FACULTAD DE INGENIERÍA DE SISTEMAS, CÓMPUTO Y TELECOMUNICACIONES

Diseño de una red privada virtual (VPN) para el acceso remoto y seguro de los usuarios del área de finanzas al sistema contable CONCAR en ARIGROUP S.A.C.

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el título profesional de Ingeniero de Sistemas y Cómputo

AUTOR:

Sanchez Medina Raul Pierre
https://orcid.org/0009-0009-8060-5344

ASESOR :

Dr. Francisco Manuel Hilario Falcon
https://orcid.org/0000-0003-3153-9343

Lima - Perú - 2025

Visualizador de documentos

Turnitin Informe de Originalidad

Procesado el: 27-oct-2025 9:55 p.m. -05
Identificador: 2750758651
Número de palabras: 11813
Entregado: 6

Trabajo de suficiencia RECORTADO - Raul Pierr...
Por Raul Pierre Sanchez Medina

Índice de similitud	Similitud según fuente	
12%	Fuentes de Internet:	10%
	Publicaciones:	2%
	Trabajos del estudiante:	4%

excluir citas | Excluir bibliografía | excluir las coincidencias menores | modo: ver informe en vista quickview (vista clásica)
imprimir | descargar

Coincidencia del <1% (Internet desde 02-abr-2025)
https://www.coursehero.com/file/72438606/Taller-2-hector-huelgos-y-camila-machadodocx/

Coincidencia del <1% (Internet desde 20-mar-2024)
https://WWW.coursehero.com/sitemap/schools/3103-St.-John's-University/courses/242331-CHEMISC/

Coincidencia del <1% (Internet desde 03-mar-2025)
https://www.coursehero.com/es/file/220349030/Laboratorio-21210-Cifrar-y-descifrar-datos-con-OpenSSL-18032230pdf/

Coincidencia del <1% (Internet desde 11-dic-2024)
https://WWW.coursehero.com/file/239912027/SEINS-Act5-Montelongo-P-Francisco-Jdocx/

Coincidencia del <1% (Internet desde 26-nov-2024)
https://www.coursehero.com/es/file/p4t5e09/Consultar-la-agenda-de-actividades-La-suscripci%C3%B3n-a-su-bolet%C3%ADn-electr%C3%B3nico-El/

Coincidencia del <1% (Internet desde 27-feb-2022)
https://www.coursehero.com/file/104065870/fernandoramirez-redesyseguridadsemana7docx/

Coincidencia del <1% (Internet desde 25-mar-2025)
https://www.coursehero.com/file/69826337/EE-AA-4-2-LGGBdocx/

Coincidencia del <1% (Internet desde 03-dic-2024)
https://WWW.coursehero.com/file/95103807/AA4pdf/

Coincidencia del <1% (Internet desde 18-abr-2025)
https://www.coursehero.com/es/file/p665r6qq/Art%C3%ADculo-22-Decisiones-individuales-automatizadas-incluida-la-elaboraci%C3%B3n-de/

Coincidencia del <1% (Internet desde 17-feb-2025)
https://WWW.coursehero.com/file/202025198/3-Criptograf%C3%ADadocx/

Coincidencia del <1% (Internet desde 07-mar-2025)
https://www.coursehero.com/file/31082017/Disponibilidadpptx/

Coincidencia del <1% (Internet desde 16-feb-2025)
https://WWW.coursehero.com/file/238787397/Actividad-1-E3-U2203052S0168-2docx/

Coincidencia del <1% (Internet desde 18-mar-2025)
https://www.coursehero.com/es/file/246971293/M1-Tema-9-An%C3%A1lisis-y-Valoraci%C3%B3n-de-Riesgo-en-Ciberseguridad-1pdf/

Coincidencia del <1% (Internet desde 12-sept-2023)
https://www.coursehero.com/file/193197970/PLAN-DE-ACCI%C3%93Ndocx/

Coincidencia del <1% (Internet desde 17-ene-2025)
https://www.coursehero.com/file/241041891/AN%C3%81LISIS-DE-HABILIDADES-DIRECTIVAS-Recuperado-autom%C3%A1ticamentedocx/

Coincidencia del <1% (Internet desde 28-abr-2025)
https://axial-erp.co/mejores-practicas-de-seguridad-en-aplicaciones-para-sistemas-erp/

Coincidencia del <1% (Internet desde 16-abr-2025)
https://axial-erp.co/seguridad-erp-en-soluciones-basadas-en-la-nube-comprendiendo-modelos-de-responsabilidad-compartida/

Coincidencia del <1% (Internet desde 27-ene-2025)
https://axial-erp.co/seguridad-en-la-arquitectura-de-erp-mejores-practicas-y-consideraciones/

Coincidencia del <1% (Internet desde 31-mar-2025)
https://axial-erp.co/arquitectura-erp-y-cumplimiento-gestion-de-la-normativa-sobre-privacidad-y-seguridad-de-datos/

Coincidencia del <1% (Internet desde 13-ene-2025)
https://axial-erp.co/entendiendo-los-requisitos-de-cumplimiento-regulatorio-en-sistemas-erp/

Coincidencia del <1% (Internet desde 09-abr-2024)
http://repositorio.uigv.edu.pe

Coincidencia del <1% (Internet desde 22-jul-2024)
http://repositorio.uigv.edu.pe

Coincidencia del <1% (Internet desde 09-abr-2024)
http://repositorio.uigv.edu.pe

Coincidencia del <1% (Internet desde 17-oct-2023)

DEDICATORIA

A Dios, por ser la luz y guía en cada paso de mi vida, por concederme la sabiduría en los momentos difíciles y la fortaleza para alcanzar mis metas.

A mi abuela, Ana María Tapia, por su inmenso amor y por ser un ejemplo de perseverancia, recordándome que, a pesar de las dificultades, siempre hay que seguir adelante.

Mi hijo, Matías, ha sido desde su nacimiento mi mayor fuente de inspiración, despertando en mí un profundo deseo de superación. Aspiro a dejarle como legado el valor de la perseverancia, para que pueda alcanzar con firmeza cada meta que se proponga.

A todos ustedes, con sincero cariño y profunda gratitud, dedico este logro. Su apoyo y compañía dieron sentido y fuerza a cada paso de este camino.

AGRADECIMIENTO

Deseo expresar mi más sincera gratitud a todas las personas e instituciones que, de una u otra manera, hicieron posible la realización de esta investigación.

En primer lugar, al Dr. Francisco Manuel Hilario Falcón, por su guía constante, su paciencia y el compromiso a lo largo de todo el proceso. Sus recomendaciones y consejos fueron fundamentales para fortalecer este trabajo y alcanzar con éxito esta investigación.

Mi agradecimiento también a la empresa ARIGROUP S.A.C., por confiar en mi propuesta. Esa confianza no solo hizo viable esta investigación, sino que su respaldo fue esencial para alcanzar el objetivo del trabajo de investigación.

De igual manera, a mis compañeros y colegas de profesión, quienes, con sus aportes experiencia, han contribuido en enriquecer este esfuerzo académico. Su apoyo durante todo el proceso fue clave para afrontar los retos y culminar con éxito esta etapa.

A todos ellos, les extiendo mi reconocimiento y gratitud, pues este logro no hubiera sido posible sin su apoyo.

RESUMEN Y PALABRAS CLAVE

Esta investigación tiene como objetivo presentar el diseño de una red privada virtual (VPN) que permitió a los usuarios del área de finanzas de ARIGROUP S.A.C. acceder de manera remota y segura al sistema contable CONCAR. La iniciativa surgió ante las limitaciones existentes para conectarse desde ubicaciones externas y la necesidad de incorporar una alternativa tecnológica que asegure la continuidad operativa de la organización.

El análisis incluyó la revisión de distintas opciones de VPN, con especial atención en los protocolos de comunicación, los esquemas de autenticación y los algoritmos de cifrado que garantizan un equilibrio entre eficiencia y seguridad. También se consideraron los requerimientos técnicos y organizacionales de ARIGROUP S.A.C., con el propósito de que el diseño se adapte adecuadamente a su infraestructura tecnológica.

En resumen, el diseño de una red privada virtual (VPN) orientada al acceso remoto y seguro del sistema contable CONCAR representó una solución robusta, confiable y compatible con múltiples plataformas. Esta propuesta no solo permitió optimizar costos asociados al acceso y mantenimiento de la infraestructura, sino que también incorporó un nivel de seguridad a la conexión remota. Dado que el trabajo remoto se ha consolidado como práctica habitual en las organizaciones modernas, la implementación de la VPN fortaleció la continuidad operativa de ARIGROUP S.A.C. y optimizó la productividad de los usuarios, ofreciendo una conexión estable y protegida al sistema contable desde cualquier ubicación.

Palabras clave: red privada virtual (VPN), OpenVPN, acceso remoto, cifrado de datos, seguridad informática.

Design of a virtual private network (VPN) for secure remote access by finance department users to the CONCAR accounting system at ARIGROUP S.A.C.

ABSTRACT AND KEYWORDS

This research aims to present the design of a virtual private network (VPN) that enabled users in the finance department of ARIGROUP S.A.C. to remotely and securely access the CONCAR accounting system. The initiative arose from the existing limitations when connecting from external locations and the need to implement a technological alternative that ensures the organization's operational continuity.

The analysis included a review of different VPN options, with particular emphasis on communication protocols, authentication schemes, and encryption algorithms that ensure a balance between efficiency and security. The technical and organizational requirements of ARIGROUP S.A.C. were also considered to ensure that the design properly adapts to its technological infrastructure.

In summary, the design of a virtual private network (VPN) focused on secure remote access to the CONCAR accounting system represented a robust, reliable, and cross-platform compatible solution. This proposal not only optimized costs associated with access and infrastructure maintenance but also strengthened the security of remote connections. Given that remote work has become a common practice in modern organizations, the implementation of the VPN enhanced the operational continuity of ARIGROUP S.A.C. and improved user productivity by providing a stable and secure connection to the accounting system from any location.

Keywords: virtual private network (VPN), OpenVPN, remote access, data encryption, information security.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

En los últimos años, el crecimiento del teletrabajo y la digitalización de los procesos empresariales han exigido que las organizaciones adopten soluciones tecnológicas que garanticen la continuidad de sus operaciones sin comprometer la seguridad de la información. Esta tendencia se intensificó a raíz de la necesidad de acceso remoto a sistemas críticos, especialmente en áreas de finanzas, donde la confidencialidad, la integridad y la disponibilidad de los datos representan factores determinantes para la sostenibilidad de la empresa (Cybersecurity Insiders, 2025).

"El acceso remoto a los sistemas contables representa un desafío importante para las organizaciones. Una conexión no protegida puede exponer información financiera a riesgos como interceptaciones, suplantación de identidad o pérdida de datos sensibles, lo que podría generar consecuencias legales y económicas. Para enfrentar estas amenazas, muchas empresas recurren a las redes privadas virtuales (VPN), una tecnología que crea canales de comunicación cifrados entre los usuarios externos y la infraestructura corporativa. Esto minimiza la probabilidad de ataques y se garantiza tanto la confidencialidad de los datos como la autenticidad de las transacciones (Cargua-García, M. I., & Torres-Palacios, M. M., 2025). En este contexto, la selección del protocolo y del equipamiento adecuado se convierte en una decisión estratégica, puesto que influye directamente en el rendimiento de la VPN, la escalabilidad de la solución y la protección de los datos transmitidos.

Entre las principales soluciones para el acceso remoto seguro destacan los protocolos de red privada virtual (VPN), ampliamente adoptados en el ámbito empresarial por su flexibilidad, escalabilidad y compatibilidad multiplataforma. En el año 2025, las VPN se mantienen como un estándar de referencia frente a otros protocolos alternativos, principalmente gracias a su sólido nivel de cifrado, sus mecanismos avanzados de autenticación y el soporte continuo en múltiples entornos tecnológicos (Akinsanya, M. O., Ekechi, C. C., & Okeke, C. D. 2024). Asimismo, estas soluciones no solo responden a la creciente necesidad de accesos remotos confiables, sino que también se alinean con los principios del modelo zero-trust ("nunca confiar, siempre verificar"), considerado una de las tendencias más relevantes en seguridad corporativa para la protección de los activos digitales en un panorama de amenazas cada vez más sofisticado (Expert Insights, 2025).

Por otra parte, el hardware de red, en particular los routers especializados en la gestión de redes seguras y eficientes, constituye una alternativa tecnológica idónea para pequeñas y medianas empresas. Estos dispositivos destacan por su capacidad de configuración, su relación costo-eficiencia y su estabilidad en entornos corporativos. Asimismo, diversas soluciones han demostrado plena compatibilidad con tecnologías de VPN, lo que las convierte en un recurso estratégico para aquellas organizaciones que buscan equilibrar altos niveles de seguridad con una optimización de costos (Semiconductor Insight, 2025).

En efecto, evaluaciones recientes señalan que estos equipos ofrecen confiabilidad para la implementación de VPN en redes empresariales, ya que permiten centralizar la gestión de accesos y fortalecer la seguridad perimetral sin necesidad de recurrir a soluciones costosas o propietarias (Semiconductor Insight, 2025).

En el caso de ARIGROUP S.A.C., empresa que emplea el sistema contable CONCAR, se ha identificado una limitación en el acceso remoto que impacta directamente en la productividad de los colaboradores del área de finanzas. La necesidad de contar con una conexión segura y confiable se hace evidente cuando los usuarios trabajan en modalidad de teletrabajo fuera de las instalaciones físicas. En ausencia de una infraestructura de seguridad adecuada, los riesgos de accesos no autorizados aumentan significativamente, comprometiendo la protección de información sensible y reduciendo la eficiencia operativa (ITPro, 2025).

La solución propuesta en este trabajo de investigación consiste en el diseño de una red privada virtual (VPN) que permita a los usuarios del área de finanzas de ARIGROUP S.A.C. acceder de manera remota y segura al sistema contable CONCAR. El diseño contempla altos estándares de seguridad, estabilidad y rendimiento, asegurando la protección de la información financiera crítica. Asimismo, se plantea una infraestructura escalable y flexible que responda no solo a las necesidades actuales de acceso remoto, sino también a los desafíos futuros, en concordancia con las tendencias globales en ciberseguridad (Tech Driven Consulting. 2023).

La relevancia de esta investigación se encuentra en que no se limita a resolver una necesidad técnica, sino que también se constituye en un eje estratégico dentro de los procesos de transformación digital. Estudios recientes muestran que las compañías que implementan soluciones de VPN empresariales obtienen mejoras significativas en continuidad operativa, además de optimizar costos de infraestructura y fortalecer la protección de la información. (Sirte. 2024).

En síntesis, esta investigación tiene como objetivo analizar y presentar el diseño de una red privada virtual como solución de acceso remoto seguro al sistema contable CONCAR de ARIGROUP S.A.C. Con ello se busca demostrar que esta propuesta es capaz de garantizar la seguridad, escalabilidad y eficiencia requeridas en un entorno empresarial moderno, consolidando la protección de los activos digitales y la sostenibilidad de las operaciones.

CAPÍTULO 1: MARCO TEÓRICO DE LA INVESTIGACIÓN

1.1 Marco histórico

A lo largo del tiempo, el desarrollo de las tecnologías de conectividad en entornos empresariales se ha guiado por la necesidad de ofrecer accesos seguros y eficientes a sistemas esenciales, especialmente en los departamentos financieros, donde los datos son de carácter altamente sensible (Maurer & Nelson, 2021). En ARIGROUP S.A.C., el ingreso al sistema contable CONCAR se efectuaba exclusivamente desde la sede principal, lo cual limitaba la autonomía de los usuarios y afectaba la continuidad de las operaciones en situaciones que requerían labores a distancia. Esta limitación puso de manifiesto la necesidad de incorporar soluciones tecnológicas que permitieran superar las barreras de conectividad, asegurando al mismo tiempo la protección de los datos y la disponibilidad de la información financiera.

Las VPN se constituyen como una solución sólida de acceso remoto, ya que crean canales cifrados que enlazan al usuario con la red empresarial y resguardan los datos frente a intrusiones o amenazas externas. En sus primeras versiones, las VPN requerían infraestructuras sofisticadas y presupuestos elevados, lo que las hacía exclusivas de grandes corporaciones. Con el tiempo, su evolución permitió que organizaciones de diversos tamaños puedan accesos remotos seguros de manera más accesible, eficiente y rentable. (Fortinet, s. f. -a).

En ARIGROUP S.A.C. surgió la necesidad de habilitar un acceso remoto al sistema CONCAR, lo cual impulsó el planteamiento de una VPN que incorporara autenticación, cifrado y protocolos de comunicación orientados a la eficiencia y la continuidad operativa, evaluando mecanismos de autenticación, cifrado y protocolos de comunicación, con el objetivo de garantizar eficiencia, seguridad y continuidad operativa. Este proceso histórico refleja una tendencia global en la modernización de la infraestructura tecnológica corporativa de muchas empresas, donde la seguridad de la información y la flexibilidad del trabajo remoto se convierten en prioridades estratégicas (Fortinet, s. f. -a).

El diseño de acceso remoto implicó planificar y estructurar la infraestructura tecnológica necesaria, esta adaptación representó un avance significativo para la empresa. El diseño de la VPN permitió un acceso confiable y seguro, optimizó costos asociados al mantenimiento de infraestructura y fortaleció la continuidad operativa de la empresa. Este diseño contempló aspectos clave como la arquitectura de la red, la elección de protocolos, la asignación de recursos de hardware y software, y la definición de métodos de autenticación y cifrado para proteger la información sensible. Gracias a estas decisiones, se establecieron las bases para que los usuarios pudieran acceder y gestionar la información en el sistema contable CONCAR de manera segura y organizada, promoviendo la productividad y la capacidad de adaptación de la organización.

En resumen, el diseño implementado para el acceso remoto seguro en ARIGROUP S.A.C. facilitó la transición desde un modelo interno restringido hacia una infraestructura digital que posibilita la conexión externa controlada. Esta transformación consolidó la seguridad de la información y fortaleció la continuidad de las operaciones empresariales.

1.2 Bases teóricas

1.2.1 Red privada virtual (VPN)

Según **(AWS, s. f.).** una VPN permite a los usuarios acceder de manera segura a una red interna desde ubicaciones externas por internet. Gracias a mecanismos como cifrado, autenticación e integridad de la información, la comunicación entre ambos extremos se mantiene confiable y protegida.

Principios de funcionamiento

Los principios fundamentales que sustentan el funcionamiento de una VPN son los siguientes **(Cloudflare, s. f.)**:

1. **Cifrado de la información:** Los datos se codifican mediante algoritmos criptográficos, de manera que solo los destinatarios autorizados puedan acceder a ellos.
2. **Autenticación de usuarios y dispositivos:** Se verifica la identidad de quienes intentan conectarse a la red, asegurando que solo usuarios y equipos autorizados puedan establecer la conexión.
3. **Integridad de la información:** Se aplican mecanismos que garantizan que los datos no sean modificados durante su tránsito, preservando su exactitud y fiabilidad.

Estos principios permiten que la comunicación a través de redes externas se mantenga segura y confiable, protegiendo la información compartida entre usuarios y sistemas corporativos.

Beneficios de las VPN

Las VPN brindan beneficios importantes para las organizaciones que necesitan mantener la conectividad y proteger su información. Al permitir que los usuarios se conecten a la red corporativa desde cualquier lugar con Internet, facilitan el teletrabajo, la movilidad y la continuidad de las operaciones, combinando acceso remoto confiable con seguridad de la información **(Fortinet, s. f.-a; Palo Alto Networks, s. f.).**

Las VPN también funcionan como un canal seguro que protege frente a los riesgos de las redes públicas, reduciendo la exposición a interceptaciones o ataques de intermediarios. Su flexibilidad permite que empresas de distintos tamaños integren nuevas sedes, usuarios o dispositivos sin complicaciones, uniendo de manera natural los conceptos de escalabilidad y adaptabilidad **(Palo Alto Networks. s. f.-a; National Institute of Standards and Technology, 2022).**

Al centralizar y proteger el acceso a servidores, aplicaciones y bases de datos, las VPN ayudan a aprovechar mejor los recursos internos, evitando duplicaciones de información y asegurando una gestión segura de los activos digitales. Asimismo, facilitan el cumplimiento de normas en entornos regulados, garantizando confidencialidad, integridad y disponibilidad de la información **(Palo Alto Networks, s.f).**

1.2.2 Tipos de VPN

Según las necesidades de conectividad y seguridad de cada organización, las VPN se pueden agrupar en distintos tipos:

1.2.2.1 VPN de sitio a sitio

La VPN de sitio a sitio permite conectar de manera permanente dos o más redes corporativas, funcionando como si todas formaran una única red interna extendida. Este tipo de conexión resulta especialmente útil para empresas con varias sucursales o filiales, ya que garantiza una comunicación segura y constante entre oficinas, sin que cada usuario deba configurar individualmente su acceso como si trabajara en la misma red **(Palo Alto Networks, s. f.-a).**

En estas VPN, la comunicación se establece mediante un modelo peer-to-peer (P2P), donde cada extremo del túnel actúa como un nodo equivalente, conectándose directamente con la otra sede sin depender de un servidor central **(Fortinet, s. f.-b).**

Para implementar una VPN sitio a sitio, cada sede necesita un router con capacidad VPN, capaz de crear y mantener los túneles cifrados que aseguran la transmisión segura de la información entre oficinas **(Fortinet, s. f.-b).**

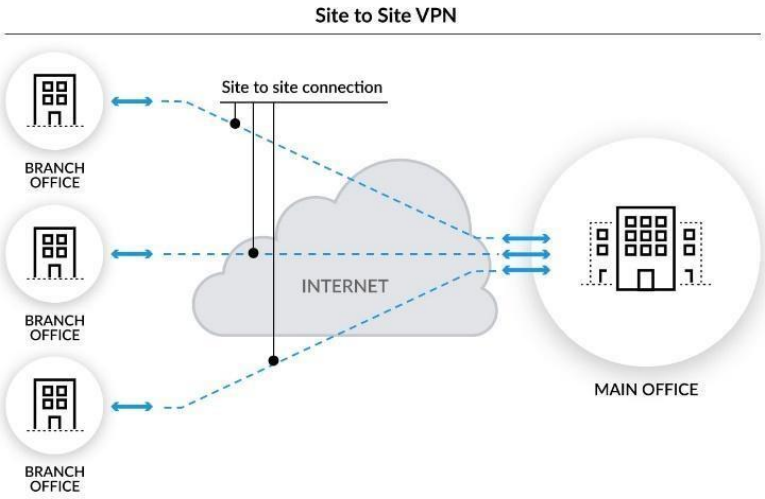

Figura 1. Esquema de VPN de sitio a sitio entre la oficina principal y las sucursales

Nota. Tomado de *Esquema de VPN de acceso remoto* [Figura], por Fortinet, s. f. https://www.fortinet.com/es/recursos/esquema-vpn

1.2.2.2 VPN de acceso remoto

La VPN de acceso remoto permite que un usuario se conecte de forma segura a la red corporativa desde cualquier ubicación externa, facilitando el teletrabajo y la movilidad de los empleados sin poner en riesgo la seguridad de la información **(Fortinet, s. f.-a).**

Para que esta conexión funcione correctamente, se utiliza un modelo cliente-servidor, donde:

- **Cliente VPN:** Es el dispositivo del usuario (computadora, laptop, tablet o smartphone) que inicia la conexión hacia la red corporativa. Todos los dispositivos deben ser compatibles con el protocolo VPN elegido **(Fortinet, s. f.-a).**
- **Servidor VPN:** Equipo de la empresa (router o servidor) que autentica al usuario, cifra los datos y proporciona acceso seguro a los recursos internos **(Fortinet, s. f.-a).**

Este modelo garantiza que la comunicación entre el cliente y la red corporativa se mantenga protegida, permitiendo que los empleados trabajen de manera remota sin comprometer la seguridad de los datos internos.

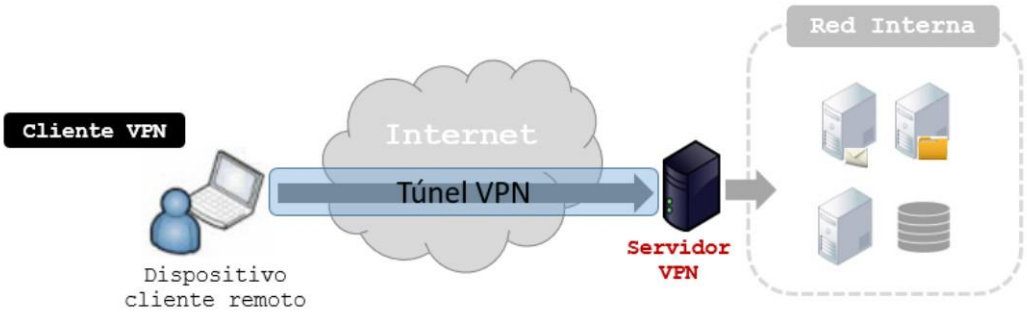

Figura 2. Esquema de arquitectura de VPN de acceso remoto para teletrabajo

Nota. Tomado de *Arquitecturas de Acceso Remoto Seguro* [Figura 3], por Centro Criptológico Nacional (CCN-CNI), 2020. https://www.ccn.cni.es/ca/docman/documentos-publicos/boletines-pytec/335-pildorapytec-31ago2020-arquitecturas-de-acceso-remoto-seguro/file

1.2.2.3 Comparativa de VPN de sitio a sitio y acceso remoto

Tabla 1. Principales diferencias entre VPN de acceso remoto y VPN de sitio a sitio

Aspecto	VPN de Acceso Remoto	VPN de Sitio a Sitio
Propósito	Permite que usuarios remotos se conecten de forma segura a la red interna de la organización.	Establece un enlace constante entre dos o más redes corporativas, integrándolas como una sola.
Ventajas principales	Facilita el teletrabajo	Comunicación continua entre oficinas
	No requiere gran inversión en equipos	
	Proporciona movilidad y flexibilidad	Mayor estabilidad en la conexión
Gestión administrativa	Se gestiona de forma individual para cada usuario o dispositivo; configuración relativamente sencilla.	Requiere ajustes más complejos en cada extremo de la red.
Escalabilidad y costos	Escalable en número de usuarios	Ampliar la solución implica inversión adicional en hardware o licencias, lo que eleva los costos
Seguridad y control	Robusta, depende de la configuración del cliente y políticas de seguridad.	Protegida por túneles cifrados entre redes; más centralizada en la infraestructura de cada sitio.
Infraestructura requerida	Solo requiere un software cliente en los dispositivos de acceso; demanda mínima de hardware.	Necesita equipos dedicados en cada sede (routers, firewalls o gateways de VPN).

Nota. Elaboración propia a partir de Fortinet (s. f.-a, s. f.-b), Palo Alto Networks (s. f., s. f.-a), AWS (s. f.), y Akinsanya et al. (2024)

1.2.3 Protocolos de comunicación VPN

Los protocolos de comunicación en una Red Privada Virtual (VPN) constituyen la base técnica que garantiza la seguridad y eficiencia de la conexión. Su función principal es establecer el túnel cifrado por el cual se transmiten los datos, además de definir los métodos de autenticación y los algoritmos de protección de la información. Entre las ventajas más destacadas se encuentran la capacidad de mantener la confidencialidad de los datos, la verificación de identidad entre los extremos de la conexión y la posibilidad de integrar diferentes tecnologías en entornos corporativos **(Alonso, J. A. (2009).**

1.2.3.1 Principales protocolos VPN y características técnicas generales

Los protocolos VPN han evolucionado con el tiempo, adaptándose a las nuevas demandas de seguridad y rendimiento, seguidamente se detallan los principales protocolos:

- **PPTP (Point-to-Point Tunneling Protocol):** Uno de los primeros en popularizarse, ofrece simplicidad en su implementación, aunque actualmente se considera inseguro debido a vulnerabilidades en su cifrado **(Snader, J. C. 2015).**
- **L2TP/IPSec (Layer 2 Tunneling Protocol):** Combinado con IPSec, proporciona mayor robustez y autenticación, siendo ampliamente usado en entornos corporativos. **(Snader, J. C. 2015).**
- **IKEv2/IPSec:** Reconocido por su estabilidad y velocidad, especialmente útil en dispositivos móviles, ya que soporta la reconexión automática tras interrupciones de red. **(Snader, J. C. 2015).**
- **OpenVPN:** Basado en SSL/TLS, es altamente configurable y cuenta con código abierto, lo que permite auditorías independientes de seguridad. **(Snader, J. C. 2015).**
- **WireGuard:** Un protocolo más reciente, diseñado para ser más rápido y eficiente que sus predecesores, con una base de código más ligera que facilita su auditoría **(Wu, P. 2019).**

Características técnicas generales:

Los protocolos de comunicación en las Redes Privadas Virtuales (VPN) presentan un conjunto de características técnicas que determinan su desempeño y nivel de seguridad. Cada protocolo establece las reglas de encapsulación, cifrado y autenticación que permiten el intercambio seguro de información a través de redes públicas como Internet (Fortinet, s. f.-a).

- **Cifrado:** AES-256 y ChaCha20 aseguran protección contra ataques criptográficos evitando descifrar datos cifrados, explotando debilidades en algoritmos **(Narayana, D. S. M., Enaganti, K. K., & Mathivanan, P, 2024,).**
- **Autenticación mutua:** Confirma la identidad de cliente y servidor, reduciendo riesgos de intermediarios utilizando para ello certificados digitales u otros mecanismos de validación **(Cloudflare, 2023).**
- **Eficiencia de recursos**: Los protocolos VPN pueden gestionar de manera óptima los recursos del sistema, ofreciendo un buen rendimiento con un bajo consumo de memoria y procesamiento, lo que resulta especialmente útil en dispositivos con hardware limitado o en redes de menor capacidad **(Tech Driven Consulting, 2023).**
- **Compatibilidad multiplataforma:** Un aspecto esencial de los protocolos VPN es su interoperabilidad. Los usuarios acceden a los sistemas corporativos desde diversos dispositivos —computadoras de escritorio, portátiles, tabletas y teléfonos inteligentes, lo que exige que los protocolos sean compatibles con múltiples sistemas operativos (Windows, Linux, macOS, iOS y Android). **(Fortinet, s. f.-a).**

1.2.3.2 Comparación de seguridad de protocolos VPN

La seguridad de un protocolo VPN depende de los algoritmos de cifrado, la solidez del proceso de autenticación y la resistencia frente a ataques conocidos. En la Tabla 2 se presenta una comparación entre los principales protocolos:

Tabla 2. Comparación de seguridad de los protocolos VPN

Protocolo VPN	Cifrado soportado	Autenticación	Nivel de seguridad	Observaciones
PPTP	MPPE (RC4 de 128 bits)	Usuario/contraseña (MS-CHAP v2)	Bajo	Obsoleto, vulnerable a ataques de diccionario y fuerza bruta.
L2TP/IPsec	3DES, AES-128/256	Certificados o claves precompartidas	Alto	Seguro si se configura con AES; requiere más recursos de CPU.
SSTP	SSL/TLS (AES-128/256)	Certificado digital	Alto	Difícil de bloquear, atraviesa firewalls fácilmente.
IKEv2/IPsec	AES-128/256	Certificados, EAP	Muy alto	Estable en movilidad (reconexión rápida). Recomendado.
OpenVPN	AES-128/256, ChaCha20	Certificados, usuario/contraseña, MFA	Muy alto	Código abierto, altamente configurable, considerado el más seguro.
WireGuard	ChaCha20	Claves públicas	Muy alto	Rendimiento superior, diseño moderno y simple; aún en evaluación en algunos entornos.

Nota. Elaboración propia a partir de Fortinet (s.f .-a, s. f.-b), Palo Alto Networks (s. f., s. f.-a), AWS (s. f.) y Akinsanya et al. (2024).

1.2.3.3 Rendimiento y escalabilidad de los protocolos VPN

El análisis del rendimiento y la escalabilidad en los protocolos de comunicación VPN resulta esencial para garantizar un servicio seguro y eficiente en entornos corporativos y personales. El rendimiento se refiere a la velocidad de transmisión de datos, la estabilidad de la conexión y el nivel de consumo de recursos del sistema, mientras que la escalabilidad implica la capacidad de soportar un número creciente de usuarios sin afectar la calidad del servicio **(Akinsanya, Ekechi, & Okeke, 2024; Tech Driven Consulting, 2023).**

El **Protocolo de túnel punto a punto (PPTP)** ofrece un rendimiento aceptable en términos de velocidad debido a su bajo nivel de cifrado, pero presenta limitaciones importantes en seguridad, lo que restringe su aplicación en redes modernas. Su escalabilidad es adecuada en entornos pequeños, aunque no se recomienda para organizaciones que requieren altos estándares de protección **(Snader, 2015; Alonso, 2009).**

El **Protocolo de túnel de capa 2 (L2TP)** combinado con IPsec mejora la seguridad, pero su doble encapsulamiento introduce una sobrecarga que puede reducir el rendimiento, especialmente en redes con gran volumen de tráfico. Aun así, su compatibilidad multiplataforma lo convierte en una opción escalable para empresas de tamaño medio **(Akinsanya, Ekechi, & Okeke, 2024).**

El **Internet Key Exchange versión 2 (IKEv2)** se distingue por su eficiencia en dispositivos móviles y su capacidad de reconexión rápida, lo que contribuye a un rendimiento estable en escenarios de movilidad. Su arquitectura permite manejar múltiples sesiones simultáneas, ofreciendo un buen balance entre rendimiento y escalabilidad **(Fortinet, s. f.-a; Tech Driven Consulting, 2023).**

OpenVPN se distingue por el uso de cifrado robusto puede demandar mayores recursos de hardware, lo que impacta en la velocidad de transmisión. Sin embargo, su flexibilidad, seguridad avanzada y compatibilidad con diferentes sistemas operativos le otorgan una alta escalabilidad en entornos corporativos complejos **(Snader, 2015; Alonso, 2009; Tech Driven Consulting, 2023).**

WireGuard emerge como un protocolo de nueva generación caracterizado por su diseño simplificado y eficiente. Su bajo consumo de recursos permite velocidades aceptables de información, con un nivel de seguridad moderno. Además, su estructura ligera facilita la integración en infraestructuras de gran escala, convirtiéndolo en una alternativa con alto potencial de adopción **futura (Donenfeld, J. A. 2017).**

1.2.4 Mecanismos de Seguridad en VPN

La seguridad constituye un factor esencial para la adopción de redes privadas virtuales en entornos corporativos y personales. Para garantizar comunicaciones confiables, las VPN implementan diversos mecanismos como protocolos de autenticación robustos y métodos de cifrado avanzados. Estos elementos trabajan en conjunto para prevenir accesos no autorizados, suplantaciones de identidad y la exposición de información sensible, protegiendo la transmisión de datos en entornos inseguros como Internet **(Palo Alto Networks, s.f.-b).**

1.2.4.1 Método de ciftrado

El cifrado es la técnica que transforma los datos originales en información ilegible para terceros no autorizados, asegurando que solo el receptor legítimo pueda interpretarlos mediante una clave correspondiente.

En las VPN, se emplean diversos tipos de cifrado para garantizar la confidencialidad y la integridad de la información, se detalla a continuación:

Cifrado simétrico: El cifrado simétrico emplea la misma clave para cifrar y descifrar la información, garantizando confidencialidad durante la transmisión de datos. Algoritmos como AES (Advanced Encryption Standard) se destacan por su rapidez y eficiencia en el manejo de grandes volúmenes de información, lo que los convierte en una opción ampliamente adoptada en entornos corporativos y sistemas críticos **(Mervana, H., 2024; González Martínez, P. 2023).**

El estándar AES se implementa en tres variantes principales: AES-128, AES-192 y AES-256, que difieren en la longitud de la clave y en el nivel de seguridad ofrecido. Mientras AES-128 proporciona un equilibrio entre velocidad y protección, AES-192 incrementa la complejidad criptográfica y fortalece la defensa frente a ataques, y AES-256 se considera el más

robusto y es el estándar actual, recomendado en entornos financieros y corporativos que requieren máxima protección de los datos

Tabla 3. Comparación entre variantes de AES (128, 192 y 256 bits)

Variante	Longitud de clave	Nivel de seguridad	Rendimiento	Estado actual (2025)	Observaciones
AES-128	128 bits	Alto	Muy rápido	Vigente	Balance entre velocidad y seguridad, recomendado en hardware limitado.
AES-192	192 bits	Muy alto	Intermedio	Vigente	Aumenta la complejidad criptográfica, aunque menos usado que AES-128 y AES-256.
AES-256	256 bits	Máximo	Más lento que AES-128	Estándar actual	Considerado el más robusto; ampliamente adoptado en banca, finanzas y VPN

Nota. Elaboración propia a partir de Takahashi & Fukunaga (2010); Paar & Pelzl (2010).

Cifrado asimétrico: El cifrado asimétrico, que se basa en pares de claves pública y privada, se utiliza principalmente para garantizar el intercambio seguro de claves iniciales en comunicaciones digitales. Este enfoque es la base de protocolos criptográficos ampliamente adoptados, como RSA y la criptografía de curva elíptica (ECC), los cuales permiten cifrar información de manera que solo el receptor autorizado pueda descifrarla **(Mervana, H., 2024).**

1.2.4.2 Funciones hash criptográficas

Las funciones criptográficas, como SHA-2 y SHA-3, son esenciales para garantizar la integridad de los datos durante su transmisión, ya que permiten verificar que la información no haya sido alterada. **(Sharma, S, & Khanum, S 2022).**

SHA-1, ya no es recomendable por su antigüedad, fue ampliamente utilizado en décadas anteriores, hoy es considerado obsoleto por su vulnerabilidad frente a ataques de colisión, por lo que ya no se recomienda en implementaciones modernas de seguridad

La combinación de estos métodos fortalece la seguridad del túnel VPN. De esta forma, se protege la información frente a intentos de interceptación o manipulación maliciosa.

Tabla 4. Comparación de algoritmos hash criptográficos SHA-1, SHA-2 y SHA-3

Algoritmo	Longitud de hash	Nivel de seguridad	Estado actual (2025)	Observaciones
SHA-1	160 bits	Bajo	Obsoleto / en desuso	Considerado inseguro desde 2017; aún presente en algunos equipos antiguos por compatibilidad, pero no recomendado
SHA-2	224, 256, 384 y 512 bits	Alto	Estándar vigente	Sigue siendo el más utilizado en entornos corporativos y en protocolos de VPN como OpenVPN e IPSec, reconocido por su estabilidad y confiabilidad
SHA-3	224, 256, 384 y 512 bits	Muy alto	En adopción creciente	Basado en Keccak, ofrece mayor resistencia frente a ataques futuros; usado en investigaciones y soluciones de seguridad avanzada, aunque su adopción masiva todavía es limitada.

Nota. Elaboración propia a partir de Olivier, G. F. (2013)

1.2.4.3 Métodos y protocolos de autenticación en VPN

Para que una VPN sea segura, es fundamental aplicar mecanismos de autenticación que garanticen que solo usuarios y dispositivos autorizados puedan establecer conexión. Estos mecanismos se dividen en **métodos de autenticación**, que validan directamente la identidad del usuario, y **protocolos de autenticación**, que definen cómo se transmiten y gestionan dichas credenciales en la red. **(Stallings, 2023; National Institute of Standards and Technology, 2017)**

Métodos de autenticación

- **Contraseñas tradicionales**. Son el método más simple y extendido. Sin embargo, su nivel de seguridad depende directamente de la complejidad de la clave y de las políticas de renovación. Contraseñas débiles o reutilizadas incrementan la vulnerabilidad frente a ataques de fuerza bruta o diccionario **(Stallings, 2023).**

- **Certificados digitales**. Basados en la infraestructura de clave pública, permiten validar la identidad de usuarios y servidores mediante terceros confiables. Este método aporta un alto nivel de seguridad y dificulta la suplantación de identidad, aunque requiere mayor gestión administrativa. **(Cloudflare, 2023)**

- **Autenticación multifactor.** Combina dos o más factores (ejemplo: contraseña + token físico o aplicación móvil + biometría). Su aplicación en entornos corporativos incrementa notablemente la seguridad, ya que dificulta el acceso no autorizado incluso en caso de robo de credenciales **(Microsoft, (2023).**

Protocolos de autenticación

- **Extensible Authentication Protocol (EAP):** Permite múltiples métodos de autenticación, incluyendo contraseñas, certificados digitales y credenciales biométricas. Su principal ventaja es la flexibilidad, ya que actúa como un marco que admite diferentes mecanismos según el nivel de seguridad requerido, lo que lo hace ampliamente utilizado en redes inalámbricas y corporativas modernas **(Stallings, W. 2023).**

- **PAP (Password Authentication Protocol):** Es un método básico que transmite contraseñas en texto plano, considerado obsoleto por su falta de seguridad. Aunque en su época resultó útil por su simplicidad de implementación, hoy solo se mantiene en algunos sistemas heredados o de compatibilidad mínima, ya que no ofrece cifrado ni protección frente a ataques de intercepción **(Kaufman, C., Perlman, R., & Speciner, M., 2022).**

- **CHAP (Challenge Handshake Authentication Protocol):** Utiliza un mecanismo de desafío y respuesta cifrada para validar credenciales, lo que lo hace más seguro que PAP. La mejora radica en que la contraseña no viaja en texto plano, reduciendo el riesgo de exposición. Sin embargo, se considera superado por protocolos más robustos, aunque todavía puede encontrarse en sistemas de acceso remoto que requieren un nivel básico de seguridad **(Kaufman, C., Perlman, R., & Speciner, M., 2022).**

- **MS-CHAPv2 (Microsoft CHAP versión 2):** Ampliamente usado en entornos corporativos con Microsoft, introdujo mejoras frente a CHAP al ofrecer autenticación mutua entre cliente y servidor y un esquema de cifrado más fuerte. Aunque se considera más seguro que sus predecesores, presenta vulnerabilidades conocidas en versiones antiguas, lo que ha impulsado la migración hacia métodos más modernos como EAP-TLS en escenarios críticos **(Kaufman, C., Perlman, R., & Speciner, M., 2022).**

- **EAP-TLS (EAP con certificados):** Es considerado uno de los métodos más seguros, ya que se basa en certificados digitales para garantizar la identidad tanto del cliente como del servidor. Entre sus mejoras se destaca la autenticación mutua, que elimina el riesgo de ataques de suplantación, y el uso de cifrado fuerte para proteger las credenciales. Se aplica ampliamente en redes corporativas, financieras y gubernamentales, donde se exige alta confiabilidad. **(Cloudflare, 2023; Stallings, W, (2023).**

1.2.5 Rendimiento y Optimización

El rendimiento de una Red Privada Virtual (VPN) es clave para que una organización mantenga sus operaciones sin interrupciones. Aunque las VPN brindan seguridad y acceso remoto confiable, un diseño inapropiado puede generar latencia, cuellos de botella o sobrecarga en los servidores. Por ello, optimizar su rendimiento requiere una visión integral que combine infraestructura tecnológica, gestión de recursos y buenas prácticas de implementación **(Tech Driven Consulting, 2023; Snader, 2015).**

1.2.5.1 Escalabilidad de VPN

La escalabilidad de una VPN indica su capacidad para aumentar el número de usuarios y dispositivos conectados sin afectar la calidad del servicio. En entornos corporativos donde el teletrabajo y la movilidad son comunes, las VPN deben soportar cientos o incluso miles de conexiones simultáneas **(Fortinet, s. f.; Palo Alto Networks, s. f.-a).**

1.2.5.2 Optimización de recursos y costos

Implementar una VPN requiere inversión en hardware, software, ancho de banda y procesamiento criptográfico constante. La optimización busca reducir el costo total de operación mediante la adecuada asignación de recursos y la distribución eficiente del tráfico de red, tomando en cuenta cuántos usuarios van a conectarse, el tipo de datos que se transmitirán en la VPN y en base a esto para determinar el hardware que se utilizarán como pueden ser servidores, routers o dispositivos de seguridad que soporten VPN, y la elección del software que permitirá crear los túneles seguros para proteger los datos de los usuarios **(AWS, s. f.; ITPro, 2025).**

1.2.5.3 Buenas prácticas de implementación

La optimización del rendimiento de una VPN no se trata solo de escoger el protocolo correcto o invertir en buen hardware; también requiere aplicar buenas prácticas en su diseño, configuración y operación. Con estas medidas se logra mantener un equilibrio entre seguridad, disponibilidad y rendimiento, haciendo que la VPN funcione de manera confiable en el día a día de la organización. A continuación, se presentan algunas de las prácticas más importantes:

- **Gestión de certificados y credenciales** Es fundamental establecer políticas claras para la emisión, revocación y renovación de certificados digitales. Asimismo, las credenciales deben gestionarse bajo esquemas de mínima exposición, con contraseñas complejas y cambios periódicos **(National Institute of Standards and Technology, 2024).**
- **Monitoreo proactivo**: Supervisar las conexiones en tiempo real ayuda a detectar cuellos de botella o fallos antes de que impacten a los usuarios. Herramientas de monitoreo de red y seguridad proporcionan mayor visibilidad y facilitan respuestas tempranas (**Palo Alto Networks, s. f.)**
- **Actualización periódica**: El software de VPN y los sistemas relacionados deben mantenerse siempre actualizados con los últimos parches de seguridad. Esto reduce la exposición a vulnerabilidades conocidas (**Palo Alto Networks, s. f.-b).**
- **Educación y concienciación del usuario**. Capacitar a los colaboradores sobre el uso seguro de la VPN, la importancia de conectarse únicamente desde dispositivos confiables y el respeto a las políticas corporativas es clave para reducir riesgos derivados de errores humanos **(BDO. s. f.).**

- **Integración con políticas de calidad de servicio (QoS)**: Priorizar el tráfico según la importancia de cada aplicación asegura que procesos críticos, como contabilidad o telefonía IP, mantengan desempeño estable incluso bajo alta demanda. **(Tech Driven Consulting, 2023).**

  Estas prácticas crean una base sólida para VPN confiables, asegurando continuidad operativa y una experiencia estable para los usuarios.

1.3 Marco legal

1.3.1 Normas de protección de datos.

Las organizaciones deben cumplir con regulaciones nacionales e internacionales que garantizan la privacidad de la información personal de los usuarios. Esto es especialmente relevante cuando se implementan soluciones de acceso remoto como VPN, que manejan datos sensibles de empleados y clientes.

1.3.1.1 Ley peruana de protección de datos personales (Ley N.° 29733 y su reglamento)

Según Ley N.° 29733, promulgada en julio de 2011 y reglamentada por el Decreto Supremo N.° 003-2013-JUS en 2013, establece las disposiciones para el tratamiento de datos personales en el Perú con el fin de proteger los derechos fundamentales de las personas y garantizar la privacidad de su información **(Congreso de la República del Perú, 2011).**

A continuación, de detallan los principios fundamentes, las obligaciones y sanciones:

Principios fundamentales establecidos por la Ley

- Principio de legalidad: el tratamiento de datos debe realizarse conforme a la ley.
- Principio de consentimiento: el titular debe otorgar su consentimiento previo, informado y libre para el tratamiento de sus datos.
- Principio de finalidad: los datos deben ser utilizados solo para fines específicos y legítimos.
- Principio de proporcionalidad: se deben recolectar únicamente los datos necesarios para el fin declarado.
- Principio de seguridad: se deben implementar medidas técnicas y organizativas para proteger los datos personales contra el acceso no autorizado, la pérdida o alteración.

Obligaciones relevantes

- La ley establece que el tratamiento de datos personales debe garantizar la confidencialidad, integridad y disponibilidad de la información.
- Se obliga a las organizaciones a implementar medidas técnicas y organizativas apropiadas para proteger los datos, sin detallar las medidas específicas.
- Los titulares de los datos tienen derechos reconocidos, conocidos como derechos ARCO: Acceso, Rectificación, Cancelación y Oposición.
- Es responsabilidad de las organizaciones facilitar el ejercicio de estos derechos.

Sanciones por incumplimiento

- Multas administrativas que varían entre 2 y 50 UIT (Unidad Impositiva Tributaria).
- Suspensión temporal o definitiva del tratamiento de datos personales.
- Otras sanciones previstas por la ley ante incumplimientos graves.

Si bien la Ley no menciona tecnologías específicas, como las VPN, los principios y obligaciones que establece Ley N.° 29733 y su reglamento son aplicables a cualquier sistema que procese datos personales, incluyendo aquellos con acceso remoto. De manera que, es imprescindible que las organizaciones que utilizan VPN para permitir el acceso remoto a datos deben asegurar el cumplimiento de estos principios y protejan adecuadamente la información.

1.3.1.2 Reglamentos internacionales y comparativos (GDPR, LGPD, CCPA)

En un entorno globalizado, las organizaciones que manejan datos personales no solo deben considerar la legislación nacional, sino también los marcos regulatorios internacionales. Normativas como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, la Ley General de Protección de Datos (LGPD) de Brasil y la California Consumer Privacy Act (CCPA) de Estados Unidos establecen estándares estrictos para el tratamiento y resguardo de información personal. Estas regulaciones buscan garantizar la privacidad y la transparencia en el uso de los datos, aspectos directamente relacionados con la implementación de tecnologías como las VPN.

GDPR (Unión Europea)

- **Derechos**: acceso, rectificación, portabilidad, olvido, oposición al tratamiento.
- **Obligaciones**: consentimiento explícito, notificación de brechas de seguridad en un plazo de 72 horas, nombramiento de una Delegado de Protección de Datos (DPO) en ciertos casos.
- **Sanciones**: hasta 20 millones de euros o el 4% de la facturación global anual, lo que resulte mayor **(Parlamento Europeo y Consejo de la Unión Europea, 2016).**

LGPD (Brasil)

- **Derechos**: confirmación de tratamiento, acceso, corrección, anonimización, portabilidad, eliminación.
- **Obligaciones**: transparencia en el uso de datos, medidas técnicas de seguridad, creación de un responsable de protección de datos (encargado).
- **Sanciones**: hasta 2% de la facturación de la empresa en Brasil, limitadas a 50 millones de reales por infracción **(Brasil, 2018).**

CCPA (California, EE. UU.)

- **Derechos**: conocimiento de qué datos se recolectan, eliminación de datos, derecho a optar por no vender información personal.
- **Obligaciones**: informar de manera clara a los consumidores, permitir mecanismos de "opt-out", proteger datos de menores de 16 años con consentimiento explícito.
- **Sanciones**: Multas de hasta USD 2,500 por infracción no intencional., hasta USD 7,500 **por infracción intencional**, Posibilidad de demandas colectivas en casos de filtraciones de datos **(State of California, 2018).**

Las regulaciones internacionales no solo marcan lineamientos jurídicos, sino que también establecen estándares de buenas prácticas que influyen en la gestión de la seguridad digital a nivel mundial. Para empresas que buscan expandirse o trabajar en entornos digitales globalizados, comprender y cumplir con estas normativas resulta esencial para garantizar la confianza de los usuarios, prevenir riesgos legales y mantener la continuidad del negocio

1.3.2 Normativas sobre seguridad de la información y ciberseguridad

La seguridad de la información y la ciberseguridad se han convertido en pilares fundamentales para las organizaciones modernas, especialmente en contextos donde el acceso remoto y las VPN son herramientas clave. Para garantizar la protección de datos, existen marcos normativos internacionales y nacionales que establecen lineamientos técnicos, organizativos y legales con el fin de mitigar riesgos, fortalecer la resiliencia digital y asegurar la continuidad de los negocios. **(National Institute of Standards and Technology, 2018; Center for Internet Security, 2021)**

1.3.2.1 Estándares internacionales (ISO/IEC 27001, NIST, CIS Controls)

Los estándares internacionales representan referentes de buenas prácticas que permiten a las organizaciones estructurar políticas y procedimientos de seguridad:

ISO/IEC 27001

- Norma internacional para la gestión de la seguridad de la información, enfocada en establecer, implementar y mejorar un Sistema de Gestión de Seguridad de la Información Requiere aplicar un enfoque basado en riesgos, incluyendo controles relacionados con acceso remoto, cifrado y gestión de incidentes.su certificación es reconocida globalmente y fortalece la confianza de clientes y socios **(International Organization for Standardization & International Electrotechnical Commission, 2022).**

NIST Cybersecurity Framework (NIST CSF)

- Desarrollado por el National Institute of Standards and Technology de EE. UU., ofrece un marco de cinco funciones clave: identificar, proteger, detectar, responder y recuperar.Es especialmente útil para la gestión de riesgos en entornos de VPN, dado que permite evaluar vulnerabilidades y definir planes de contingencia **(Center for Internet Security, 2021).**

CIS Controls, (Center for Internet Security)

- Conjunto de 18 controles priorizados que ayudan a reducir la superficie de ataque. Incluye buenas prácticas como gestión de dispositivos remotos, segmentación de red y monitoreo continuo. Es ampliamente usado como guía práctica para complementar marcos más amplios como ISO 27001 o NIST **(Center for Internet Security, 2021).**

En conjunto, estos estándares sirven como referencia obligatoria para organizaciones que buscan alinear sus operaciones con la seguridad internacionalmente reconocida, especialmente en el diseño y operación de VPN corporativas.

1.3.2.2 Normativas nacionales aplicables en ciberseguridad (ej. DS N.° 050-2018-PCM, que aprueba la Política Nacional de Ciberseguridad en Perú)

En el caso peruano, la ciberseguridad cuenta con un marco regulatorio que busca garantizar un entorno digital confiable y seguro:

- **Decreto Supremo N.° 050-2018-PCM**

  Aprueba la Política Nacional de Ciberseguridad y establece lineamientos para la protección de infraestructuras críticas, el fortalecimiento de capacidades técnicas, la gestión de riesgos cibernéticos y la cooperación entre el Estado, el sector privado y la sociedad civil. Exige la adopción de medidas preventivas como monitoreo de incidentes, protección de redes y mecanismos de respuesta coordinada ante ataques cibernéticos **(Presidencia del Consejo de Ministros, 2018).**

- **Ley N.° 30999 Ley de Ciberseguridad**

  Complementa el DS 050-2018-PCM al definir responsabilidades de las entidades públicas y privadas frente a incidentes de ciberseguridad. Establece la obligación de reportar incidentes al Centro Nacional de Seguridad Digital (CNSD). Define sanciones administrativas en caso de incumplimiento y enfatiza la corresponsabilidad de todos los actores del ecosistema digital **(Congreso de la República, 2019).**

Estas normativas no mencionan explícitamente a las VPN, pero al establecer la obligación de proteger infraestructuras críticas de información y redes de comunicaciones, se entiende que las soluciones de acceso remoto, como las VPN, también deben incluirse dentro de las políticas de ciberseguridad de las organizaciones.

1.3.3 Consideraciones éticas en accesos remotos

El acceso remoto a sistemas corporativos plantea no solo retos técnicos y legales, sino también dilemas éticos relacionados con la privacidad de los empleados, el uso responsable de la información y la confianza digital. Al implementar tecnologías como las VPN, las organizaciones deben garantizar que el control de la seguridad no vulnere los derechos individuales ni se convierta en un mecanismo de vigilancia desproporcionada. **(Floridi & Taddeo, 2016)**

1.3.3.1 Investigaciones Internacionales.

- En países de la Unión Europea, investigaciones vinculadas al Reglamento General de Protección de Datos (GDPR) resaltan la importancia de respetar la minimización de datos: recolectar solo la información estrictamente necesaria para la operación remota **(Parlamento Europeo y Consejo de la Unión Europea, 2016).**

- En Estados Unidos, investigaciones académicas han demostrado que existe un dilema entre la seguridad corporativa y la privacidad de los trabajadores, en especial cuando se utilizan registros de actividad o monitoreo en tiempo real **(Nurse et al., 2021).**

1.3.3.2 Investigaciones Nacionales

- En el contexto peruano, instituciones como la Autoridad Nacional de Protección de Datos Personales ha señalado la necesidad de que las empresas sean transparentes respecto al tratamiento de datos recolectados en accesos remotos **(Autoridad Nacional de Protección de Datos Personales, 2013).**

- También se ha observado que, en entornos corporativos, la falta de capacitación ética en ciberseguridad puede llevar a prácticas como el uso indebido de credenciales compartidas, debilitando tanto la seguridad como la cultura organizacional **(Congreso de la República del Perú, 2019).**

1.3.3.3 Brechas identificadas y oportunidad de investigación

- **Ausencia de marcos éticos claros:** Aunque existen normas legales y técnicas, pocas regulaciones abordan de manera directa los dilemas éticos que surgen en el acceso remoto.

- **Desigualdad en la protección de datos:** Las grandes corporaciones suelen contar con políticas robustas, mientras que muchas pequeñas y medianas empresas carecen de mecanismos adecuados, lo que genera una brecha ética y de seguridad.

- **Oportunidad de investigación:** Es necesario desarrollar modelos que combinen la seguridad técnica con principios éticos como la transparencia, la privacidad y el consentimiento informado, especialmente en entornos de VPN y acceso remoto dentro del ámbito empresarial peruano.

1.4 Marco conceptual

1.4.1 Definición de VPN

Una Red Privada Virtual (VPN, por sus siglas en inglés Virtual Private Network) es una tecnología que permite establecer una conexión segura y cifrada a través de redes públicas, como Internet. Su principal función es garantizar la confidencialidad, integridad y autenticidad de la información transmitida entre un usuario y una red corporativa o entre dos puntos geográficamente distantes. La VPN crea un "túnel virtual" que protege los datos de accesos no autorizados, reduciendo el riesgo de interceptación y robo de información sensible. **(AWS, s. f.).**

1.4.2 Beneficios estratégicos de la VPN

El uso de VPN ofrece beneficios que van más allá de la seguridad técnica:

- **Seguridad de la información:** Cifra la comunicación, protegiendo datos confidenciales frente a ciberataques (**National Institute of Standards and Technology 2024).**
- **Acceso remoto seguro:** Permite que empleados, clientes o proveedores accedan a recursos corporativos desde cualquier ubicación **(Microsoft, 2025).**
- **Optimización de costos:** Reduce la necesidad de infraestructuras físicas de comunicación, aprovechando Internet como canal seguro. **(BDO, 2025).**
- **Continuidad del negocio:** Mantiene la operación de la organización frente a contingencias, como desastres naturales o emergencias sanitarias. **(Palo Alto Networks, s. f.).**
- **Cumplimiento normativo:** Facilita la alineación con regulaciones nacionales e internacionales de protección de datos **(Cisco, 2025).**

Estos beneficios han convertido a las VPN en herramientas estratégicas, especialmente en entornos donde el trabajo remoto se ha consolidado como una práctica habitual.

1.4.3 Aplicaciones en el ámbito empresarial

Las VPN tienen múltiples usos en organizaciones de distintos sectores:

- **Teletrabajo:** Garantizan que los empleados accedan de forma segura a servidores, sistemas internos y aplicaciones empresariales **(Microsoft, 2025).**
- **Sucursales y filiales:** Conectan redes distribuidas geográficamente, asegurando el intercambio de información corporativa.
- **Entornos educativos:** Universidades y colegios emplean VPN para habilitar accesos remotos a bibliotecas digitales y sistemas académicos **(Fortinet, s. f.).**
- **E-commerce y banca digital:** Refuerzan la seguridad en operaciones críticas, como transacciones financieras o gestión de clientes. **(Palo Alto Networks, s. f.).**
- **Gobierno electrónico:** Permiten que instituciones estatales manejen datos sensibles con altos niveles de protección (**National Institute of Standards and Technology 2024).**

En resumen, las VPN son un componente clave dentro de la infraestructura tecnológica de cualquier organización moderna que busque productividad, seguridad y confiabilidad.

1.4.4 Conceptos Clave: Acceso remoto, cifrado, autenticación

- **Acceso remoto:** Proceso mediante el cual un usuario se conecta a los recursos de una red interna desde ubicaciones externas, garantizando disponibilidad y productividad sin necesidad de presencia física **(NIST, s. f.).**
- **Cifrado:** Técnica criptográfica que convierte la información en un formato ilegible para terceros no autorizados, asegurando que los datos transmitidos sean confidenciales e **íntegros (NSA, 2021).**
- **Autenticación:** Mecanismo de validación que asegura que la identidad del usuario es legítima. Puede realizarse mediante contraseñas, certificados digitales o autenticación multifactor (MFA) (**National Institute of Standards and Technology, 2022).**

Estos conceptos forman la base operativa de las VPN y se interrelacionan para establecer entornos digitales confiables y alineados con las mejores prácticas de seguridad informática.

CAPÍTULO 2: PLANTEAMIENTO DEL PROBLEMA

2.1 Descripción de la realidad problemática

En ARIGROUP S.A.C. en el área de finanzas depende de manera directa del sistema contable CONCAR, el sistema permite registrar transacciones, elaborar estados financieros y reportes.

Actualmente, ARIGROUP S.A.C. no cuenta con un servicio de conexión VPN que permita a sus colaboradores acceder al sistema contable de forma remota y segura. Esta limitación obliga a que todas las actividades relacionadas con el CONCAR deban ejecutarse exclusivamente dentro de la oficina.

Esta limitación genera una serie de problemas que afectan directamente al personal y a los procesos de la empresa:

- **Limitaciones en el acceso remoto**: los usuarios del área de finanzas no pueden conectarse al sistema contable de forma remota. Esto significa que se necesita validar una operación, revisar información o presentar un reporte en una situación de urgencia, debe esperar hasta encontrarse físicamente en la empresa.
- **Riesgos de seguridad en la información**: la ausencia de una conexión segura como una VPN puede llevar a que se utilicen programas o servicios inseguros que incrementan las vulnerabilidades del sistema, generando un mayor riesgo de accesos no autorizados y posibles filtraciones de datos.
- **Impacto en la productividad y flexibilidad**: depender exclusivamente del acceso presencial genera un retraso en las operaciones del área de finanzas. Además, impide que la empresa adopte modalidad de trabajo remoto, que hoy resultan necesarias en entornos empresariales cambiantes.

En síntesis, la falta de una conexión VPN segura en ARIGROUP S.A.C. no solo compromete la seguridad de la información financiera, sino que también limita la eficiencia del trabajo de los colaboradores y restringe la capacidad de la empresa de adaptarse a nuevas formas de gestión tecnológica.

2.2 Formulación del problema general y específicos

Problema general

¿Cómo garantizar una conexión estable y segura para los usuarios del área de finanzas de ARIGROUP S.A.C. mediante el diseño de una VPN que permita el acceso remoto al sistema contable CONCAR, asegurando la continuidad de las operaciones y la confiabilidad de la información?

Problemas específicos

- ¿Qué tipo de VPN resulta más adecuado para implementar en ARIGROUP S.A.C., considerando las necesidades de estabilidad, escalabilidad y facilidad de acceso remoto al sistema contable CONCAR?

- ¿Qué mecanismos y protocolos de seguridad deben incorporarse en el diseño de la VPN para proteger la confidencialidad, integridad y disponibilidad de la información financiera?

- ¿Qué métodos y herramientas de implementación permiten configurar de manera eficiente la VPN, garantizando un rendimiento óptimo para los usuarios del área de finanzas?

- ¿De qué forma el diseño de la VPN contribuye a mejorar la continuidad operativa y la confiabilidad del acceso remoto al sistema contable CONCAR en ARIGROUP S.A.C.?

2.3 Objetivo general y específicos

Objetivo general

Diseñar una red privada virtual (VPN) para garantizar una conexión estable y segura que permita a los usuarios del área de finanzas de ARIGROUP S.A.C. acceder de forma remota al sistema contable CONCAR, asegurando la continuidad de las operaciones y la confiabilidad de la información.

Objetivos específicos

1. Identificar las dificultades que se presentan hoy para acceder al sistema CONCAR de forma remota.
2. Determinar los requerimientos técnicos y los protocolos de seguridad necesarios para el diseño de la VPN.
3. Diseñar la topología de la red privada virtual (VPN), considerando criterios de seguridad, rendimiento y facilidad de acceso.
4. Evaluar el impacto del diseño de la VPN en la continuidad operativa y la confiabilidad del acceso remoto al sistema contable CONCAR.

CAPÍTULO 3: JUSTIFICACIÓN Y DELIMITACIÓN DE LA INVESTIGACIÓN

2.1 Justificación e importancia del diseño

El diseño de una red privada virtual (VPN) en ARIGROUP S.A.C. resulta fundamental debido a la creciente necesidad de garantizar la continuidad operativa del área de finanzas, la cual depende directamente del sistema contable CONCAR. Actualmente, el acceso remoto a este sistema se efectúa mediante aplicaciones de control remoto de terceros, tales como TeamViewer o AnyDesk, este proceso requiere el uso de equipos de cómputo que permanecen encendidos y conectados a la red interna para permitir la sesión remota y así acceder al sistema contable CONCAR. Sin embargo, este método no constituye un mecanismo seguro ni estandarizado, lo que expone a la organización a riesgos de seguridad informática, posibles pérdidas de información y limitaciones en la productividad del personal que requiere trabajar fuera de las instalaciones físicas.

La propuesta de diseño se justifica porque permitirá lo siguiente:

- Fortalecer la seguridad de la información financiera mediante el diseño de una VPN soportado en el protocolo **OpenVPN**, el cual permitirá establecer túneles de comunicación cifrados y autenticados. Como mecanismos de seguridad se empleará el **algoritmo de cifrado AES-256** para garantizar la confidencialidad de los datos transmitidos y el algoritmo de autenticación **SHA-2** para asegurar su integridad y verificación, considerados estándares robustos y confiables.
- **Optimizar la operatividad del área de finanzas**, ya que permitirá a los usuarios acceder de manera remota y confiable al sistema contable. Con ello se asegura la continuidad de los procesos en escenarios de teletrabajo, evitando retrasos en reportes y análisis financieros que son esenciales para la gestión de la empresa.
- **Contribuir a la modernización tecnológica de la empresa**, al implementar una solución de diseño escalable y flexible que se pueda adaptar a futuras necesidades de conectividad segura, alineándose con las tendencias de transformación digital en el sector empresarial.

La importancia de este diseño propuesto de una red privada virtual (VPN) para ARIGROUP S.A.C. se justifica plenamente porque responde a necesidades críticas de la organización. Por un lado, refuerza la seguridad de la información financiera mediante estándares de cifrado y autenticación reconocidos en la ciberseguridad, lo que garantiza la protección de datos sensibles. Asimismo, asegura la continuidad y eficiencia de los procesos contables al ofrecer un acceso remoto confiable en escenarios de teletrabajo, evitando interrupciones que afectan la gestión financiera. Finalmente, contribuye a la modernización tecnológica de la empresa, al implementar una solución escalable y flexible que prepara a la organización para afrontar futuras demandas de conectividad segura. De esta manera, la propuesta no solo atiende un requerimiento actual, sino que también potencia la competitividad y sostenibilidad de la empresa al facilitar un esquema de teletrabajo seguro y eficiente, capaz de garantizar la continuidad de los procesos financieros en un entorno digital cada vez más exigente.

En conclusión, el análisis técnico realizado en los capítulos anteriores demostró que, entre los principales protocolos evaluados, OpenVPN se posiciona como la opción más estable y segura, gracias a su robusto nivel de cifrado, alta estabilidad y compatibilidad con diferentes sistemas operativos. Estas características lo convierten en la opción más adecuada para entornos corporativos que requieren seguridad, flexibilidad y escalabilidad sostenida, situándolo como la base tecnológica ideal para el diseño de la VPN propuesta en ARIGROUP S.A.C.

2.2 Delimitación del diseño

La presente investigación se delimita en los siguientes aspectos:

Ámbito institucional:

El diseño de la VPN solo considera la sede principal de ARIGROUP S.A.C ubicada en Lima, donde se gestionan los procesos contables y financieros a través del sistema contable CONCAR.

Contenido técnico:

La investigación se centra en la elaboración de un diseño de red privada virtual (VPN) que asegure el acceso remoto al sistema contable CONCAR. Para ello, se consideran aspectos de seguridad, rendimiento, escalabilidad y facilidad de implementación, aplicando protocolos de cifrado y buenas prácticas de seguridad informática.

Temporalidad:

El estudio comprende el análisis, diseño y justificación de la propuesta tecnológica durante el periodo 2025, delimitándose exclusivamente a la fase de diseño de la VPN, con miras a su futura implementación.

Cobertura funcional:

El alcance del estudio está orientado a garantizar que los usuarios del área de finanzas accedan al sistema contable CONCAR de manera remota, segura y confiable. No se incluyen otros sistemas de la empresa ni áreas diferentes a finanzas.

CAPÍTULO 4: FORMULACIÓN DEL DISEÑO

3.1 Diseño esquemático

El diseño de la red privada virtual (VPN) propuesto se elaboró considerando las necesidades operativas identificadas de la situación actual de ARIGROUP S.A.C. Entre los requerimientos funcionales se considera una VPN de acceso remoto para al sistema contable CONCAR, adquisición de un RouterBOARD Mikrotik, que tendrá la función de gestionar el servicio de VPN, la disponibilidad de una dirección IP pública; la habilitación de los puertos de la base de datos SQL Server del sistema CONCAR; la definición del uso de un software cliente VPN en los equipos de los usuarios y la facilidad de uso para los usuarios del área de finanzas. Por otro lado, los requerimientos no funcionales comprenden la seguridad de la información mediante mecanismos y protocolos de cifrado robustos, el rendimiento de la conexión y la estabilidad de la infraestructura de red.

El diseño propuesto se integra con la infraestructura de red existente, que incluye el switch LAN y el servidor CONCAR, un Router Cisco de propiedad de Optical Network con Internet dedicado 1:1 simétrico. Esta integración permite aprovechar los recursos ya instalados.

A nivel de arquitectura, la solución se estructura en tres componentes principales: infraestructura de red, mecanismos de seguridad y acceso a recursos corporativos. La infraestructura de red contempla el equipamiento y la conectividad necesarios para establecer los canales de comunicación. Los mecanismos de seguridad se basan en el protocolo OpenVPN, que asegura la autenticación de usuarios y la protección de los datos mediante cifrado. Dentro de este esquema, el acceso a los recursos corporativos posibilita que los usuarios del área de finanzas trabajen de forma remota con el sistema CONCAR, asegurando la disponibilidad y continuidad operativa durante la jornada laboral.

3.2 Descripción de los aspectos básicos del diseño

Se adopta el diseño de aplicación porque permite trasladar los conceptos teóricos a una propuesta práctica, estructurando los elementos técnicos: infraestructura de red, protocolos de seguridad y mecanismos de acceso necesarios para garantizar un acceso remoto seguro al sistema contable CONCAR en ARIGROUP S.A.C.

Los aspectos básicos del diseño se describen en los siguientes puntos:

Infraestructura de red

La infraestructura contempla los elementos físicos y lógicos que soportarán la conexión remota:

- **RouterBOARD Mikrotik RB760iGS (nuevo):** Este equipo será el encargado de gestionar el servicio de VPN. Este modelo fue seleccionado por sus características técnicas: capacidad de manejar túneles de acceso remoto, soporte para el protocolo OpenVPN, cinco puertos Gigabit Ethernet, bajo consumo energético y una relación costo-beneficio adecuada para una empresa de tamaño mediano como ARIGROUP S.A.C. (**véase Anexo A para las especificaciones técnicas).**
- **Dirección IP pública (nuevo recurso contratado):** requisito fundamental que permite que el RouterBOARD Mikrotik sea accesible desde internet y, de esta forma, los usuarios remotos puedan establecer el túnel VPN hacia la red corporativa de ARIGROUP S.A.C. **(véase Anexo B para la documentación del servicio de IP pública contratada)**
- **Servidor CONCAR (existente):** Servidor ya implementado en Windows Server 2022 Standard, con base de datos SQL Server, que centraliza la gestión contable y constituye el principal recurso corporativo al que accederán los usuarios. . **(véase Anexo C para las características del Servidor CONCAR)**

- **Switch HP 1410- Port24 GE (existente):** Actualmente instalado, encargado de distribuir la conectividad en la red interna y garantiza la comunicación entre el RouterBOARD, el servidor CONCAR y otros dispositivos locales.
- **Estaciones de trabajo de usuarios (existente):** Equipos que actualmente utilizan los trabajadores y que se configurarán con el software cliente VPN para permitir el acceso remoto seguro al servidor CONCAR.
- **Enlace de internet (existente)**: conexión simétrica de fibra óptica **1:1** provista por el proveedor **Optical Network**, con 400 Mbps de subida y 400 Mbps de bajada, que garantiza ancho de banda estable y confiable para la operación de la VPN.

Tabla 5. Direccionamiento IP y Puertos habilitados

Componente	Dirección / Rango	Puerto	Descripción
IP pública contratada	170.81.99.125	-	Acceso desde internet al RouterBOARD
Router Cisco Optical Network	192.168.1.1/24	-	
RouterBOARD Mikrotik	IP WAN: 192.168.1.2/24 IP LAN: 192.168.20.1/24	1194	Puerto UDP/TCP para OpenVPN
Servidor CONCAR	192.168.20.10/24	1433	Puerto TCP para SQL Server (sólo accesible desde VPN)
Estaciones de trabajo	10.8.0.10/24 al 10.8.0.30/24	-	Rango IPs asignado a usuarios externos del área de finanzas

Nota. Elaboración propia.

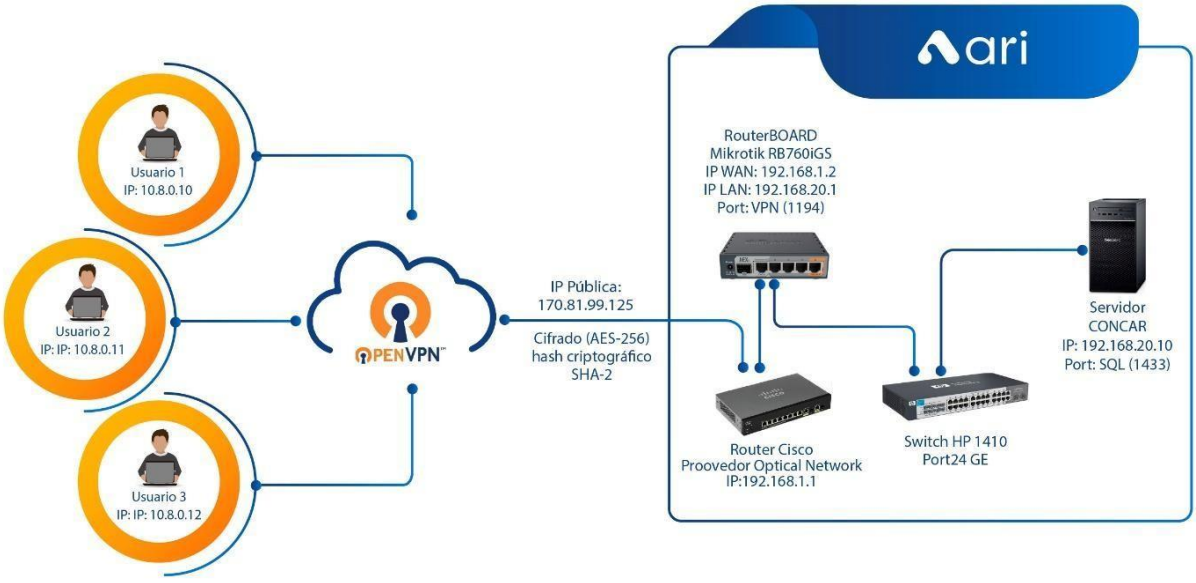

Figura 3. Esquema de la infraestructura de red propuesta.

Nota: Elaboración propia

b) Mecanismos de seguridad

Los mecanismos de seguridad se basan en protocolos y configuraciones que aseguran la integridad y confidencialidad de la información:

- **Protocolo OpenVPN**: seleccionado por su robustez y estabilidad, emplea cifrado de grado militar basado en TLS 1.3 y soporta algoritmos como AES-256 y SHA-2, brindando un canal seguro entre los usuarios remotos y la infraestructura interna. Su compatibilidad multiplataforma y código abierto facilitan la auditoría y verificación constante de su seguridad

- **Autenticación de usuarios:** cada empleado contará con credenciales individuales (usuario y contraseña) complementadas con un certificado digital personal, emitido por la organización para acceder al servicio VPN. Esta configuración asegura la validación de identidad y evita accesos no autorizados o suplantación de usuarios.

- **Cifrado de datos:** se aplicará el algoritmo **AES-256**, reconocido por su eficiencia y fortaleza criptográfica. Este estándar garantiza la confidencialidad de los datos transmitidos entre los usuarios remotos y el servidor contable **CONCAR**, protegiéndolos frente a posibles interceptaciones o ataques de fuerza bruta **(NIST, 2024).**

- **Integridad de la información:** se implementará el algoritmo **SHA-2**, que permite la validación mediante huellas digitales (hashes) únicas para cada paquete de datos. De esta manera, se asegura que la información no sea modificada ni corrompida durante la transmisión, preservando su integridad.

- **Restricción de puertos:** Dentro del diseño de la VPN se establecerá una política de firewall que limite el tráfico exclusivamente a los servicios necesarios. Se permitirá el puerto 1194/UDP para la comunicación del servicio OpenVPN y el puerto 1433/TCP para el acceso remoto al servidor SQL Server del sistema contable CONCAR. Esta restricción minimiza la superficie de exposición y contribuye a mantener la red interna protegida frente a accesos no autorizados.

c) Acceso a los recursos corporativos

El diseño propuesto garantiza que los usuarios remotos del área de finanzas puedan acceder de forma segura, estable al sistema contable **CONCAR**, asegurando la continuidad operativa de los procesos administrativos y financieros de la organización.

- **Conexión al sistema contable CONCAR:** acceso directo y seguro al software y a la base de datos SQL Server, necesarios para la gestión contable.
- **Usuarios del área de finanzas**: el diseño contempla el acceso remoto de tres colaboradores del área contable, quienes trabajarán bajo un esquema rotativo en el horario de 08:00 a 18:00 horas. Cada usuario dispondrá de credenciales individuales y un certificado digital corporativo, lo que asegura la autenticación confiable y el control de las sesiones activas dentro del entorno VPN.
- **Facilidad de uso:** el cliente de conexión OpenVPN estableciendo rápidas y sencillas, reduciendo la complejidad para el usuario final.
- **Disponibilidad del servicio:** la arquitectura diseñada asegura continuidad operativa durante la jornada laboral, incluso en escenarios de trabajo remoto.

d) Consideraciones de rendimiento

El diseño de la red privada virtual contempla aspectos orientados a garantizar la eficiencia**,** estabilidad **y** escalabilidad del servicio, asegurando un acceso remoto fluido al sistema contable CONCAR y a los recursos corporativos de ARIGROUP S.A.C.

Ancho de banda dedicado: Se dispondrá de un **enlace de Internet simétrico (fibra óptica 1:1)** que proporciona la misma velocidad tanto en subida como en bajada, lo que optimiza la transmisión de datos contables entre los usuarios remotos y el servidor interno. Esta característica es esencial para mantener la estabilidad de las conexiones VPN durante las operaciones simultáneas.

Conexiones simultáneas: el equipo RouterBOARD Mikrotik RB760iGS posee recursos de hardware suficientes (CPU de cuatro núcleos y memoria RAM optimizada) para manejar de manera eficiente hasta seis conexiones concurrentes mediante el protocolo OpenVPN, sin degradar el rendimiento general de la red ni afectar la latencia.

Escalabilidad: la arquitectura propuesta es modular y escalable, permitiendo incorporar nuevos usuarios o integrar otros sistemas corporativos en el futuro, sin requerir modificaciones estructurales significativas. Esto garantiza que la solución pueda adaptarse al crecimiento operativo o a la expansión tecnológica de la empresa.

Monitoreo de red: se implementarán las herramientas nativas de Mikrotik (Traffic Flow, Torch y Graphing) para el control en tiempo real del tráfico VPN, detección de anomalías y análisis de desempeño. Este monitoreo continuo permitirá tomar acciones preventivas ante posibles incidentes o congestiones, contribuyendo a mantener un servicio estable y confiable.

3.3 Flujo de conexión VPN

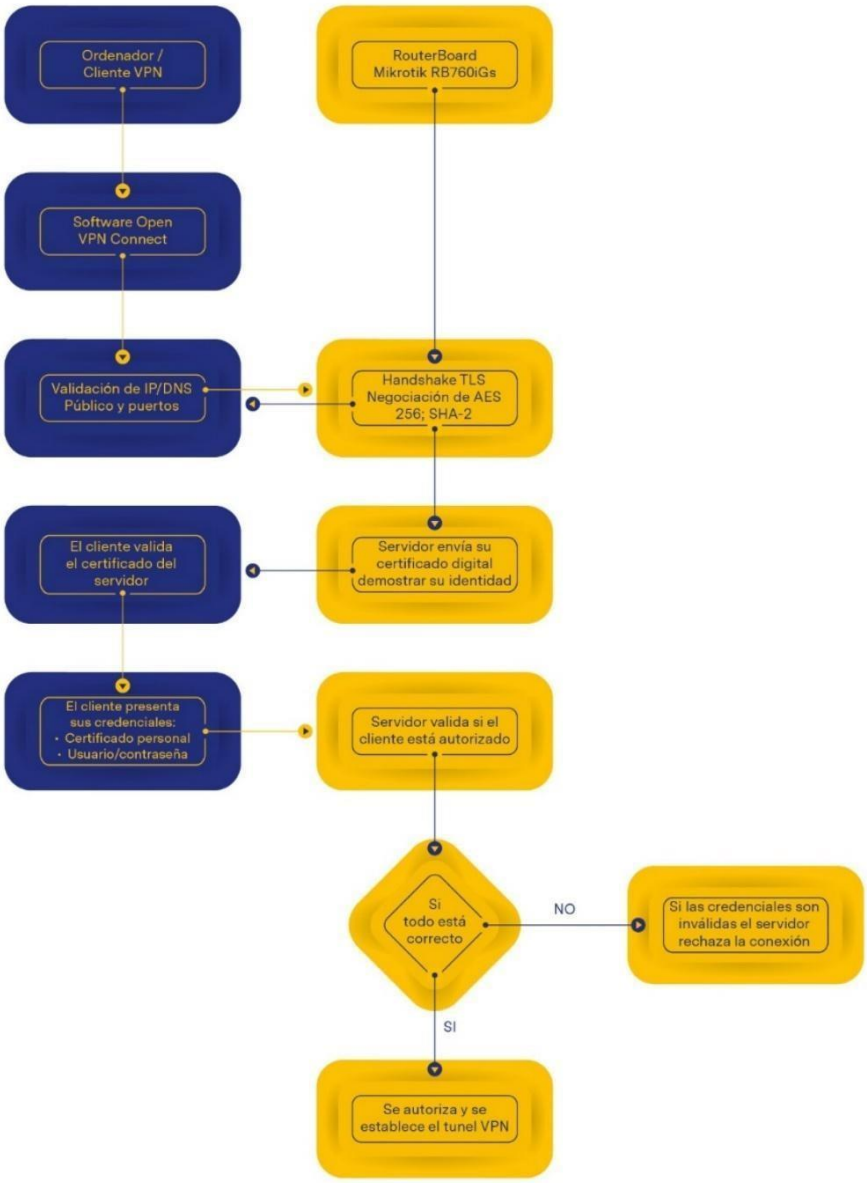

Figura 4. Flujo de conexión VPN.

Fuente: Elaboración propia

3.4 Buenas prácticas para la VPN

La correcta implementación y mantenimiento del servicio de red privada virtual requiere la adopción de buenas prácticas orientadas a fortalecer la seguridad, estabilidad y eficiencia operativa del sistema. Estas acciones complementan el diseño técnico y garantizan la confiabilidad del acceso remoto al sistema contable CONCAR y a los recursos internos de ARIGROUP S.A.C.

Segmentación de red: se recomienda aislar el tráfico proveniente de la VPN respecto al resto de la red corporativa mediante segmentación de red o reglas de enrutamiento específicas. Esta separación lógica reduce el riesgo de propagación de amenazas y facilita la gestión del tráfico entre los distintos segmentos.

Firewall restrictivo: el RouterBOARD Mikrotik RB760iGS debe configurarse con políticas de filtrado que limiten el acceso únicamente a los servicios indispensables, como el puerto 1194/UDP para el túnel OpenVPN y el puerto 1433/TCP para la base de datos SQL Server del sistema CONCAR. De esta forma se minimiza la superficie de exposición ante intentos de intrusión externa.

Actualización de firmware: mantener el firmware del RouterBOARD y los clientes VPN actualizado es fundamental para corregir vulnerabilidades conocidas y optimizar el rendimiento del servicio. Las actualizaciones deben realizarse siguiendo las recomendaciones oficiales del fabricante y previo respaldo de la configuración actual.

Registro y monitoreo de accesos: se debe habilitar el registro detallado (**logs**) de las conexiones VPN, incluyendo fecha, hora y dirección IP de origen. Este control permite auditar el uso del servicio, detectar patrones anómalos y responder de manera oportuna ante intentos de acceso no autorizado.

Las credenciales de acceso deben cumplir con estándares de complejidad (mínimo de 12 caracteres, combinación de letras, números y símbolos) y renovarse de forma periódica. Esta práctica reduce la probabilidad de ataques de fuerza bruta o robo de credenciales.

CAPÍTULO 5: PRUEBA DE DISEÑO

4.1 Aplicación de la propuesta de solución

El presente capítulo describe el procedimiento de aplicación y validación del diseño de red privada virtual (VPN) propuesto para la empresa **ARIGROUP S.A.C.**, con el objetivo de permitir el acceso remoto seguro al sistema contable **CONCAR** mediante un túnel cifrado **OpenVPN**, implementado sobre el router **MikroTik RB750r2**.

El diseño propuesto se centra en garantizar la seguridad, integridad y disponibilidad de la información financiera, permitiendo el acceso remoto controlado para los usuarios del área de Finanzas asegurando un acceso controlado desde ubicaciones externas mediante autenticación y cifrado de extremo a extremo.

4.1.1 Entorno y equipamiento de prueba

El entorno de validación se basó en la infraestructura real de **ARIGROUP S.A.C.**, en la cual el proveedor **Optical Network** suministra la conexión principal a Internet mediante un **router Cisco** con dirección **192.168.1.1/24**.

El router **MikroTik RB750r2** actúa como servidor VPN, con interfaz **WAN (ether1)** en la dirección **192.168.1.2/24** y **LAN (ether2)** en **192.168.20.1/24**, gestionando la comunicación interna con el servidor contable **CONCAR (192.168.20.10)**.

Para habilitar el acceso remoto desde Internet, se solicitó al proveedor Optical Network la creación de una regla NAT 1:1, que redirige el tráfico proveniente de la IP pública 170.81.99.125 hacia la IP privada del MikroTik (192.168.1.2) en el puerto 1194/TCP, correspondiente al servicio OpenVPN.

El área de Finanzas cuenta con tres usuarios autorizados (finanzas01 a finanzas05) que disponen de credenciales únicas y certificados digitales. Con el rango de IPs 10.8.0.10 – 10.8.0.30/24.

Cada usuario representa un equipo remoto que se conecta a la red VPN y accede al sistema CONCAR a través del túnel cifrado.

Esta configuración permite que los clientes externos se conecten mediante un túnel seguro y autenticado hacia la red interna de la empresa.

4.1.2 Configuración técnica aplicada

La configuración técnica para el diseño servidor VPN en el router MikroTik se desarrolló siguiendo un conjunto ordenado de fases que garantizan la seguridad y correcta comunicación entre las redes internas y remotas.

Para la implementación del diseño de la VPN, se emplearon comandos basados en la documentación oficial del fabricante **MikroTik (MikroTik, 2025).** Los detalles completos de la configuración se encuentran en el Anexo X. Estos comandos fueron adaptados y ejecutados según las necesidades del entorno de ARIGROUP S.A.C.

A continuación, se describen las principales fases de configuración y los parámetros establecidos para la propuesta de diseño de VPN.

a) Asignación de direcciones IP y ruta por defecto

Se configuraron las interfaces de red y la puerta de enlace (gateway) hacia el router Optical Network, permitiendo la salida a Internet y la gestión del tráfico entrante de la VPN. Los comandos empleados se presentan en el **Anexo 1**.

b) Configuración DNS

Se establecieron servidores DNS públicos (8.8.8.8 y 1.1.1.1) para resolver nombres de dominio desde el entorno VPN.

c) Creación del pool de direcciones VPN

Se definió el rango de direcciones virtuales 10.8.0.10 – 10.8.0.30, que serán asignadas a los clientes remotos autenticados (**Anexo 1**).

d) Generación de certificados digitales

Se implementó un esquema de autenticación mixta mediante usuario y certificado digital, generando una Autoridad Certificadora (CA), un certificado para el servidor VPN y un certificado para el cliente finanzas01**.** Los comandos se detallan en el **Anexo 2.**

e) Activación del servidor OpenVPN

El servicio OpenVPN fue habilitado en el puerto 1194/TCP, con cifrado AES-256 y autenticación SHA-2, asegurando la comunicación cifrada entre los equipos remotos y el servidor interno, según el **Anexo 2**

f) Configuración de firewall y NAT

Se aplicaron reglas de seguridad que permiten exclusivamente el tráfico necesario para el funcionamiento del servicio VPN y el acceso controlado a los recursos internos de la empresa:

- **Entrada al puerto 1194/TCP (OpenVPN):** habilita las conexiones de los usuarios remotos autenticados.
- **Acceso VPN → CONCAR (192.168.20.10:1433):** autoriza únicamente la comunicación de los clientes VPN (rango 10.8.0.0/24) hacia el servidor contable mediante el puerto 1433/TCP del servicio SQL Server.
- **Comunicación VPN ↔ LAN:** permite el intercambio de información entre los usuarios remotos y los equipos internos de la red.
- **Bloqueo de accesos no autorizados desde la WAN:** protege la red interna frente a intentos de conexión externos no autenticados.

  Asimismo, se configuraron reglas de **NAT (masquerade)** para permitir el acceso a Internet tanto desde la red LAN interna como desde los usuarios conectados mediante VPN.

  El proveedor **Optical Network** complementa esta configuración mediante una redirección **NAT 1:1**, que direcciona el tráfico público 170.81.99.125**:1194** hacia el router MikroTik (**192.168.1.2:1194**), garantizando la disponibilidad del servicio OpenVPN desde Internet.

El detalle completo de las reglas de firewall, las políticas NAT locales y la redirección gestionada por el proveedor se presenta en el **Anexo 3**.

g) Archivo de configuración del cliente VPN

Para los usuarios remotos del área de Finanzas se elaboró un archivo de configuración compatible con OpenVPN Connect, el cual contiene los certificados digitales y parámetros de conexión hacia el servidor con IP pública 170.81.99.125, puerto 1194/TCP.

El archivo define el tipo de cifrado (AES-256), la autenticación (SHA-2) y las rutas de los certificados exportados.

Cada usuario dispone de una versión personalizada del archivo, adaptada a sus credenciales de acceso. El contenido completo del archivo y sus certificados asociados se detallan en el **Anexo 4.**

4.1.3 Resultados esperados

De acuerdo con la configuración aplicada, los resultados esperados son los siguientes:

- Conectividad VPN estable: los clientes remotos se conectan y reciben una dirección IP del rango 10.8.0.10–10.8.0.30.
- Acceso seguro al sistema contable: los usuarios autenticados acceden a CONCAR (192.168.20.10) mediante el puerto 1433/TCP.
- La conexión se establece cifrada con AES-256, autenticación SHA-2, y certificados digitales únicos.
- Control de acceso: el firewall permite únicamente el tráfico autorizado VPN ↔ LAN, reforzando la seguridad de la red.

El diseño VPN propuesto garantiza un acceso remoto seguro y confiable al sistema contable corporativo, preservando la confidencialidad y la integridad de los datos transmitidos.
El uso de certificados digitales, cifrado robusto y la segregación de redes (WAN, LAN y VPN) optimiza la seguridad lógica de la infraestructura.

La configuración NAT 1:1 realizada por el proveedor Optical Network constituye un elemento crítico para la exposición controlada del servicio OpenVPN, asegurando que el túnel sea accesible únicamente mediante la IP pública asignada (170.81.99.) y el puerto específico (1194/TCP).

El resultado final valida la viabilidad del diseño planteado en el Capítulo IV y establece las bases para una futura implementación operativa en la infraestructura real de la organización.

CONCLUSIONES

1. La implementación del diseño de red privada virtual (VPN) permitió garantizar un acceso remoto seguro y confiable al sistema contable CONCAR, resolviendo las limitaciones de conectividad iniciales en el área de finanzas.
2. El uso del protocolo OpenVPN con cifrado AES-256 y autenticación SHA-2 fortaleció la protección de los datos financieros transmitidos, asegurando la integridad y confidencialidad de la información.
3. El diseño propuesto demostró ser escalable y compatible con la infraestructura existente, garantizando la continuidad operativa y la eficiencia del trabajo remoto.

RECOMENDACIONES

1. Implementar de forma progresiva la VPN, comenzando con el área de finanzas y extendiéndola a otras áreas críticas.
2. Establecer políticas de mantenimiento y actualización del servidor VPN, certificados y protocolos de seguridad.
3. Capacitar al personal sobre el uso correcto de la VPN y las buenas prácticas de seguridad informática.
4. Evaluar la integración futura con soluciones en la nube para mejorar la resiliencia y disponibilidad del servicio.

REFERENCIAS BIBLIOGRÁFICAS

Cybersecurity Insiders. (2025). VPN Exposure Report 2025: Why organizations are adopting a modern secure access strategy. Cybersecurity Insiders. https://www.cybersecurity-insiders.com/vpn-exposure-report-2025-why-organizations-are-adopting-a-modern-secure-access-strategy/

Cargua-García, M. I., & Torres-Palacios, M. M. (2025). Seguridad y regulaciones de privacidad en la contabilidad digital para proteger datos financieros sensibles. Revista Metropolitana de Ciencias Aplicadas, 8(2), 74-84. https://remca.umet.edu.ec/index.php/REMCA/article/view/874/844

Akinsanya, M. O., Ekechi, C. C., & Okeke, C. D. (2024). Virtual private networks (vpn): a conceptual review of security protocols and their application in modern networks. Engineering Science & Technology Journal, 5(4), 1452-1472. https://doi.org/10.51594/estj.v5i4.1076

Expert Insights. (2025). Zero Trust adoption statistics and trends in 2025. https://expertinsights.com/zero-trust/zero-trust-adoption-statistics-and-trends

Semiconductor Insight. (2025). Secure VPN routers market 2025. https://semiconductorinsight.com/report/secure-vpn-routers-market/

Real Systems. (2025). Condiciones y requisitos técnicos https://realsystems.com.pe/condiciones-y-requisitos-tecnicos

ITPro. (2025). Is remote work really insecure?. https://www.itpro.com/security/is-remote-work-really-insecure

Tech Driven Consulting. (2023). Enhancing VPN performance to enable remote work: A comprehensive guide. https://techdrivenconsulting.com/enhancing-vpn-performance-to-enable-remote-work-a-comprehensive-guide/

Sirte. (2024). La importancia de las redes privadas virtuales (VPN) en las empresas. https://sirte.com/la-importancia-de-las-redes-privadas-virtuales-vpn-en-las-empresas/

Maurer, T., & Nelson, A. (2021). La ciberamenaza mundial. Finanzas y Desarrollo. Fondo Monetario Internacional. https://www.imf.org/external/pubs/ft/fandd/spa/2021/03/pdf/global-cyber-threat-to-financial-systems-maurer.pdf

Fortinet. (s.f.-a). ¿Qué es una VPN de acceso remoto? Fortinet. https://www.fortinet.com/lat/resources/cyberglossary/remote-access-vpn

AWS. (s. f.). ¿Qué es una VPN? Recuperado. https://aws.amazon.com/es/what-is/vpn/

Palo Alto Networks. (s. f.). ¿Qué es una VPN de sitio a sitio? Palo Alto Networks. https://www.paloaltonetworks.es/cyberpedia/what-is-a-site-to-site-vpn

Fortinet. (s.f.-b). ¿Qué es la VPN entre pares (P2P)? https://www.fortinet.com/lat/resources/cyberglossary/peer-to-peer-p2p vpnFortinet+2Fortinet+2

Palo Alto Networks. (s.f.-a). What Is a VPN? A Complete Guide to Virtual Private Networks. https://www.paloaltonetworks.com/cyberpedia/what-is-a-vpn

National Institute of Standards and Technology. (2022). Holiday travel tip: Use public Wi-Fi safely. https://www.nccoe.nist.gov/sites/default/files/2022-11/HolidayTravelTip-UsePublicWiFiSafely.pdf

Snader, J. C. (2015). VPNs Illustrated: Tunnels, VPNs, and IPsec. Addison-Wesley Professional.

Wu, P. (2019). Analysis of the WireGuard protocol. Master's Thesis, Analysis of the WireGuard protocol, Eindhoven University of Technology. https://www.lekensteyn.nl/files/pwu-wireguard-thesis-final.pdf

Alonso, J. A. (2009). Redes privadas virtuales. Alfaomega Grupo Editor.

Narayana, D. S. M., Enaganti, K. K., & Mathivanan, P. (2024, June). Enhancing image security using novel scrambling and chaotic techniques with chacha20 algorithm. In 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT) (pp. 1-6). IEEE.

Donenfeld, J. A. (2017). WireGuard: Next generation kernel network tunnel. Network and Distributed System Security Symposium (NDSS). https://www.wireguard.com/papers/wireguard.pdf

Palo Alto Networks. (s.f.-b). VPN Security: Are VPNs Safe and Secure? Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/vpn-security

Mervana, H. (2024). Encryption standards: AES, RSA, ECC, SHA, and other protocols. Dev.to. https://dev.to/hardy_mervana/encryption-standards-aes-rsa-ecc-sha-and-other-protocols-460c

Sharma, S., & Khanum, S. (2022). Performance analysis of SHA 2 and SHA 3. In Proceedings of the International Conference on Innovative Computing & Communication (ICICC).

González Martínez, P. (2023). Seguridad del dato en sistemas de Big Data. https://openaccess.uoc.edu/server/api/core/bitstreams/5c710f3d-7f2d-4f46-9dc3-802aac445c63/content

Microsoft. (2025). Extensible Authentication Protocol (EAP) for network access. https://www.microsoft.com

Cisco. (2025). Compare TACACS+ and RADIUS. https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html Cisco

BDO. (2025). Preparing for coming changes to digital certificates. https://www.bdo.com/insights/assurance/preparing-for-coming-changes-to-digital-certificates BDO

Mavroudis, V. (2024). Zero-Trust Network Access (ZTNA). arXiv preprint arXiv:2410.20611. https://arxiv.org/abs/2410.20611

Triana Gómez, J. A. (2025). Análisis de los métodos de autenticación multifactor (MFA) y su eficiencia en la protección de accesos, aplicados a la carrera de ingeniería en sistemas de información (Bachelor's thesis, Babahoyo: UTB-FAFI. 2025). https://dspace.utb.edu.ec/handle/49000/17945

Giner Bornay, Á. (2024). Buenas prácticas en la administración de sistemas informáticos (Doctoral dissertation, Universitat Politècnica de València). https://riunet.upv.es/handle/10251/210581

Congreso de la República del Perú. (2011). Ley N.° 29733: Ley de protección de datos personales. Diario Oficial El Peruano. https://www.gob.pe/institucion/pcm/normas-legales/343678-ley-n-29733

Takahashi, J., & Fukunaga, T. (2010). Differential fault analysis on AES with 192 and 256-bit keys. Cryptology ePrint Archive. https://eprint.iacr.org/2010/023.pdf

Paar, C., & Pelzl, J. (2010). Understanding cryptography: A textbook for students and practitioners. Springer-Verlag. https://doi.org/10.1007/978-3-642-04101-3

Olivier, G. F. (2013). Estudo e implementação do algoritmo de resumo criptográfico SHA-3 (Doctoral dissertation, Universidade de Brasília). https://core.ac.uk/download/pdf/196875655.pdf

Cloudflare (s.f.-b). ¿Qué es la autenticación mutua? Cloudflare.

https://www.cloudflare.com/es-es/learning/access-management/what-is-mutual-authentication/

Stallings, W. (2023). Cryptography and network security: Principles and practice (8th ed.). Pearson. https://mrce.in/ebooks/Cryptography%20&%20Network%20Security%208th%20Ed.pdf

Microsoft. (2023). Multi-factor authentication (MFA). Microsoft Learn. https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks

National Institute of Standards and Technology. (2017). Digital identity guidelines: Authentication and lifecycle management (SP 800-63B). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-63b

National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). NIST. https://doi.org/10.6028/NIST.CSWP.04162018

Kaufman, C., Perlman, R., & Speciner, M. (2022). Network security: Private communication in a public world (3rd ed.). Pearson Education.

https://www.pearson.com/en-us/subject-catalog/p/network-security-private-communications-in-a-public-world/P200000000360/9780136643524

Brasil. (2018). Lei N° 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Presidência da República. https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

Parlamento Europeo y Consejo de la Unión Europea. (2016). *Reglamento (UE) 2016/679 (GDPR).* Diario Oficial de la Unión Europea. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679

State of California. (2018). California Consumer Privacy Act (CCPA), Assembly Bill No. 375. Legislative Counsel of California https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

Presidencia del Consejo de Ministros. (2018). Decreto Supremo N.° 050-2018-PCM que aprueba la Política Nacional de Ciberseguridad. Diario Oficial El Peruano. https://www.gob.pe/institucion/pcm/normas-legales/247733-050-2018-pcm

Center for Internet Security. (2021). CIS Controls v8. Center for Internet Security. https://www.cisecurity.org/controls/v8

International Organization for Standardization & International Electrotechnical Commission. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. ISO. https://www.iso.org/standard/82875.html

Floridi, L., & Taddeo, M. (2016). What is data ethics? Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 374(2083), 20160360. https://doi.org/10.1098/rsta.2016.0360

National Institute of Standards and Technology. (2024). *Guide to IPsec VPNs* (NIST Special Publication 800-77, Revision 1). U.S. Department of Commerce. https://csrc.nist.gov/pubs/sp/800/77/r1/final

BDO. (s. f.). Ciberseguridad y resiliencia. BDO España.

https://www.bdo.es/es-es/servicios/advisory/risk-advisory/otros-servicios-de-risk-advisory/ciberseguridad-y-resiliencia

Nurse, J. R. C., Williams, N., Collins, E., Panteli, N., Blythe, J., & Koppelman, B. (2021). Remote Working Pre- and Post-COVID-19: An Analysis of New Threats and Risks to Security and Privacy. arXiv. https://arxiv.org/abs/2107.03907 arXiv

National Security Agency. (2021). Selecting and hardening remote access VPN solutions [Cybersecurity Information Sheet]. National Security Agency. https://media.defense.gov/2021/Sep/28/2002863184/-1/-1/0/csi_selecting-hardening-remote-access-vpns-20210928.pdf

NIST. (s. f.). remote access [Definición]. CSRC Glossary. https://csrc.nist.gov/glossary/term/remote_access

MikroTik. (2025). Virtual Private Networks. MikroTik Documentation. https://help.mikrotik.com/docs/display/ROS/Virtual+Private+Networks.

ANEXOS

Anexo 1. Configuración base del MikroTik RB750r2

```
/ip address add address=192.168.1.2/24 interface=ether1 comment="WAN Optical"
/ip address add address=192.168.20.1/24 interface=ether2 comment="LAN interna"
/ip route add dst-address=0.0.0.0/0 gateway=192.168.1.3 comment="Gateway Optical"
/ip dns set servers=8.8.8.8,1.1.1.1 allow-remote-requests=yes
/ip pool add name=vpn-pool ranges=10.8.0.10-10.8.0.30
/ppp profile add name=default-encryption local-address=10.8.0.1 remote-address=vpn-pool use-encryption=yes only-one=no
```

Anexo2. Certificados digitales y servidor OpenVPN

```
/certificate add name=CA common-name=CA key-usage=key-cert-sign,crl-sign

/certificate sign CA name=CA

/certificate set CA trusted=yes

/certificate add name=server common-name=server key-usage=digital-signature,key-encipherment,tls-server

/certificate sign server ca=CA name=server
```

Certificados de clientes

/certificate add name=finanzas01 common-name=finanzas01 key-usage=tls-client

/certificate add name=finanzas02 common-name=finanzas02 key-usage=tls-client

/certificate add name=finanzas03 common-name=finanzas03 key-usage=tls-client

/certificate sign finanzas01 ca=CA name=finanzas01

/certificate sign finanzas02 ca=CA name=finanzas02

/certificate sign finanzas03 ca=CA name=finanzas03

/certificate export-certificate CA

/certificate export-certificate finanzas01 export-passphrase=""

/certificate export-certificate finanzas02 export-passphrase=""

/certificate export-certificate finanzas03 export-passphrase=""

Usuarios VPN

/ppp secret add name=finanzas01 password= F1na7$2025%+ service=ovpn profile=default-encryption

/ppp secret add name=finanzas02 password= F1na7$2025%+ service=ovpn profile=default-encryption

/ppp secret add name=finanzas03 password= F1na7$2025%+ service=ovpn profile=default-encryption

/interface ovpn-server server set enabled=yes port=1194 mode=ip protocol=tcp netmask=24 \

default-profile=default-encryption certificate=server \

require-client-certificate=yes auth=sha1 cipher=aes256 keepalive-timeout=60 user-auth-method=pap

Anexo 3. Reglas de firewall y NAT

/ip firewall filter

add chain=input action=accept protocol=tcp dst-port=1194 comment="Permitir OpenVPN TCP 1194"

/ip firewall filter

add chain=forward src-address=10.8.0.0/24 dst-address=192.168.20.10 protocol=tcp dst-port=1433 action=accept comment="VPN -> CONCAR SQL"

/ip firewall filter

add chain=forward src-address=10.8.0.0/24 dst-address=192.168.20.0/24 action=accept comment="VPN -> LAN general"

/ip firewall filter

add chain=forward src-address=192.168.20.0/24 dst-address=10.8.0.0/24 action=accept comment="LAN -> VPN"

/ip firewall filter

add chain=input action=drop comment="Drop general INPUT"

/ip firewall filter

add chain=forward action=drop comment="Drop general FORWARD"

Anexo 4. Configuración del cliente OpenVPN

Cada usuario del área de Finanzas utiliza un archivo .ovpn que establece la conexión cifrada con el servidor OpenVPN.

El siguiente ejemplo corresponde al usuario **finanzas01**.

```
client

dev tun

proto tcp

remote 170.81.99.125 1194

resolv-retry infinite

nobind

persist-key

persist-tun

auth-user-pass

remote-cert-tls  server

cipher AES-256-CBC

auth SHA2

verb 3

ca "cert_export_CA.crt"

cert "cert_export_finanzas01.crt"

key "cert_export_finanzas01.key"
```

Archivos requeridos

- cert_export_CA.crt
- cert_export_finanzas01.crt
- cert_export_finanzas01.key

Credenciales de acceso (definidas en el MikroTik):

- **Usuario 1:** finanzas01 → Contraseña Clave01 F1na7$2025%+
- **Usuario 2:** finanzas02 → Contraseña Clave02 F1n4$2025%+
- **Usuario 3:** finanzas03 → Contraseña Clave03 F1n45$2025%+

(Estas credenciales fueron creadas mediante el Comando /Ppp Secret Add descrito en el **Anexo 2.)**

Procedimiento de conexión

1. Instalar el cliente OpenVPN Connect.
2. Copiar el archivo .ovpn y certificados en la carpeta de configuración.
3. Iniciar el cliente y conectar el perfil correspondiente.
4. Verificar el mensaje “Initialization Sequence Completed”.
5. Confirmar acceso al servidor CONCAR (192.168.20.10) mediante prueba de conectividad.