareas de aprovisionamiento, con horizontes de extensibilidad hacia servicios avanzados (Fu, Wang, Liu, & Wang, 2024; Hauser, Haeberle, Schmidt, & Menth, 2020).

El aseguramiento de QoS en VPN mantiene relevancia transversal. Modelos de control de flujos con garantías mínimas por flujo sostienen un uso eficiente del ancho de banda. En tramos metro/core con GMPLS y en dominios de operador con MPLS/MP-BGP, combinaciones DiffServ, WFQ y WRED muestran mejoras en retardo, jitter y pérdida, lo que favorece acuerdos de nivel de servicio en servicios multisede y colaboración remota (Sabrina & Rogers, 2007; Rea et al., 2008; Beyene & Argaw, 2019).

Las políticas y su corrección inter-dominio siguen como punto crítico. Definiciones formales de requisitos y criterios de corrección reducen errores de configuración, mientras auditorías de MPLS/VPN con análisis inverso de configs priorizan mitigaciones sobre perímetros expuestos. Además, técnicas de reducción de reglas IPSec disminuyen tiempos de actualización sin degradar requisitos de seguridad

(Yang, Martel, Fu, & Wu, 2006; Llorens & Serhrouchni, 2007; Sadeghi, Ali, Pedram, Deghan, & Sabaei, 2009).

Los casos de uso aportan evidencias prácticas. En logística, la combinación VPN + GPS eleva eficiencia operativa y control de flotas; en nube y big data, el binomio VPN + firewall mejora seguridad con impacto limitado sobre rendimiento, siempre que exista dimensionamiento adecuado. Dichos resultados refuerzan la viabilidad de arquitecturas de costo contenido en PYMES y sector público (Alhadidi, Baniata, Baniata, Al-Ali, & Althwaini, 2012; Shah, ud Din, Abizar, ud Din, & Khan, 2020).

La adopción de Zero Trust no elimina la superficie de riesgo cuando sobreviven dispositivos heredados de firewall/VPN en el perímetro. El análisis de amenazas en ZTNA expone vectores de explotación y recomienda contramedidas, lo que sugiere planes de transición que contemplen convivencia y endurecimiento de activos existentes (Kim & Sohn, 2024). En IoT-MANET, configuraciones de VPN elevan resiliencia frente a jammers y mejoran retardo, rendimiento y pérdidas, con efectos verificables en simulación para diferentes cargas y potencias de interferencia (Nourildean, 2024).

Las propuestas open-source complementan el panorama. OpenVPN aporta flexibilidad, autenticación variada y operación tras NAT con ventajas económicas, mientras EdgeVPN.io ejemplifica conectividad privada y programable en edge/fog con Kubernetes en nodos con NAT heterogéneo. No obstante, evaluaciones de hipervisores de red muestran limitaciones de confiabilidad para producción amplia, lo que impone pruebas graduales y hardening específico (Skendzic & Kovacic, 2017; Figueiredo & Subratie, 2020; Nurkahfi, Mitayani, Mardiana, & Dinata, 2019).

El fortalecimiento de procesos de ingeniería también resulta clave. Bancos de prueba con VM permiten validación previa, detección de errores de configuración y reajustes controlados, y servidores SSL-VPN de alta concurrencia mejoran desempeño

con colas, temporizadores y estructuras de E/S adecuadas. Estos recursos favorecen ciclos de despliegue más seguros y medibles (Chen & Lin, 2013; Chu, 2013).

Conclusiones

El campo de VPN y ciberseguridad muestra madurez tecnológica y diversidad de escenarios. IPSec y SSL/TLS cubren necesidades complementarias, con decisiones que deben alinearse con requisitos de latencia, caudal, control criptográfico, auditoría y operación multientorno. La evidencia comparativa y los resultados de simulación y laboratorio validan selecciones específicas por sector y por caso de uso (Mao et al., 2012; Narayan et al., 2008).

La convergencia con SDN/SD-WAN y con P4 reconfigura el plano de control y el de datos. SD-VPN y P4-IPsec abren rutas de automatización y elasticidad, y amplían la frontera de rendimiento y de gestión centralizada. Estas trayectorias requieren estándares de prueba, perfiles de riesgo por dominio y gobernanza de políticas para evitar errores en topologías dinámicas (Fu et al., 2024; Hauser et al., 2020).

El aseguramiento de QoS mantiene un papel estructural. Modelos de control de flujos, técnicas DiffServ/WFQ/WRED y validaciones en GMPLS/MPLS confirman ganancias en métricas clave y permiten SLA confiables en colaboración, voz y videoconferencia distribuida (Sabrina & Rogers, 2007; Rea et al., 2008; Beyene & Argaw, 2019).

La agenda de seguridad demanda tres líneas prioritarias. Primero, políticas correctas y auditables con métodos formales y reducción de reglas; segundo, transición a Zero Trust con inventario de activos y endurecimiento de equipos heredados; tercero, resiliencia IoT/5G con perfiles de latencia y tácticas contra interferencia y tráfico cifrado de difícil inspección (Yang et al., 2006; Llorens & Serhrouchni, 2007; Kim & Sohn, 2024; Nourildean, 2024).

Las líneas futuras incluyen validación formal y adopción de WireGuard, clasificación de tráfico cifrado con aprendizaje profundo, VPN cuántico-seguras con QKD en tramos metropolitanos y planificación específica para 5G con garantías de servicio. Dichos frentes delinean una agenda de investigación que combina criptografía, redes programables y analytics de tráfico cifrado con evaluación rigurosa de impacto en operación real (Lipp, Blanchet, & Bhargavan, 2019; Xian, 2021; Alia et al., 2024; Cheng & Zhou, 2022).

Referencias bibliográficas

Alhadidi, B., Baniata, L., Baniata, M., Al-Ali, M. y Althwaini, S. (2012). «Resolución del problema de las agencias de transporte mediante VPN intranet y VPN sitio a sitio». En 3.ª Conferencia Internacional sobre Tecnología Informática y Desarrollo (ICCTD 2011) (Vol. 3).

Alia, O., Huang, A., Luo, H., Amer, O., Pistoia, M. y Lim, C. (2024). Túnel VPN IPsec de sitio a sitio de 10 Gbps con seguridad cuántica a través de fibra desplegada de 46 km. En Conferencia y Exposición sobre Comunicaciones por Fibra Óptica (OFC) 2024.

Badra, M. y Hajjeh, I. (2006). Habilitación de VPN y acceso remoto seguro mediante el protocolo TLS. En WIMOB 2006: 2.ª Conferencia Internacional IEEE sobre Computación, Redes y Comunicaciones Inalámbricas y Móviles.

Bahnasse, A., Louhab, F. E., Khiat, A., Badri, A., Talea, M. y Sahel, A. (2019). Influencia de la red privada virtual multipunto dinámica en la calidad del servicio de videoconferencia. En 2.ª Conferencia Internacional sobre Aplicaciones Informáticas y Seguridad de la Información (ICCAIS).

Beyene, A. M. y Argaw, S. A. (2019). Mejora de la calidad del servicio de la red privada virtual de conmutación de etiquetas multiprotocolo del protocolo de puerta de enlace fronteriza de los acuerdos de nivel de servicio de EthioTelecom. En Tecnología de la información y la comunicación para el desarrollo de África (ICT4DA 2019) (pp. 293-308). Springer. https://doi.org/10.1007/978-3-030-26630-1_24

Bibraj, R., Chug, S., Nath, S. y Singh, S. L. (2018). Estudio técnico del acceso remoto VPN y sus ventajas sobre el VPN de sitio a sitio para analizar la posibilidad de configuraciones híbridas en estaciones de radar con tecnología de comunicación móvil en evolución. Mausam.

Cai, L. Z., Yu, S. S. y Zhou, J. L. (2004). Investigación e implementación del servicio de protocolo de escritorio remoto sobre VPN SSL. En Conferencia Internacional IEEE 2004 sobre Computación de Servicios.

Chen, C. S. y Lin, M. H. (2013). Creación de un subsistema de pruebas temporal basado en VM para evaluar la validez de un sistema híbrido SSL-VPN. En Mecatrónica, Robótica y Automatización (pp. 833-838). https://doi.org/10.4028/www.scientific.net/AMM.373-375.833

Cheng, T. y Zhou, F. (2022). Análisis de la metodología de planificación de redes privadas virtuales 5G. En 14.ª Conferencia Internacional sobre Comunicaciones Inalámbricas y Procesamiento de Señales (WCSP).

https://doi.org/10.1109/WCSP55476.2022.10039428Chu, J. (2013). Diseño e implementación de un servidor VPN SSL de alta concurrencia. En Instrumentación industrial y sistemas de control, partes 1-4 (pp. 2424-2428).

https://doi.org/10.4028/www.scientific.net/AMM.241-244.2424

Deshmukh, D., & Iyer, B. (2017). Diseño de una red privada virtual IPSec para acceso remoto. En Conferencia Internacional IEEE 2017 sobre Computación, Comunicación y Automatización (ICCCA).

Elkeelany, O., Matalgah, M. M. y Qaddour, J. (2004). Arquitectura de red privada virtual de acceso remoto para usuarios de Internet inalámbrico de alta velocidad. Comunicaciones inalámbricas y computación móvil, 4(8), 917-928. https://doi.org/10.1002/wcm.197

Eizen, K., Saito, M., Kobara, K., Nakato, Y., Kuroda, T. e Ishihara, K. (2013). Protección de SSL-VPN con LR-AKE para acceder a registros médicos personales. En MedInfo 2013: Actas del 14.º Congreso Mundial sobre Informática Médica y Sanitaria (pp. 930-934).

https://doi.org/10.3233/978-1-61499-289-9-930Figueiredo, R. y Subratie, K. (2020).

Demo: EdgeVPN.io: red privada virtual de código abierto para una computación periférica sin fisuras con Kubernetes. En Simposio IEEE/ACM 2020 sobre computación periférica (SEC 2020). https://doi.org/10.1109/SEC50012.2020.00032

Fu, C., Wang, B., Liu, H., y Wang, W. (2024). Red privada virtual definida por software para SD-WAN. Electronics, 13(13), 2674. https://doi.org/10.3390/electronics13132674

Hauser, F., Haeberle, M., Schmidt, M., y Menth, M. (2020). P4-IPsec: VPN de sitio a sitio y de host a sitio con IPsec en SDN basado en P4. IEEE Access, 8, 136879-136894. https://doi.org/10.1109/ACCESS.2020.3012738

Hashiyana, V., Haiduwa, T., Suresh, N., Bratha, A., y Ouma, F. K. (2020). Diseño e implementación de una red privada virtual IPSec: un estudio de caso en la Universidad de Namibia. En Conferencia IST-África 2020 (IST-África).

Jangid, M. K. y Trivedi, P. (2016). Mejora del rendimiento de la relación sucesiva para redes privadas virtuales. En 8.ª Conferencia Internacional sobre Inteligencia Computacional y Redes de Comunicación (CICN). https://doi.org/10.1109/CICN.2016.26

Jung, H., Han, K., & Lee, G. (2011). Un método de diseño de VPN SSL para el desarrollo de sistemas de seguridad FMC empresariales. En Convergencia y tecnología de la información híbrida.

Kim, E., & Sohn, K. (2024). Investigación sobre amenazas de seguridad utilizando VPN en entornos de confianza cero. En Aplicaciones de seguridad de la información, WISA 2023 (pp. 50–63). Springer.

https://doi.org/10.1007/978-981-99-8024-6_5Koot, M. (2020). Nota de campo sobre CVE-2019-11510: Pulse Connect Secure SSL-VPN en los Países Bajos. Amenazas digitales: investigación y práctica, 1(3),

1-10. https://doi.org/10.1145/3382765

Lee, H., Nah, J. y Jung, K. (2005). El acceso remoto a la puerta de enlace IPsec-VPN a través de IPv6 móvil. En 7.ª Conferencia Internacional sobre Tecnología de Comunicación Avanzada (Vols. 1-2, pp. 624-629). https://doi.org/10.1109/ICACT.2005.245934

Li, C. y Cai, J. (2015). La investigación sobre la aplicación de la tecnología SSL VPN en el campus digital. En Actas de la Conferencia Internacional de 2015 sobre Tecnología Educativa, Gestión y Ciencias Humanas (ETMHS 2015).

Lipp, B., Blanchet, B. y Bhargavan, K. (2019). Una prueba criptográfica mecanizada del protocolo de red privada virtual WireGuard. En 4.º Simposio Europeo IEEE sobre Seguridad y Privacidad (EuroS&P). https://doi.org/10.1109/EuroSP.2019.00026

Llorens, C. y Serhrouchni, A. (2007). Verificación de la seguridad de una red privada virtual sobre MPLS. En Control e ingeniería de redes para QoS, seguridad y movilidad, IV.

Mache, J. y Likarish, T. (2005). Evaluación del rendimiento de las puertas de enlace SSL VPN basadas en navegador. En ICOMP '05: Actas de la Conferencia Internacional sobre Computación en Internet de 2005.

Mao, H., Zhu, L. y Qin, H. (2012). Investigación comparativa sobre SSL VPN e IPSec VPN. En Conferencia Internacional sobre Comunicaciones Inalámbricas, Redes y Computación Móvil (WiCOM) de 2012.

Narayan, S., Kolahi, S. S., Brooking, K. y de Vere, S. (2008). Evaluación del rendimiento de los protocolos de redes privadas virtuales en el entorno Windows 2003. En Conferencia Internacional de 2008 sobre Teoría e Ingeniería Informática Avanzada. https://doi.org/10.1109/ICACTE.2008.187

Nourildean, S. W. (2024). Mejora del rendimiento basada en redes privadas virtuales frente a interferencias en MANET basadas en IoT. Revista de Ciencia y Tecnología de la Ingeniería.

Nurkahfi, G. N., Mitayani, A., Mardiana, V. A. y Dinata, M. M. M. (2019). Comparación entre FlowVisor y OpenVirtex como soluciones de servicios VPN de sitio a sitio basadas en SDN. En Conferencia Internacional de 2019 sobre Radar, Antenas, Microondas, Electrónica y Telecomunicaciones (ICRAMET).

Rea, L., Pompei, S., Valenti, A., Matera, F., Zema, C. y Settembre, M. (2008). Control de la calidad del servicio basado en servicios de red privada virtual en un banco de pruebas óptico Gigabit Ethernet de área amplia. Fibra y óptica integrada, 27(3), 221-233. https://doi.org/10.1080/01468030802192609

Rybin, D., Piliugina, K. y Piliugin, P. (2018). Investigación de la aplicabilidad del protocolo SSL/TLS para VPN en APCS. En Actas de la Conferencia IEEE 2018 de Jóvenes Investigadores Rusos en Ingeniería Eléctrica y Electrónica (EIConRus).

Sabrina, F., y Rogers, G. (2007). Control de flujo dinámico con reconocimiento de QoS en redes privadas virtuales. En 2007 IEEE International Conference on Communications (pp. 531–535). https://doi.org/10.1109/ICC.2007.53

Sadeghi, M. M. G., Ali, B. M., Pedram, H., Deghan, M., & Sabaei, M. (2009). Un nuevo método para crear políticas de seguridad eficientes en redes privadas virtuales. En Computación colaborativa: redes, aplicaciones y trabajo compartido.

Shah, H., ud Din, A., Abizar, ud Din, S. y Khan, A. (2020). Mejora de la calidad del servicio de la computación en la nube en big data mediante el uso de redes privadas virtuales y cortafuegos en modo denso. Revista internacional de informática avanzada y aplicaciones, 11(5).

Skendzic, A. y Kovacic, B. (2017). Sistema de código abierto OpenVPN en una función de red privada virtual. Innovative Ideas in Science 2016, 200(1), 012065. https://doi.org/10.1088/1757-899X/200/1/012065

Song, Y., Li, H., Cheng, L., Xiang, M. y Cai, J. (2016). Técnicas de optimización del registro de recursos SSL VPN basadas en el algoritmo de filtro Bloom. En 2016 IEEE Information Technology, Networking, Electronic and Automation Control Conference (ITNEC).

Stytz, M. R. y Banks, S. B. (2007). Habilitación de la seguridad multinivel de simulación distribuida mediante tecnología de máquinas virtuales y redes privadas virtuales. En Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security 2007. https://doi.org/10.1117/12.724256

Wi, H., Jang, C. K., Lee, J. H. y Yi, O. (2017). Sugerencia SSL-VPN para el sistema de control de señales de tráfico. Advanced Science Letters, 23(11), 10886-10889. https://doi.org/10.1166/asl.2017.10887

Wu, J. (2009). Implementación de una red privada virtual basada en el protocolo IPSec. En Conferencia Internacional ETP 2009 sobre el Futuro de la Informática y las Comunicaciones (FCC 2009). https://doi.org/10.1109/FCC.2009.16

Wu, K., Zhao, P., Cui, W., Zhang, X. y y Cui, A. (2019). Túnel SSL VPN basado en PF_RING. En Actas de la 10.ª Conferencia Internacional IEEE 2019 sobre Ingeniería de Software y Ciencia de Servicios (ICSESS 2019). https://doi.org/10.1109/ICSESS47205.2019.9040747

Xian, K. (2021). Un algoritmo de reconocimiento optimizado para el tráfico cifrado del protocolo SSL VPN. Informatica, 45(6), 925-936. https://doi.org/10.31449/inf.v45i6.3730

Yang, Y., Martel, C. U., Fu, Z. (J.) y Wu, S. F. (2006). Corrección y garantía de la política de seguridad IPsec/VPN. Journal of High Speed Networks, 15(1), 45–59.

Yu, D., Chen, N. y Tan, C. (2009). Diseño e implementación de un sistema de acceso de seguridad móvil (MSAS) basado en SSL VPN. En Actas del primer taller internacional sobre tecnología educativa y ciencias de la computación (Vol. 3). https://doi.org/10.1109/ETCS.2009.559

Zhou, L., Tan, F. y Gao, X. (2010). Investigación e implementación de redes LAN inalámbricas seguras basadas en EAP-TLS e IPSec VPN. En Coloquio Internacional sobre Informática, Comunicación, Control y Gestión (CCCM 2010) (Vol. 1, pp. 94-99). https://doi.org/10.1109/TAAI.2010.24

Zhu, Y., Wang, B. y Zhang, W. (2013). Sistema SSL VPN basado en NIC virtual simulada. En Cuarta Conferencia Internacional sobre Redes y Computación Distribuida (ICNDC) 2013. https://doi.org/10.1109/ICNDC.2013.42.