UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

UNIVERSIDAD NACIONAL DEL ALTIPLANO

FACULTAD DE INGENIERÍA MECÁNICA ELÉCTRICA, ELECTRÓNICA Y SISTEMAS

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

DISEÑO DE UN RED PRIVADA (VPN) BASADO EN SOFTWARE LIBRE PARA MEJORAR LA SEGURIDAD DE LA INFORMACIÓN EN LA EMPRESA GS MAQUINARIAS Y CONSTRUCTORA E.I.R.L., JULIACA, 2023

TESIS

PRESENTADA POR:

YARMANDU KEVIN ACERO ZANABRIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE SISTEMAS

PUNO – PERÚ

2024

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

Reporte de similitud

NOMBRE DEL TRABAJO

DISEÑO DE UN RED PRIVADA (VPN) BAS ADO EN SOFTWARE LIBRE PARA MEJOR AR LA SEGURIDAD DE LA INFORMACIÓN EN LA EMPRESA GS MAQUINARIAS Y C ONSTRUCTORA E.I.R.L., JULIACA 2023

AUTOR

YARMANDU KEVIN ACERO ZANABRIA

RECUENTO DE PALABRAS

29388 Words

RECUENTO DE CARACTERES

161087 Characters

RECUENTO DE PÁGINAS

155 Pages

TAMAÑO DEL ARCHIVO

4.4MB

FECHA DE ENTREGA

Jun 6, 2024 1:40 PM GMT-5

FECHA DEL INFORME

Jun 6, 2024 1:43 PM GMT-5

● **19% de similitud general**

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base de datos.

- 15% Base de datos de Internet
- 3% Base de datos de publicaciones
- Base de datos de Crossref
- Base de datos de contenido publicado de Crossref
- 13% Base de datos de trabajos entregados

● **Excluir del Reporte de Similitud**

- Material bibliográfico
- Material citado
- Coincidencia baja (menos de 10 palabras)

Mg. Aldo H. Zanabria Galvez
INGENIERO DE SISTEMAS
CIP 84584

V°B° Guina G. Sotomayor A.

Resumen

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

DEDICATORIA

Dedico este trabajo a mi familia en especial a mi pareja que me acompaño en esta travesía Brizaida A.M.

Yarmandu Kevin Acero Zanabria

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

AGRADECIMIENTOS

Sumamente agradecido con mis docentes y mi familia por haberme apoyado incondicionalmente en este arduo camino

Yarmandu Kevin Acero Zanabria

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

ÍNDICE GENERAL

Pág.

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

Área: Nuevas Tecnologías - Informática, Educación y Sociedad

Tema: Diseño de Red VPN basado en Software Libre

FECHA DE SUSTENTACIÓN: 17 de junio del 2024

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

ÍNDICE DE TABLAS

Pág.

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

ÍNDICE DE FIGURAS

Pág.

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

ÍNDICE DE ANEXOS

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

ÍNDICE DE ACRÓNIMOS

AES: Advanced Encryption Standard

DDoS: Distributed Denial of Service

DLP: Data Loss Prevention

EPIS: Escuela Profesional de Ingeniería de Sistemas

GS: Empresa GS Constructora y Maquinarias, Juliaca

IAM: Identity and Access Management

IDS: Intrusion Detection System

IPS: Intrusion Prevention System

NAS: Network Attached Storage (Almacenamiento Conectado a la Red)

PC: Personal Computer

PKI: Public Key Infrastructure

PYMES: Pequeña y mediana empresa

SHA512: Secure Hash Algorithm of 512 bits

SGSI: Sistemas de Gestión de Seguridad de la Información

SSL: Secure Sockets Layer

TLS: Transport Layer Security

UNAP: Universidad Nacional del Altiplano

VPN: Virtual Point Network

PKCS: Public Key Cryptography Standards (Estándar de Criptografía de Clave Pública)

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

RESUMEN

En el sector de la Construcción, las empresas están interesadas en adopciones tecnológicas a fin de gestionar y salvaguardar su información sensible cuando se envía y recibe, entre las que destaca las tecnologías de Red Privada Virtual (VPN). Es por ello que el objetivo de este estudio fue diseñar una Red Privada Virtual (VPN) basado en Software Libre para la optimización de la seguridad de la información en la Empresa GS Maquinarias y Constructora E.I.R.L., Juliaca, 2023. Para analizar la situación actual de la seguridad de la información de la empresa GS, se utilizó la metodología Top-Down donde se empezó con el análisis de requerimientos según las necesidades, para luego diseñar la topología lógica y física de la red, pasando a documentar la VPN y finalmente evaluar la viabilidad del diseño desde un enfoque financiero. La VPN fue evaluada por los 14 trabajadores del proyecto Lari - Madrigal y se utilizó el instrumento "*Encuesta sobre apreciación de la seguridad de la información"* arrojando una confiabilidad de Alfa de Cronbach de 0.84 y 0.73 en Pretest y Postest. Se encontró que el diseño de la Red Privada Virtual (VPN) Master_GSVPN basado en Software Libre mejoró la seguridad de la información ya que pasó de ser evaluado de Malo-Regular a Bueno en un 93%. Asimismo, la significancia bilateral con la prueba de Wilcoxon tuvo un valor de 0.001 que es menor a 0.05 evidenciando que existe suficiente evidencia estadística para afirmar que la VPN mejoró la seguridad de la información con la incorporación de un servidor NAS que aloja la VPN. Del mismo modo la rentabilidad de la inversión resultó ser viable con un VAN de 26560, un TIR de 0.44 y periodo de recuperación de 2 meses y 4 días logrando un ahorro significativo para la empresa.

Palabras Clave: VPN, Empresas, Seguridad, Criptografía, Top-Down, Juliaca

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

ABSTRACT

In the Construction sector, companies are increasingly embracing technological advancements to manage and safeguard sensitive information during both transmission and reception. Among these technologies, Virtual Private Network (VPN) solutions play a pivotal role. Hence, the objective of this study is to design a Virtual Private Network (VPN) based on Open-Source Software to enhance information security at GS Maquinarias y Constructora E.I.R.L., Juliaca, 2023. To assess the current information security status at GS, the Top-down methodology was employed. This involved initiating the analysis of requirements based on the company's needs, followed by the design of the network's logical and physical topology. Subsequently, the VPN was documented, and its feasibility was evaluated from a financial perspective. The evaluation process involved 14 current employees at project Lari - Madrigal, utilizing the "Information Security Appreciation Survey" instrument, which yielded a Cronbach's Alpha reliability of 0.84 and 0.73 in Pretest and Posttest phases. Results indicated that the design of the Virtual Private Network (VPN) Master_GSVPN, based on Open-Source Software, significantly enhanced information security, transitioning from a rating of Poor-Regular to Good by 93%. The Wilcoxon test demonstrated a bilateral significance value of 0.001, which is less than 0.05, providing sufficient statistical evidence to assert that the VPN improved information security with the incorporation of a NAS server hosting the VPN. Furthermore, the investment's profitability proved viable, with a Net Present Value (NPV) of 26560, an Internal Rate of Return (IRR) of 0.44, and a payback period of 2 months and 4 days, leading to substantial cost savings for the company.

Keywords: VPN, Enterprises, Security, Cryptography, Top-Down, Juliaca

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

CAPÍTULO I

INTRODUCCIÓN

Internet posiblemente sea la mayor invención de la humanidad y de los avances tecnológicos más fructíferos que han traído cambios y avances sorprendentes en el mundo de la tecnología. Las redes privadas virtuales (VPN) son una de las grandes soluciones que necesitan las grandes empresas, el poder contar con una red privada que hacen la comunicación de diferentes equipos dentro de la red y remotamente de manera segura. Hoy en día, las empresas más allá de su rubro, aspiran a nuevos mercados, para lo cual se están expandiendo a nuevos lugares en diferentes regiones o incluso dentro de regiones. Es así que se creó la tecnología VPN (Virtual Point Network) que como sus siglas lo dice es la conexión virtual a un punto de forma remota que hacen posible que las empresas puedan manejar sus recursos de forma privada. Las VPN utilizan estándares como el protocolo 3DES (Triple Encryption Standard), que se ha escalado para cifrar los mensajes que se envían, y una forma de IPSec (IP Security) que transmite el tráfico a través del software. Además, proporcionan autenticación de restricción mediante una clave que verifica los datos personales del usuario presentándose como buenas soluciones de seguridad con bases criptográficas.

El presente estudio se justifica tanto en la conectividad remota que se convierte en un imperativo estratégico para GS Maquinarias y Constructora E.I.R.L. en un entorno empresarial moderno. La implementación de una red privada virtual (VPN) basada en software libre busca una gestión eficiente de datos y operaciones a distancia. La conexión remota agiliza la colaboración entre equipos dispersos geográficamente, potenciando la productividad y adaptándose a las dinámicas actuales de trabajo, donde la movilidad y la flexibilidad son fundamentales.

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

Asimismo, responde a la necesidad de evaluar la viabilidad económica de una VPN basada en software libre en comparación con alternativas como servicios en la nube o la contratación de expertos externos. La conexión a través de servicios en la nube puede implicar costos elevados y dependencias externas, mientras que la contratación de expertos para gestionar la seguridad podría generar gastos continuos. La implementación de una VPN interna presenta la oportunidad de un análisis costo-beneficio a largo plazo, considerando la inversión inicial en infraestructura.

Por otro lado, la metodología Top-Down viene siendo versátil en cada entidad el cual inicialmente rescata las necesidades para luego resolverlas mediante el diseño lógico, físico y la documentación. Es así que el presente trabajo comienza con el Capítulo I, "Introducción", contextualiza la investigación sobre el diseño de una Red Privada Virtual (VPN) para mejorar la seguridad de la información en GS Maquinarias y Constructora E.I.R.L., presentando preguntas, objetivos e hipótesis. En el Capítulo II, "Revisión Literaria", se examinan antecedentes internacionales y nacionales sobre VPN, abordando bases teóricas y estableciendo el marco conceptual. El Capítulo III, "Metodología", detalla el tipo de estudio, población, muestra, instrumento y procedimientos utilizados. El Capítulo IV, "Resultados", presenta tablas, el diseño lógico, físico y la documentación del diseño de la VPN, resuelve hipótesis mediante análisis estadísticos, compara con estudios similares, realiza un juicio crítico y aborda limitaciones e implicancias. Para finalmente plantear las conclusiones y recomendaciones correspondientes.

1.1. PLANTEAMIENTO DEL PROBLEMA

La necesidad de acceder de manera segura y confiable a recursos a través de redes privadas virtuales (VPN) ha cobrado una gran relevancia en diversos ámbitos, incluyendo el empresarial, académico y gubernamental. Sin embargo, se han identificado desafíos y

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

preocupaciones en relación con la seguridad de la información, la confiabilidad de las conexiones VPN y la escalabilidad de la infraestructura utilizada. Estos desafíos plantean interrogantes sobre cómo garantizar la protección de la información sensible, asegurar conexiones VPN confiables y escalables, y optimizar la utilización de los recursos en entornos distribuidos geográficamente como el caso del proyecto de Lari - Madrigal de la empresa GS Maquinarias y Constructora E.I.R.L., Juliaca."

La falta de investigaciones específicas en el contexto peruano que aborden los retos y oportunidades asociados al uso de VPN en entornos empresariales y de proyectos, representa una brecha en la literatura científica y práctica. Además, con la creciente necesidad de acceso remoto a recursos y la creciente preocupación por la seguridad de la información, resulta relevante investigar cómo las VPN son implementadas y utilizadas en el contexto peruano, y cómo estos factores impactan en la seguridad, confiabilidad y escalabilidad de la información en entornos distribuidos geográficamente.

Sin olvidar que los servicios gratuitos de almacenamiento en la Nube tales como Drive de Google o OneDrive de Microsoft bajo sus políticas de privacidad hacen que el usuario renuncie a información sensible como datos personales o empresariales. Los conocidos Data brokers o vendedores de información (Madela, 2017). Que cada vez estás empresas van actualizando sus políticas de privacidad. Lo que hace que una empresa privada se cuestione si los datos internos que se maneja deban mantenerse privados.

Las redes VPN son importantes en el sentido que permite la extensión de una red geográficamente lo que es relevante para las empresas privadas. Las principales características que presentan esta tecnología son: seguridad, integridad, escalabilidad y confidencialidad. Lo que permite que la red VPN permita el compartir ficheros de

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

cualquier tipo, lo que hace que todo el equipo tendría los mismos archivos en todo momento (Jimenez, 2014).

En la actualidad, las empresas privadas enfrentan constantemente desafíos en términos de seguridad, confiabilidad, escalabilidad y privacidad en sus redes privadas virtuales (VPN). La seguridad se ha vuelto una preocupación primordial debido a la creciente amenaza de ciberataques y violaciones de datos, lo que pone en riesgo la información sensible y confidencial de la empresa y sus clientes. La confiabilidad es esencial para garantizar un acceso estable y continuo a los recursos y servicios a través de la VPN, sin interrupciones ni caídas del sistema, lo que afectaría la operatividad del negocio. Por último, la escalabilidad es necesaria para adaptarse al crecimiento y expansión de la empresa, permitiendo que la VPN pueda manejar un mayor número de conexiones y usuarios, así como soportar mayores volúmenes de datos y tráfico de red.

En el contexto de "GS Maquinarias y Constructora E.I.R.L., Juliaca", es esencial que la VPN implementada cumpla con altos estándares de seguridad, confiabilidad y escalabilidad y por ende privacidad, debido a la naturaleza de su negocio y la necesidad de proteger la información confidencial de la empresa, así como garantizar un acceso seguro, confiable y privado a los recursos y servicios a través de la red. Esto asegurará la integridad y confidencialidad de los datos, así como la continuidad de las operaciones comerciales, lo que es crucial para el éxito y la competitividad en el mercado empresarial actual.

1.2. FORMULACIÓN DEL PROBLEMA

1.2.1. Problema General

- ¿El diseño de la VPN basada en software libre mejorará la seguridad de la información en la empresa GS Maquinarias y Constructora E.I.R.L.?

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

1.2.2. Problemas específicos

- ¿El análisis de los requerimientos con la metodología Top-Down permitirá identificar los riesgos a la seguridad de la información en la Empresa GS Maquinarias y Constructora E.I.R.L., Juliaca, 2023?
- ¿El diseño de la red lógica permitirá mitigar los riesgos a la seguridad de la información en la Empresa GS Maquinarias y Constructora E.I.R.L., Juliaca, 2023?
- ¿La documentación y evaluación de la VPN permitirá validar la mejora de la seguridad de la información en la Empresa GS Maquinarias y Constructora E.I.R.L., Juliaca, 2023?
- ¿El retorno de inversión de la implementación de la VPN será positivo en la Empresa GS Maquinarias y Constructora E.I.R.L., Juliaca, 2023?

1.3. JUSTIFICACIÓN DEL ESTUDIO

La seguridad en las empresas es una preocupación constante en la actualidad. Las amenazas cibernéticas acechan en cada esquina, esperando la oportunidad de infiltrarse en los sistemas y causar estragos. La confidencialidad de los datos y la integridad de la información son vitales para mantener la reputación y la continuidad del negocio. En una empresa como GS Maquinarias y Constructora E.I.R.L., Juliaca, que maneja datos sensibles y realiza transacciones comerciales a nivel nacional e internacional, la seguridad de su red privada virtual (VPN) es crucial. Este estudio es necesario para identificar y proponer mejoras en la seguridad de la VPN, con el fin de proteger la información de la empresa de posibles ataques y asegurar la confidencialidad de sus datos.

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

La confiabilidad es otro aspecto fundamental en el uso de una VPN en una empresa privada. GS Maquinarias y Constructora E.I.R.L., Juliaca, depende de su VPN para establecer conexiones seguras y confiables entre sus oficinas y sucursales en diferentes ubicaciones geográficas. Sin embargo, las interrupciones en el servicio, los tiempos de inactividad y los problemas de conectividad pueden tener un impacto significativo en la operación del negocio. Es imperativo realizar este estudio para identificar y proponer mejoras en la confiabilidad de la VPN, con el objetivo de garantizar una conexión estable y confiable que permita a la empresa llevar a cabo sus actividades sin interrupciones ni pérdidas de productividad.

La escalabilidad es otro factor crítico para una empresa en crecimiento como GS Maquinarias y Constructora E.I.R.L., Juliaca. Con la expansión del negocio y la incorporación de nuevas sucursales, se requiere una VPN que pueda adaptarse y crecer en capacidad para satisfacer las necesidades de comunicación y colaboración de la empresa. Sin una VPN escalable, la empresa podría enfrentar limitaciones en su capacidad de expansión y desarrollo. Este estudio es fundamental para identificar y proponer mejoras en la escalabilidad de la VPN, con el objetivo de asegurar que la infraestructura de red de la empresa sea capaz de soportar su crecimiento y evolución futura.

La seguridad, confiabilidad y escalabilidad son aspectos esenciales en el funcionamiento de una VPN en una empresa privada como GS Maquinarias y Constructora E.I.R.L., Juliaca. La protección de la información, la confidencialidad de los datos, la continuidad del negocio y la capacidad de expansión son elementos clave para el éxito y la competitividad de la empresa en el mercado. Por lo tanto, este estudio fue necesario para proponer mejoras en estos aspectos y asegurar que la VPN de la

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

empresa cumpla con los más altos estándares de seguridad, confiabilidad y escalabilidad, garantizando así un entorno de red seguro, confiable y escalable para el crecimiento y desarrollo del negocio.

1.3.1. Objetivo General

- Diseñar una Red Privada Virtual (VPN) basado en Software Libre, para la mejora de la seguridad de la información en la Empresa GS Maquinarias y Constructora E.I.R.L., Juliaca, 2023.

1.3.2. Objetivo Específico

- Analizar los requerimientos con la metodología Top-Down para la optimización de la seguridad de la información en la Empresa GS Maquinarias y Constructora E.I.R.L., Juliaca, 2023.
- Diseñar la Red Lógica para la optimización de la seguridad de la información en la Empresa GS Maquinarias y Constructora E.I.R.L., Juliaca, 2023.
- Documentar y evaluar la VPN para la mejora de la seguridad de la información en la Empresa GS Maquinarias y Constructora E.I.R.L., Juliaca, 2023.
- Evaluar el retorno de inversión con el uso del VAN, TIR y PCR de la implementación de la VPN en la Empresa GS Maquinarias y Constructora E.I.R.L., Juliaca, 2023.

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

1.4. HIPÓTESIS DE LA INVESTIGACIÓN

1.4.1. Hipótesis General

- El diseño de la VPN basada en software libre mejora la seguridad de la información en la empresa GS Maquinarias y Constructora E.I.R.L.

1.4.2. Hipótesis específicas

- El análisis de los requerimientos con la metodología Top-Down permite identificar los riesgos a la seguridad de la información en la Empresa GS Maquinarias y Constructora E.I.R.L., Juliaca, 2023.

- El diseño de la red lógica permite mitigar los riesgos a la seguridad de la información en la Empresa GS Maquinarias y Constructora E.I.R.L., Juliaca, 2023.

- La documentación y evaluación de la VPN permite validar la mejora de la seguridad de la información en la Empresa GS Maquinarias y Constructora E.I.R.L., Juliaca, 2023.

- El retorno de inversión de la implementación de la VPN es positivo en la Empresa GS Maquinarias y Constructora E.I.R.L., Juliaca, 2023.

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

CAPÍTULO II

REVISIÓN DE LITERATURA

2.1. ANTECEDENTES DE LA INVESTIGACIÓN

2.1.1. Antecedentes Internacionales

Marcelo (2021), en Ecuador en su estudió implementó una Red Privada Virtual (VPN) utilizando herramientas de Software Libre en la Comisión Fulbright del Ecuador, con software libre. Tuvo de muestra 1 computador y 4 laptops con los que realizado las pruebas el autor concluye que debe usarse Linux CentOS en la versión 8, y que se logró implementar satisfactoriamente la red VPN con software libre. Además, realizo las recomendaciones de implementar VPN de fácil acceso remotamente para los trabajadores, que necesariamente las instituciones deberían de adquirir un mejor plan de internet de más de 100MB simétrico, además de usar sistemas operativos Windows 8 o superiores por temas de compatibilidad y armar la red VPN con un enlace para que los trabajadores no tengan la necesidad de trabajar presencialmente.

Riascos y otros (2014), en Cali Colombia en su artículo científico titulado *"Seguridad de los sistemas de información en las Pymes de Santiago de Cali (Colombia)"* tuvieron el objetivo de evaluar el nivel de seguridad de los sistemas de información de las Pymes, para ello fueron a encuestar a diferentes empresas con preguntas de qué, cómo y cuáles son los diferentes niveles de seguridad en su institución donde labora. Estos autores obtuvieron como resultado que las Pymes en Santiago de Colombia tienen un nivel medio con un 60.75% de seguridad como mecanismo. Los autores concluyen que el nivel de seguridad en Cali va mejorando y que los trabajadores presenciaron mecanismos de seguridad como medios

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

seguros de ingreso, envío de información y autenticación con contraseñas y que están preocupados por los niveles de seguridad.

2.1.2. Antecedentes Nacionales

Casanova (2020), en su trabajo de suficiencia profesional de la Universidad Tecnológica de Lima titulado *"Diseño de una Red Privada Virtual orientado al Teletrabajo de organizaciones con escasos recursos económicos por la coyuntura del Covid-19"*, tuvo como objetivo diseñar una red privada VPN con Mikrotik RouterBOARD, donde busca optimizar el rendimiento de la infraestructura de redes física y lógica controlando bajo costo y trabajar remotamente. El autor no define la metodología y la muestra, pero logra diseñar la red VPN y concluye que el uso de las redes VPN en las organizaciones es viable en todos los niveles, no siendo ninguna limitante el tamaño o complejidad de la misma y que significa una inversión de bajo costo la implementación. El autor recomienda que las organizaciones se actualicen constantemente, que la organización pueda tener IP pública estática para las conexiones. Que los trabajadores implementen protocolos de seguridad por temas de ataques. Asimismo, menciona que a mayor cantidad de nodo cliente conectados, mayor ancho de banda para el servidor y finalmente que usar VPN como teletrabajo puede traer problemas de salud como el sedentarismo.

Carrión (2018), en su tesis doctoral intitulado *"Metodología Adaptativa basada en un modelo de seguridad informática en redes privadas virtuales para mejorar el intercambio de información académica contextualizada en entornos de conexiones públicas"*, tuvo el objetivo de garantizar el intercambio de información académica entre redes públicas y redes privadas. Uso la metodología

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

adaptativa para el diseño de modelo de seguridad informático de red privada. Su muestra es de 32 empleados de la Oficina General de Sistemas Informáticos de la Universidad Nacional Pedro Ruiz Gallo. Concluye que las organizaciones requieren medidas de seguridad respecto a su información, también por que los trabajadores no conocen muy bien sobre normas de seguridad de información y que no son capacitados en el tema. Asimismo, menciona que el modelo de seguridad ha sido parcialmente implementado a nivel inicial. Recomienda que la aplicación de metodologías en materia de seguridad entre sedes principales y sucursales de una institución.

Garcia (2021), en su tesis de grado de la UTP denominado *"Implementación de una VPN tipo cliente para una entidad financiera"*, tuvo el objetivo de brindar servicio de VPN de tipo cliente para una entidad financiera. Uso la metodología de 3 fases, como Mapeo de procesos AS-IS, TO-BE, Diagrama de bloques. La muestra se comprende con los equipos de la entidad financiera. Concluye que se logró brindar continuidad de las labores de los trabajadores de la entidad financiera, también que se logró elevar las medidas de seguridad Host Information Profiles de Palo Alto (HIP) y habilitación del MFA con Azure y en el caso de elevarse los trabajadores a más de 1024 conexiones usar el Firewall pasivo a activo para que soporte 1843 conexiones simultaneas. El autor recomienda buenas prácticas en temas de seguridad con el teletrabajo.

Torres & Espinoza (2019), de la Universidad Peruana de Ciencias e Informática, en su tesis de grado titulado *"Propuesta de un Sistema de Gestión de Seguridad de la Información para una Empresa de Consultoría Financiera en Lima, 2021, Según la Norma ISO/IEC 27001:2013",* tuvieron como objetivo

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

proponer un Sistema de gestión de Seguridad de la Información, para ello tuvo como muestra a 18 trabajadores de la consultora financiera. Uso el enfoque cuantitativo, de diseño descriptivo. Creó un instrumento denominado *"*Propuesta de un sistema de gestión de seguridad de la información para una empresa de consultoría financiera en Lima, 2021, según la norma ISO/IEC 27001:2013*",* la cual sometió a prueba de expertos consiguiendo un valor de alfa de Cronbach de 0.85. El autor concluye que se logró efectuar un inventario de los eventos de violaciones a la ciberseguridad, un diagrama de Pareto con la frecuencia de estos eventos y un diagrama de Ishikawa con las principales causa-raíz identificadas, lográndose identificar los diferentes tipos de eventos ocurridos, tales como hackeo de identidad, robo de información, infección con código malicioso, infección con malware, acceso indebido a sistemas, acceso indebido a información y detección de exploits. Finalmente recomienda que las entidades deben actualizarse en nuevas tecnologías mejorando la cultura de seguridad presencial y remota, asimismo el uso de servicios Cloud y Firewalls y antivirus robustos.

Lazarte (2022), en su tesis de grado titulado *"Diseño de una red privada virtual (VPN) basada en software libre para la mejora de la seguridad de la información de la jurisdicción de la dirección de redes integradas de salud Lima Centro"*, tuvo el objetivo de determinar la influencia del Diseño de una Red Privada Virtual (VPN) Bajo Software Libre para la optimización de la seguridad de la información entre los establecimientos de la Dirección de Redes Integradas de Salud Lima Centro. Su muestra estuvo constituida por 10 personas trabajadores que ayudan con la opinión en las encuestas. El autor concluye que la implementación de la VPN mejoro significativamente dando seguridad, confiabilidad y escalabilidad al poder lograr correctas conexiones VPN usando

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

llaves con certificación RSA de 1024 bits, lo que deniega ataques malintencionados. La escalabilidad de la VPN está basada en algoritmos lo que permite el dinamismo en la cantidad de conexiones al servidor central. Recomienda que las entidades deben implementar túneles de acceso a recursos, del mismo modo que se capacite al personal para que adopte mejores comportamientos en mejora de la seguridad de la información.

De la Cruz & Vera (2019), en su tesis de grado que lleva de título *"Implementación de una VPN con open source para la gestión de aplicaciones de intranet en la Universidad Nacional Pedro Ruiz Gallo"*, tuvieron el objetivo de mejorar la gestión de aplicaciones a nivel de intranet usando tecnologías VPN de código abierto en la universidad. La muestra estuvo conformada por los trabajadores administrativos que trabajan en la Universidad Pedro Ruiz Gallo. Uso la metodología Top-Down Network Design que propone 4 fases: identificación de necesidades, Diseño Lógico, Diseño Físico, Fase de Prueba, implementación y Documentación. Los autores concluyen que los requerimientos e implementación de la VPN es viable y de bajos costos como lo quiere la Universidad, que la implementación de la VPN respeta el VAN, TIR, PR, que son indicadores de retorno de inversión. Además, que se logró diseñar por completo la red VPN. Los autores recomiendan usar la función DNS de softether.net, asimismo, de que se le haga capacitación a los trabajadores por más mínima que esta sea. También de usar Softether VPN Server Manager como herramienta visual de conexiones VPN para clientes, en este caso los trabajadores.

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

2.1.3. Antecedentes Locales

Montes de Oca & Ramos (2021), en su trabajo de investigación que lleva de título *"La Metodología Top-Down En La Optimización Del Servicio De Internet En Educación Continua De La Universidad Nacional Del Altiplano 2019"*, tuvieron el objetivo de optimizar el servicio de internet en las instalaciones de Educación Continua de la Universidad Nacional del Altiplano, Puno usando la metodología de Top-Down con el uso de herramientas Mikrotik basados en el protocolo VRRP. Con una muestra de 63 trabajadores sometidos a evaluación de las encuestas y bajo un diseño cuasi experimental es que los autores lograron demostrar que la disponibilidad y el ancho de banda obtuvo una mejora significativa bajo una prueba estadística paramétrica de t-student con p-valor de 0.002. Asimismo, aumentó la disponibilidad del servicio en el 99.94% del tiempo y aumentando el ancho de banda pasando de 469 Mbps a 480 Mbps. Esto se logró rediseñando la topología de la red, entrelazando Switches y colocando 2 router centrales manifestando que si uno se caía el otro router tomaba su lugar y así se evitaba la caída de la red.

2.2. MARCO TEÓRICO

2.2.1. Red Privada Virtual (VPN)

2.2.1.1. Concepto y características

El concepto de una Red Privada Virtual (VPN) se refiere a una solución que permite a las empresas extender de manera segura su intranet privada utilizando la infraestructura de una red pública, como Internet. Se describe que una VPN proporciona características de seguridad esenciales, como autenticación y privacidad de datos como menciona la (IBM, 2010).

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

Las VPN son tecnologías que permite extender una red local sobre una red pública, como Internet. El proceso se lleva a cabo mediante el encapsulamiento de los paquetes de datos que circulan por la red pública y, en caso de ser necesario, mediante la encriptación de esos paquetes para garantizar la privacidad de la información transmitida.

2.2.1.2. Tipos de VPN

- **VPN de acceso remoto:** que se utiliza para permitir que un ordenador cliente remoto acceda a una red local, otorgándole al cliente remoto la mayoría de los privilegios que tendría si estuviera físicamente dentro de la red local como se ve en la Figura 1. Para lograr esto, se asigna al cliente una dirección IP perteneciente a la red local a través de la VPN (Bonet, 2004).

Figura 1

VPN de Acceso remoto

Nota**:** (Bonet, 2004).

- **La VPN punto a punto:** se establece entre dos ordenadores, permitiendo el acceso entre las redes locales (LAN) de dichos ordenadores. Su principal uso radica en la interconexión de distintas sedes de empresas, posibilitando el intercambio de información de manera segura y eficiente entre las LAN

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

correspondientes (Bonet, 2004). A diferencia de las redes punto a punto tradicionales, que pueden resultar costosas desde el punto de vista económico, las VPN punto a punto brindan una alternativa más económica para establecer conexiones privadas entre redes locales geográficamente separadas, en tanto que la VPN se comporta como un puente, como se muestra en la Figura 2.

Figura 2

VPN Punto a punto

Nota: (Bonet, 2004).

- **VPN interna:** Este tipo de VPN utiliza la red local del edificio donde se encuentra en lugar de Internet como medio de acceso. Esto aumenta el nivel de seguridad, ya que no depende de una red WiFi y se aprovechan las cualidades de una VPN tradicional (Álvarez et al., 2014).

- **VPN basada en firewall:** En este tipo de VPN, se aprovechan los mecanismos de seguridad del servidor de seguridad o firewall. Se restringe el acceso a la red interna, se realiza la traducción de direcciones y se cumplen los requisitos de autenticación. Los firewalls comerciales también optimizan el sistema operativo al

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

eliminar servicios innecesarios o peligrosos, lo que proporciona seguridad adicional para la VPN. Sin embargo, la desventaja es la optimización eficiente del rendimiento sin afectar las aplicaciones del sistema operativo (Pomar, 2019).

- **VPN basada en software:** Las VPN basadas en software son ideales cuando los extremos de la VPN no son controlados por la misma organización o cuando se implementan diferentes firewalls y enrutadores. Estas VPN independientes ofrecen mayor flexibilidad en la gestión del tráfico de red. Los productos basados en software permiten que el tráfico de túnel dependa de la dirección o protocolo, a diferencia de los productos basados en hardware que encapsulan el tráfico sin importar el protocolo. Sin embargo, el manejo del software puede ser más complicado que el cifrado de los enrutadores, ya que requiere familiaridad con el sistema operativo del host, la solicitud en sí y los mecanismos de seguridad adecuados. Algunos paquetes de software de VPN también pueden requerir cambios en las tablas de enrutamiento y sistemas de direccionamiento de red (Pomar, 2019).

2.2.1.3. Protocolos VPN

Existen varios protocolos utilizados en las VPN para asegurar la comunicación y el transporte de datos. Para Amaya (2018) y UPM (2017), los protocolos son:

- **SSTP (Secure Socket Tunneling Protocol):** Utiliza el puerto TCP 443 y proporciona una conexión segura a través de un túnel.

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

- **L2TP** (Layer 2 Tunneling Protocol) sobre IPSec (Internet Protocol Security):

- **Puerto UDP 500:** Utilizado por IKE (Internet Key Exchange) para el intercambio de claves de seguridad.

- **Puerto UDP 4500:** Utilizado por IPSec NAT-T (IPsec NAT Traversal) para permitir la transmisión de paquetes IPSec a través de dispositivos de traducción de direcciones de red.

- **OpenVPN:** Utiliza los puertos mayormente por UDP y también por TCP, en el puerto 1194 y es un protocolo de código abierto que brinda una conexión segura y confiable.

- **SSL-VPN:** Utiliza el puerto TCP 443 y se basa en el protocolo SSL (Secure Sockets Layer) o su sucesor TLS (Transport Layer Security). Proporciona un acceso remoto seguro a través de un navegador web sin necesidad de instalar software adicional.

Como dice Amaya (2018), estos protocolos permiten la compatibilidad con diversos sistemas operativos, como Windows, Linux, MacOS y Android, sin requerir la instalación de clientes específicos de VPN. Además, existen otros protocolos y tecnologías utilizados en las VPN, como IPSec, GRE, L2TPv3, Draft Martini pseudowires, IEEE 802.1Q tunneling (Q-en-Q) y MPLS.

2.2.1.4. Criptografía

La criptografía ha existido desde tiempos remotos donde emperadores querían un mensaje, esta tenía que estar cifrada y se

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

desencriptaba con una llave que pudiera darle contexto al mensaje. Podemos mencionar el Cifrado César o cifrado por desplazamiento que mueve cada letra un determinado número de espacios en el alfabeto. En este ejemplo se suma 5 posiciones a cada letra, donde (Carrión, 2020).

Mensaje Original: CRIPTOGRAFIA ES SEGURIDAD

Mensaje cifrado: HWNUYTLWFKNF JX XJLZWNIFI

Para Río (2021), en su libro *"Introducción a la Criptografía"* menciona que la criptografía es una ciencia que se encarga de representar información de manera opaca con el objetivo de que solo los agentes autorizados puedan revelar el mensaje oculto. El proceso de ocultar la información se conoce como cifrado o encriptado, mientras que el proceso de revelarla se denomina descifrado o desencriptado. El concepto de criptosistema modela estos procesos de cifrado y descifrado.

Figura 3

Criptografía de Cesar

Nota: (O. Carrión, 2020).

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

Un criptosistema simétrico, también conocido como de clave privada, está compuesto por un conjunto K, donde los elementos son las claves, y una regla que asocia dos aplicaciones a cada clave k ∈ K:

$$ck: Mk \rightarrow Ck$$

$$dk: Ck \rightarrow Mk$$

Estas aplicaciones tienen la propiedad de que al aplicar la función de descifrado (dk) sobre el resultado del cifrado (ck) de un mensaje x ∈ Mk, se obtiene nuevamente el mensaje original:

$$dk(ck(x)) = x, para\ todo\ x \in Mk$$

En una VPN, la criptografía se utiliza para cifrar los datos que se transmiten entre dos puntos de la red, como un dispositivo cliente y un servidor VPN. El cifrado convierte los datos en un formato ilegible llamado texto cifrado, de modo que, si alguien intercepta los datos en tránsito, no podrá entender su contenido sin la clave de cifrado adecuada. Existen diferentes protocolos y algoritmos criptográficos que se utilizan en las VPN para garantizar la confidencialidad, la integridad y la autenticación de los datos. En el estudio de Tomás (2008) los protocolos criptográficos comunes utilizados en las VPN son:

- **IPSec (Protocolo de seguridad de IP):** Es un conjunto de protocolos que se utiliza para asegurar las comunicaciones IP en una red. IPSec puede operar en dos modos principales: modo túnel y modo transporte. Proporciona autenticación, integridad y confidencialidad de los datos a través de algoritmos criptográficos

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

como AES (Estándar de cifrado avanzado) y 3DES (Triple Data Encryption Standard) (Tomás, 2008).

- **SSL/TLS (Capa de sockets seguros/Protocolo de seguridad de transporte):** Estos protocolos se utilizan comúnmente para establecer conexiones seguras a través de Internet. SSL y su sucesor TLS utilizan certificados digitales para autenticar los servidores y cifrar la comunicación entre el cliente y el servidor utilizando algoritmos como RSA (Rivest-Shamir-Adleman) y AES (Marchand & Rueda, 2020).

- **OpenVPN:** Es un protocolo de VPN de código abierto que utiliza una combinación de tecnologías, incluyendo el protocolo SSL/TLS para la autenticación y el cifrado de los datos. OpenVPN ofrece flexibilidad y es ampliamente compatible con diferentes sistemas operativos (Tomás, 2008).

Estos protocolos criptográficos aseguran que los datos transmitidos a través de una VPN estén protegidos contra posibles amenazas, como la interceptación, la manipulación o el acceso no autorizado. Al utilizar algoritmos criptográficos robustos y claves de cifrado seguras, las VPN garantizan la confidencialidad y la integridad de los datos, protegiendo así la privacidad de los usuarios y la seguridad de la información transmitida.

2.2.1.5. Certificación de seguridad

Los certificados de seguridad juegan un papel fundamental en las redes privadas virtuales (VPN), al garantizar la autenticación y el establecimiento de conexiones seguras mediante el uso de criptografía

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

asimétrica y la infraestructura de clave pública (PKI) (Rifá, 2013). En el contexto de las VPN, se emplean diferentes tipos de certificados, entre los cuales destacan:

- **Certificados X.509:** Estos certificados siguen el estándar X.509, que define el formato de los certificados digitales utilizados en la PKI. Los certificados X.509 contienen información como el nombre del titular, la clave pública, la entidad emisora y el período de validez. Estos certificados se utilizan para la autenticación y el cifrado de datos en la VPN (Rifá, 2013).

- **Certificados SSL/TLS:** Los certificados SSL/TLS se utilizan para asegurar las conexiones VPN mediante el protocolo SSL/TLS. Estos certificados son emitidos por una autoridad de certificación y garantizan la autenticidad del servidor y opcionalmente del cliente. Los certificados SSL/TLS son ampliamente utilizados para establecer conexiones seguras en Internet y son compatibles con numerosos dispositivos y aplicaciones según The Open Web Application Security Project (OWASP, 2015).

- **Certificados PGP (Pretty Good Privacy):** Los certificados PGP se basan en el estándar PGP, que utiliza criptografía de clave pública para garantizar la confidencialidad y la autenticidad de los datos en la VPN. Estos certificados se utilizan principalmente en entornos de correo electrónico seguro, pero también pueden aplicarse en el contexto de las VPN (Cisco, 2018).

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

- **Certificados IPSec:** En las VPN basadas en el protocolo IPSec, se utilizan certificados para el intercambio de claves y la autenticación de los participantes. Los certificados IPSec son fundamentales para garantizar la seguridad de las conexiones VPN y asegurar que solo los usuarios autorizados puedan acceder a la red (Centro Criptológico Nacional, 2018).

La gestión adecuada de los certificados implica la emisión, renovación y revocación de los mismos. Esto se lleva a cabo mediante la utilización de una autoridad de certificación confiable, que emite y firma los certificados, y una infraestructura de gestión de claves que garantiza la seguridad de las claves privadas asociadas a los certificados.

2.2.1.6. Tipos de VPN basadas en Software Libre

Según Guerreo (2009), el software libre también ha tenido presencia respecto a las VPN, en la actualidad una gran variedad de servicios gratuitos se vienen creando. Con estas licencias GNU permiten a los usuarios disfrutar de las siguientes libertades como:

- **Libertad de uso:** Los usuarios son libres de utilizar el software con cualquier propósito.

- **Libertad de acceso al código fuente**: Los usuarios tienen acceso al código fuente del software, lo que les permite estudiar cómo funciona, realizar modificaciones y adaptarlo a sus necesidades.

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

- **Libertad de modificar el software:** Los usuarios tienen la libertad de realizar cambios en el código fuente del software y adaptarlo según sus requisitos o preferencias.

- **Libertad de distribuir cambios:** Si los usuarios realizan modificaciones en el software, tienen la libertad de distribuir esas versiones modificadas a otros usuarios. También pueden distribuir el software sin realizar modificaciones.

Entre los principales VPN de software libre encontramos: OpenConnect, ProtonVPN, SoftEther VPN, OpenVPN, OpenSwan, StrongSwan, TincVPN, entre muchas más.

2.2.1.7. OpenVPN

OpenVPN es una aplicación de código abierto (con licencia GPL) utilizada para implementar redes privadas virtuales. Fue desarrollado inicialmente por James Yonan en 2002 y actualmente es respaldado por (OpenVPN Technologies Inc., 2023). Una de las fortalezas de OpenVPN radica en su robusta seguridad, ya que se basa en el protocolo SSL/TLS. Aunque no es tan ampliamente conocido y utilizado como otras soluciones, es considerado sencillo, potente y seguro.

OpenVPN está disponible para una variedad de sistemas operativos, como MS Windows, Linux, MacOS, xBSD, Solaris, Android e iOS. Una característica interesante de OpenVPN es su capacidad para multiplexar todos los puertos en uno solo, por defecto utiliza el puerto 1194 tanto para el protocolo UDP como para el TCP. Esto facilita su integración con dispositivos de red como routers y firewalls que realizan

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

el enrutamiento y filtrado de paquetes (OpenVPN Technologies Inc., 2023).

En cuanto a su arquitectura, OpenVPN sigue un modelo cliente-servidor y permite el uso de direcciones IP dinámicas en ambos extremos de la conexión, lo que mantiene la sesión activa. Además, opera en el espacio de usuario, lo que significa que no requiere privilegios de administrador para su ejecución. OpenVPN también tiene la capacidad de soportar tarjetas inteligentes PKCS#11, que son similares a los DNIe (Documento Nacional de Identidad electrónico). Esto permite una autenticación segura utilizando certificados almacenados en estas tarjetas (Departamento de Sistemas Telemáticos y Computación, 2014).

Para iniciar el demonio del servicio se ejecuta en la terminal:

```
openvpn start
```

Para detener el demonio del servicio se ejecuta en la terminal:

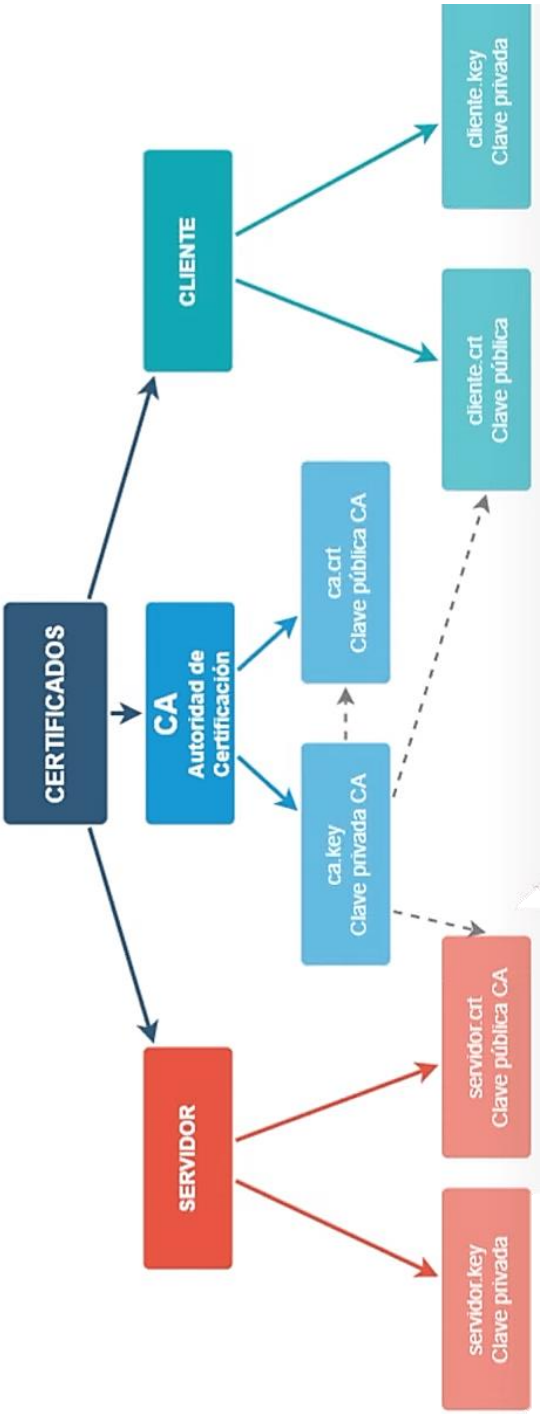
```
openvpn stop
```


repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

Figura 4

Infraestructura de certificación de OpenVPN: Claves Públicas y Privadas



Nota: (RedesPlus, 2022).

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

2.2.1.8. Ventajas y desventajas de las VPN

Tenemos las siguientes ventajas y desventajas según (Cornejo et al., 2019).

- **Ventajas:** Una de las principales ventajas de utilizar una VPN es que permite a los usuarios acceder a una red privada con todas las características y funcionalidades de dicha red. Al conectarse a través de una VPN, el cliente adquiere plenamente la condición de miembro de la red privada, lo que significa que se aplican todas las directrices de seguridad y se otorgan los permisos correspondientes. Esto permite acceder a recursos y servicios específicos de la red privada, como bases de datos y documentos internos, incluso desde una conexión pública a Internet. Además, todas las conexiones a Internet realizadas desde el cliente VPN se enrutan a través de los recursos y conexiones de la red privada, brindando un mayor nivel de seguridad.

  La compañía CISCO (2015), menciona las siguientes ventajas:

  - **Protección de datos y recursos confidenciales:** Una conexión VPN ayuda a proteger la información transmitida a través de la red y asegura la confidencialidad de los recursos utilizados.

  - **Acceso remoto conveniente y seguro:** Permite a los trabajadores remotos o empleados acceder a la red corporativa desde cualquier ubicación, manteniendo la seguridad de la red y sus recursos.

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

- **Mayor seguridad en las comunicaciones:** La comunicación a través de una conexión VPN ofrece un nivel avanzado de seguridad en comparación con otros métodos de comunicación remota, protegiendo la red privada contra accesos no autorizados.

- **Privacidad y protección de ubicación:** Los usuarios de VPN pueden ocultar su ubicación geográfica real y protegerse de exposiciones no deseadas en redes compartidas o públicas, como Internet.

- **Escalabilidad y facilidad de agregar usuarios:** Las VPN son altamente ajustables, lo que facilita la incorporación de nuevos usuarios o grupos de usuarios a la red sin necesidad de componentes adicionales o configuraciones complicadas.

- **Desventajas:** Entre las desventajas de las VPN, se puede mencionar una mayor carga en el cliente VPN debido a la necesidad de encapsular los paquetes de datos adicionales. Esta sobrecarga se incrementa aún más cuando se realiza encriptación de datos, lo que puede ralentizar la mayoría de las conexiones. También puede haber una mayor complejidad en el tráfico de datos, lo que puede generar efectos no deseados, como cambios en la numeración asignada al cliente VPN y requerir modificaciones en la configuración de aplicaciones o programas, como proxies, servidores de correo y permisos basados en nombre y número IP.

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

Estos aspectos adicionales pueden implicar una mayor complejidad en la configuración y gestión de la VPN.

Asimismo, existen riegos como lo sugiere (CISCO, 2015):

- **Riesgo de seguridad por mala configuración:** Debido a la complejidad del diseño e implementación de una VPN, es crucial confiar en profesionales con experiencia para configurar la conexión y garantizar que la seguridad de la red privada no se vea comprometida.

- **Confiabilidad y tiempo de inactividad:** La conexión VPN depende de la conexión a Internet, por lo que es importante elegir un proveedor confiable que ofrezca un excelente servicio de Internet y garantice un tiempo de inactividad mínimo o nulo.

- **Escalabilidad y problemas técnicos:** Al agregar nueva infraestructura o realizar nuevas configuraciones, pueden surgir problemas técnicos debido a incompatibilidades, especialmente si implica diferentes productos o proveedores distintos a los ya utilizados.

- **Problemas de seguridad en dispositivos móviles:** Al usar dispositivos móviles para iniciar la conexión VPN, pueden surgir problemas de seguridad, especialmente cuando se utiliza una conexión de red inalámbrica. Algunos proveedores no verificados, como los "proveedores de VPN

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

gratuitos", pueden incluso instalar malware en el dispositivo. Se deben tomar medidas adicionales de seguridad al usar dispositivos móviles para prevenir estos problemas.

- **Velocidades de conexión lentas:** Si se utiliza un cliente VPN que ofrece un servicio gratuito, es posible que se experimenten velocidades de conexión más lentas, ya que estos proveedores no priorizan la velocidad de la conexión.

2.2.2. Seguridad de la Información

Los Hackers son creativos y siempre encuentran nuevas formas de penetrar en la seguridad de las empresas, Por ello, para estar un paso más delante de los atacantes, siempre se necesita nuevas ideas como menciona una empresa de seguridad de Alemania (KALWEIT ITS, 2022).

Según la Universidad Nacional de Córdoba (2015), menciona que la seguridad de la información es un concepto fundamental en el ámbito de las tecnologías de la información. Se busca preservar y proteger la información de acuerdo con diversas características claves como:

- **La confidencialidad:** que es esencial para garantizar que solo las personas autorizadas puedan acceder a la información. Esto implica que la información se mantenga oculta y solo sea accesible para aquellos que tienen los permisos adecuados.

- **La integridad de la información:** se refiere a la protección de su exactitud y totalidad. Es vital asegurar que la información no sea

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

alterada de manera no autorizada y que los métodos de procesamiento utilizados sean seguros y confiables.

- **La disponibilidad**: que es otro aspecto crucial de la seguridad de la información. Se busca asegurar que los usuarios autorizados puedan acceder a la información y a los recursos relacionados en el momento en que lo necesiten. Esto implica la implementación de medidas para evitar interrupciones o denegaciones de servicio.

- **La autenticidad:** que se refiere a garantizar la validez de la información en términos de su origen, tiempo y distribución. Se busca evitar la suplantación de identidades y validar la autenticidad del emisor.

- **La auditabilidad:** es otro concepto importante, que implica el registro y seguimiento de todos los eventos y acciones dentro de un sistema. Esto permite un control posterior y la capacidad de rastrear y analizar actividades en busca de posibles vulnerabilidades o anomalías.

- **La protección a la duplicación:** que es importante para evitar que una transacción se realice más de una vez, a menos que se especifique lo contrario. Se busca prevenir la grabación y reproducción de transacciones para simular múltiples peticiones, lo que podría llevar a problemas de integridad o disponibilidad.

- **El no repudio:** que es un aspecto clave para evitar que una entidad niegue haber enviado o recibido información. Se implementan

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

medidas técnicas y legales para asegurar que las partes involucradas no puedan refutar su participación en las transacciones.

- **La legalidad:** que se refiere al cumplimiento de las leyes, normas, reglamentaciones y disposiciones a las que está sujeta una organización. La seguridad de la información debe estar alineada con los marcos legales y reglamentarios aplicables para garantizar su validez y cumplimiento.

2.2.2.1. Importancia de la seguridad en las organizaciones

Las organizaciones como piezas en la economía de los países han demostrado evolucionar más rápido apoyándose de la tecnología. Por lo que estar a la vanguardia les ha permitido tener ingresos y permanecer en los mercados. Se apoya principalmente en estructuras complejas de datos, esto para que se tenga conocimiento en todo tiempo de cómo fluyen los datos.

Para Martínez (2015), el nivel de seguridad en las organizaciones normalmente varía en cuanto al tamaño de la organización en cuestión. Asimismo, habla de la seguridad de la información en pequeñas y medianas empresas haciendo referencia al uso de (SGSI) Sistemas de gestión de seguridad de la información, donde indica que las pequeñas y medianas empresas están expuestas a ataques, por lo que necesariamente deben usar algún sistema de gestión de seguridad. Además, que menciona que se debería usar el ISO 27001:2013 para que la mayoría de errores y fallos de seguridad sean evitadas. Porque parte desde una posición donde menciona que los errores humanos que conllevan al riesgo de la seguridad

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

pueden ser evitadas siguiendo normas de seguridad. Del mismo modo indica que implementar estos estándares de calidad conllevan cierto nivel de gasto para las PYMES.

En el ámbito de las grandes empresas, la seguridad de la información se convierte en una prioridad estratégica debido a la magnitud de los datos y la complejidad de las operaciones. Estas organizaciones suelen implementar una variedad de medidas y prácticas avanzadas para proteger su información y datos sensibles como:

- **Infraestructura de seguridad de red avanzada:** Las grandes empresas suelen implementar una infraestructura de seguridad de red sólida y sofisticada. Esto puede incluir firewalls de próxima generación, sistemas de prevención de intrusiones (IPS), sistemas de detección y respuesta (IDS/IDR), sistemas de prevención de pérdida de datos (DLP) y soluciones de seguridad perimetral. Estas tecnologías ayudan a proteger la red empresarial de amenazas internas y externas, así como a detectar y responder rápidamente a incidentes de seguridad (Villanova, 2023).

- **Gestión centralizada de identidad y acceso:** Las grandes empresas suelen implementar sistemas de gestión centralizada de identidad y acceso (IAM) para garantizar un control adecuado sobre quién tiene acceso a los sistemas y datos. Estas soluciones permiten la administración eficiente de cuentas de usuario, privilegios y autenticación, así como la implementación de políticas de acceso basadas en roles (ManageEngine, 2022).

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

- **Sistemas de cifrado avanzados:** Para proteger los datos sensibles almacenados y transmitidos, las grandes empresas hacen uso de algoritmos de cifrado avanzados. Estos algoritmos, como AES (Advanced Encryption Standard), garantizan que los datos estén protegidos incluso si son interceptados o comprometidos (Montoya Benitez & Ospina, 2020).

- **Monitorización y análisis de seguridad en tiempo real:** Las grandes empresas implementan sistemas de monitorización y análisis de seguridad en tiempo real para detectar y responder a incidentes de seguridad de manera proactiva. Estas soluciones recopilan y analizan datos de múltiples fuentes, como registros de eventos, sistemas de detección de intrusiones y sistemas de gestión de registros, para identificar patrones sospechosos o actividades anómalas (Nebot, 2023).

- **Programas de concienciación y formación en seguridad:** Las grandes empresas reconocen la importancia de la concienciación y formación en seguridad para sus empleados. Implementan programas de educación en seguridad que incluyen capacitaciones periódicas, simulacros de phishing, políticas de seguridad claras y actualizadas, y prácticas de buenas prácticas de seguridad. Esto ayuda a garantizar que todos los miembros de la organización estén informados sobre las amenazas y las mejores prácticas de seguridad (León & Rodriguez, 2021).

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

2.2.2.2. Seguridad en las VPN

Amaya (2018), menciona que las VPN como su nombre lo indica son redes privadas, y se rompe la seguridad de las VPN, siempre que está ya no sea privada. El autor los divide en 3 aspectos importantes:

- **Privacidad:** o conocido como confidencialidad, que los recursos compartidos sólo serán autorizados por 2 nodos que quieran conectarse, más no otros.

- **Confiabilidad:** o conocido como integridad que nos dice que la información no debe ser manipulada o tergiversada cuando pasa por la red pública.

- **Disponibilidad:** menciona que la información siempre deberá estar disponible cuando se requiera.

Otro de los aspectos de una VPN es el nivel de escalabilidad, esto se refiere a la amplitud de conexiones simultaneas que se conectan de acceso remoto o punto a punto. Para el Centro Criptológico Nacional (2022) de España, menciona que las VPN deben implementarse siguiendo principios de:

- **Seguridad:** La seguridad es el aspecto fundamental en el diseño y despliegue de una VPN. Utilizar un dispositivo físico dedicado se considera una opción más segura, ya que su único propósito es gestionar las conexiones VPN. En cambio, si el dispositivo realiza múltiples funciones, existe un mayor riesgo de vulnerabilidades que podrían ser explotadas por un atacante. Proteger

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

adecuadamente el dispositivo es una tarea compleja que requiere conocimientos sólidos en seguridad (Centro Criptológico Nacional, 2018).

- **Rendimiento:** El funcionamiento de una VPN puede consumir recursos significativos, especialmente debido a las operaciones de cifrado y descifrado de datos. En el caso de un dispositivo físico dedicado, es necesario dimensionarlo adecuadamente para soportar la carga. Si se utiliza un dispositivo existente en la red, podría haber una carga excesiva que resulte en interrupción del servicio. También es posible que el rendimiento de la VPN se vea afectado por picos de consumo de CPU causados por otras funciones del dispositivo. Una solución viable es utilizar tarjetas criptográficas especializadas para realizar estas funciones (Montoya Benitez & Ospina, 2020).

- **Escalabilidad:** La escalabilidad se refiere a la capacidad de expandir la VPN para agregar más conexiones remotas, usuarios o equipos. En el caso de dispositivos físicos dedicados, la escalabilidad está limitada por las características del equipo. En algunos casos, puede ser necesario adquirir un nuevo equipo con mayor capacidad. Si se utilizan otros dispositivos de la infraestructura, es posible ampliar sus recursos (agregando procesadores, memoria, etc.) o migrar la VPN a un dispositivo con más capacidad (Vidal, 2016).

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

- **Operación y mantenimiento:** Los dispositivos físicos dedicados requieren más tareas de mantenimiento en comparación con otros dispositivos de la infraestructura. Esto se debe a que se agregan nuevos equipos con características específicas, que incluso pueden tener su propio sistema operativo. Las tareas de operación pueden volverse más complejas en este caso (Morales, 2012).

- **Capacidades de control:** Al utilizar dispositivos de la infraestructura existente, se pueden perder algunas capacidades de control relacionadas con el equipo físico y el software base, como el sistema operativo y otras utilidades. Por ejemplo, reiniciar el dispositivo para restablecer el funcionamiento de la VPN debe planificarse cuidadosamente para no afectar la disponibilidad de otras funciones. Además, puede haber restricciones en la instalación de actualizaciones o componentes de software adicionales debido a su impacto potencial en otras funciones (Estriégana, 2014).

- **Costo:** En general, los dispositivos físicos dedicados son más costosos. Además del costo inicial de adquisición e implementación, existen diversos factores que influyen en el costo total. La escalabilidad es un aspecto clave que impacta significativamente en el costo, ya que, si la solución elegida no es escalable, el costo aumentará considerablemente a medida que la VPN supere su capacidad. Por lo tanto, es importante calcular el costo a largo plazo y realizar una comparativa adecuada entre las

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

diferentes opciones de implementación (Montes de Oca & Ramos, 2021).

2.2.2.3. Enfoques y tecnologías de seguridad

Según la empresa de seguridad KPMG (2023), los enfoques y tecnologías de seguridad son aspectos fundamentales para garantizar la protección de la información en entornos tecnológicos. Entre los más utilizados tenemos:

- **Firewall:** Un firewall es una barrera de seguridad que controla el tráfico de red entre redes separadas, como la red interna y la red externa de una organización. Su función principal es filtrar y bloquear el tráfico no autorizado, protegiendo así la red y los sistemas contra amenazas externas. Los firewalls pueden implementarse tanto a nivel de hardware como de software (Avila & Echeverria, 2022).

- **Sistemas de Detección y Prevención de Intrusiones (IDS/IPS):** Estos sistemas monitorean y analizan el tráfico de red en busca de actividades sospechosas o maliciosas. Un IDS (Intrusion Detection System) detecta intrusiones y alerta al administrador del sistema, mientras que un IPS (Intrusion Prevention System) va un paso más allá al bloquear o tomar medidas para las intrusiones en tiempo real (CCN, 2021).

- **Sistemas de Prevención de Pérdida de Datos (DLP):** Los sistemas DLP son tecnologías diseñadas para prevenir la fuga o pérdida no autorizada de datos confidenciales. Estos sistemas

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

pueden identificar y controlar la transferencia de información sensible, ya sea a través de la red, dispositivos de almacenamiento o medios de comunicación como menciona el centro de seguridad (Basque Cybersecurity Centre, 2023).

- **Sistemas de Autenticación:** La autenticación es un proceso para verificar la identidad de un usuario o dispositivo antes de otorgar acceso a recursos o servicios. Los sistemas de autenticación utilizan diversos métodos, como contraseñas, tokens de seguridad, certificados digitales o biometría, para asegurar que solo las personas autorizadas puedan acceder a los sistemas y datos.

- **Sistemas de Gestión de Identidad y Acceso (IAM):** Estos sistemas permiten administrar de manera centralizada los derechos y privilegios de acceso de los usuarios a los recursos de una organización. El IAM incluye la gestión de identidad (creación, modificación y eliminación de cuentas de usuario), así como la gestión de accesos (asignación de roles, permisos y políticas de acceso) como lo sugiere la empresa de seguridad (EVIDIAN IAM, 2022).

- **Encriptación:** La encriptación es el proceso de convertir información en un formato ilegible para protegerla de accesos no autorizados. Se utiliza tanto para proteger datos en tránsito (como las comunicaciones a través de una VPN) como para proteger datos en reposo (almacenados en dispositivos de almacenamiento). Los algoritmos de encriptación, como AES o SSL/TLS que aseguran la

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

confidencialidad de la información como lo declaran los autores (Kuthnik et al., 2019).

2.2.3. Metodología Top-Down

Esta metodología fue desarrollada por primera vez en la década de 1950 por el ingeniero de software estadounidense David Parnas en el que propuso que el diseño de un sistema se pudiera dividir en tres niveles como lo menciona en este artículo (Parnas & Clements, 1986). Parnas dividió entre estos 3 niveles que son: Nivel de sistema: Este nivel describe el propósito general del sistema y sus componentes principales; Nivel de subsistema: Este nivel describe los subsistemas individuales que componen el sistema y Nivel de componente: Este nivel describe los componentes individuales que componen los subsistemas.

Posteriormente esta metodología fue refinada y mejorada gracias a muchos otros ingenieros en los que se destaca Grady Booch, Ivar Jacobson, James Rumbaugh. Es así que esta metodología tuvo el objetivo central de comprender el marco del diseño y del desarrollo del sistema dividiéndolos en partes más pequeñas y manejables. Entre las principales ventajas es que se tiene mejor comprensión del sistema, fácil comprensión y comunicación entre clientes y usuarios y mayor flexibilidad. Por otro lado, las desventajas más relevantes son que pueden ser más costoso porque requiere más trabajo de diseño inicial y puede en ocasiones ser lento por la complejidad de desarrollar el sistema (Mestanza & Ninaquispe, 2022).

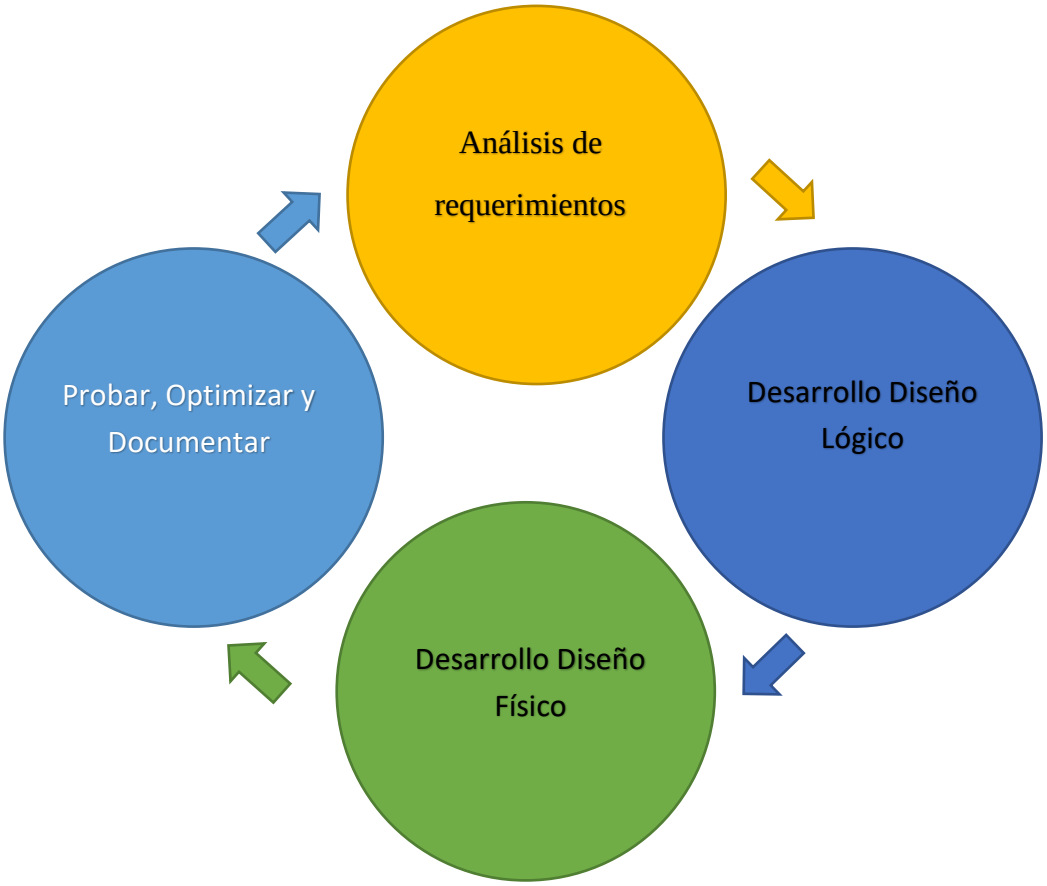
repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

Esta metodología consta de 4 fases que son:

Figura 5

Fases de la Metodología Top-Down



Nota: Elaboración propia.

2.2.3.1. Análisis de requerimientos

La primera fase de la metodología Top-Down es el análisis de requisitos. En esta fase, se identifican los requisitos del sistema. Los requisitos pueden ser funcionales, no funcionales o de interfaz. El objetivo de esta fase es comprender los requisitos del sistema para poder desarrollar un diseño que cumpla con las necesidades de los usuarios. Estos requisitos pueden ser recopilados a través de diversas técnicas, como entrevistas, encuestas, grupos de enfoque y pruebas de usuario y pueden ser clasificados en diferentes categorías, como funcionales, no funcionales e interfaz (Espitia & López, 2020).

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

2.2.3.2. Desarrollo del diseño Lógico

Aquí se desarrolla el diseño lógico del sistema. El diseño lógico describe la arquitectura general del sistema y las funciones que realizarán los diferentes componentes del sistema. El objetivo de esta fase es desarrollar un diseño que cumpla con los requisitos del sistema. Estas se hacen a través de diferentes técnicas, como diagramas de flujo, diagramas de entidades-relaciones, diagramas de clases y ser independiente de la plataforma y el lenguaje de programación sin olvidar que debe ser modular, para que pueda ser implementado y mantenido de forma sencilla (Cueva & Mishahuaman, 2019).

2.2.3.3. Desarrollo del diseño Físico

Es esta etapa se desarrolla el diseño físico del sistema. El diseño físico describe los componentes específicos del sistema y debe buscar ser compatible cumpliendo con los factores de rendimiento, seguridad y confiabilidad. El diseño físico debe ser documentado para que pueda ser implementado y mantenido de forma sencilla. El objetivo principal de esta etapa es que el diseño pueda ser implementado en la plataforma o lenguajes de programación elegidos (Cueva & Mishahuaman, 2019).

2.2.3.4. Prueba, Documentación y Evaluación

Aquí se prueba el diseño del sistema para garantizar que cumpla con los requisitos. También se optimizan los parámetros del sistema para mejorar el rendimiento y la seguridad. Finalmente, se documenta el diseño del sistema para que pueda ser implementado por el personal de la empresa buscando ser seguro y confiable. Para ello se pueden hacer diferentes tipos

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

de pruebas como caja blanca, pruebas de caja negra y pruebas de usabilidad y luego buscar su optimización. Sin olvidar que la documentación del sistema debe ser completa y precisa para que pueda ser implementada y mantenida de forma sencilla como el sistema lo exija (Sergei & Azúa, 2023).

Entonces, esta metodología tiene gran compatibilidad cuando de diseños de red se trata. Es por ello que se propusieron fases o entregables para una implementación o mejora en instituciones públicas o empresas privadas para la seguridad, confiabilidad y escalabilidad de la red se trata como el trabajo de (Lazarte, 2022). Estos cumplen con requisitos de la seguridad. Las instituciones privadas y públicas suelen tener requisitos de seguridad estrictos para sus redes. El enfoque Top-Down permite a los ingenieros de redes, diseñar redes que sean seguras desde el principio. Por otro lado, la escalabilidad que presenta esta metodología logra que las instituciones privadas y públicas suelen necesitar redes que puedan escalarse para adaptarse al crecimiento. Según Lazarte (2022), menciona los siguientes entregables:

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

2.2.3.5. Fases y entregables de la metodología Top-Down

Tabla 1

Fases y entregables de la metodología Top-Down

Fases	Procesos	Entregables
Fase1: Analizar requerimientos	Analizar metas del negocio	Diagnóstico del estado actual de los equipos, personal y servicios de los cuales disponen.
	Analizar metas técnicas	Diagnóstico de las políticas de seguridad tecnológica.
	Analizar red existente	Topología de la red física de la oficina central. Topología de las redes sucursales
	Analizar tráfico existente	Diagnóstico de las políticas ya acciones de seguridad.
Fase 2: Desarrollar Diseño Lógico	Diseñar topología de red	Diseñar el medio de transmisión Mapeo de usuarios Puntos de red Mapeo de equipos de red Características del cableado
	Diseñar modelos de direccionamiento y hostnames	Segmentación de direccionamiento lógico Direccionamiento de las IP
	Seleccionar protocolos para Switching y Routing	Protocolos LAN Protocolos de Ruteo
	Desarrollar estrategias de seguridad	Esquema de la zona desmilitarizada (DMZ)
	Desarrollar estrategias de administración de red	Plan de mantenimiento a los dispositivos de red, servidores y el UPS.
Fase 3: Desarrollar Diseño Físico	Seleccionar tecnologías y dispositivos para redes de campus	Documentos de aprobación del proyecto. Estándares para la adquisición de tecnologías y dispositivos.
	Seleccionar tecnologías y dispositivos para redes empresariales	Análisis de factibilidad
Fase 4: Probar, optimizar y documentar diseño	Probar el diseño de la red	
	Optimizar el diseño de la red	Implementación de la red.
	Documental el diseño	

Nota*:* (Lazarte, 2022).

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

2.2.4. Protocolos de conexión a Internet

2.2.4.1. Protocolos para Switches y Routing

Las redes LAN (Local Area Network) son sistemas informáticos que permiten la conexión y comunicación entre diferentes dispositivos, como computadoras, dentro de un área local, como una oficina o un edificio. Estas redes no pueden establecer una conexión directa entre los dispositivos de forma automática, ya que necesitan parámetros y reglas que definan cómo se realizará el intercambio de datos, cómo se enrutará la información y cómo se controlarán los posibles riesgos (CISCO, 2019).

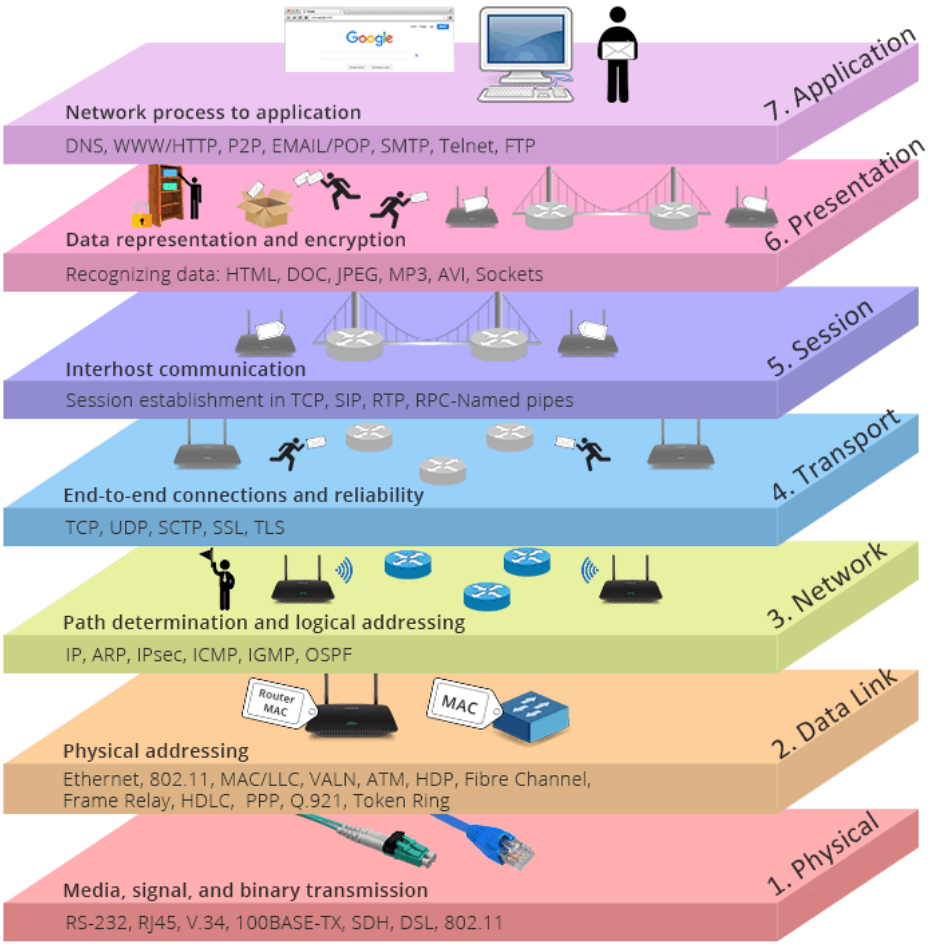
Cuando se habla de capas en las redes LAN, se refiere a la estructura en la que se organizan las diferentes funciones y procesos necesarios para que los dispositivos se comuniquen entre sí. Esta estructura se basa en el modelo OSI (Open Systems Interconnection), que es un conjunto de estándares validados por la ISO (Organización Internacional de Normalización) para describir el funcionamiento de las redes informáticas (FSCommunity, 2021). El modelo OSI divide el proceso de comunicación en redes en siete capas, cada una con su función específica. Estas capas incluyen aspectos como la transmisión de datos, el enrutamiento, la seguridad y el control de errores. Al seguir este modelo, se puede lograr una comunicación eficiente y confiable entre los dispositivos de una red LAN.

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

Figura 6

Protocolos LAN



Nota: Extraído de la página web (FSCommunity, 2021).

2.2.4.2. Protocolos de Ruteo

Los protocolos de ruteo son utilizados en el proceso de mover datos entre diferentes redes de capa 3, es decir, en el enrutamiento. Los routers son dispositivos que desempeñan esta función, aunque también pueden hacerlo otros dispositivos como los switches (FSCommunity, 2021).

El uso de un protocolo de enrutamiento permite anunciar las rutas descubiertas por otros medios, como otros protocolos de enrutamiento, rutas estáticas o rutas conectadas directamente. Esto se conoce como entrega. Aunque es deseable utilizar un solo protocolo de enrutamiento en

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

toda una red IP, es común encontrar entornos de enrutamiento multiprotocolo por diversas razones, como estándares comerciales, gestión de múltiples departamentos a cargo de diferentes administradores de red o entornos con múltiples proveedores. La implementación de diferentes protocolos de enrutamiento generalmente forma parte del diseño de la red, pero esto requiere tener en cuenta la redistribución. La redistribución se realiza para abordar las diferencias en las características de los protocolos de enrutamiento, como métricas, distancia administrativa y capacidades clasificadas y no clasificadas (Araya, 2017).

Existen diferentes tipos de enrutamiento:

- **Enrutamiento Estático:** Es una forma manual de agregar rutas en el router. Se utiliza cuando hay una única conexión y se establece una ruta estática. Es útil cuando un usuario desea administrar la conexión y el enrutamiento sin compartir con otros (Mosalvo, 2013).

- **Enrutamiento Predeterminado:** El router utiliza una ruta predeterminada cuando no encuentra una ruta específica para un destino. Es una forma más dinámica y flexible de enrutar los dominios de salida (Araya, 2017).

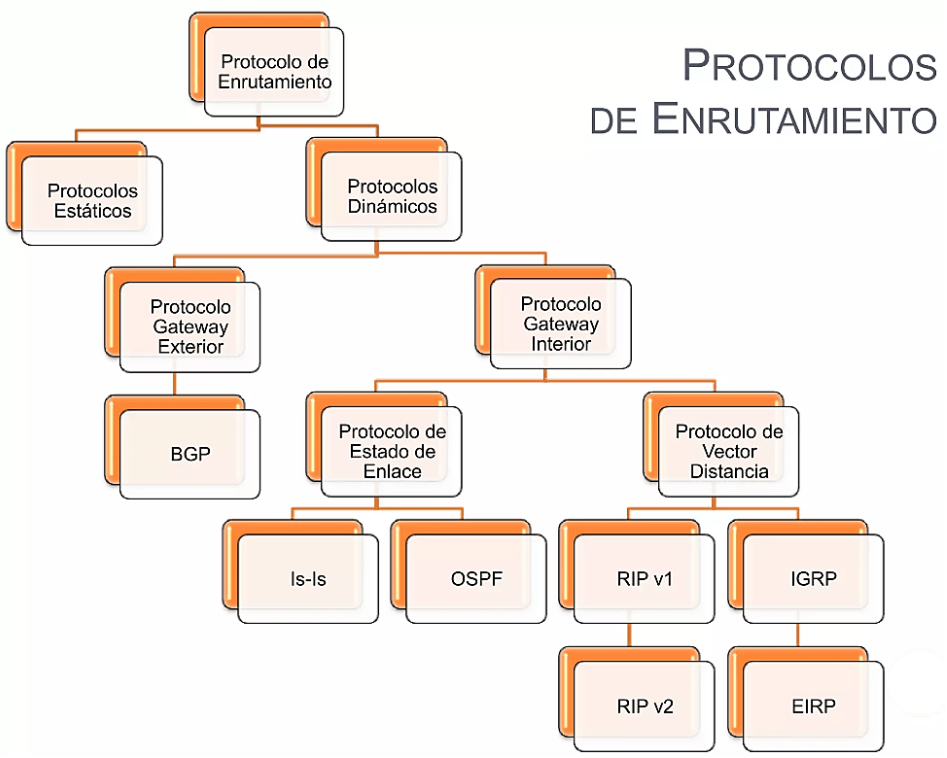
- **Enrutamiento Dinámico:** Se basa en tablas de información y permite que las rutas se actualicen automáticamente según los cambios en la red. Este enfoque es más recomendado, ya que proporciona respaldo en caso de fallos y permite medir la eficiencia de las rutas (Anónimo, 2012).

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

Figura 7

Protocolos de Enrutamiento



Nota: Autoría de (Mosalvo, 2013).

2.2.4.3. Desarrollar Estrategias de seguridad

2.2.4.3.1 Esquema de Zona Desmilitarizad (DMZ)

La DMZ es una estrategia de seguridad que consiste en utilizar un firewall y una red local como una zona intermedia entre Internet y la red interna de una empresa. La DMZ permite conexiones desde Internet y desde la red interna, pero no permite conexiones desde la DMZ hacia la red interna. Esto se hace para proteger los servidores que tienen acceso a Internet, ya que son más vulnerables a ataques. Si un ciberdelincuente logra ingresar a un servidor en la DMZ, será difícil acceder a la red interna de la organización debido a las restricciones de conexión (INCIBE, 2019).

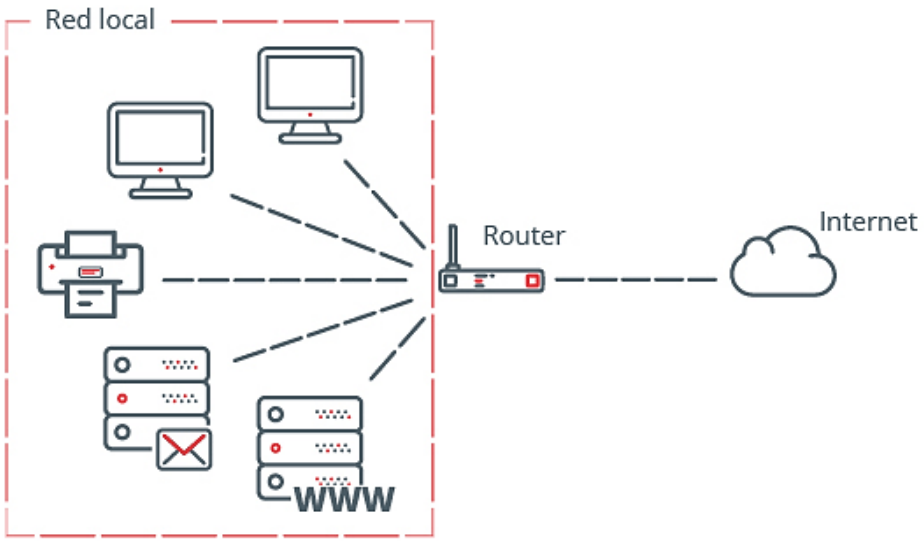
repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

Los diagramas de red son herramientas visuales que ayudan a las organizaciones a entender cómo funcionan los dispositivos y las redes. Permiten representar visualmente las interconexiones entre los componentes de la red, como enrutadores, firewalls y dispositivos, para facilitar la comprensión, solución de problemas y mantenimiento de la seguridad y el cumplimiento. Estos diagramas pueden ser tan detallados o amplios como sea necesario, mostrando dispositivos individuales, aplicaciones o áreas específicas de servicio (INCIBE, 2019).

Figura 8

Red de una Organización Simple



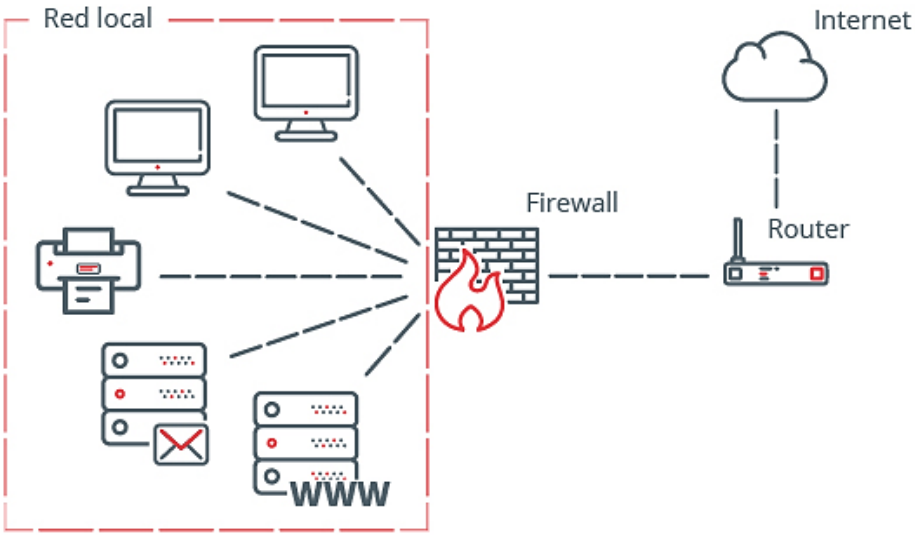
Nota: Extraído de Blogs de seguridad de (INCIBE, 2019).

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

Figura 9

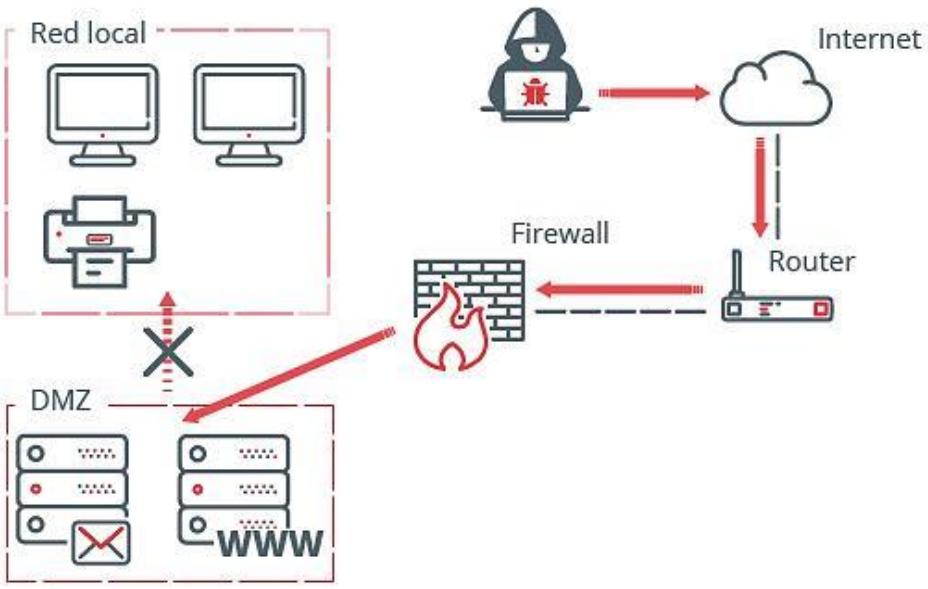
Red de una organización con Cortafuegos - Firewall



Nota: Extraído de Blogs de seguridad de (INCIBE, 2019).

Figura 10

Red segura con Cortafuegos (Firewall) y DMZ



Nota: Extraído de Blogs de seguridad de (INCIBE, 2019).

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

2.3. MARCO CONCEPTUAL

Encriptación: La encriptación es un proceso mediante el cual la información se convierte en un formato ilegible utilizando un algoritmo criptográfico y una clave de encriptación. Solo las personas o sistemas autorizados que poseen la clave adecuada pueden revertir el proceso y acceder a la información original. La encriptación es fundamental en la protección de la confidencialidad de los datos en una VPN (Rosero, 2021).

Algoritmo AES-256: AES (Advanced Encryption Standard) es un algoritmo de cifrado simétrico ampliamente utilizado en la criptografía moderna. AES-256 se refiere a la variante de AES que utiliza una clave de 256 bits, lo que proporciona un alto nivel de seguridad. Este algoritmo se utiliza comúnmente en la encriptación de datos en las VPN para proteger la confidencialidad de la información transmitida (Medina & Miranda, 2015).

PKI (Infraestructura de Clave Pública): La PKI es un conjunto de servicios, estándares y tecnologías utilizados para gestionar y autenticar certificados digitales. Proporciona los medios para emitir, revocar y validar los certificados de seguridad utilizados en las VPN y otras aplicaciones criptográficas. La PKI incluye componentes como autoridades de certificación, certificados digitales, infraestructuras de confianza y protocolos de intercambio de claves (Jarauta et al., 2006).

Firewall de aplicación: Un firewall de aplicación es un componente de seguridad que controla y supervisa el tráfico de red en busca de amenazas específicas de aplicaciones. Se utiliza para proteger las VPN y otros sistemas contra ataques dirigidos a vulnerabilidades conocidas de aplicaciones. El firewall de aplicación

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

inspecciona los paquetes de datos en busca de patrones maliciosos y aplica políticas de seguridad para prevenir el acceso no autorizado (CITRIX, 2022).

Certificado X.509: El certificado X.509 es un estándar ampliamente utilizado para la emisión y gestión de certificados digitales en la infraestructura de clave pública (PKI). Estos certificados se utilizan en las VPN para autenticar y asegurar las comunicaciones. El formato X.509 define la estructura de los certificados, incluyendo información como el nombre del titular, la clave pública y la firma digital, lo que garantiza la autenticidad y la integridad de los certificados (CCIT, 2008).

Gestión de claves: La gestión de claves es un conjunto de prácticas y procedimientos para generar, distribuir, almacenar y revocar claves criptográficas utilizadas en la seguridad de la información. En el contexto de las VPN, la gestión de claves se encarga de administrar las claves utilizadas en los protocolos de encriptación, como AES o SSL/TLS. Esto incluye la generación segura de claves, su distribución a los usuarios autorizados y su protección contra pérdida o compromiso (Torres & Espinoza, 2019).

Tunneling (Enrutamiento en Túnel): El tunneling es una técnica utilizada en las VPN para encapsular y proteger el tráfico de red en un túnel seguro a través de una red pública o no confiable. Este proceso implica el encapsulamiento de los paquetes de datos en un protocolo de nivel superior, que se utiliza para transportar los paquetes a través de la VPN. El tunneling asegura la confidencialidad y la integridad de los datos al proporcionar un canal seguro para la transmisión (Andrés & Herías, 2009).

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

Algoritmo de Hash SHA-256: Son funciones criptográficas que toman un conjunto de datos y generan una cadena de caracteres única e irreproducible. Estas cadenas, conocidas como hashes, se utilizan para verificar la integridad de los datos y garantizar que no hayan sido modificados. El algoritmo SHA-256 (Secure Hash Algorithm 256 bits) es ampliamente utilizado en las VPN y otras aplicaciones de seguridad para garantizar la integridad de la información transmitida (Domínguez Gómez, 2018).

AES-256-GSM: Es un método de cifrado utilizado para proteger información confidencial en línea. Utiliza una técnica llamada AES (Advanced Encryption Standard) con una clave de 256 bits para convertir los datos en un formato ilegible, lo que garantiza su privacidad y seguridad durante la transmisión. El "GCM" se refiere al modo de operación que también verifica la integridad de los datos, asegurando que no hayan sido alterados durante el proceso de cifrado y descifrado (Ahmad et al., 2018).

Certificado digital: Un certificado digital es un archivo electrónico que vincula la identidad de una entidad (por ejemplo, una persona, una organización) con una clave pública. Los certificados digitales son emitidos y firmados por una autoridad de certificación confiable y se utilizan para establecer la autenticidad y confianza en las comunicaciones en línea. En las VPN, los certificados digitales desempeñan un papel crucial en la autenticación de los participantes y en la creación de túneles seguros para el intercambio de datos (CISCO, 2019).

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

CAPÍTULO III

MATERIALES Y MÉTODOS

Se obtuvo el consentimiento informado del Sr. Abelardo, jefe ejecutivo de la empresa GS Constructora y Maquinarias, respetando la confidencialidad y anonimato de la información y las entrevistas recolectadas. Se registró datos de los equipos de red, incluyendo routers, las computadoras utilizadas en la empresa y las personas que laboran en la sede central la topología de la red. Estos registros han sido realizados de acuerdo a los procedimientos establecidos por la empresa con la metodología Top-Down. Seguidamente se procedió evaluar el nivel de seguridad de la información antes de la construcción de la VPN con $OpenVPN$, para luego volver a evaluar el nivel de seguridad en $Master\_GSVPN$.

3.1. UBICACIÓN GEOGRÁFICA DEL ESTUDIO

El estudio se llevó a cabo en dos etapas en diferentes ubicaciones geográficas: En la primera fase, se realizó una prueba piloto del entorno seguro en la ciudad de Juliaca en la sede central de GS, donde se evaluó su funcionalidad y efectividad en un ambiente controlado. Una vez confirmado que el entorno seguro funcionaba correctamente, se procedió a la segunda fase de prueba de conexión, que se llevó a cabo en el distrito de Lari, provincia de Caylloma, del departamento de Arequipa, donde se ubicaba el proyecto "MEJORAMIENTO DE LA CARRETERA LARI - MADRIGAL". Estas dos etapas permitieron evaluar el desempeño del entorno seguro en diferentes ubicaciones geográficas y obtener datos relevantes para el análisis posterior de los resultados.

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

Figura 11

Proyecto "Carretera Lari - Madrigal"

Nota**:** Google Maps.

3.2. PERIODO DE DURACIÓN DEL ESTUDIO

El estudio inició en el mes de abril del 2023 y concluyó en agosto del 2023, teniendo una duración de 5 meses de ejecución y análisis de resultados.

3.3. DISEÑO, TIPO Y METODOLOGÍA

3.3.1. Diseño de investigación

El diseño es cuasi experimental. Que corresponde a los estudios experimentales. Este estudio intenta comparar entre la medición del antes del experimento y el después del experimento, de la variable que se estudia en la determinada muestra (Agudelo et al., 2008).

$$G \longrightarrow O_1 \longrightarrow X \longrightarrow O_2$$

Donde:

G: Grupo muestral

X: Tratamiento experimental (Diseño VPN con Software Libre)

O1: Pre test

O2: Post test

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

3.3.2. Tipo de investigación

Según su enfoque, esta investigación de tipo cuantitativo que se caracteriza por utilizar datos numéricos y estadísticos para analizar y comprender fenómenos. Según Hernández (2014) destaca que este tipo de investigación se basa en la recolección y análisis de datos cuantitativos para responder a preguntas de investigación específicas.

En cuanto a su profundidad, esta investigación es de tipo aplicativa se caracteriza por buscar soluciones prácticas y aplicables a problemas o situaciones del mundo real. Que según Arias y otros (2022) mencionan que la investigación aplicada se centra en la generación de conocimiento útil y aplicable en contextos prácticos y concretos.

En relación a su inferencia, este estudio es de tipo hipotético-deductiva porque consiste en un procedimiento que intenta dar respuesta a los distintos problemas que se plantea la ciencia a través de la postulación de hipótesis que se toman como verdaderas. No habiendo ninguna certeza acerca de ellas. , quienes desarrollaron el enfoque de teoría fundamentada, que se basa en la construcción de teorías a partir de datos inductivos obtenidos de la realidad empírica (Ñaupas et al., 2018).

En cuanto a su temporalidad, una investigación de corte transversal se realiza en un momento específico del tiempo, sin seguimiento a lo largo del tiempo Mitchell y Espinoza & Toscano (2015) mencionan que este tipo de investigación se realiza en un momento dado para analizar una situación o fenómeno en un momento específico, sin considerar cambios longitudinales a lo largo del tiempo.

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

3.4. METODOLOGÍA DE INVESTIGACIÓN

El proceso metodológico usado fue el Top-Down, fue desarrollado en varias fases secuenciales para el diseño de la red VPN del proyecto madrigal. En la Fase I de Análisis de requerimientos, se evaluaron las necesidades, objetivos y requisitos técnicos, junto con la viabilidad para la implementación del proyecto. Esta etapa incluyó el análisis exhaustivo de la red existente y del tráfico actual. Posteriormente, en la Fase II de Diseño Lógico de la red, se diseñaron diagramas de red que se basaron en los equipos ya disponibles en la empresa. Asimismo, se actualizó el plan del proyecto con los datos recopilados en la fase previa. Se procedió a diseñar la topología de la red, definiendo modelos de direccionamiento y asignación de nombres a los dispositivos. Además, se establecieron estrategias de seguridad y administración de la red. Durante la Fase III de Diseño de la red física, se eligieron con detenimiento las tecnologías y dispositivos más adecuados para la infraestructura. Finalmente, en la Fase IV de Pruebas, Optimización y documentación del diseño de la Red, se estableció un cronograma de implementación. Se sometió un prototipo a pruebas y se monitorizó su rendimiento. En caso de identificar fallas, se optimizó el diseño de la red, concluyendo con la documentación exhaustiva del diseño final. En todo el proceso, se enfatizó la retroalimentación constante y la comunicación cercana con los usuarios, con el objetivo de incorporar sugerencias, mejoras y necesidades de nuevas aplicaciones para el monitoreo efectivo de la red en cada una de sus etapas (Hernández Hipólito et al., 2021).

3.5. POBLACIÓN Y MUESTRA

La población de estudio está conformada por 44 trabajadores, los cuales se distribuyen en distintos proyectos de la empresa GS Maquinarias y Constructora E.I.R.L Juliaca, que se encuentra en el ámbito de la actividad constructora, la empresa tiene cuatro proyectos en proceso, cada proyecto conformado entre 11 a 17 trabajadores. Estos

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

trabajadores laboran en obras de proyectos llevados a cabo por la empresa en distintas ubicaciones geográficas, con diversas características y con diferentes temporalidades.

Por otro lado, la muestra seleccionada para el estudio son 14 trabajadores del proyecto “Mejoramiento de la carretera Lari - Madrigal, Arequipa”, el cual se distribuye en 5 trabajadores de logística y 9 en obra. Este proyecto ha sido seleccionado mediante un muestreo no probabilístico por conveniencia. Cabe destacar que, aunque esta muestra no sigue un proceso de selección aleatorio, se considera representativa y adecuada para los objetivos planteados en el estudio por ser el proyecto que actualmente la empresa está ejecutando.

3.6. MATERIALES Y EQUIPOS UTILIZADOS

3.6.1. Materiales

- Laptop ASUS S510U
- Smartphone Android
- Cables de red UTP y otros accesorios de conectividad.

3.6.2. Hardware

- Servidor virtual para alojar el servidor VPN
- Dispositivos de red de alta capacidad (Routers, Switches, etc.)
- Servidor NAS

3.6.3. Software

- Sistema operativo de servidor Ubuntu 22.04 LTS Jammy Jellyfish

3.6.4. Servicios

- Internet simétrico de 50Mb/s
- Software de monitoreo de conexión (OpenVPN, OpenVPN Log y Wireshark)

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

3.6.5. Técnica e Instrumento de recolección de datos

La técnica es la entrevista y el instrumento es la *"Encuesta sobre apreciación de la seguridad de la información"*, (véase Anexo C: Instrumento de investigación). Esta encuesta fue respondida en una primera etapa conocida como el Pre Test para luego mostrarles la $VPN\ Master\_GSVPN$ desarrollada para volver a evaluar el Post Test entre los 14 colaboradores de GS Constructora y Maquinarias. Habiendo recolectado los datos se procedió a hacer la comparación del antes con el después para demostrar que la red privada VPN basado en software libre mejora la seguridad de la información usando el estadístico de Wilcoxon.

3.7. OPERACIONALIZACIÓN DE VARIABLES

Tabla 2

Variables y Dimensiones

Variables	Dimensiones	Descripción
Red Privada Virtual (VPN)	Acceso remoto seguro	Se refiere a la capacidad de una VPN para proporcionar acceso remoto a la información sensible de una empresa de manera segura. Esto significa que la VPN debe ser capaz de proteger la información sensible de accesos no autorizados, alteraciones, divulgación o destrucción de la información.
Seguridad de la información	Seguridad	Es la capacidad de una VPN para proteger la información sensible de una empresa contra accesos no autorizados, alteraciones, divulgación o destrucción. En base al nivel de seguridad, encriptación y cifrado.
	Confiabilidad	Es la capacidad de una VPN para proporcionar acceso a la información sensible de una empresa de manera confiable respecto a la integridad y confidencialidad durante la transmisión de datos, autenticación, autorización y procedimientos de restauración.

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

Escalabilidad	Es la capacidad de una VPN para adaptarse a las necesidades cambiantes de una empresa cuidando la protección, posibles amenazas cibernéticas y adaptación de conexiones simultaneas y aumento de la cantidad de datos.

Nota: Elaboración propia.

3.8. CONSIDERACIONES ÉTICAS

Entendemos por ética a la rama de la filosofía deontológica que estudia la moral, es decir, el conjunto de normas que rigen la conducta humana. La ética profesional, por su parte, se refiere a las normas morales que deben seguir los profesionales en el ejercicio de su profesión. Según el artículo 15 del código de ética del Colegio de Ingenieros del Perú (CIP) vigente, creada bajo la Ley N° 24648, establece los valores morales que deben seguir los ingenieros en el ejercicio de su profesión. Estos valores son: Honestidad, Integridad, responsabilidad, Eficiencia y Solidaridad (Código de Ética del Colegio de Ingenieros del Perú, 2018).

En este contexto, para fines investigativos el profesional Ingeniero de Sistemas deberá obtener el consentimiento informado de los jefes ejecutivos o administrativos y otros empleados de las empresas privadas para el acceso de datos bajo los principios morales, estas corresponden a la lealtad, el honor profesional y respeto. Es por ello que, en la empresa GS Maquinarias y Constructora E.I.R.L., Juliaca, se obtuvo el consentimiento y autorización del recojo de datos dentro de la empresa respetando la confidencialidad de datos como la información financiera, propiedad intelectual, cartera de clientes y datos sensibles de los empleados cumpliendo con las consideraciones éticas antes mencionadas.

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

Este capítulo está dividido en 4 partes siguiendo el orden de los 4 objetivos específicos propuestos en el capítulo I. Empezando por el análisis de requerimientos en el área de Tecnologías de la Empresa GS Maquinarias y Constructora E.I.R.L., Juliaca, 2023. Seguido del diseño de la red lógica y Física de la empresa, continuando con la documentación de la VPN ejecutado en un servidor Ubuntu 22.04 en la versión Jammy Jellyfish junto con la evaluación estadística experimental que fue sometido a los colaboradores de GS, para finalmente evaluar el retorno de inversión de la implementación de la VPN como proyecto en la empresa GS Maquinarias y Constructora E.I.R.L., Juliaca, 2023.

4.1. ANÁLISIS DE REQUERIMIENTOS DE GS

Se realizó la visita a la empresa y mediante la entrevista al jefe ejecutivo y los diferentes colaboradores, junto con la observación y recopilación de la topología lógica y física de la red. Lográndose analizar los siguientes requerimientos bajo el enfoque Top-Down en el área de tecnología en la empresa GS Maquinarias y Constructora E.I.R.L., Juliaca, 2023.

Se logró evidenciar la inexistencia de algún servidor como punto de entrada y salida de datos. Asimismo, que actualmente GS hace el uso de Power BI como servicio en la nube donde se hace el uso de almacenamiento en la nube y acceso a un sistema de información básico donde los colaboradores tienen acceso para la transferencia de datos sensibles como reportes, documentos, expedientes, planos geográficos y topográficos propios del rubro de GS. Sin olvidar el uso de Gmail y WhatsApp para la comunicación.

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

4.1.1. Analizar metas del Negocio en el área de Tecnología

4.1.1.1. Metas de negocio de la Empresa GS

1. Acceso a archivos sensibles de los proyectos de licitaciones.
2. Seguridad en la transferencia de archivos sensibles de los proyectos.
3. Fácil conexión de archivos de manera remota y segura.
4. Alto ancho de banda para la lectura y escritura de archivos que pesan más de 1GB de manera remota por la red como expedientes, planos, etc.
5. Seguro y confiable con la transferencia de archivos sensibles con algún tipo de cifrado de seguridad.
6. Que deniega accesos no autorizados a la red local mediante algún tipo de autenticación.
7. Que pueda soportar más de 40 equipos entre PC, Laptops y dispositivos móviles conectadas a la red simultáneamente como requerimiento futuro de crecimiento de GS.
8. Que sea robusto y tolerante a fallos.
9. Capacitación en el uso y correcto manejo de tecnologías que usa GS para los colaboradores frecuentemente.

4.1.1.2. Lista de restricciones de la Empresa GS

1. Que no supere un presupuesto total de 1000 dólares mensuales (es el precio aproximado que GS gasta mensualmente en el pago de acceso a colaboradores en Power BI y almacenamiento en la nube).
2. Que se use los equipos de red de la empresa, quizás se requiera la adquisición de (servidores, routers, etc.).
3. Implementación de políticas de información sobre manejo de la red corporativa.

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

4.1.2. Diagnóstico del estado actual de los equipos, personal de GS

Se procedió con el diagnóstico actual de los equipos de cómputo mediante la observación de los equipos de la empresa GS Maquinarias y Constructores E.I.R.L, verificando el estado y detalles de los equipos obteniendo lo siguiente.

Tabla 3

Personal de GS y características de sus equipos

Nro.	Cargo	Características de equipo
1	Administrador	i7-9700 10gen, 16 GB RAM, Windows 11
2	Logística	AMD Ryzen 5 5600X, 12 GB RAM, Windows 10
3	Contabilidad	i5-10400 10gen, 8 GB RAM, Windows 10
4	Costos	i3-9100 9gen, 8 GB RAM, Windows 10
5	Asistente De Contabilidad	AMD Ryzen 3 3300X, 8 GB RAM, Windows 10
6	Controlador	i5-9400 9gen, 8 GB RAM, Windows 10
7	Gestor De Cobranza	AMD Ryzen 5 3600, 12 GB RAM, Windows 10
8	Sociólogo	Intel Core i7-11700, 8 GB RAM, Windows 10
9	Op. De Volquete	Intel i3 G6400, 4 GB RAM, Windows 10
10	Op. De Volquete	Intel i5 G6400, 8 GB RAM, Windows 10
11	Op. De Volquete	Intel i3 G6400, 4 GB RAM, Windows 10
12	Guardian	AMD Athlon 3000G, 8 GB RAM, Windows 10
13	Guardian	AMD Athlon 3000G, 8 GB RAM, Windows 10
14	Guardian	AMD Athlon 3000G, 8 GB RAM, Windows 10

Nota: Elaboración propia.

4.1.3. Diagnóstico de Personal de GS

Se diagnosticó en la ubicación del Jr. Progreso 736 de Juliaca, se verificó 2 grupos de personal, los trabajadores de mano de obra y el personal

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

administrativo de logística (la gerencia). Es el personal administrativo quienes harán uso de la VPN para la evaluación.

Se observó al personal que:

1. Son pocos colaboradores encargados de la gestión administrativa, por lo que falta personal especialista en el área de tecnología.

2. Para la gestión de proyecto usan Power BI, porque mencionan que es fiable y de bajo costo de paga.

3. Falta de un software interno para la administración de los proyectos, se basan únicamente con software de paga.

4. Falta de un servidor como central de datos.

4.1.4. Analizar metas técnicas

Entre las importantes metas técnicas que mencionó el director ejecutivo de GS son:

1. Se pretende tener un sistema de información general interna robusta que logre interconectar toda la información entre diferentes departamentos y colaboradores de manera local y de forma remoto.

2. Usar una VPN robusta y sencilla de usar para poder interconectar a la red local de la sede central para el acceso y uso de recursos internos. Ya que los proyectos se realizan por periodos y son lejanos.

3. Que está tecnología sea propia y robusta que no genere gastos de mantenimiento más de 1000 dólares mensuales.

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

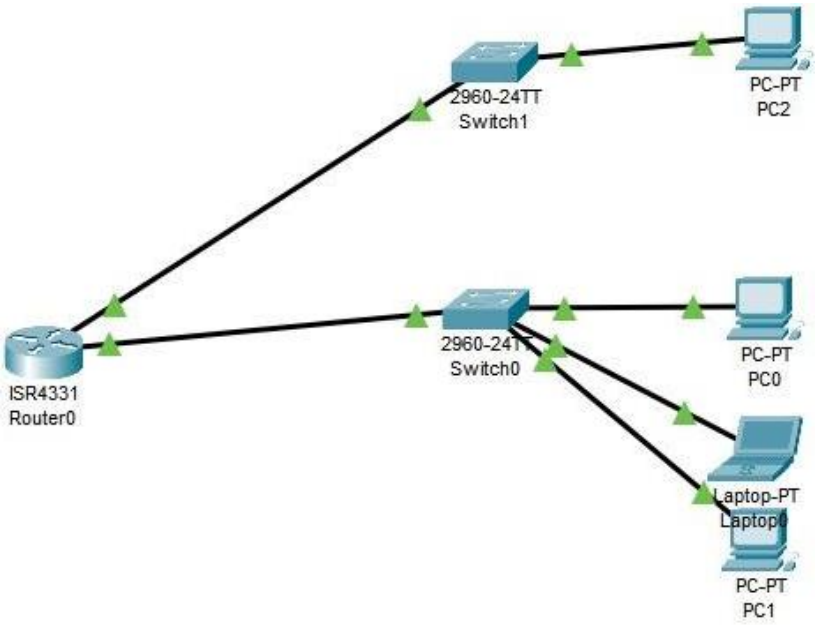
UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

4.1.5. Analizar Red existente

La red por ahora se encuentra en le sede central de GS Maquinarias y Constructoras. En tanto que, cuando se presenta un nuevo proyecto se hace un módulo en el lugar del proyecto que normalmente queda en zonas rurales del sur del país. En la oficina central de GS tiene el servicio de Internet Movistar de una velocidad simétrica de subida y bajada de 100Mb/s. La siguiente figura demuestra la situación actual de la topología de la red lógica de *MasterGS* donde se demuestra que existe un router principal y 2 Switches, uno para cada piso.

Figura 12

Topología lógica de la red actual de GS



Nota: Elaboración propia con Cisco Pack Tracer.

4.2. DISEÑO LÓGICO Y FÍSICO DE LA RED DE GS

4.2.1. Diseño de la Topología Lógica de la Red

Se propone el nuevo diseño de la red de GS con la inserción de un Switch Mikrotik junto con el servidor NAS que alojará la VPN Master GS. Del mismo modo, el servidor tendrá una capacidad de 20 terabytes de almacenamiento

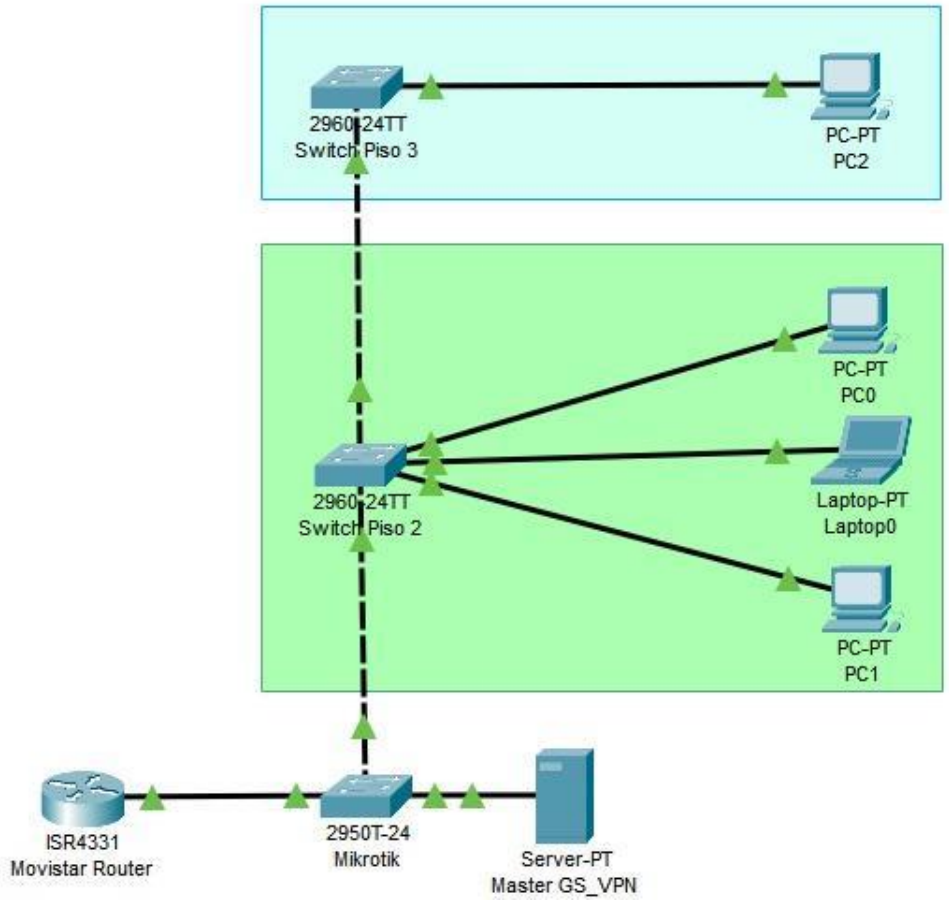
repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

expansible, en el cual se alojará sistemas de información de carácter local y bases de datos compartidos. Es así que, todos los equipos de GS tendrán acceso al servidor NAS junto con la VPN Master GS de manera local. Para las conexiones remotas los colaboradores que están fuera podrán acceder al servidor usando su llave "$.ovpn$" desde sus teléfonos móviles o laptops como si estuvieran dentro de la torre de GS. Se recalca que el servidor NAS será usado como almacén de datos y alojamiento de sistemas de información locales que desee implementar.

Figura 13

Propuesta de la topología lógica de la red de GS



Nota: Elaboración propia.

Por ello, se reconoció a los colaboradores con los puntos de red que usarán está nueva arquitectura que se enlista a continuación.

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

Tabla 4

Lista de usuarios con sus cargos en GS

N	DNI	Apellidos Y Nombres	Cargo	Condición
1	47288337	Morocco Vargas Abelardo	Administrador	Interno
2	74386025	Yana Paucar Soledad	Logística	Interno
3	46755414	Aceituno Neira, Lucia	Contabilidad	Interno
4	71940754	Coaquira Caceres Denis Mirian Lucero	Costos	Interno
5	72011704	Choque Huanaco Nedy Edith	Asistente de Contabilidad	Interno
6	21270305	Luicho Luna, Martin	Controlador	Interno
7	02144579	Gonzales Yucra, Rufino Valeriano	Gestor De Cobranza	Interno
8	40695094	Vilca Gutierrez, Juan Guido	Sociologo	Interno
9	44019679	Surco Mamani Grover Ivan	Op. De Volquete	Interno
10	40510007	Colca Mamani Juan Cesar	Op. De Volquete	Interno
11	43368706	Mamani Larico Elvis	Op. De Volquete	Interno
12	80668163	Condori Choquehuanca Vidal	Guardian	Interno
13	70170219	Mamani Mamani Alex Wagner	Guardian	Interno
14	42448532	Mamani Ylaquijo Juan Pastor	Guardian	Interno

Nota: Elaboración propia extraída de lista del personal interno de GS.

Tabla 5

Puntos de red por oficinas en GS

Oficina	Dirección de Red	Mascara de Red	Puerto de Enlace	Nombre del Equipo	Piso
Área de Administración	192.168.1.1	255.255.255.0	192.168.1.30	Oficina2	2do Piso
Área de Administración	192.168.1.1	255.255.255.0	192.168.1.31	Oficina3	2do Piso
Área de Administración	192.168.1.1	255.255.255.0	192.168.1.32	Oficina4	2do Piso
Área de Ingeniería	192.168.1.1	255.255.255.0	192.168.1.51	Compu1	3er Piso
Área de Ingeniería	192.168.1.1	255.255.255.0	192.168.1.52	Compu2	3er Piso
Oficina de Administración	192.168.1.1	255.255.255.0	192.168.1.60	Principal	2do Piso

Nota: Elaboración propia extraída de lista del personal interno de GS

4.2.1.1. Características de cableado Estructurado

Al hacer la revisión de la infraestructura se evidenció los tipos de cable usado en los equipos de comunicación:

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

Categoría 5: El cable de categoría 5 es un tipo de cable de par trenzado cuya categoría es uno de los grados de cableado UTP descritos en el estándar EIA/TIA 568B el cual se utiliza para ejecutar CDDI y puede transmitir datos a velocidades de hasta 100 Mbps a frecuencias de hasta 100 MHz.

4.2.1.2. Lista de Equipos de comunicación

Tabla 6

Lista de equipos de comunicación

Equipo	Marca	Modelo	Cantidad	Descripción
Router	MitraStar	HGU GPT-2541GNAC	1	Equipo instalado por movistar
Switch	Tp-link	SG1024D	1	Equipo instalado por la empresa de 24 puertos
Switch	Tp-link	TL-SF1016D	1	Equipo instalado por la empresa de 16 puertos
UPS	APC Back	BX600C	1	Equipo de sistema de alimentac ión interrumpida
Servidor NAS	QNAP	TS-453D-4G	1	Equipo servidor de almacenamiento de 20TB expansible, 8GB RAM DDR4

Nota: Elaboración propia.

4.2.2. Diseño de la Topología Física de la Red

La prueba de esta red VPN se implementará como lo menciona en la Figura 9. Donde el equipo funcionará como Firewall y servidor que estará ubicado en la sede central de GS Maquinarias y Constructora. Quien otorgará acceso remoto de otros puntos de la VPN que intenten conectarse y tener un acceso LAN.

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

Tabla 7

Equipos utilizados para la VPN GS Master

Características	Sede central GS	Sede de proyecto Lari
Procesador	Intel core I7 10100U	AMD Ryzen 3
RAM	32 GB (3200Mz)	8 GB (2660Mz)
Almacenamiento	2 TB SSD	500 GB HDD
S.O.	Ubuntu 22.04 Jammy Jellyfish LTS	Windows 10
Aplicación de conexión	OpenVPN	OpenVPN Connect (Escritorio y Android)

Nota: Elaboración propia.

4.2.2.1. Seleccionar Tecnologías y dispositivos para redes de campus

- Ubuntu 22.04 Cliente Jammy Jellyfish LTS
- OpenVPN Debian V. 2.6.3.
- OpenVPN Gui Client V. 11.43
- Samba V. 4.11.6

4.2.2.2. Análisis de Factibilidad

Según lo detallado en los requerimientos tecnológicos que tiene la empresa GS Maquinarias y Constructora se estableció cuál es el futuro tecnológico entre ellas y la conexión segura que se debe tener cuando se haga un nuevo proyecto con la sede central de GS mediante una VPN robusta. En el 2023 la empresa GS está iniciando con la construcción tecnológica porque busca crecer como empresa y llevar a cabo más de 5 proyectos simultáneamente, por lo que se debe tener claro las normativas de seguridad en los sistemas de información internos como con las conexiones remotas de proyectos. Es por ello la importancia de empezar con la VPN como solución de comunicación remota inicial.

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

La sede central GS manejará como servidor Ubuntu 22.04 Jammy Jellyfish LTS que es una versión estable y que tiene gran apoyo por la comunidad de software libre y es la distribución más usada a nivel mundial. Asimismo, son manejables porque tienen un entorno de escritorio amigable que es GENOME. Además de ello, se requiere tener control del personal con un identificador Key propio y que los encargados sepan quienes están accediendo a la red desde su llave privada. Los usuarios que se conecten a las VPN podrán hacerlo desde cualquier dispositivo. Ya que $OpenVPN$ tiene aplicativos para Linux, Windows y Android, Así los colaboradores tendrán el total acceso una vez conectado a las VPN.

4.2.2.3. Factibilidad Técnica

La empresa GS no cuenta con un servidor por lo cual se adquirirá un servidor NAS de alta capacidad, se dejará la documentación respectiva para la implementación de la VPN Master GS, allí se detallará el código de comandos para su correcta instalación y generaciones de llaves privadas para cada colaborador. Asimismo, esto contará con la política de seguridad informática respectiva para su correcto funcionamiento y mantenimiento. Las características de los equipos según la Tabla 5 tienen la suficiente capacidad para poder levantar la VPN por lo que no será un problema significativo.

4.2.2.4. Sistema Operativo

Ubuntu 22.04 Jammy Jellyfish LTS en su carpeta $/etc/openvpn/$ contendrá 2 carpetas internas, que son $client\ y\ server$. Dentro de $client$ se crea todas las llaves para cada colaborador con sus respectivas carpetas

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

propias según su identificador el cual deberán ser ordenadas próximamente. Y dentro de la carpeta server se gestionarán el certificado de claves, archivos criptográficos importantes con el certificado $.ca$, y la llave $.ta$ y la configuración de la VPN Master GS.

4.2.2.5. Conclusión de Factibilidad Técnica

Existe suficiente factibilidad para la implementación de la VPN, cumpliendo con las metas tecnológicas de GS, respetando el margen de costo de mantenimiento y asegurando la robustes y flexibilidad de un software libre como lo es $OpenVPN$. Y podrá ser utilizado fácilmente por los colaboradores de GS para el acceso remoto de recursos a la sede central.

4.3. DOCUMENTACIÓN Y EVALUACIÓN DE LA VPN

4.3.1. Comandos de configuración en el Bash Ubuntu 22.04

Instalación del software y la CA: Este código se utiliza para instalar $OpenVPN$ y Easy-RSA en Ubuntu 22.04 y para crear una autoridad de certificación (CA). La CA se utiliza para generar certificados para los servidores y clientes $OpenVPN$.

```
sudo apt install openvpn easy-rsa -y
sudo cp -r /usr/share/easy-rsa /etc/openvpn/
cd /etc/openvpn/easy-rsa/
sudo ./easyrsa init-pki
sudo ./easyrsa build-ca
Nota: Generado con OpenVPN v2.6.3
```

Crear Claves del Servidor: Este código se utiliza para generar un certificado para el servidor $OpenVPN$. El certificado se utiliza para autenticar el servidor OpenVPN ante los clientes.

```
sudo ./easyrsa gen-req Master_GSVPN nopass
```


repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

```
sudo ./easyrsa sign-req server Master_GSVPN
sudo cp /etc/openvpn/easy-
rsa/pki/issued/Master_GSVPN.crt /etc/openvpn/server/
sudo cp /etc/openvpn/easy-rsa/pki/ca.crt
/etc/openvpn/server/
sudo cp /etc/openvpn/easy-
rsa/pki/private/Master_GSVPN.key /etc/openvpn/server/
```

Nota: Generado con OpenVPN v2.6.3

Creando la clave TLS-CRYPT: Este código se utiliza para generar una clave TLS para el servidor $OpenVPN$. La clave TLS se utiliza para establecer una conexión segura entre el servidor y los clientes.

```
cd /etc/openvpn/server
sudo openvpn --genkey --secret ta.key
```

Nota: Generado con OpenVPN v2.6.3

Generación de claves: Este código genera un certificado y una clave privada para un cliente. El certificado y la clave privada se almacenan en el directorio $/etc/openvpn/client/keys$ y se utilizan para autenticar el cliente ante el servidor.

```
sudo mkdir /etc/openvpn/client/keys
sudo chmod -R 700 /etc/openvpn/client
cd /etc/openvpn/easy-rsa
sudo ./easyrsa gen-req KevinConnect nopass
sudo ./easyrsa sign-req client KevinConnect
cp /etcopenvpneasy-rsa/pki/issued/KevinConnect.crt
/etc/openvpn/client/keys
sudo cp /etc/openvpn/easy-
rsa/pki/issued/KevinConnect.crt
/etc/openvpn/client/keys/
sudo cp /etc/openvpn/easy-
rsa/pki/private/KevinConnect.key
/etc/openvpn/client/keys/
sudo cp /etc/openvpn/easy-rsa/pki/ca.crt
/etc/openvpn/client/keys
sudo cp /etc/openvpn/server/ta.key
/etc/openvpn/client/keys/
```

Nota: Generado con OpenVPN v2.6.3

Configuración del servidor: Este código se utiliza para copiar la configuración de ejemplo del servidor $OpenVPN$ al directorio

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

/etc/openvpn/server/. La configuración de ejemplo se descomprime y se abre en el editor de texto Nano y se copia los comandos de configuración de $Master\_GSVPN$. Luego, se elimina la configuración de ejemplo y se crea una nueva configuración personalizada.

```
ls /usr/share/doc/openvpn/examples/sample-config-
files/
sudo cp /usr/share/doc/openvpn/examples/sample-
config-files/server.conf.gz /etc/openvpn/server/
sudo gunzip /etc/openvpn/server/server.conf.gz
sudo nano /etc/openvpn/server/server.conf
cd ..
cd server
ls -l
sudo rm server.conf
sudo nano server.conf
```

Nota: Generado con OpenVPN v2.6.3

Configuración del cliente: Este código se utiliza para copiar la configuración de ejemplo del cliente $OpenVPN$ al directorio $/etc/openvpn/client/$. Luego, se utiliza el comando sudo su para cambiar al usuario root y abrir la configuración del cliente $OpenVPN$ en el editor de texto Nano para editarla con los comandos de configuración de cliente.

```
sudo cp /usr/share/doc/openvpn/examples/sample-
config-files/client.conf /etc/openvpn/client/
sudo su
nano client.conf
```

Nota: Generado con OpenVPN v2.6.3

Cortafuegos y reinicio del servidor: Este código se utiliza para configurar el firewall de Linux para permitir el tráfico en el puerto 1194 y para habilitar e iniciar el servicio $OpenVPN$. Una vez que se haya ejecutado este código, el servidor estará listo para aceptar conexiones de los clientes.

```
sudo iptables -A INPUT -p udp --dport 1194 -j ACCEPT
sudo nano /etc/sysctl.conf
```


repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

```
sudo echo 1 > /proc/sys/net/ipv4/ip_forward
sudo iptables -t nat -I POSTROUTING 1 -s 10.8.0.0/24
-o wlp2s0 -j MASQUERADE
sudo iptables -I INPUT 1 -i tun0 -j ACCEPT
sudo iptables -I FORWARD 1 -i wlp2s0 -o tun0 -j
ACCEPT
sudo iptables -I FORWARD 1 -i tun0 -o wlp2s0 -j
ACCEPT
sudo iptables -I INPUT 1 -i wlp2s0 -p udp --dport
1194 -j ACCEPT

sudo iptables -L -nv
sudo iptables -t nat -L -nv
sudo apt install iptables-persistent -y
sudo netfilter-persistent save
sudo systemctl -f enable openvpn-
server@server.service
sudo service openvpn-server@server start
sudo service openvpn-server@server status
```

Nota: Generado con OpenVPN v2.6.3

Creando ficheros "*.ovpn*": Este código se utiliza para generar una configuración personalizada del cliente para el usuario *KevinConnect* como ejemplo. Una vez que se haya ejecutado este código, el usuario podrá conectarse al servidor utilizando la configuración personalizada generada. El usuario debe colocar el archivo de configuración personalizada en su dispositivo móvil o computadora para poder conectarse al servidor *Master_GSVPN*.

```
sudo cp /etc/openvpn/client/client.conf
/etc/openvpn/client/plantilla.conf
nano /etc/openvpn/client/plantilla.conf
nano /etc/openvpn/client/make_config.sh
sudo mkdir /etc/openvpn/client/files
chmod 700 /etc/openvpn/client/make_config.sh
./make_config.sh KevinConnect
sudo cp /etc/openvpn/client/files/KevinConnect.ovpn
/home/kevin/Escritorio
cd /home/kevin/Escritorio
sudo chmod 444 KevinConnect.ovpn
```


repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

```
Nota: Generado con OpenVPN v2.6.3
```

4.3.2. Comandos de configuración del Servidor VPN Master_GSVPN

El servidor se ejecuta en la dirección IP, en el puerto utilizando el protocolo UDP. El servidor utiliza el dispositivo de red TUN y está autenticado con un certificado de CA. El servidor utiliza el cifrado AES-256-GCM y el algoritmo de autenticación SHA512.

```
local 179.7.225.194
port 1194
proto udp
dev tun
ca ca.crt
cert Master_GSVPN.crt
key Master_GSVPN.key
dh none
topology subnet
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist /var/log/openvpn/ipp.txt
push "redirect-gateway def1 bypass-dhcp"
keepalive 10 120
tls-crypt ta.key
cipher AES-256-GCM
auth SHA512
max-clients 100
user nobody
group nogroup
persist-key
persist-tun
status /var/log/openvpn/openvpn-status.log
verb 3
explicit-exit-notify 1
```

```
Nota: Generado con OpenVPN v2.6.3
```

4.3.3. Comandos de configuración de Clientes (KevinConnect)

El cliente se conecta al servidor en la dirección IP, utilizando el protocolo UDP. El cliente utiliza el dispositivo de red TUN y está autenticado con el certificado del servidor. Usando el cifrado AES-256-GCM y el algoritmo de autenticación de cifrado de SHA512.

```
client
remote my-server1 1194
proto udp
dev tun
resolv-retry infinite
```


repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

```
nobind
user nobody
group nogroup
persist-key
persist-tun
remote-cert-tls server
cipher AES-256-GCM
auth SHA512
verb 3
```

Nota: Generado con OpenVPN v2.6.3

4.3.4. Evaluación de la VPN bajo Pruebas de Hipótesis de instrumento

Los colaboradores de GS son quienes usarán la VPN, por tanto, para evaluar que la VPN mejora la seguridad de la información, es que se creó el instrumento *"Encuesta sobre apreciación de la seguridad de la información"*, véase (Anexo C: Instrumento de investigación), el cual se sometió a prueba de alfa de Cronbach, que es un índice de confiabilidad para instrumentos, que intenta medir la consistencia interna inter preguntas, misma que se evidencia en el Anexo 2 (Prueba de confiabilidad).

$$\alpha = \frac{K}{K}\left(\frac{1 - \sum_{i=1}^{k} S_i^2}{S_T^2}\right)$$

$\alpha =$ 0.85 en Pre-Test

$\alpha =$ 0.73 en Post Test

4.3.4.1. Prueba de Hipótesis al Objetivo General

En base al objetivo general se intenta demostrar que la VPN desarrollada mejoró la seguridad de la información en GS Constructora y Maquinarias. Para ello se planteará la hipótesis nula y de investigación:

Hipótesis Nula:

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

(H_o): El Diseño de una Red Privada Virtual (VPN) Bajo Software Libre no mejora la seguridad de la información en la Empresa GS Maquinarias y Constructora E.I.R.L., Juliaca, 2023.

$$H_0 : p \geq 0.05$$

Hipótesis de Investigación:

(H_i): El Diseño de una Red Privada Virtual (VPN) Bajo Software Libre mejora la seguridad de la información en la Empresa GS Maquinarias y Constructora E.I.R.L., Juliaca, 2023

$$H_i : p < 0.05$$

Habiendo definido la hipótesis nula y de investigación se probará con el estadístico de Wilcoxon para comparar los resultados de entrada con los de salida (Pre Test vs Post Test) al 95% de confiabilidad y un margen de error del 5%. Para una muestra de 14 colaboradores y revisando la significancia asintótica bilateral es menor a 0.05 propuesta en la hipótesis nula y de investigación como regla de decisión.

Tabla 8

Estadístico descriptivo del objetivo general

Estadísticos descriptivos

	N	Media	Desv. Desviación	Mínimo	Máximo
PreTest	14	22.93	3.562	16	26
PostTest	14	41.50	2.739	36	46

Nota: Elaboración propia generado con SPSS v25.

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

Tabla 9

Prueba de Rangos con Wilcoxon del objetivo general

Rangos

		N	Rango promedio	Suma de rangos
PostTest - PreTest	Rangos negativos	0[a]	.00	.00
	Rangos positivos	14[b]	7.50	105.00
	Empates	0[c]		
	Total	14		

a. PostTest < PreTest

b. PostTest > PreTest

c. PostTest = PreTest

Nota: Elaboración propia generado con SPSS v25

Tabla 10

Estadística de Prueba del objetivo general

Estadísticos de prueba[a]

	PostTest - PreTest
Z	-3.301[b]
Sig. asintótica(bilateral)	.001

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Nota: Elaboración propia generado con SPSS v25

La Tabla descriptiva indica que la media del Post-Test es de 41 y 23 del Pre-Test. Asimismo, en la prueba de rangos de Wilcoxon, fueron positivas y el estadístico de prueba muestra que la significancia es de 0.001 que es menor al 0.05. Lo que indica que existe suficiente evidencia estadística para rechazar la hipótesis nula y aceptar la hipótesis de investigación que menciona que existe mejora en la seguridad de la información.

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

4.3.4.2. Prueba de Hipótesis al Objetivo Específico 1

En base al objetivo general se intenta demostrar que la VPN desarrollada mejoró la seguridad de la información en GS Constructora y Maquinarias. Para ello se planteará la hipótesis nula y de investigación:

Hipótesis Nula:

(H_o): La Red Privada Virtual (VPN) basado en Software Libre no logra optimizar la seguridad de la información en la Empresa GS Maquinarias y Constructora E.I.R.L., Juliaca, 2023.

$$H_0 : p \geq 0.05$$

Hipótesis de Investigación:

(H_i): La Red Privada Virtual (VPN) basado en Software Libre logra optimizar la seguridad de la información en la Empresa GS Maquinarias y Constructora E.I.R.L., Juliaca, 2023.

$$H_i : p < 0.05$$

Después de establecer claramente la hipótesis nula y la hipótesis de investigación, se utilizó el estadístico de Wilcoxon para analizar las diferencias entre los resultados antes y después (Pre Test vs. Post Test) con un nivel de confianza del 95%. Además, al revisar la significancia asintótica de manera bidireccional.

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

Tabla 11

Estadístico descriptivo del objetivo específico 1

Estadísticos descriptivos

	N	Media	Desv. Desviación	Mínimo	Máximo
Pre Seguridad	14	2.71	.469	2	3
Post Seguridad	14	4.64	.497	4	5

Nota: Elaboración propia generado con SPSS v25

Tabla 12

Prueba de Rangos con Wilcoxon del objetivo específico 1

Rangos

		N	Rango promedio	Suma de rangos
Post Seguridad - Pre Seguridad	Rangos negativos	0[a]	.00	.00
	Rangos positivos	14[b]	7.50	105.00
	Empates	0[c]		
	Total	14		

a. Post Seguridad < Pre Seguridad

b. Post Seguridad > Pre Seguridad

c. Post Seguridad = Pre Seguridad

Nota: Elaboración propia generado con SPSS v2

Tabla 13

Estadística de Prueba del objetivo específico 1

Estadísticos de prueba[a]

	Post Seguridad - Pre Seguridad
Z	-3.402[b]
Sig. asintótica(bilateral)	.001

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Nota: Elaboración propia generado con SPSS v25

La Tabla descriptiva indica que la media del Post-Test es de 4.64 y 2.71 del Pre-Test. Asimismo, en la prueba de rangos de Wilcoxon, fueron

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

positivas y el estadístico de prueba muestra que la significancia es de 0.001 que es menor al 0.05. Lo que indica que existe suficiente evidencia estadística para rechazar la hipótesis nula y aceptar la hipótesis de investigación que menciona que existe mejora en la seguridad de la información.

4.3.4.3. Prueba de Hipótesis al Objetivo Específico 2

En base al objetivo general se intenta demostrar que la VPN desarrollada mejoró la confiabilidad de la información en GS Constructora y Maquinarias. Para ello se planteará la hipótesis nula y de investigación:

Hipótesis Nula:

(H_o): La Red Privada Virtual (VPN) basado en Software Libre no logra mejorar de la confiabilidad de la información en la Empresa GS Maquinarias y Constructora E.I.R.L., Juliaca, 2023.

$$H_0 : p \geq 0.05$$

Hipótesis de Investigación:

(H_i): La Red Privada Virtual (VPN) basado en Software Libre logra mejorar de la confiabilidad de la información en la Empresa GS Maquinarias y Constructora E.I.R.L., Juliaca, 2023.

$$H_i : p < 0.05$$

Habiendo definido la hipótesis nula y de investigación se probó con el estadístico de Wilcoxon para comparar los resultados de entrada con los de salida (Pre Test vs Post Test) al 95% de confiabilidad y un margen de error del 5%. Para una muestra de 14 colaboradores y revisando la

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

significancia asintótica bilateral es menor a 0.05 propuesta en la hipótesis nula y de investigación como regla de decisión.

Tabla 14

Estadístico descriptivo del objetivo específico 2

Estadísticos descriptivos

	N	Media	Desv. Desviación	Mínimo	Máximo
Pre Confiabilidad	14	2.07	.475	1	3
Post Confiabilidad	14	4.21	.426	4	5

Nota: Elaboración propia generado con SPSS v25

Tabla 15

Prueba de Rangos con Wilcoxon del objetivo específico 2

Rangos

		N	Rango promedio	Suma de rangos
Post Confiabilidad - Pre Confiabilidad	Rangos negativos	0[a]	.00	.00
	Rangos positivos	14[b]	7.50	105.00
	Empates	0[c]		
	Total	14		

a. Post Confiabilidad < Pre Confiabilidad
b. Post Confiabilidad > Pre Confiabilidad
c. Post Confiabilidad = Pre Confiabilidad

Nota: Elaboración propia generado con SPSS v25

Tabla 16

Estadística de Prueba del objetivo específico 2

Estadísticos de prueba[a]

	Post Confiabilidad - Pre Confiabilidad
Z	-3.376[b]
Sig. asintótica(bilateral)	.001

a. Prueba de rangos con signo de Wilcoxon

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

b. Se basa en rangos negativos.

Nota: Elaboración propia generado con SPSS v25

La Tabla descriptiva indica que la media del Post-Test es de 4.21 y 2.07 del Pre-Test. Asimismo, en la prueba de rangos de Wilcoxon, fueron positivas y el estadístico de prueba muestra que la significancia es de 0.001 que es menor al 0.05 por lo que rechazamos la hipótesis nula.

4.3.4.4. Prueba de Hipótesis al Objetivo Específico 3

En base al objetivo general se intenta demostrar que la VPN desarrollada mejoró la escalabilidad de la información en GS Constructora y Maquinarias. Para ello se planteará la hipótesis nula y de investigación:

Hipótesis Nula:

(H_o): La Red Privada Virtual (VPN) basado en Software Libre no influye positivamente en la escalabilidad de la información en la Empresa GS Maquinarias y Constructora E.I.R.L., Juliaca, 2023.

$$H_0 : p \geq 0.05$$

Hipótesis de Investigación:

(H_i): La Red Privada Virtual (VPN) basado en Software Libre influye positivamente en la escalabilidad de la información en la Empresa GS Maquinarias y Constructora E.I.R.L., Juliaca, 2023.

$$H_i : p < 0.05$$

Después de haber definido de manera precisa tanto la hipótesis nula como la hipótesis de investigación, se empleó el estadístico de Wilcoxon para examinar las diferencias entre los resultados obtenidos antes y después (Pre Test vs. Post Test) con un nivel de confianza del 95% y un margen de

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

error del 5%. Este análisis se llevará a cabo utilizando una muestra compuesta por 14 colaboradores. Además, al evaluar la significancia asintótica en ambas direcciones, se ha fijado un umbral de significación por debajo del 0.05, el cual servirá como criterio para tomar decisiones en relación tanto a la hipótesis nula como a la hipótesis de investigación.

Tabla 17

Estadístico descriptivo del objetivo específico 3

Estadísticos descriptivos

	N	Media	Desv. Desviación	Mínimo	Máximo
Pre Escalabilidad	14	1.93	.267	1	2
Post Escalabilidad	14	4.21	.426	4	5

Nota: Elaboración propia generado con SPSS v25

Tabla 18

Prueba de Rangos con Wilcoxon del objetivo específico 3

Rangos

		N	Rango promedio	Suma de rangos
Post Escalabilidad - Pre Escalabilidad	Rangos negativos	0[a]	.00	.00
	Rangos positivos	14[b]	7.50	105.00
	Empates	0[c]		
	Total	14		

a. Post Escalabilidad < Pre Escalabilidad

b. Post Escalabilidad > Pre Escalabilidad

c. Post Escalabilidad = Pre Escalabilidad

Nota: Elaboración propia generado con SPSS v25

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

Tabla 19

Estadística de Prueba del objetivo específico 3

Estadísticos de prueba[a]	
	Post Escalabilidad - Pre Escalabilidad
Z	-3.448[b]
Sig. asintótica(bilateral)	.001

Nota: Elaboración propia generado con SPSS v25

4.4. EVALUACIÓN DEL RETORNO DE INVERSIÓN DE LA VPN

4.4.1. Presupuestos de equipos

Tabla 20

Lista de equipos a comprar

Equipo/Hardware	Descripción	Modelo	Precio (S/.)
Router Mikrotik	Router principal que gestionará la VPN y las conexiones remotas.	Mikrotik RB750Gr3	400.00
UPS (Sistema de alimentación ininterrumpida)	Protege contra cortes de energía y asegura la disponibilidad.	APC Back-UPS BX600C	500.00
Rack o Gabinete	Para alojar y organizar los equipos de manera adecuada.	Varios fabricantes	300.00
Servidor NAS	Servidor de almacenamiento con capacidad de hasta 20 terabytes, expansible en SSD y HDD con velocidad de transferencia de Lectura de 680 Mb/s y 530 Mb/s de Escritura, 8GB RAM DDR4, instalable Docker como Sistema Operativo.	Servidor NAS (QNAP TS-453D-4G)	4,800.00

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

Cableado Estructural	Canaletas, bandejas y otros accesorios para organizar los cables de manera ordenada.	Varios fabricantes	400.00
Costo de Instalación	Instalación de equipos y configuración inicial.	-	440.00
TOTAL			**6,840.00**

Nota: Elaboración propia bajo requerimientos

En la Tabla 19 se muestra los equipos necesarios para la instalación del VPN, dado que en la empresa no cuentan con estos equipos.

4.4.2. Presupuestos de software

Tabla 21

Lista de Software OpenSource

Software	Descripción	Costo
OpenVPN	Para configurar y administrar la VPN.	Gratuito
Samba	Para configurar carpetas compartidas en la red local.	Gratuito
MySQL o PostgreSQL	Para alojar bases de datos utilizadas por aplicaciones.	Gratuito
Apache, Nginx o Caddy	Servidores web para alojar sitios y aplicaciones web.	Gratuito
Docker	Para crear y gestionar contenedores de aplicaciones.	Gratuito
Git	Para gestionar el control de versiones de proyectos.	Gratuito
SSH Server	Para administrar el NAS de forma remota de manera segura.	Gratuito

Nota: Elaboración propia bajo requerimientos

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

4.4.3. Presupuestos de servicio

Tabla 22

Servicios Mensuales de la VPN

Servicio	Descripción	Costo Mensual S/.
Mantenimiento del Servidor NAS, Monitoreo y Soporte Remoto	Actualizaciones de software, parches de seguridad, monitorización, y soporte técnico. Servicio de monitoreo constante y soporte técnico remoto para resolver problemas.	200.00
Capacitación al personal	Capacitación y mantenimiento a personal en el uso de la VPN	50.00
TOTAL		**250.00**

Nota: Elaboración propia bajo requerimientos.

4.4.4. Rentabilidad

Para determinar la rentabilidad del proyecto se realizó cálculos como el VAN y el TIR, los cuales nos darán de forma detallada la rentabilidad de este proyecto. La empresa destina aproximadamente $1000 dólares al mes, este gasto se pude mitigar de modo que la empresa pueda ahorrar el dinero destinado en ello.

4.4.5. Inversión total del proyecto

Tabla 23

Inversión total de la VPN

Inversión total del proyecto			
Ítem	Detalle		Total
1	Inversión fija	S/	7,090.00
2	Imprevistos al 5%	S/	342.00
Total		**S/**	**7,432.00**

Nota: Elaboración propia bajo requerimientos

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

4.4.6. Cálculo de VAN

El valor neto actual de los flujos, esto nos muestra un panorama de cuanto se puede ganar o perder al implementar la VPN en la empresa. Para poder hallarlo utilizamos la siguiente formula.

$$VAN = \sum_{t=1}^{n} \frac{FN_t}{(1+k)^t} - I_0$$

Donde:

FN_t = flujos netos de cada mes

I_0 = es el valor del desembolso inicial de la inversión

n = es el numero periodos considerados

k = es la tasa de interés

$$VAN = \frac{37400}{(1+0.1)} - 7432$$

$$VAN = 26{,}568.00$$

Como el VAN salió 26,568.00 siendo este mayor a 0, entonces podemos indicar que el proyecto es viable, porque genera un beneficio.

4.4.7. Tasa de Interna de Retorno (TIR)

La tasa de descuento o rentabilidad de una inversión representa el porcentaje de ganancia o pérdida que generará la inversión en relación con los fondos que permanezcan en el proyecto sin retirar. Se calcula mediante la siguiente fórmula:

$$0 = \sum_{t=0}^{n} \frac{FN_t}{(1+TIR)^t}$$

Donde:

FN_t = representa los flujos netos cada periodo t

n = es el número de periodos considerados

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

Reemplazando obtenemos que:

$$0 = -7432 + \frac{37400}{(1 + TIR)}$$

$$TIR = 0.44$$

Quiere decir que el proyecto tiene una rentabilidad del 44%, por lo tanto, se determina que el presente proyecto es viable.

4.4.8. El periodo de Recuperación (PR)

Tabla 24

Periodo de Recuperación mensual

	PR			
Mes	Flujo económico			Acumulado
mes 0	S/	7,432.00	-S/	7,432.00
mes 1	S/	3,400.00	-S/	4,032.00
mes 2	S/	3,400.00	-S/	632.00
mes 3	S/	3,400.00	S/	2,768.00
mes 4	S/	3,400.00	S/	6,168.00
mes 5	S/	3,400.00	S/	9,568.00
mes 6	S/	3,400.00	S/	12,968.00
mes 7	S/	3,400.00	S/	16,368.00
mes 8	S/	3,400.00	S/	19,768.00
mes 9	S/	3,400.00	S/	23,168.00
mes 10	S/	3,400.00	S/	26,568.00
mes 11	S/	3,400.00	S/	29,968.00

Nota: Elaboración propia.

En la Tabla podemos observar que el periodo de recuperación calculado en meses, nos indica que la inversión inicial se recupera a los 2 meces y 4 días, a partir de 2 meses y el 5to día ya empieza a generar ingresos (ahorro a la empresa).

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

4.5. DISCUSIÓN

El diseño de la Red Privada Virtual basado en software libre demostró mejora en la seguridad de la información pasando de Malo-Regular a ser evaluado al 93% como Bueno gracias al diseño de la VPN. Del mismo modo, se calculó la significancia bilateral con la prueba de Wilcoxon con un valor de 0.001 que es menor a 0.05 demostrando la mejora a nivel de seguridad, confiabilidad y escalabilidad.

Estos resultados encontrados tienen similitud con la VPN desarrollada por Marcelo (2021), quien concluye que su VPN logró conectar remotamente a los empleados de COMISION FULBRIGHT DEL ECUADOR habiendo usado como SO del servidor Linux CentoOS, Firewalld, SquidProxy y OpenVPN con solamente tener acceso a Internet desde cualquier punto. Esto demuestra que el uso de Software Libre tanto en el sistema operativo como en la VPN son seguros, confiables y escalables. Del mismo modo existe similitud con Lazarte (2022), quien demostró que usar OpenVPN otorga seguridad, confiabilidad y escalabilidad en DIRESA Lima centro, donde logró limitar el uso malintencionado de la red denegando el acceso de Internet a los trabajadores que daban mal uso de la red.

En tanto que, Hernández y otros (2021) demostraron que la metodología Top-Down es recomendable en cuanto soluciones de redes se trata. Del mismo modo que, Montes de Oca & Ramos (2021) demostró que el rediseño de la topología de la red lógica mostraba la carga de datos y los cuellos de botella. Que bajo un entrelazado de conexiones entre Switches y la colocación de 2 routers centrales lograba que la casi completa disponibilidad de la red a un 98%. Estos resultados son similares con el presente estudio ya que al rediseñar la topología de la red se evidenció una mejor distribución de carga de datos con la incorporación de un servidor NAS junto a la VPN que está conectado a una

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

UPS lo que asegura la disponibilidad constante del servidor a pesar de los cortes de luz u otros inconvenientes.

Garcia (2021), utilizó el tipo de seguridad IPSec, el cual ofrece seguridad duradera y estable en la capa 3 del modelo OSI que tiene 2 protocolos de seguridad como EPS y AH, que también soporta muchos algoritmos criptográficos del momento. Este tipo de seguridad. Estas capas de seguridad son importantes porque a mayor cantidad de protocolos es más difícil para atacantes. Del mismo modo, en este estudio se utilizó el TLS Crypt, el cifrado AES-256-GCM y autenticación SHA512. Es gracias a estas capas y protocolos de seguridad que una VPN logra tener la seguridad necesaria. Respecto a la confiabilidad de una VPN Carrión (2018), muestra su preocupación con que los trabajadores del sector público mencionan que estos no conocen buenas políticas de seguridad y todo aquello con lo que refiere al uso de llaves, claves o diversos maneras prácticas y confiables de acceso y uso de recursos tecnológicos como los son las VPN. Esto refleja el similar comportamiento de los colaboradores de GS entiendan claramente que la criptografía es segura, pero no comprenden completamente cómo funcionan. En tanto que Casanova (2020), logró diseñar un prototipo de VPN para empresas de bajos recursos reutilizando equipos con los que ya se cuenta. Sin olvidar que, con los años, las empresas siempre demandan más equipos, más personal, del mismo modo que la cantidad de archivos que se transmiten aumenta.

Respecto a la inversión de estas tecnologías De la cruz Bernilla & Vera (2019), obtuvieron un Periodo de Retorno de 1 año de un presupuesto total de 13 mil soles, un VAN de 2618 soles y un TIR del 31% demostrando que la inversión tiene rentabilidad siendo superior al 10% del VAN. Estos resultados denotan similitud con los obtenidos de este estudio donde se evidencia la viabilidad de la inversión con un presupuesto total de

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

6840 y 250 soles de manteamiento se obtuvo un VAN de 26% y un TIR de 44%, y con un PR de 2 meses y 4 días. Esto demuestra que el PR puede afectarse significativamente en cuanto mayor sea la inversión. Por ello, no se puede estimar una inversión mayor de lo que una empresa pueda permitirse lo que sugiere que existe un límite de inversión sobre una propuesta de mejora de la red y lo sistemas que incluyen en un proyecto.

Todos estos hallazgos esbozan que las tecnologías que usan las empresas del sector privado pueden ser diversas, algunas usan servicio Cloud y sistemas de información pagando montos mensuales o anuales para su uso por servicio de almacenamiento como lo hace GS. No olvidemos que las políticas de privacidad de empresas como Google y Microsoft pueden afectar la privacidad de la información haciendo uso de ellas. Es por ello que futuros investigadores realizan estudios de políticas de privacidad y como está afecta o influyen en la privacidad de personas y empresas. Otro aspecto interesante son las nuevas maneras de seguridad biométricas como otro medio de seguridad de autenticación.

Las limitaciones de la investigación en el contexto de la propuesta de mejora de implementar una VPN en la empresa privada GS Maquinarias y Constructora E.I.R.L., Juliaca. Que tiene como director ejecutivo el Sr. Abelardo son importantes de tener en cuenta. En primer lugar, se ha identificado que la restricción más significativa está relacionada con la confidencialidad y seguridad de la información que se intercambia en la empresa actualmente. El director ejecutivo ha expresado su preocupación por proteger la información sensible de la empresa de manera privada. Además, debido a que la empresa opera en proyectos de licitación en diferentes ubicaciones geográficas, la limitación geográfica también es un factor a tener en cuenta. Algunos proyectos pueden estar ubicados en áreas remotas o de difícil acceso, lo que podría dificultar el traslado y

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

la implementación de la VPN en sitios alejados y fuera de cobertura. Esto implica que la prueba de la VPN puede requerir un esfuerzo adicional en términos de logística y transporte para acceder a estos lugares y evaluar su funcionamiento. Por otro lado, cuando se hizo la verificación de las instalaciones no se encontró un servidor propio, del mismo modo, no se encontró algún personal jefe de tecnología o a fines quien maneje toda la información de datos en la empresa. Lo que conllevo en cierto modo a explicar a los colaboradores de qué es una VPN y como está debe funcionar. Del mismo modo el personal tuvo dificultades para comprender el funcionamiento de esta tecnología.

Más allá de la empresa GS, este estudio es relevante para las instituciones públicas quienes son sujeto de ataque como los ocurridos con el grupo Guacamaya de México donde el Ejército peruano sufrió el mayor hackeo de su historia en el 2022. Del mismo modo, a las empresas privadas que buscan el crecimiento de su poder logístico y de conocimientos que los hacen enfrentar a la competencia año tras año con mejores medidas de seguridad, confiabilidad y escalabilidad.

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

V. CONCLUSIONES

PRIMERA: El diseño de la VPN Master_GSVPN mejoró la seguridad de la información pasando de ser Malo-Regular a Bueno a un 93%. Asimismo, la significancia bilateral con la prueba de Wilcoxon tuvo un valor de 0.001 que es menor a 0.05 evidenciando que existe suficiente evidencia estadística para afirma que la VPN mejoró la seguridad de la información misma que fue aceptada por los 14 colaboradores, lo que se entiende que les pareció seguro, confiable y escalable.

SEGUNDA: El análisis de requerimientos bajo la metodología Top-Down evidenció la ineficiencia de seguridad porque se venía haciendo uso de un servicio de almacenamiento en la nube para el acceso a recurso de manera remota, lo que se traduce en inseguridad en la transferencia de datos, un pago mensual a Power BI de 1000 dólares mensuales, la inexistencia de un servidor que aloje bases de datos y sistemas de información propios de la empresa, la falta de políticas de seguridad y la falta de un profesional encargado en el área de tecnologías dentro de la empresa.

TERCERO: Gracias al rediseño lógico de la red se logró demostrar un buen proceso de autenticación, recuperación y accesibilidad de llaves de los colaboradores y gracias al cifrado robusto AES-256-GCM junto con la autenticación criptográfica SHA512, del mismo modo, la incorporación del servidor NAS donde se aloja la VPN $Master\_GS$, también almacena bases de datos y sistemas de información que permite conexiones simultaneas, transferencia masiva de datos en alta velocidad, el acceso a recursos de

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

manera remota desde cualquier dispositivo, todo alimentado por un UPS que mantiene el sistema disponible en todo momento.

CUARTO: Se logró documentar la VPN tanto para la configuración del servidor Master_GS como para clientes, sin olvidar el Script que genera llaves únicas a partir de ‘ca’, ‘crt’, ‘csr’, ‘key’ de cada colaborador. Asimismo, los colaboradores evaluaron esta tecnología con el PreTest versus el PosTest, demostrando que se obtuvo una mejora significativa a nivel de seguridad, confiabilidad y escalabilidad con una significancia bilateral de 0.001 en las 3 dimensiones bajo el estadístico no paramétrico de Wilcoxon. Asimismo, se logra ser escalable ya que el servidor NAS está diseñado para aumentar su capacidad de almacenaje o poder ser trasladada a un servidor de mayor demanda.

QUINTO: De acuerdo a la viabilidad de la inversión se obtuvo un VAN de 26 560 nuevos soles lo que significa que el costo de la inversión se recuperará en un plazo menor a un año, ya que el VAN es positivo. Asimismo, con un TIR de 0.44, la inversión generará un retorno de 44% sobre el costo inicial. En tanto que el periodo de recuperación se calculó en 2 meses y 4 días, lo que demuestra que bajo estas herramientas empresariales el proyecto es viable y rentable porque ayudará con el ahorro, pasando de gastar 1000 dólares mensuales a 250 soles mensuales haciendo uso de estas tecnologías que aparte de mejorar la seguridad de la información también ayudan con los egresos de la empresa GS.

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

VI. RECOMENDACIONES

PRIMERA: A los equipos de tecnologías de las empresas privadas que hacen uso de VPN en su organización a capacitar a todo su personal sobre posibles ataques de ingeniería social, ya que por sí misma la seguridad criptográfica ha demostrado ser altamente segura, misma que se usa en instituciones del estado peruano sumado a eso el permiso de acceso con la IP y la dirección física MAC para cada colaborador que accede a la red. Es así que los atacantes ante la poca posibilidad de opciones de ataque frente a una VPN en la que se requiere una llave de acceso para atacar, es que se recurren a otros métodos sociales.

SEGUNDA: A las organizaciones que implementan VPN se enfoquen en la elección de protocolos de seguridad duraderos como IPSec y utilicen cifrado robusto como AES-256-GCM, junto con autenticación sólida como SHA512, para garantizar la máxima seguridad en sus redes virtuales privadas como el uso de un firewall y una zona desmilitarizada para denegar todo tipo de ataques antes de entrar a la red local de la empresa.

TERCERO: A las organizaciones que implementan VPN brinden capacitación y concienciación adecuadas a sus colaboradores sobre la importancia de las políticas de seguridad y el funcionamiento de tecnologías como las VPN frente a distintos tipos de ataques, el uso correcto de las llaves que se les otorga. Esto garantizará una mayor confiabilidad en el uso de recursos tecnológicos y una comprensión más sólida de la criptografía subyacente en las VPN.

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

CUARTO: A los líderes de tecnología que al diseñar sistemas de información, incluyan una visión de escalabilidad para anticipar futuras demandas de recursos. Esto es especialmente relevante en el caso de VPN, donde el crecimiento en equipos, personal y la transmisión de archivos pueden ser significativos con el tiempo.

QUINTO: A las empresas proveedoras de servicios tecnológicos de VPN, Sistemas de información y seguridad informática a verificar el total de inversión que la empresa está dispuesta a gastar, recopilar los gastos mensuales y usar herramientas financieras como el VAN, TIR, PR para proveer soluciones tecnológicas rentables y que no excedan la inversión que tiene la empresa en cuestión utilizando buenas prácticas de seguridad con el uso de Software Libre reconocidos que no presentes vulneraciones a lo largo de los años.

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

VII. REFERENCIAS BIBLIOGRÁFICAS

Agudelo, G., Aigneren, M., & Ruiz, J. (2008). *Diseños De Investigación Experimental Y No-Experimental. Centro de Estudios de Opinión*, 1–46. http://bibliotecadigital.udea.edu.co/dspace/bitstream/10495/2622/1/AgudeloGabriel_disenosinvestigacionexperimental.pdf

Ahmad, N., Wei, L. M., & Hairol Jabbar, M. (2018). *Advanced Encryption Standard with Galois Counter Mode using Field Programmable Gate Array*. *Journal of Physics: Conference Series*, *1019*(1). https://doi.org/10.1088/1742-6596/1019/1/012008

Álvarez D., D., Jorquera C., C., Sepúlveda J., G., & Zamora E., C. (2014). *Redes Privadas Virtuales (VPN)*. 9. http://profesores.elo.utfsm.cl/~agv/elo322/1s14/projects/reports/G20/Redes Privadas Virtuales %28VPN%29.pdf

Amaya, L. E. (2018). *Capítulo 3 VPN*. *En VPN (pp. 1–21)*. Universidad Autónoma de mëxico. http://www.ptolomeo.unam.mx:8080/jspui/bitstream/132.248.52.100/204/6/A6.pdf

Andrés, F., & Herías, C. (2009). *Manual de la Práctica 2 : Túneles y Redes Virtuales Privadas*. https://rua.ua.es/dspace/bitstream/10045/11323/1/IEA-STD9186-P2.pdf

Anónimo. (2012). *Practica Redes VLAN y Enrutamientos (Estático y Dinámico)*. https://juannava64.files.wordpress.com/2012/02/par-practica-redes-vlan-y-enrutamientos-a_b_c.pdf

Araya, G. (2017). *Enrutamiento: Conceptos Fundamentales.* En Docplayer.Es. https://docplayer.es/50079045-Enrutamiento-conceptos-fundamentales.html

Arias Gonzáles, J. L., Holgado Tisoc, J., Tafur Pittman, T. L., & Vasquez Pauca, M. J. (2022). *Metodología de la investigación: El método ARIAS para realizar un proyecto de tesis.* En Repositorio Concytec (Primera Ed). https://repositorio.concytec.gob.pe/bitstream/20.500.12390/3109/1/2022_Metodologia_de_la_investigacion_El_metodo_

Avila, A., & Echeverria, T. (2022). *Directrices y políticas de firewall*. Ingente Americana, 2(2), 15–28. https://doi.org/10.21803/ingecana.2.2.496

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

Basque Cybersecurity Centre. (2023). *Sistema de Prevención de Pérdida de datos DLP o Data Loss Prevention*. https://www.ciberseguridad.eus/sites/default/files/2022-04/dlp_es.pdf

Bonet, E. V. (2004). *Redes privadas virtuales*. Ingeniería y Región, 3, 107–111. https://doi.org/10.25054/22161325.864

Carrión, G. (2018). *Metodología adaptativa basada en un modelo de seguridad informática en redes provadas virtuales para mejorar el intercambio de información académica contextualizada en entornos de conexiones públicas* [Universidad Señor de Sipán]. https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/4723/CARRION BARCO GILBERTO.pdf

Carrión, O. (2020). *Criptografía para principiantes : método Julio César y Vinegère*. En Boletín SAPM (pp. 13–15). http://funes.uniandes.edu.co/24505/1/Carrión2020Criptografía.pdf

Casanova, A. (2020). *Diseño de una red privada virtual orientada al teletrabajo de organizaciones con escasos recursos económicos por la coyuntura del COVID-19.* Repositorio UNTELS, 110. https://repositorio.untels.edu.pe/jspui/bitstream/123456789/586/1/T088A_41900029_T.pdf

CCIT. (2008). *Unión Internacional De Telecomunicaciones La Guia-Marco De Autenticacion*.

CCN. (2021). *Guía de Seguridad de las TIC Taxonomía de productos STIC- Anexo C . 1 : Herramientas IDS , IPS y AntiDDoS.*

Centro Criptológico Nacional. (2018). *Recomendaciones de Seguridad para VPN IPSec 1. INTRODUCCIÓN A LAS VPN*. https://oc.ccn.cni.es

Centro Criptológico Nacional. (2022). *Guía de Seguridad de las TIC. CCN-STIC-836. Seguridad en Redes Privadas Virtuales (VPN)*. 8. https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/2299-ccn-stic-836-seguridad-en-vpn-en-el-marco-del-ens/file.html

Cisco. (2018). *Configuración del concentrador Cisco VPN 3000 y de la red asociada al*

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

cliente PGP Configure el Network Associates PGP Client para Conectarse al.

CISCO. (2015). *Conexión de Red privada virtual (VPN) de la configuración usando el asistente para la configuración en el router de las RV34x Series*. https://www.cisco.com/c/es_mx/support/docs/smb/routers/cisco-rv-series-small-business-routers/smb5552-configure-virtual-private-network-vpn-connection-using-the-s.pdf

CISCO. (2019a). *Capítulo 3 : Protocolos y comunicación de red*. En CCNA routing y switching (Vol. 6). https://www.uv.mx/personal/angelperez/files/2019/02/CCNA_ITN_Chp3.pdf

CISCO. (2019b). *Cisco VPN Sitio-a-Sitio con Certificado Digital*.

CITRIX. (2022). *Los 6 aspectos escenciales que debe tener un WAF para lograr la eficacia en la seguridad de las aplicaciones*.

Código de Ética del Colegio de Ingenieros del Perú, Colegio De Ingenieros Del Perú 1 (2018). http://cdlima.org.pe/wp-content/uploads/2018/04/CÓDIGO-DE-ÉTICA-REVISIÓN-2018.pdf

Cornejo, E., Matamala, G., Díaz, M., & Rojas, M. (2019). *Redes privadas virtuales (VPN), una respuesta a lo limitado por la ubicación*. http://profesores.elo.utfsm.cl/~agv/elo322/1s19/projects/reports/VPN.pdf

Cueva, T. T., & Mishahuaman, X. X. (2019). *Metodología top down network design para elevar la eficiencia de la red de datos en la Municipalidad Provincial de Huánuco – 2019 [Universidad Nacional Hermilio Valdizán]*. En Repositorio UNHV. http://repositorio.unheval.edu.pe/handle/20.500.13080/5525

De la cruz Bernilla, S., & Vera, jean R. S. (2019). *Implementación de una VPN con open source para la gestión de aplicaciones de intranet en la Universidad Nacional Pedro Ruiz Gallo [Universidad Nacional Pedro Ruiz Gallo]*. En Respositorio UNPRG. https://hdl.handle.net/20.500.12893/8266

Departamento de Sistemas Telemáticos y Computación. (2014). OpenVPN. *Departamento de Sistemas Telem´aticos y Computaci´on*, 1–32. https://gsyc.urjc.es/~mortuno/sro/openvpn

Domínguez Gómez, J. (2018). *Criptografía: Función SHA-256.* Publicaciones Bit2me,

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

0.01, 18. https://academy.bit2me.com/wp-content/uploads/2019/10/Criptography_SHA_256_es.pdf

Espinoza, E., & Toscano, D. (2015). *Metodología de la investigación técnica y educativa*. En Ediciones UTMACH (1ra Edició, Número p). Ediciones UTMACH.

Espitia, A., & López, J. (2020). *Diseño de nueva arquitectura de red para la empresa colombiana ENTERSOFT S.A.S. En GEPCOMM*. Universidad Cooperativa de Colombia.

Estriégana, R. (2014). *Redes Privadas Virtuales (VPN)*. http://profesores.elo.utfsm.cl/~agv/elo322/1s14/projects/reports/G20/Redes Privadas Virtuales %28VPN%29.pdf

EVIDIAN IAM. (2022). *Los 7 métodos de Autentificación más utilizados*. https://www.evidian.com/pdf/wp-strongauth-es.pdf

FSCommunity. (2021). *¿Cuál es la diferencia entre modelo OSI y modelo TCP/IP?* https://community.fs.com/es/blog/tcpip-vs-osi-whats-the-difference-between-the-two-models.html

Garcia, D. (2021). *Implementación de una VPN tipo cliente para una entidad financiera* [Universidad Tecnológica del Perú]. https://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/4997/D.Garcia_Trabajo_de_Suficiencia_Profesional_Titulo_Profesional_2021.pdf?sequence=1&isAllowed=y

Guerreo, G. (2009). *Diseño y análisis de soluciones seguras vpn basadas en software libre* [Universidad Central de Venezuela]. http://mendillo.info/seguridad/tesis/Guerrero.pdf

Hernández Hipólito, J., de la Cruz Gámez, E., Cadena Mendoza, E., & Montero Valverde, J. A. (2021). *Propuesta de diseño e implementación de una red para proporcionar servicio de internet inalámbrico con garantía de QOS en habitaciones de un hotel*. Programación Matemática y Software, 13(3), 31–38. https://doi.org/10.30973/progmat/2021.13.1/4

Hernández, R. (2014). *Metodología de la Investigación* (6ta Edició). McGRAW-HILL.

IBM. (2010). *Redes privadas virtuales de seguridad*.

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

https://www.ibm.com/docs/es/ssw_ibm_i_71/rzaja/rzaja.pdf

INCIBE. (2019). *Qué es una DMZ y cómo te puede ayudar a proteger tu empresa*. Blogs. https://www.incibe.es/empresas/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa

Jarauta, J., Sierra, J., & Palacios, R. (2006). *Seguridad Informática Tema 12 : Infraestructuras de Clave Pública-PKI*. https://pascua.iit.comillas.edu/palacios/seguridad/cap08.pdf

Jimenez, R. (2014). *Seguridad en redes vpn*. universidad piloto de Colombia, 5. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2876/00001896.pdf?sequence=1&isAllowed=y

KALWEIT ITS. (2022). *Visión de la economía de la seguridad desde la perspectiva de Ross Anderson, Tyler Moore y otros*. Economía. https://kalweit-its.de/es/vision-de-la-economia-de-la-seguridad-de-la-informacion-desde-la-perspectiva-de-ross-anderson-tyler-moore-y-otros/#

KPMG. (2023). *Un nuevo enfoque sobre Ciber Seguridad*. https://assets.kpmg.com/content/dam/kpmg/pdf/2016/07/feel-free-cyber-security-brochure-español.pdf

Kuthnik, T., Martin, D., Gerardi, T., Cortes, I., & Vergara, A. (2019). *La Criptografía y la Seguridad Informática*. Publicaciones de Sistemas deinformación, 7. https://grupogemis.com.ar/wp-content/uploads/2019/05/SyO_J_CriptografiaSegInf.pdf

Lazarte, D. (2022). *Diseño de una red privada virtual (VPN) basada en software libre para la mejora de la seguridad de la información de la jurisdicción de la dirección de redes integradas de salud Lima Centro [Universidad Cesar Vallejo]*. En Respositotio UCV. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/50737/Cusma_GM-SD.pdf?sequence=1&isAllowed=y

León, D. G., & Rodriguez, J. carlos. (2021). *Formulación e Imlementación de una plan de concientización de seguridad de la información hacia los funcionarios de la Alcaldía de Sopó [Universidad Piloto de Colombia]*. En Publicacion en seguridad informática.

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

http://journal.unilak.ac.id/index.php/JIEB/article/view/3845%0Ahttp://dspace.uc.ac.id/handle/123456789/1288

Madela, M. (2017). *Data brokers, mercaderes de la intimidad*. Blog AUDEA. https://www.audea.com/data-brokersutm_sourceblogutm_mediumblogutm_contentlegal/

ManageEngine. (2022). *Futuras tendencias en la Gestión de Identidades y Accesos*.

Marcelo, L. (2021). *Estudio para la Implementación de una Red Privada Virtual (VPN) utilizando herramientas de Software Libre. Caso de estudio de la Comisión Fulbright del Ecuador*. Repositorio PUCE, 153. http://repositorio.puce.edu.ec/bitstream/handle/22000/18899/MTI TESIS_Quishpe Iza Luis Marcelo_2021-03-29.pdf

Marchand, W., & Rueda, E. (2020). *Encryption with TLS Protocol version 1 . 2 and Web*. Editoriales Rosario, 172–179.

Martínez, J. (2015). *Seguridad de la Información en pequeñas y medianas empresas (pymes). Polux - Universidad Piloto de Colombia, 8.* http://polux.unipiloto.edu.co:8080/00002332.pdf

Medina, T., & Miranda, A. (2015). *Comparison of Algorithms Based Cryptography Symmetric DES, AES and 3DES*. Revista Mundo Fesc, 9, 14–21.

Mestanza, F. E., & Ninaquispe, J. E. (2022). *FACULTAD DE INGENIERÍA Y ARQUITECTURA 01 Facultad de Ingeniería y Arquitectura [Universidad César Vallejo]*. En Repositorio UCV. http://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/47102/Gutierrez_RS-SD.pdf?sequence=1&isAllowed=y

Montes de Oca, A., & Ramos, R. (2021). *La Metodología Top Down En La Optimización Del Servicio De Internet En Educación Continua De La Universidad Nacional Del Altiplano 2019 [Universidad Nacional del Altiplano]*. En Repositorio UNAP. https://repositorio.unap.edu.pe/handle/20.500.14082/16823

Montoya Benitez, A. O., & Ospina, B. (2020). *Benchmark para determinar el sistema de cifrado con mejor rendimiento sobre dispositivos inteligentes.* Informador Técnico, 84(2), 175–191. https://doi.org/10.23850/22565035.2782

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

Morales, C. (2012). *E g p f Criterio de evalaución de proyectos – u a n 5 – c e r*. https://finanzasdelproyecto.files.wordpress.com/2012/06/unidad5_er.pdf

Mosalvo, O. (2013). *Protocolos de Enrutamiento*. Slideshare. https://es.slideshare.net/oswaldomonsalvo/protocolos-de-enrutamiento-28533187

Ñaupas, H., Valdivia, M. R., Palacios, J. J., & Romero, H. E. (2018). *Metodología de la investigación cuantitativa-cualitativa y redacción de la tesis.* En Journal of Chemical Information and Modeling (Edición, 5). Ediciones de la U. https://doi.org/10.1017/CBO9781107415324.004

Nebot, N. (2023). *Escuela Técnica Superior de Ingeniería Informática Monitorización y gestión del tráfico de VPNs mediante un orquestrador de conexiones*. Universidad Técnica de Valencia.

OpenVPN Technologies Inc. (2023). *OpenVPN*. https://openvpn.net

OWASP. (2015). *Certificados digitales SSL y TLS*. https://owasp.org/www-pdf-archive/6.OWASP_Day_Costa_Rica_Didier.pdf

Parnas, D. L., & Clements, P. C. (1986). *A Rational Design Process: How and Why to Fake It.* IEEE Transactions on Software Engineering, SE-12(2), 251–257. https://doi.org/10.1109/TSE.1986.6312940

Pomar, R. (2019). *Implementación de una red privada virtual de software libre en una empresa*. 57. https://pdfs.semanticscholar.org/ccfc/4870a72b121cc62397e0a00c47b037fc14d6.pdf%0Ahttp://hdl.handle.net/10609/94606

RedesPlus. (2022). *Instalar y configurar OpenVPN en Ubuntu*. https://www.youtube.com/watch?v=P7i-oLe2bHk

Riascos Erazo, S. C., Castro, A. A., & Ávila Fajardo, G. P. (2014). *Seguridad de los sistemas de información en las Pymes de Santiago de Cali (Colombia)*. Libre Empresa, 11(1), 107–118. https://doi.org/10.18041/1657-2815/libreempresa.2014v11n1.3015

Rifá, H. (2013). *Infraestructura de clave pública (OKI)*. https://es.slideshare.net/junral/actividad-n5-26596212

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

Río, A. (2021). *Introducción a la Criptografía* (Vol. 1). Universidad de Murcia. https://www.um.es/adelrio/Docencia/Criptografia/Criptografia.pdf

Rosero, J. S. (2021). *Formulación de propuesta para la implementación de una VPN en el Colegio centro Don Bosco* [Universidad Santo Tomas]. https://repository.usta.edu.co/bitstream/handle/11634/33538/2021juanrosero.pdf?sequence=1&isAllowed=y

Sergei, P., & Azúa, Z. (2023). *Pruebas para aplicaciones Web Keyword*. https://gc.scalahed.com/recursos/files/r161r/w21843w/presentation_content/external_files/U7.pdf

Tomás, J. (2008). *Servicio VPN de acceso remoto basado en SSL mediante OpenVPN* [Universidad Politécnica de Cartagena]. http://hdl.handle.net/10317/758

Torres, C. B., & Espinoza, J. C. (2019). *Propuesta de un Sistema de Gestión de Seguridad de la Información para una Empresa de Consultoría Financiera en Lima, 2021, Según la Norma ISO/IEC 27001:2013* [Universidad Peruana de Ciencias e Informática]. En Repositorio UPCI. http://repositorio.upci.edu.pe/handle/upci/79

Universidad Nacional de Córdoba. (2015). *Política de Seguridad de la Información para la Universidad Nacional de Córdoba*. https://www.unc.edu.ar/sites/default/files/PoliticadeSeguridad08.pdf

UPM. (2017). Contenido. En *Guía de conexión a la VPN de ETSIINF-UPM* (pp. 1–6). Universidad Politécnica de madrid. https://www.etsiinf.upm.es/docs/servicios/red-acceso/373_Guia_VPN-Windows_7.pdf

Vidal, S. (2016). *Escalabilidad de Redes Definidas por Software en la Red Académica Proyecto de grado* [Universidad de la República]. https://www.colibri.udelar.edu.uy/jspui/bitstream/20.500.12008/19030/1/2529.pdf

Villanova, O. (2023). *Ciberseguridad dentro de una red empresarial* [Universidad de basrcelona]. https://diposit.ub.edu/dspace/bitstream/2445/202029/1/tfg_villanova_medina_oriol.pdf

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

ANEXOS

ANEXO 1 Matriz de Consistencia

Preguntas	Objetivos	Hipótesis	Variables	Prueba Estadística
PG: ¿El diseño de la VPN basada en software libre mejorará la seguridad de la información en la empresa GS Maquinarias y Constructora E.I.R.L.?	**OG:** Diseñar una Red Privada Virtual (VPN) basado en Software Libre, para la mejora de la seguridad de la información en la Empresa GS Maquinarias y Constructora E.I.R.L., Juliaca, 2023.	**Hi:** El diseño de la VPN basada en software libre mejorará la seguridad de la información en la empresa GS Maquinarias y Constructora E.I.R.L.	**Variable Independiente:** Red Privada Virtual "VPN" **Variable dependiente:** Seguridad de la información	**Tipo de investigación:** Aplicada **Diseño:** Cuasi Experimental (Pre-Test) y (Post-Test) **Población:** 4 proyectos con 44 trabajadores de GS Maquinarias y Constructora E.I.R.L., Juliaca **Muestra:** 14 trabajadores de GS Maquinarias y Constructora E.I.R.L., Juliaca, de muestreo censal. **Método de investigación:** **Técnica:** Encuesta **Instrumento:** "Encuesta sobre apreciación de la seguridad de la información". Metodología de desarrollo: TOP DOWN **Prueba de hipótesis**: Prueba no paramétrica con signo de Wilcoxon
Preguntas Específicas	**Objetivos específicos**	**Hipótesis específicas**		
PE1: ¿El análisis de los requerimientos con la metodología TOPDOWN permitirá identificar los riesgos a la seguridad de la información en la Empresa GS Maquinarias y Constructora E.I.R.L., Juliaca, 2023? **PE2:** ¿El diseño de la red lógica permitirá mitigar los riesgos a la seguridad de la información en la Empresa GS Maquinarias y Constructora E.I.R.L., Juliaca, 2023.? **PE3:** ¿La documentación y evaluación de la VPN permitirá validar la mejora de la seguridad de la información en la Empresa GS Maquinarias y Constructora E.I.R.L., Juliaca, 2023.? **PE4:** ¿El retorno de inversión de la implementación de la VPN será positivo en la Empresa GS Maquinarias y Constructora E.I.R.L., Juliaca, 2023.?	**OE1:** Analizar los requerimientos con la metodología TOPDOWN para la optimización de la seguridad de la información en la Empresa GS Maquinarias y Constructora E.I.R.L., Juliaca, 2023. **OE2:** Diseñar la RED LÓGICA para la optimización de la seguridad de la información en la Empresa GS Maquinarias y Constructora E.I.R.L., Juliaca, 2023. **OE3:** Documentar y evaluar la VPN para la mejora de la seguridad de la información en la Empresa GS Maquinarias y Constructora E.I.R.L., Juliaca, 2023. **OE4:** Evaluar el retorno de inversión con el uso del VAN, TIR y PR de la implementación de la VPN en la Empresa GS Maquinarias y Constructora E.I.R.L., Juliaca, 2023.	**HE1:** El análisis de los requerimientos con la metodología TOPDOWN permitirá identificar los riesgos a la seguridad de la información en la Empresa GS Maquinarias y Constructora E.I.R.L., Juliaca, 2023. **HE2:** El diseño de la red lógica permitirá mitigar los riesgos a la seguridad de la información en la Empresa GS Maquinarias y Constructora E.I.R.L., Juliaca, 2023. **HE3:** La documentación y evaluación de la VPN permitirá validar la mejora de la seguridad de la información en la Empresa GS Maquinarias y Constructora E.I.R.L., Juliaca, 2023. **HE4:** El retorno de inversión de la implementación de la VPN será positivo en la Empresa GS Maquinarias y Constructora E.I.R.L., Juliaca, 2023.		

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

ANEXO 2 Resultados de Confiabilidad de Instrumento

Para verificar la confiabilidad del Instrumento del cuestionario "*Encuesta sobre apreciación de la seguridad de la información",* se sometió a la prueba de confiabilidad para determinar la consistencia interna existente entre las preguntas planteadas, buscando el nivel de correlación entre ellas. Se utilizó el Alfa de Cronbach con el software SPSS en su versión 26 obteniendo los siguientes resultados:

Tabla 25

Escala de valores de Alfa de Cronbach

Valor	Confiabilidad
Alrededor de 0.9	Nivel elevado de confiabilidad
0.8 o superior	Confiable
Alrededor de 0.7	Baja
Inferior a 0.6	Inaceptable

Nota: Hogan (2004).

Tabla 26

Resultados de Confiabilidad de Instrumento

Instrumento	Alfa de Cronbach	Nro. de Ítems
Pre Test (Seguridad de información)	0.847889	10
Post Test (Seguridad de información)	0.730972	10

Nota: Elaboración propia.

En base a los resultados obtenidos se logra determinar una alta confiabilidad siendo esta aplicable en otros estudios. Resultando un valor de Pre test de 0.84 y Post test de 0.73 que son niveles confiables.

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

ANEXO 3 Instrumeno de Investigación

ENCUESTA SOBRE APRECIACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (PRE - TEST)

INTRODUCCIÓN: El siguiente cuestionario tiene la finalidad de evaluar su apreciación como colaborados respecto a la seguridad de la Información en GS. Estimado colaborador, responda con sinceridad, no existen respuestas buenas o malas. La información recabada será exclusivamente de uso investigativo. Marque con una X.

N°	ÍTEM	Muy Malo	Malo	Regular	Bueno	Muy Bueno
	SEGURIDAD					
1	¿Cuál es su apreciación sobre las medidas de seguridad implementadas en GS de la información sensible almacenada en la empresa?					
2	¿Cuál es su apreciación en cuanto a la seguridad en GS respecto a la transferencia de datos?					
3	¿Qué tan satisfecho se siente con el nivel actual de protección de la información ante posibles amenazas cibernéticas en GS?					
4	¿Cuál es su apreciación sobre la seguridad de las claves que usa en GS para el sistema de información?					
	CONFIABILIDAD					
5	¿Cómo evalúa la confiabilidad de los sistemas y datos de la empresa en cuanto a la prevención de intentos de acceso no autorizado?					
6	¿Cuál es su apreciación sobre la efectividad de los procedimientos de autenticación y acceso a la información sensible en GS?					
7	¿Cómo evaluaría la confiabilidad de los métodos de copia de seguridad y recuperación de datos en caso de incidentes en GS?					
	ESCABILIDAD					
8	¿Cuál es su apreciación sobre la escalabilidad de las soluciones de seguridad en GS para adaptarse a las necesidades de protección?					
9	¿Cuál es su percepción sobre la seguridad en cuanto a conexiones simultáneas en GS?					
10	¿Cuál es su percepción sobre la escalabilidad y seguridad en cuanto si la cantidad de datos y archivos pesados aumenta en GS?					

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

ENCUESTA SOBRE APRECIACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (POST - TEST)

INTRODUCCIÓN: El siguiente cuestionario tiene la finalidad de evaluar su apreciación como colaborados respecto a la seguridad de la Información en GS. Estimado colaborador, responda con sinceridad, no existen respuestas buenas o malas. La información recabada será exclusivamente de uso investigativo. Marque con una X.

N°	ÍTEM	Muy Malo	Malo	Regular	Bueno	Muy Bueno
	SEGURIDAD					
1	¿Cuál es su apreciación sobre las medidas de seguridad implementadas en GS de la información sensible almacenada en la empresa con la VPN?					
2	¿Cuál es su apreciación en cuanto a la seguridad en GS respecto a la transferencia de datos con la VPN?					
3	¿Qué tan satisfecho se siente con el nivel actual de protección de la información ante posibles amenazas cibernéticas en GS con la VPN?					
4	¿Cuál es su apreciación sobre la seguridad de las claves que usa en GS para el sistema de información con la VPN?					
	CONFIABILIDAD					
5	¿Cómo evalúa la confiabilidad de los sistemas y datos de la empresa en cuanto a la prevención de intentos de acceso no autorizado con la VPN?					
6	¿Cuál es su apreciación sobre la efectividad de los procedimientos de autenticación y acceso a la información sensible en GS con la VPN?					
7	¿Cómo evaluaría la confiabilidad de los métodos de copia de seguridad y recuperación de datos en caso de incidentes en GS con la VPN?					
	ESCALABILIDAD					
8	¿Cuál es su apreciación sobre la escalabilidad de las soluciones de seguridad en GS para adaptarse a las necesidades de protección con la VPN?					
9	¿Cuál es su percepción sobre la seguridad en cuanto a conexiones simultáneas en GS con la VPN?					
10	¿Cuál es su percepción sobre la escalabilidad y seguridad en cuanto si la cantidad de datos y archivos pesados aumenta en GS con la VPN?					

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

ANEXO 4 Base de datos Pre test y Post test

	Pre Test										Post Test									
	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10
1	2	3	3	3	1	3	2	2	3	3	4	5	4	5	5	3	4	4	3	5
2	1	3	3	3	2	3	3	2	3	3	4	5	4	5	4	4	5	4	3	5
3	2	3	3	2	2	3	3	2	2	3	4	5	4	4	5	3	4	4	4	4
4	2	3	3	3	1	3	2	3	3	3	5	4	5	5	4	4	4	5	4	4
5	2	2	2	2	2	3	2	2	3	3	3	4	4	4	4	3	5	4	3	4
6	1	3	2	3	1	2	2	3	4	3	4	4	4	4	4	3	4	4	3	4
7	2	2	2	2	2	3	2	2	3	3	4	5	4	5	5	4	4	4	3	5
8	2	3	3	3	1	3	2	2	3	3	4	4	5	5	5	3	4	5	4	5
9	1	2	2	2	2	2	1	1	2	2	3	4	3	4	4	3	4	4	3	4
10	2	3	3	3	1	3	2	3	3	3	5	4	5	5	4	4	5	5	4	5
11	1	2	2	2	2	2	1	1	2	2	4	5	4	4	4	3	5	4	3	4
12	2	2	2	2	2	3	2	2	3	2	4	5	4	5	5	4	4	4	3	4
13	1	2	2	2	1	2	1	1	2	2	4	4	4	5	4	3	4	4	4	5
14	2	3	3	2	2	3	3	2	2	3	4	5	4	5	4	4	5	4	3	5

Nota: Elaboración propia.

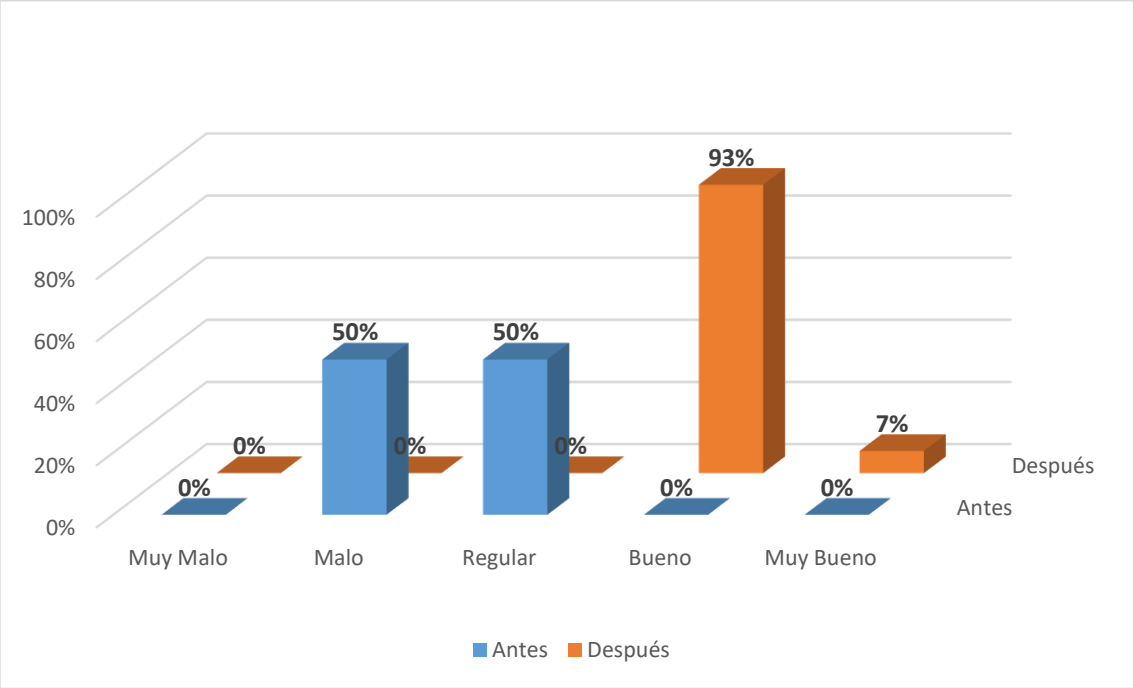
repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

ANEXO 5 Datos complementarios de la Encuesta

Figura 14

Gráfica comparativa entre el Pre test y el Post test



Nota: Elaboración propia generada con Microsoft Excel 2019

Interpretación: De acuerdo a la encuesta realizada a los 14 colaboradores de la empresa privada GS Maquinarias y Constructora E.I.R.L., se logró recabar las fichas del antes y después habiéndoles mostrado el funcionamiento de la VPN. Es así, que se obtuvo que la apreciación antes de la VPN era considerada por los colaboradores entre malo y regular en un 50%. Una vez mostrado el funcionamiento de la VPN mejoró significativamente a ser apreciado como nivel bueno en un 93% y 7% como excelente. Lo que indica que la VPN tuvo buena apreciación por parte de los colaboradores quienes quieren usar la VPN. En otras palabras, consideran que el usar una VPN como acceso a recursos de GS mejoraría en un nivel bueno la seguridad de información con que se trabaja tanto de manera local como remotamente.

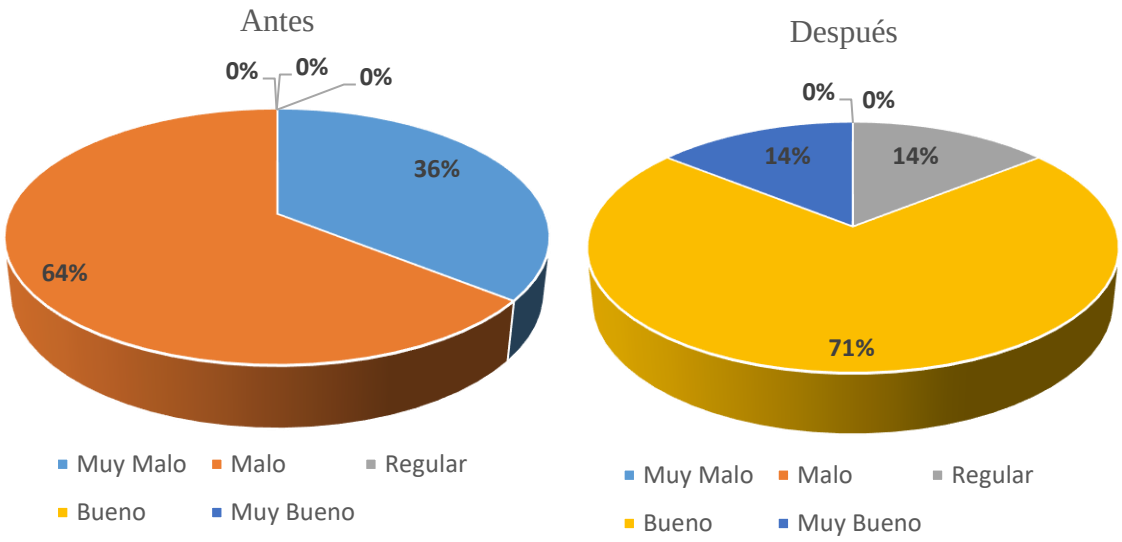
repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

Pregunta 1: ¿Cuál es su apreciación sobre las medidas de seguridad implementadas en GS para proteger la información sensible en la empresa?

Figura 15

Resultados descriptivos de la Pregunta 1



Nota: Elaboración propia generada con Microsoft Excel 2019

Interpretación: La figura anterior, se logra apreciar que antes de la implementación del VPN el 64% lo describió como malo y el 36% como muy malo, luego de la implementación el 71% como bueno, el 14% como muy bueno y el otro 14% como regular.

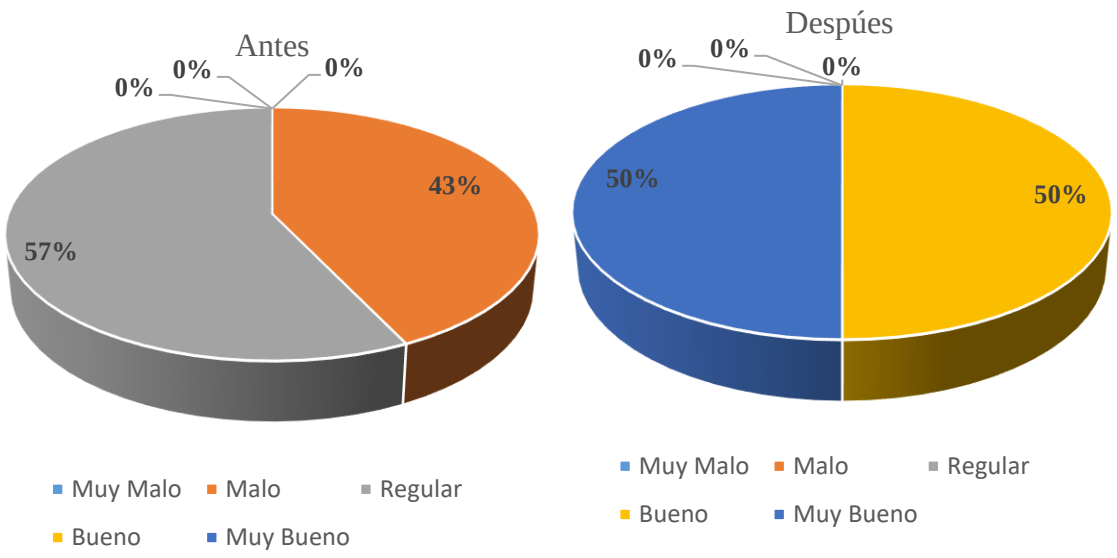
repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

Pregunta 2: ¿Cuál es su apreciación en cuanto a la seguridad en GS respecto a la transferencia de datos?

Figura 16

Resultados descriptivos de la Pregunta 2



Nota: Elaboración propia generada con Microsoft Excel 2019

.

Interpretación: La figura anterior, se logra apreciar que antes de la implementación del VPN el 57% lo describió como regular y el 43% como malo, luego de la implementación el 50% como bueno y el 50% como muy bueno.

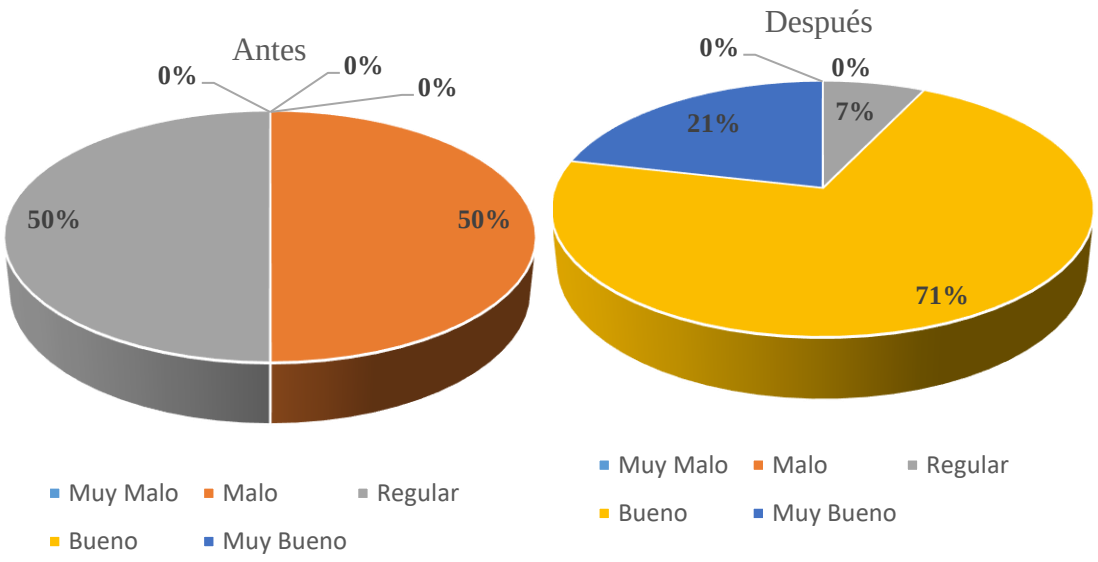
repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

Pregunta 3: ¿Qué tan satisfecho se siente con el nivel actual de protección de la información ante posibles amenazas cibernéticas en GS?

Figura 17

Resultados descriptivos de la Pregunta 3



Nota: Elaboración propia generada con Microsoft Excel 2019

Interpretación: La figura anterior, se logra apreciar que antes de la implementación del VPN el 50% lo describió como regular y el 50% como malo, luego de la implementación el 71% como bueno, el 21% como muy bueno y el otro 7% como regular.

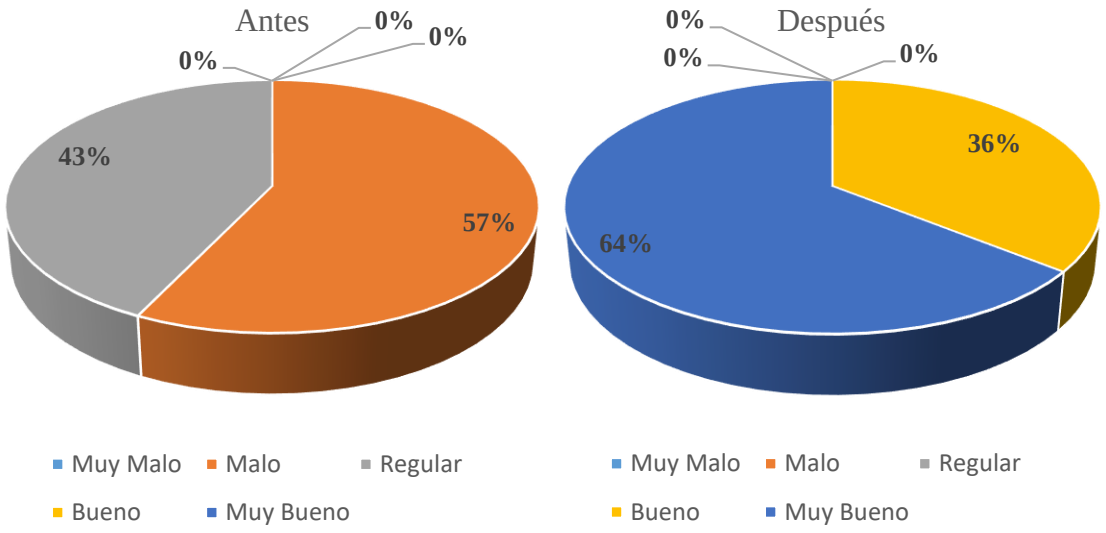
repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

Pregunta 4: ¿Cuál es su apreciación sobre la seguridad de las claves que usa en GS para el sistema de información?

Figura 18

Resultados descriptivos de la Pregunta 4



Nota: Elaboración propia generada con Microsoft Excel 2019

Interpretación: La figura anterior, se logra apreciar que antes de la implementación del VPN el 57% lo describió como malo y el 43% como regular, luego de la implementación el 64% como muy bueno y el 36% como bueno.

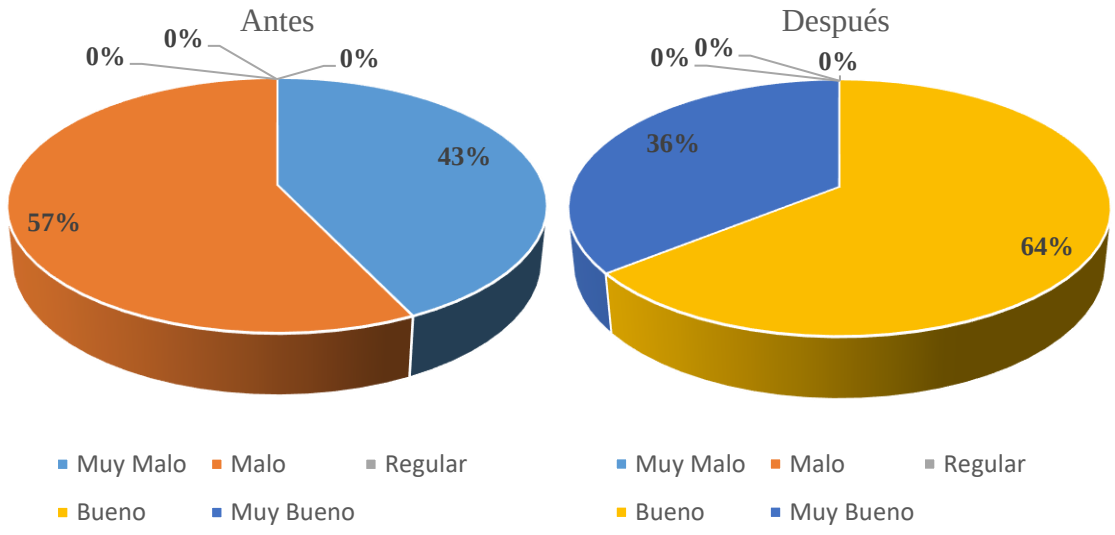
repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

Pregunta 5: ¿Cómo evalúa la confiabilidad de los sistemas y datos de la empresa en cuanto a la prevención de intentos de acceso no autorizado?

Figura 19

Resultados descriptivos de la Pregunta 5



Nota: Elaboración propia generada con Microsoft Excel 2019

Interpretación: La figura anterior, se logra apreciar que antes de la implementación del VPN el 57% lo describió como malo y el 43% como muy malo, luego de la implementación el 64% como bueno y el 36% como muy bueno.

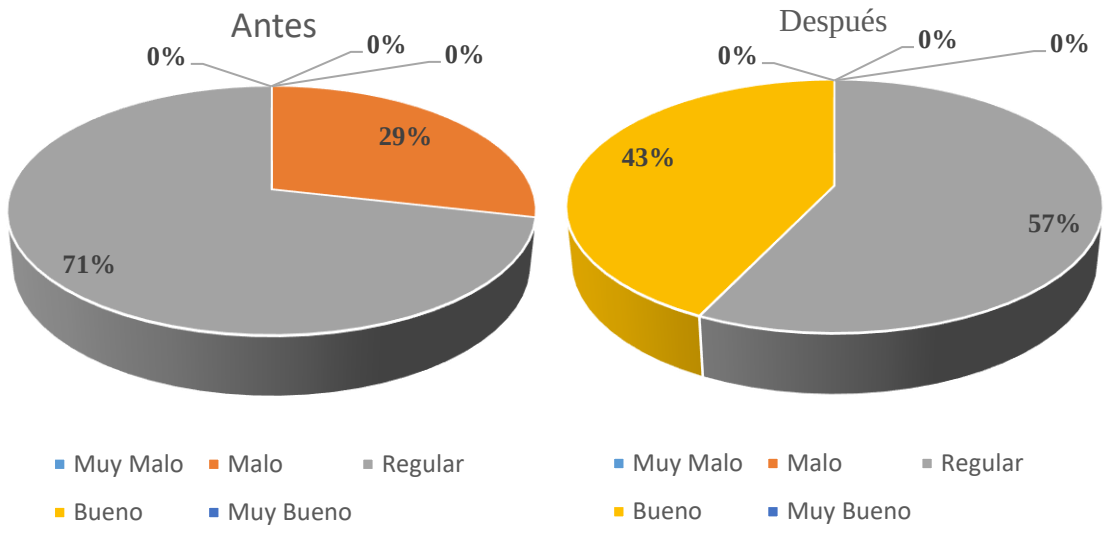
repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

Pregunta 6: ¿Cuál es su apreciación sobre la efectividad de los procedimientos de autenticación y acceso a la información sensible en GS?

Figura 20

Resultados descriptivos de la Pregunta 6



Nota: Elaboración propia generada con Microsoft Excel 2019

Interpretación: La figura anterior, se logra apreciar que antes de la implementación del VPN el 71% lo describió como regular y el 29% como malo, luego de la implementación el 43% como bueno y el 57% como regular.

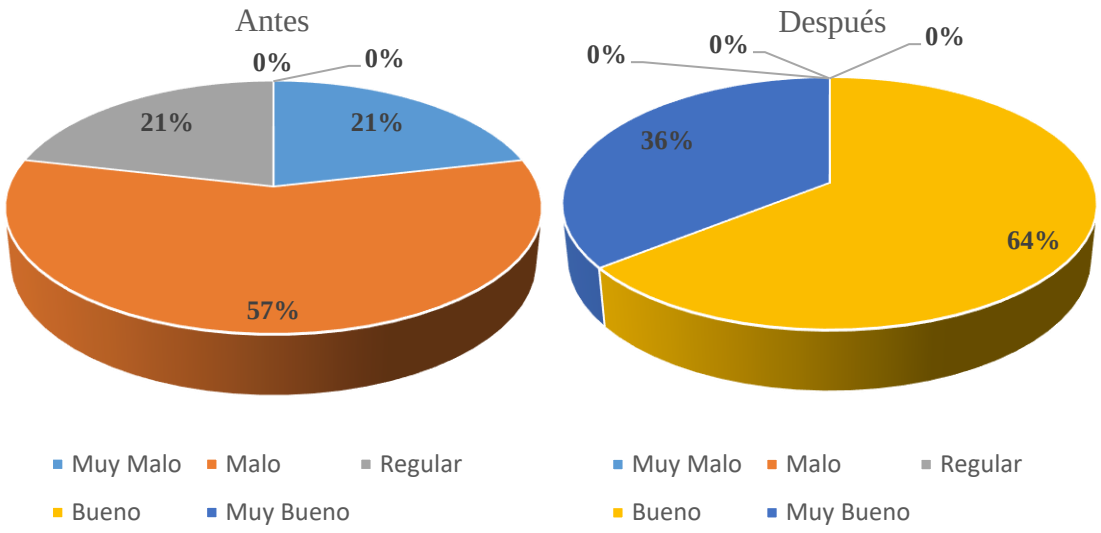
repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

Pregunta 7: ¿Cómo evaluaría la confiabilidad de los métodos de copia de seguridad y recuperación de datos en caso de incidentes en GS?

Figura 21

Resultados descriptivos de la Pregunta 7



Nota: Elaboración propia generada con Microsoft Excel 2019

Interpretación: La figura anterior, se logra apreciar que antes de la implementación del VPN el 57% lo describió como malo, el 21% como muy malo y el 21% como regular, luego de la implementación el 36% como muy bueno y el 64% como bueno.

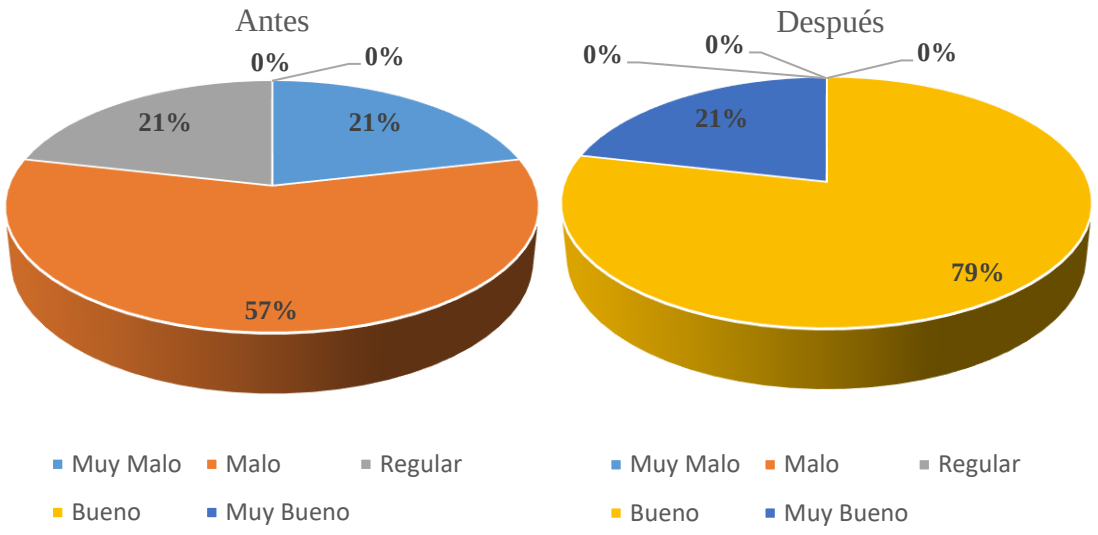
repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

Pregunta 8: ¿Cuál es su apreciación sobre la escalabilidad de las soluciones de seguridad en GS para adaptarse a las necesidades de protección?

Figura 22

Resultados descriptivos de la Pregunta 8



Nota: Elaboración propia generada con Microsoft Excel 2019

Interpretación: La figura anterior, se logra apreciar que antes de la implementación del VPN el 57% lo describió como malo, el 21% como muy malo y el 21% como regular, luego de la implementación el 79% como bueno y el 21% como muy bueno.

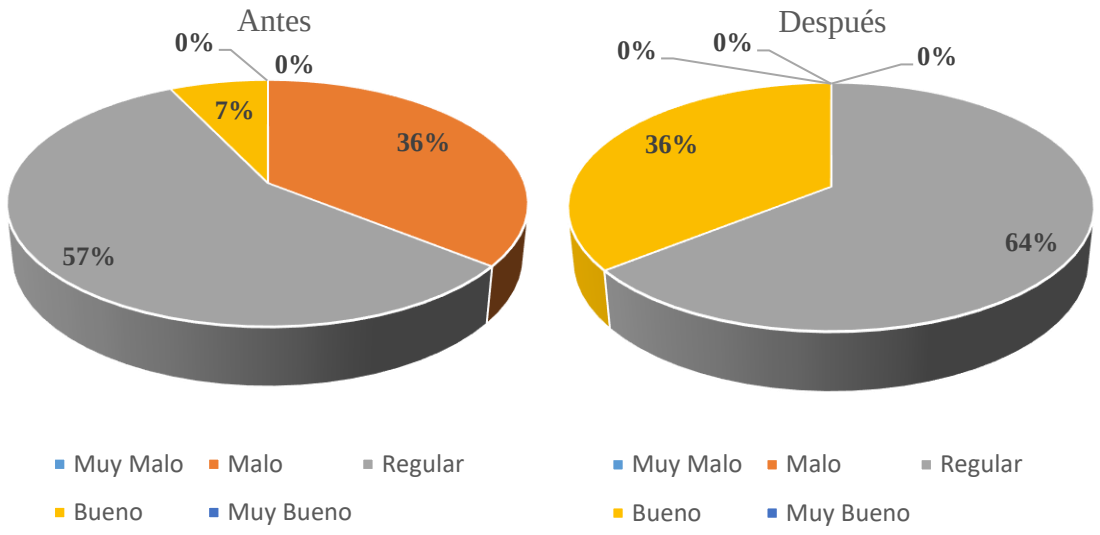
repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

Pregunta 9: ¿Cuál es su percepción sobre la seguridad en cuanto a conexiones simultáneas en GS?

Figura 23

Resultados descriptivos de la Pregunta 9



Nota: Elaboración propia generada con Microsoft Excel 2019

Interpretación: La figura anterior, se logra apreciar que antes de la implementación del VPN el 57% lo describió como regular, el 7% como bueno y el 36% como malo, luego de la implementación el 64% como regular y el 36% como bueno.

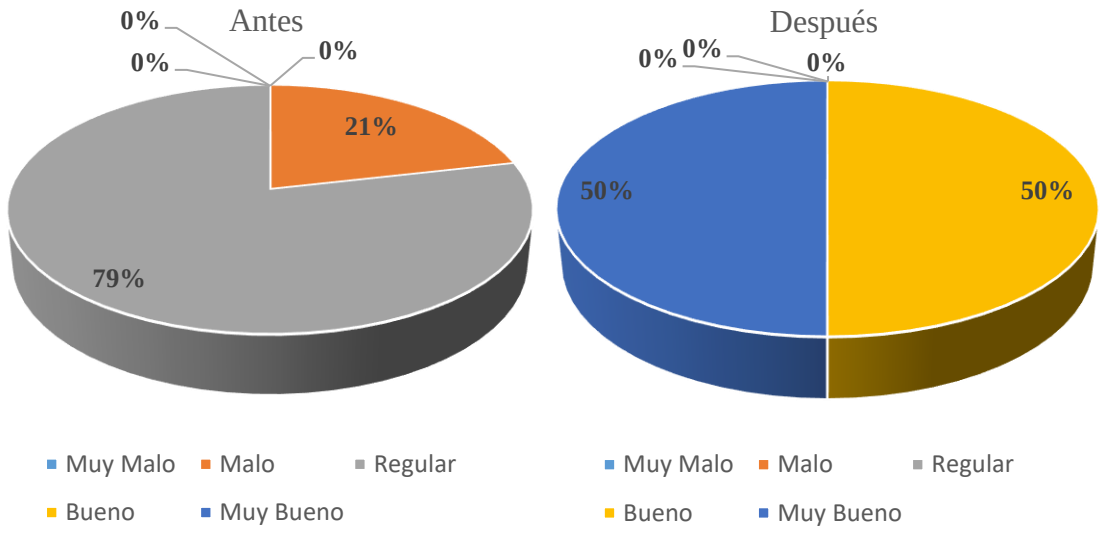
repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

Pregunta 10: ¿Cuál es su percepción sobre la escalabilidad y seguridad en cuanto si la cantidad de datos y archivos pesados aumenta en GS?

Figura 24

Resultados descriptivos de la Pregunta 10



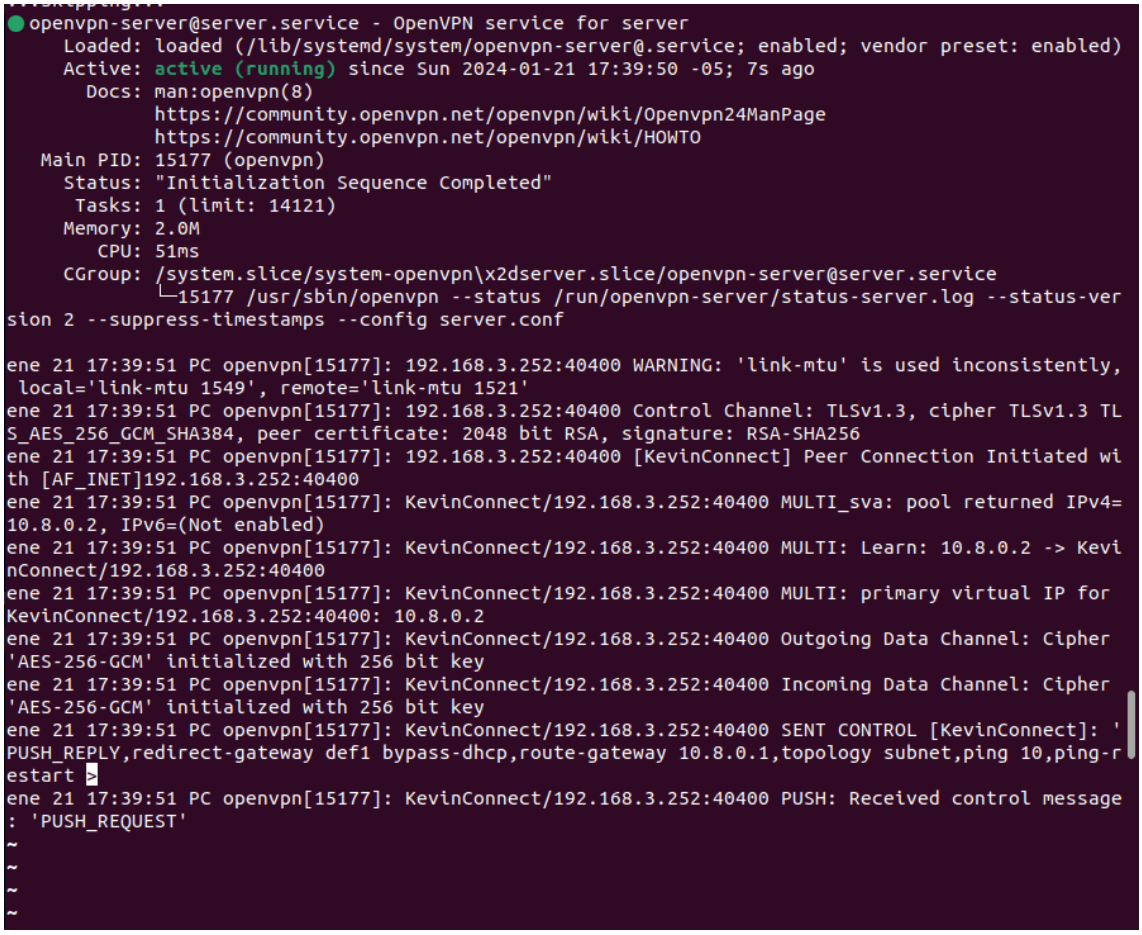
Nota: Elaboración propia generada con Microsoft Excel 2019

Interpretación: La figura anterior, se logra apreciar que antes de la implementación del VPN el 79% lo describió como regular y el 21% como malo, luego de la implementación el 50% como bueno y el 50% como muy bueno.

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

ANEXO 6 Levantamiento del servidor VPN Master GS



Bajo un entorno de prueba seguro el servicio es levantado con el comando en terminal:

sudo service openvpn-server@server start

sudo service openvpn-server@server status

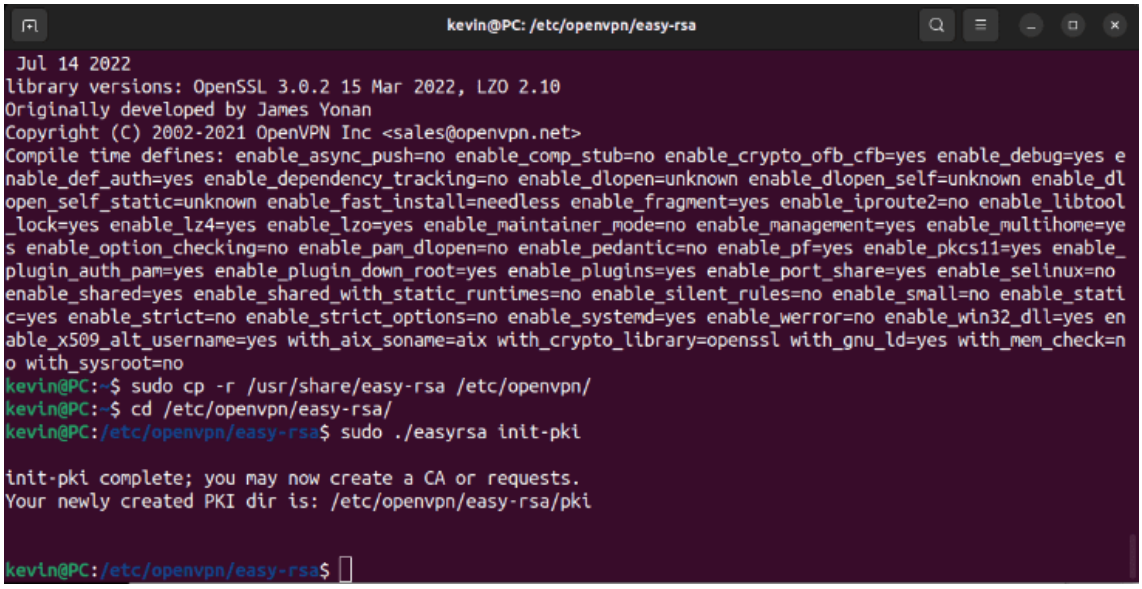
Con el primer comando se logra iniciar y con segundo se conoce el estado, aquí podemos evidenciar si la VPN está activa, inactiva o con algún fallo, del mismo modo se puede conocer todos los equipos que se conectan en tiempo real a la red. En el caso anterior se evidencia la conexión de un equipo con la IP: 192.168.3.252 en el puerto 40400, el puerto es asignado al equipo de manera aleatoria el cual gestiona la VPN. Por último, el posible atacante necesariamente deberá tener la llave, el archivo "*.ovpn*" para al menos poder intentar atacar, por lo son muy pocas las opciones de algún atacante, lo que lleva a comprender que las VPN están específicamente diseñadas para este tipo de privacidad.

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

ANEXO 7 Capturas de la terminal del Servidor en Ubuntu 22.04

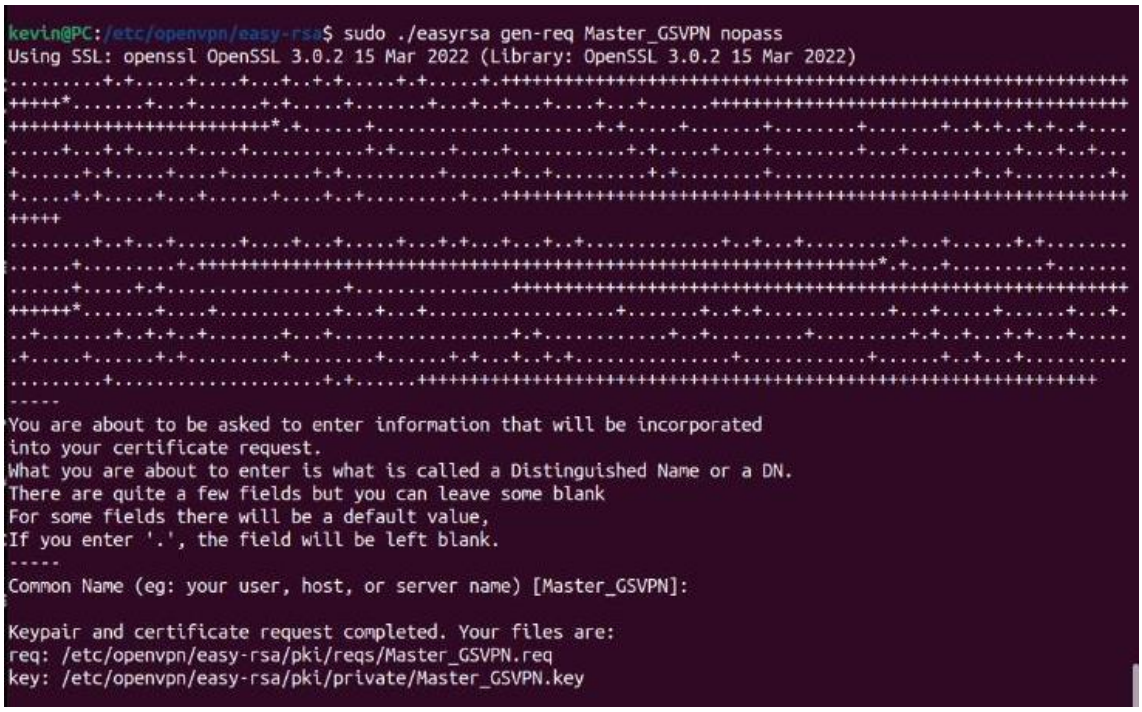
Nota: La captura muestra la instalación del software *openvpn* en el terminal *Bash* del servidor con sistema operativo del Software Libre Ubuntu 22.04.



Nota: La captura muestra que se copia la carpeta $easy-rsa$ y seguidamente inicializa la infraestructura de claves pública (PKI) para *OpenVPN* con lo que creamos el certificado de $Master\_GSVPN$.

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

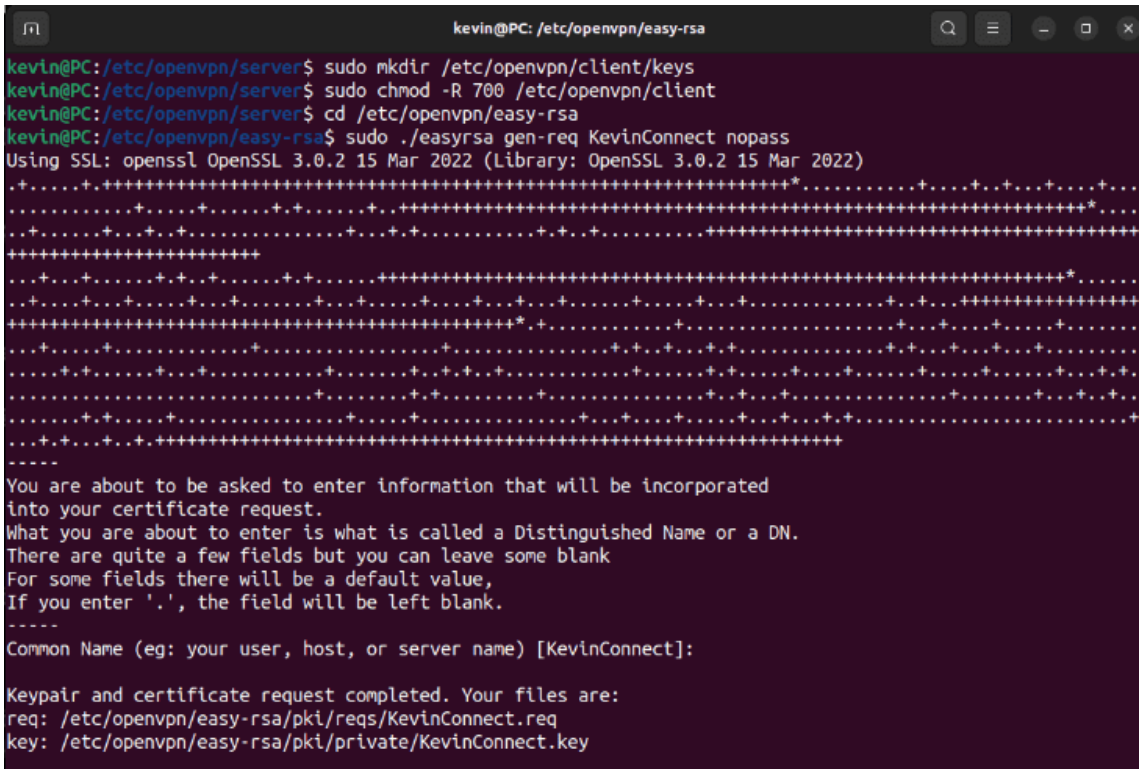


Nota: La captura muestra que generará una solicitud de certificado para el servidor $OpenVPN$

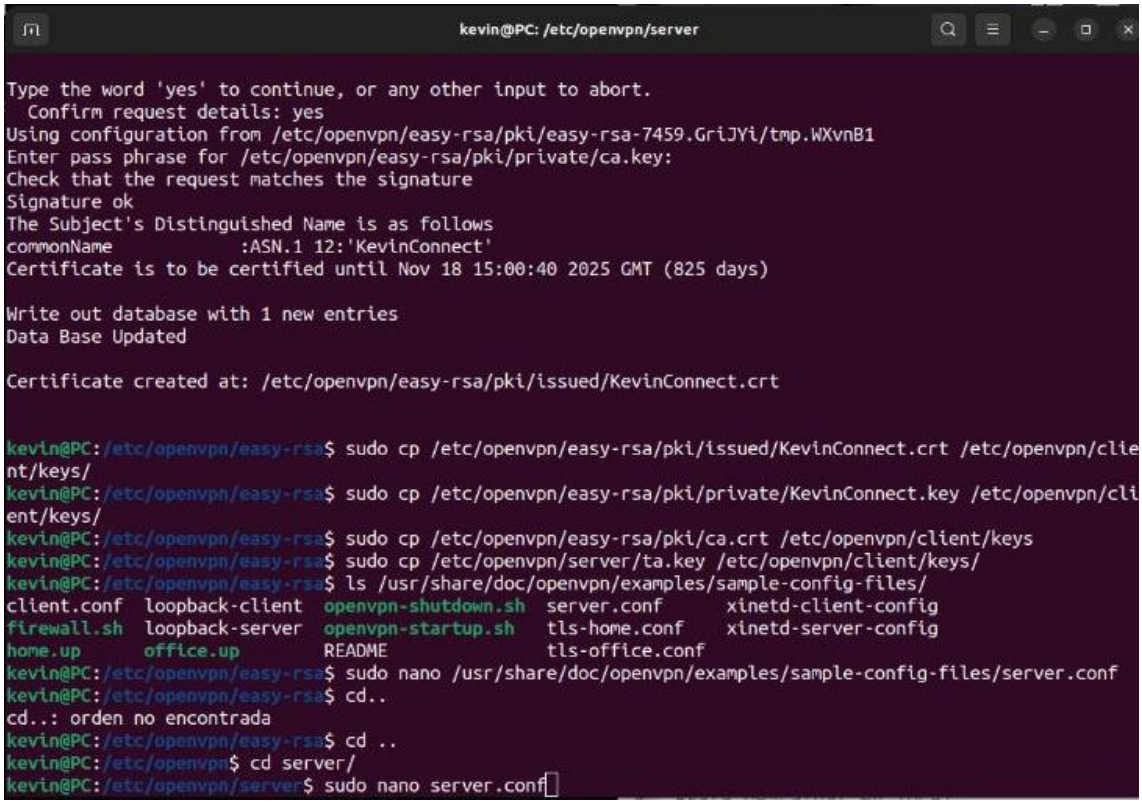
Nota: La captura muestra que el certificado firma la solicitud de certificado del servidor $OpenVPN$ con el nombre $Master\_GSVPN$.

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional



Nota: La captura muestra el cambio de permisos de la carpeta '*keys*' del mismo modo que genera una solicitud de certificado para *KevinConnect*.

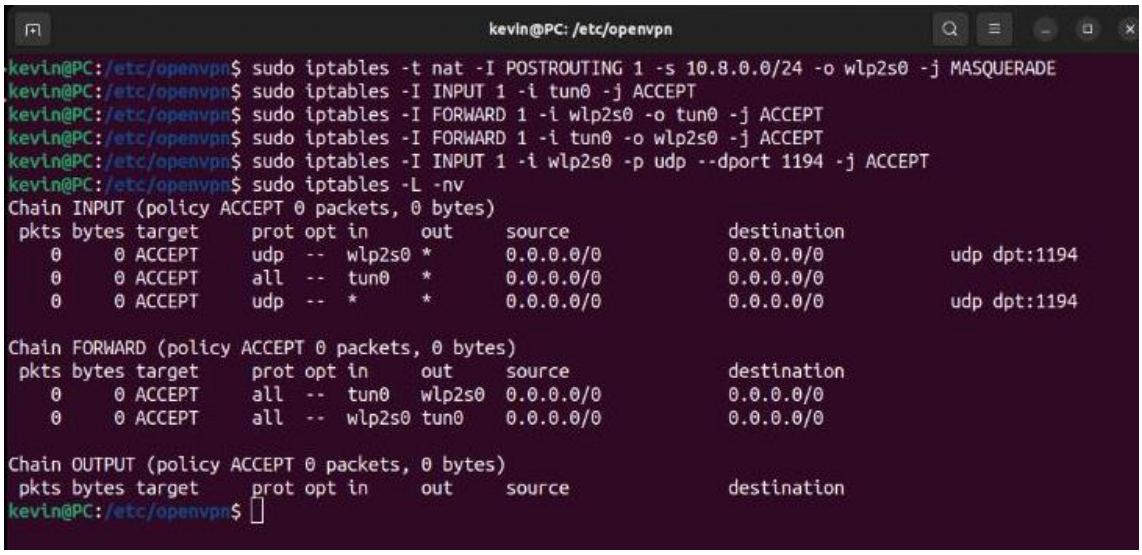


Nota: Se muestra que se copió las llaves del cliente y se copian dentro de '*keys*' para finalmente configurar el servidor con 'sudo nano *server.conf*' y del cliente '*KevinConnect*'.

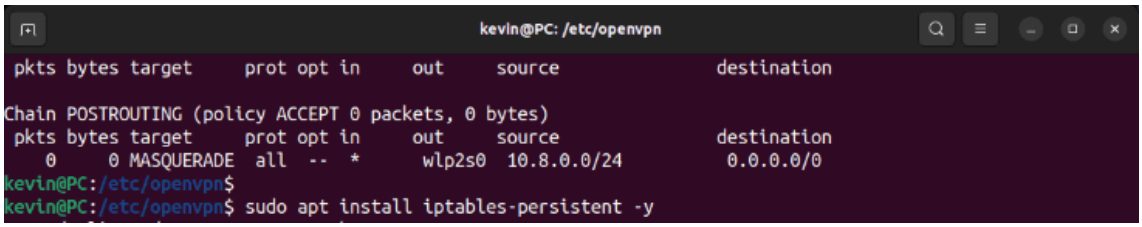
repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

Nota: La captura se muestra que se agrega una nueva regla a la tabla de reglas de entrada de *iptables*. Esta regla permite todo el tráfico UDP entrante en el puerto 1194 y se edita '*sysctl.conf*'.



Nota: La captura muestra las reglas de permiso de transferencia de paquetes para acceso de tráfico, encapsulamiento, acceso a recursos de la red, respuesta de tráfico y conexión al servidor. Asimismo con '*iptables − L − nv*' se enlista las reglas creadas.



Nota: Las reglas creadas se restablecen cuando el servidor se reinicia, por tanto se instala el paquete '*iptables − persistent*' para que cuando se reinicie mantenga las reglas creadas y así proporcione un servicio que guarda y restaura las reglas de '*iptable's*.

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

```
kevin@PC:/etc/openvpn/server$ sudo service openvpn-server@server start
kevin@PC:/etc/openvpn/server$ sudo service openvpn-server@server status
● openvpn-server@server.service - OpenVPN service for server
     Loaded: loaded (/lib/systemd/system/openvpn-server@.service; enabled; vendor preset
     Active: active (running) since Wed 2023-08-16 12:00:30 -05; 4s ago
       Docs: man:openvpn(8)
             https://community.openvpn.net/openvpn/wiki/Openvpn24ManPage
             https://community.openvpn.net/openvpn/wiki/HOWTO
   Main PID: 19213 (openvpn)
     Status: "Initialization Sequence Completed"
      Tasks: 1 (limit: 14121)
     Memory: 1.8M
        CPU: 19ms
     CGroup: /system.slice/system-openvpn\x2dserver.slice/openvpn-server@server.service
             └─19213 /usr/sbin/openvpn --status /run/openvpn-server/status-server.log --

ago 16 12:00:30 PC openvpn[19213]: Could not determine IPv4/IPv6 protocol. Using AF_INET
ago 16 12:00:30 PC openvpn[19213]: Socket Buffers: R=[212992->212992] S=[212992->212992]
ago 16 12:00:30 PC openvpn[19213]: UDPv4 link local (bound): [AF_INET][undef]:1194
ago 16 12:00:30 PC openvpn[19213]: UDPv4 link remote: [AF_UNSPEC]
ago 16 12:00:30 PC openvpn[19213]: GID set to nogroup
ago 16 12:00:30 PC openvpn[19213]: UID set to nobody
ago 16 12:00:30 PC openvpn[19213]: MULTI: multi_init called, r=256 v=256
ago 16 12:00:30 PC openvpn[19213]: IFCONFIG POOL IPv4: base=10.8.0.2 size=253
ago 16 12:00:30 PC openvpn[19213]: IFCONFIG POOL LIST
ago 16 12:00:30 PC openvpn[19213]: Initialization Sequence Completed
kevin@PC:/etc/openvpn/server$
```

Nota: Una vez listo, es que iniciamos el servidor con el demonio '*start*' con lo que el servicio correrá en segundo plano. Para ello se evidencia la línea 'Active: active (running)', lo que indica que la VPN se inició correctamente.

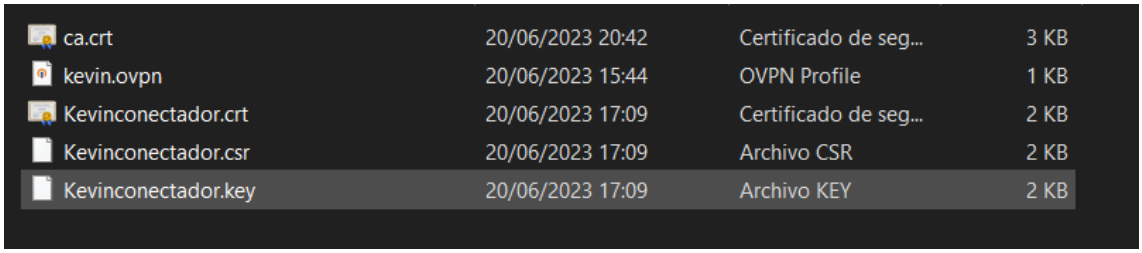
```
root@PC: /etc/openvpn/client
 GNU nano 6.2                    /etc/openvpn/client/make_config.sh
#!/bin/bash

#First argument: KevinConnect

KEY_DIR=/etc/openvpn/client/keys
OUTPUT_DIR=/etc/openvpn/client/files
BASE_CONFIG=/etc/openvpn/client/plantilla.conf

cat ${BASE_CONFIG} \
        <(echo -e '<ca>') \
        ${KEY_DIR}/ca.crt \
        <(echo -e '</ca>\n<cert>') \
        ${KEY_DIR}/${1}.crt \
        <(echo -e '</cert>\n<key>') \
        ${KEY_DIR}/${1}.key \
        <(echo -e '</key>\n<tls-crypt>') \
        ${KEY_DIR}/ta.key \
        <(echo -e '</tls-crypt>') \
        > ${OUTPUT_DIR}/${1}.ovpn
```

Nota: La captura evidencia la creación de un script que genera un archivo de configuración en base a las llaves generadas de un cliente.

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

Nota: La captura muestra la ejecución de una única llave '*.ovpn*' corriendo el comando './make_config.sh *KevinConnect*'.



Nota: '*Kevin.ovpn*', es la única llave que une todas las llaves en una sola, lo que se puede importar en '*OpenVPN GUI*' para Windows o '*OpenVPN Client*' en Android, con lo que el archivo es compartido cuidadosamente a cliente que se conectará a *MasterGSVPN* y logrará tener acceso a los recursos y sistema de información de GS de manera remota.

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

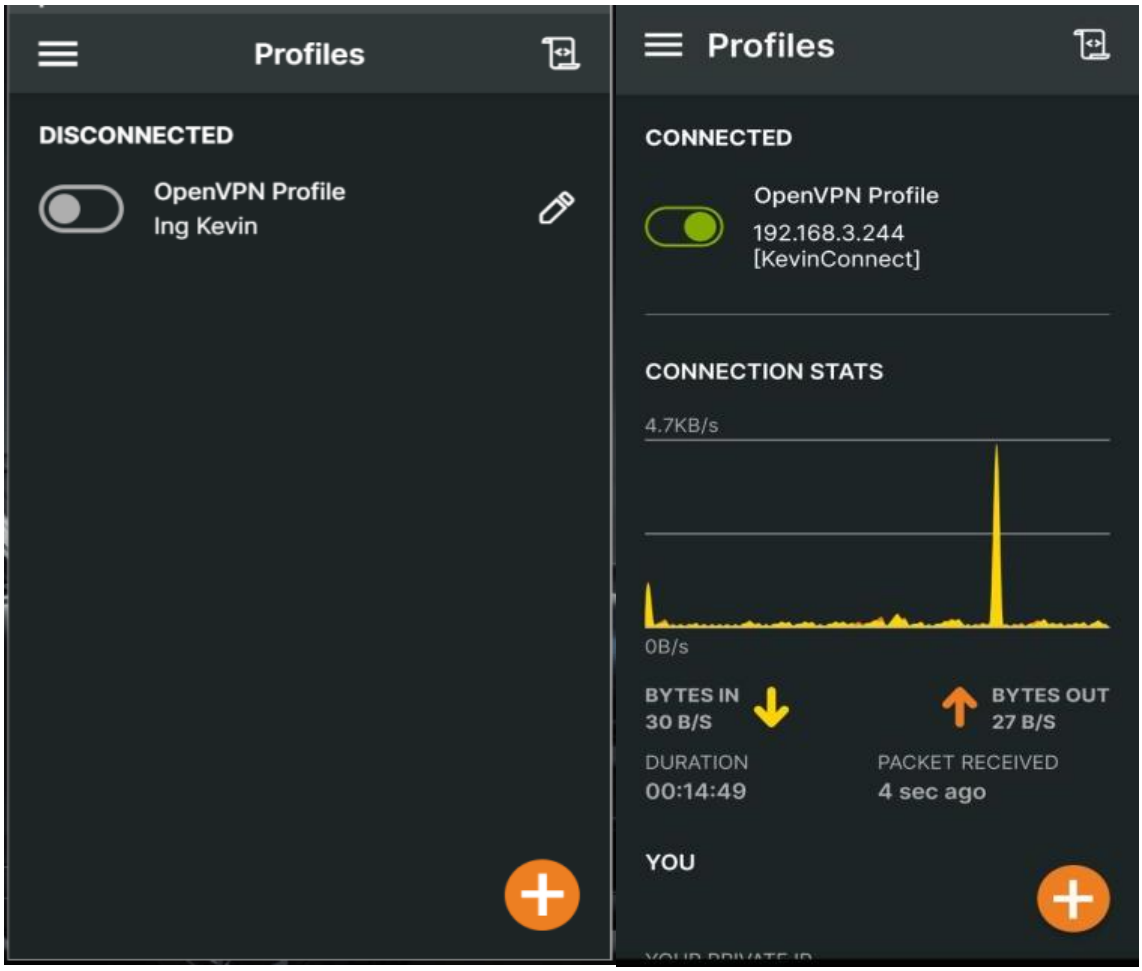
UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

```
-----BEGIN CERTIFICATE-----
MIIDTjCCAjagAwIBAgIUDTBRVXzxIbPBhvH05azrf5MYvOQwDQYJKoZIhvcNAQEL
BQAwFzEVMBMGA1UEAwwMTWFzdGVyX0dTVlBOMB4XDTIzMDgxNTE5MDQzMloXDTMz
MDgxMjE5MDQzMlowFzEVMBMGA1UEAwwMTWFzdGVyX0dTVlBOMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuNZ3RRLrGSlyUaLREaMzcYVoLcGBv5FLARIG
WQIWDCv+/A7ImJlvsqsE62efh2QM/z+aXaoJZwJpVPTFaw9tf15q78mv58oTjdsR
zfAskwlwGfVt2BiHZqeWFn6EQWf1608sbDlXNCTNE6U6ExFOMo2LZK4LA6YYht6E
n8oQi+b/2H977n/xSD6YAZ8rec1eg37hpX5o477uhCxTS1o0/r22LiqwdImfoa/f
CK1rmcfpscbVTO9NZKDUnyn19dDNGEWa/9dKq5QjCRjf6CdItMH6h15z8EtdmZKE
8C4S6tCvQ1KuXc0b374UkEj0E8Q7xQouClYhUFB9vYMltoHTQwIDAQABo4GRMIGO
MB0GA1UdDgQWBBTHmuX8Rciu7kaOV0QGAM9D7ghD/TBSBgNVHSMESzBJgBTHmuX8
Rciu7kaOV0QGAM9D7ghD/aEbpBkwFzEVMBMGA1UEAwwMTWFzdGVyX0dTVlBOghQN
MFFVfPEhs8GG8fTlrOt/kxi85DAMBgNVHRMEBTADAQH/MAsGA1UdDwQEAwIBBjAN
BgkqhkiG9w0BAQsFAAOCAQEACxKx3QJcTQ12kYWVIaqjCSnvHh2xfU66FMfNxfBG
Rs0llib8TN+Cg4gq1fbFu1qDqcLE/h5RDBHY4++hlAqBykLtS2e/Vivhptakp4xD
aPMSZ4pu3FUQQTwcJHlZ1yhba4thlE2kQWinxobQraG0u8+YB6xhxBmu4r1N4IxC
Ra+1ao8wNJjp0Jzq+n5xIRL5Wmnn68wAudMV/Ce4/GqDZbO3SNVZfyaQQD6IQolU
MQA9OlZWVJCjPFQIXO3M76gMDpBVCaQhJ3DDoMnRt8d2XbE/IPRhfq6hDllCIK0c
8ngakK0OZRxVEFesazRM1uknJNOftMvqRbVnaqdXc6qhtQ==
-----END CERTIFICATE-----
</ca>
<cert>
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            08:6c:59:b5:db:a8:02:40:11:09:fa:3d:cd:dd:b5:5b
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN=Master_GSVPN
        Validity
            Not Before: Aug 16 15:00:40 2023 GMT
            Not After : Nov 18 15:00:40 2025 GMT
        Subject: CN=KevinConnect
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:a7:2c:78:9a:ca:b1:52:2b:f9:fe:6c:52:ac:39:
                    90:cb:95:8e:11:d4:4c:35:9f:81:d2:8b:65:5e:96:
                    9b:b6:7e:19:e7:71:24:84:1a:64:87:5f:bf:66:5e:
                    ee:93:51:78:25:b7:18:fc:10:ba:ab:8f:fb:c8:eb:
                    d2:b5:12:94:45:78:35:6a:0c:d7:6f:b0:cd:6a:9a:
                    72:ea:c8:3c:6e:1f:05:76:78:28:5d:a5:f5:0c:bf:
                    fe:18:a4:97:a8:82:c5:bd:e9:ac:f0:c8:30:cf:fa:
                    5b:ee:a3:53:18:18:53:02:23:d3:d0:c1:8d:9c:11:
                    37:cd:f3:81:46:bb:6f:17:08:de:00:b3:37:97:80:
                    e9:6c:6f:56:47:e4:a9:56:b8:2e:1a:00:d2:94:a4:
                    3e:49:b1:d3:0f:4c:9a:68:39:f0:b9:e8:69:ad:e2:
                    53:c9:90:fa:e0:d0:16:46:ab:43:71:40:ec:e6:8a:
```

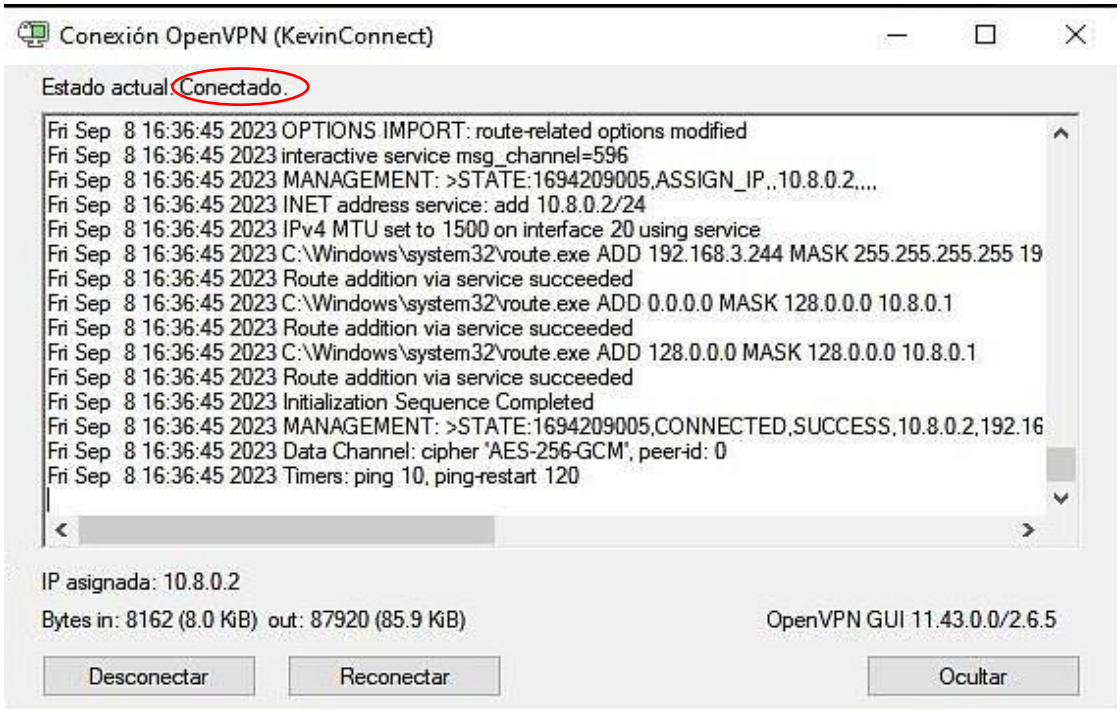
Nota: La captura evidencia la estructura de las primeras líneas del archivo '*.ovpn*', se muestra que están implícitamente las llaves '*.ca*','*crt*','*csr*','*key*' generadas para el cliente Kevin.

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional



Nota: El archivo '.ovpn' se logró conectar desde Android importando el archivo.



Nota: El archivo '*.ovpn*' se logró conectar desde Windows 10.

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

ANEXO 8 Pruebas de ataque a Master_GSVPN

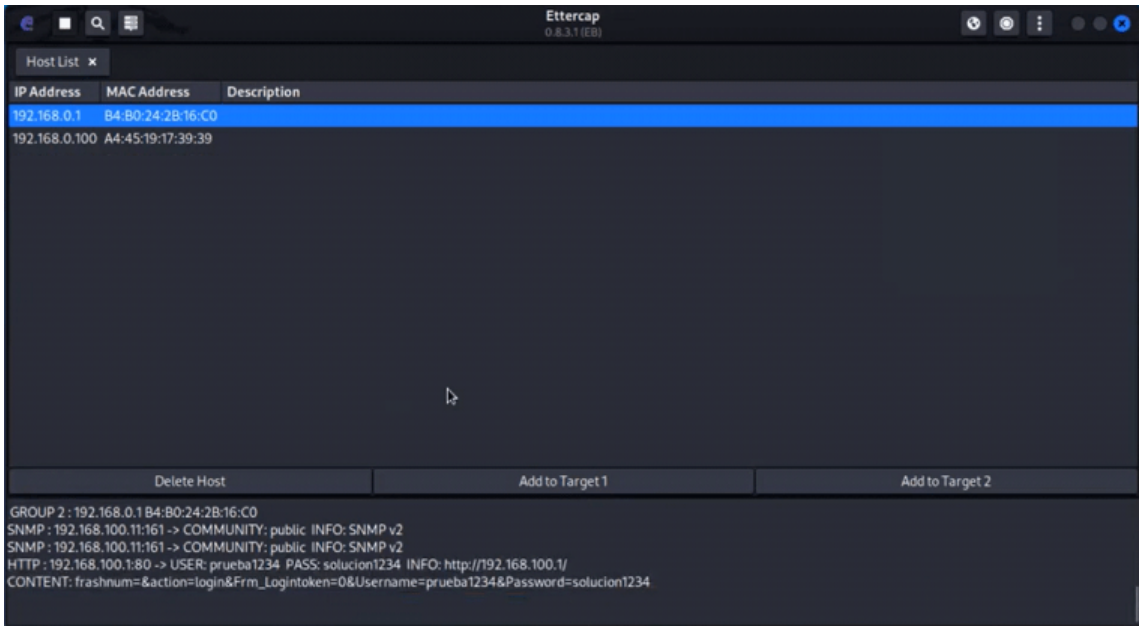
ATAQUE POR ETHERCAP ANTES DE LA IMPLEMENTACIÓN DE LA VPN

Se llevó a cabo un ataque utilizando ETHERCAP, un interceptor/sniffer/registrador utilizado en redes LAN conmutadas. Esta herramienta, empleada principalmente para auditorías en distintos tipos de redes, demostró su utilidad en entornos LAN con switches. Para la demostración de este ataque, se utilizaron dos máquinas: una donde un trabajador de la empresa intentó iniciar sesión (ingresar a una web) y otra con el sistema operativo KALI. En esta última, mediante la herramienta nativa ETHERCAP Gráfica, se intentó obtener los datos ingresados por el trabajador. Primero, se inició el programa ETHERCAP. Luego, se seleccionó el tipo de red en uso; en este caso, se utilizó el tipo eth0. El programa comenzó a ejecutar y escanear los dispositivos conectados a la red. Seguidamente, se seleccionó la opción de Scan Host, que mostró los hosts conectados a la red. En nuestra prueba, solo se obtuvieron dos: el nuestro y el del trabajador víctima.

Se agregó la IP de la máquina víctima en "TARGET 1" y se agregó nuestra IP en "TARGET 2". Luego, se seleccionó la opción de "ARP POISONING", iniciando así el envenenamiento de la red. De esta forma, se enviaron protocolos "snmp" a la máquina víctima, manteniéndonos en escucha. Para la demostración, en la máquina víctima se abrió una web con login creada en nuestro SERVIDOR LOCAL. Aquí, el trabajador intentó registrarse con los siguientes datos: prueba1234 (usuario) y solucion1234 (contraseña). Al finalizar el ingreso, el programa ETHERCAP interceptó y mostró los datos ingresados, demostrando así lo vulnerable que podría ser la red de la empresa sin una VPN.

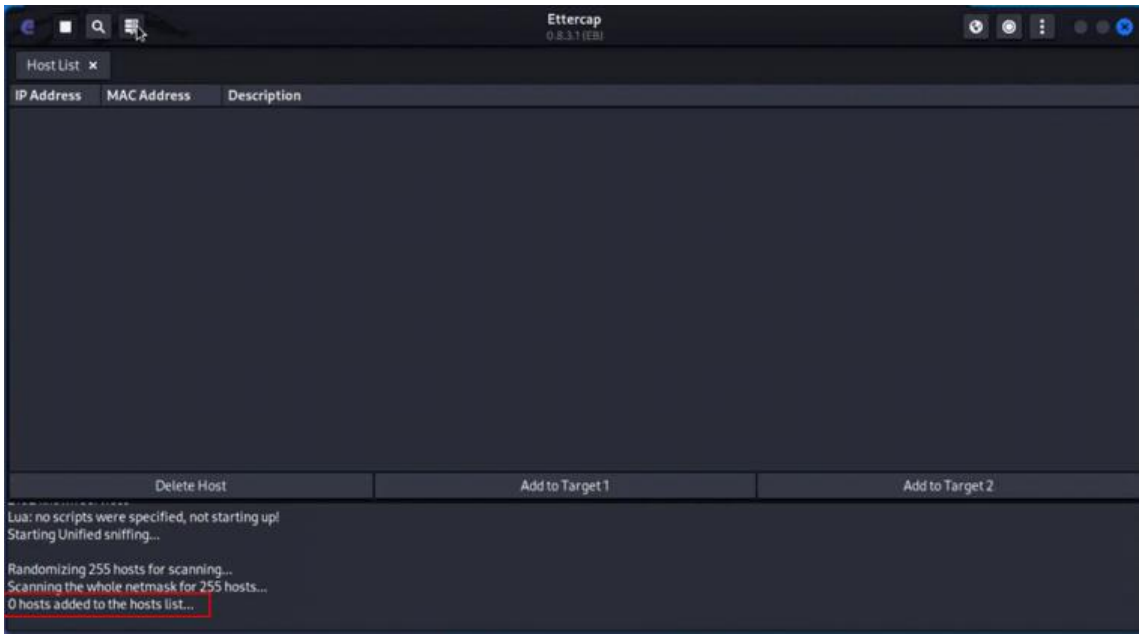
repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional



ATAQUE POR ETHERCAP DESPUÉS DE LA IMPLEMENTACIÓN DE LA VPN

Posteriormente, se activó la VPN "Master_GSVPN" e intentamos replicar todos los pasos anteriores para conseguir los datos de inicio de sesión. Se inició el programa ETHERCAP y se comenzó a escanear los dispositivos conectados a la red. Sin embargo, esta vez el programa no mostró ninguna máquina conectada, impidiendo así continuar con los pasos necesarios para lanzar el ataque.



repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

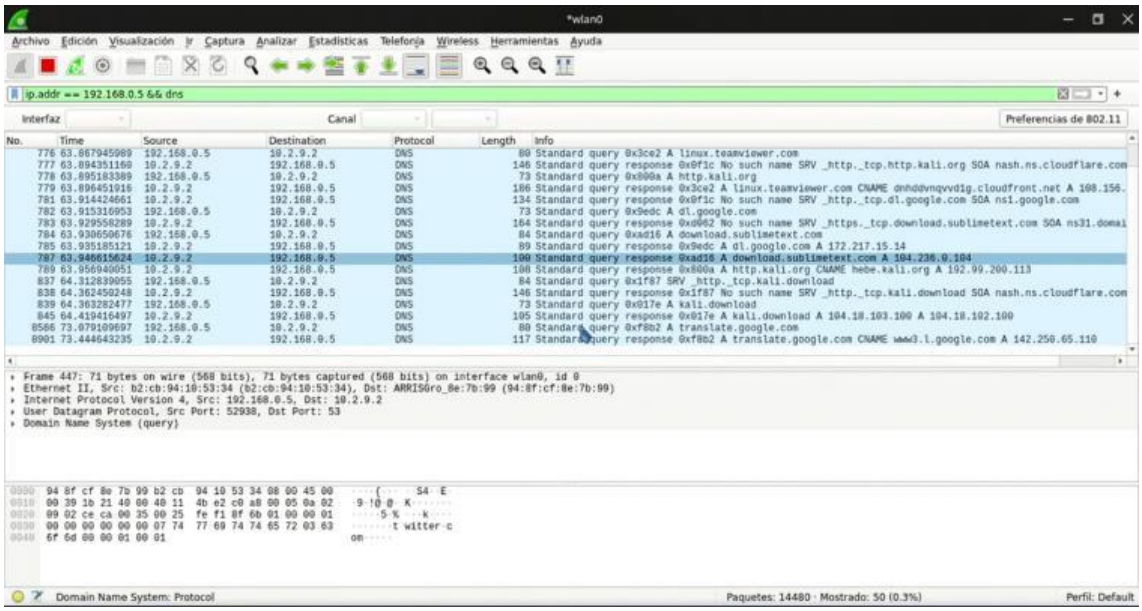
ATAQUE POR MAN-IN-THE-MIDDLE CON WIRESHARK ANTES DE LA IMPLEMENTACIÓN DE LA VPN

Un ataque Man-in-the-Middle (MitM) es una técnica en la que un atacante se inserta furtivamente en una comunicación entre dos partes, interceptando y posiblemente alterando los datos transmitidos sin que las partes lo perciban. Este tipo de ataque permite al intruso capturar información sensible, como credenciales de inicio de sesión, y puede incluso modificar los mensajes intercambiados para su propio beneficio. Si una persona maliciosa lograba tener acceso a la red de la empresa, podía desplegar algunos programas que le permitían escanear los datos, interceptarlos y fungir como intermediario, obteniendo así información valiosa. Uno de los programas más utilizados para esta técnica era Wireshark.

Wireshark es una herramienta que permite capturar y analizar paquetes de datos intercambiados a través de protocolos web y de red. Usando Wireshark dentro de la red, se intentó capturar los datos de un usuario que también estaba conectado y navegaba por la red. Para la prueba, el trabajador realizó búsquedas sobre algunos programas y abrió páginas como Google.com, Twitter.com y Google Translate. Mediante la herramienta, se pudo ver y captar paquetes con facilidad. Una vez interceptados los datos, se pudo establecer un ataque de Man-in-the-Middle como se muestra a continuación.

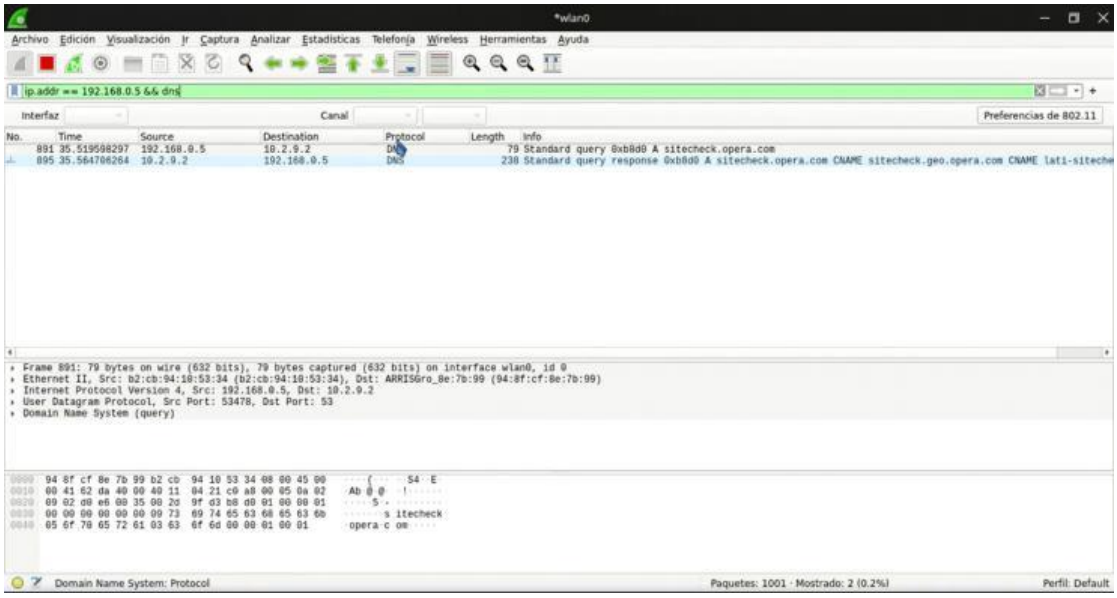
repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional



ATAQUE POR MAN-IN-THE-MIDDLE CON WIRESHARK DESPUÉS DE LA IMPLEMENTACIÓN DE LA VPN

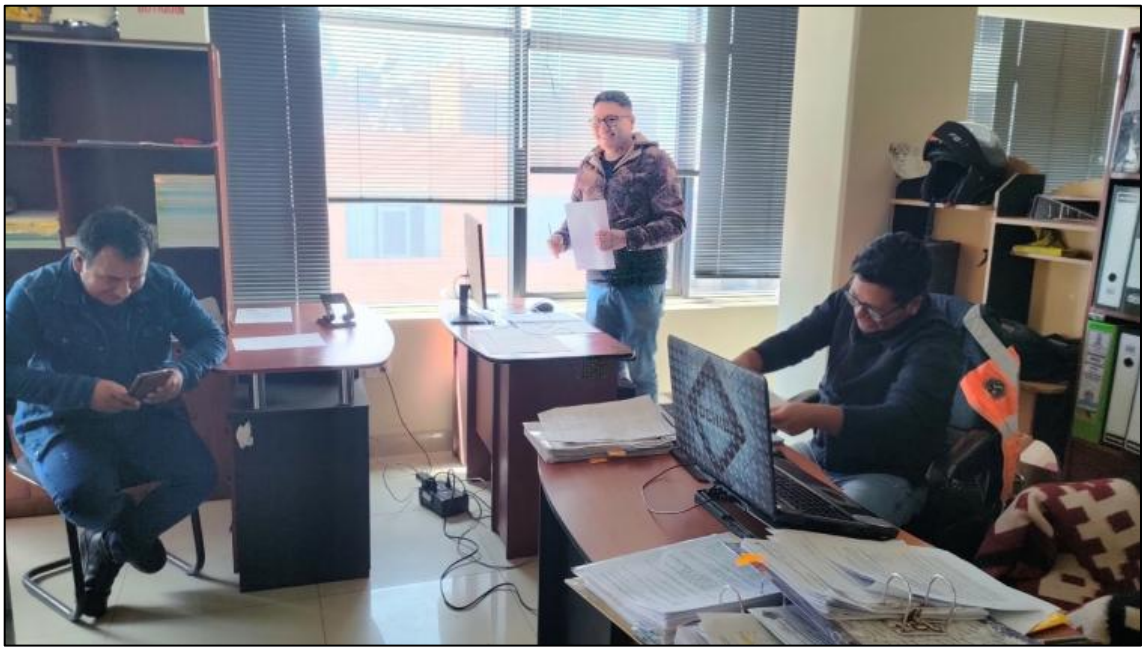
Posteriormente, se activó el servidor VPN y se intentó interceptar los datos de navegación del trabajador, quien repitió las mismas acciones anteriores. Sin embargo, se notó que el programa Wireshark tuvo una mayor dificultad para poder interceptar los paquetes de comunicación, demostrando así la efectividad de la VPN en proteger la red contra este tipo de ataques.



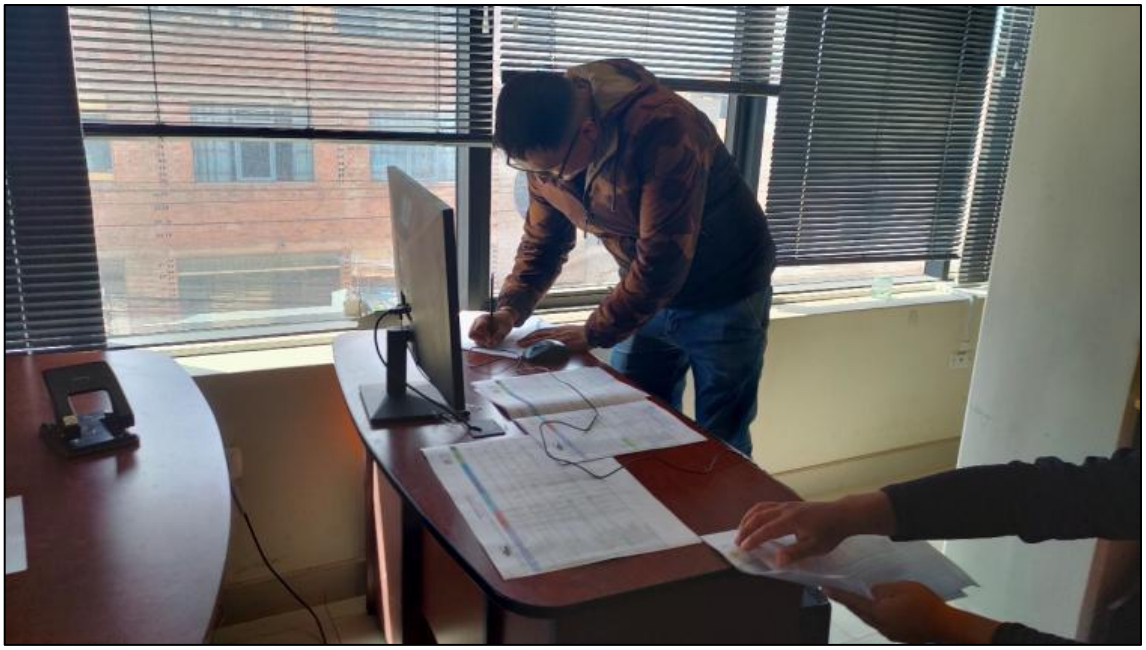
repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

ANEXO 9 Panel Fotográfico



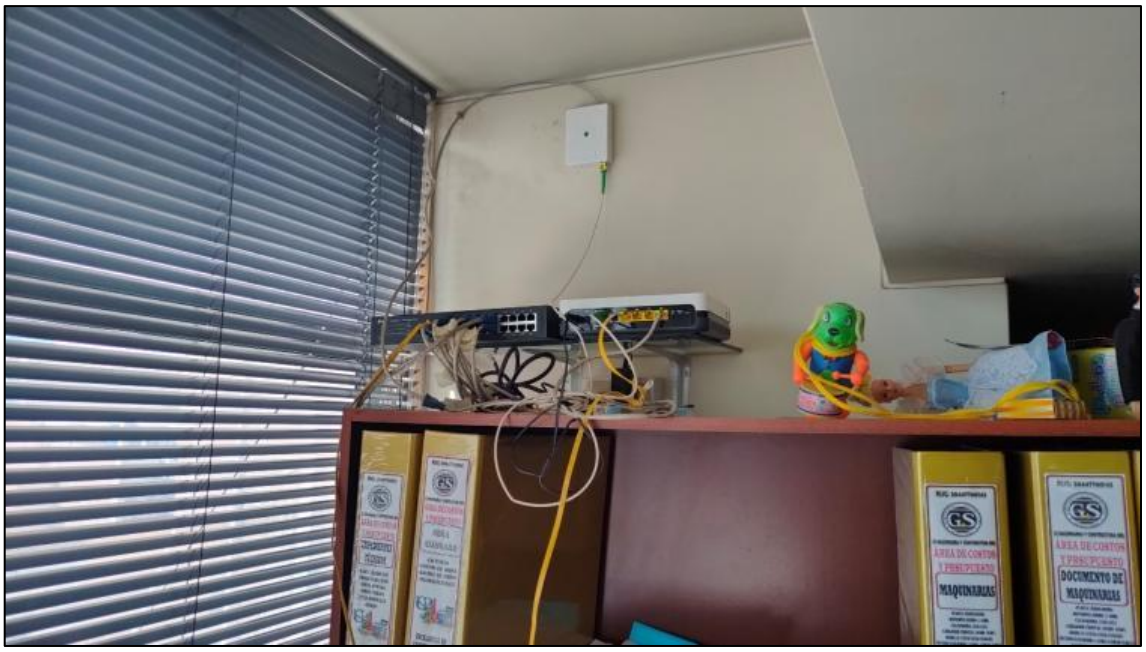
Nota: Se hace la respectiva entrevista y evaluación con el instrumento de investigación, con lo que se pudo conversar con el personal de GS como el jefe el Sr. Abelardo al lado izquierdo.



Nota: En esta fotografía se está recopilando la información de las computadoras como su topología lógica y física de la red.

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional



Nota: Se logra apreciar los equipos de comunicación de la segunda planta de GS. Se ve claramente un router (color blanco) de la empresa Movistar que está repartiendo a un Switch (color negro). Del mismo modo que reparte a la tercera planta por otro cable UTP.

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

ANEXO 10 Declaración jurada de autenticidad de tesis

Universidad Nacional del Altiplano Puno | Vicerrectorado de Investigación | Repositorio Institucional

DECLARACIÓN JURADA DE AUTENTICIDAD DE TESIS

Por el presente documento, Yo YARMANDU KEVIN ACERO ZANABRIA,
identificado con DNI 70465080 en mi condición de egresado de:

☒ **Escuela Profesional,** ☐ **Programa de Segunda Especialidad,** ☐ **Programa de Maestría o Doctorado**
INGENIERIA DE SISTEMAS,
informo que he elaborado el/la ☒ **Tesis** o ☐ **Trabajo de Investigación** denominada:
"DISEÑO DE UNA RED PRIVADA (VPN) BASADO EN SOFTWARE LIBRE PARA MEJORAR LA SEGURIDAD DE LA INFORMACION EN LA EMPRESA GS MAQUINARIAS Y CONSTRUCTORA E.I.R.L. JULIACA, 2023."

Es un tema original.

Declaro que el presente trabajo de tesis es elaborado por mi persona y **no existe plagio/copia** de ninguna naturaleza, en especial de otro documento de investigación (tesis, revista, texto, congreso, o similar) presentado por persona natural o jurídica alguna ante instituciones académicas, profesionales, de investigación o similares, en el país o en el extranjero.

Dejo constancia que las citas de otros autores han sido debidamente identificadas en el trabajo de investigación, por lo que no asumiré como suyas las opiniones vertidas por terceros, ya sea de fuentes encontradas en medios escritos, digitales o Internet.

Asimismo, ratifico que soy plenamente consciente de todo el contenido de la tesis y asumo la responsabilidad de cualquier error u omisión en el documento, así como de las connotaciones éticas y legales involucradas.

En caso de incumplimiento de esta declaración, me someto a las disposiciones legales vigentes y a las sanciones correspondientes de igual forma me someto a las sanciones establecidas en las Directivas y otras normas internas, así como las que me alcancen del Código Civil y Normas Legales conexas por el incumplimiento del presente compromiso

Puno 05 de JUNIO del 2024

FIRMA (obligatoria)

Huella

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis

UNIVERSIDAD
NACIONAL DEL ALTIPLANO
Repositorio Institucional

ANEXO 11 Autorización para el depósito de tesis en el Repositorio Institucional

Universidad Nacional del Altiplano Puno | VRI Vicerrectorado de Investigación | Repositorio Institucional

DECLARACIÓN JURADA DE AUTENTICIDAD DE TESIS

Por el presente documento, Yo YARMANDU KEVIN ACERO ZANABRIA,
identificado con DNI 70465080 en mi condición de egresado de:

☒ **Escuela Profesional,** ☐ **Programa de Segunda Especialidad,** ☐ **Programa de Maestría o Doctorado**
INGENIERIA DE SISTEMAS,
informo que he elaborado el/la ☒ **Tesis** o ☐ **Trabajo de Investigación** denominada:
" DISEÑO DE UNA RED PRIVADA (VPN) BASADO EN SOFTWARE LIBRE PARA MEJORAR LA SEGURIDAD DE LA INFORMACION EN LA EMPRESA GS MAQUINARIAS Y CONSTRUCTORA E.I.R.L. JULIACA, 2023. "

Es un tema original.

Declaro que el presente trabajo de tesis es elaborado por mi persona y **no existe plagio/copia** de ninguna naturaleza, en especial de otro documento de investigación (tesis, revista, texto, congreso, o similar) presentado por persona natural o jurídica alguna ante instituciones académicas, profesionales, de investigación o similares, en el país o en el extranjero.

Dejo constancia que las citas de otros autores han sido debidamente identificadas en el trabajo de investigación, por lo que no asumiré como suyas las opiniones vertidas por terceros, ya sea de fuentes encontradas en medios escritos, digitales o Internet.

Asimismo, ratifico que soy plenamente consciente de todo el contenido de la tesis y asumo la responsabilidad de cualquier error u omisión en el documento, así como de las connotaciones éticas y legales involucradas.

En caso de incumplimiento de esta declaración, me someto a las disposiciones legales vigentes y a las sanciones correspondientes de igual forma me someto a las sanciones establecidas en las Directivas y otras normas internas, así como las que me alcancen del Código Civil y Normas Legales conexas por el incumplimiento del presente compromiso

Puno 05 de JUNIO del 2024

FIRMA (obligatoria) Huella

repositorio.unap.edu.pe
No olvide citar adecuadamente esta tesis