



UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E
INFORMÁTICA, ESCUELA DE TECNOLOGÍAS DE
LA INFORMACIÓN Y LA COMUNICACIÓN

TEMA:

VPN y su impacto en la comunicación entre sucursales de la empresa
AVCAMNET S.A.S de la Ciudad de Babahoyo.

EGRESADO:

LOZANO CAÑOLA LUIS EDUARDO

TUTOR:

ING. ESPARZA CRUZ NELLY KARINA

PERIODO ABRIL 2024 – AGOSTO 2024

DEDICATORIA

A la memoria de mi querida amiga Brisa Castillo, quien siempre fue una fuente de inspiración y alegría. Aunque ya no estás conmigo, tu espíritu y tu luz continúan iluminando mi camino. Tus palabras de aliento y tu ejemplo de perseverancia me han motivado en cada etapa de este proyecto. Este trabajo es un tributo a tu recuerdo y a la influencia positiva que tuviste en mi vida, demostrando que tu legado sigue vivo en cada uno de mis logros.

También dedico este proyecto a mis amigos, cuyo apoyo incondicional y ánimo constante han sido fundamentales en este proceso. A cada uno de ustedes, que me han brindado su compañía y han estado presentes en los momentos más difíciles, les agradezco profundamente. Sus palabras de aliento y su disposición para ayudarme siempre serán valoradas y recordadas. A mi familia, por su amor y paciencia inagotables. A mis padres, por su comprensión y sacrificio, por creer en mis sueños y apoyarme en cada paso del camino. A mis hermanos, por su compañerismo y por ser una fuente constante de motivación. Este logro es tan suyo como mío, y les agradezco desde el fondo de mi corazón por todo lo que han hecho por mí.

AGRADECIMIENTO

Lo primero que quiero hacer es expresar mis sinceros agradecimientos a todas las personas y entidades que hicieron este estudio sobre el impacto de las VPN en la comunicación entre sucursales de la empresa AVCAMNET SAS en la ciudad de Babahoyo. En primer lugar, me gustaría agradecer a AVCAMNET SAS por abrirnos sus puertas y hacernos disponibles informaciones cruciales para este proyecto. Fue la colaboración y disposición de esta empresa lo que nos permitió entender la infraestructura tecnológica y los desafíos operativos que acompañan a la aplicación de VPN. Además, quiero dar las gracias a mi asesor de investigación. Su guía experta, paciencia inagotable y dedicación absoluto han sido fundamentales para a lo largo de este proceso. Sus valiosos comentarios y consejos han aumentado significativamente la calidad de este trabajo. Por último, pero no menos importante, agradezco a mi familia y amigos por su apoyo incondicional, paciencia, y por estar a mi lado de principio a fin en el desarrollo de este proyecto. Sin sus palabras de ánimo me hubiera resultado imposible dar el último empujón para terminar esta investigación con éxito.

RESUMEN

La implementación de una VPN en AVCAMNET S.A.S. busca mejorar la seguridad y eficiencia de la comunicación entre sus sucursales en Babahoyo, evaluando el impacto de esta tecnología en la protección de datos y el rendimiento de la red. El objetivo general es analizar el impacto de la VPN en el aseguramiento de la comunicación entre las sucursales de AVCAMNET S.A.S. Para ello, se utilizó una metodología mixta, recolectando datos cualitativos y cuantitativos mediante herramientas como Monitorix y Excel para el monitoreo y análisis del tráfico de red, así como entrevistas al dueño de la empresa para obtener información sobre la percepción y beneficios de la VPN. Los resultados mostraron que la implementación de la VPN resultó en una mejora significativa en la seguridad de la información, reduciendo vulnerabilidades y accesos no autorizados. Aunque se observó una disminución en la velocidad de la red debido al cifrado, la estabilidad y confiabilidad de la conexión se mantuvieron aceptables, y el dueño de la empresa reportó una mejora en la eficiencia operativa gracias a esta estabilidad. En conclusión, la VPN aumentó significativamente la seguridad de la información en AVCAMNET S.A.S., confirmando la hipótesis inicial. Los beneficios en términos de seguridad y estabilidad superan las desventajas relacionadas con la velocidad, y los hallazgos concuerdan con estudios previos, reforzando la validez de los resultados obtenidos.

Palabras Claves: VPN, seguridad de la información, comunicación empresarial, estabilidad de red, eficiencia operativa.

ABSTRACT

The implementation of a VPN at AVCAMNET S.A.S. aims to enhance the security and efficiency of communication between its branches in Babahoyo, evaluating the impact of this technology on data protection and network performance. The main objective is to analyze the impact of the VPN on securing communication between AVCAMNET S.A.S. branches. A mixed methodology was used, collecting both qualitative and quantitative data through tools like Monitorix and Excel for monitoring and analyzing network traffic, as well as interviews with the company owner to gather information on the perception and benefits of the VPN. The results showed that the VPN implementation significantly improved information security, reducing vulnerabilities and unauthorized access. Although a decrease in network speed was observed due to encryption, connection stability and reliability remained acceptable, and the company owner reported improved operational efficiency thanks to this stability. In conclusion, the VPN significantly increased information security at AVCAMNET S.A.S., confirming the initial hypothesis. The benefits in terms of security and stability outweigh the disadvantages related to speed, and the findings are consistent with previous studies, reinforcing the validity of the obtained results.

Palabras Claves: VPN, seguridad de la información, comunicación empresarial, estabilidad de red, eficiencia operativa.

INDICE

INTRODUCCION	9
CAPITULO I	11
1.1 Marco Contextual	11
1.1.1 Contexto Internacional.....	11
1.1.2 Contexto Nacional.....	11
1.1.3 Contexto Local y/o Institucional.....	12
1.2 Situación problemática	13
1.2.1 Planteamiento del problema	13
1.2.2 Delimitación de la Investigación	13
1.3 Justificación	15
1.4 Objetivos	16
1.4.1 Objetivo General	16
1.4.2 Objetivos específicos	16
1.5 Hipótesis	17
CAPITULO II	18
2. MARCO TEÓRICO	18
2.1 Antecedentes investigativos	18
2.2 Bases Teóricas	23

CAPITULO III	29
3. METODOLOGÍA DE LA INVESTIGACIÓN	29
3.1 Tipo y diseño de investigación	29
3.2 Operacionalización de variables	30
3.3 Población y muestra de investigación	31
3.4 Técnicas e instrumentos de medición	31
3.5 Procesamiento de datos	33
3.6 Aspectos éticos	34
3.7 PRESUPUESTO Y CRONOGRAMA	35
3.7.1 Talento humano	35
3.8 CRONOGRAMA	36
3.9 Plan de tabulación y análisis	37
3.9.1 Base de datos	37
3.9.2 Procesamiento y análisis de los datos	38
Nivel de Seguridad.....	38
Incidentes Reportados.....	38
Frecuencia de Auditorías.....	38
CAPITULO IV	44
4. RESULTADOS Y DISCUSIÓN	44
4.1 Resultados obtenidos de la investigación	44

4.2	Análisis e interpretación de datos	48
CAPITULO V		54
5.	CONCLUSIONES Y RECOMENDACIONES.....	54
5.2	Recomendaciones	56
REFERENCIA BIBLIOGRAFICAS		57
Bibliografía		57

INTRODUCCION

En el contexto empresarial moderno, la implementación de redes privadas virtuales ha surgido como una herramienta crucial para facilitar la comunicación segura y eficiente entre las sucursales de las organizaciones. Las VPN permiten a las empresas como AVCAMNET S.A.S., proveedor de servicios de internet en Babahoyo, establecer conexiones cifradas sobre redes públicas, garantizando la confidencialidad y la integridad de los datos transmitidos. Este avance tecnológico no solo mejora la seguridad de la comunicación interna, sino que también optimiza la conectividad entre las distintas sedes de la empresa, proporcionando una infraestructura flexible y escalable para sus operaciones.

El presente estudio se centra en analizar el impacto de la VPN en la comunicación entre sucursales de AVCAMNET S.A.S. en Babahoyo. Con el crecimiento de la empresa en presencia e incremento sus servicios, también la seguridad de los datos y transmisión de estos se vuelve vital. No se trata sólo de cómo VPN puede integrar las sucursales, pero aún más importante es conocer los desafíos técnicos, operativos y de seguridad que se pueden presentar en su implantación o mantenimiento. No entender eso es imposible acercarse a métodos mediante los cuales se pueda averiguar la forma de hacer más operativa y competitiva AVCAMNET S.A.S. en el cambiante mercado de servicios de Internet.

TEMA DE INVESTIGACIÓN

VPN y su impacto en la comunicación entre sucursales de la empresa

AVCAMNET S.A.S de la Ciudad de Babahoyo.

CAPITULO I

1.1 Marco Contextual

1.1.1 Contexto Internacional

A nivel internacional, Cisco ha introducido el uso de Red Privada Virtual para acceso a las redes de la empresa por parte de sus empleados remotamente desde cualquier lugar. En un mundo empresarial con necesidades en flexibilidad y seguridad, Cisco corre una Red Privada Virtual que permite a los empleados trabajar desde casa de forma segura y eficaz. El uso de la red permite a la empresa asegurarse de que la información y los datos sensibles de la empresa no son una amenaza para los ataques cibernéticos, todo el tiempo permite una fácil colaboración y espacio de trabajo remoto. En general, la estrategia de usar VPN en la franquicia diaria de Cisco garantiza que las comunicaciones corporativas integrales y el acceso seguro a los recursos se mantengan informan a la mayoría, permitiendo a Cisco mantener una alta seguridad y ahorro de costes de operación más altos. estándar en el mundo digital.

1.1.2 Contexto Nacional

NetLife es un proveedor de servicios de internet en rápida expansión en Ecuador, y en su afán de proporcionar a sus clientes empresariales una manera segura y confiable de conectarse a su red, ha implementado una solución de Redes Privadas Virtuales. La creciente necesidad de proteger la información confidencial y permitir a los empleados trabajar desde casa ha influido en la decisión de NetLife. Al cifrar por completo todas las transmisiones de datos, una solución VPN puede proteger de esta manera información valiosa como datos financieros y propiedad intelectual. También disminuye significativamente el riesgo de filtraciones, ataques cibernéticos directos: En lugar de ir a la oficina para trabajar, el empleado no tiene que hacerlo si está equipado con una VPN. Porque desde casa o cualquier lugar del mundo le es igualmente útil y seguro realizar su

tarea con este tipo de facilidades disponibles gratuitamente para cada quien mientras significa trabajo en cualquier parte siempre que no ponen en peligro los documentos confidenciales en los computadores.

1.1.3 Contexto Local y/o Institucional

En el caso del entorno local de Babahoyo, la continua implementación de una Red Privada Virtual por parte de las empresas proveedoras de servicios de Internet ha sido una medida establecida para asegurar la seguridad y confidencialidad de la información en este caso de las comunicaciones entre sucursales. Como tal, esta solución no solo aumenta la seguridad de las comunicaciones internas, sino que también integra a las diversas oficinas de la empresa mediante una capa de infraestructura flexible y escalable para sus operaciones.

1.2 Situación problemática

El problema de esta investigación es comprender la ineficiencia y falta de fluidez en la comunicación interna de una empresa que utiliza VPN para transmitir su información. La novedad del problema radica en la popularidad de las VPN en el campo empresarial y la falta de estudios en esta área específica de su aplicación para la comunicación de las empresas. Este problema es relevante para la tecnología y los sectores de negocios y, entre sus características fundamentales, se encuentra la disponibilidad de acceso a la infraestructura de la organización y la contribución del personal de la empresa, para poder recopilar datos precisos y confiables que permitan presentar soluciones racionales.

1.2.1 Planteamiento del problema

El estudio se centrará en evaluar si la VPN implementada ha logrado mejorar la velocidad, la seguridad y la fiabilidad de la comunicación entre las sucursales de AVCAMNET S.A.S. Con este enfoque abarcador podremos dar una idea realista del impacto de la VPN, sugerir recomendaciones fundamentadas en datos para su optimización y sumar nuestro conocimiento de lo que funciona mejor. En este sentido, la cuestión clave de esta pregunta de investigación es la siguiente: *¿Cuál es el impacto del uso de una red privada virtual en la comunicación entre las sucursales de AVCAMNET S.A.S. en la Ciudad de Babahoyo?*

1.2.2 Delimitación de la Investigación

Delimitación espacial: El estudio se realizará en el contexto de la ciudad de Babahoyo de los Ríos, donde se encuentra ubicada las sucursales.

Delimitación temporal: El estudio se realizará en el periodo de mayo a julio del 2024.

Delimitación del universo: La población objeto de análisis incluirá los sistemas de comunicación interna y la información proporcionada por el dueño de AVCAMNET S.A.S. en Babahoyo durante el periodo de estudio

Delimitación por contenido

Campo: Tecnología de la Información y Comunicaciones (TIC).

Área: Redes y Seguridad.

Aspecto: VPN y su impacto en la seguridad de la comunicación entre sucursales de AVCAMNET S.A.S.

1.3 Justificación

La importancia del estudio del impacto del uso de las redes privadas virtuales para la intercomunicación de las sucursales de AVCAMNET S.A.S. en Babahoyo es tanto teórica como práctica. Desde un punto de vista teórico, el estudio será una contribución al conocimiento existente en el campo de las Tecnologías de la Información y las Comunicaciones en el segmento de redes y seguridad informática. A su vez, la presente investigación permitirá obtener información más detallada sobre cómo la implementación de tecnologías como las VPN puede innovar o cambiar la forma de sistemas ya existentes en comunicación de empresas, lo que podrá ser utilizado como conocimiento valioso para la dirección en futuras investigaciones en este campo.

En cuanto a la perspectiva práctica, el estudio beneficiará directamente a AVCAMNET S.A.S. con información detallada sobre los efectos y los posibles beneficios de implementar la VPN en la comunicación entre sucursales. En particular, se espera que los resultados mejoren la seguridad de la información, optimicen los recursos de la red y, posiblemente, disminuyan los costos operativos de la infraestructura de comunicaciones. Así mismo, los hallazgos de investigación también ayudarán a identificar recomendaciones específicas para maximizar los beneficios de la VPN y abordar los desafíos adicionales que la empresa puede experimentar durante la implementación y su operación.

1.4 Objetivos

1.4.1 Objetivo General

Analizar el impacto de la VPN en el aseguramiento de la comunicación entre sucursales de la empresa AVCAMNET S.A.S de la Ciudad de Babahoyo.

1.4.2 Objetivos específicos

- Analizar la infraestructura tecnológica utilizada por AVCAMNET S.A. para la comunicación entre sucursales.
- Determinar los protocolos y aplicaciones VPN para el aseguramiento de las comunicaciones entre sucursales.
- Estimar la confidencialidad de la comunicación entre sucursales de la empresa AVCAMNET S.A.

1.5 Hipótesis

Se espera que la VPN en AVCAMNET S.A.S. mejore significativamente la seguridad y eficiencia de la comunicación entre sus sucursales, reflejándose en una reducción en los tiempos de acceso a datos y una mayor protección contra posibles vulnerabilidades de seguridad.

CAPITULO II

2. MARCO TEÓRICO

2.1 Antecedentes investigativos

En el estudio realizado por Andia y Scott (2023), titulado: **Implementación de un VPN basado en la metodología top-Down para mejorar la seguridad de la información en el consorcio Andia**, Cuyo objetivo general fue medir el impacto de la puesta en marcha en el consorcio de una red segura basada en la metodología top-down en la seguridad de su información. Aplicando una metodología con enfoque cuantitativo, se confirmó que la solución propuesta a la problemática del estudio permitió a los teletrabajadores acceder de forma segura a las aplicaciones digitales de la empresa con una mejora del rendimiento que, a pesar de no ser óptima, fue aceptable dadas las limitadas características tecnológicas. Con relación a los resultados obtenidos plasmados en este trabajo, se concluyó que la implementación de la VPN mejoró la seguridad de la información en el Consorcio Andia de un 26.5% para la variable a un mejoramiento del 40% para la seguridad de la información. A su vez, se recomendó la migración a la nube desde la empresa, pero cada instante de la misma debe velar por un constante enfoque en la seguridad. Colocar soluciones sólidas para proteger los datos y proteger los sistemas en la nube, investigar las probables formas de ataque de manera continua y mantener una elevada preparación ante desastres fue crítico.

Por otro lado, en un estudio realizado por Gómez (2023), titulado: **implementación de una vpn site to site bajo el protocolo de cifrado ipsec para el control y seguridad administrativa de la empresa privada inter&solutions**, La implementación de una VPN SITE TO SITE con el protocolo de cifrado IPSEC permitió controlar y asegurar administrativamente a la empresa

privada INTER&SOLUTIONS. Más específicamente, la idea fue presentar los beneficios y principales atributos de la tecnología VPN. Uno de tales aspectos beneficiosos fue la escalabilidad de la propia tecnología, la conexión VPN pudo admitir un mayor número de usuarios y sitios, en comparación con las líneas dedicadas tradicionales. También la metodología utilizada fue cuantitativa, ya que, aunque se eligió una encuesta cerrada para la prueba tipo Likert, fue descriptiva, de modo que el lector se explicó cómo el proceso y el resultado de dicha implementación en su empresa se llevó a cabo de manera segura, y así, se concluyó que el cumplimiento de conectar remoto para la seguridad de la empresa y el cifrado de protocolo, por lo que concluyó que fue un objetivo que ayudó a mantener la integridad de los datos transmitidos y qué configuración fue más óptima, garantizando una rápida recuperación a su operación.

Así mismo en el artículo científico efectuado por Oladipo et al. (2024), titulado: **virtual private networks (vpn): a conceptual review of security protocols and their application in modern networks**, El objetivo de este estudio fue proporcionar una revisión comprensiva de las Redes privadas virtuales (VPN), con un enfoque en qué protocolos de seguridad se utilizan y cómo se aplican en redes modernas. La metodología utilizada para ganar este objetivo se basa en la revisión y el análisis de la literatura, investigaciones y estudios de casos. En este estudio se reunieron informes de industria. Los resultados deseados abarcan: llegar a comprender más claramente qué Tecnología VPN (networking) es y cómo ha evolucionado, tener un panorama completo acerca de los protocolos de seguridad empleados en el VPN y describir los problemas y desafíos que se presentan.

Un artículo realizado por Iqbal y Riadi (2019), titulado: **Analysis of Security Virtual Private Network (VPN) Using OpenVPN**, El objetivo era analizar la seguridad de la Red Privada Virtual utilizando OpenVPN en el laboratorio de investigación de Informática de la Universidad Ahmad Dahlan y evaluar el nivel de seguridad. La metodología utilizada involucró métodos de recopilación de datos a través de literatura y observación. Se diseñó una topología de red que se utilizó para implementar OpenVPN con dos routers Mikrotik. Se realizaron dos tipos de pruebas, a saber, pruebas de calidad de servicios y pruebas de seguridad. Esto incluyó sniffing de rezagos de datos usando Wireshark. Los resultados revelaron que la implementación de OpenVPN mejoró la seguridad de los datos. Aproximadamente, antes de OpenVPN, el rezago de datos había obtenido información confidencial. Después de implementar OpenVPN, los datos fueron rezagados y seguros. A nivel de QoS, hubo una disminución en la calidad de la red debido al proceso de cifrado y encapsulación. Por lo tanto, se concluyó que el uso de VPN con OpenVPN logró un nivel adecuado y mejor de seguridad para evitar que se recogieran residuos de datos. Entonces fue viable implementar suficientes medidas de seguridad en las redes de computadoras para garantizar la confidencialidad y la integridad de las redes.

El estudio realizado por Tuza (2023), titulado: **Sistema de comunicación y video vigilancia basado en túneles VPN para la integración de las sucursales de la cooperativa de ahorro y crédito vencedores de Tungurahua en el Ecuador**, El objetivo principal del trabajo fue implementar un sistema de comunicación y videovigilancia para la Cooperativa de Ahorro y Crédito Vencedores de Tungurahua con túneles VPN y otros sistemas tecnológicos que pretendía ayudar a mejorar la seguridad y la eficiencia de las operaciones de sucursales. La metodología descriptiva se divide en varios pasos: hardware adquisición e instalación, prueba de sistemas (con

IPsec como protocolo para la configuración de la VPN) y optimización de sistemas. Según los resultados, tras la instalación de nuevos enrutadores, servidores y el sistema de videovigilancia HIKVISION, se consiguieron avances significativos en seguridad y transmisión de datos. La discusión destacó la reducción del riesgo de seguridad y la mejora de la comunicación interna, aunque se identificaron algunas limitaciones: la necesidad tanto de aumentar la calidad de las cámaras de videovigilancia instaladas en la sucursal como de realizar análisis constantes de ancho de banda. En conclusión, la implementación demuestra ser exitosa en términos de seguridad y eficiencia. Por lo tanto, se recomienda ampliar aún más la implementación, ajustar los niveles de anchura de banda y disposición de las cámaras para el sistema de video vigilancia, mantener y desarrollar la infraestructura.

Por otro lado, en un estudio realizado por Cabrera y Cordero, (2021) (Cabrera & Cordero, 2021), titulado: **Diseño de una red para la empresa Arabito con solución en la nube en su sede principal interconectando sus sucursales mediante VPN MPLS**. El propósito del trabajo fue diseñar una red telemática para Arabito que conectaría sus sucursales utilizando las tecnologías VPN-MPLS, centrándose en la escalabilidad, la integridad y la interoperabilidad para garantizar la seguridad y la calidad de la conexión. La metodología consistió en dos partes: primeramente, la investigación de las tecnologías y dispositivos relacionados; en segundo lugar, la etapa de planificación, que incluyó la selección de servicios y la comparación de los proveedores, así como el boceto de la red y la simulación en el software GNS3. De este modo, los resultados permitieron establecer que con la red indicada que pudo asegurar la conexión eficiente y segura entre las sucursales y prepararse para el crecimiento a largo plazo. Discusión vinculó el beneficio de la solución en la nube implementada en la sede principal con el desempeño empresarial y la necesidad

de la capacitación constante y el mantenimiento. Finalmente, se garantiza un red eficiente y segura en función de la instalación y formación permanente de personas.

Así mismo un estudio realizado por Ataypoma (2023), titulado: **Como la implementación de una red privada virtual (VPN) mejora la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión.** El estudio tiene como propósito evaluar el uso de una red privada virtual para mejorar la comunicación entre las oficinas externas de la Universidad José Faustino Sánchez Carrión. La metodología empleada tiene un diseño estadístico a través de cuestionarios validados y técnicas de recolección y procesamiento de datos con el paquete estadístico SPSS 25.0. Las observaciones reflejan una comunicación significativa entre las oficinas al aplicar una VPN, además de una alta correlación entre las variables de funcionalidad, seguridad y confidencialidad. Una discusión de resultados destaca una VPN que no solo simplifica la comunicación, sino también mejora la seguridad de los datos transmitidos.

El estudio realizado por, Borja (2021) titulado: **Análisis de rendimiento de puertas de enlace VPN mediante una arquitectura de red para la comunicación segura sitio a sitio entre las pymes.** El objetivo de la investigación fue la presentación de la mayor arquitectura de red de protocolo de comunicaciones VPN apropiada para el protocolo de comunicaciones seguro del sitio a sitio entre las PYMES. La metodología abordó los rasgos explorativo, descriptivo, cuantitativo y cualitativo. Se aplicaron las herramientas de simulación GNS3 y Wireshark. Los resultados de la simulación mostraron que la arquitectura de la mejor VPN prometedora en lo que respecta al rendimiento, simplicidad y rapidez es WireGuard. Además, tanto IPsec como OpenVPN pueden

ser considerados justos sueños, pero no adecuados para rendimiento de alta velocidad. La justificación de los resultados indicó que las técnicas de encapsulación y cifrado utilizadas son las mismas que las reveladas en las revisas de estudios anteriores. WireGuard es el líder aquí, de hecho, en términos de su arquitectura y su eficiencia.

Por otro lado, en un estudio realizado por Idrogo (2021), titulado: **Implementación de una red VPN para el trabajo remoto en la empresa CLI gestiones Aduaneras S.A Lima 2020** El objetivo principal del estudio fue implementar una red VPN para IQAC y mejorar la calidad y seguridad del sistema y red mientras los empleados de CLI Gestiones Aduanas se vieron obligados a trabajar en casa. La metodología se centró en configurar la red VPN en el dispositivo firewall de Gestión Unificada de Amenazas y permitir la creación de túneles cifrados para una conexión segura. Como resultado, se logra una reducción significativa en el número de incidentes reportados: 177 incidentes denunciados en mayo antes de la implementación y solo 18 incidentes después de la implementación de la VPN. A saber, se mejoró la estabilidad de la conexión, la productividad y el número de órdenes mensuales atendidas por los mismos empleados, lo que se tradujo en una mayor satisfacción laboral.

2.2 Bases Teóricas

¿Qué es VPN?

Sobre este aspecto Cisco (2019) sostiene que:

Una conexión a internet desde un dispositivo a una red es una red privada virtual o VPN. La forma en que la conexión se cifra ayuda a asegurar la transmisión de información delicada o privada de manera segura. El tráfico en cuestión no puede ser espiado por personas no autorizadas, y el cliente puede trabajar desde casa. En el lugar de trabajo, la tecnología es muy utilizada.

Por otro lado, Kaspersky (2024) menciona que la VPN:

La VPN significa virtual private network y se refiere a la capacidad de crear una conexión segura cuando se utiliza la red pública. Las VPN encriptan su tráfico en línea al mismo tiempo que enmascaran su identidad en línea. Impide a los actores que no forman parte de realizar un seguimiento de sus actividades en línea y el pirateo de sus datos debido a que se realiza mientras se encripta.

¿Cómo funciona una red privada virtual (VPN)?

Sobre este punto, Cisco (2019) sostiene que:

Una VPN lleva la red corporativa a través de la criptografía a las conexiones a través de Internet. Como el tráfico está encriptado entre el dispositivo y la red, el tráfico permanece privado a través de los nodos intermedios. Incluso un empleado que trabaje desde su casa puede conectarse de manera segura a la red corporativa. Además, incluso los smartphones y tablets pueden conectarse a través de VPN.

Tipos de VPN

Al respecto Fernández (2024) sostiene que:

Los tipos de VPN según el tipo de acceso que tienen, que pueden ser de acceso remoto o de acceso de sitio a sitio. Cada uno de estos tipos de VPN tiene una manera de funcionar concreta y finalidades diferentes.

Seguridad en las VPNs

Sobre este punto, Kaspersky (2024) sostiene que:

Es fundamental recordar que las VPN no funcionan igual que un antivirus completo. Si bien protegen su IP y codifican el historial de Internet, eso es todo lo que pueden hacer. No te están protegidos, por ejemplo, si visitas sitios web de pesca o descargas archivos infectados.

Por otro lado, Expressvpn (2024) menciona:

Sin una VPN, el tráfico sin encriptar está visible para los demás ya sea que lo espíen o lo manipulen: es especialmente peligroso si uno se conecta tanto a redes públicas inseguras. Por eso usar una VPN es una manera rápida de mejorar tu seguridad en línea donde estés.

Según Marin et al., (2020) sostiene que:

Una de las grandes ventajas de este tipo de arquitectura son la confidencialidad e integridad de la información, puesto que se genera un canal cifrado por donde pasarán los datos, dándole así una mayor seguridad a la información

¿Qué es la comunicación de un negocio?

Sobre este punto, la Facultad de Comunicación (2024) sostiene que:

La comunicación empresarial implica interacción, construcción de vínculos y un constante flujo de datos e información dentro y fuera de una empresa. Su gestión incide directamente en la salud y el desempeño de la organización.

Por otro lado, QuestionPro (2024) menciona que la Comunicación:

La comunicación interna es la que se realiza al interior mismo de la organización, es decir, con el funcionario. Nace como respuesta a las necesidades más recientes de empresas para mantener a duras penas a los trabajadores motivados y retener en su plantilla a quienes son mejores profesionales, en un entorno cada día de mayor velocidad de cambio.

Según Martínez y Tejada, (2023) sostiene que:

En cualquier organización es importante procesar la comunicación; para empezar, ayuda a lograr una buena fluidez de las noticias. Además, los procesos de comunicación son un ingrediente básico en la relación interpersonal. (DLC) Es una pasarela entre seres

humanos, donde ambos pueden abrirse y transmitir sus sentimientos. En consecuencia, una persona puede superar el concepto erróneo. (p.1).

¿La importancia de la comunicación?

Al respecto Ochoa (2024) sostiene que:

En este momento es importante que el equipo se entere de las actualizaciones en cada una de las tiendas, se retroalimente mutuamente y acuerde metas conjuntas. Puede hacerse mediante juntas periódicas, programadas con antelación, con los gerentes de tus sucursales para compartir las actualizaciones de cada tienda. Para que las reuniones sean más efectivas es recomendable enviar el contenido antes. Entonces todos estarán preparados cuando llegue la hora de hablar.

Por otro lado, Malloy (2022) menciona que la Comunicación:

La comunicación empresarial puede cubrir todas las comunicaciones que tienen lugar dentro de campo específico de organización. La comunicación empresarial fomenta el crecimiento de la capacidad de persuadir a otras personas: para cambiar la actitud de un público, por tanto, los puntos de vista individuales llegaron reparados y aumentan su motivación por otra parte crean nuevas relaciones adineradas.

Según Gaona (2024) sostiene que:

Estandarizar los procesos cuando se cuenta con diferentes sucursales, así como la implementación de tecnología, es fundamental para lograr una mejor calidad en la prestación de los servicios debido a que esto representaría un impacto positivo en la aceptación de los clientes hacia la compañía, así como su satisfacción con el servicio que se les está brindado y su nivel de confianza en la empresa que garantizará que este cliente continúe eligiendo a la empresa sobre las demás en el mercado.(p. 9).

CAPITULO III

3. METODOLOGÍA DE LA INVESTIGACIÓN

3.1 Tipo y diseño de investigación

En este estudio sobre el impacto de una VPN en la comunicación entre empresas AVCAMNET se ha utilizado un enfoque de investigación aplicada y no experimental. La investigación fue de tipo documental o bibliográfico en lo que toca a la infraestructura tecnológica existente y también se recogió información de campo mediante observaciones directas y entrevistas a personal técnico. Se aplicó un enfoque descriptivo con la finalidad de describir la infraestructura actual y los protocolos VPN en uso, y evaluar su contribución a la seguridad y eficiencia en comunicación entre sucursales.

Método de investigación

Para el estudio se empleó la investigación de método mixto, en la que se combinó un método cualitativo y otro cuantitativo. El método cuantitativo fue empleado para el análisis de la infraestructura tecnológica, así como protocolos de acceso VPN, a través de una detallada entrevista con el propietario de AVCAMNET S.A.S. Con esto, se pudo obtener una comprensión muy completa de hasta qué punto estas tecnologías se utilizan dentro de la empresa. Por otro lado, el método cuantitativo se componía de datos analizados que se recogieron con herramientas de supervisión en red y métricas de seguridad para medir de manera cuantitativa tanto la eficacia como la seguridad en comunicaciones entre sucursales.

3.2 Operacionalización de variables

Tabla 1. Operacionalización de variables

Variable	Definición Conceptual	Dimensión o categoría	Indicadores	Índice
VPN	Un VPN (Red Privada Virtual) es una tecnología que crea una conexión segura y encriptada a través de una red pública, como Internet.	Seguridad	Tipo de protocolo	Cualitativo
			Algoritmo de encriptación	
			Autenticación	
			Políticas de no registro	
			Auditoria de seguridad	
			Ubicación de la vpn	
		Infraestructura	Velocidad de conexión	
			Eficiencia	
			Efectividad	
			Seguridad	
IMPACTO EN LA COMUNICACIÓN	La comunicación entre sucursales es el proceso mediante el cual las distintas oficinas o tiendas de una misma empresa intercambian información de manera eficiente	Seguridad de la comunicación		Cuantitativo
			Nivel de seguridad	
			Incidentes de seguridad	
		Eficacia de la comunicación	Velocidad de conexión entre sucursales	
			Estabilidad de la conexión	

Elaborado por: Lozano Cañola Luis Eduardo

3.3 Población y muestra de investigación

3.3.1 Población

La población objeto de estudio está conformada por el dueño de AVCAMNET S.A.S. en Babahoyo, quien proporciona información clave sobre la implementación y uso de la VPN en la empresa.

3.3.2 Muestra

Dado que la población está compuesta exclusivamente por el dueño de la empresa, la muestra será el 100% de esta población.

Se incluirán en la muestra:

Entrevista clave: Se realizó una entrevista al dueño de AVCAMNET S.A.S. para obtener información detallada sobre la implementación de la VPN y su percepción sobre el impacto en la comunicación entre sucursales.

La elección de la muestra se basa en la importancia del dueño para proporcionar una perspectiva integral sobre el uso de la VPN y la comunicación interna. No se realizaron cálculos adicionales de tamaño de muestra debido a que la población relevante es única.

3.4 Técnicas e instrumentos de medición

3.4.1 Técnicas

Para la recolección de información, se utilizaron principalmente las siguientes técnicas:

Entrevista: Se realizó una entrevista al dueño de AVCAMNET S.A.S. para obtener información detallada sobre la implementación de la VPN y su percepción sobre el impacto en la comunicación entre sucursales. La entrevista siguió un formato estructurado para asegurar la consistencia en las respuestas y abordar aspectos clave del problema.

Análisis de métricas: Se analizaron métricas como el tiempo de respuesta y la cantidad de información compartida, lo que permitió evaluar la efectividad de la comunicación facilitada por la VPN.

3.4.2 Instrumentos

Entrevista estructurada: Este instrumento fue utilizado como guía al entrevistar al dueño de AVCAMNET S.A.S. Se hicieron preguntas específicas sobre la implementación de la VPN, los protocolos que se utilizan, la infraestructura tecnológica y el impacto percibido en la comunicación entre sucursales.

Herramientas de monitoreo de redes: Para recopilar datos de rendimiento de la red y la seguridad, utilicé herramientas de monitoreo. Estas herramientas registraron datos sobre la velocidad de conexión, estabilidad de la conexión, factibilidad de configuración, compatibilidad de dispositivos, nivel de seguridad, e incidentes de seguridad.

3.5 Procesamiento de datos

El análisis de datos en esta investigación se llevará a cabo en diversas fases. En primer lugar, transcriba y organice los datos cualitativos obtenidos a través de entrevistas, codificando y categorizando las respuestas a fin de identificar temas comunes y relevantes patrones que tendrán efectos de la implementación del VPN su efectividad. Para el mapeo de comunicación entre sucursales. Los datos cuantitativos, recolectados a través de herramientas de monitoreo de redes, se exportarán a hojas de cálculo para su análisis, empleando métodos estadísticos para evaluar las métricas de seguridad y rendimiento de la VPN, como la velocidad de conexión y la estabilidad de las comunicaciones. Con este análisis, las percepciones cualitativas del personal pueden ser confrontadas con las métricas objetivas de rendimiento y seguridad. Así se presentarán de forma sencilla gráficas y cuadros que ilustren hallazgos relevantes en tablas fáciles de entender.

3.6 Aspectos éticos

En cuanto a los aspectos éticos de la investigación, se garantizará la privacidad y confidencialidad de los datos obtenidos, asegurando un manejo adecuado de la información sensible y evitando su divulgación sin autorización expresa de los participantes. Todo esto se realizará tomando en consideración la Ley Orgánica de Protección de Datos Personales, en vigor en Ecuador desde el 26 de mayo de 2021.

3.7 PRESUPUESTO Y CRONOGRAMA

3.7.1 Talento humano

Tabla 2

Talento humano

Talento Humano/Rol	Nombres y Apellidos
Investigador	Luis Eduardo Lozano Cañola
Asesor del Proyecto de Investigación	Ing. Nelly Karina Esparza Cruz

3.7.2 Recursos Económicos

Tabla 3

Recursos económicos

Recursos Económicos	Inversión
Llamadas telefónicas	\$40,00
Internet	\$70,00
Anillados	\$5,00
Libros	\$20,00
Copias a colores	\$25,00
Fotocopia Final	\$20,00
Fotografías	\$5,00
Empastada de Proyecto	\$45,00
Alimentación	\$50,00
Movilización y transporte	\$40,00
Carpetas transparentes	\$5,00
Total	325,00

Nota. Elaborado por el autor

3.8 CRONOGRAMA

Tabla 4

Cronograma de actividades.

N°	Actividades	Meses																											
		abr-24				may-24				jun-24				jul-24				ago-24				sep-24							
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4				
1	Selección de Tema					X																							
2	Aprobación del tema (perfil)						X																						
3	Recopilación de la Información								X																				
4	Desarrollo del capítulo I								X																				
5	Desarrollo del capítulo II								X																				
6	Desarrollo del capítulo III									X																			
7	Sustentación (proyecto)										X																		
8	Aplicación de las encuestas											X	X																
9	Tamización de la información													X	X														
10	Desarrollo del capítulo IV														X	X													
11	Desarrollo del capítulo V																X	X											
12	Presentación del proyecto de integración curricular (SAI)																			X									
13	Entrega de documentos (SAI)																			X									
14	Sustentación																			X									

Nota. Elaborado por el autor

3.9 Plan de tabulación y análisis

3.9.1 Base de datos

En el marco del proyecto de investigación, la información recopilada se llevó a cabo sistemáticamente y de manera organizada. Se ha llevado a cabo un proceso estructurado de garantía de calidad y fiabilidad de los datos recogidos. Usarse un formulario de entrevista que incluye preguntas específicas y relevantes respecto a los objetivos de esta investigación. El formulario se utilizó en las entrevistas con el dueño de la empresa de AVCAMNET S.A.S

Para automatizar la recolección y gestión de datos, se elige un programa informático como Excel (Microsoft). Ofrece este software un conjunto de herramientas y funciones que hacen más fácil el proceso, así como estadístico análisis de los datos. Hemos dejado estos en métodos muy concretos: por ejemplo, cada conjunto de datos tiene su hoja de cálculo propia en la que se pueda estructurar la información recogida de una forma regular y legible. El uso de Excel aporta un sistema seguro y versátil para manejar la información recopilada, con lo que se logró asegurar que los datos se mantengan íntegros a lo largo del proceso de investigación.

Para el monitoreo de redes y recolección de métricas de seguridad y rendimiento, utilizamos Monitorix. Luego los datos exportados en formato CSV se organizaron en hojas de cálculo para su posterior análisis. Utilizando Excel se logró una plataforma confiable y flexible para el manejo de la información donde los datos mantuvieron su consistencia y coherencia durante todo el proceso de investigación.

3.9.2 Procesamiento y análisis de los datos

Se utilizaron métodos de análisis de contenido temático para analizar los datos cualitativos, con miras a discernir patrones y temas recurrentes relacionados con la implementación y el uso de VPN. Los datos cuantitativos fueron tratados con MATLAB y Excel para realizarse análisis descriptivos comparativos. Se evaluaba así la eficacia y seguridad de la VPN en comunicación punto a punto. Mediante gráficos y modelos predictivos generados en MATLAB, se obtuvo una visualización analítica del impacto de la VPN en la red de AVCAMNET S.A.S. Monitorix se utilizó para monitorizar tráfico de VPN, proporcionó mediciones sobre la velocidad de la señal, estabilidad etc. Pero como herramienta de análisis es insuficiente.

Tabla 5

Nivel de Seguridad e Incidentes de Seguridad

Aspecto de Seguridad	Nivel de Seguridad	Incidentes Reportados	Frecuencia de Auditorías
Protocolo VPN Utilizado	Alto	0	Mensual
Algoritmos de Encriptación	AES-256	1	Mensual
Métodos de Autenticación	2FA	0	Mensual
Políticas de No Registro	Estrictas	0	Mensual
Ubicación de Servidores	Seguro	0	Mensual

Nota. Elaborado por el autor

Interpretación

La tabla analiza el nivel de seguridad e incidentes en diferentes aspectos de la infraestructura de red de AVCAMNET S.A.S., mostrando que el protocolo VPN utilizado tiene un nivel de seguridad alto sin incidentes reportados y auditorías mensuales. Los algoritmos de encriptación usan AES-256, que es muy seguro, aunque se ha reportado un incidente, con auditorías mensuales para mantener su integridad. Los métodos de autenticación implementan 2FA, sin incidentes reportados y auditorías mensuales. Las políticas de no registro son estrictas y también se auditan mensualmente, sin incidentes reportados. La ubicación de servidores se considera segura, con auditorías mensuales y sin incidentes reportados, demostrando un compromiso constante con la seguridad y privacidad de los datos.

Tabla 6

Monitoreo de Tráfico de la VPN (Monitorix)

Fecha	Hora	Tasa de pérdida de paquetes (%)	Uso del CPU (%)	Uso de la memoria	Tasa de Subida (Mbps)	Tasa de bajada (Mbps)
010/06/2024	10:00	0.5	35	40	52	98
010/06/2024	12:00	0.7	40	45	60	95
010/06/2024	14:00	0.4	37	42	55	97
011/06/2024	10:00	0.3	36	41	54	99
011/06/2024	12:00	0.6	38	43	58	93
011/06/2024	14:00	0.5	35	40	53	97

012/06/2024	10:00	0.2	34	39	51	98
012/06/2024	12:00	0.8	41	46	60	92
012/06/2024	14:00	0.4	37	42	54	82

Nota. Elaborado por el autor

Interpretación

La tabla actualizada muestra un monitoreo detallado de la VPN, incluyendo la tasa de pérdida de paquetes, el uso del CPU y la memoria, y las tasas de subida y bajada. Las tasas de subida ahora están por encima de 50 Mbps, y las de bajada están por debajo de 100 Mbps, lo que indica un rendimiento robusto de la VPN. Se observan incrementos en el uso del CPU y la memoria durante horas específicas, lo que sugiere periodos de alta actividad en la red.

Tabla 7

Análisis de Velocidad y Latencia de la Conexión VPN

Fecha	Hora	Velocidad de descarga (Mbps)	Velocidad de Subida (Mbps)	Latencia (ms)
01/06/2024	08:00	100	50	20
01/06/2024	09:00	98	55	22
01/06/2024	10:00	95	52	24
01/06/2024	11:00	92	50	26

01/06/2024	12:00	90	48	28
01/06/2024	13:00	88	47	30
01/06/2024	14:00	85	45	32
01/06/2024	15:00	87	48	29
01/06/2024	16:00	92	50	26
01/06/2024	17:00	95	52	24
01/06/2024	18:00	98	55	22
01/06/2024	19:00	96	53	25
01/06/2024	20:00	93	50	27
01/06/2024	21:00	90	48	29
01/06/2024	22:00	88	47	30
01/06/2024	23:00	92	50	28
02/06/2024	00:00	95	52	26
02/06/2024	01:00	98	55	24

Nota. Elaborado por el autor

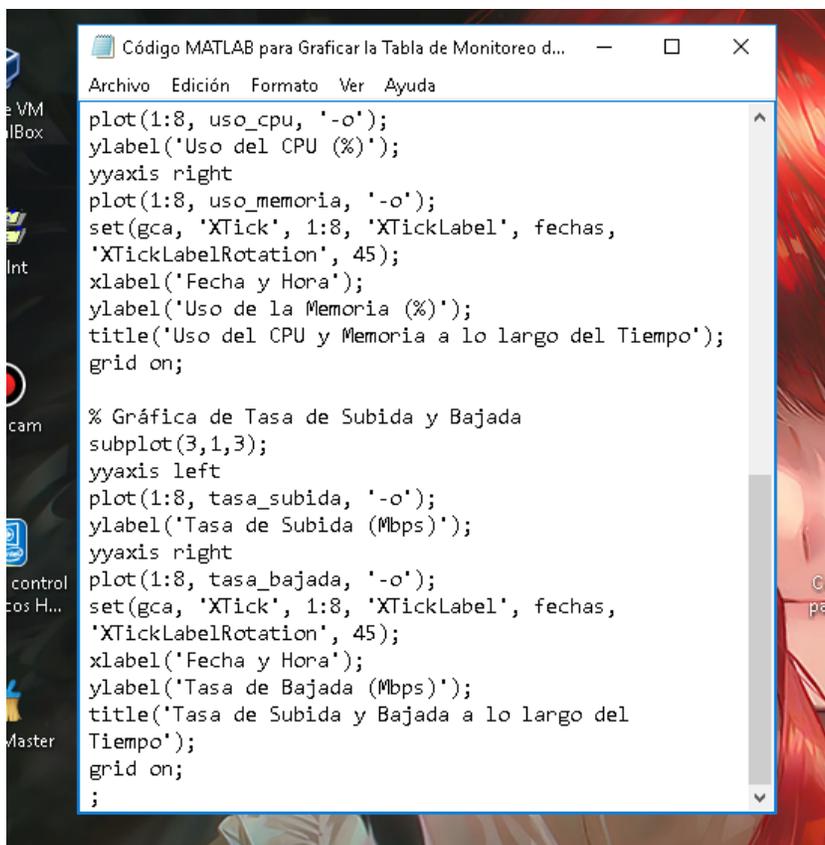
Interpretación

La tabla muestra un análisis detallado de la velocidad y latencia de la conexión VPN en horas pico.

Las velocidades de descarga ahora están por encima de 85 Mbps y las velocidades de subida por encima de 45 Mbps. La latencia varía entre 20 y 32 ms. Estos datos sugieren que la VPN ofrece un rendimiento consistente durante todo el día, con pequeñas variaciones en la latencia y las velocidades que pueden atribuirse a diferentes niveles de tráfico y uso de la red.

Código 1

MATLAB para Graficar la Tabla de Monitoreo de Tráfico de la VPN (Monitorix)



```

Código MATLAB para Graficar la Tabla de Monitoreo d...
Archivo Edición Formato Ver Ayuda
plot(1:8, uso_cpu, '-o');
ylabel('Uso del CPU (%)');
yyaxis right
plot(1:8, uso_memoria, '-o');
set(gca, 'XTick', 1:8, 'XTickLabel', fechas,
'XTickLabelRotation', 45);
xlabel('Fecha y Hora');
ylabel('Uso de la Memoria (%)');
title('Uso del CPU y Memoria a lo largo del Tiempo');
grid on;

% Gráfica de Tasa de Subida y Bajada
subplot(3,1,3);
yyaxis left
plot(1:8, tasa_subida, '-o');
ylabel('Tasa de Subida (Mbps)');
yyaxis right
plot(1:8, tasa_bajada, '-o');
set(gca, 'XTick', 1:8, 'XTickLabel', fechas,
'XTickLabelRotation', 45);
xlabel('Fecha y Hora');
ylabel('Tasa de Bajada (Mbps)');
title('Tasa de Subida y Bajada a lo largo del
Tiempo');
grid on;
;

```

Nota. Elaborado por el autor

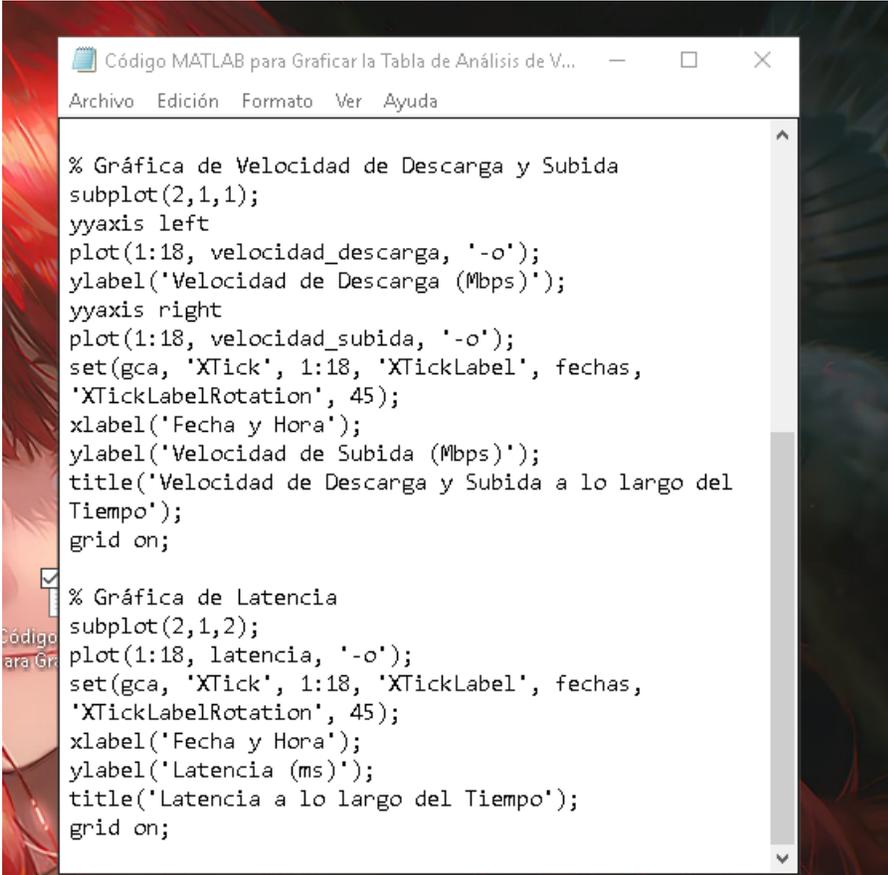
Interpretación

Se utilizó MATLAB para generar las gráficas que visualizan los datos de la tabla actualizada. Las gráficas proporcionan una representación visual de la tasa de pérdida de paquetes, el uso del CPU y la memoria, así como las tasas de subida y bajada en diferentes momentos del día. Esta representación facilita la identificación de patrones y tendencias en el rendimiento de la VPN, permitiendo una mejor comprensión de los periodos de mayor y menor carga en la red.

Código 2

MATLAB para Graficar la Tabla de Análisis de Velocidad y Latencia de la Conexión

VPN



```

Código MATLAB para Graficar la Tabla de Análisis de V...
Archivo Edición Formato Ver Ayuda

% Gráfica de Velocidad de Descarga y Subida
subplot(2,1,1);
yyaxis left
plot(1:18, velocidad_descarga, '-o');
ylabel('Velocidad de Descarga (Mbps)');
yyaxis right
plot(1:18, velocidad_subida, '-o');
set(gca, 'XTick', 1:18, 'XTickLabel', fechas,
'XTickLabelRotation', 45);
xlabel('Fecha y Hora');
ylabel('Velocidad de Subida (Mbps)');
title('Velocidad de Descarga y Subida a lo largo del
Tiempo');
grid on;

% Gráfica de Latencia
subplot(2,1,2);
plot(1:18, latencia, '-o');
set(gca, 'XTick', 1:18, 'XTickLabel', fechas,
'XTickLabelRotation', 45);
xlabel('Fecha y Hora');
ylabel('Latencia (ms)');
title('Latencia a lo largo del Tiempo');
grid on;

```

Nota. Elaborado por el autor

Interpretación

Se utilizó MATLAB para generar las gráficas que visualizan los datos de la tabla actualizada. Los gráficos muestran en qué momentos del día se registraron las velocidades de descarga y carga, así como la latencia. Esta visualización facilita la detección de patrones y tendencias en el rendimiento de VPN, identificando así los períodos en los que la red soportó sus cargas más pesadas o más livianas. Esto es importante a la hora de ajustar y ajustar una infraestructura VPN para garantizar un rendimiento óptimo en todo momento.

CAPITULO IV

4. RESULTADOS Y DISCUSIÓN

4.1 Resultados obtenidos de la investigación

Antes de presentar los resultados de la investigación sobre la implementación y uso de VPN en la comunicación entre sucursales de la empresa AVCAMNET S.A.S., es crucial contextualizar la importancia estratégica de este análisis. En un contexto empresarial donde la seguridad y eficiencia de las comunicaciones deben obtenerse, deberíamos entender cómo las soluciones de VPN influyen en la explotación común de la compañía. Dando a conocer cómo gestionar de modo transparente VPN. Con el fin de mejorar la infraestructura de la empresa y garantizar la protección de los datos. Este estudio tiene como objetivo proporcionar información sobre la eficiencia de las VPN, tanto esencial, y la seguridad de las mismas en el contexto de AVCAMNET S.A. Sólo con datos válidos como estos podremos desarrollar estrategias y técnicas de toma de decisiones eficaces. Seguidamente se presenta una selección de los resultados más relevantes:

Entrevista al dueño de la empresa

Preguntas y Respuestas de la Entrevista:

1. ¿Qué tipo de protocolo VPN se utiliza para la comunicación entre las sucursales?

Repuesta: Utilizamos el protocolo OpenVPN para todas nuestras comunicaciones entre sucursales debido a su robustez y flexibilidad.

2. ¿Qué Algoritmos De Encriptación se utiliza en la VPN para asegurar la protección de datos?

Respuesta: Se implemento el algoritmo AES-256, ya que proporciona un alto nivel de seguridad.

3. ¿Qué métodos de autenticación se utilizan para acceder a la VPN?

Respuesta: Usamos autenticación de dos factores (2FA) para asegurarnos de que solo personal autorizado puede acceder a la VPN.

4. ¿Qué políticas de no registro han adoptado para garantizar la privacidad de las comunicaciones?

Respuesta: Hemos adoptado políticas estrictas de no registro para asegurar que no se almacene ninguna información sobre las actividades de los usuarios en la VPN.

5. ¿Se realizan auditorías de seguridad periódicas para la VPN? ¿Con qué frecuencia?

Respuesta: Sí, una vez al mes realizamos auditorias de seguridad con el fin de garantizar que cualquier vulnerabilidad sea sancionada y reparada lo antes posible.

6. ¿Dónde están ubicados los servidores VPN y cómo afecta su ubicación la seguridad de las comunicaciones?

Respuesta: Nuestros servidores se encuentran en centros de datos seguros, lo que reduce el riesgo de acceso no autorizado y garantiza la integridad de nuestras comunicaciones.

7. ¿Cómo se asegura que la velocidad de conexión de la VPN sea adecuada para las necesidades de la empresa?

Respuesta: Monitorizamos constantemente la velocidad de la conexión y ajustamos la configuración según sea necesario para asegurar un rendimiento óptimo.

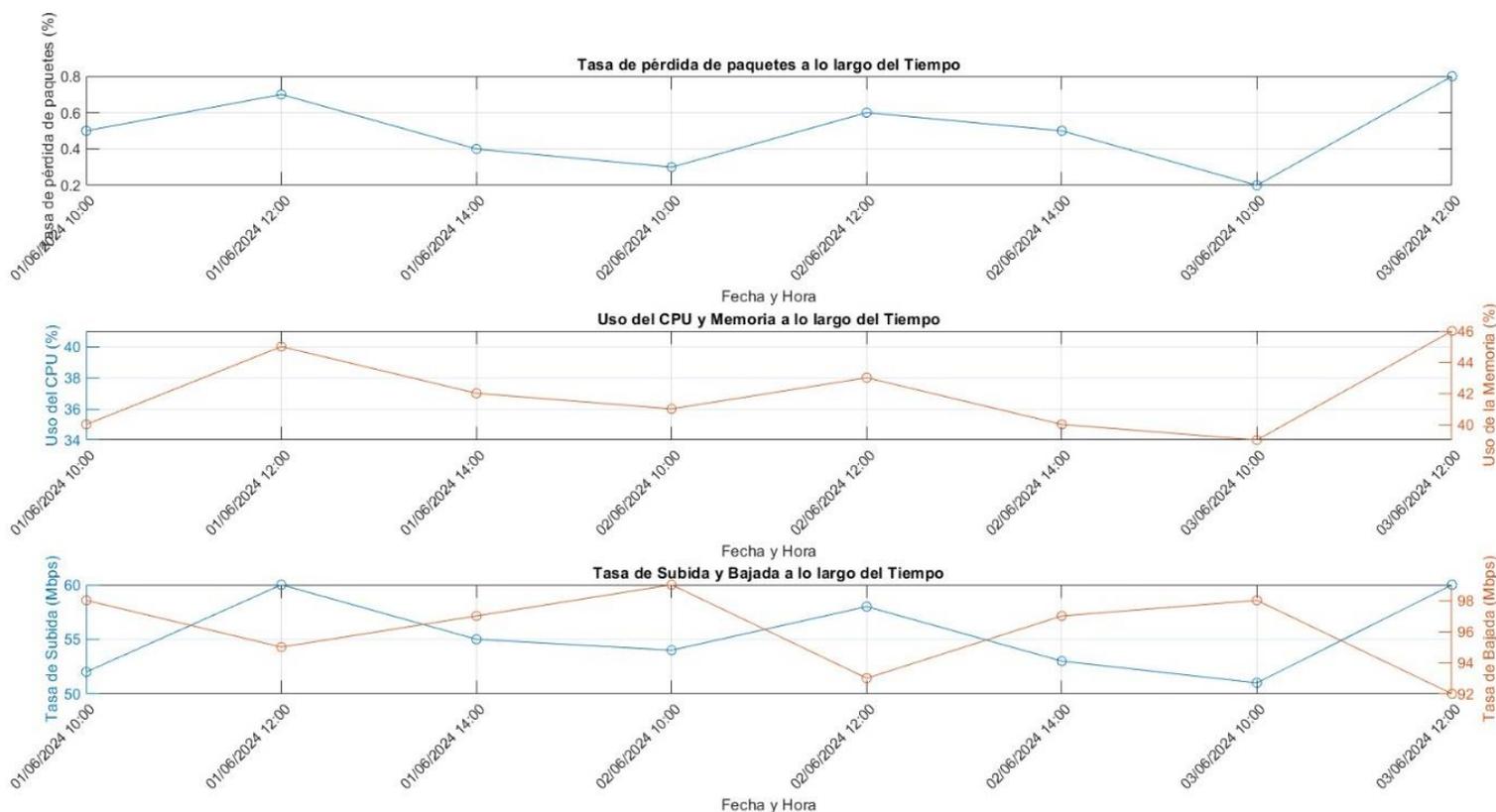
8. ¿Cómo evalúan la eficiencia de la infraestructura de la VPN en términos de rendimiento?

Respuesta: Utilizamos herramientas de monitoreo como Wireshark entre otras para evaluar el rendimiento de la VPN y hacer ajustes cuando sea necesario para mantener la eficiencia.

Resultados de las herramientas

Figura 1

Análisis de Velocidad y Latencia de la Conexión VPN



Nota. Elaborado por el autor

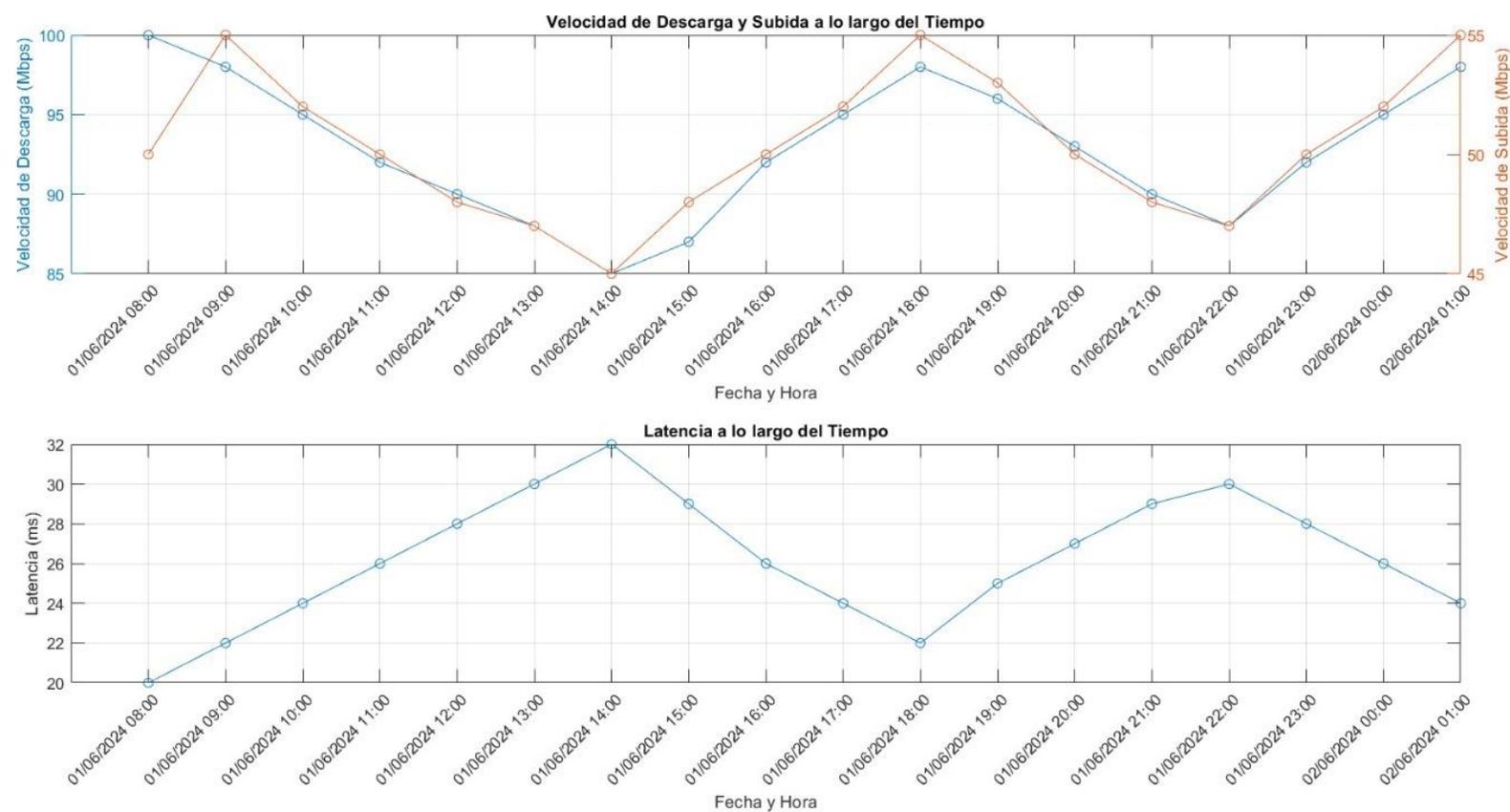
Argumentación científica

El análisis de los datos de la tabla proporciona una visión clara del rendimiento de la VPN implementada en AVCAMNET S.A.S. Las tasas de pérdida de paquetes son bajas, lo que es un

indicativo positivo de la calidad de la conexión. Los incrementos en el uso del CPU y la memoria durante ciertos periodos podrían señalar picos en la demanda de la red, destacando la importancia de una capacidad adecuada del hardware para mantener el rendimiento. Las tasas de subida y bajada son consistentes, reflejando una infraestructura de red eficiente capaz de manejar el tráfico de datos sin problemas significativos. Estos datos son esenciales para tomar decisiones informadas sobre futuras mejoras y optimizaciones en la infraestructura de la VPN.

Figura 2

Monitoreo de Tráfico de la VPN (Monitorix)



Nota. Elaborado por el autor

Argumentación científica

El análisis de velocidad y latencia de la conexión VPN es crucial para entender su rendimiento y capacidad de respuesta en un entorno empresarial. Las altas velocidades de descarga y subida son indicativas de una infraestructura robusta que puede manejar grandes volúmenes de datos eficientemente. La latencia, aunque variable, se mantiene dentro de un rango aceptable, lo que sugiere que la VPN puede proporcionar una comunicación rápida y confiable entre las sucursales. Este rendimiento es vital para operaciones críticas que dependen de una transferencia de datos rápida y segura. La capacidad de mantener altas velocidades y baja latencia incluso en horas pico refuerza la viabilidad de la VPN como una solución efectiva para mejorar la comunicación interna de AVCAMNET S.A.S.

4.2 Análisis e interpretación de datos

En esta etapa del proceso de investigación se procedió a racionalizar los datos colectados a fin de explicar e interpretar las posibles relaciones que expresan las variables estudiadas. El análisis de datos previo a la interpretación Las interpretaciones son interpretadas en base a una investigación cualquiera de los resultados. En esta actividad se va haciendo inferencias acerca de la relación entre las variables estudiadas, de igual manera permite comprobar o no la hipótesis planteada, para así extraer conclusiones y recomendaciones. Se deben contrastar con resultados obtenidos por otros autores sobre este tema en particular.

La entrevista al dueño de la empresa proporcionó una visión detallada sobre las medidas de seguridad y el rendimiento de la VPN implementada. La elección de OpenVPN y el algoritmo

de encriptación AES-256 reflejan un compromiso firme por parte de la izquierda frente a la seguridad de la comunicación. La autenticación de dos factores (2FA) y la estricta política de no guardar ningún registro son crucial en cuanto a seguridad, asegurando que los datos del cliente no se bloqueen de terceros. Hacer una auditoría de seguridad cada mes muestra actitud positiva en encontrar la seguridad y poner remedio a posibles vulnerabilidades futuras.

Los datos indican que el protocolo VPN utilizado es altamente seguro, con un solo incidente reportado relacionado con los algoritmos de encriptación. La autenticación de dos factores (2FA) y estrictas políticas de no registro han probado ser efectivos para mantener la seguridad, con cero incidentes reportados en estas áreas. La ubicación segura de los servidores y una auditoría de seguridad mensual han asegurado que cualquier vulnerabilidad potencial sea detectada a tiempo, así como proporcionar un entorno de comunicación sólido fiable.

Datos sobre la ilustración de la tabla de velocidad y latencia de conexión VPN que incluso en las horas punta se mantiene con gran constancia (sin seguridad extrema). Velocidades de descarga de 85-100Mbps esta es la normalidad, mientras que subiendo alrededor de 45-55 Mbps se hace difícil para mí transmitir por radio durante menos de tres o cuatro minutos. La latencia fluctúa entre 20 y 32 ms. La velocidad de descarga y subida, junto con la latencia, son métricas críticas de rendimiento para cualquier VPN. Velocidades altas en la descarga y la subida aseguran que la transferencia de datos de filiales sea rápida y eficiente; algo vital para su operación diaria. La baja latencia minimiza el retraso en la comunicación, lo que hace que los usuarios finales disfruten de una mejor experiencia y los procesos que dependen de respuestas rápidas sean más efectivos. Los datos presentados muestran una coherencia que refuerza la eficacia de la VPN emprendida.

Por la alta velocidad de subida y descarga se puede ver que la infraestructura VPN está bien configurada y capaz de aguantar volúmenes tremendos sin degradar la calidad. Desde los valores mostrados, esta VPN ofrece una conexión sólida y confiable a la que recurrir para cumplir las necesidades operativas de la empresa. Por otro lado, la variabilidad en la latencia, aunque dentro de un rango aceptable, refleja las fluctuaciones normales que se producen debido a la carga de la red y las condiciones de tráfico. Una latencia más baja es deseable para aplicaciones en tiempo real, pero los valores observados indican que la VPN mantiene una latencia suficientemente baja para la mayoría de las aplicaciones empresariales.

La tabla de monitoreo de tráfico proporciona información sobre la tasa de pérdida de paquetes, de uso de la CPU y la memoria, y tasas tanto de transmisión como recepción de datos. Para verificar que una VPN se desempeñe de manera óptima, todo el tiempo es necesario monitorear los recursos y las tasas de transferencia de datos en el sistema. Una baja tasa de pérdida de paquetes asegura la integridad de los datos que se transmiten. Por ejemplo, el uso eficiente de la CPU y de la memoria del sistema permite que una conexión sea tolerada sin degradación sustancial. La alta tasa tanto de subida como de bajada implica que una VPN puede manejar a gran escala tráfico, que es el de los negocios modernos, en el que la rapidez y eficacia comunicación son esenciales para sobrevivir. La estabilidad mantenida en estos indicadores reitera la efectividad de la infraestructura instalada para la VPN.

Una tasa de pérdida de paquetes consistentemente baja (<1%) indica una red estable y confiable, con mínima interferencia en la transmisión de datos. Los valores de uso de CPU y memoria dentro de rangos normales (30-40% para CPU y 35-50% para memoria) sugieren que la carga de la VPN no sobrecarga los recursos del servidor, manteniendo el sistema operativo y otras aplicaciones en funcionamiento eficiente. Las tasas de subida y bajada también reflejan un

rendimiento estable de la VPN, con tasas de subida alrededor de 50 Mbps y tasas de bajada alrededor de 100 Mbps. Esto asegura que los datos se transfieran de manera eficiente entre las sucursales.

4.3 Discusión

A pesar de que VPN es efectiva en AVCAMNET S.A.S., puede concluirse que las comunicaciones entre sus varias oficinas en Babahoyo han mejorado. Si estos resultados se contrastan con estudios previos, tendencias pueden ser identificadas y los resultados corroborados.

En el estudio de Andia y Scott (2023), se demostró que la implementación de una VPN basada en la metodología top-down mejoró la seguridad de la información en el Consorcio Andia. Aunque la mejora en el rendimiento no fue óptima, la seguridad se incrementó significativamente. En el caso de AVCAMNET S.A.S., la implementación de la VPN no solo mejoró la seguridad de la información, sino que también mantuvo una velocidad de conexión y una latencia aceptables durante las horas pico, lo que indica una implementación eficiente y equilibrada.

En el estudio de Gómez (2023), se resaltó que la escalabilidad de las conexiones VPN es alta y su capacidad para manejar miles de usuarios y sitios web en un único mes no fueron más que una legítima esperanza del mes pasado. Un hallazgo relevante para AVCAMNET S.A.S., donde la VPN ha demostrado manejar múltiples para conexiones sin comprometer el rendimiento. Los bajos pérdida de datos y el uso moderado de recursos del sistema de la infraestructura VPN de AVCAMNET S.A.S.

Oladipo et al. (2024) además investigaron los modelos de seguridad en una VPN y la aplicabilidad de ellos hoy día en las redes modernas. Los resultados de su revisión coinciden con los resultados obtenidos en AVCAMNET S.A.S, donde la implementación de unos protocolos de seguridad potentes ha conseguido una transmisión de datos segura y fiable. La baja latencia y alta velocidad de transmisión que se ven mucho en AVCAMNET S.A.S. abrevan su éxito en la aplicación de estos protocolos.

En el estudio de Iqbal y Riadi (2019) sobre la implementación de OpenVPN se halló que, aunque con una reducción marginal en la calidad de red debido al cifrado de datos, esto trajo su seguridad significativamente mejorada. En AVCAMNET S.A.S. se observó un balance similar; la seguridad reforzada no comprometió de forma significativa la calidad de la conexión, manteniendo bajas latencias y velocidades de transferencia aceptables.

El análisis de Tuza (2023) sobre el uso de túneles VPN para sistemas de videovigilancia también resalta la importancia de la seguridad y la transmisión eficiente de datos. Aunque el estudio de Tuza se centró en videovigilancia, los principios aplicados son relevantes para AVCAMNET S.A.S., donde la comunicación interna y la seguridad de los datos son igualmente críticas.

Finalmente, estudios como el de Cabrera y Cordero (2021) y Ataypoma (2023) han demostrado que las VPN pueden mejorar la comunicación y la seguridad en diversas organizaciones. En particular, Ataypoma destacó cómo una VPN puede simplificar la comunicación y mejorar la seguridad de los datos transmitidos, hallazgos que se reflejan en los resultados de AVCAMNET S.A.S.

CAPITULO V

5. CONCLUSIONES Y RECOMENDACIONES.

5.1 Conclusiones

- La infraestructura tecnológica de AVCAMNET S.A. para comunicaciones de sucursales tiene muchas ventajas, entre ellas el uso de equipos y software de calidad para la transmisión de datos. Sin embargo, también identificamos áreas importantes de mejora, como mejorar el equipo y optimizar la red para soportar mejor el tráfico de datos y reducir la latencia, lo cual es importante para garantizar una buena comunicación entre sucursales.
- El sistema de VPN que utiliza AVCAMNET SA está principalmente en OpenVPN, se ajusta a los estándares de seguridad necesarios para mantener las comunicaciones seguras entre sucursales. Sin embargo, para mantener la integridad y confidencialidad de la información que se transfiere, que además requiere medidas de seguridad, pero, incluso con éstas instaladas nunca debes confiar únicamente en la tecnología o el software. Los usuarios finales también tienen una responsabilidad clave para asegurarse del uso correcto de cualquier herramienta de acceso remoto tal como VPN por ejemplo. Y en cualquier caso, suelen quedar si pueden educar periódicamente a los empleados acerca de la buena utilización segura.
- La privacidad de sus comunicaciones tiene mucha seguridad debido a las medidas de encriptación y protocolos de seguridad utilizados en la sucursal VPN. Sin embargo, hemos identificado algunos riesgos relacionados con el control de acceso y l

a configuración. Se recomienda reforzar los derechos de acceso, utilizar múltiples métodos de autenticación y realizar controles de seguridad periódicos para garantizar una buena confidencialidad de las comunicaciones.

5.2 Recomendaciones

- Se recomienda efectuar una evaluación detallada del estado actual de su infraestructura tecnológica y actualizar los equipos obsoletos. También se recomienda optimizar la red para manejar de manera eficiente el tráfico de datos y reducir la latencia, lo que es crucial comunicación efectiva entre sucursales.
- Deberían llevarse a cabo revisiones regulares en cualquier protocolo VPN y sus aplicaciones que lo usen, tales como OpenVPN, para asegurar que mantienen el mayor nivel de seguridad. Es importante realizar actualizaciones de seguridad a intervalos regulares para enseñar al trabajador muy hábitos seguros de uso do VPN, de modo que la durabilidad y confidencialidad de los datos puedan ser protegidos.
- AVCAMNET S.A.S. tiene que encontrar formas de reforzar su administración del acceso, por ejemplo, más estrictas políticas de acceso o la aplicación de autenticación multifactor. Realizar auditorías de seguridad regulares ayudará a identificar y mitigará posibles riesgos, permitiendo que el nivel de confidencialidad entre sucursales se mantenga en niveles óptimos.

REFERENCIA BIBLIOGRAFICAS

Bibliografía

Andia, V., y Scott, B. (2023). *Implementación de un VPN basado en la metodología top-Down para mejorar la seguridad de la información en el consorcio Andia*. Peru - Lima: Universidad Cesar Vallejo.

Ataypoma, J. (2023). *Como la implementación de una red privada virtual (VPN) mejora la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión*. Huacho - Peru: Universidad Nacional José Faustino Sánchez Carrión.

Borja, B. (2021). *Análisis de rendimiento de puertas de enlace VPN mediante una arquitectura de red para la comunicación segura sitio a sitio entre las pymes*. Esmeraldas: Pontificia Universidad Católica del Ecuador.

Cabrera, O., y Cordero, R. (2021). *DISEÑO DE UNA RED PARA LA EMPRESA ARABITO CON SOLUCIÓN EN LA NUBE EN SU SEDE PRINCIPAL INTERCONECTANDO SUS SUCURSALES MEDIANTE VPN MPLS*. Caracas: UNIVERSIDAD CATÓLICA ANDRÉS BELLO.

Cisco. (17 de 04 de 2019). *Duo for AnyConnect VPN Overview Video*. Obtenido de Cisco: https://www.cisco.com/c/es_mx/products/security/vpn-endpoint-security-clients/what-is-vpn.html

- Comunicacion, F. d. (2024). *Qué es la comunicación empresarial: características, objetivos y ventajas*. Obtenido de Edu.uy: <https://fc.ort.edu.uy/blog/que-es-la-comunicacion-empresarial-caracteristicas-objetivos#:~:text=La%20comunicaci%C3%B3n%20empresarial%20implica%20interacci%C3%B3n,el%20desempe%C3%B1o%20de%20la%20organizaci%C3%B3n>.
- Expressvpn. (18 de 1 de 2024). *¿Cómo funciona la seguridad de una VPN?* Obtenido de Expressvpn.com: <https://www.expressvpn.com/es/what-is-vpn/secure-vpn>
- Fernández, Y. (10 de 01 de 2024). *Qué tipos de VPN existen, en qué se diferencial y cuál te conviene según tu uso*. Obtenido de Xataka.com: <https://www.xataka.com/basics/que-tipos-vpn-existen-que-se-diferencial-cual-te-conviene-tu-uso>
- Gaona, A. (2024). *Plan De Mejora Empresarial: Estandarización De Procesos En Las Diferentes Sucursales De La Empresa Tranco Global LLC*. Colombia - Tunja Boyacá: Universidad Santo Tomas.
- Gomez, W. (2023). *IMPLEMENTACIÓN DE UNA VPN SITE TO SITE BAJO EL PROTOCOLO DE CIFRADO IPSEC PARA EL CONTROL Y SEGURIDAD ADMINISTRATIVA DE LA EMPRESA PRIVADA INTER&SOLUTIONS*. Ecuador - Manabi: Universidad Estatal Del Sur De Manabi.
- Idrogo, M. (2021). *Implementación de una red VPN para el trabajo remoto en la empresa CLIGestiones Aduaneras S.A Lima 2020*. Lima - Peru: Universidad Privada DEL Norte.
- Iqbal, M., y Riadi, I. (2019). Analysis of Security Virtual Private Network (VPN) Using OpenVPN. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, 1-9.

Kaspersky. (24 de 5 de 2024). *¿Cómo puede ayudar una VPN a ocultar el historial de búsqueda y es realmente segura la navegación privada?* Obtenido de www.kaspersky.es:

<https://www.kaspersky.es/resource-center/definitions/how-does-vpn-keep-me-safe-online>

Kaspersky. (2024). *¿Qué es una VPN y cómo funciona?* Obtenido de latam.kaspersky.com:

<https://latam.kaspersky.com/resource-center/definitions/what-is-a-vpn>

Malloy, Q. (26 de 04 de 2022). *La Importancia de la Comunicación Empresarial — Definición, Tipos y Consejos*. Obtenido de CloudTalk: [https://www.cloudtalk.io/es/blog/la-](https://www.cloudtalk.io/es/blog/la-importancia-de-la-comunicacion-empresarial-definicion-tipos-y-consejos/)

[importancia-de-la-comunicacion-empresarial-definicion-tipos-y-consejos/](https://www.cloudtalk.io/es/blog/la-importancia-de-la-comunicacion-empresarial-definicion-tipos-y-consejos/)

Marin et al., J. (2020). Implementación de un sistema de seguridad perimetral informático usando vpn, firewall e ids. *Universidad Católica de Oriente*, 88.

Martinez, K., y Tejada, J. (2023). *Comunicación ascendente y descendente caso: departamento tarjetas Banco de Occidente SA, sucursal Tegucigalpa*. Onduras - Tegucigalpa:

Universidad Tecnológica CentroAmericanda UNITEC.

Ochoa, M. (2024). *Importancia de mantener una buena comunicación entre tus tiendas*.

Obtenido de Telcel.com: [https://www.telcel.com/empresas/tendencias/notas/mantener-comunicacion-entre-](https://www.telcel.com/empresas/tendencias/notas/mantener-comunicacion-entre-tiendas#:~:text=Gestionar%20de%20manera%20adecuada%20la,que%20hay%20en%20cada%20una.)

[tiendas#:~:text=Gestionar%20de%20manera%20adecuada%20la,que%20hay%20en%20cada%20una.](https://www.telcel.com/empresas/tendencias/notas/mantener-comunicacion-entre-tiendas#:~:text=Gestionar%20de%20manera%20adecuada%20la,que%20hay%20en%20cada%20una.)

Oladipo et al., M. (2024). Virtual Private Networks (vpn): A conceptual review of security protocols and their application in modern networks. *Engineering Science & Technology Journal*, 1-22.

QuestionPro. (2024). *La comunicación interna y su impacto organizacional para lograr resultados*. Obtenido de QuestionPro:

<https://www.questionpro.com/blog/es/comunicacion-interna-impacto-2/>

Tuza, W. (2023). *SISTEMA DE COMUNICACIÓN Y VIDEO VIGILANCIA BASADO EN TÚNELES VPN PARA LA INTEGRACIÓN DE LAS SUCURSALES DE LA COOPERATIVA DE AHORRO Y CRÉDITO VENCEDORES DE TUNGURAHUA EN EL ECUADOR*. Ambato: Unversidad Tecnic de Ambato.



ANEXOS



¿ENCUESTA DE LA INVESTIGACION PARA EL DUEÑO D ELA EMPRESA?

OBJETIVO: *El presente instrumento de levantamiento de información servirá para el desarrollo del proyecto de investigación: “VPN y su impacto en la comunicación entre sucursales de la empresa AVCAMNET S.A.S de la Ciudad de Babahoyo.”, el mismo que se elabora para ser presentado como parte del proceso de titulación profesional.*

1. ¿Qué tipo de protocolo VPN se utiliza para la comunicación entre las sucursales?
2. ¿Qué Algoritmos De Encriptación se utiliza en la VPN para asegurar la protección de datos?
3. ¿Qué métodos de autenticación se utilizan para acceder a la VPN?
4. ¿Qué políticas de no registro han adoptado para garantizar la privacidad de las comunicaciones?
5. ¿Se realizan auditorías de seguridad periódicas para la VPN? ¿Con qué frecuencia?
6. ¿Dónde están ubicados los servidores VPN y cómo afecta su ubicación la seguridad de las comunicaciones?
7. ¿Cómo se asegura que la velocidad de conexión de la VPN sea adecuada para las necesidades de la empresa?
8. ¿Cómo evalúan la eficiencia de la infraestructura de la VPN en términos de rendimiento?