OFICINA DE POSGRADO

Tema:

RED SEGURA EN LAS AGENCIAS DE LA COOPERATIVA DE AHORRO Y CRÉDITO SEMILLA DEL PROGRESO

Proyecto de investigación previo a la obtención del título de Magister en Ciberseguridad

Línea de Investigación:

PROTECCIÓN DE DATOS Y COMUNICACIONES

Autor:

David Elías Guamán Condolo

Director:

Mg. Alberto Leopoldo Arellano Aucancela

Ambato – Ecuador

Enero 2024

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE AMBATO

APROBACION DEL TRIBUNAL DE GRADO

Tema:

RED SEGURA EN LAS AGENCIAS DE LA COOPERATIVA DE AHORRO Y CRÉDITO SEMILLA DEL PROGRESO

Línea de Investigación:

PROTECCIÓN DE DATOS Y COMUNICACIONES

Autor:

David Elías Guamán Condolo

Alberto Leopoldo Arellano Aucancela, Ing. Mg. f._____
CALIFICADOR

Verónica Maribel Pailiacho Mena, Ing. Mg. f._____
CALIFICADOR

Galo Mauricio López Sevilla, Ing. Mg. f._____
CALIFICADOR

Juan Carlos Acosta Teneda, P. PhD. f._____
OFICINA DE POSGRADOS

Hugo Rogelio Altamirano Villarroel, Dr. f._____
SECRETARIO GENERAL PUCESA

Pontificia Universidad Católica del Ecuador
SECRETARIA GENERAL
PROCURADURÍA

Ambato – Ecuador

Diciembre 2023

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo: **DAVID ELÍAS GUAMÁN CONDOLO**, con **cédula de ciudadanía 1104958424**, autor del trabajo de graduación titulado: "RED SEGURA EN LAS AGENCIAS DE LA COOPERATIVA DE AHORRO Y CRÉDITO SEMILLA DEL PROGRESO", previo a la obtención del título profesional de **MAGISTER EN CIBERSEGURIDAD**, en la **OFICINA DE POSGRADO**

1. Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través del sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de la Universidad.

Ambato, enero 2024

David Elías Guamán Condolo

CC. 1104958424

DEDICATORIA

Este proyecto está dedicado:

A Dios por estar siempre en todos los momentos como guía y fortaleza durante mi vida y sobre todo en este proceso académico.

A mi madre María Alejandrina Condolo y a mi padre Manuel Luis Guamán por su apoyo incondicional durante todo el proceso de mi formación profesional ya que con sus oraciones, consejos y palabras de aliento hicieron de mí, una persona perseverante y capaz para lograr cumplir todos mis sueños.

A mi compañera sentimental Georgina Suarez y a mi hijo Elián Guamán quienes son mi inspiración y mi apoyo, porque siempre me extienden su mano en los momentos más difíciles, GRACIAS por el amor brindado y siempre los llevaré presentes en mis actividades.

AGRADECIMIENTO

Mi gratitud siempre irá dirigida a Dios por la vida, las bendiciones derramadas sobre mí y toda mi familia. Mi profundo agradecimiento a mi familia, a mi compañera sentimental y a mi hijo por la paciencia y por confiar en mis capacidades para dar un paso más en mi desarrollo profesional.

De igual manera extiendo mis agradecimientos a los docentes de la Pontificia Universidad Católica del Ecuador sede Ambato por brindarme este espacio para crecer en conocimientos, gracias a sus valiosas enseñanzas porque hicieron que cada momento aprenda nuevas cosas. Gracias por la paciencia, dedicación y amistad.

Por otra parte, quiero expresar mi más grande y sincero agradecimiento al Mg. Alberto Arellano, por su colaboración, paciencia, compromiso y dedicación durante todo mi proceso de titulación. Gracias por siempre estar al pendiente resolver ante cualquier duda y se resolver de mejor manera.

RESUMEN

En la Cooperativa de Ahorro y Crédito Semilla del Progreso, existe un déficit en la comunicación, ya que las agencias no se interconectan por un mismo enlace de datos que brinde seguridad y esta es una debilidad muy importante, por ello, se necesita de una comunicación y un intercambio de datos seguro que permita a que todas las agencias garanticen la seguridad de la información para la modificación y trasmisión de forma segura hasta llegar al servidor de base de datos de manera íntegra y confiable. El objetivo del presente trabajo de investigación es mejorar la seguridad en las comunicaciones a través de una red privada local de las agencias de la Cooperativa de Ahorro y Crédito Semilla de Progreso, por lo tanto, se propone la implementación de una red privada virtual (VPN) basada en OpenVPN, brindando una solución sólida y confiable; para lograr este objetivo se necesita configurar una VPN en una distribución de Linux que brinde integridad, confiabilidad ya que el tráfico viaja a través de un túnel de forma encriptada, para ello se emplea una investigación cuantitativa y un diseño no experimental. Con este trabajo de investigación se espera que la COAC Semilla del Progreso, proteja sus activos de información y pueda mitigar posibles riesgos, brindando seguridad y confianza a sus socios e inversionistas.

Palabras Claves: Encriptación, Linux, VPN, OpenVPN, Túnel.

ABSTRACT

In the Cooperativa de Ahorro y Crédito Semilla del Progreso, there is a deficit in communication, since the agencies are not interconnected by the same data link that provides security and this is a very important weakness, therefore, a secure communication and data exchange is needed that allows all the agencies to guarantee the security of the information for the modification and transmission in a secure way until reaching the database server in an integral and reliable way. The objective of this research work is to improve the security of communications through a local private network of the agencies of the Cooperativa de Ahorro y Crédito Semilla de Progreso, therefore, the implementation of a virtual private network (VPN) based on OpenVPN is proposed in the COAC Semilla del Progreso, providing a solid and reliable solution and all this is done by configuring a VPN in a Linux distribution providing integrity, reliability as traffic travels through an encrypted tunnel, for this, the type of research used is quantitative and non-experimental design. With this research work, it is expected that COAC Semilla del Progreso will protect its information assets and mitigate possible risks, providing security and confidence to its partners and investors.

Keywords: Encryption, Linux, VPN, OpenVPN, Tunnel.

ÍNDICE GENERAL DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

En la actualidad el internet se ha convertido en una herramienta fundamental ya que el mundo se interconecta gracias a las redes de comunicación, debido a que ofrecen ventajas y distintas posibilidades de comunicación de manera óptima y eficiente, implementando soluciones de seguridad para mitigar los riesgos constantes.

En este aspecto una de las tecnologías de comunicación que brinda la protección de datos en su transmisión son las redes privadas virtuales o comúnmente conocidas como VPN que se ha convertido en una alternativa práctica y segura en las comunicaciones de las empresa, instituciones u organismos; las mismas que utilizan una infraestructura pública como Internet para crea un canal de comunicación privada. (Zapata, Pacheco, De la Torre, & Vallejo, 2017)

Las empresas usan las redes privadas virtuales porque permiten crear una conexión segura y cifrada hacia otra red a través del Internet, creando así un túnel cifrado de comunicación para mantener la privacidad de la información, debido a que la mayoría de las empresas usan el internet como una herramienta fundamental de trabajo. (Aliaga & Asamba, 2021)

En la Cooperativa de Ahorro y Crédito Semilla del Progreso, no existe una comunicación cifrada, ya que todas las agencias no se interconectan por un mismo enlace de datos, cinco de las agencias tiene el servicio de internet por medio de un proveedor seguro, por otro lado la dificultad de acceso a los territorios por la zona geográfica en las que se ubican hace que dos agencias se interconectan a través de otro proveedor, el mismo que no presta las condiciones de seguridad óptima en los enlaces de datos.

Para la Cooperativa de Ahorro y Crédito Semilla del Progreso, el riesgo siempre está presente, ya que el activo de información puede ser alterado o manipulado. En dos agencias el problema es frecuente por la zona geográfica en la que se encuentran y cabe mencionar que no existe otro proveedor de servicio de internet para este sitio, adicionalmente el tipo de información que se genera y transmite en

la dentro de la entidad financiera es altamente confidencial en todas las agencias. Esta información al estar expuesta corre el riesgo de fuga, porque su transmisión se realiza de manera abierta a través de internet. En la cooperativa el activo con mayor valor es la información de los quince mil socios, cuentas bancarias, inversiones y créditos, así como la información de los proveedores de la cooperativa. Por esta razón, el presente trabajo de titulación propone mitigar los riesgos cifrando el tráfico ante posible pérdida de paquetes disminuyendo el riesgo mediante la implementación de una red privada virtual.

En este trabajo de titulación se realiza el mejoramiento de la seguridad en las comunicaciones a través de una red privada virtual en las agencias de la Cooperativa de Ahorro y “Crédito Semilla del Progreso”, en primera instancia se realizará la fundamentación teórica en lo que respecta a la red segura en instituciones financieras, como segunda etapa se realizará un diagnóstico de los enlaces de cada una de las agencias a un servidor de base de datos y web en la nube; cabe mencionar que por seguridad de la institución todo el proceso se realiza a un servidor de pruebas, para luego definir una metodología para la implementación de una red segura y por último se desarrolló la propuesta de implementación de una red privada virtual sobre una infraestructura tecnológica en la nube a través de un servidor OpenVPN.

El objetivo principal del presente trabajo es mejorar la seguridad en la comunicación de las agencias de la Cooperativa de Ahorro y “Crédito Semilla de Progreso” Cía. Ltda. Usando la tecnología VPN y la herramienta OpenVPN de esta manera mitigar los riesgos de perdida de datos en la capa de red, debido a que es una solución de código abierto que admite clientes multiplataforma y su implementación se hizo en una distribución de Linux, haciendo uso la infraestructura de hardware y software existente de la cooperativa.

Una red privada virtual está diseñada para acceder a los recursos que tiene la cooperativa en uno de los servidores el cual se conecta todas las agencias, facilitando el acceso a través de un amplio número de dispositivos seguros, la tecnología aporta a la institución a mejorar su seguridad de esta manera garantizar a los socios que su información está protegida.

CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA

En el presente trabajo de investigación se agrupan diferentes artículos de varios autores en donde mencionan la seguridad en el ámbito internacional, nacional y a nivel local las cuales tiene relación con las entidades financieras, problemas en la protección de datos y en la seguridad de la información en la capa de red por donde viaja la información.

Ciberseguridad a nivel internacional

Según la OEA (2023) en su reporte sobre la fuerza laboral en ciberseguridad menciona que la pandemia y la pospandemia han generado un fuerte impacto en la economía global y un amplio crecimiento de amenazas, riesgos y cambio laboral. El gran aumento de amenazas cibernéticas, los esfuerzos por aumentar las capacidades en ciberseguridad han crecido y la escasez de personal capacitado y calificado pone en desventaja a las instituciones ante esta creciente necesidad.

Los ataques en el ámbito cibernético en los últimos años en contra del interés de las naciones y empresas privadas han incrementado la curiosidad por aplicar en el área de protección de datos, como resultado de estos sucesos las empresas están aumentando los esfuerzos por la defensa de los activos de información más críticos. (Carlini, 2016)

La creación de estrategias cibernéticas en cada una de la capa de protección, pueden ser mecanismos esenciales para prevenir los riesgos, porque las ciberamenazas pueden poner en peligro o perder el control de la infraestructura informática de las organizaciones o empresas.

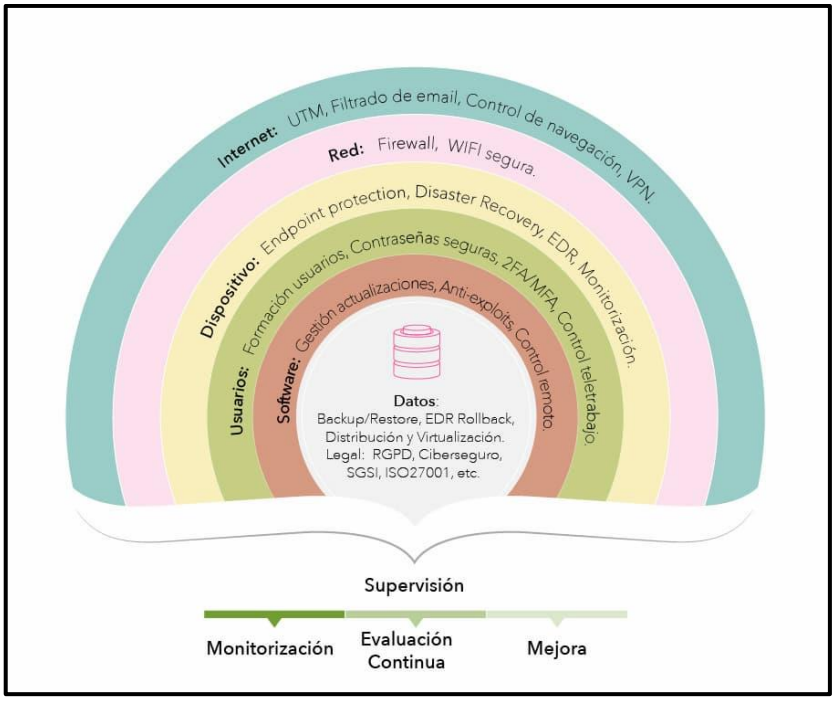
En la actualidad las sociedades occidentales dependen de las aplicaciones informáticas para todos los procesos industriales, fábricas, comercios, bancos entre otras organizaciones, las políticas de seguridad informática son reglas que se debe cumplir con el fin de asegurar la integridad, disponibilidad y privacidad de las infraestructuras, entonces la seguridad informática es una prioridad y nace al mismo tiempo que el internet. (Carisio, 2020)

La ciberseguridad se genera con la combinación de métodos, reglas y habilidades que permiten mejorar los niveles de protección de riego de información y de esta manera proteger su integridad y disponibilidad, para ello, se debe tomar en cuenta los niveles de riesgo para lograr una protección eficaz de la información a nivel del hardware, software y de comunicación.

Como lo menciona Raboyo (2022) en su tesis, describe a la Ciberseguridad como un estado deseable para que un sistema de información permita resistir a los eventos de ciberespacio cuyo objetivo es aseguras la confidencialidad, integridad y disponibilidad de la información mientras está siendo procesada, almacenada y trasportada de acuerdo a las normas de la Agencia de Seguridad de la Información.

En la actualidad se cuenta con información importante que proteger ya sea en dispositivos, aplicaciones, factor humano, red interna y todo lo que se conecta al internet, el esquema que puede ser complejo por ello surge medidas de protección por capaz es salvaguardar el activo más importante que son los datos, recomendadas por García (2021) para ello definen las siguientes capas:

Figura 1: Capas de protección de datos.



Fuente: (García, 2021)

Ciberseguridad a nivel nacional y Latinoamericana

Según, la publicación del periódico “La República”, señala, en el Reporte de Ciberseguridad 2020 del Banco Interamericano de desarrollo, la pandemia mundial del COVID-19 ha marcado un punto de inflexión y de necesidad por la dependencia de la infraestructura tecnológica. Incluso en las instancias más críticas de la pandemia el Internet ha hecho lo posible por la provisión de servicios esenciales y ha permitido a las empresas continuar operando y manteniendo al mundo en contacto. El resultado de esta transición ha sido un extraordinario aumento de posibilidades para los ataques cibernéticos, debido a que en el contexto de un ecosistema digital se incluyen más de 20.000 millones de dispositivos conectados en todo el mundo.

Según el Índice Global de Ciberseguridad 2017 (IGC), de la UIT del 6 de julio del 2017, Ecuador se encuentra en la etapa de maduración, pues está desarrollando compromisos complejos a favor de la prevención de este tipo de delitos que incluyen la participación en iniciativas y programas de seguridad cibernética.

Ecuador tiene una tarea pendiente en el tema de seguridad debido a que a nivel regional es uno de últimos países por delante de Venezuela y Bolivia, según el Índice Global de Ciberseguridad en 2018. Además, señala que el Ecuador fue calificado con 0.367 puntos lo cual está en el grupo de interés medio de compromisos.

Seguridad de la información en instituciones financieras

Las amenazas constantes de la seguridad de la información han ido evolucionando de manera frecuente en el mundo digital moderno, muy independiente del tamaño y su naturaleza las empresas se encuentran bajo amenazas de riegos cibernéticos.

Entre los desafíos que enfrentan las entidades de la Economía Popular y Solidaria está la seguridad en los servicios financieros digitales para mantener un equilibrio entre la seguridad y la experiencia del usuario, la importancia de la protección de datos personales y la privacidad; así como las normas y directrices claras que

permitan contar con mecanismos para proteger los datos frente a las amenazas generando confianza frente los socios.

De acuerdo con las declaraciones de Margarita Hernández Naranjo en torno a los retos para Superintendencia de Economía Popular y Solidaria (SEPS) ante los riegos de ciberseguridad menciona que, en el año 2020 represento el 18.41% del PIB ha sido uno de los de mayor digitalización. Ya que cada vez es mayor el número de socios y/o clientes que hacen uso de los sistemas financieros por medios electrónicos; es así que el 53,20% de las transacciones de servicios financieros del sector son realizadas en canales electrónicos y ejecutadas por medio del Internet, seguidas de los servicios brindados por tecnología celular, con el 38,79%. Así mismo la demanda crece en torno a los servicios en canales digitales: 45% para crédito, 42% en cajeros automáticos, 38% en billetera electrónica, y 28% en transferencias electrónicas. (Itahora, 2021)

Se considera la Ciberseguridad entre los 5 riesgos globales más relevantes, por ellos surge la necesidad de las organizaciones en buscar una estrategia de protección alineados a los objetivos de negocio. Por ello la SEPS ha propuesto aumentar los esfuerzos con expertos en esta disciplina con el fin de promover reflexiones y acciones en materia de ciberseguridad ya que en muchos casos hay poca inversión en tecnología o en temas de seguridad y Ciberseguridad por parte de las entidades financieras.

Para Ginger Saltos Subgerente de Ciberseguridad del Banco de Guayaquil el análisis de gestión de riesgos de terceros debe ir más allá del análisis de riesgos específicos, hay que ampliar en todos los aspectos de giro de negocios de las organizaciones. (It Ahora, Deloitte, 2021)

Así mismo Juan Mejía Gerente de Seguridad de la Información de la cooperativa JEP menciona que no existe una normativa para proveedores externos por lo tanto no se ven obligados a un cumplimiento de seguridad y mantenimiento de datos, de modo que es obligación de las entidades que contrata este servicio. (It Ahora, Deloitte, 2021)

Según datos de la fiscalía general del Estado, hasta agosto de 2020, se registran 5048 denuncias por delitos informáticos en el Ecuador. El 92% se concentra en los delitos como: suplantación de identidad, falsificación y uso de documento falso y apropiación fraudulenta por medios electrónicos. (Hernández, 2022)

Dentro de las entidades financieras la información se encuentra en diferentes módulos que conforman el core-financiero cuyas actividades comprenden los siguientes: Gestión de usuarios, Gestión de perfiles y se considera la base de todo el sistema financiero. Junto a ello también se encuentra el control de red, control de acceso a los dispositivos e incluso la administración interna de la entidad.

Red privada virtual y tipos

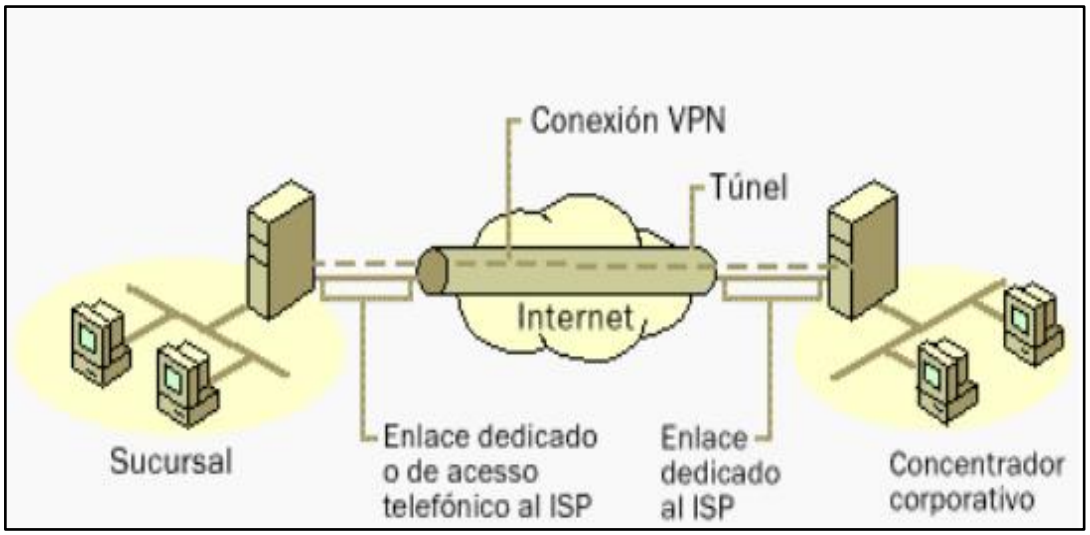
Una red privada virtual o también conocida como VPN se forman sobre una infraestructura de red pública. La VPN ofrece un uso asequible y competente del ancho de banda, funcionalidad escalable, flexible, conexiones seguras y remotas, ofreciendo una línea segura virtual entre dos sitios de red donde el tráfico pasa de un extremo a otro. (Abdulazeez, 2020)

Una Red Privada Virtual es una tecnología que establece una conexión virtual segura, conocida como túnel, diseñada sobre una red física insegura o una red pública de internet. Una VPN proporciona múltiples mecanismos de seguridad para proteger la información transmitida, y para permitir el acceso seguro y controlado a los recursos que protege. (Ministerio de Defensa, 2022)

El funcionamiento de una VPN depende de los elementos y factores que hace posible que la información sea transmitida a través de túneles virtuales, usando los procedimientos de seguridad que garanticen la confiabilidad e integridad de la información.

En la siguiente figura muestra los elementos de una conexión VPN, los cuales se describe también en la tabla 1:

Figura 2: Diferentes componentes de una conexión VPN



Fuente: (Jota, Ramirez, & Penagos, 2018)

Una Red Privada Virtual diseñada correctamente consta de varios elementos y brinda a las empresas muchos beneficios que son:

- Ampliación de la conectividad
- Reducción de costos
- Reducir tiempos de tráfico y traslado de usuarios
- Aumenta la producción
- Simplifica cualquier topología de red
- Brinda soporte mediante teletrabajo

Las funciones principales que tiene una VPN bien diseñada son:

- Seguridad
- Confiabilidad
- Escalabilidad
- Red y políticas administrables

Además, esta red debe tener los siguientes elementos:

Tabla 1: Elementos de una conexión con VPN

Elemento	Función
Servidor VPN	Administra los clientes VPN
Cliente VPN	Clientes remotos
Túnel	Encapsulación de datos
Conexión VPN	Encriptación de datos
Protocolos de Túnel	Administra los túneles
Datos del túnel	Se transmiten sobre el túnel
Red de Tránsito	Red pública de enlace

Fuente: Elaboración de propia

Las Red Privadas Virtuales envían la información de forma segura a través del Internet, las terminales pueden estar bastante lejos de las sucursales, oficinas y los socios comerciales en una red corporativa extendida, siendo una tecnología escalable lo que ayuda a ahorrar tiempo al crear un nuevo enlace entre la sede central y los nuevos edificios o sucursales mediante el uso de la infraestructura de proveedores de servicios de Internet (ISP).

La seguridad por medio de VPN cubre las siguientes características: confidencialidad, integridad de datos y autenticidad ya que tiene el mecanismo de cifrado y emplea mecanismo de hashing.

La implementación de VPN llega ser más económico en comparación con la implementación de comunicaciones seguras como enlaces privados dedicados o alquiler de infraestructura de empresa de telecomunicaciones. En cuestiones de ampliación de la infraestructura se puede realizar de manera simple es decir es escalables y su configuración es rápida, entonces la seguridad se vuelve flexible.

Las tecnologías VPN pueden ser implementadas mediante soluciones basadas en software o mediante soluciones software/hardware en equipos dedicados, a pesar de las ventajas que tiene esta tecnología hay que tomar en cuenta que se debe aseguras también de la red interna con el fin de garantizar la confidencialidad, integridad y disponibilidad de la comunicación a través del cual se transmite la información por medio de la infraestructura. (Ministerio de Defensa, 2022)

La VPN es una tecnología que permite tener conexiones seguras, remotas y cifradas hacia otra red a través del internet sin importar las distancias, es decir, dar conexión a oficinas o sucursales de una red corporativa reduciendo el tiempo y costos en la implementación de un nuevo enlace desde la matriz central a las otras sedes mediante el IPS.

En el mundo actual, radica la necesidad de cambio constante de información por medio del internet donde la información es confidencial, por lo que, debe ser trasportada por un medio que garantice la seguridad, confiabilidad de la comunicación y sobre todo que la información llegue de manera íntegra.

Las soluciones VPN que se suelen utilizar son GRE, IPSec, PPTP y TLS, las Redes Privadas Virtuales son complejas, por lo que, algunas implementaciones de VPN tienen vulnerabilidades de seguridad que aún no se han descubierto. (Winawang, 2021)

Funcionamiento de VPN

La comunicación que nace al usar una red privada virtual es mediante un túnel virtual de internet en donde los paquetes son enviados de manera segura encriptados y encapsulados en paquetes IP, en donde por medio de la tunelización proporciona al origen de datos la encapsulación de su datagrama, estos paquetes encapsulados brindan protección contra lectura o modificación a través de diferentes protocolos cifrados de datos, así lo menciona. (Pomar Pascual, 2019)

1.1. Tipos de redes privadas virtuales

Existen diferentes tipos de VPN que se describen a continuación:
VPN PPTP: Es una VPN utilizada por usuarios remotos para conectarse a través del Internet por medio de un usuario y una contraseña de autenticación, donde se requiere solamente un cliente VPN; es compatible con Linux, Mac y Windows. Su desventaja es que no ofrece codificación en los datos algo que es importante tener un nivel de seguridad a nivel empresarial.

VPN site to site: este tipo de VPN se utiliza para conectar diferentes agencias o sucursales de una empresa mediante una red pública, utiliza en cada extremo de la conexión un servidor VPN que trabaja como enrutador, donde el servidor origen hace una llamada al servidor de destino y para establecer la conexión se requiere que los dos se autentiquen. (Pomar Pascual, 2019)

VPN Híbrida: es una VPN de modo MPLS creada sobre la seguridad de IPSec, para funcionar necesita tener en un extremo un túnel VPN IPSec y en otro extremo una VPN MPLS, brindando los beneficios de seguridad igual a IPSec.

VPN basada en hardware

Una Red Privada Virtual basada en hardware usa equipos, dedicados como Reuters ya que son seguros y fáciles de usar, tiene un gran rendimiento y los procesos están dedicados al funcionamiento de la red, basados en Reuters encriptados donde requiere una configuración correcta y definida. Su instalación es fácil y rápida, aunque su costo es elevado. Poseen la capacidad de asegurar los paquetes que viajan en la red a través del tunneling, aunque su desventaja es el costo económico. (Quezada L., 2016)

VPN basada en el firewall

Este tipo de firewall aprovecha los mecanismos de seguridad del servidor como las restricciones de acceso a la red interna y realiza las traducciones de direcciones. La mayoría de los firewalls comerciales optimizan al núcleo del sistema operativo,

al despojar a los servicios innecesarios o peligrosos, proporcionando seguridad adicional para el servidor VPN. (Quezada L., 2016)

La VPN basada en firewall tiene la ventaja que simplifica las arquitecturas de red a un único punto de control de la seguridad, por lo que los encargados de la seguridad solo administran el firewall. El firewall autoriza o no el ingreso o la salida de la información es decir filtran las comunicaciones.

VPN basados en software

Ideal para ambos extremos de una VPN que no son controlados por la misma organización o cuando diferentes firewall y enrutadores se implementan dentro del mismo sistema. (Quezada L., 2016)

Para este caso se utiliza un servidor con un sistema operativo que puede ser Windows o Linux en el cual se instala o se habilita VPN y puede mantener habitados varios servicios al mismo tiempo que se establece una conexión a través de un cliente. La desventaja es que esta VPN puede ser afectada por la misma vulnerabilidad del sistema operativo.

1.2. Protocolos usados en VPN

El Protocolo IPsec

IPsec en una de las tecnologías de VPN de estándares abiertos para garantizar las comunicaciones privadas en las redes públicas, garantizando así la seguridad, confidencialidad y autenticidad de la información y se ha convertido en el control de seguridad de la capa de red más común, que suele utilizarse para crear una red privada virtual.

El protocolo IPSec es uno de los protocolos de seguridad muy importante lo usan muchas empresas actualmente, como: ASUS, AVM e incluso D-Link están integrando esta tecnología en sus equipos ya que proporcionan servicios de seguridad a la capa IP y todos los protocolos superiores como TCP, UDP. Las principales características de IPSec es que trabaja en la capa 3 del modelo OSI.

IPSec funciona con dos nodos por un lado está el túnel y por el otro está el trasporte.

El túnel se usa cuando se realiza transferencias de datos en redes públicas con el fin de mejorar la protección ante acceso o modificación no autorizadas, los datos se encriptan junto a la carga útil y el encabezado, añadiendo un nuevo encabezado al final.

El transporte se encarga de cifrar la carga útil de los paquetes de datos dejando el encabezado IP original, lo que facilita la identificación de la dirección de destino de cada uno de los paquetes. (De la luz, 2023)

IPSec se basa en el intercambio de claves en una comunicación para establecer la seguridad y luego enviar datos de un extremo a otro tanto modificando los paquetes IP originales o encapsulando el paquete original completo más la cabecera. Funciona combinando mecanismos fundamentales como la cabecera de autenticación (AH), Carga de seguridad encapsulada (ESP) y Fases de la negociación (IKE) junto a dos métodos de transmisión: modo túnel y el modo trasporte.

Fases de la negociación (IKE)

El protocolo de establecimiento y mantenimiento de las SA utilizado por IPSec se denomina IKE, su función principal es realizar el acuerdo de claves para las SAs. En donde se implementa la autenticación mutua en los dos extremos y se realiza el intercambio secreto de las claves para tener una sesión compartida.

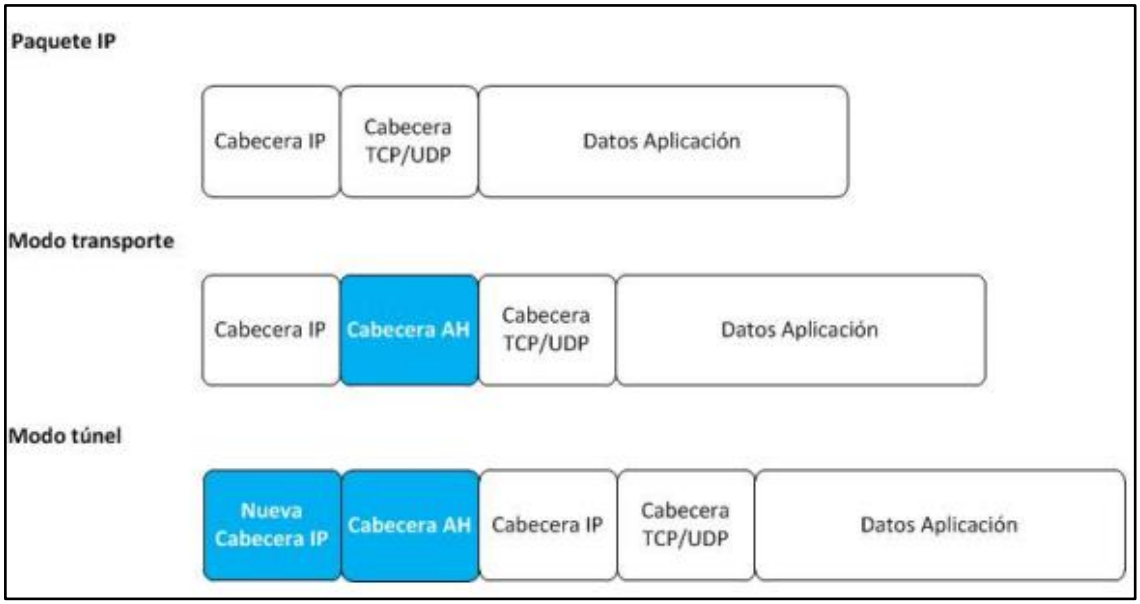
Existen dos versiones de protocolo IKEv1 e IKEv2, la segunda versión más actual que la primera

La seguridad que brinda IPSec se basa en dos protocolos diferentes que son el núcleo de la tecnología, por un lado, AH (Autentication Header, estandarizado en RFC 4302, y ESP (Encapsulating Security Payload, estandarizado en la RFC 4303).

Cabecera de autentificación (AH)

Brinda la identificación del origen, así como la integridad de datos, protección contra spoofing y ataques de repartición. Los mecanismos de autenticación se aplican a todo el paquete incluido los campos cambiantes como las direcciones IP. En la siguiente figura muestra el paquete cuando se utiliza el protocolo.

Figura 3: Construcción de paquete AH

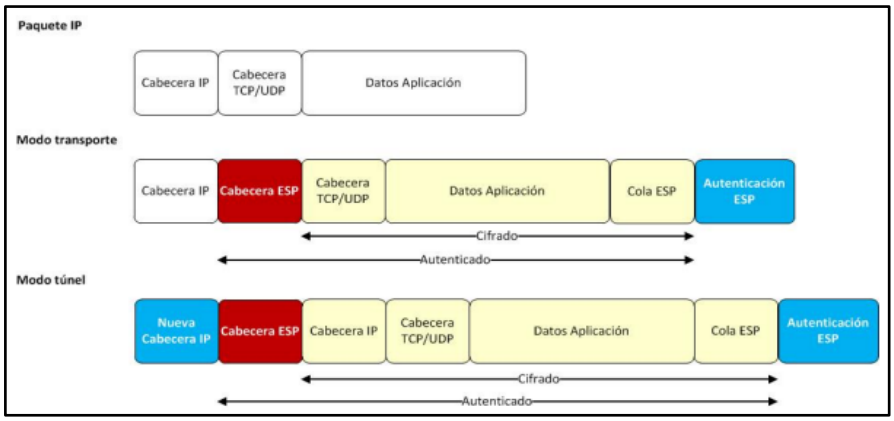


Fuente: (CN- PYTEC, 2018)

Carga de seguridad encapsulada (ESP)

ESP brinda la protección de la confidencialidad y la integridad de los paquetes IP, utiliza también autenticación extrema a extremo y el no repudio. A diferencia de AH aquí solamente autentica el Playload, por lo que cuando se trabaja en modo transporte no se autentica la cabecera IP del paquete. En la siguiente figura muestra un claro ejemplo de la carga de seguridad encapsulada. (CN- PYTEC, 2018)

Figura 4: Construcción de paquetes ESP



Fuente: (CN- PYTEC, 2018)

1.3. Túnel IP

1.4.

Un túnel IP es un canal de comunicación de la red del Protocolo de Internet. Se utiliza para transportar otros protocolos de red mediante encapsulación de sus protocolos de red en paquetes TCP/IP, paquetes que se transportan por Internet. Los túneles IP se utilizan para conectar dos redes IP separadas que no están directamente conectadas entre sí. (Matthews, 2020)

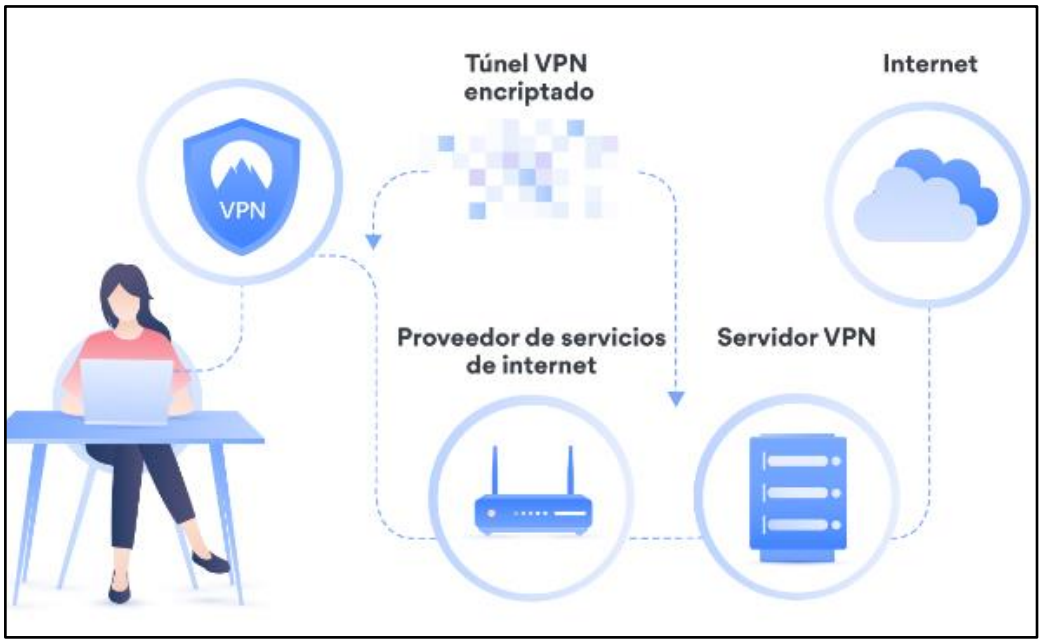
Se usan para conectar dos redes IP separadas que no cuentan con un enrutamiento nativo entre sí, por ello su conexión es a través de protocolo subyacente en una red de trasporte intermedia.

Túneles de VPN

Los túneles de VPN es una conexión encriptada entre las computadora o dispositivo móvil e internet en general. Gracias a que su conexión está encriptada, nadie a lo largo del túnel VPN puede interceptar, monitorear ni alterar sus comunicaciones. Los túneles pueden ocultar la naturaleza del tráfico que circula, utilizando estándares de encriptación para reempaquetar los datos de tráfico en una forma diferente. Los protocolos de tunelización funcionan utilizando la porción de datos del paquete (carga útil) para transportar paquetes que proporcionan servicios, utilizando modelos de protocolo por capas. (Matthews, 2020)

Túnel en VPN viene a ser la forma de conexión encriptada con el fin de proteger la comunicación para que no sea alterada y manipulada ocultando su tráfico circulante que difícilmente se puede identificar o rastrear su ubicación como se muestra en la siguiente figura. (Matthews, 2020)

Figura 5. Tráficos por medio de VPN



Fuente: (Matthews, 2020)

VPN Site-to-Site y VPN de acceso remoto

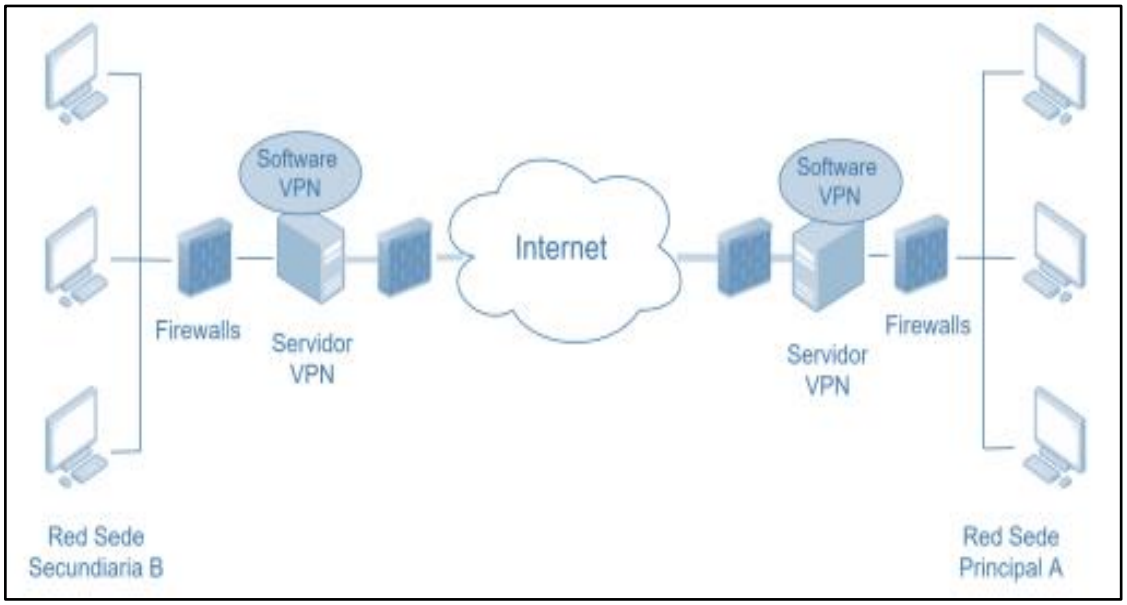
La VPN de acceso remoto proporciona acceso por comunicación remota de una organización a la red de origen, las solicitudes de acceso remoto son realizadas por un número cada vez mayor de usuarios que quieren acceder a la red de área local (LAN) de la corporativa, es decir, sin importar qué tipo de conexión que tengan las sedes o las casas de los usuarios, tan sólo necesitan acceso del IPS y utilizar el mismo protocolo VPN para conectarse a la red. (Aragón, 2021)

VPN de Acceso Remoto es un tipo de VPN que crea una ruta segura y fija entre un sitio y otro, es decir, entre la sede central y las sucursales a través de Internet, entonces los ordenadores situados en la LAN de la sucursal pueden acceder a los datos situados en la LAN de la oficina central. (Zhiwei & Jie, 2020)

En cualquiera de las tecnologías de puede tener conexión sitio a sitio o acceso remoto lo que significa tener conectividad entre las agencias y la matriz de una organización y también permitiría conectar 2 o más hogares entre sí para tener acceso a todos los recursos compartidos, como si estuviera físicamente; entonces el servidor VPN se encarga de hacer este vínculo permanente a internet y acepta todas las conexiones que provienen de otros sitios y establece el túnel VPN.

En el VPN site-to-site se implementa un servidor VPN, en cada extremo de la comunicación, para que exista la conexión segura entre ambos servidores el tráfico es automáticamente enrutando a través de la VPN implementada, como muestra la figura siguiente.

Figura 6. VPN site-to-site



Fuente: (Ministerio de Defensa, 2022)

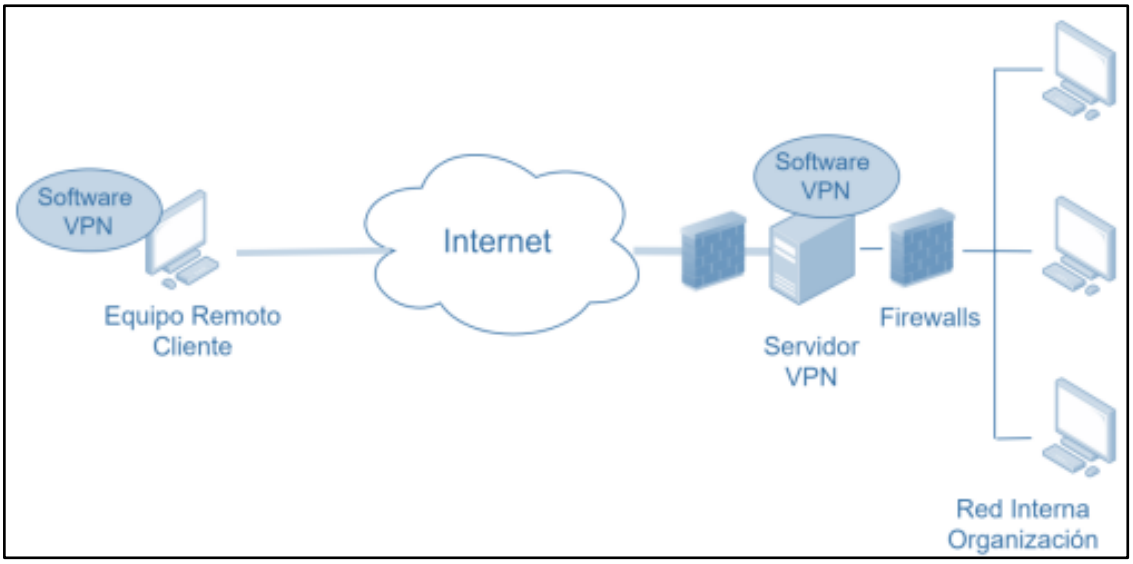
VPN de acceso remoto

Las tecnologías de comunicación de acceso remoto realizan una conexión desde un sitio a otro que pueden ser muy distantes en el ámbito geográfico, se ha vuelto importante en el mundo de las redes porque las empresas promueven el trabajo desde diferentes lugares como las sucursales donde los empleados tienen acceso a la red privada de la organización, haciendo usos de los recursos tecnológicos que dispone la empresa.

Como lo menciona el Ministerio de Defensa (2022) en su informe, una VPN de acceso remoto es empleada para proteger las comunicaciones entre los equipos de un usuario y la red interna de las empresas, se emplea para los usuarios que trabajan de forma remota y usan recursos internos de la empresa a través de la infraestructura proporcionada por la red pública**.**

En este tipo de VPN el cliente debe tener configurado en su terminal el VPN, y su conexión a la red de la organización se da por medio de la autenticación como muestra la siguiente figura.

Figura 7. VPN de acceso remoto



Fuente**:** (Ministerio de Defensa, 2022)

OpenVPN

El servidor OpenVPN Access es una de las soluciones VPN, es muy adecuada para empresas particulares porque es fácil de configurar y se puede instalar en un servidor local. De acuerdo con Quishpe (2021) OpenVPN no es solo un protocolo de comunicación sino también es una aplicación de código abierto que permite conexiones VPN con licencia de software libre.

La seguridad y la estabilidad del acceso mediante OpenVPN tienen una calidad de servicio que se acerca al acceso directo, tiene una diferencia de paquetes enviados

en comparación con los paquetes recibidos en torno al 1,7%. Además, OpenVPN ofrece una alternativa liviana y rentable en comparación con otras tecnologías VPN y se adaptan al mercado de pequeñas y medianas empresas.

Características de OpenVPN

Las principales características que tiene de OpenVPN es que usa un adaptador de red Ethernet virtual en el puerto UDP y TCP, usa herramientas para encriptar y autenticar la información, por ende, la certificación de biblioteca SSL permite proteger la red privada, además de usar el cifrado convencional en base a clave estática o el cifrado de clave pública qué se basa en certificados. Utiliza cifrado de 256 bits, SSL permite tener comunicaciones seguras al momento de usar el internet y finalmente OpenVPN crea la red de túneles a través de firewall o túneles sobre NAT.

Arquitectura de OpenVPN

La arquitectura de OpenVPN está diseñada para trabajar en multiplataforma y brinda estabilidad, escalabilidad ya que su instalación es muy fácil, soporta IP dinámicas y NAT, en su módulo completo admite métodos de autenticación alternativos. De manera que trabaja en varias plataformas como Solaris, Linux, Mac OpenBSD y Windows. (Quishpe Iza, 2021)

Autenticación de OpenVPN

Clave estática

Desde el punto de vista de Valburg (2018) este modo de autenticación las claves de sesión ya han sido distribuidas antes de iniciar la conexión, lo que es usada como mecanismo de autenticación y para cifrar/descifrar los datos del túnel. Pero se omite al protocolo de enlace TLS y el posterior intercambio de claves y tampoco proporciona confidencialidad hacia delante ya que una nueva clave no se puede renegociar sobre la marcha y deberá redistribuirse fuera de la sesión.

Autenticación TLS

La biblioteca SSL/TLS puede utilizarse para realizar la autenticación y encriptación, ya que cada cliente que se conecta generará dinámicamente una nueva clave para su sesión y renegociará las claves después de que se cumplan ciertos criterios. OpenVPN usa el protocolo TLS para asegurar un canal que luego se usa para negociar una clave y opcionalmente para autenticar las credenciales del usuario.

Esta clave de sesión es el equivalente a la clave pre distribuida en modo de clave estática y se utiliza para cifrar el túnel de datos y esta biblioteca forma parte de OpenSSL, que se instala en la mayoría de los sistemas operativos modernos. Las sesiones TLS con autenticación bidireccional son negociadas entre el cliente y el servidor**,** es decir, ambos deben presentar sus propios certificados y se utiliza para generar de forma segura las claves de sesión.

Diferencia entre OpenVPN y otros paquetes VPN

Dentro de las grandes ventajas que se puede encontrar están que OpenVPN es multiplataforma, puede hacer uso de OpenSSL o PolarSSL, ofrece una interfaz de gestión para el control de forma remota o gestionar de forma centralizada un dominio de OpenVPN, ha sido diseñado para operar de manera confiable en redes poco seguras. Tiene un diseño modular ya que toda la criptografía es manejada por la biblioteca SSL, finalmente OpenVPN brinda muchas opciones para controlar los parámetros de seguridad del túnel VPN y también ofrece opciones para proteger la seguridad del propio servidor. (VPNRanks, 2023)

Protocolo WireGuard

Se trata de un protocolo VPN innovador ya que ofrece una solución más segura, sencilla y rápida a sus usuarios con respecto a otros protocolos, debido a que aplica criptografía de última generación para ofrecer conexiones seguras en línea, es más rápido y fácil de configurar que OpenVPN y permite una excelente usabilidad y compatibilidad multiplataforma, aunque su interfaz es básica. (VPNRanks, 2023)

WireGuard es un protocolo de código abierto, se caracteriza por tener alto nivel de seguridad ya que elimina todo tipo de vulnerabilidad, usa técnicas de defensa profunda, está integrada en varios sistemas operativos como Linux, Mac, Windows y también iOS y Android. Consta de 4000 líneas de código, pero es fácil de auditar.

Red privada virtual en Linux

Una de las tecnologías útiles de mayor seguridad son las VPNs, ya que cifran las comunicaciones y permite trabajar de manera segura, para ello, se requiere un cliente instalado en el ordenador personal, un servidor instalado y configurado para que brinde acceso a la red local a través de la red pública.

Como menciona, Castro (2021) en su tesis existen tres tipos diferentes de seguridad informática la primera es la seguridad de hardware la cual se encarga de los dispositivos físicos (equipos de cómputo, firewall, servidores proxy entre otros). La segunda es la seguridad en la red la cual se encarga de la accesibilidad a través del internet y todo lo que transmite es decir documentos, imágenes, datos y entre otros). Finalmente se encuentra la tercera que es la seguridad de software que es la cargada y necesaria para proporcionar integridad y autenticación del software para que esté a su disposición entre ellos las aplicaciones, sistemas operativos y el kernel.

En base al análisis de las tecnologías para una conexión segura se ha optado por usar OpenVPN, por ser de código abierto, cuenta con los protocolos seguros lo que garantizan la confidencialidad, integridad, autenticidad y permite crear túneles de comunicación cifrada por medio de protocolos SSL basados en una serie de algoritmos encriptados.

CAPÍTULO II. DISEÑO METODOLÓGICO

2.1. Caracterización de la Institución

La Cooperativa de Ahorro y Crédito Semilla del Progreso ubicado en la provincia del Loja cantón Saraguro forma parte de las entidades financieras reguladas por la Superintendencia de Economía Popular y Solidaria, fundada en el año 2007, cuenta con 7 agencias ubicadas en las provincias, Loja y Zamora Chinchipe. Actualmente tiene dificultad de acceso de enlaces de datos debido a la zona geográfica en la que se encuentra, además de no garantizar la óptima seguridad en la comunicación.

La COAC Semilla del Progreso cuanta con 28 usuarios activos en su Core-financiero distribuidos en 7 agencias como se lo muestra en la Tabla 2.

Tabla 2: Distribución de los usuarios

AGENCIAS	Número de Personas
Matriz	17
Yacuambi	2
Guayzimi	2
Zamora	2
Yanztzaza	2
Loja	2
Manu	1
TOTAL	28

Fuente: Elaboración propia.

El proyecto se plantea en base a dos agencias de la cuales el proveedor no brinda las seguridades necesarias, por ende, se han catalogado a una de las agencias como generadora de archivos spam lo cual preocupa que sea blanco de algunas amenazas en tema de seguridad de la información. Además de sufrir constantes caídas del enlace.

Las agencias son Guayzimi y Yacuambi que son dos agencias separadas geográficamente en donde existe un único proveedor, siendo única empresa que brinda servicio de internet corporativo a estos sectores.

Misión

La Cooperativa de Ahorro y Crédito “Semilla del Progreso” es una entidad que promueve el desarrollo económico y social de sus socios, apoyando los emprendimientos productivos que generan ingresos para beneficio de los socios y sus familias, en el marco de la interculturalidad.

Visión

La Cooperativa de Ahorro y Crédito “Semilla del Progreso” será una entidad líder en la oferta de productos y servicios financieros de calidad en su área de influencia; caracterizada por su confiabilidad, solidaridad y competitividad; sostenible y sustentable, que satisface las necesidades de sus socios y sociedad en general.

2.2. Metodología de Investigación

La metodología de investigación es una forma estructurada del proceso de investigación que permite la obtención de información suficiente y necesaria con el fin de dar solución a un problema, es decir, el método es la manera muy organizada y estructurada del trabajo de investigación, o son los procesos que permiten obtener información de manera organizada de los aspectos importantes para ser analizados, revisados y finalmente, procesados a deducir.
A medida que avanza en la búsqueda de información se mejora la visión y surgen nueva formas y recursos más relevantes respecto al tema, lo que permite delimitas

los hallazgos permitiendo así encontrar información fundamental para complementar la investigación (Gómez, Navas, Mayor, & Buitrago, 2014)

Investigación Bibliográfica

En el proceso de investigación bibliográfica es muy importante nos permite dar relevancia al tema de investigación y asegurar su originalidad para ellos se contó con material informativo como libros, revistas de divulgación o de investigación científica, sitios web; información necesaria para iniciar el estudio, la investigación se basó en búsqueda de información bibliográfica en tesis similares, artículos científicos relacionados con la red privada virtual en repositorios como: Mendeley, Redalyc, IEEE Explore y diferentes fuertes.

Método Cualitativo

Según menciona Roberto Sampieri (1990) el método sirve como un guía por áreas o temas significativos de investigación. Sin embargo, en lugar de que la claridad sobre las preguntas de investigación e hipótesis preceda a la recolección y el análisis de los datos (como en la mayoría de los estudios cuantitativos), los estudios cualitativos pueden desarrollar preguntas e hipótesis antes, durante o después de la recolección y el análisis de los datos. Con frecuencia, estas actividades sirven para descubrir cuáles son las preguntas de investigación más importantes y después, para perfeccionarlas y responderlas.

Es decir, este método permite llevar de manera centralizada el trabajo de investigación y también es útil para llevar de forma organizada los puntos importantes en la investigación para ser analizados y revisados, es fundamental ya que ayuda a la comprensión de la realidad de la institución desde distintas perspectivas.

Ayuda en el análisis de los resultados obtenidos de la situación actual que han permitido fundamentar la problemática, de esta manera planificar la investigación bibliográfica y las metodologías de desarrollo.

Método Inductivo

Esta metodología ha permitido generar conocimiento esencial de forma racional acoplados a la realidad de la institución, ha permito organizar la situación actual y de esta manera organizar por etapas la metodología de desarrollo. Definiendo así el punto de partida y la solución concreta que conlleva a tener resultados óptimos en la mitigación de riesgos.

Instrumentos de investigación

Entrevista

Es una técnica utilizada frecuentemente como un medio para obtener información por lo que muchas personas prefieren hablar y no escribir. En este proceso existen las interacciones entre el entrevistador y el entrevistado donde se puede apreciar la sinceridad en las respuestas y aclarar muchas dudas.

La entrevista que se realizó a los jefes de las agencias, gerencia, y al personal relacionados con la tecnología de información y comunicación. Se optó por utilizar esta herramienta para la obtención de datos. Ya que de esta manera se obtiene respuestas claras, concretas, aclaraciones ante las dudas y dar la explicación correcta a las preguntas las cuales fueron planteadas en la entrevista, Anexo 1. Modelo de entrevista realizada que se muestran en la sección última.

Población y muestra

Se llama población al conjunto de individuos, objeto o personas que tienen características en común y son objeto de estudio para la investigación, para este estudio se llama muestra al número total de empleados de la entidad financiera siendo un total de 28 personas hasta fecha de investigación, de los cuales se toma 9 personas. En la tabla 3 se encuentra una descripción de manera general a las personas entrevistadas para obtener datos para el estudio.

Tabla 3: Muestra para el estudio del caso

Agencia	Cargo	Número de Personas
Agencia Loja	Jefe de Agencia	1
Agencia Zamora	Jefe de Agencia	1
Agencia Yantzaza	Jefe de Agencia	1
Agencia Guayzimi	Jefe de Agencia	1
Agencia Yacuambi	Jefe de Agencia	1
Agencia Manu	Jefe de Agencia	1
Área de TIC	Asistente de TIC	1
Agencia Matriz	Gerencia General	1
TOTAL		**9**

Fuente Elaboración de propia

2.3. Metodología de Desarrollo

Para desarrollar un proyecto es necesario tener un enfoque claro de secuencias sistemáticas y definir una metodología de desarrollo, que influye directamente en este proceso de construcción y se procede a elaborar a partir de un marco definido por uno o varios ciclos de vida o como un conjunto de pasos y procedimientos que se deben seguir para el desarrollo.

Magerit responde a lo que se denomina Proceso de Gestión de los Riesgos, es decir, implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los organismos del gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información. Esta metodología es importante porque el crecimiento de la tecnología dentro de las organizaciones se está dando de manera exponencial, por lo tanto, es necesario minimizar los riesgos asociados al uso de los sistemas garantizando la autenticidad, confidencialidad,

integridad, disponibilidad y trazabilidad, con la finalidad de generar confianza en los clientes tanto internos como externos de la organización. (Tejena Macías, 2018)

Por ello, Magerit tiene como fin hacer conciencia sobre la existencia de riesgos y la necesidad de gestionarlos, por otro lado, ofrece un método sistemático haciendo uso de tecnologías de información y comunicación, de esta manera planificar el tratamiento y poder controlar el riesgo y estar preparado para una posible auditoria o evaluación para la certificación según corresponda.

El objetivo es proteger la información que se transmite dentro de la entidad financiera teniendo en cuenta las dimensiones de seguridad.

Disponibilidad: La disponibilidad de todos los servicios existentes es fundamental dentro de la cooperativa y deber ser usado de manera correcta la carencia de la disponibilidad que supone una interrupción del servicio y reduce la productividad de la entidad.

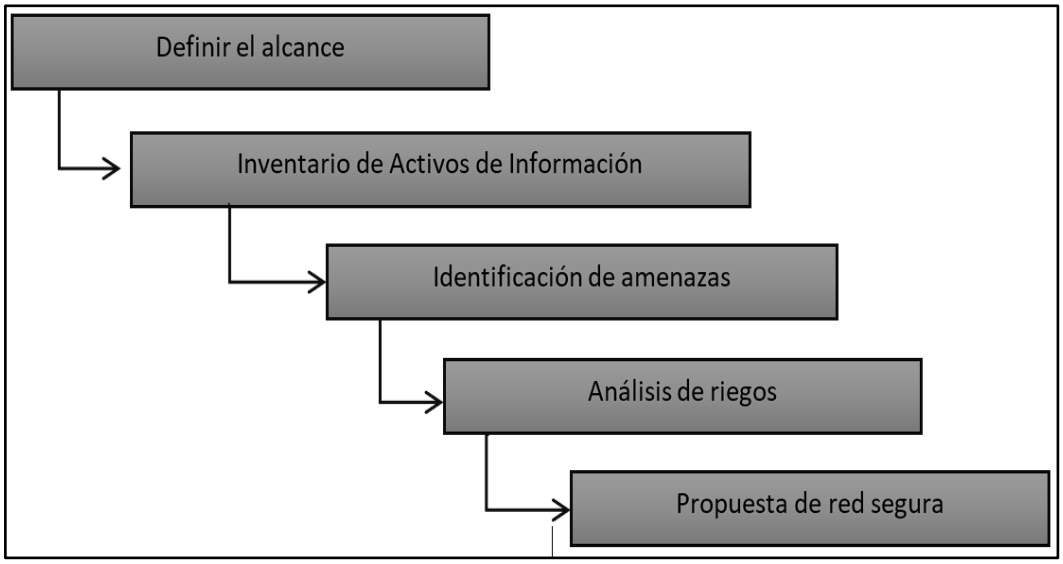
Integridad: la información producida dentro de la COAC puede aparecer manipulada, corrupta o incompleta. La integridad afecta directamente al correcto desempeño de las funciones de una entidad.

Confidencialidad: De acuerdo con el tipo de información que se maneja en la COAC se deber compartir información solamente entre las personas autorizadas. Contra la confidencialidad o secreto pueden darse fugas y filtraciones de información, así como accesos no autorizados.

Autenticidad: La propiedad o característica consistente en una entidad es quien garantiza la fuente de la que procesan los datos. Generar la información y estar monitoreando los sucesos para evitar la manipulación del origen o del contenido de los datos.

Trazabilidad: La trazabilidad es esencial para analizar los incidentes, perseguir a los atacantes y aprender de la experiencia. La trazabilidad se materializa en la integridad de los registros de actividad. Magerit maneja un esquema sencillo de todas sus etapas como se muestra a continuación en la figura 8.

Figura 8. Etapas de la metodología Magerit



Fuente: Elaboración propia

ETAPA 1. Definir el alcance

En esta primera etapa consiste en dar una explicación fundamentada de las razones delimitadas, es decir, definir los trabajos realizados para completar satisfactoriamente, lo que incluye y lo que no incluye en el proyecto.

La COAC Semilla del Progreso cuenta en la actualidad con 7 agencias distribuidos en puntos estratégico de las provincias de Loja y Zamora Chinchipe por el área geográfica las conexiones en dos agencias, se interconectan con el servicio a través de un proveedor que no presta las condiciones de seguridad, por ende, se requiere optar por un enlace a través de una VPN, para proteger la comunicación de las agencias. Para ello se pretende instalar en una versión libre de Linux en un equipo en donde se harán las configuraciones necesarias, y poder salir con los enlaces a diferentes agencias, para luego probar el nivel de seguridad, haciendo uso de los recursos existentes y aprovechando al máximo su infraestructura.

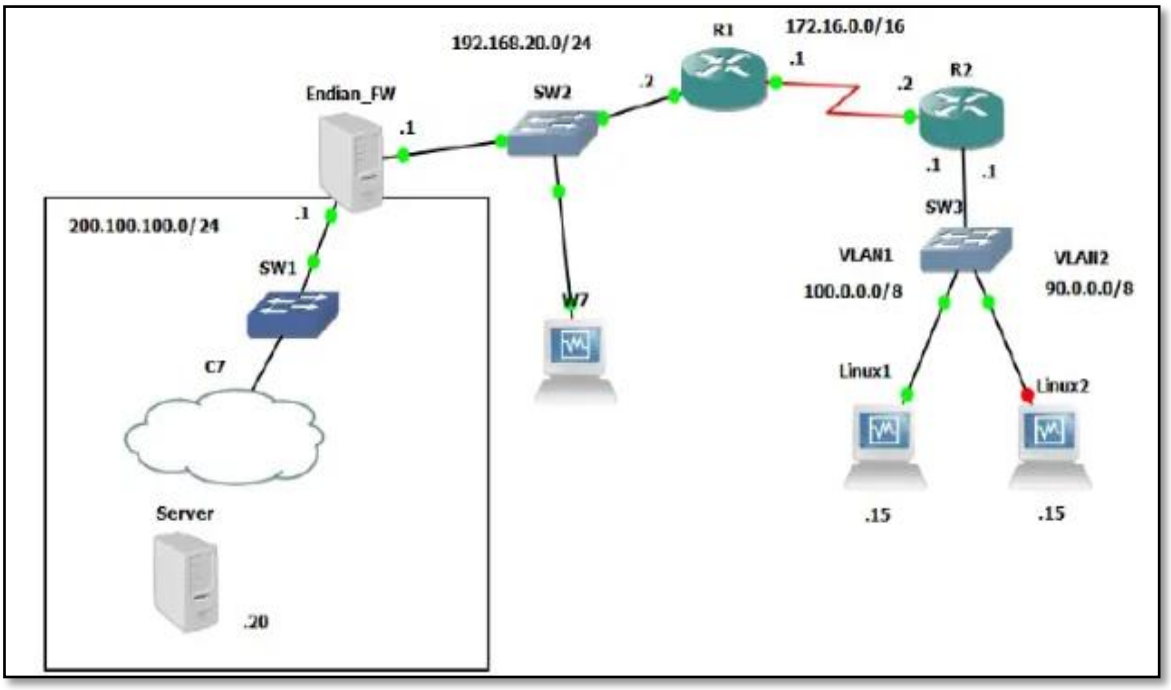
ETAPA 2. Inventario de Activos de Información

Como parte del inventario aquí se describe la parte fundamental que son los equipos y software que permiten la interacción entre el usuario y el equipo, el cual está definido de acuerdo con su nivel jerárquico y de las funciones asignadas a cada uno de los empleados. Para ellos se define como Nivel 1 Altos Directivos Nivel 2. Administrativos. Nivel 3 Operativos.

Dentro del software que tiene cada uno de los equipos, como base está el Sistema Operativo Windows 7, Windows 10, CentOS 7, CentOS 6 y Windows Server 2012, adicionalmente cuenta con el paquete de office 2013, adicionalmente todos los equipos tienen Windows defender que es propio del sistema operativo. Durante el último semestre del año 2021 la entidad de control que regulan a las cooperativas emitió un comunicado de contar son servidores en la nube, por ende, la cooperativa por cuestiones de inversión está migrando partes de la infraestructura física a la nube y hasta el momento cuenta con dos servidores que están de prueba como de detalla en la tabla 4.

Como parte del inventario de activos de información en lo que respecta al hardware de la cooperativa, está la infraestructura tecnológica para entender mejor como está diseñada la red y por cuestión de seguridad no se muestra a detalle todo el esquema sino parte de la red como se indica en la figura 9.

Figura 9: Diseño de la red empresarial.



Fuente: Elaboración propia

Dentro de los dispositivos del personal que realiza las actividades propias de la cooperativa, se encuentran equipos con diferentes sistemas operativos la mayoría de ellos pertenecen al fabricante, gran parte de los usuarios utilizan el sistema operativo Windows, en sus diferentes versiones, antiguas y actuales como se detalla a continuación en la tabla 4.

Tabla 4: Inventario de equipos dentro de Cooperativa

CANT.	DETALLE DEL EQUIPO	Infraestructura	SISTEMAS OPERATIVOS
28	CPU DELL Optiplex 3000 Sistema Operativo x64, 2.5 Ghz, con 8 Gb de RAM y 250GB SD.	Física	Windows 10
2	CPU Clon Sistema Operativo x64, 2.5 GHz, con 16 de Gb de RAM y 250GB SD.	Física	CentOS 6
1	CPU Clon Sistema Operativo x64, 2.5 GHz, con 16 de Gb de RAM y 250GB SD.	Física	Elastik
1	Servidor hp Proliant DL300 Gen9|	Física	Windows server 2012
1	Servidor hp Proliant DL300 Gen10	Física	Windows server 2012
1	Servidor de Web con 2 de RAM 250 de almacenamiento	Nube	Alma Linux
1	Servidor de Base de Datos con 8 de RAM 250 de almacenamiento	Nube	Alma Linux

Fuente: Elaboración propia

Activos de Información

Para que los funcionarios de la cooperativa puedan realizar su trabajo con normalidad y puedan acceder a todos los servicios dentro de cada area o en cada una de las agencia se tiene incorporado un acceso directo al sistema financiero, el mismo que se encuentra en uno de los servidores de la matriz, adicionalmente se tiene acceso al servidor de archivos y acceso al chat interno por medio de Spark, y otras herramientas que son de servicio web y en la tabla 5 se listan los servicios con los que cuentan los equipos distribuidos por oficinas.

Tabla 5: Listado de activos de información.

Herramientas	Módulo de Sistema Financiero	Herramientas adicionales	Número de Usuarios
Core Financiero	Contabilidad	Accesos a los servicios del Banco Central del Ecuador. Acceso al SRI	2
	Activos fijos		1
	Inversiones	Acceso a las cuentas de bancos de la cooperativa Acceso al servicio de UAFE	7
	Créditos	Acceso a consultas en el buro	8
	Control Interno		1
	Talento Humando	Ministerio de relaciones laborales.	1
	Secretaria General		1
	Cobranzas		1
	Cumplimiento	UAFE SEPS	1
	Cajas		8
	Sistemas		2

Fuente: Elaboración propia

Como parte de los activos de información se detalla a continuación en la tabla 6 los proveedores de los servicios de internet y enlace a los puntos en cada una de las agencias que tiene la entidad financiera.

Tabla 6: ISP para la cooperativa

PROVEEDOR	AGENCIAS
TELCONET	Matriz
TELCONET	Manu
TELCONET	Loja
TELCONET	Zamora
CNT	Guayzimi
TELCONET	Yantzaza
CNT	Yacuambi

Fuente: Elaboración propia

ETAPA 3. Identificación de amenazas

Según menciona Tejena Macías (2018) en su artículo las amenazas pueden ser internas como externas que ocasionan robo de identidad o información, bases de datos, información sensible de clientes, pérdida de credibilidad y daños financieros que pueden afectar la sostenibilidad de la entidad.

Se llama amenaza a la posibilidad de que ocurra un evento o acción que produzca daño material o inmaterial a sobre los elementos de un sistema informático.

En la institución financiera el factor más importante que debe ser protegido es la información, por lo cual, desde el punto de vista de la investigación la capa de red del modelo OSI es quien define la ruta por donde se transmite la información y es aquí donde se identifican las amenazas. La cooperativa de ahorro y crédito cuenta con dos agencias que reciben el servicio a través de un proveedor no seguro.

Una vez realizada la investigación a través del método inductivo, tomados como muestra la agencia Guayzimi y Yacuambi han permitido generar resultados

después del análisis y se ha definido que los datos deben viajar de forma segura ya que mucha información es confidencial y se debe tener acceso solo a las personas autorizadas.

Desde la creación y funcionamiento de los sistemas informáticos en general se ha visto que requiere que los factores técnicos, de infraestructura, humanos y organización requieren implementar seguridades para la gestión de riesgos y dar continuidad al negocio.

En las organizaciones deben tener la metodología adecuada donde incluya las herramientas, procedimientos y software que permita definir el análisis adecuado de posibles riesgos dentro de cada organización.

A través de la siguiente tabla se identifican las probabilidades de amenazas encontradas luego del análisis de riesgos.

Tabla 7. Posibles amenazas

Nº	Descripción
1	Accesos no autorizados
2	Riesgo reputación
3	Alteración de las autenticaciones
4	Manipulación de la información
5	Cambio de legitimidad de información
6	Interrupción en el servicio de base de datos
7	Interrupción en las comunicaciones
8	Denegación de accesos a recursos
9	Violación a la confidencialidad, integridad y disponibilidad
10	Secuestro de secciones

Fuente: Elaboración propia

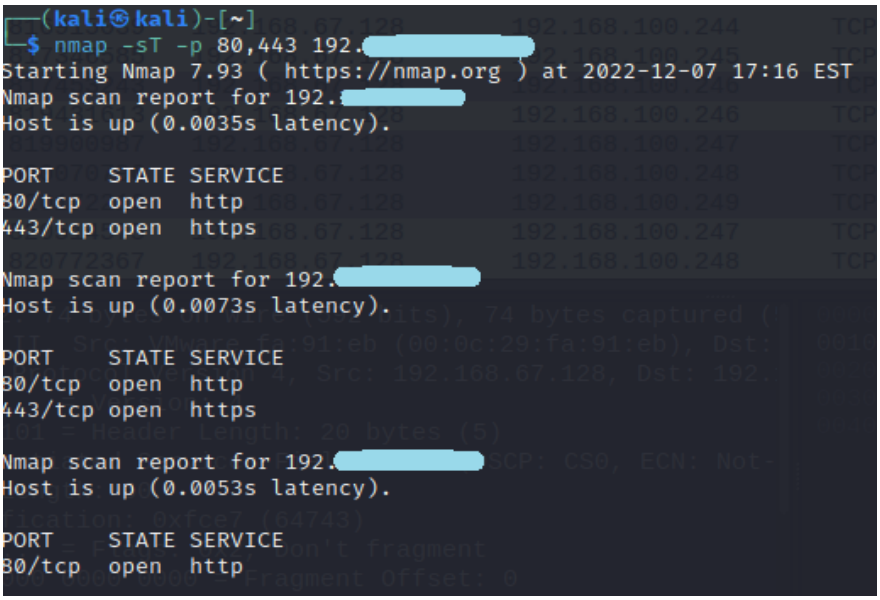
La infraestructura tecnológica cuenta con las seguridades necesarias, mientras que la infraestructura en la nube por ser implementado durante este año no tiene aún la seguridad en cuanto al tráfico que viaja por la red. Cabe recalcar que en esta infraestructura existen dos servidores de pruebas que muy pronto entrarán en producción. Una de las amenazas existentes es que al no contar con una red privada virtual al consultar la dirección IP pública se observan varios detalles de la red, lo cual pone en riesgo la comunicación, en la figura 10 se observan los datos encontrados.

Figura 10: Prueba de consulta de dirección IP

Fuente: Elaboración propia

En la figura 11, se observa la amenaza que existe a nivel de los puertos abiertos que necesitan ser analizados de acuerdo a la utilidad y al servicio.

Figura 11: Escaneo de puertos usando NMAP



Fuente: Elaboración propia

Así como también se muestra en la figura 12, si se escanea uno de los hosts debe tener mayor seguridad ya que en ella reposa toda la informa relevante y se observa que existen muchos puertos abiertos y por seguridad deben ser cerrados o que no sean visibles para todos. De esta manera se aprecia que no existe una comunicación segura. Aunque también existen hosts seguros con puertos bloqueados o que no se puede visualizar como se muestra en la figura 12.

Figura 12: Escaneo de un host determinado

Fuente: Elaboración propia

ETAPA 4. Análisis de riegos

Existe un esquema lógico a seguir para implementar políticas de seguridad de los sistemas de información, en las cuáles se debe hacer un inventario y valoración de los activos de información, posteriormente identificar y valorar las amenazas tomando en cuenta las medias de seguridad existente, para luego definir los objetivos de la seguridad de la información, conjuntamente determinar un sistema de medición de riesgo e impacto y seleccionar las medias de protección.

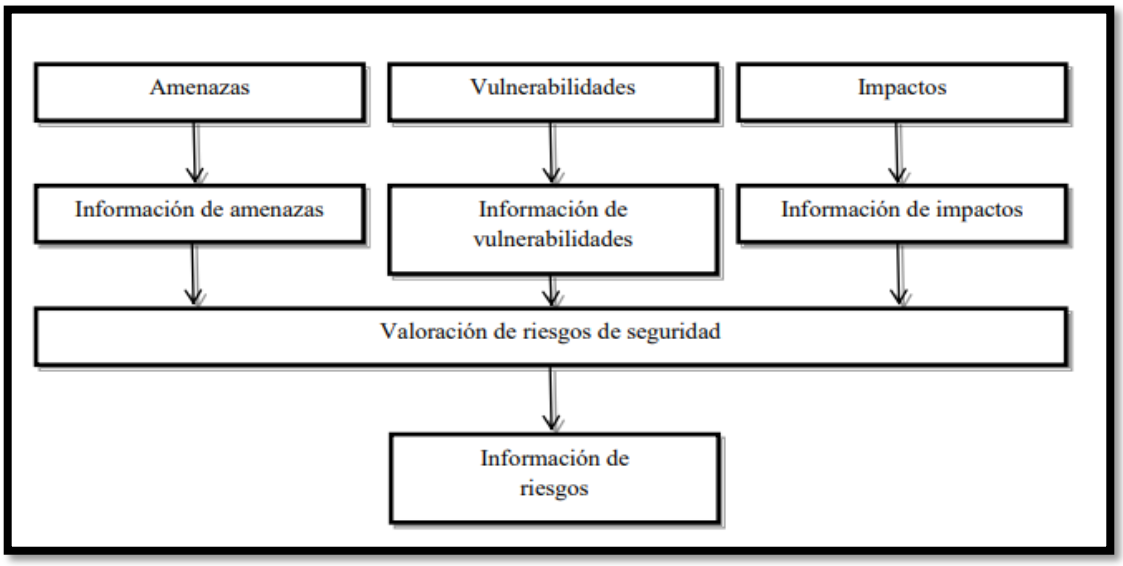
Tabla 8. Riegos

Numero	Riesgos
1	Información confidencial vulnerables
2	Espionaje de información confidencial
3	Conexión de Internet inestable
4	Rastreo por medio de anuncios de internet
4	Amenazas de actualizaciones diarias innecesarias.

Fuente: Elaboración propia

En la tabla 8 muestra los posibles riesgos a tener nuestra conexión expuesta, ya no existen políticas de seguridad que garantices que nuestra información esta protegida.

Figura 13: Componentes del proceso de Análisis de riesgo



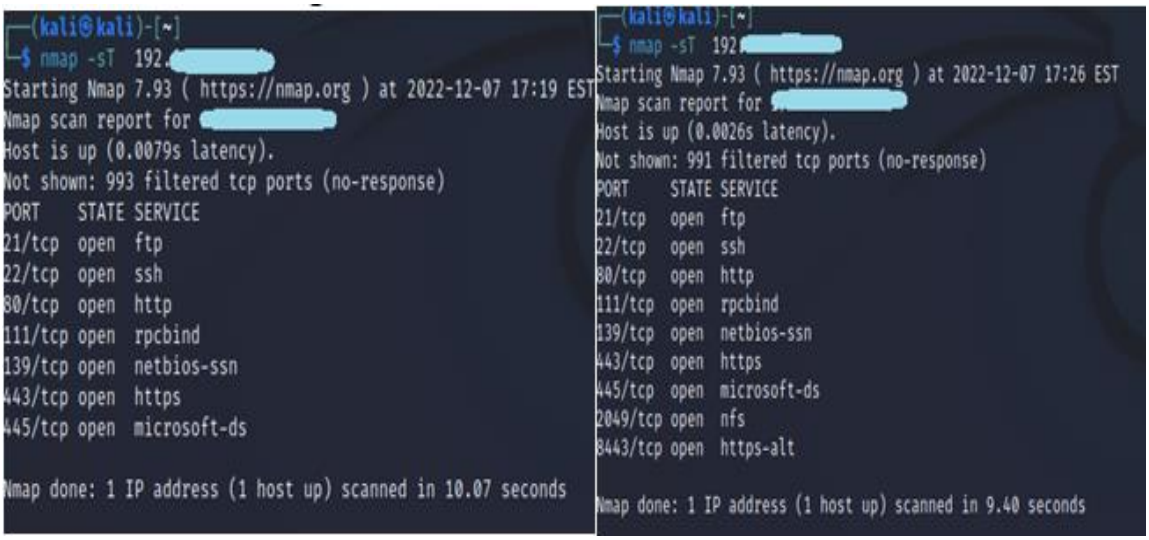
Fuente: Elaboración propia

Haciendo el uso de herramientas para el escaneo de vulnerabilidad se puede medir y valorar los controles de seguridad tanto internos como externos con el fin de obtener una visión amplia de las debilidades existentes e identificar las amenazas en la institución. Las diversas herramientas libres y de pago NMAP, NESSUS y WIRESHARK, permiten recolectar, identificar y analizar las vulnerabilidades.

NMAP

Esta herramienta es de código abierto permite escanear la red para conocer los puertos, detectar los sistemas operativos, tipo de Firewall, etc. Se aplican varios comandos de esta herramienta y como resultado se identifican vulnerabilidades presentes en la red y en los equipos, además, se analizan los puertos y se obtiene la cantidad de puertos y servicios. Así como también detalles como sistemas operativos, versiones, impresoras, computadoras y teléfonos IP que se encuentren en la red y en la figura 14 se muestra los datos recolectados.

Figura 14: Escaneo de un host

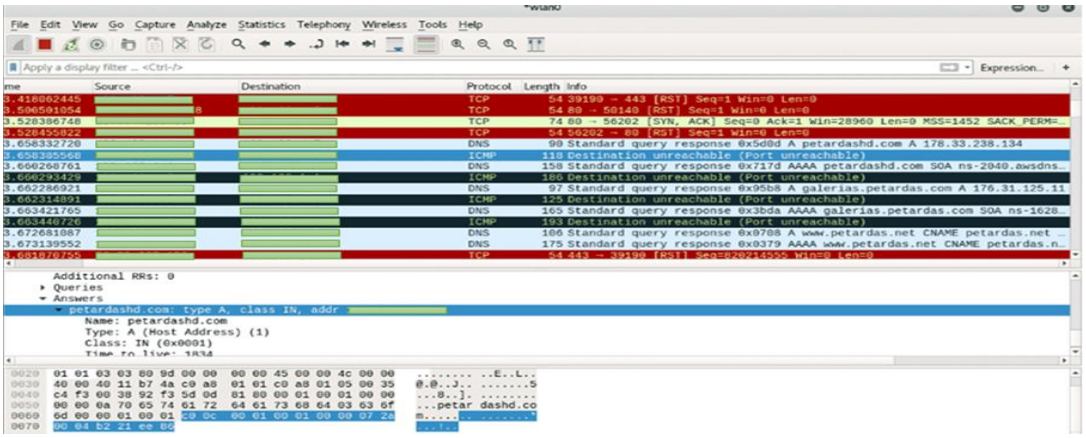


Fuente**:** Elaboración propia

WIRESHARK

Es un analizador de paquetes de red y se usa para capturar la información que pasa por la red, así como también para realizar análisis de la red de la institución y hacer la auditoria de seguridad. Para el análisis de la red es muy importante hacer uso de esta herramienta porque escanea toda la red o un determinado host, para nuestro caso se realizó el análisis de la red a nivel de los dispositivos que debería tener mayor nivel de seguridad con él que se obtuvo tráfico en tiempo real, información de paquetes enviados y utilización de protocolos durante las comunicaciones. Todos estos hallazgos se muestran en la figura 15.

Figura 15: Escaneo de la red usando Wireshark



Fuente**:** Elaboración propia

ETAPA 5. Propuesta de red segura

Descripción de la propuesta

Luego de realizar el análisis de la infraestructura de red, entre ellos, los servidores, los enlaces de las agencias hacia los servidores de prueba que se encuentran en la nube, se pudo constatar que la entidad financiera no cuenta con una infraestructura segura y las condiciones adecuadas en cuanto a seguridad física y lógica, las que por resolución solicita la Superintendencia de Economía Popular y Solidaria (SEPS).

Durante el segundo semestre del 2022 la entidad ha empezado a migrar parte de su infraestructura tecnológica a la nube y como la disposición tiene un plazo 36 meses para el cumplimiento se ha visto factible que el servidor VPN se instale en la infraestructura en la nube. De esta manera contribuir con el cumplimiento y brindar seguridad a la información a los servidores de pruebas.

Dentro de los protocolos existentes están WireGuard, que es un protocolo que aparece en el 2016, es sencillo de poco código y su seguridad es poco probada, usa algoritmos criptográficos CHaCHa20 para cifrado y Poly1035 para autenticación que es similar a AES-256.

OpenVPN usa encriptación AES y otros algoritmos como Blowfish, también soporta ChaCha20-Poly1305 debemos recalcar también que aquí se usa OpenSSL que permite seleccionar algoritmos de encriptación algo que no permite hacer en WireGuard.

El protocolo IPsec utiliza puertos WellKnown 500 y 4500 UDP, a veces existe incompatibilidad en este protocolo entre diferentes fabricantes, se usa más para conexiones LAN2LAN, mientras que para conexiones remotas el OpenVPN es mucho mejor porque es más segura, estable y compatible con todos los Sistemas Operativos.

En la implementación de la infraestructura VPN se usará el servidor con Alma Linux 8, en el cual se encuentra alojado el servicio de base de datos y un servicio web que son parte de infraestructura existente de la entidad. En la que se implementará de la seguridad de VPN y los clientes son los hosts de la cooperativa tanto de matriz como de las agencias. Se escoge como servidor OpenVPN por ser una herramienta de conectividad basada en software libre ya que ofrece conectividad segura mediante una infraestructura pública y compatibilidad con todos los Sistemas Operativos. Puesto que con esta tecnología se podrá llevar un control de conexiones realizadas mediante la creación de clientes en el servidor OpenVPN.

Planteamiento de la propuesta

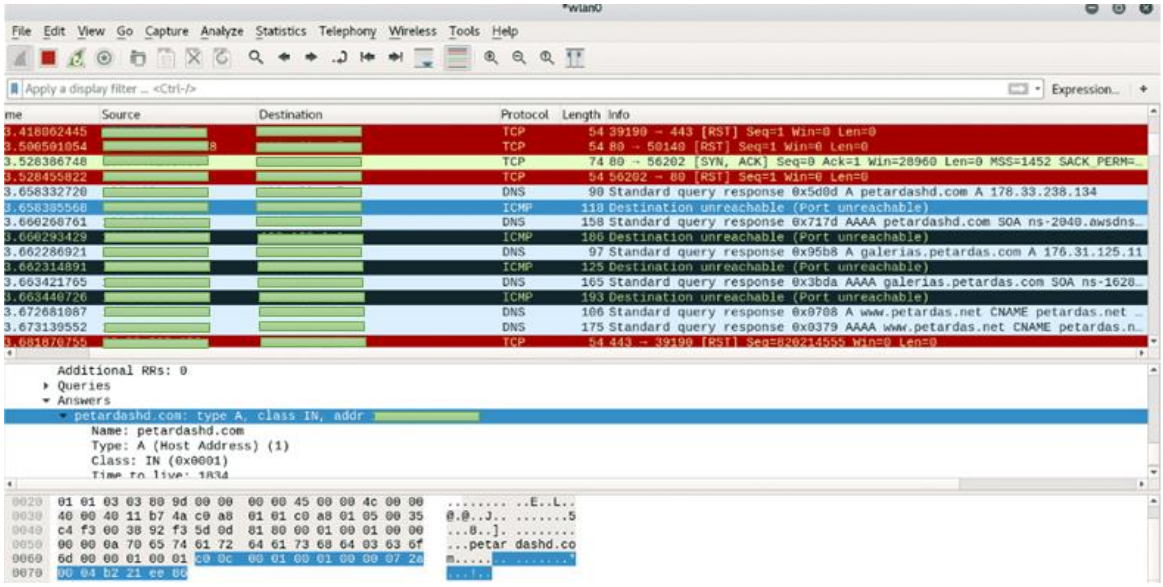
Objetivo del proyecto

Mejorar la seguridad en las comunicaciones a través de una red privada virtual de las agencias de la Cooperativa de Ahorro y “Crédito Semilla del Progreso”

Etapas de la propuesta

Etapa 1. Análisis de las seguridades durante la comunicación entre los hosts y los servidores de la nube donde se detectó que su información está expuesta ya que no existe ningún tipo de cifrado como se muestra en la figura 16.

Figura 16: Captura de tráfico sin seguridad

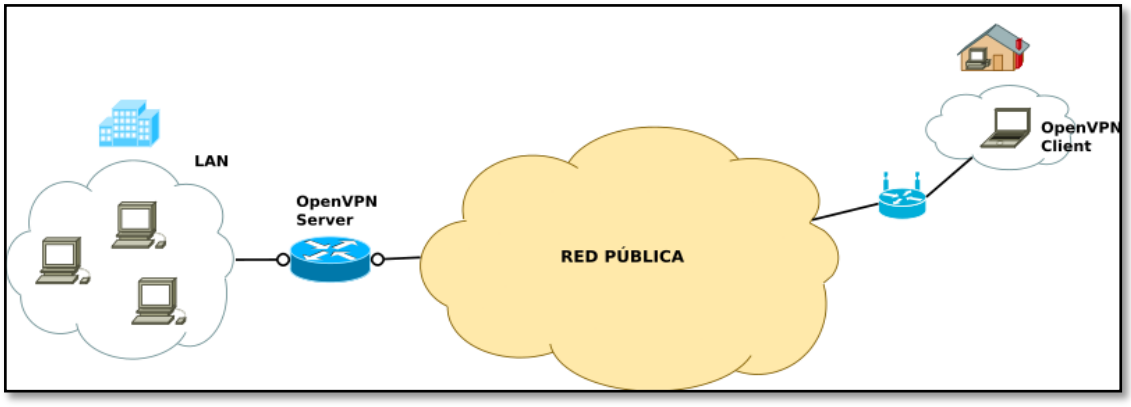


Fuente**:** Elaboración propia

Etapa 2. En esta parte se procede a elegir el tipo de VPN tomando en cuenta el nivel seguridad. Para ello, se eligió OpenVPN por ser de código abierto, multiplataforma, por su conectividad, brinda la posibilidad de seleccionar el protocolo de tunelización, utiliza puertos UDP o TCP haciendo una configuración flexible y tiene un cifrado de 256 bits.

En la figura 17, se muestra un esquema de cómo está constituido OpenVPN, y por otro lado los servidores que están en la nube, junto a ellos un servidor con OpenVPN, por la cual se pasa la comunicación por medio del internet, mientas que en otro extremo están los clientes distribuidos en diferentes puntos.

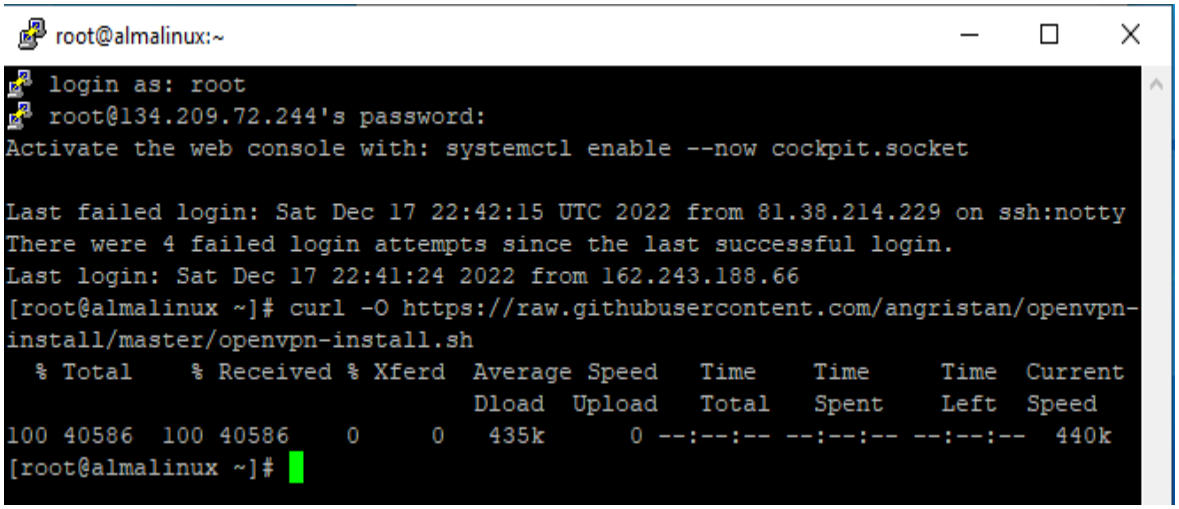
Figura 17: Esquema VPN con OpenVPN



Fuente**:** Elaboración propia

Etapa 3. En esta etapa se realiza la instalación de OpenVPN para ello se utilizó el script existente en GitHub como se muestra en el Anexo 2. Instalación el servidor OpenVPN en AlmaLinux 8 donde constan todos los pasos a seguir y también se muestra la configuración como en la figura 18.

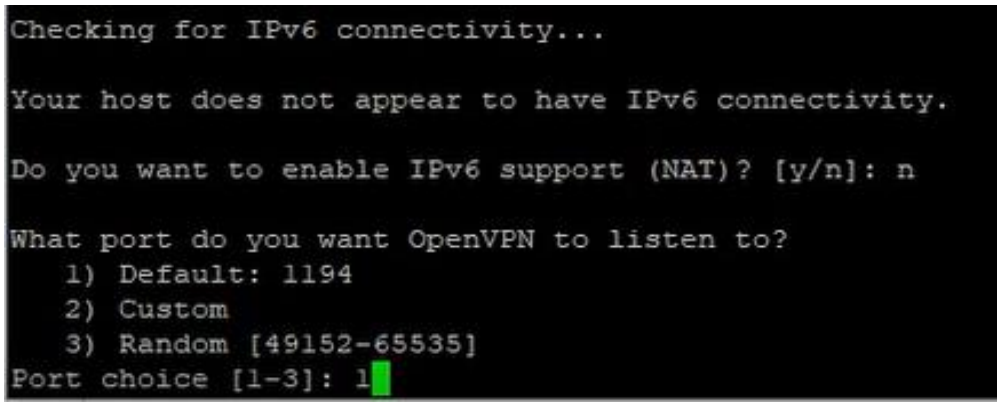
Figura 18: Descarga del repositorio



Fuente: Elaboración propia

En la figura 19, se observa la pregunta sobre si se requiere optar por el puerto de escucha que usa OpenVPN, en el cual, se debe escoger la que está por defecto.

Figura 19: Configuración del puerto



Fuente: Elaboración propia

En la figura 20, nos muestra que protocolo se va a usar, para ello puede ser TCP o UDP, para el presente caso se usó el protocolo UDP.

Figura 20: Configuración de protocolo

Fuente: Elaboración propia

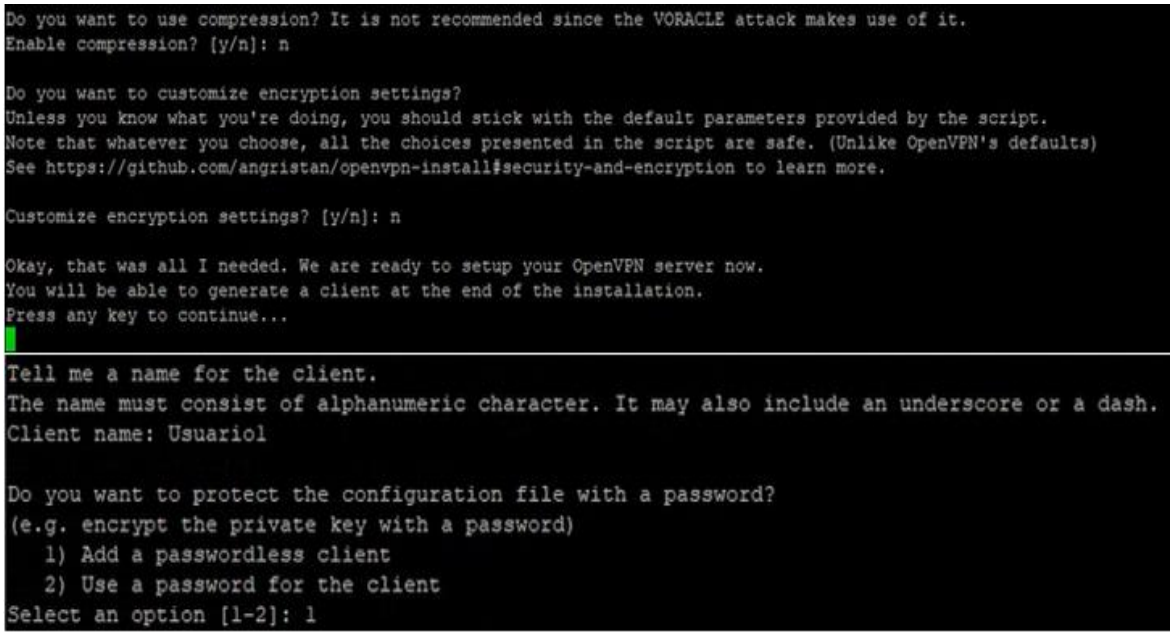
En la figura 21 se indica la selección para el DNS para la red de OpenVPN.

Figura 21: Configuración de DNS

Fuente: Elaboración propia

En la figura 22 se observa la seguridad para el cliente y lograr un acceso a la red VPN y así poder obtener la comunicación entre los diferentes servicios que están alojados en la nube.

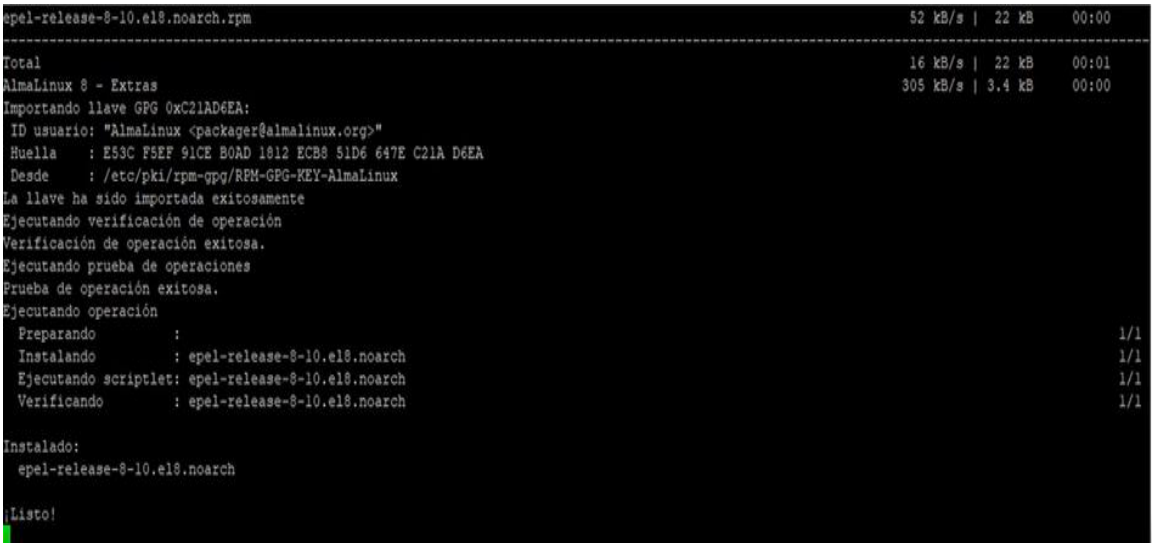
Figura 22: Encriptación de paquetes



Fuente**:** Elaboración propia

En la figura 23 nos indica que se ha instalado de manera correcta el servicio de OpenVPN y se encuentra listo para hacer uso esta tecnología.

Figura 23: Encriptación de paquetes

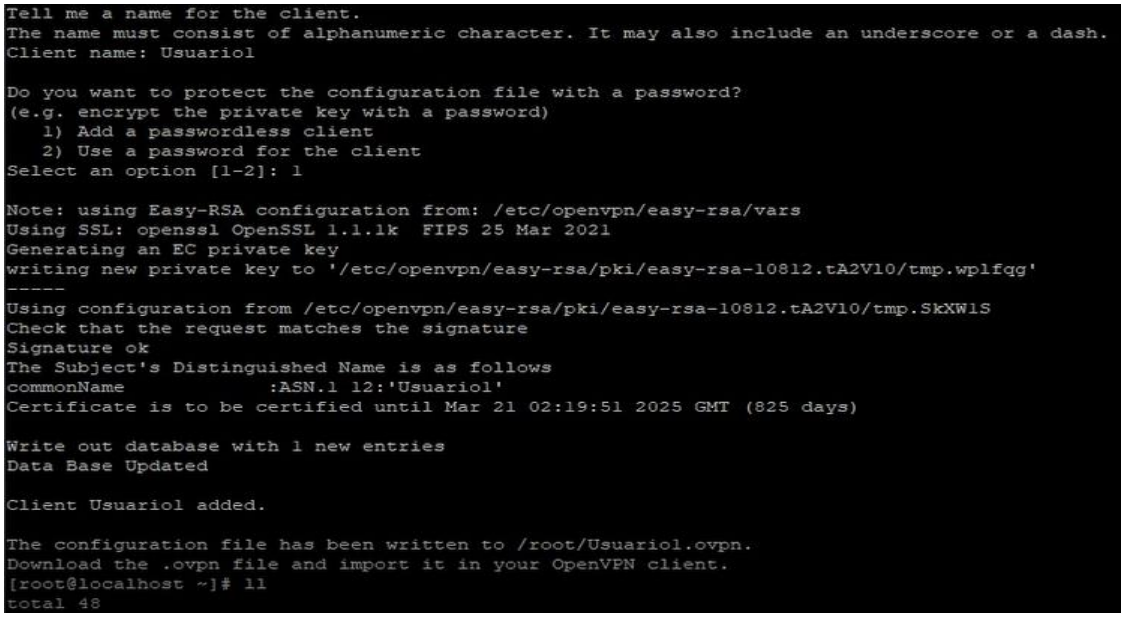


Fuente**:** Elaboración propia

Como siguiente paso se procede a crear usuarios para los host o clientes así lo muestra la figura 24 creaciones del usuario OpenVPN junto a la clave encriptada, hasta este punto se encuentra listo un cliente registrado en el servidor para

proceder a descargar el cliente OpenVPN y tener conexión desde el host hacia los servicios en la nube.

Figura 24: Creación de Cliente VPN



Fuente**:** Elaboración propia

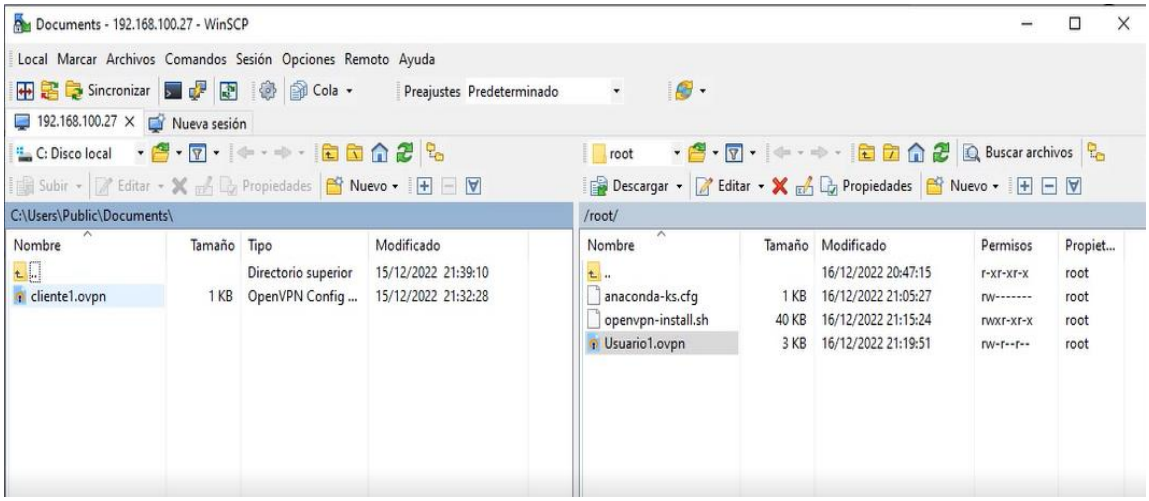
En la figura 25 se observa que se encuentra creado y configurado el archivo del usuario OpenVPN listo para probar la conexión.

Figura 25: Visualización de Cliente VPN

Fuente**:** Elaboración propia

En la siguiente figura 26 se muestra la copia del archivo creado, para este caso es Usuario1.ovpn, a continuación, se usa la herramienta WinSCP para poder copiar el archivo hacia el equipo del cliente.

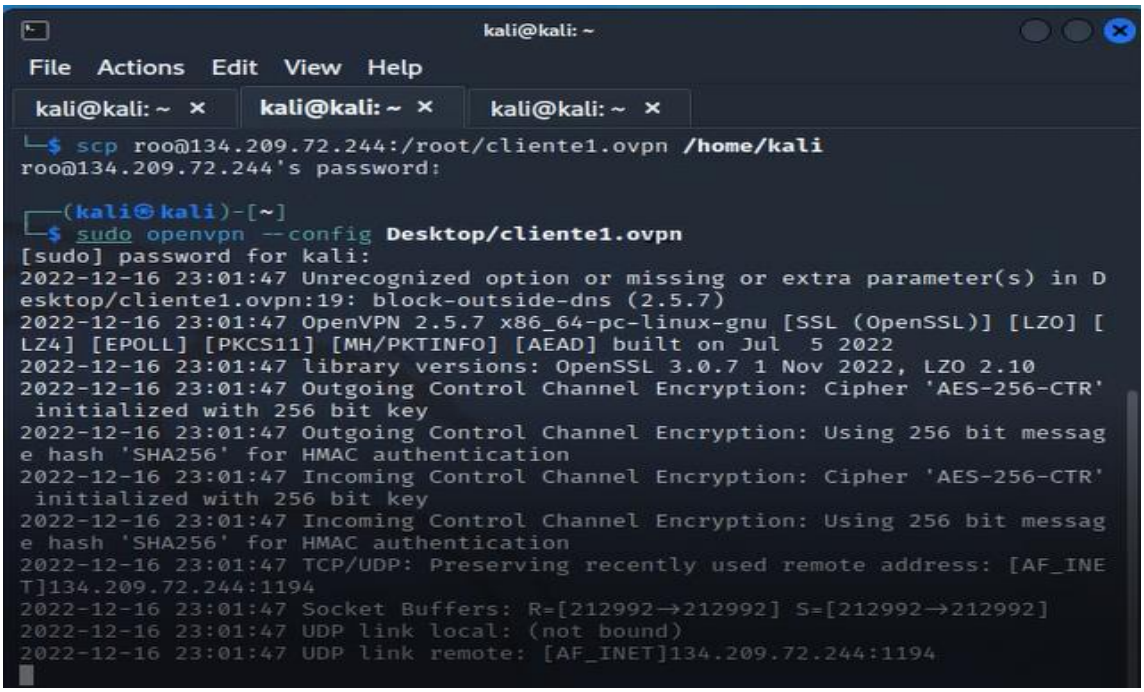
Figura 26: Envió de archivo Cliente VPN



Fuente**:** Elaboración propia

El archivo con extensión ovpn que se descargó se lo coloco en la máquina del cliente, con el que se procede a ejecutar como se muestra en la figura 27 y a través de la línea de comando del cliente se procede a ejecutar el archivo de esta manera poder navegar dentro de la VPN con total seguridad en las comunicaciones.

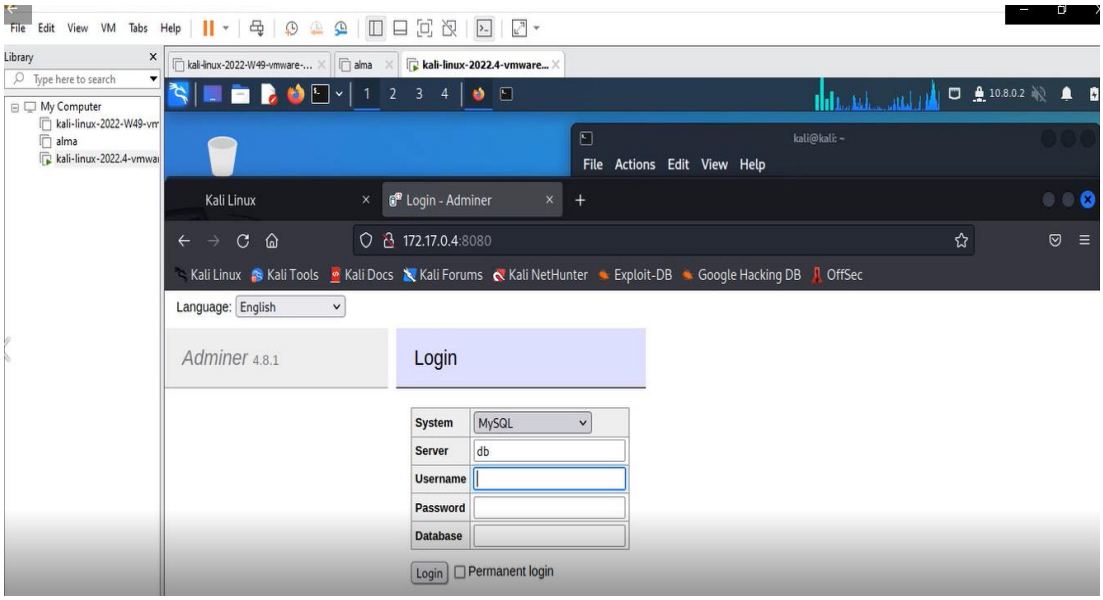
Figura 27: Instalación del archivo Cliente VPN



Fuente**:** Elaboración propia

En esta parte de la propuesta luego de crear el cliente VPN, las descargas y la ejecución en el cliente remoto, ya se tiene acceso a los servicios a través de la red privada virtual y en la figura 28 se observa que ya se logró acceder al servidor de base de datos que se encuentra en la Nube.

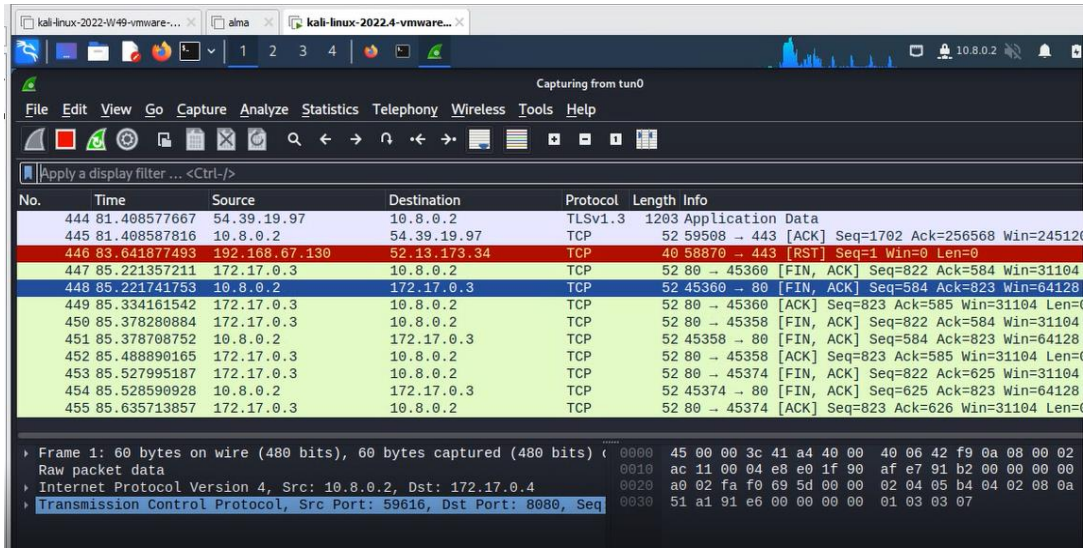
Figura 28: Acceso el servidor de BBDD



Fuente: Elaboración propia

Una vez que el cliente tiene acceso se ingresa nuevamente a la red para capturar el tráfico usando Wireshark y en la figura 29 se muestra diferentes datos como: host de destino, protocolos y también se aprecia que la información se transmite de manera segura; es decir existe un tráfico encriptado

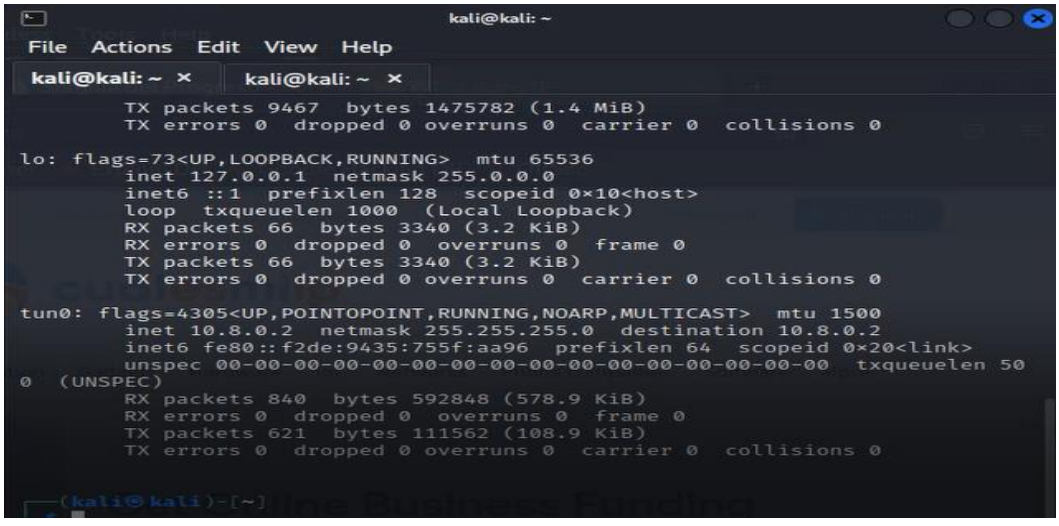
Figura 29: Captura de tráfico con VPN



Fuente: Elaboración propia

Para concluir y asegurarnos de que se está navegando por una red privada virtual se hace una consulta de la interfaz de red usada, en la figura 30 se aprecia que se ha creado un túnel de navegación.

Figura 30: Túnel de navegación



Fuente**:** Elaboración propia

De esta manera se ha implementado esta tecnología para acceder a los recursos por medio de un túnel e intercambiar información con conexiones remotas, además de canalizar todo el tráfico de forma segura al servidor OpenVPN por medio de túnel SSL y el servidor asigna a la interfaz una dirección IP de manera automática.

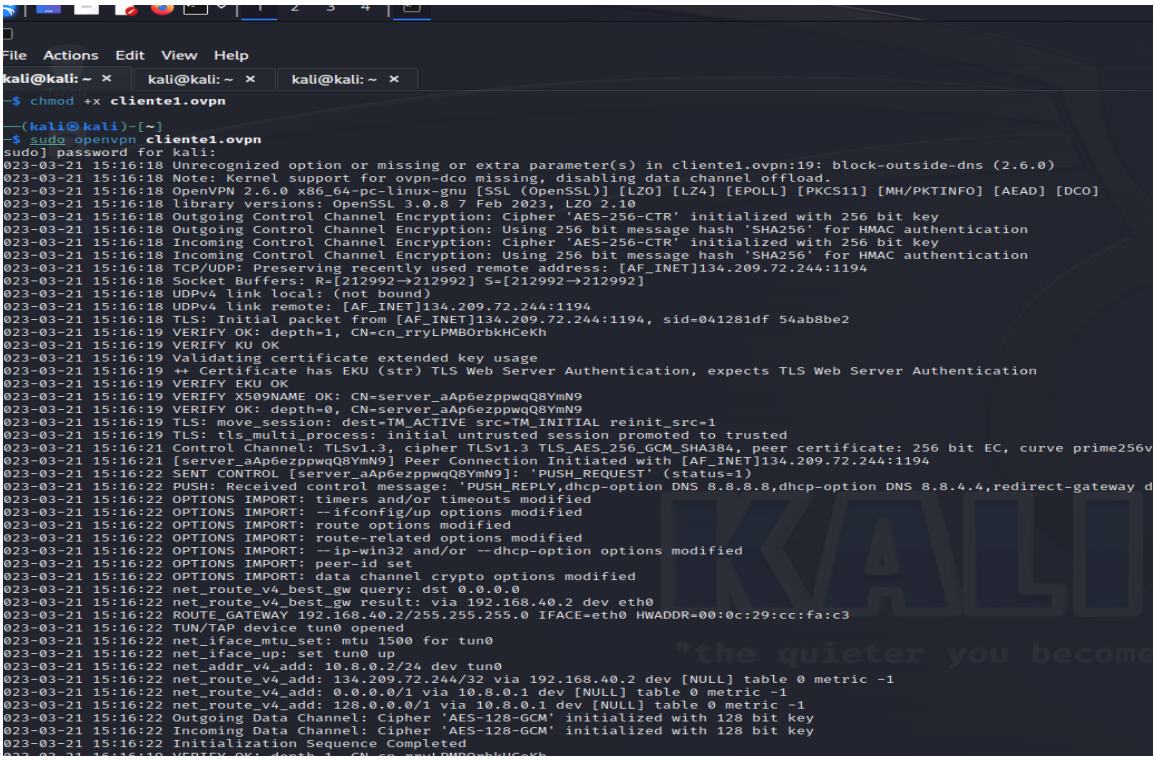
CAPÍTULO III. ANÁLISIS DE LOS RESULTADOS DE LA INVESTIGACIÓN

Luego de la configuración en el servidor OpenVPN donde se procedió a crear un usuario para cada uno de los hosts, se debe descargar el archivo del cliente VPN para luego ser instalado en terminales de todos los empleados de la entidad Financiera.

3.1. Validación de la propuesta

Al tener instalado el servidor VPN, sin tener conexión en ninguna terminal se puede evidenciar el estado del servidor antes del ingreso y no tener comunicación con los servicios alojados en la nube. Como se muestra en la siguiente figura.

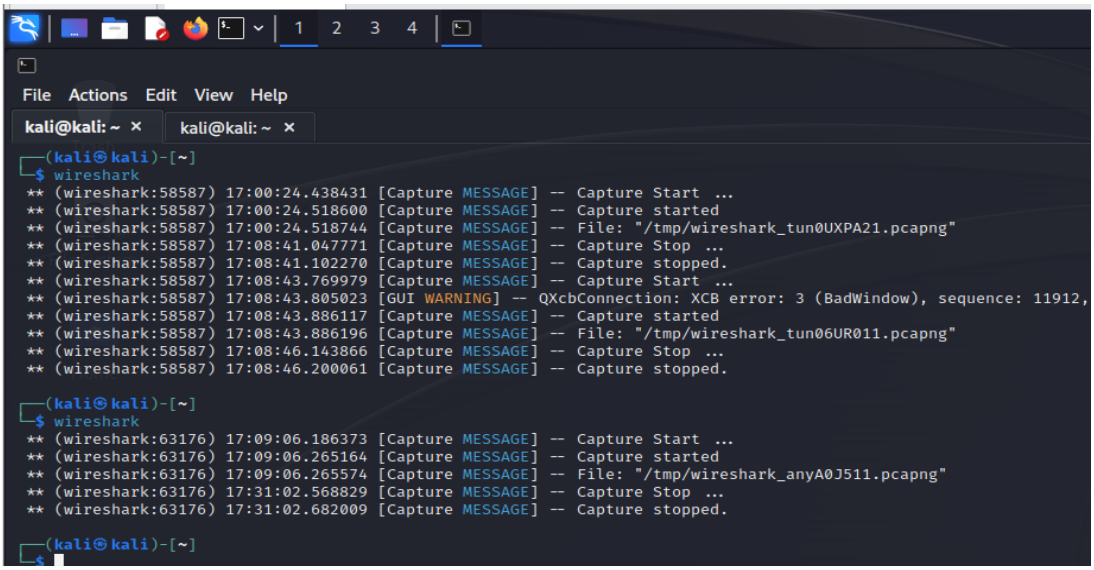
Figura 31: Estado del servidor sin conexiones



Fuente: Elaboración de propia

Luego de que existe comunicación en las terminales, se procede hacer una prueba de tráfico existente para ello se usa WireShark. Donde se muestra el tráfico con 5 terminales interconectados desde diferentes puntos que son las agencias de esta entidad financiera.

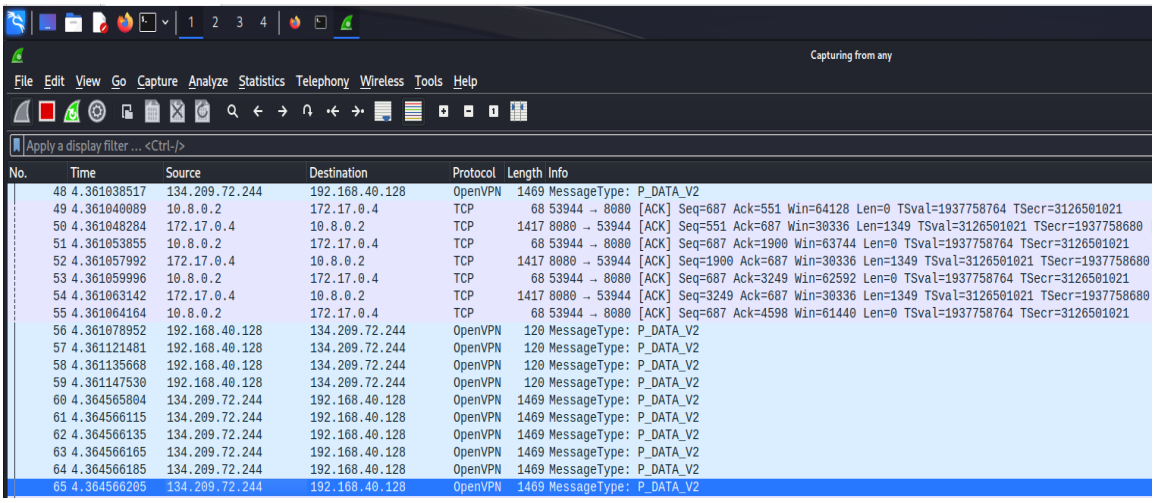
Figura 32: Estado del servidor con conexiones



Fuente: Elaboración propia

Viendo desde otra perspectiva, en esta ocasión también se captura el tráfico donde se muestra que está protegido por el protocolo OpenVPN, así lo muestra en esta figura.

Figura 33: Trafico protegido

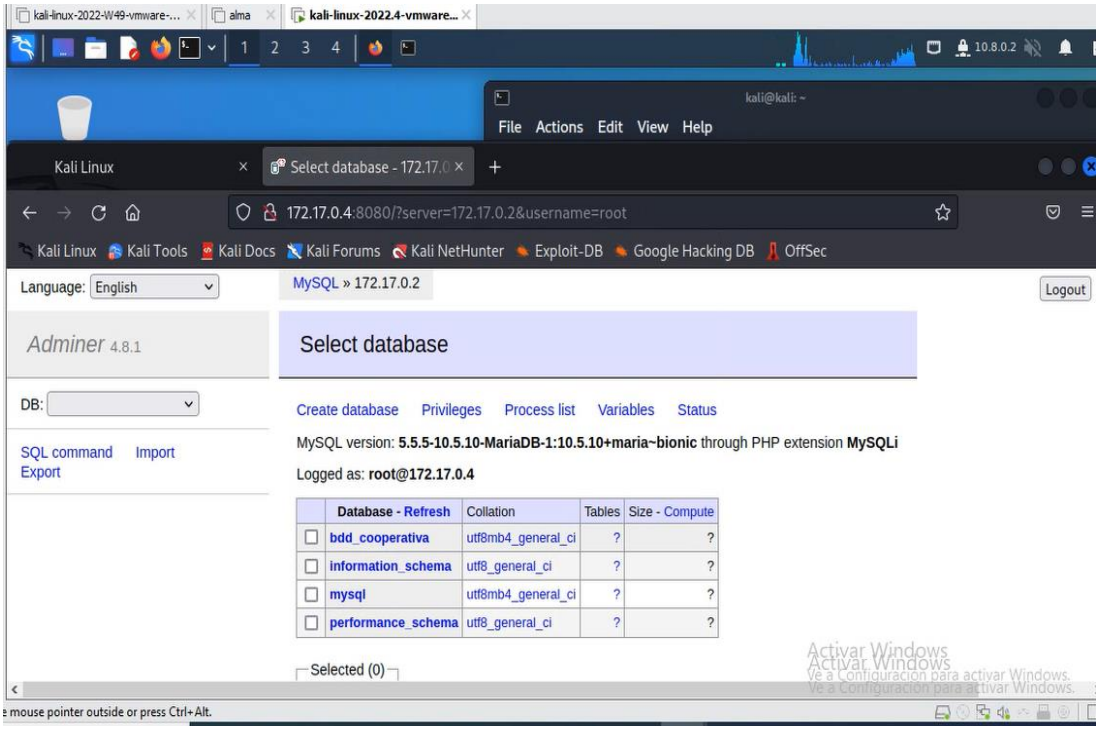


Fuente: Elaboración de propia

Además, se procede a validar que existe conexión desde el cliente VPN hasta el servidor y hacia los servicios que se encuentran en la nube y de esta manera asegurarse de tener una conexión cifrada y la comunicación es transmita de manera segura.

Como se muestra a continuación en la figura 34 y se ha ingresado con normalidad al servidor de base de datos que se encuentra en la infraestructura en la nube.

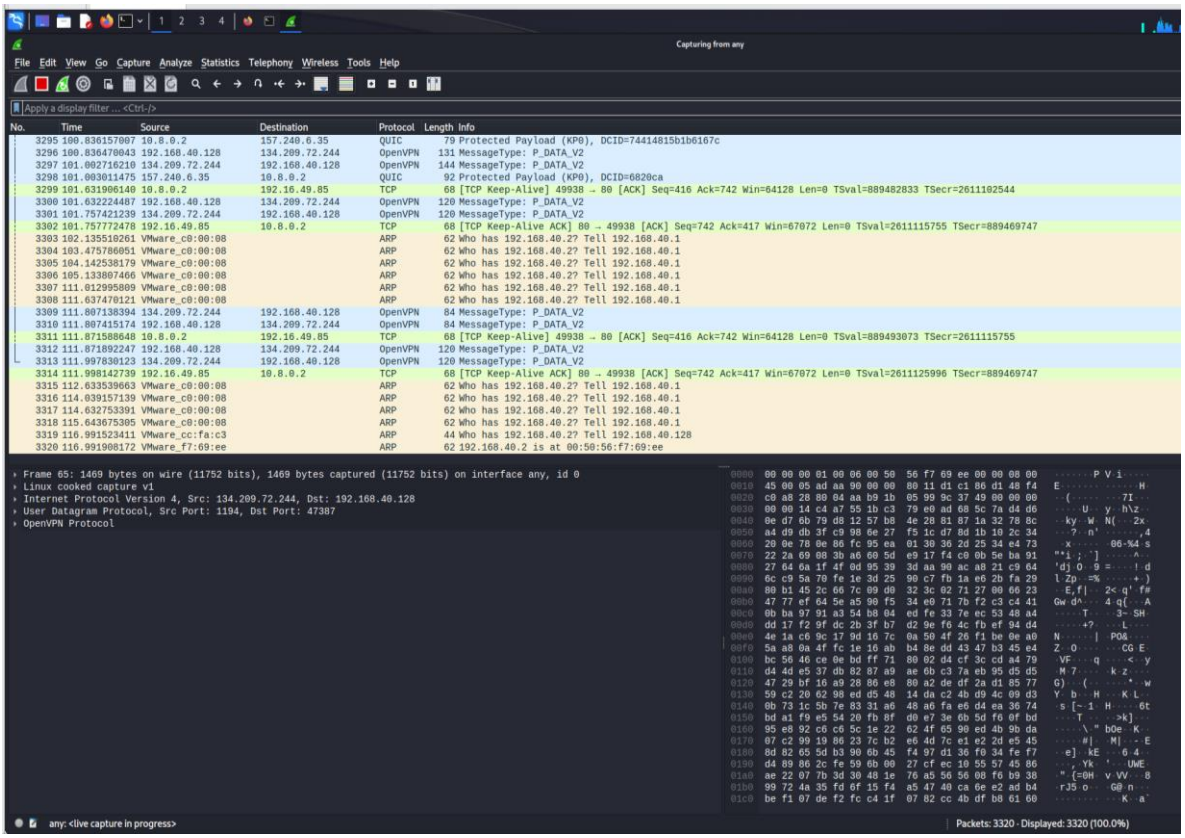
Figura 34: Acceso al servidor de base de datos



Fuente: Elaboración de propia

Otra forma de validar que existe la conexión segura es con la herramienta Wireshark donde muestra que existe conexión por una red muy diferente a la red local y así se asegura que la información de los paquetes es cifrada y también la comunicación viaja de manera confiable y en la figura 35 se muestra el tráfico de la red.

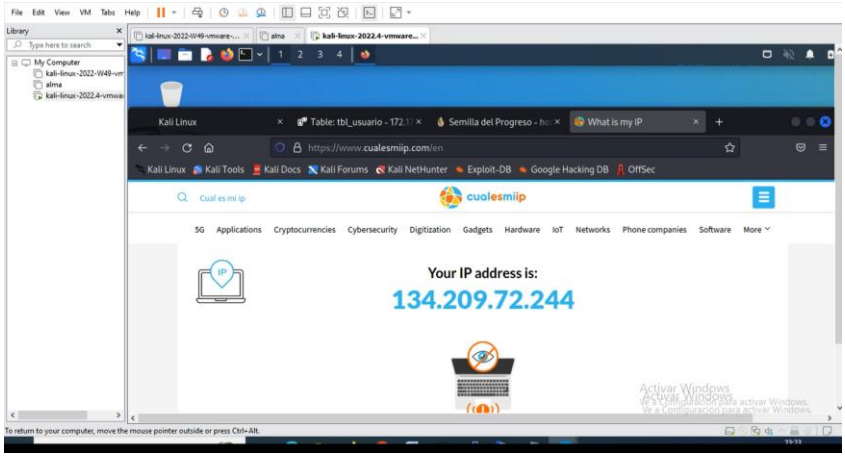
Figura 35: Tráfico seguro a través de VPN



Fuente: Elaboración propia.

También otra manera de comprobar que se está navegando por una red privada virtual es al consultar cual es la dirección IP y en la figura 36 se muestra la dirección IP diferente a la de la red.

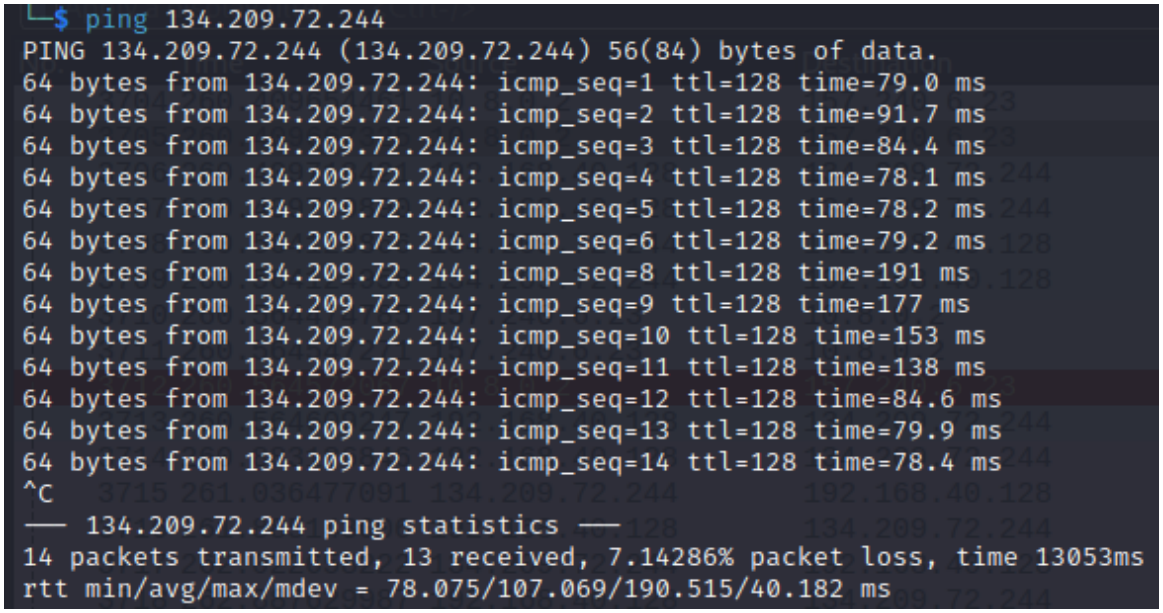
Figura 36: Dirección IP publicas luego túnel VPN



Fuente: Elaboración propia.

Adicionalmente para probar la conexión existente se necesita ver la latencia al servidor OpenVPN mediante un ping y comprobar la conexión donde muestra la efectividad y eficiencia de la comunicación desde las estaciones de trabajo de la cooperativa hasta llegar a los servicios en la nube.

Figura 37: Latencia desde los clientes hacia el servidor



Fuente: Elaboración de propia

En la figura 37 muestra que existe conexión desde una de las estaciones de trabajo hacia el servidor teniendo los siguientes resultados: 14 paquetes enviados, 1 paquete perdido, 7,14% de paquetes perdidos, tiempo de respuesta de 13.053 segundos.

Mencionar una vez más que por seguridad de la información de la COAC todas la pruebas y conexión para este informe se hacen al servidor de pruebas donde consta un servidor de Base de Datos y el servidor web de manera virtualizado.

Por ende, se accedió a la página web de la cooperativa, como se muestra en la siguiente figura.

Figura 38: Acceso al servidor web

Fuente: Elaboración de propia

Para mayor seguridad de conexión existente y como evidencia de que existe la conexión en esta ocasión se captura los datos como las direcciones IP en los logs del sistema.

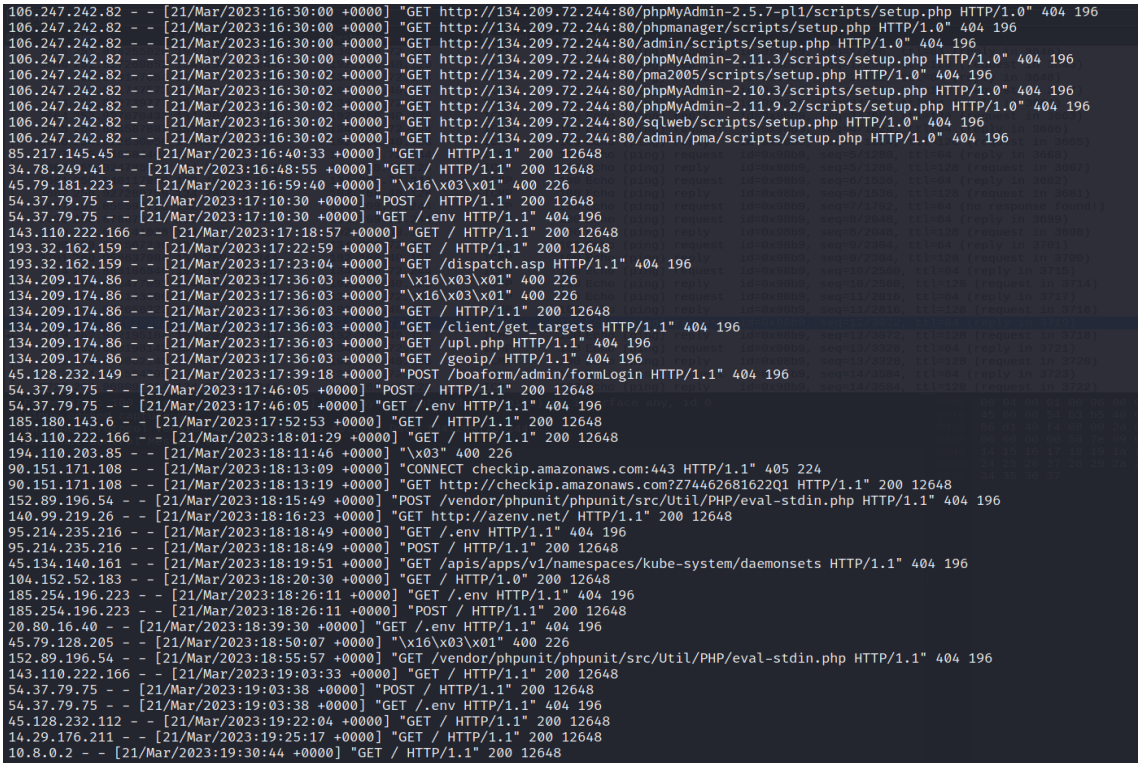
Figura 39: Log de acceso al servidor web

```
[root@almalinux logsmysql]# docker logs -f 70c1d0207e1d
AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using 172.17.0.3. Set the 'ServerName' directive globally to suppress this message
AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using 172.17.0.3. Set the 'ServerName' directive globally to suppress this message
[Fri Dec 16 19:35:03.120124 2022] [mpm_event:notice] [pid 1:tid 140148666322240] AH00489: Apache/2.4.54 (Unix) configured -- resuming normal operations
[Fri Dec 16 19:35:03.120270 2022] [core:notice] [pid 1:tid 140148666322240] AH00094: Command line: 'httpd -D FOREGROUND'
157.100.88.2 - - [16/Dec/2022:19:35:10 +0000] "GET / HTTP/1.1" 200 12648
157.100.88.2 - - [16/Dec/2022:19:35:10 +0000] "GET /modules/system/assets/js/framework.js HTTP/1.1" 404 196
157.100.88.2 - - [16/Dec/2022:19:35:10 +0000] "GET /modules/system/assets/css/framework.extras.css HTTP/1.1" 404 196
157.100.88.2 - - [16/Dec/2022:19:35:10 +0000] "GET /modules/system/assets/js/framework.extras.js HTTP/1.1" 404 196
157.100.88.2 - - [16/Dec/2022:19:35:13 +0000] "GET / HTTP/1.1" 304 -
157.100.88.2 - - [16/Dec/2022:19:35:13 +0000] "GET /modules/system/assets/js/framework.js HTTP/1.1" 404 196
157.100.88.2 - - [16/Dec/2022:19:35:13 +0000] "GET /modules/system/assets/css/framework.extras.css HTTP/1.1" 404 196
157.100.88.2 - - [16/Dec/2022:19:35:13 +0000] "GET /modules/system/assets/js/framework.extras.js HTTP/1.1" 404 196
185.246.221.101 - - [16/Dec/2022:19:37:12 +0000] "GET / HTTP/1.1" 200 12648
157.100.88.2 - - [16/Dec/2022:19:37:49 +0000] "GET / HTTP/1.1" 200 12648
157.100.88.2 - - [16/Dec/2022:19:37:50 +0000] "GET /modules/system/assets/js/framework.js HTTP/1.1" 404 196
157.100.88.2 - - [16/Dec/2022:19:37:50 +0000] "GET /modules/system/assets/js/framework.extras.js HTTP/1.1" 404 196
157.100.88.2 - - [16/Dec/2022:19:37:50 +0000] "GET /modules/system/assets/css/framework.extras.css HTTP/1.1" 404 196
157.100.88.2 - - [16/Dec/2022:19:37:58 +0000] "GET /modules/system/assets/js/framework.js HTTP/1.1" 404 196
157.100.88.2 - - [16/Dec/2022:19:37:58 +0000] "GET /modules/system/assets/js/framework.extras.js HTTP/1.1" 404 196
157.100.88.2 - - [16/Dec/2022:19:37:58 +0000] "GET /modules/system/assets/css/framework.extras.css HTTP/1.1" 404 196
157.100.88.2 - - [16/Dec/2022:19:38:49 +0000] "GET / HTTP/1.1" 304 -
157.100.88.2 - - [16/Dec/2022:19:38:50 +0000] "GET /modules/system/assets/js/framework.js HTTP/1.1" 404 196
157.100.88.2 - - [16/Dec/2022:19:38:50 +0000] "GET /modules/system/assets/js/framework.extras.js HTTP/1.1" 404 196
157.100.88.2 - - [16/Dec/2022:19:38:50 +0000] "GET /modules/system/assets/css/framework.extras.css HTTP/1.1" 404 196
157.100.88.2 - - [16/Dec/2022:19:38:51 +0000] "GET / HTTP/1.1" 304 -
157.100.88.2 - - [16/Dec/2022:19:38:52 +0000] "GET /modules/system/assets/js/framework.js HTTP/1.1" 404 196
157.100.88.2 - - [16/Dec/2022:19:38:52 +0000] "GET /modules/system/assets/js/framework.extras.js HTTP/1.1" 404 196
157.100.88.2 - - [16/Dec/2022:19:38:52 +0000] "GET /modules/system/assets/css/framework.extras.css HTTP/1.1" 404 196
157.100.88.2 - - [16/Dec/2022:19:39:29 +0000] "GET / HTTP/1.1" 304 -
157.100.88.2 - - [16/Dec/2022:19:39:29 +0000] "GET /modules/system/assets/js/framework.js HTTP/1.1" 404 196
157.100.88.2 - - [16/Dec/2022:19:39:30 +0000] "GET /modules/system/assets/js/framework.extras.js HTTP/1.1" 404 196
157.100.88.2 - - [16/Dec/2022:19:39:30 +0000] "GET /modules/system/assets/css/framework.extras.css HTTP/1.1" 404 196
```

Fuente: Elaboración de propia

Se muestra además la captura de la petición HTTP al servicio de la página web

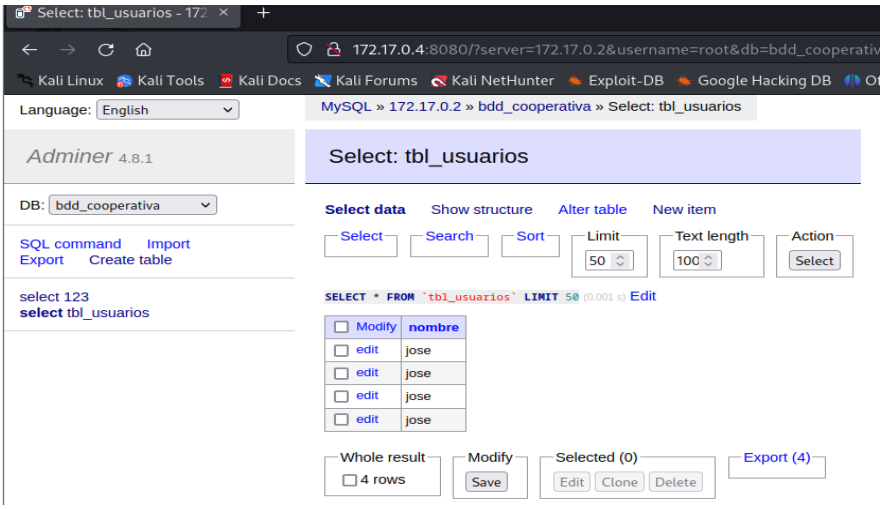
Figura 40: Acceso al servidor web por HTTP



Fuente: Elaboración de propia

Por otra parte, se visualiza además el Log a la base de datos, donde se observa el ingreso a la administración.

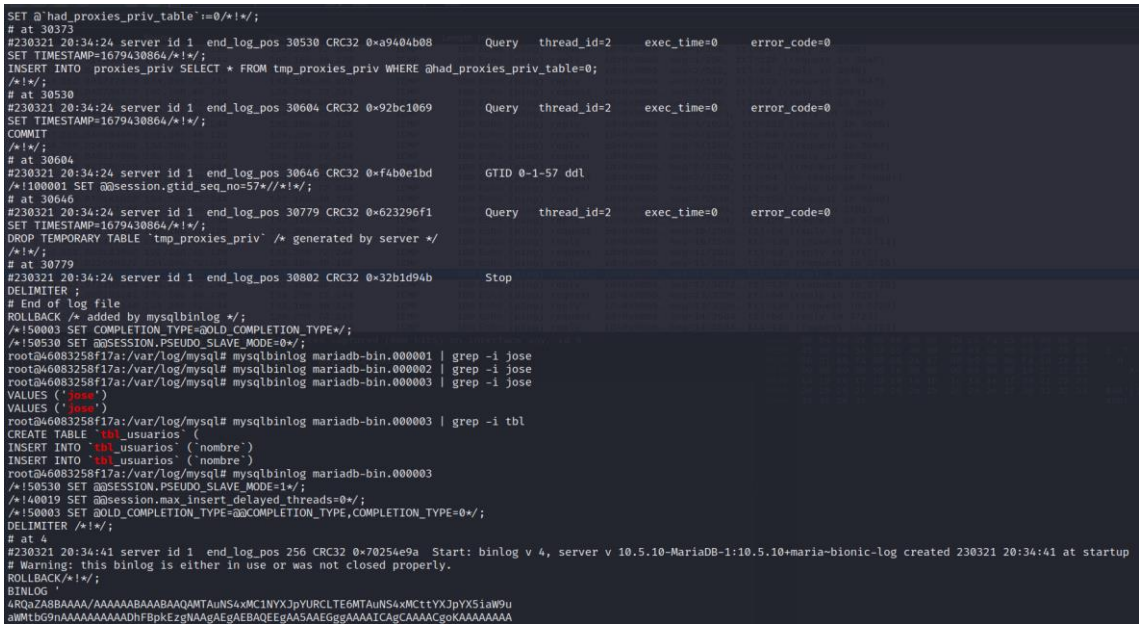
Figura 41: Acceso al servidor de base de datos



Fuente Elaboración de propia

La virtualización de los logs del sistema con la creación e inserción de datos gracias a la conexión que brinda la VPN se visualiza que ha existido ingreso e inserción de información en la base de datos de prueba.

Figura 42: Acceso del Log y la inserción a la Base de Datos



Fuente Elaboración de propia

Al usar la tecnología la red se ha extendido, nuestra red local se encuentra conectado con las agencias y a los servidores que se encuentran en la nube manteniendo la seguridad, funcionalidad y políticas de una red privada virtual con una conexión segura; de esta manera se está protegiendo al activo más importante que es la información.

Gracias al uso del protocolo OpenVPN se ha podido mitigar los riesgos en la perdida de datos durante la comunicación de las agencias hacia los servicios o recursos que se encuentra bajo los servidores de la Cooperativa de Ahorro y Crédito “Semilla del Progreso” Cía. Ltda. Ya que las comunicaciones son seguras porque se está navegado por un protocolo de internet diferente a red local, además su información es cifrada bajo el protocolo OpenVPN como se muestra en la figura 36.

CONCLUSIONES

- La fundamentación Teórica para el desarrollo de la investigación es la parte primordial en todo el proceso donde se pretende tener éxito en un proyecto, en esta investigación se determinó que la seguridad de la información es nuevo reto debido a los cambios tecnológicos que trae consigo vulnerabilidades, que hasta el 2020 se han registrado 5048 denuncias por delitos informáticos en entidades financieras.

- Las entidades financieras han empezado a contratar personal relacionado con la seguridad de la información o Ciberseguridad por lo que hasta el 2020, el 56% de las entidades financieras ya cuentan con personal encargado en seguridad de la información, aunque la oferta de personal especializado es muy baja.

- Para el desarrollo de este proyecto se utilizó la metodología Magerit ya que implementa procesos de gestión de Riesgos, permitió gestionar el tratamiento y el control de los riesgos teniendo en cuenta el uso te las tecnologías enfatizando los activos de información en varios grupos.

- Teniendo presente que los riesgos están en todas las organizaciones y su adecuada gestión frente a las tecnologías depende el éxito, con esta metodología se presentó la propuesta de fácil comprensión por la alta gerencia porque se expresan en términos generales para la toma de decisiones.

- Usar OpenVPN es tener conexión multiplataforma con excelente estabilidad y escalabilidad para cientos o miles de usuarios su agilidad es la principal característica debido a lo liviano de los protocoles de encriptación y comprensión de los datos.

- Facilidad en momento de configurar ya que usa mínima línea de comando además de soportar IPv6 y cuenta con una comunidad activa de usuarios, ha hecho que se opte por esta tecnología, y como producto final de esta

investigación se desarrolló la propuesta de la implementación de red privada virtual en la infraestructura tecnológica en la nube, para ello se instaló el servidor con OpenVPN y se creó clientes para ser instalados en los terminales. De esta manera obtener la comunicación de manera cifrada mediante uso de protocolos.

RECOMENDACIONES

- Todas las entidades financieras deben tener una metodología, herramientas y procedimiento definidos para analizar los posibles riesgos a sufrir, enfocados a las tecnologías de la información y las amenazas existentes.

- Para mayor seguridad al compartir la información de la matriz con las agencias el encargado de la red deberá configurar las seguridades necesarias y el permiso de ingreso dependiendo de los perfiles de usuarios y el tipo de trabajo que realiza.

- En trabajos futuros donde se pretenda instalar una red privada virtual se recomienda tener un servidor con un sistema operativo actualizado, ya que, el software para los servidores está dejando de tener actualizaciones.

- Los requisitos básicos para poder instalar una red privada virtual que se deben tomar en cuenta son las tecnologías a instalar y escoger las mejores opciones acorde a los niveles de seguridad y siguiendo las normas acordes a la protección de la comunicación.

- Es fundamental analizar el número de usuarios que va tener nuestra Red Privada Virtual y comparar con el ancho de banda de nuestra red pública para obtener un correcto funcionamiento.

BIBLIOGRAFÍA

Amazon. (2023). ¿Qué es IPsec? Recuperado el 13 de 04 de 2023, de aws amazon: https://aws.amazon.com/es/what-is/ipsec/

Abdulazeez, A. M., Salim, B. W., Zeebaree, D. Q., & Doghramachi, D. (2020). Comparison of VPN Protocols at Network Layer Focusing on Wire Guard Protocol. International Journal of Interactive Mobile Technologies, 14(18), 157–177. https://doi.org/10.3991/ijim.v14i18.16507

Avigdys Roo. (2004). RED PRIVADA VIRTUAL COMO ALTERNATIVA PARA EL ACCESO REMOTO. Redalyc, 3.

Aragón, R. (2021). Diferencias entre VPN Site-to-Site de las VPN de Acceso Remoto. https://www.syscomblog.com/2021/01/diferencias-entre-vpn-site-to-site-de.html

Aliaga, E., & Asanza Briones, A. (2021). *ANÁLISIS DE VULNERABILIDADES SOBRE PROTOCOLOS VPN.* GUAYAQUIL.

Carisio, E. (2018). Políticas de seguridad informática y su aplicación en la empresa. Barcelona: ADNCLOUD Innovación en la sociedad digital.

Carlini, A. (2016). Ciberseguridad: un nuevo desafio para la comunidad internacional. https://doctrine.af.mil/download.jsp?filename=3-

Castro, Y. A. (2021). SEGURIDAD INFORMÁTICA EN EL SISTEMA OPERATIVO LINUX EN SUS DIVERSAS DISTRIBUCIONES APLICADAS A LAS TECNOLOGÍAS DE LA INFORMACIÓN. Colombia.

García, D. (26 de 05 de 2021). Dagara Informática. Obtenido de La importancia de la seguridad por capas: https://dagara.net/la-importancia-de-la-seguridad-por-capas/

Gómez, L., Navas, D., Mayor, G., & Buitrago, L. (2014). Literature review methodology for scientific and information management, through its structuring and systematization. Medellín.

CN- PYTEC. (2018). Recomendaciones de Seguridad para VPN IPSec. España: CN- PYTEC CCN. Obtenido de Recomendaciones de Seguridad para VPN

Daniel, L.-A., De Ruiter, J., & Poll, E. (n.d.). Inferring OpenVPN State Machines Using Protocol State Fuzzing. Retrieved October 16, 2022, from https://github.com/jderuiter/

De la luz, S. (09 de 02 de 2023). Redeszone. Obtenido de Mejora la seguridad de tu VPN con el protocolo IPsec: https://www.redeszone.net/tutoriales/vpn/ipsec-que-es-como-funciona/

Frankel, S., Kent, K., Lewkowski, R., D Orebaugh, A., W Richey, R., & R Sharma, S. (2005). Guide to IPsec VPNs. Nist Special Publication.

Hernández, M. (2022). Situación de los servicios financieros digitales, la seguridad de la información y ciberseguridad en el Sector Financiero Popular y Solidario. X-Pedientes Económicos, 18-32.

IBM Corporation. (2021). Protocolo Internet (Internet Protocol) - Documentación de IBM. https://www.ibm.com/docs/es/aix/7.2?topic=protocols-internet-protocol

It Ahora, Deloitte. (2021). Segundo estudio - Estado actual del Ciberseguridad en Ecuador 2021. Guayaquil.

Itahora. (19 de abril de 2021). La revista lider en Tecnología . Obtenido de Retos para la Superintendencia de Economía Popular y Solidaria – SEPS ante los riesgos de Ciberseguridad y Seguridad de la Información: https://itahora.com/2021/04/19/retos-para-la-superintendencia-de-economia-popular-y-solidaria-seps-ante-los-riesgos-de-ciberseguridad-y-seguridad-de-la-informacion-en-el-sector-financiero-popular-y-solidario/#_ftn1

Jota, Y., Ramirez, D., & Penagos, A. (2018). DISEÑO DE UNA RED PRIVADA VIRTUAL (VPN) CON SEGURIDAD L2PT PARA LA EMPRESA LABORATORIOS EXPOFARMA S.A. Bogotá.

larepublica. (n.d.). Aumenta la preocupación por la ciberseguridad en Latinoamérica | La República EC. Retrieved October 23, 2022, from https://www.larepublica.ec/blog/2021/03/24/aumenta-la-preocupacion-por-la-ciberseguridad-en-latinoamerica/

López, J. T. (2011). Capas de seguridad en red. https://www.elmundoenbits.com/2011/10/capas-de-seguridad-en-red.html#.Y1X8UXZBzIV

Lis, V. M. (20 de enero de 2000). Glossary from the VPN Mailing List. Obtenido de http://kubarb.phsx.ukans.edu/~tbird/vpn/vpnglossary.html>

Matthews, R. (2020). NORDVPN. Obtenido de https://nordvpn.com/es/blog/que-es-tunel-vpn/

Ministerio de Defensa. (2022). Seguridad en Redes Privadas Virtuales (VPN). Madrid: Esquema Nacional de Seguridad.

MINTEL. (n.d.). Ecuador trabaja en medidas preventivas para evitar los “ciberdelitos” – Ministerio de Telecomunicaciones y de la Sociedad de la Información. Retrieved October 23, 2022, from https://www.telecomunicaciones.gob.ec/ecuador-trabaja-en-medidas-preventivas-para-evitar-los-ciberdelitos/

OEA. (2023). FUERZA LABORAL DE CIBERSEGURIDAD.

OpenVPN. (10 de 03 de 2022). OpenVpn Community. Obtenido de https://community.openvpn.net/openvpn/wiki/OverviewOfOpenvpn

OVL. (26 de febrero de 2006). La necesidad de VPNs Autenticación y Encripción de datos Los retos reales de implementar VPNs. págs. 26-41.

Peña Catalá, J. L., Pérez Torres, W., & Blanco García, Y. (2006). El Sistema Operativo LINUX y el cambio necesario. Panorama Cuba y Salud, 1, 44–50.

Protocolos de tunelización VPN. (2012). https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc771298(v=ws.10)?redirectedfrom=MSDN

Pomar Pascual, R. (2019). Implementación de una red privada virtual de software libre en una empresa. España de Creative Commons.

Quezada L., H. D. (2016). Diseño de una VPN para el acceso a las bases de datos científicas de la Universidad Nacional de Loja. Loja.

Quishpe Iza, L. M. (2021). ESTUDIO PARA LA IMPLEMENTACIÓN DE UNA RED PRIVADA VIRTUAL(VPN) UTILIZANDO HERRAMIENTAS DE SOFTWARE LIBRE. QUITO.

Raboyo, V. (2022). MODELO DE MEJORA DEL ESTADO DE LA CIBERSEGURIDAD EN LA GOBERNACIÓN DE TUNGURAHUA. AMBATO.

Razo, A. (2023). ANÁLISIS CONCEPTUAL DEL PROTOCOLO VXLAN PARA LA VIRTUALIZACIÓN DE CENTRO DE DATOS PARA EOT. Quito.

Roberto Sampieri, Collado, C., & Lucio, M. (1990). Metodologia de la Investigacion. https://doi.org/978-1-4562-2396-0

Sofia, P., & Sofía, D. (2004). Linux: Hacia una revolución silenciosa de la sociedad de la información. Revista de Ciencias Sociales (Ve), X(2), 207–223. https://www.redalyc.org/articulo.oa?id=28010202

Tejena-Macías, M. A. (2018). Análisis de riesgos en seguridad de la información. Polo Del Conocimiento, 3(4), 230. https://doi.org/10.23857/pc.v3i4.809

Vienažindytė, I. (2019). TCP vs. UDP, comparamos los dos protocolos. NordVPN. https://nordvpn.com/es/blog/protocolo-tcp-udp/

VLEX. (2009). Deloitte: Menos ataques a los bancos, pero más sofisticados. Libros y Revistas - VLEX 229105409. https://vlex.es/vid/deloitte-menos-ataques-sofisticados-229105409

Winawang, Y. (2021). Implementasi Keamanan Jalur Internet Menggunakan IP Tunneling pada OpenVPN Access Server dengan Protokol OpenVPN dan Protokol DNS Over HTTPS. Jurnal Health Sains, 2(4), 712–730. https://doi.org/10.46799/jsa.v2i4.207

Xu, Z., & Ni, J. (2020). Research on network security of VPN technology. Proceedings - 2020 International Conference on Information Science and

Education, ICISE-IE 2020, 539–542. https://doi.org/10.1109/ICISE51755.2020.00121

Zapata, M., Pacheco, F., De la Torre, E., & Vallejo, M. (2017). Evaluación de Parámetros de QoS en una Red VPN-MPLS Diffservbajo un Entorno Completo de Emulación de Software Libre. 9.

Zárate, I. R., Carbajal, M. O., Godínez, F. I. P., Barrón, E. R., Ramírez, A. M., & Quimby, L. A. R. (2005). Introducción a la Seguridad con IP Seguro en Internet (IPSec). Polibits, (32), 16–21. https://www.redalyc.org/articulo.oa?id=402640445004

ANEXOS

Anexo 1. Modelo de entrevista realizada

Pontificia Universidad Católica del Ecuador | Sede Ambato

Modelo de entrevista realizada

Esta Entrevista tiene como fin poder obtener la información necesaria sobre la seguridad de la información en la entidad financiera de esta manera poder realizar el proyecto de Investigación.

Estimados señores permítame hacer las siguientes preguntas:

1. **¿Qué entiende por seguridad de la información?**
2. **¿Cree usted que tiene la suficiente la protección ante posibles amenazas?**
3. **¿Conoce usted algún método de protección de la información a nivel de la red?**
4. **¿Ha escuchado hablar de la rede Privada Virtuales o VPN?**
5. **¿Qué entiende por encriptación o cifrado de datos?**
6. **¿Cree usted que debe mejorar su nivel de protección ante las nuevas amenazas existentes?**
7. **¿Desea usted mejorar su seguridad usando las VPN de esta manera poder tener una comunicación a través de un túnel seguro entres dispositivos?**

Anexo 2. Instalación el servidor OpenVPN en AlmaLinux 8

Requisitos previos

- Un servidor ejecutando uno de los siguientes sistemas operativos: AlmaLinux 8.
- Se recomienda utilizar una instalación nueva del sistema operativo para evitar posibles problemas.

Paso 1. Primero, debemos asegurar de que su sistema esté actualizado.

```
sudo dnf update
sudo dnf install epel-release
```

Paso 2. Instalar el servidor OpenVPN en AlmaLinux 8.

Instalar el servidor OpenVPN, ejecute el siguiente comando para descargar el instalador OpenVPN desde la página de GitHub:

```
curl -O https://raw.githubusercontent.com/angristan/openvpn-install/master/openvpn-install.sh
```

Una vez descargado el archivo, convertir en ejecutable:

```
chmod +x openvpn-install.sh
```

```
./openvpn-install.sh
```

El script iniciará el proceso de instalación con una serie de preguntas seguidas de un mensaje y su respuesta:

Después de eso, agregar un nuevo cliente y verá la siguiente pantalla de salida donde se debe definir el Nombre del cliente:

```
Okay, that was all I needed. We are ready to setup your OpenVPN server now.
You will be able to generate a client at the end of the installation.
Press any key to continue...
```

Tell me a name for the client.

The name must consist of alphanumeric character. It may also include an underscore or a dash.

Client name: coacsemilla

A continuación, le pregunta si desea proteger el archivo de configuración con una contraseña:

Do you want to protect the configuration file with a password?

(e.g. encrypt the private key with a password)

1) Add a passwordless client

2) Use a password for the client

Select an option [1-2]: 1

Finalmente, se muestra el mensaje de que el proceso ha sido exitoso:

Client coacsemilla added.

The configuration file has been written to /home/user/idroot.ovpn.

Download the .ovpn file and import it in your OpenVPN client.