EPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

TEMA:

"EVALUACIÓN DE LA EFECTIVIDAD DE VPN OPEN SOURCE EN ESTRATEGIAS DE CIBERSEGURIDAD: UN ESTUDIO INTEGRAL SOBRE IMPLEMENTACIÓN, DESAFÍOS Y MEJORES PRÁCTICAS"

Trabajo de Titulación previo a la obtención del Título de Magíster en Computación con Mención en Seguridad Informática

AUTOR: MORALES BERRONES ROMEO JAVIER
DIRECTOR: PHD. PUSDÁ CHULDE MARCO REMIGIO
ASESOR: PHD. GARCÍA SANTILLÁN IVÁN DANILO

IBARRA - ECUADOR

2025

DEDICATORIA

A mi esposa e Hijos,

Dedicar este trabajo a ustedes es una manera de expresar mi profundo agradecimiento por todo el amor, apoyo y sacrificio que han brindado a lo largo de mi vida y especialmente durante este trayecto académico. Su constante aliento y ejemplo han sido mi mayor inspiración, y cada logro que alcanzo es un reflejo de la dedicación y valores que me han inculcado. A través de sus enseñanzas, he aprendido la importancia del esfuerzo, la perseverancia y el compromiso, y hoy, al completar esta tesis de maestría, celebro también sus sacrificios y su inquebrantable fe en mí. Gracias por ser mis pilares de fortaleza y por creer en mis sueños incluso cuando yo dudaba. Este logro es también suyo, y lo comparto con ustedes con todo mi amor y gratitud.

Con cariño,

Morales Berrones Romeo Javier

AGRADECIMIENTO

Queridos profesores, compañeros, familia y amigos,

Hoy, al presentar esta tesis que marca el final de mi trayecto de maestría, quiero tomarme un momento para expresar mi más profundo agradecimiento a Dios por todas sus bendiciones y a todas las personas que han contribuido a este logro significativo en mi vida.

En primer lugar, quiero agradecer a la Universidad Técnica del Norte por brindarme la oportunidad de cursar este programa de maestría. Ha sido una experiencia transformadora que ha enriquecido no solo mi conocimiento académico, sino también mi crecimiento personal y profesional. Agradezco a mis profesores por su dedicación, orientación y apoyo constante a lo largo de este viaje académico. Sus enseñanzas han sido invaluables para mi desarrollo como investigador y profesional en formación.

A mi familia, quiero expresarles mi más profundo agradecimiento. Su amor incondicional, apoyo emocional y sacrificio han sido los pilares que me han sostenido durante este proceso. A pesar de los desafíos y las dificultades, ustedes siempre estuvieron ahí para brindarme aliento y motivación. Agradezco especialmente a mi esposa y a mis hijos, por su paciencia, comprensión y aliento constante. Este logro no habría sido posible sin su inquebrantable apoyo.

También quiero reconocer y agradecer a mis amigos y seres queridos que estuvieron a mi lado, brindándome su amistad, comprensión y aliento en los momentos difíciles. Sus palabras de aliento y sus gestos de solidaridad me han dado la fuerza para seguir adelante incluso en los momentos más desafiantes, Su contribución fue fundamental para el desarrollo y la conclusión de este trabajo académico. ¡Gracias infinitas!

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el repositorio digital institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CEDULA DE IDENTIDAD:	1802794154		
NOMBRES Y APELLIDOS:	MORALES BERRONES ROMEO JAVIER		
DIRECCIÓN:	EL BAMBU Y EL TEJO AMBATO - ECUADOR		
EMAIL:	rjmoralesb@utn.edu.ec		
TELÉFONO FIJO:	032527958	**TELÉFONO MÓVIL**	0992527720

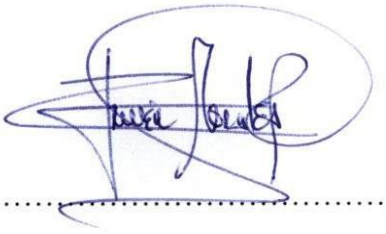
DATOS DE LA OBRA	
TÍTULO	"EVALUACIÓN DE LA EFECTIVIDAD DE VPN OPEN SOURCE EN ESTRATEGIAS DE CIBERSEGURIDAD: UN ESTUDIO INTEGRAL SOBRE IMPLEMENTACIÓN, DESAFÍOS Y MEJORES PRÁCTICAS"
AUTOR:	MORALES BERRONES ROMEO JAVIER
FECHA:	**02/06/2025**
PROGRAMA	POSTGRADO
TÍTULO POR EL QUE OPTA:	MAGÍSTER EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA
ASESOR/DIRECTOR PHD. GARCÍA SANTILLÁN IVÁN DANILO	**DIRECTOR: ASESOR:** PHD. PUSDÁ CHULDE MARCO REMIGIO

CONSTANCIAS

El autor(es) manifiesta(n) que la obra de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y es (son) el (los) titular (es) de los derechos patrimoniales, por lo que asumen la responsabilidad sobre el contenido de la misma y saldrá(n) en defensa de la universidad en caso de reclamación por parte de terceros.

Ibarra, a los 6 días del mes de junio de 2025.

EL AUTOR:



(Firma).....

Nombre: Morales Berrones Romeo Javier

CERTIFICACION DIRECTOR DEL TRABAJO DE INTEGRACION CURRICULAR

Ibarra ,02 de junio de 2025

Ing. Marco Remigio Pusdá Chulde, PhD.

DIRECTOR DEL TRABAJO DE INTEGRACION CURRICULAR

CERTIFICA:

Haber revisado el presente informe final del trabajo de Integración Curricular, mismo que se ajusta a las normas vigentes de la Universidad Técnica del Norte; en consecuencia, autorizo su presentación para los fines legales pertinentes.

MARCO
REMIGIO
PUSDA CHULDE

Firmado digitalmente por MARCO REMIGIO PUSDA CHULDE
Fecha: 2025.06.02 15:12:03 -05'00'

.....

Ing. Marco Remigio Pusdá Chulde, PhD.
Cc; 0401200951

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

PROGRAMA DE MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

"EVALUACIÓN DE LA EFECTIVIDAD DE VPN OPEN SOURCE EN ESTRATEGIAS DE CIBERSEGURIDAD: UN ESTUDIO INTEGRAL SOBRE IMPLEMENTACIÓN, DESAFÍOS Y MEJORES PRÁCTICAS"

.

Autor: Romeo Javier Morales Berrones
Tutor: PHD. PUSDÁ CHULDE MARCO
Año: 2025

RESUMEN

El objetivo de esta investigación fue analizar la eficacia de las VPN de código abierto dentro de las estrategias de ciberseguridad, a través de un estudio exhaustivo que abarca su implementación, los retos que conlleva y las mejores prácticas recomendadas. En un contexto de creciente interconectividad y amenazas cibernéticas, las Redes Privadas Virtuales (VPN) han adquirido un papel fundamental en la protección y privacidad de las comunicaciones en línea. Las soluciones VPN de código abierto representan una alternativa flexible y accesible, brindando a las organizaciones la posibilidad de personalizar y gestionar sus propias medidas de seguridad.

Este estudio tiene como propósito evaluar el desempeño de estas herramientas en la protección de datos y comunicaciones frente a diversas amenazas digitales, identificar las dificultades técnicas y operativas que pueden surgir en su implementación y mantenimiento, y ofrecer recomendaciones basadas en evidencia para optimizar su uso en entornos corporativos.

La investigación combinará una revisión bibliográfica, el análisis de casos de estudio y pruebas prácticas. Para ello, se seleccionarán distintas soluciones VPN de código abierto, evaluando aspectos como seguridad, rendimiento, facilidad de uso y el respaldo de la

comunidad.

A través de este trabajo, se busca aportar un análisis detallado sobre las ventajas y limitaciones de las VPN de código abierto en el ámbito de la ciberseguridad. Con esta información, se pretende facilitar la toma de decisiones en las organizaciones respecto a la adopción de estas tecnologías, permitiendo mejorar su seguridad y optimizar sus recursos tecnológicos.

El estudio integral de las VPN de código abierto permitirá determinar su efectividad en la protección de la información, los desafíos que implica su implementación y las mejores prácticas para su uso eficiente. Este conocimiento resulta clave para fortalecer las estrategias de ciberseguridad en un entorno digital en constante cambio.

Palabras clave: Seguridad de la información, amenazas, vulnerabilidades, riesgos, VPN, virtualización.

ABSTRACT

The purpose of this research is to assess the effectiveness of open-source VPNs in cybersecurity strategies through a comprehensive study that covers their implementation, associated challenges, and best practices. In the current context of increasing interconnectivity and cyber threats, Virtual Private Networks (VPNs) have become essential tools for ensuring the security and privacy of online communications. Open-source VPN solutions offer a flexible and cost-effective alternative, allowing organizations to customize and control their security implementations.

This study aims to analyze the performance of these tools in protecting data and communications against various cyber threats, examine the technical and operational challenges that may arise when deploying and maintaining open-source VPN solutions, and provide evidence-based recommendations to optimize their implementation and management in corporate environments.

The research will be conducted through a combination of literature review, case study analysis, and practical testing. Various open-source VPN solutions will be selected for evaluation, considering factors such as security, performance, ease of use, and community support.

This work seeks to contribute to a better understanding of the advantages and limitations of open-source VPNs in the field of cybersecurity. By providing a detailed analysis, organizations can make informed decisions about adopting these tools, thereby enhancing their security posture and optimizing their technological resources.

A comprehensive evaluation of open-source VPNs will help identify their effectiveness in protecting information, the challenges associated with their implementation, and the best practices for their optimal use. This knowledge is essential to strengthen cybersecurity strategies in an ever-evolving digital environment.

Keywords: Information security, threats, vulnerabilities, risk, VPN, virtualization.

CAPITULO I

1. EL PROBLEMA

1.1 Problema de investigación

En la actualidad, la creciente necesidad de conectividad remota y la transmisión de información sensible a través de redes públicas han incrementado los riesgos de ciberseguridad para individuos, organizaciones y empresas.

Según (Jones, 2021)Con el auge del teletrabajo, el uso de servicios en la nube y la demanda de conexiones seguras tanto en entornos personales como corporativos, las redes privadas virtuales (VPN) han adquirido un papel fundamental en la protección de datos y la privacidad digital.

Según (Brown, 2022)En este escenario, las VPN de código abierto se han posicionado como una alternativa viable y accesible frente a las soluciones comerciales, ya que brindan mayor transparencia en su código, permiten auditorías de seguridad y ofrecen la posibilidad de ser adaptadas a las necesidades específicas de los usuarios.

No obstante, a pesar de sus múltiples beneficios, aún persisten dudas sobre su nivel de seguridad y eficacia en comparación con las VPN propietarias. Aunque soluciones como OpenVPN y WireGuard emplean protocolos de cifrado y autenticación robustos, una configuración incorrecta o la falta de actualizaciones pueden generar vulnerabilidades que podrían ser aprovechadas por atacantes. Además, la creciente sofisticación de las amenazas cibernéticas, como el robo de credenciales, la interceptación de información y la alteración de paquetes de datos, exige una evaluación minuciosa de la confiabilidad y resistencia de estas herramientas ante posibles riesgos.

Otro aspecto relevante es la complejidad que implica la implementación y administración de las VPN de código abierto. A diferencia de las soluciones comerciales, que suelen incluir configuraciones predefinidas y soporte técnico especializado, las VPN de código abierto requieren un conocimiento técnico avanzado para su correcta instalación, configuración y mantenimiento.

Según (Robinson, 2020)La integración de estas herramientas con otras soluciones de seguridad, como firewalls, sistemas de detección de intrusos (IDS) y autenticación multifactor (MFA), es esencial para garantizar una protección efectiva. Sin embargo, este proceso puede representar desafíos tanto a nivel técnico como organizacional, ya que exige una administración activa de la configuración y un monitoreo constante para prevenir posibles brechas de seguridad.

En este contexto, es imprescindible llevar a cabo una evaluación integral de la efectividad de las VPN de código abierto, considerando factores clave como su resistencia a ataques, facilidad de implementación, escalabilidad, rendimiento y compatibilidad con diversos sistemas y dispositivos. La presente investigación tiene como objetivo abordar estas cuestiones mediante un análisis detallado que permita identificar tanto sus fortalezas como sus limitaciones, además de definir las mejores prácticas para su implementación en entornos de ciberseguridad.

Asimismo, este estudio busca ofrecer información clave que facilite la toma de decisiones a empresas, instituciones y usuarios que requieren alternativas seguras y confiables para resguardar sus comunicaciones y datos en redes no seguras. A través de pruebas en entornos controlados, análisis de vulnerabilidades y comparaciones con soluciones propietarias, se pretende formular recomendaciones basadas en evidencia para optimizar el uso de VPN de código abierto. De esta manera, se contribuirá al desarrollo de estrategias más sólidas y efectivas para la protección de la información, fortaleciendo la seguridad digital en un mundo cada vez más interconectado y vulnerable a múltiples amenazas cibernéticas.

Según (Simpson, 2021)Las herramientas de seguridad de código abierto, incluyendo soluciones VPN, presentan desafíos únicos en términos de evaluación y validación. Aunque señalan la carencia de estudios sistemáticos que apliquen metodologías de prueba de penetración específicamente diseñadas para evaluar implementaciones VPN de código abierto. Los autores argumentan que "la naturaleza diversa de las implementaciones de código abierto dificulta la generalización de resultados de seguridad, requiriendo enfoques evaluativos adaptados a cada solución específica. Esta observación fundamenta la necesidad de desarrollar marcos metodológicos flexibles que puedan aplicarse a diversas soluciones VPN de código abierto, considerando sus arquitecturas particulares y modelos de desarrollo, mientras mantienen parámetros comparativos consistentes.

Para (Easttom, 2021) argumenta que "la efectividad de soluciones de seguridad como VPNs debe evaluarse considerando principios fundamentales como mínimo privilegio, defensa en profundidad y segmentación, independientemente de su naturaleza comercial o de código abierto. El autor establece criterios evaluativos basados en principios que trascienden implementaciones específicas, facilitando análisis objetivos que consideren aspectos fundamentales de seguridad. Esta perspectiva basada en principios resulta esencial para desarrollar marcos evaluativos que mantengan validez a través del tiempo, incluso mientras tecnologías específicas evolucionan, asegurando que evaluaciones permanezcan relevantes durante el ciclo de vida completo de implementaciones VPN.

Por lo tanto, es esencial llevar a cabo una evaluación de la efectividad de las VPN de código abierto, teniendo en cuenta factores clave como su capacidad para resistir ataques, la facilidad de su implementación, su escalabilidad, rendimiento y compatibilidad con diferentes sistemas y dispositivos. Esta investigación tiene como objetivo abordar estas cuestiones mediante un análisis detallado, que permita identificar tanto las fortalezas como las debilidades de estas herramientas, así como definir las mejores prácticas para su implementación en el

ámbito de la ciberseguridad.

De igual manera, este estudio busca proporcionar información relevante que facilite la toma de decisiones a empresas, instituciones y usuarios que necesiten soluciones seguras y confiables para proteger sus comunicaciones y datos en redes no seguras. A través de pruebas en entornos controlados, análisis de vulnerabilidades y comparaciones con soluciones propietarias, se pretende ofrecer recomendaciones basadas en evidencia para mejorar el uso de VPN de código abierto, contribuyendo así al desarrollo de estrategias más sólidas y efectivas para la protección de la información en un mundo cada vez más interconectado y vulnerable a amenazas cibernéticas.

De acuerdo con Espinoza y Colina (2022) las VPN de código abierto proporcionan una opción más asequible, pero también se topan con retos técnicos y operativos. Así pues, resulta imprescindible valorar su eficacia en estrategias de ciberseguridad, teniendo en cuenta factores técnicos, operativos y jurídicos. Este análisis exhaustivo examinará la aplicación técnica, los retos corporativos y las mejores prácticas para mejorar el desempeño y la seguridad de las VPN de fuente abierta. Se pretende reconocer sus puntos fuertes y débiles en comparación con las soluciones de negocio, ofreciendo sugerencias útiles para su aplicación eficaz. Este esfuerzo ayudará a reducir la brecha en la literatura y favorecerá a las entidades que desean potenciar su seguridad informática con VPN de fuente abierta.

Ante este panorama, es fundamental implementar acciones dirigidas a enfrentar los diversos desafíos de ciberseguridad que afectan el desarrollo de las actividades empresariales, con el propósito de proteger los recursos de información que circulan en internet y que están expuestos a múltiples amenazas, como ataques de denegación de servicio, robo de datos y suplantación de identidad, entre otros.

Para (Green, 2021)Si bien existen soluciones comerciales diseñadas para mitigar estos riesgos, como las redes privadas virtuales (VPN), muchas organizaciones y usuarios

individuales enfrentan limitaciones económicas que dificultan su adopción. Esto resalta la importancia de contar con alternativas de código abierto que permitan garantizar la seguridad de la información transmitida a través de la red.

1.2 Interrogantes de la investigación.

En función del problema identificado, se formulan las siguientes preguntas de investigación, las cuales servirán como eje orientador para el desarrollo del presente estudio.

¿Qué tan efectivas son las VPN de código abierto en comparación con las soluciones comerciales en términos de seguridad y rendimiento?

¿Cuáles son los métodos más efectivos para integrar las soluciones de VPN de código abierto con otros sistemas de seguridad, como firewalls y sistemas de detección de intrusiones (IDS)?

¿Cómo se puede evaluar la efectividad de una VPN de código abierto en términos de implementación segura, considerando aspectos como la configuración, el cifrado y la autenticación?

¿Qué vulnerabilidades son más comunes en las VPN de código abierto y qué medidas se pueden tomar para mejorar su resiliencia frente a amenazas conocidas?

¿Cuáles son las mejores prácticas de implementación para garantizar la seguridad y eficacia de una VPN de código abierto en entornos de ciberseguridad empresarial?

1.3 Objetivos de la investigación.

1.3.1 Objetivo general

Evaluar la efectividad de las VPN de código abierto como una herramienta estratégica de ciberseguridad, abordando aspectos claves como la implementación segura, la evaluación de vulnerabilidades, la resiliencia frente a las amenazas y la identificación de mejores prácticas

1.3.2 Objetivos específicos

1. Diseñar un ambiente de pruebas que permita simular una red VPN Open Source en un entorno controlado.

2. Realizar un análisis de las posibles vulnerabilidades y amenazas asociadas con las redes VPN Open Source, identificando riesgos específicos en el contexto de estrategias de ciberseguridad.

3. Integrar las soluciones de VPN Open Source con otros sistemas de seguridad, como firewalls y sistemas de detección de intrusiones (IDS).

4. Evaluar la efectividad de la red VPN Open Source simulada en términos de implementación segura, identificación de vulnerabilidades y resiliencia frente a amenazas

1.4 Hipótesis de trabajo

Evaluar la efectividad de las VPN de código abierto como una herramienta estratégica de ciberseguridad, permitirá implementación segura, la evaluación de vulnerabilidades, la resiliencia frente a las amenazas y la identificación de mejores prácticas.

1.5 Hipótesis alternativa

"Evaluar la efectividad de las VPN de código abierto como una herramienta estratégica de ciberseguridad no tendrá un impacto significativo en la implementación segura, la evaluación de vulnerabilidades, la resiliencia frente a las amenazas o la identificación de mejores prácticas en comparación con otras soluciones de ciberseguridad."

1.6 Categorización de las Variables

Las variables que se desprenden de las hipótesis formuladas son.

Variable Independiente:

Implementación segura, la evaluación de vulnerabilidades, y la resiliencia frente a las amenazas

***Variable dependiente**:*

Evaluar la efectividad de las VPN de código abierto como una herramienta estratégica de ciberseguridad

1.7 Justificación

Este estudio sobre la efectividad de las VPN de código abierto en las estrategias de ciberseguridad realiza una valiosa contribución al conocimiento en esta área, ofreciendo datos significativos sobre las mejores prácticas, los principales desafíos y los aspectos esenciales que deben tenerse en cuenta para su correcta implementación y optimización. La mejora de la seguridad digital no solo beneficia a las organizaciones e individuos, sino que también tiene un impacto positivo en la sociedad en general, al garantizar la protección de la privacidad y la integridad de los datos personales y empresariales. Este avance en la ciberseguridad juega un papel crucial en la salvaguarda de los derechos digitales y la seguridad de los ciudadanos en el entorno en línea, especialmente en una era cada vez más interconectada y digitalizada.

Los resultados obtenidos a partir de este estudio pueden abrir nuevas líneas de investigación, así como enriquecer la comprensión de cómo las herramientas de VPN de código abierto pueden ser aliadas clave en la protección de la privacidad y la seguridad digital. En un mundo donde la protección de datos y la seguridad de las comunicaciones son cada vez más relevantes, evaluar la efectividad de las VPN Open Source proporciona a los usuarios la información necesaria para tomar decisiones informadas sobre las mejores soluciones de seguridad que se adapten a sus necesidades. Esto también permitirá optimizar la manera en que los usuarios protegen su seguridad en la red, ajustando las herramientas a sus requerimientos específicos.

En el ámbito corporativo, la adopción de VPN de código abierto ofrece múltiples beneficios, tales como la reducción de costos al ser opciones gratuitas o de bajo costo, eliminando así la necesidad de incurrir en gastos adicionales por licencias y mantenimiento. Además, estas soluciones permiten una mayor flexibilidad y personalización, adaptándose de manera más eficiente a las necesidades particulares de cada organización en términos de seguridad y redes. Su naturaleza de código abierto también garantiza mayor transparencia y facilita la auditoría, lo que favorece el cumplimiento de normativas de seguridad y privacidad. Las empresas se benefician de un mayor control e independencia, ya que no dependen de proveedores comerciales para gestionar su infraestructura. Igualmente, el soporte comunitario

activo garantiza actualizaciones constantes y parches de seguridad, lo que contribuye a mantener las soluciones siempre a la vanguardia. Por último, las VPN Open Source son altamente compatibles y escalables, integrándose con diversos dispositivos y sistemas operativos, lo que facilita su implementación en entornos diversos. Si se configuran correctamente, estas herramientas ofrecen niveles elevados de protección contra amenazas externas, asegurando la confidencialidad y la integridad de los datos, lo que las convierte en una opción estratégica para las organizaciones que buscan una protección robusta y económica.

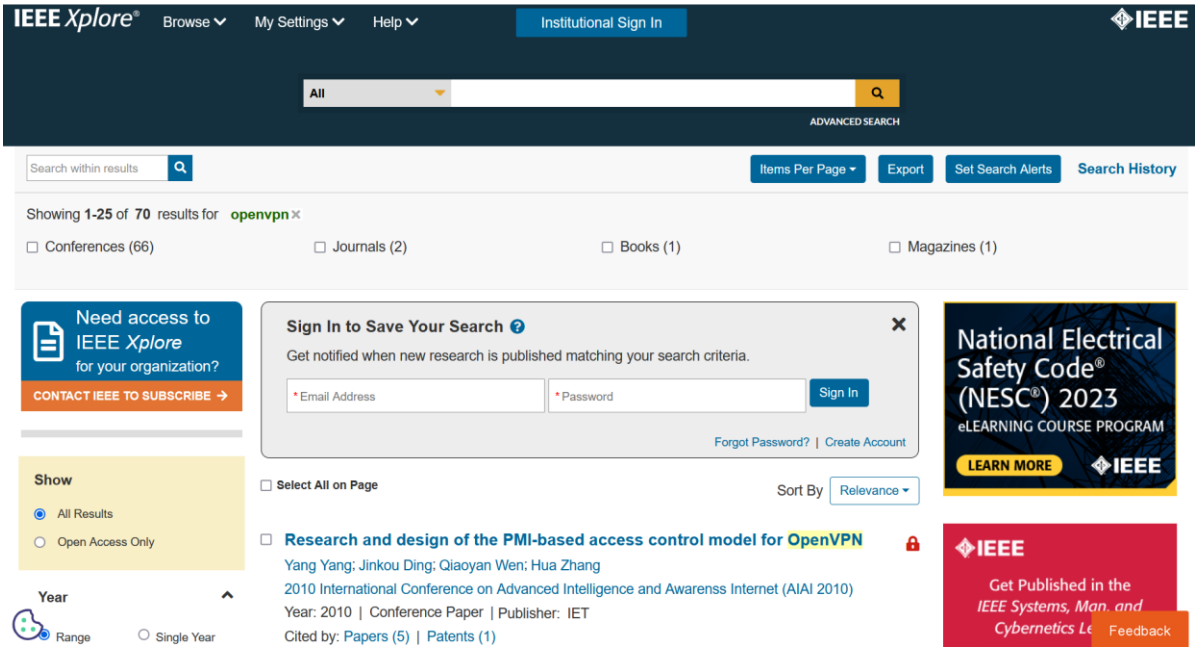
CAPITULO II

2. MARCO REFERENCIAL

2.1Antecedentes

Para identificar los estudios pertinentes a esta investigación, se llevó a cabo una revisión preliminar de la literatura, siguiendo un protocolo de búsqueda estandarizado propio de este tipo de estudios. En primer lugar, se definió una cadena de búsqueda diseñada para responder a la siguiente pregunta de investigación: ¿Qué tan efectivas son las VPN de código abierto en comparación con las soluciones comerciales? La búsqueda se realizó en IEEE Xplore en la figura 1, una base de datos digital que proporciona acceso a una amplia gama de artículos, libros, revistas, actas de conferencias y otros recursos en áreas como ciencias de la computación, ingeniería eléctrica, electrónica y disciplinas relacionadas. Como resultado, se obtuvieron 70 publicaciones entre artículos y libros relevantes para el estudio, además se encontró mas material que sirvió de ayuda para el desarrollo de esta tesis.

Figura 1. Información acerca de OpenVPN en IEEE Explore



En el artículo de (Coonjah, Catherine, & Soyjaudah, 2015), Se realiza una comparación empírica de cómo ambos protocolos afectan la eficiencia y la confiabilidad de la conexión en términos de velocidad de transferencia, latencia, y tasa de pérdida de paquetes. El trabajo pone de manifiesto las ventajas y desventajas de cada protocolo en escenarios de uso real, identificando que TCP, aunque más confiable debido a su control de flujo y retransmisión de paquetes perdidos, introduce una mayor latencia, lo que podría reducir la velocidad de la conexión. Por otro lado, UDP, al no realizar retransmisión de paquetes perdidos y no contar con control de flujo, ofrece una mayor velocidad, pero con el riesgo de pérdida de datos, y concluye que la elección entre TCP y UDP depende del uso específico de la red y de las prioridades de los usuarios en cuanto a la estabilidad o la velocidad de la conexión.

En el trabajo de investigación de Edgar Torres (2006), respecto al diseño e implementación de una VPN en una compañía de comercio, le brindó la oportunidad de mostrar los pros y contras de la implementación de esta red empleando la tecnología IPSec, lo que contribuyó a seleccionar la tecnología más adecuada para la implementación de la VPN.

Según Limari (2004) en su análisis de protocolos de seguridad para VPN, señala que

estos proporcionan un entendimiento extenso del funcionamiento de una red, incluyendo su implementación, estructura, diseño y seguridad entre locales a distancia.

Para Tomás, J (2008), en su proyecto de un plan de Servicio VPN de acceso a distancia basado en SSL a través de OpenVPN, valoró las oportunidades que brinda la aplicación tecnológica seleccionada. El escritor indica que, con el objetivo de establecer conexiones seguras en la infraestructura de redes públicas, se utiliza el protocolo SSL, tiene un vínculo directo con lo que se plantea, ya que en ambas se ha empleado la tecnología OpenVPN para la implementación de la red. Además, muestra las configuraciones para la implementación de esta herramienta, así como la seguridad necesaria para establecer una red.

Lara, F (2014), en su investigación acerca de la creación de una red privada virtual con tecnología MPLS para la carrera de Ingeniería de Networking, llevó a cabo una descripción de la tecnología de Conmutación Multi-Protocolo a través de Etiquetas, utilizando una red privada virtual para la comunicación de la Universidad de Guayaquil en su estudio de Ingeniería en Networking. Se llevó a cabo una descripción de la tecnología MPLS con VPN, destacando sus atributos, beneficios y limitaciones del empleo de las VPN como mecanismo de protección frente a ciberataques.

Según (Quishpe, 2021).Una red privada virtual es una tecnología que facilita la creación de una conexión segura y encriptada entre dos lugares en una red. La mayor ventaja de una VPN comercial sería que oculta la IP. Esta conexión resguarda los datos enviados y encubre la dirección IP del usuario, ofreciendo privacidad y protección en el entorno digital. Esto asegura la privacidad y la seguridad de tus comunicaciones en línea, y facilita la conexión con otros dispositivos como si estuviera en la misma red que ellos

De acuerdo a Fernández, Edwin; Aldás, Alberto; Villarreal, Verónica; Coro, Katherine (2024) Las VPN, se han transformado en un emblema de protección en la red. Las VPN contribuyen a proteger tus contraseñas y otros datos personales importantes de la vista

inadvertida, guiando tu tráfico en Internet a través de un servidor seguro. Esta habilidad también ha hecho que las VPN sean valiosas para desbloquear contenidos limitados, explorar la web de manera anónima, realizar torrents de manera segura, entre otros.

Según (Roo, 2004) dice que en un entorno digital donde la protección de la información y la privacidad son esenciales, las redes privadas virtuales (VPN) surgen como una respuesta vital para abordar retos relacionados con la seguridad de las comunicaciones en línea. Las VPN facilitan la transferencia segura de datos a través de redes públicas, generando la impresión de una conexión privada y segura entre aparatos. Frente a las múltiples alternativas comerciales de VPN existentes, las soluciones de software libre se destacan por su claridad y versatilidad, facilitando la revisión de implementaciones, la adaptación del software y, en consecuencia, asegurando una administración de la seguridad fundamentada en la confianza y la adaptabilidad.

En el artículo de (Hickey & Arcuri, 2020) El capítulo titulado "Redes Privadas Virtuales", perteneciente al libro Manos en el hackeo: Conviértete en un experto en las próximas pruebas de penetración y el equipo púrpura, explora el uso de las VPN en el ámbito de la ciberseguridad y las pruebas de penetración.

Este capítulo ofrece una introducción detallada sobre el funcionamiento de las VPN y su papel en la protección de las comunicaciones en línea. Explica cómo estas tecnologías contribuyen a ocultar la identidad del usuario en la web y a garantizar conexiones seguras entre dispositivos y redes corporativas. Asimismo, analiza las vulnerabilidades que los atacantes pueden explotar en implementaciones de VPN durante pruebas de penetración.

Dado que forma parte de un libro sobre hacking ético y pruebas de seguridad, el capítulo probablemente profundiza en las técnicas de análisis y evaluación de la seguridad en redes privadas virtuales. También aborda estrategias y herramientas clave que los profesionales en ciberseguridad pueden emplear para proteger sus redes de manera efectiva.

Este recurso es valioso para comprender la gestión y fortalecimiento de las VPN en entornos de seguridad informática, así como para desarrollar estrategias de defensa ante posibles ataques.

El artículo titulado "Análisis de rendimiento de los puntos finales VPN virtualizados" (Lackovic & Tomi., 2017), presentado en el 40º Convenio Internacional de Tecnologías de la Información y la Comunicación, Electrónica y Microelectrónica (MIPRO) en 2017, se centra en evaluar el rendimiento de los puntos finales de las VPN (Redes Privadas Virtuales) cuando son virtualizados.

En este estudio, los autores realizan un análisis exhaustivo de cómo la virtualización de los puntos finales de VPN afecta el rendimiento de las conexiones. La virtualización puede introducir una serie de variables que influyen en la eficiencia de las VPN, como la carga de procesamiento adicional y los posibles cuellos de botella en la red, que pueden afectar la velocidad de conexión, la latencia y la estabilidad.

El artículo analiza el impacto de la virtualización en el rendimiento de las VPN, explorando diferentes configuraciones y metodologías para evaluar cómo los puntos finales virtualizados gestionan el tráfico de datos. Destaca tanto los beneficios como los desafíos de implementar esta tecnología en entornos corporativos, así como las oportunidades de optimización para mejorar la eficiencia y seguridad de las comunicaciones. Además, proporciona información clave sobre la gestión y optimización de infraestructuras virtualizadas en el contexto de la ciberseguridad y la administración de redes.

El artículo titulado "Evaluación del Desempeño y Análisis de OpenVPN en Android" (Qu, Li, & Dang, 2012), presentado en la Cuarta Conferencia Internacional de Ciencias Computacionales y de la Información en 2012, se enfoca en analizar y evaluar el rendimiento de OpenVPN cuando se utiliza en dispositivos Android.

En el estudio, los autores realizan pruebas de rendimiento para determinar cómo

OpenVPN, una de las soluciones de VPN más populares, se comporta en el sistema operativo Android en términos de velocidad, eficiencia y estabilidad. El análisis se centra en los aspectos clave de la conexión, como la latencia, la velocidad de transferencia de datos y el uso de recursos del dispositivo, específicamente en móviles, donde las limitaciones de hardware y la variabilidad de las redes pueden tener un impacto significativo.

El artículo también aborda posibles desafíos en la implementación de OpenVPN en dispositivos móviles, como las restricciones de la red móvil, el consumo de batería y la necesidad de optimización del rendimiento para asegurar una experiencia de usuario adecuada. A lo largo del estudio, los autores proponen recomendaciones sobre cómo mejorar el desempeño de OpenVPN en Android y cómo los desarrolladores pueden optimizar la configuración de las VPN para que se adapten mejor a las necesidades de los usuarios móviles.

El artículo proporciona una evaluación crítica del rendimiento de OpenVPN en dispositivos Android y ofrece recomendaciones clave para mejorar su implementación y eficiencia en un entorno móvil.

Las VPN crean un túnel seguro para la transmisión de datos mediante cifrado y autenticación. Las empresas utilizan VPN para ofrecer a sus empleados un acceso remoto seguro a las redes corporativas, incluso cuando están fuera de la oficina. A través de una VPN, los dispositivos remotos, como laptops, pueden operar como si estuvieran conectados a la red local. Muchos dispositivos de enrutamiento VPN permiten manejar múltiples túneles simultáneamente, lo que garantiza que todos los empleados puedan acceder a la información de la empresa sin importar su ubicación, brindando un nivel de seguridad superior a otras opciones de comunicación remota, asegurando que las redes privadas estén protegidas de usuarios no autorizados y manteniendo privadas las ubicaciones geográficas y otros datos sensibles de los usuarios.

El proceso de una VPN incluye cifrar los datos en el dispositivo del usuario, enviarlos a través de un túnel seguro a un servidor VPN, y luego descifrar la información y devolverla al usuario, todo sin revelar su identidad o ubicación, siendo una opción económica, eficiente y segura para conectar usuarios remotos a redes corporativas, especialmente cuando se utilizan a través de la red pública de Internet.

OpenVPN, una solución VPN basada en SSL/TLS, ofrece un alto nivel de seguridad y flexibilidad. Utiliza certificados SSL/TLS para autenticar a los usuarios y gestionar el intercambio de claves de cifrado, proporcionando un sistema de autenticación bidireccional y garantizando una comunicación segura. Este estudio destaca la creciente importancia de las VPN Open Source, que han ganado popularidad debido a su accesibilidad, transparencia y capacidad de adaptación, aunque la efectividad de estas herramientas en ciberseguridad aún requiere un análisis más profundo.

2.2. Marco Teórico

2.2.1. Seguridad de la información

La protección de la información es un pilar esencial en la actualidad digital, ya que previene el acceso no autorizado, la modificación, divulgación o eliminación de los datos. Dado el acelerado avance tecnológico, las empresas y organizaciones deben adoptar estrategias sólidas que garanticen la confidencialidad, integridad y disponibilidad de la información. Para ello, es fundamental implementar políticas de seguridad, mecanismos de control de acceso, cifrado, auditorías y planes de respuesta ante posibles incidentes. Asimismo, la formación y sensibilización de los usuarios resulta crucial para minimizar riesgos, puesto que muchas vulneraciones de seguridad derivan de fallos humanos.

Según (Stallings W. &., 2018), la criptografía es una herramienta esencial para la seguridad de los datos, proporcionando mecanismos que aseguran la autenticidad y privacidad de la información transmitida en redes.

Asimismo, (Tipton, 2007) destacan la importancia de un enfoque integral en la gestión de la seguridad de la información, abarcando aspectos técnicos, administrativos y legales. En el contexto actual, la ciberseguridad es un desafío creciente, impulsado por el aumento de ciberataques y amenazas sofisticadas que ponen en riesgo tanto a empresas como a individuos. Es por ello que las normativas internacionales, como el estándar ISO/IEC 27001, ofrecen un marco de referencia para establecer y mantener sistemas de gestión de seguridad de la información efectivos. La constante evolución del panorama tecnológico obliga a las organizaciones a actualizar sus estrategias y adoptar nuevas tecnologías para proteger sus activos digitales.

Objetivos de la seguridad de la información

Los propósitos de la seguridad de la información se enfocan en proteger los datos a través de tres pilares esenciales: confidencialidad, integridad y disponibilidad.

La confidencialidad garantiza que solo las personas autorizadas puedan acceder a la información, evitando exposiciones no deseadas o accesos no permitidos.

La integridad se encarga de mantener la exactitud y confiabilidad de los datos, previniendo modificaciones no autorizadas.

Por otro lado, la disponibilidad asegura que la información y los sistemas estén accesibles para los usuarios legítimos en el momento que los necesiten, reduciendo posibles interrupciones o fallos. Para alcanzar estos objetivos, las organizaciones implementan diversas estrategias de seguridad, tales como mecanismos de control de acceso, encriptación, respaldos de datos, monitoreo continuo de redes y planes de recuperación ante incidentes, en la figura 2 se resumen los objetivos de la seguridad de la Información.

Figura 2 Objetivos de la Seguridad de la Información (Ley de Protección de datos 2020)

De acuerdo con (Whitman, 2022), una estrategia eficaz de seguridad debe considerar estos principios básicos y aplicarlos en un marco de gestión integral para prevenir incidentes y responder de manera adecuada a posibles amenazas.

Además, (Stallings, W., 2018) señala que la evolución de los riesgos en el ámbito digital exige una actualización constante de las políticas y herramientas de seguridad, ya que las amenazas cibernéticas son cada vez más sofisticadas. En este sentido, normativas como la ISO/IEC 27001 proporcionan un marco estructurado para la gestión de la seguridad de la información, permitiendo a las organizaciones establecer controles adecuados y mejorar continuamente sus sistemas de protección. La implementación de estos objetivos no solo protege los activos digitales, sino que también fortalece la confianza de los clientes y socios comerciales, quienes dependen de la seguridad de la información para la continuidad de sus operaciones.

Importancia de la seguridad de la información

De acuerdo con Arévalo et al. (2020) la salvaguarda de la información se ha convertido en un elemento esencial para el funcionamiento de las organizaciones hoy en día, ya que todas

ellas manejan datos para llevar a cabo su actividad y necesitan garantizar su protección e integridad de acuerdo con las regulaciones Los sistemas de seguridad informática deben tener la habilidad de manejar el riesgo presente y suprimirlo con la mínima repercusión para la organización. Esto significa que deben asegurar la resistencia de la organización y sus sistemas de seguridad, con el fin de prevenir, prevenir y resolver cualquier peligro o ataque que se origine en el manejo de la información y la información.

Según (Guaña-Moya, 2023), las organizaciones necesitan disponer de soluciones tecnológicas apropiadas que no solo garanticen la protección, sino que también permitan la comunicación constante de su estado y que ofrezcan los recursos necesarios para asegurar la continuidad de las organizaciones y su actividad en caso de que se enfrenten a un ataque

2.2.2 Amenaza

En el estudio de (de la Rosa Rodríguez, 2020) En ciberseguridad, la situación propensa a que un sistema vulnerable sea objeto de un ciberataque es lo que se conoce como amenaza. Un sistema de computación se enfrenta a este tipo de amenaza en tres formas: ataques digitales de origen externo como el malware; violación de las estrategias de autoprotección digital; o situaciones de contingencia como un incendio o robo. Las amenazas cibernéticas más significativas incluyen: el malware y particularmente el ransomware, el phishing o suplantación de identidad, la ingeniería social, la amenaza persistente sofisticada, los ataques de denegación de servicio (DoS), las redes sociales, los botnets, la contratación de servicios en la nube y la negligencia de los usuarios.

2.2.3 Vulnerabilidad

Tal como lo expresan Guevara et al. (2023) una vulnerabilidad se refiere a una debilidad o fragilidad en un sistema, cuyos datos se encuentran vulnerables a ataques informáticos que afectan su integridad, disponibilidad o privacidad. Otros términos son fisura, fisura o fisura de seguridad. Se pueden presentar por múltiples motivos: imperfecciones en el diseño,

configuración inadecuada, ausencia de procedimientos, fallos en la programación, negligencias en las actualizaciones

Por su parte Marcillo et al. (2020) expresan que después de su identificación y localización, desactivarlas resulta relativamente fácil. La ciberseguridad establece la magnitud y severidad de las vulnerabilidades de un sistema, con el objetivo de llevar a cabo las intervenciones requeridas en el menor tiempo posible. Estas fisuras digitales sitúan a los equipos o unidades de computación de una compañía o persona ante múltiples riesgos, incrementando la severidad de un ciberataque

2.2.4 Riesgo

Según (Mora Navarro, 2022), un riesgo se refiere al margen de posibilidad de que una unidad o estructura de computación sufra un ataque digital, es decir, que una amenaza cibernética se convierta en realidad. Para determinar el nivel de riesgo de un sistema, se identifica la existencia de una vulnerabilidad en él. Por lo tanto, el riesgo es la posibilidad de que la amenaza se realice, parasitando una vulnerabilidad no identificada o no solucionada

Para (Bailón-Lourido, 2019), la estrategia de ciberseguridad de una compañía se basa en reducir al mínimo el peligro de su infraestructura física o tecnológica. Para ello, una vez identificadas las vulnerabilidades, deben ser neutralizadas para prevenir que las amenazas próximas puedan convertirse en efectivas

2.2.5 Virus

Según Cando-Segovia y Medina-Chicaiza (2021), los virus de computación son programas malintencionados creados para modificar el funcionamiento habitual de los sistemas de computación sin la aprobación del usuario. Su meta principal es extenderse a otros dispositivos y, en numerosas situaciones, provocar daños que oscilan entre la pérdida de información hasta la desactivación total del sistema. Estos programas tienen la capacidad de replicarse y propagarse por medios variados, tales como archivos adjuntos en emails, descargas

de la web o dispositivos de almacenamiento extraíbles

Existen distintos tipos de virus informáticos, como lo muestra la figura 3, cada uno con particularidades y objetivos específicos. Uno de los más frecuentes es el **virus de archivo**, el cual se esconde en programas ejecutables y se activa cuando el usuario los abre. También se encuentran los **virus de macro**, que afectan documentos de aplicaciones como Microsoft Word o Excel, utilizando las macros para ejecutar código malicioso. Otro tipo es el **virus de sector de arranque**, que infecta la parte del disco duro o dispositivos extraíbles encargados de iniciar el sistema operativo, impidiendo que el equipo arranque de manera adecuada. Los **virus polimórficos** representan una gran amenaza, ya que alteran su código con cada replicación, lo que dificulta su detección por los antivirus convencionales. Asimismo, existen los **virus residentes**, que permanecen en la memoria RAM y pueden ejecutarse de manera continua sin depender de un archivo específico, lo que complica su eliminación. Finalmente, están los **virus de enlace o directivos**, los cuales modifican las rutas de acceso a los archivos para redirigir la ejecución hacia su código malicioso.

Figura 3: tipos de Virus (Autoría Propia)

Historia de los Virus Informáticos

Según (Han, 2021), "Creeper" fue el primer virus informático identificado, creado en 1971 por Robert Thomas Morris. Este software infectaba ordenadores PDP-11 vinculados a ARPANET, dando lugar al mensaje: "Soy el más inquietante (creeper); atrápame si es posible". Con el transcurso de las décadas, los virus han avanzado en cuanto a complejidad y magnitud. El virus Brain, originado en Pakistán en 1986, contaminó la primera zona de los disquetes. Posteriormente, en 1988, el gusano de Morris desencadenó una de las primeras epidemias masivas en internet, afectando alrededor del 10% de los ordenadores conectados en ese momento.

Métodos de Propagación

Los virus informáticos pueden propagarse a través de diversos métodos, entre los cuales se encuentran:

Dispositivos de almacenamiento extraíbles: Como unidades USB o discos duros externos, que pueden transportar malware de un equipo a otro.

Correos electrónicos: A través de archivos adjuntos infectados o enlaces maliciosos enviados por ciberdelincuentes.

Descargas en internet: Mediante la obtención de software o documentos desde sitios web no confiables.

Redes compartidas: Aprovechando vulnerabilidades en redes locales o en internet para extenderse a otros dispositivos.

Prevención y Protección

Para protegerse contra los virus informáticos, se recomienda seguir estas medidas:

Instalar un programa antivirus confiable y mantenerlo actualizado para detectar y eliminar posibles amenazas.

Aplicar con frecuencia las actualizaciones de seguridad proporcionadas por los desarrolladores para corregir vulnerabilidades.

Obtener programas y documentos únicamente desde sitios web oficiales o fuentes confiables.

Evitar abrir archivos adjuntos o hacer clic en enlaces de mensajes provenientes de remitentes desconocidos o dudosos.

Respaldar regularmente la información importante para prevenir pérdidas en caso de infección.

2.2.6 Antivirus

Los antivirus son herramientas esenciales en la protección de sistemas informáticos contra amenazas como virus, malware, ransomware y otras formas de software malicioso. Su función principal es detectar, prevenir y eliminar estos programas dañinos antes de que comprometan la integridad de los dispositivos y la información almacenada en ellos. Con el avance de la tecnología, los antivirus han evolucionado para incorporar técnicas más sofisticadas, como la detección basada en comportamiento y el análisis en la nube, permitiendo así una mayor eficacia en la identificación de nuevas amenazas.

Según (Smith, 2020) en su libro "Cybersecurity Essentials: Protecting Your Digital Assets" (2020), los antivirus desempeñan un papel crucial dentro de una estrategia de seguridad integral. El autor destaca que, si bien estas herramientas son fundamentales, no deben considerarse la única línea de defensa, sino que deben complementarse con medidas como firewalls, sistemas de detección de intrusos y prácticas adecuadas de ciberseguridad. De acuerdo con (Schneier, 2020), los antivirus han evolucionado significativamente, pasando de simples escáneres a sistemas de protección en tiempo real que supervisan la actividad del equipo y bloquean posibles ataques antes de que ocurran.

Además, (Vacca, 2019) destaca que el uso de software antivirus debe complementarse con otras estrategias de seguridad, como la actualización periódica del sistema operativo y la implementación de buenas prácticas de navegación. Aunque los antivirus son una primera línea de defensa, no pueden ofrecer una protección absoluta contra todas las amenazas, por lo que es

crucial combinarlos con firewalls, sistemas de detección de intrusos y herramientas de monitoreo de redes. En el entorno digital actual, donde los ataques informáticos son cada vez más sofisticados, contar con una solución antivirus robusta y actualizada es fundamental para mitigar riesgos y proteger los datos personales y empresariales.

Historia de los Antivirus

La historia de los antivirus comenzó en los primeros días de la informática, cuando los sistemas eran más simples y los virus no representaban el peligro global que representan hoy en día. El primer software antivirus, llamado "Brain", fue creado en 1986 por los hermanos Basit y Amjad Farooq Alvi en Pakistán, como respuesta al creciente problema de los virus que se diseminaban a través de discos de intercambio de software. Este virus, que se activaba al ejecutar un programa infectado, marcó el inicio de la necesidad de desarrollar herramientas para proteger los sistemas de estos intrusos. A medida que los virus se volvían más complejos, los antivirus también fueron evolucionando. Durante la década de 1990, compañías como McAfee y Norton crearon programas antivirus más avanzados, que no solo detectaban los virus conocidos, sino que también proporcionaban protección en tiempo real contra amenazas nuevas.

Según (Kaspersky, Kaspersky: The Story of a Revolution in Cybersecurity, 2011) el desarrollo de los antivirus siguió una línea de progreso, pasando de simples bases de datos de firmas a sofisticadas técnicas de detección heurística, que permiten detectar nuevos virus mediante el análisis de su comportamiento. Con el tiempo, los antivirus se convirtieron en una herramienta indispensable para la protección de sistemas en todo el mundo, especialmente a medida que los ciberataques y las amenazas en línea aumentaban. En la actualidad, los antivirus han evolucionado para incluir funciones avanzadas como protección contra ransomware, spyware y otras amenazas cibernéticas, y se han integrado con tecnologías de inteligencia artificial y aprendizaje automático para adaptarse a nuevas formas de ataque. Esta evolución demuestra cómo los antivirus han sido una respuesta constante a la creciente amenaza de los

virus y el malware en el mundo digital.

Funcionamiento de los Antivirus

Los antivirus operan mediante una combinación de técnicas para detectar, prevenir y eliminar software malicioso en los sistemas informáticos. Una de las estrategias más comunes es el **análisis por firmas**, que compara los archivos con una base de datos de virus conocidos, identificando aquellos que coinciden con las características específicas de malware previamente registrado. No obstante, este método no es suficiente para enfrentar amenazas nuevas que aún no han sido identificadas. Por ello, los antivirus también emplean **detección heurística**, un enfoque proactivo que analiza el comportamiento de los archivos mientras se ejecutan, evaluando si podrían ser peligrosos, incluso si no corresponden a una firma conocida. Los antivirus más avanzados incluyen **análisis en tiempo real**, supervisando constantemente las actividades del sistema y notificando al usuario si detectan comportamientos inusuales. Además, algunos programas utilizan **inteligencia artificial** y **aprendizaje automático**, lo que les permite adaptarse a nuevas amenazas y mejorar su capacidad para identificar y bloquear virus desconocidos. También se recurre a la **sandboxing**, un entorno controlado donde se ejecutan archivos sospechosos para observar su comportamiento sin comprometer la seguridad del sistema principal.

Según (Stallings, W., 2020) los antivirus modernos están en constante evolución, incorporando nuevas tecnologías y estrategias para enfrentarse a amenazas cada vez más complejas y sofisticadas, como el ransomware y el spyware. A pesar de estas capacidades avanzadas, los antivirus no son infalibles, por lo que es importante combinarlos con otras medidas de seguridad, como firewalls, copias de seguridad y actualizaciones periódicas del sistema operativo, para proporcionar una protección integral.

Importancia de los Antivirus

Los antivirus son fundamentales debido a su papel esencial en la protección de los

sistemas informáticos y los datos que contienen, frente a una creciente diversidad de amenazas cibernéticas. En un mundo digital cada vez más complejo, donde los ataques de malware se vuelven más sofisticados y frecuentes, los antivirus funcionan como la primera barrera de defensa contra virus, troyanos, ransomware, spyware y otros tipos de software malicioso.

Según (Stallings, W., 2020), los antivirus no solo son esenciales para detectar y eliminar virus conocidos, sino que también juegan un papel importante en la prevención de infecciones mediante tecnologías de monitoreo en tiempo real y análisis de comportamientos sospechosos. Esto es especialmente crítico dado que muchos usuarios no siguen buenas prácticas de seguridad, como mantener sus sistemas actualizados o descargar software solo de fuentes confiables. Además, con el auge de las amenazas dirigidas, como el ransomware, que puede bloquear el acceso a los datos y exigir rescates, los antivirus proporcionan una capa adicional de seguridad al proteger los archivos esenciales. En un contexto en el que los datos son un recurso valioso tanto a nivel personal como empresarial, contar con un programa antivirus actualizado se ha vuelto indispensable para evitar la pérdida de información, el robo de datos o daños irreparables en los sistemas. Asimismo, los antivirus permiten mitigar los riesgos de propagación de infecciones a otros usuarios y dispositivos, asegurando la integridad de las redes y contribuyendo a la seguridad global en el ciberespacio.

De acuerdo con (Kaspersky, Kaspersky: The Story of a Revolution in Cybersecurity, 2019), la adopción de un antivirus robusto es esencial no solo para proteger los equipos personales, sino también para garantizar la seguridad de infraestructuras críticas, empresas y gobiernos frente a ciberamenazas cada vez más avanzadas.

Mejores Prácticas para el Uso de Antivirus

Según (Kaspersky, Kaspersky: The Story of a Revolution in Cybersecurity, 2019), el uso adecuado de los antivirus es esencial para garantizar la protección de los sistemas

informáticos y los datos almacenados. Para comenzar, es importante instalar un antivirus confiable y mantenerlo actualizado regularmente, ya que las actualizaciones contienen nuevas definiciones de virus y mejoras en las capacidades de detección, lo que aumenta su efectividad ante nuevas amenazas.

Además, para (Stallings, W., 2020), se debe realizar un análisis completo del sistema de manera periódica, no solo para detectar malware ya conocido, sino también para identificar posibles infecciones que aún no se han propagado completamente. Los antivirus también deben configurarse para que ofrezcan protección en tiempo real, lo que significa que monitorean continuamente las actividades del sistema en busca de comportamientos sospechosos, bloqueando amenazas antes de que puedan causar daño.

Es crucial que los usuarios no desactiven las funciones de protección del antivirus, incluso si notan que su dispositivo está funcionando más lentamente, ya que esto podría dejar los sistemas expuestos a riesgos. Además, se recomienda habilitar funciones adicionales, como la protección web y de correo electrónico, para evitar que los virus lleguen a través de sitios web infectados o archivos adjuntos en correos electrónicos. Por último, es recomendable hacer copias de seguridad de los archivos importantes, ya que, aunque los antivirus son útiles para prevenir infecciones, no siempre logran eliminar el daño provocado por ciertos tipos de malware, como el ransomware. El uso de un antivirus debe complementarse con otras medidas de seguridad, como evitar descargar software de fuentes no confiables y mantener actualizado tanto el sistema operativo como otras aplicaciones para maximizar la protección.

2.2.7 Software Libre

El software libre se refiere a los programas cuya licencia otorga a los usuarios la posibilidad de usar el software sin restricciones, así como de estudiar, modificar y distribuir su código fuente. Este tipo de software promueve la libertad de los usuarios, a diferencia de los

programas propietarios que limitan el acceso y la alteración del código. El movimiento del software libre nació en la década de 1980, gracias a Richard Stallman, quien creó el Proyecto del Sistema Operativo GNU con el objetivo de desarrollar un sistema operativo completamente libre. El software libre no solo implica la gratuidad del programa, sino también la posibilidad de modificarlo y compartirlo, fomentando así una cultura de colaboración. Algunos ejemplos notables de software libre son el sistema operativo Linux, el servidor web Apache y el navegador Firefox. El software libre es crucial porque promueve la transparencia, la seguridad y la innovación, dado que cualquiera puede contribuir al desarrollo, identificar y corregir errores, y mejorar sus funcionalidades. Además, al ser de código abierto, permite a las empresas y organizaciones adaptar las soluciones a sus necesidades sin depender de un proveedor específico.

De acuerdo con (Raymond, 2001), el modelo de desarrollo abierto del software libre ha demostrado ser una alternativa viable y sostenible frente a los modelos cerrados tradicionales, contribuyendo al avance tecnológico y ofreciendo una mayor seguridad, ya que el código es accesible para ser auditado por la comunidad.

2.2.8 Open Source

El término "Open Source" (código abierto) se refiere a los programas de software cuyo código fuente está disponible para ser modificado, utilizado y distribuido por cualquier persona. A diferencia del software propietario, cuyo código está restringido y no puede ser modificado por los usuarios, el Open Source ofrece una mayor flexibilidad y control sobre el software. Esta filosofía promueve la colaboración abierta, permitiendo que desarrolladores de todo el mundo contribuyan a mejorar un proyecto, lo que, a su vez, impulsa la innovación y la creación de soluciones más robustas y eficaces. El concepto de Open Source se basa en la transparencia y la competencia libre, lo que lo hace una opción atractiva para empresas, organizaciones y desarrolladores individuales. Algunos ejemplos destacados de software Open Source incluyen

el sistema operativo Linux, el servidor web Apache y la base de datos MySQL. A lo largo del tiempo, el movimiento Open Source ha probado ser no solo una alternativa válida al software propietario, sino también una forma de democratizar el acceso a la tecnología, permitiendo a las comunidades personalizar y mejorar las herramientas según sus necesidades.

Según (Feller, 2002), el Open Source ha revolucionado el desarrollo de software, ya que permite una mayor transparencia, colaboración y participación de una comunidad global. Además, este enfoque ha sido esencial para la creación de tecnologías que han transformado el mundo digital, como el desarrollo de Internet y las plataformas de comunicación.

2.2.9 Virtualización

La virtualización es una tecnología fundamental en la informática actual que posibilita la creación de versiones virtuales de recursos físicos como servidores, sistemas operativos, almacenamiento y redes. Gracias a la virtualización, un solo servidor físico puede hospedar múltiples máquinas virtuales (VM), lo que mejora la utilización de los recursos y aumenta la eficiencia operativa. Este método ha transformado la infraestructura tecnológica, permitiendo a las organizaciones reducir los costos de hardware, incrementar la flexibilidad y optimizar la administración de los recursos. Un ejemplo común de virtualización es el uso de hipervisores, programas que gestionan las máquinas virtuales, creando entornos aislados para cada una, lo que permite ejecutar diferentes sistemas operativos en el mismo hardware físico de manera independiente. Además de la virtualización de servidores, también se incluye la virtualización de almacenamiento, que centraliza y hace más eficiente la gestión del almacenamiento físico, así como la virtualización de redes, que permite la creación de redes virtuales dentro de una infraestructura física ya existente.

Según (Garg, 2012), la virtualización ha revolucionado la forma en que las empresas manejan sus recursos informáticos, proporcionando ventajas significativas en términos de ahorro de costos, escalabilidad y recuperación ante desastres. La adopción de esta tecnología se

ha expandido rápidamente en los últimos años, especialmente con el auge de la computación en la nube, donde los recursos virtualizados se gestionan a través de plataformas de nube pública o privada. La virtualización también facilita la implementación de entornos de prueba y desarrollo, proporcionando la capacidad de crear instancias de sistemas operativos para probar aplicaciones sin afectar el entorno de producción.

Para (Moreno, 2021).El término virtualización se refiere a una tecnología que posibilita la implementación de múltiples máquinas virtuales en una máquina física, con la finalidad de optimizar los recursos de un sistema y potenciar su desempeño. Es crucial resaltar que a todas las máquinas virtuales se pueden asignarle recursos (memoria, unidades de almacenamiento, procesados, etc.) que serán extraídos de la máquina física y que estas ejecutarán una copia propia de un sistema operativo (Windows, GNU/Linux, entre otros)

La virtualización permite crear un entorno de computación virtual en el que un solo equipo puede ejecutar diferentes funciones, como servidor web o servidor de archivos, incluso cuando todos los servicios se encuentran en la misma máquina física. Esto facilita la creación de instancias con diferentes sistemas operativos en un único dispositivo, lo que reduce la cantidad de equipos necesarios para ejecutar diversas aplicaciones.

Una de las principales ventajas de la virtualización es que, aunque los programas se ejecutan en un entorno virtual, los usuarios los perciben como si estuvieran funcionando en una computadora exclusiva para ellos. En realidad, estos programas están encapsulados dentro del sistema operativo que gestiona la virtualización. Además, la virtualización permite que varios sistemas operativos se ejecuten simultáneamente sin que interfieran entre sí ni afecten el rendimiento de la máquina física que alberga el entorno virtual.

Existen dos componentes clave en el funcionamiento de la virtualización:

Máquina virtual (VM): Es el núcleo de la virtualización. Se crea completamente mediante software y tiene la capacidad de ejecutar sistemas operativos y aplicaciones, respaldada por los

recursos de un equipo físico.

Hipervisor: Es responsable de crear la capa de virtualización y asignar dinámicamente los recursos necesarios a cada máquina virtual, asegurando que el hardware físico del equipo anfitrión esté disponible para su uso, independientemente del sistema operativo que se ejecute en la máquina virtual.

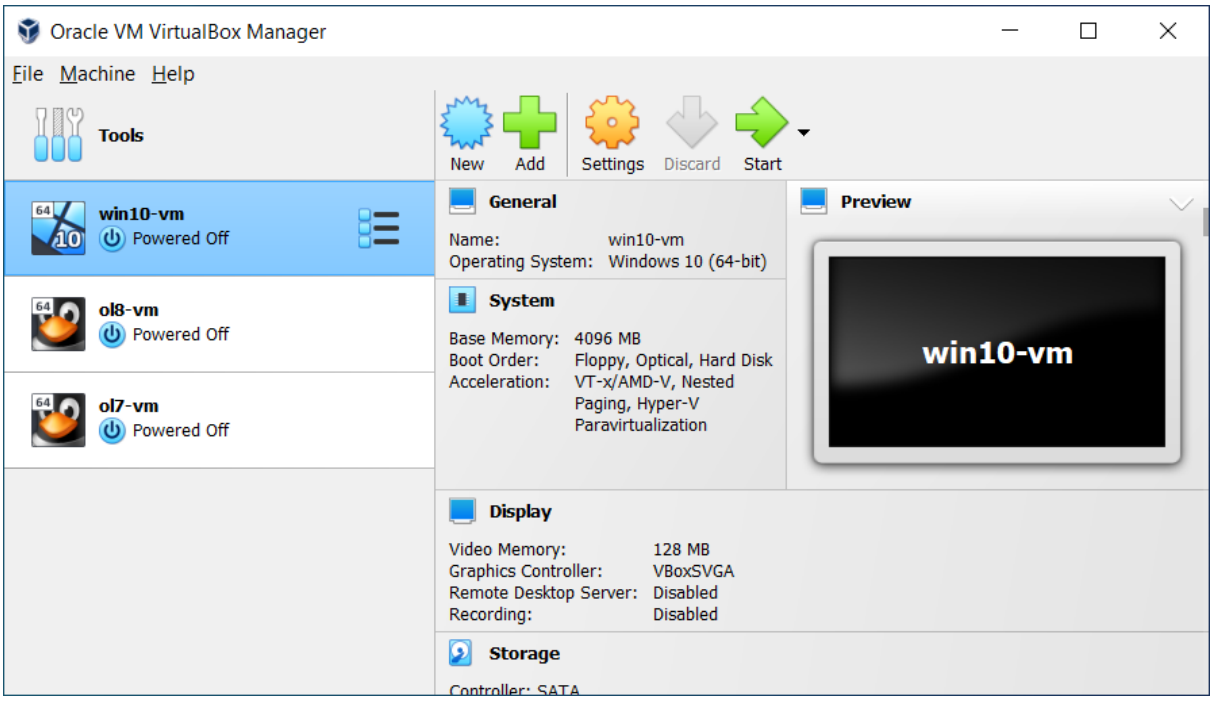
Software de Virtualización

Según (Portnoy, 2012), El software de virtualización es una herramienta clave en la gestión moderna de recursos informáticos, que permite la creación de entornos virtuales dentro de una infraestructura física. A través de este tipo de software, es posible ejecutar varios sistemas operativos en un solo equipo, optimizando al máximo el uso del hardware disponible. Entre los componentes fundamentales del software de virtualización se encuentra el hipervisor, que es responsable de gestionar las máquinas virtuales y asignarles los recursos necesarios de manera eficiente. Existen dos tipos principales de hipervisores: los de tipo 1, que funcionan directamente sobre el hardware físico (bare-metal), y los de tipo 2, que operan sobre un sistema operativo anfitrión. El software de virtualización facilita la creación de entornos aislados para cada máquina virtual, lo que permite que diferentes aplicaciones y sistemas operativos funcionen simultáneamente sin interferir entre sí. Esta capacidad es esencial para entornos de desarrollo y pruebas, ya que permite replicar diversas configuraciones sin necesidad de hardware adicional. Además, la virtualización proporciona una mayor flexibilidad en la gestión de recursos, ya que se pueden realizar tareas como la migración de máquinas virtuales entre servidores, la asignación dinámica de recursos y la creación de clones para la recuperación ante desastres. El software de virtualización ha sido un motor fundamental en la evolución de la infraestructura tecnológica empresarial, ofreciendo ventajas significativas en términos de eficiencia, ahorro de costos, y escalabilidad, al reducir la necesidad de equipos físicos y mejorar la utilización de los recursos existentes.

VirtualBox

Según (Hows, 2015), VirtualBox es una plataforma de virtualización de código abierto y gratuita, desarrollada por Oracle, que permite a los usuarios crear y gestionar máquinas virtuales en sus sistemas. Esta herramienta ofrece una interfaz sencilla y potente, que permite la ejecución simultánea de múltiples sistemas operativos sobre un solo equipo físico, lo que optimiza el uso de los recursos del sistema. VirtualBox es compatible con una amplia variedad de sistemas operativos anfitriones, incluyendo Windows, macOS, Linux y Solaris, y puede ejecutar máquinas virtuales con sistemas operativos invitados como Windows, Linux, BSD y otros. Uno de los puntos más destacados de VirtualBox es su capacidad para integrar características avanzadas, como la asignación dinámica de memoria, la virtualización anidada, el soporte para redes internas y la creación de instantáneas, lo que permite a los usuarios guardar el estado de una máquina virtual en un punto específico y restaurarla más tarde. Además, VirtualBox facilita la integración entre el sistema operativo anfitrión y los invitados mediante herramientas de adición de invitados, lo que permite compartir carpetas, portapapeles y otras funcionalidades. Gracias a su facilidad de uso, flexibilidad y soporte para diversas plataformas, VirtualBox es una opción popular tanto para desarrolladores, administradores de sistemas como para entusiastas de la tecnología que necesitan ejecutar varios entornos operativos sin depender de hardware adicional. Su código abierto fomenta la colaboración y la mejora constante por parte de la comunidad de usuarios, lo que le ha permitido mantenerse como una de las soluciones de virtualización más accesibles y eficientes disponibles, en la figura 4 se muestra el entorno de inicio a la aplicación

Figura 4. VirtualBox tomado de *(oracle, 2022)*

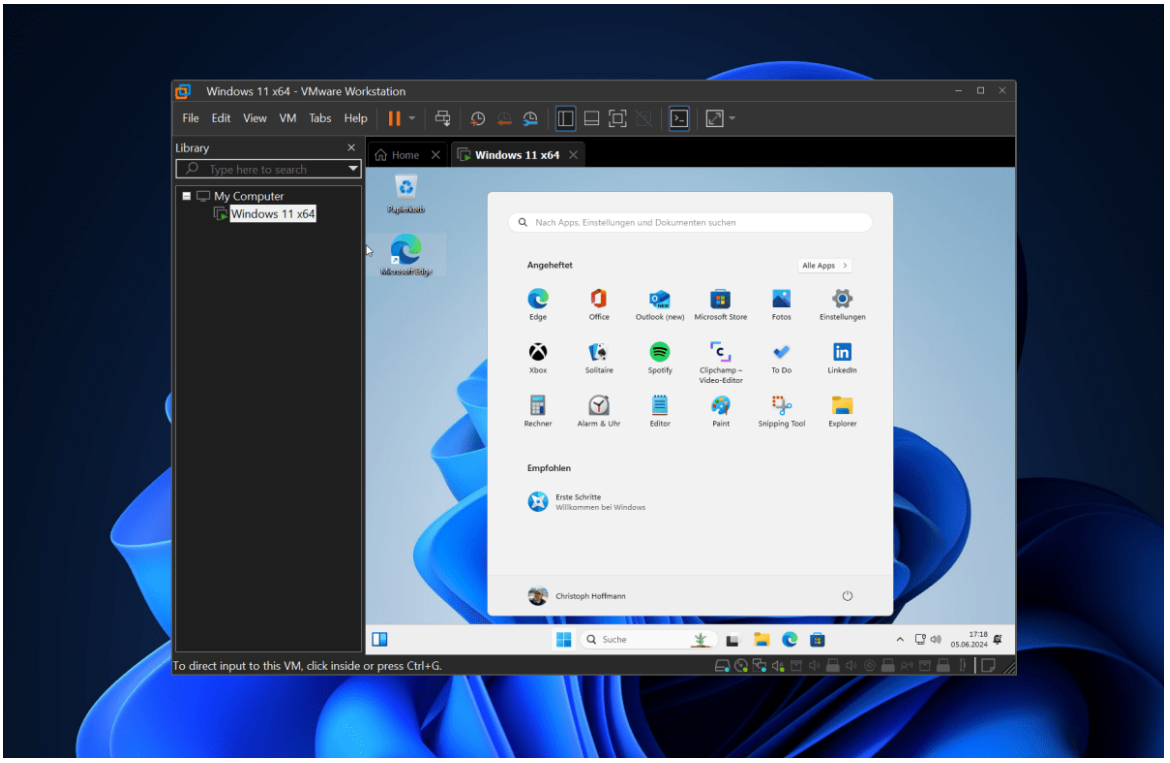


VMWARE

Para (Frank Denneman, 2018), VMware es una de las soluciones de virtualización más utilizadas en el ámbito empresarial, ofreciendo una amplia gama de herramientas para la creación, gestión y optimización de máquinas virtuales. Fundada en 1998, la compañía VMware ha sido pionera en la virtualización de servidores, permitiendo que empresas de todo el mundo maximicen la eficiencia de su infraestructura de TI. A través de su plataforma insignia, VMware vSphere, las organizaciones pueden crear centros de datos virtualizados donde los servidores físicos se convierten en recursos virtuales gestionables. VMware no solo facilita la consolidación de servidores, sino que también proporciona características avanzadas como la alta disponibilidad, el balanceo de carga, la migración en vivo de máquinas virtuales y la protección contra desastres. Además, su software está diseñado para trabajar con sistemas operativos de servidores y escritorios, permitiendo ejecutar aplicaciones críticas sin necesidad de grandes cantidades de hardware. La flexibilidad de VMware también se extiende a su capacidad para integrar diversas plataformas, incluidos entornos en la nube híbrida y pública. VMware ha cambiado el panorama de la infraestructura tecnológica empresarial, ofreciendo

soluciones que no solo optimizan el uso de los recursos, sino que también mejoran la agilidad, escalabilidad y disponibilidad de los sistemas informáticos. Debido a su enfoque en la eficiencia, la fiabilidad y la seguridad, VMware sigue siendo la opción preferida para muchas empresas que buscan una infraestructura de TI moderna y dinámica, en la figura5 se ve el inicio de WMware.

Figura 5. VMWARE tomado de (pcworld, 2021)



Comparación de VirtualBox y VMware

Según (Chris Wolf, 2005), presenta una tabla comparativa entre VirtualBox y VMware, que resalta las principales diferencias entre ambos productos:

Tabla 1. Comparación entre VirtualBox y Vmware

Característica	**VirtualBox**	**VMware**
Licencia	Código abierto (gratuito)	Propietario, con versiones de pago (vSphere, Workstation)

Plataformas soportadas	Windows, Linux, macOS, Solaris	Windows, Linux, macOS (dependiendo del producto)
Máquinas virtuales soportadas	Virtualiza tanto servidores como escritorios	Virtualiza tanto servidores como escritorios, con soluciones específicas para cada tipo
Facilidad de uso	Fácil de instalar y configurar, orientado a usuarios no expertos	Requiere conocimientos avanzados, especialmente en versiones empresariales
Funciones avanzadas	Soporte para instantáneas, integración con el sistema anfitrión	Migración en vivo, alta disponibilidad, balanceo de carga
Soporte para redes	Redes internas, adaptadores puenteados, NAT	Redes definidas por software, configuraciones de red avanzadas
Rendimiento	Menor rendimiento comparado con VMware en entornos empresariales	Mejor rendimiento, especialmente en entornos empresariales
Coste	Gratuito	Paga por versiones avanzadas como VMware vSphere
Popularidad	Popular entre usuarios y desarrolladores individuales	Usado principalmente por grandes empresas y centros de datos
Soporte y comunidad	Amplia comunidad y soporte activo en foros online	Soporte premium con documentación detallada y asistencia dedicada

Fuente: (Virtualization: A Manager's Guide, 2005)

2.2.10 VPN

De acuerdo con (Stallings W. , Cryptography and Network Security: Principles and Practice (7th ed.), 2017), Las Redes Privadas Virtuales (VPN) son una tecnología crucial para la protección de la privacidad y seguridad en entornos digitales. Al crear un túnel cifrado entre el usuario y un servidor remoto, una VPN garantiza que los datos transmitidos estén protegidos contra interceptaciones y accesos no autorizados, incluso cuando se utilizan redes públicas o no confiables. Esto es especialmente importante en contextos empresariales y personales, donde el acceso remoto a sistemas corporativos o la navegación segura por internet son necesidades fundamentales. Las VPN permiten a los usuarios eludir restricciones geográficas, acceder a contenido bloqueado o censurado, y proteger su identidad en línea mediante el enmascaramiento de su dirección IP. Además, existen diferentes tipos de VPN, como las de acceso remoto y las de sitio a sitio, que se utilizan según el propósito y la estructura de la red. Los protocolos que soportan las VPN, como IPsec, OpenVPN, y L2TP, garantizan que los datos sean cifrados y asegurados adecuadamente durante la transmisión. Sin embargo, también presentan ciertos retos, como la posible reducción en el rendimiento debido al cifrado o las vulnerabilidades asociadas con la mala implementación de algunos protocolos. Las VPN son una herramienta indispensable en la era digital actual, donde la seguridad de la información y la privacidad en línea son más importantes que nunca.

La historia de las VPN

Según (Kaufman, 2011), La historia de las Redes Privadas Virtuales (VPN) se remonta a la década de 1990, cuando las empresas comenzaron a buscar métodos más seguros para conectar sus redes internas a través de Internet sin comprometer la integridad de sus datos. Uno de los primeros desarrollos significativos en este campo fue el protocolo PPTP (Point-to-Point Tunneling Protocol), introducido por Microsoft en 1996, que permitía a los usuarios establecer conexiones seguras a través de redes públicas. Con el tiempo, la creciente necesidad de mayor

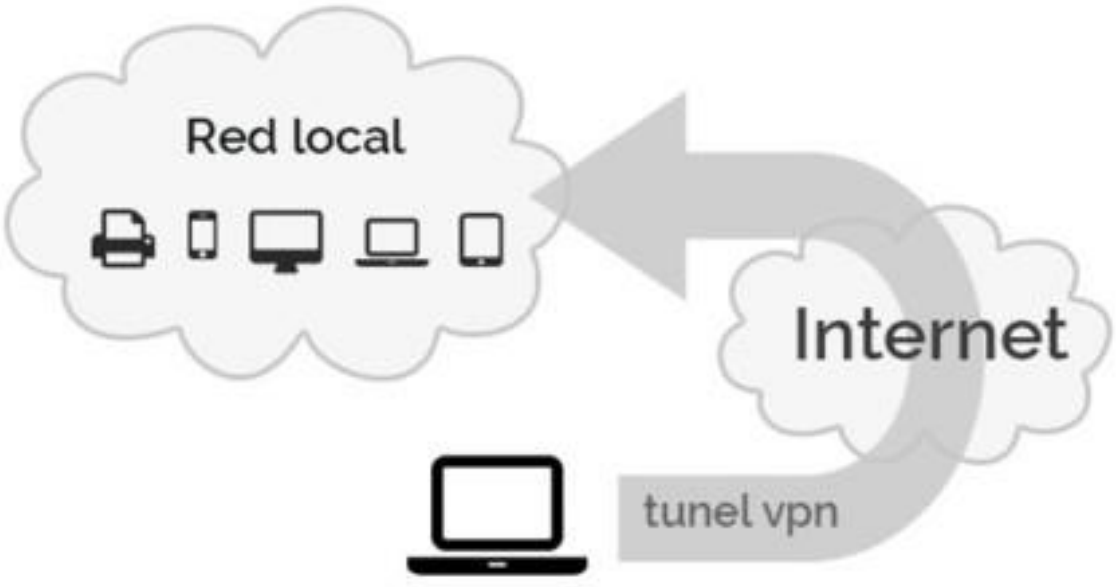
seguridad impulsó el desarrollo de nuevos protocolos, como IPSec (Internet Protocol Security) y SSL/TLS (Secure Sockets Layer/Transport Layer Security), los cuales mejoraron el cifrado y la autenticación en las conexiones VPN. A medida que Internet se expandía y las amenazas cibernéticas aumentaban, las VPN evolucionaron de ser una herramienta utilizada exclusivamente por empresas a convertirse en una solución popular para usuarios individuales que deseaban proteger su privacidad y eludir restricciones geográficas. En la actualidad, las VPN han alcanzado un nivel de sofisticación que permite no solo la protección de datos mediante cifrado avanzado, sino también una optimización en el rendimiento de las conexiones, con la introducción de protocolos modernos como WireGuard y OpenVPN. Su uso se ha diversificado ampliamente, desde la protección de información corporativa hasta la lucha contra la censura en países con restricciones en el acceso a la web. Gracias a estos avances, las VPN continúan desempeñando un papel crucial en la seguridad informática y la privacidad en línea.

¿Cómo funciona una VPN?

A criterio de (Hacking, 2019), Las Redes Privadas Virtuales (VPN) funcionan creando un túnel seguro y cifrado entre el dispositivo del usuario y un servidor remoto, lo que garantiza que los datos que se transmiten a través de una red pública (como Internet) estén protegidos de accesos no autorizados. Al conectarse a una VPN, el dispositivo del usuario se autentica con el servidor mediante credenciales seguras y establece una conexión cifrada utilizando diversos protocolos de seguridad, como IPsec (Internet Protocol Security), L2TP (Layer 2 Tunneling Protocol), o OpenVPN. Una vez que se establece este túnel, los datos que se envían entre el usuario y el servidor son cifrados, lo que dificulta su interceptación o manipulación. Además, la VPN oculta la dirección IP del usuario, lo que hace que su tráfico de internet parezca provenir del servidor al que está conectado, en lugar de su ubicación física, protegiendo su identidad y ofreciendo un nivel adicional de privacidad. Las VPN pueden ser configuradas para acceder a contenido restringido geográficamente o permitir el acceso remoto a redes privadas, lo que es

esencial tanto en entornos empresariales como para usuarios individuales que desean mantener su privacidad mientras navegan por la web. A pesar de sus beneficios, el uso de una VPN puede introducir una leve disminución en la velocidad de la conexión debido al proceso de cifrado, aunque esto depende del protocolo utilizado y de la infraestructura de la VPN, en la figura 6 se ilustra el funcionamiento de una VPN.

Figura 6. VPN tomado de *(xataka, 2025)*



¿Cuáles son los beneficios de una conexión VPN?

Para (Reinders, 2020), Una conexión VPN ofrece múltiples beneficios, convirtiéndola en una herramienta esencial para quienes buscan mejorar la seguridad y privacidad en línea. En primer lugar, una de las ventajas más destacadas es la protección de la información personal. Al cifrar todo el tráfico de datos, una VPN impide que los hackers, especialmente en redes Wi-Fi públicas, puedan interceptar comunicaciones sensibles, como contraseñas o información bancaria. Además, al ocultar la dirección IP del usuario, una VPN refuerza la privacidad, lo que dificulta que terceros, como proveedores de servicios de Internet o anunciantes, puedan rastrear la actividad en línea del usuario. Otra ventaja clave es el acceso a contenido restringido

geográficamente. Las VPN permiten conectarse a servidores ubicados en diferentes países, lo que hace posible el acceso a servicios de streaming, sitios web o aplicaciones que podrían estar bloqueados en ciertas regiones. En un contexto empresarial, las VPN permiten a los empleados acceder de manera segura a redes corporativas desde cualquier ubicación, lo que es especialmente útil en el entorno de trabajo remoto. Además, las VPN son herramientas efectivas para evitar la censura en línea, permitiendo a los usuarios eludir restricciones impuestas por gobiernos o proveedores de servicios de internet. Aunque el uso de una VPN puede reducir ligeramente la velocidad de conexión debido al cifrado y al recorrido más largo de los datos, los beneficios de seguridad, privacidad y acceso remoto siguen siendo razones clave para su adopción.

Tipos de VPN

En su libro (Lowe, 2016),dice Las Redes Privadas Virtuales (VPN) han evolucionado para adaptarse a distintos entornos y necesidades, ofreciendo soluciones seguras y eficientes para la conectividad en el mundo digital. Existen diversos tipos de VPN, cada una diseñada para cumplir funciones específicas en el ámbito empresarial, gubernamental y personal. Uno de los tipos más utilizados es la VPN de acceso remoto, que permite a los usuarios conectarse a una red privada desde cualquier ubicación con acceso a Internet. Este tipo de VPN es especialmente útil para empleados de empresas que trabajan de forma remota, ya que les proporciona un canal de comunicación seguro con la red corporativa, evitando el acceso de terceros no autorizados. Para garantizar la seguridad, este tipo de VPN emplea protocolos de cifrado como PPTP (Point-to-Point Tunneling Protocol), L2TP/IPSec (Layer 2 Tunneling Protocol con IP Security) y OpenVPN, que protegen la información transmitida contra posibles ataques o interceptaciones.

Otro tipo de VPN ampliamente utilizado es la VPN de sitio a sitio, que permite interconectar redes completas de diferentes ubicaciones, como sucursales de una empresa o entidades gubernamentales, garantizando una comunicación segura y eficiente sin la necesidad

de establecer múltiples conexiones individuales. Dentro de esta categoría, se encuentran las VPN de intranet, que conectan distintas oficinas de la misma organización, y las VPN de extranet, diseñadas para conectar la red interna de una empresa con la de sus socios comerciales o proveedores, facilitando el intercambio seguro de información sin comprometer la seguridad de los datos.

En los últimos años, con el auge de la computación en la nube, han surgido las VPN basadas en la nube, que permiten a las empresas acceder a recursos virtualizados con mayor flexibilidad y seguridad. Estas VPN son administradas por proveedores de servicios en la nube y garantizan conexiones seguras para los empleados y sistemas que operan en infraestructuras descentralizadas. Su principal ventaja es que eliminan la necesidad de mantener hardware adicional, ya que toda la infraestructura de la VPN se gestiona en la nube.

Por otro lado, las VPN móviles están diseñadas para dispositivos en constante movimiento, como teléfonos inteligentes y tabletas, proporcionando conexiones seguras incluso cuando el usuario cambia de red. Estas VPN son esenciales para profesionales que necesitan acceder a datos sensibles mientras viajan o se conectan a redes públicas, como las de aeropuertos y cafeterías. A diferencia de las VPN tradicionales, que requieren una conexión estable, las VPN móviles pueden mantener la sesión activa incluso si el usuario cambia de red o experimenta interrupciones en la conectividad.

Finalmente, existen las VPN empresariales, que combinan varias de las características anteriores para ofrecer soluciones personalizadas de seguridad y conectividad a grandes organizaciones. Estas VPN suelen contar con niveles avanzados de cifrado, autenticación multifactor y herramientas de monitoreo en tiempo real para detectar posibles amenazas. Las empresas pueden optar por implementar VPN internas, donde los servidores y la infraestructura son administrados directamente por el departamento de TI, o bien utilizar servicios de terceros especializados en VPN para gestionar la seguridad de sus conexiones.

Cada clase de VPN presenta sus propios beneficios y dificultades, por lo que seleccionar la opción más adecuada dependerá de los requerimientos particulares de cada usuario o empresa. Con el continuo avance del entorno digital, la demanda de VPN seguirá en expansión, motivada por la creciente importancia de salvaguardar la privacidad, asegurar la integridad de la información en tránsito y proporcionar un acceso remoto confiable a los recursos tecnológicos.

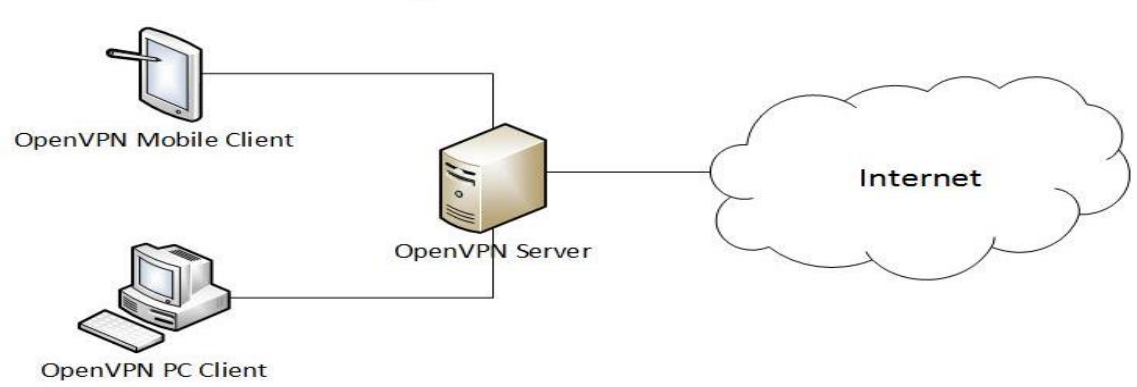
Las redes privadas virtuales (VPN) son una herramienta fundamental para garantizar la privacidad y seguridad en el entorno digital. Sin embargo, su efectividad en la protección de los datos varía según varios factores, como el protocolo que emplean, el tipo de cifrado implementado y la política de registro de información de cada proveedor. Una VPN correctamente configurada y que utilice protocolos robustos como OpenVPN, WireGuard o IPsec puede proporcionar una seguridad elevada, ya que cifra el tráfico y oculta la dirección IP del usuario. No obstante, no todas las VPN ofrecen el mismo nivel de protección. Algunas opciones gratuitas pueden registrar la actividad en línea de los usuarios y comercializar esos datos con terceros, lo que supone un riesgo para la privacidad. Asimismo, si una VPN emplea cifrados obsoletos o débiles, los datos pueden quedar expuestos a ataques cibernéticos, como la interceptación de información por parte de piratas informáticos o entidades gubernamentales. También hay amenazas adicionales, como las fugas de DNS, que pueden revelar detalles sobre la navegación del usuario, o los ataques de intermediario (MITM), que pueden comprometer la seguridad si la conexión no está adecuadamente protegida. Además, las VPN no ofrecen defensa total contra amenazas como malware o ataques de phishing, por lo que es recomendable utilizarlas en conjunto con otras estrategias de seguridad, como un software antivirus confiable y la autenticación en dos pasos. En definitiva, la protección que brinda una VPN depende en gran medida de su implementación y del proveedor que la administra, por lo que resulta esencial optar por un servicio de confianza, con políticas estrictas de no registro y cifrado de última generación.

2.2.11 OpenVPN

Dice (Kurose, 2020), que OpenVPN es una de las soluciones más populares y confiables en el ámbito de las redes privadas virtuales (VPN). Se trata de un protocolo y software de código abierto que permite establecer conexiones seguras a través de Internet utilizando tecnologías de cifrado avanzadas. Su flexibilidad y compatibilidad con múltiples plataformas lo han convertido en una opción preferida tanto para usuarios individuales como para empresas que buscan garantizar la seguridad y privacidad en sus comunicaciones en línea. Una de las principales ventajas de OpenVPN es su capacidad para atravesar cortafuegos y adaptarse a diferentes configuraciones de red, lo que lo hace ideal para entornos donde otras soluciones VPN podrían no funcionar correctamente. A diferencia de otros protocolos propietarios, OpenVPN permite a los usuarios revisar su código fuente y adaptarlo a sus necesidades, asegurando transparencia y confiabilidad en la protección de los datos.

Según (Álvarez, 2010), OpenVPN es un programa de código abierto destinado a la implementación de redes privadas virtuales (VPN). Facilita la formación de vínculos seguros y encriptados a través de redes públicas o privadas, asegurando la privacidad e integridad de la información enviada. James Yonan lo desarrolló en 2001 y se utiliza extensamente en contextos corporativos y personales gracias a su versatilidad, protección y compatibilidad con diversas plataformas, en la figura7 muestro el esquema de openVPN.

Figura 7.*Esquema de openVPN tomado de (openvpn, 2018)*



Características de OpenVPN

OpenVPN se distingue por una serie de características que lo convierten en una solución robusta y segura para la implementación de redes privadas virtuales. Una de sus principales fortalezas es el uso del protocolo SSL/TLS para la autenticación y el establecimiento de túneles cifrados, lo que garantiza que los datos transmitidos entre el cliente y el servidor sean seguros y no puedan ser interceptados por terceros. Además, OpenVPN es altamente configurable y permite la implementación de autenticación basada en certificados, credenciales de usuario y autenticación en dos factores para mejorar la seguridad. Otra característica importante es su capacidad para funcionar en diferentes puertos y protocolos, como TCP y UDP, lo que le permite sortear bloqueos de red y restricciones impuestas por proveedores de servicios de Internet o administradores de red. También soporta algoritmos de cifrado avanzados, como AES-256, que garantizan un nivel de seguridad adecuado para proteger información sensible.

Beneficios de OpenVPN

Los beneficios de OpenVPN son diversos y abarcan desde la seguridad hasta la facilidad de implementación y compatibilidad con múltiples dispositivos y sistemas operativos. En términos de seguridad, su cifrado fuerte y su capacidad para ocultar la dirección IP del usuario garantizan una protección eficaz contra ataques cibernéticos y la vigilancia en línea. Además, su naturaleza de código abierto permite auditorías constantes por parte de la comunidad de desarrolladores y expertos en ciberseguridad, lo que ayuda a mantener la solución actualizada y libre de vulnerabilidades. En el ámbito corporativo, OpenVPN facilita la conexión remota segura de empleados y equipos distribuidos en diferentes ubicaciones, permitiendo el acceso a redes internas sin comprometer la seguridad de los datos. Otro de sus beneficios es la compatibilidad con diversas plataformas, incluyendo Windows, macOS, Linux, Android e iOS, lo que permite a los usuarios configurar una VPN segura en cualquier dispositivo.

OpenVPN es una alternativa sofisticada, versátil y confiable para establecer redes

privadas virtuales. Su facilidad para ajustarse a distintos entornos y su énfasis en la protección de datos y la privacidad lo posicionan como una opción fundamental tanto para usuarios que desean resguardar su actividad en línea como para empresas que necesitan conexiones seguras y estables en sus operaciones.

Tabla 2. Ventajas y Desventajas de OpenVPN

Aspecto	**Ventajas**	**Desventajas**
Seguridad	Utiliza cifrado avanzado (AES-256) y protocolos seguros como SSL/TLS, garantizando una protección robusta de los datos.	Puede requerir una configuración avanzada para garantizar la máxima seguridad, lo que podría ser complejo para usuarios sin experiencia técnica.
Compatibilidad	Funciona en múltiples plataformas, incluyendo Windows, macOS, Linux, Android e iOS, facilitando su implementación en distintos entornos.	Algunas plataformas móviles pueden requerir configuraciones adicionales o aplicaciones específicas para un funcionamiento óptimo.
Flexibilidad	Se puede configurar para trabajar con diferentes puertos y protocolos (TCP/UDP), lo que permite adaptarse a distintas necesidades de red.	Su versatilidad implica que su configuración inicial puede ser más compleja en comparación con otras soluciones VPN preconfiguradas.
Estabilidad	Su capacidad para atravesar firewalls y adaptarse a distintas condiciones de red lo hace una opción confiable en entornos restringidos.	Puede presentar una leve disminución en la velocidad en comparación con protocolos más livianos como WireGuard.
Código Abierto	Al ser de código abierto, permite auditorías de seguridad constantes y modificaciones según las	Al depender de la comunidad para soporte y mantenimiento, algunas soluciones empresariales pueden

	necesidades del usuario o empresa.	preferir alternativas comerciales con soporte técnico dedicado.

Fuente: (Stallings W. , Cryptography and Network Security: Principles and Practice (7th ed.), 2017)

Elegir entre las VPN de pago y las gratuitas

A criterio de (Kurose, 2020), a la hora de elegir entre una VPN de pago y una gratuita, es fundamental considerar diversos factores que impactan en la seguridad, privacidad, velocidad y funcionalidad del servicio. Las VPN de pago suelen ofrecer una mayor protección al emplear protocolos de cifrado avanzados, garantizar una política estricta de no registro de datos y proporcionar un ancho de banda ilimitado, lo que resulta clave para quienes buscan estabilidad en la conexión y protección total de su información. Además, estas VPN incluyen servidores optimizados en múltiples ubicaciones, lo que permite una mejor experiencia en la navegación, acceso a contenidos restringidos geográficamente y un menor riesgo de congestión en la red. Por otro lado, las VPN gratuitas pueden ser una opción atractiva para quienes buscan una solución básica sin incurrir en costos, pero suelen presentar importantes limitaciones, como la presencia de anuncios, restricciones de velocidad y una menor cantidad de servidores disponibles. Además, algunas VPN gratuitas pueden comprometer la privacidad de los usuarios al registrar y vender sus datos de navegación a terceros con fines comerciales, lo que contradice el propósito fundamental de utilizar una VPN: la protección de la información. Asimismo, las VPN de pago ofrecen soporte técnico especializado, lo que resulta ventajoso en caso de problemas de configuración o conexión, mientras que, en las versiones gratuitas, la asistencia al usuario suele ser limitada o inexistente. En conclusión, si bien las VPN gratuitas pueden ser útiles para necesidades ocasionales y básicas, las opciones de pago representan la mejor alternativa para quienes priorizan la seguridad, el rendimiento y la privacidad de sus datos en el entorno digital.

Tabla 3. Comparativa entre VPN gratuitas y de pago

Característica	**VPN Gratuitas**	**VPN de Pago**
Costo	Gratuito	Requiere suscripción mensual o anual
Velocidad	Generalmente más lenta debido a servidores limitados	Mayor velocidad y estabilidad en servidores dedicados
Seguridad	Menor nivel de cifrado y protección	Encriptación avanzada (AES-256) y protocolos más seguros
Privacidad	Puede almacenar logs (información de navegación)	No registra logs o utiliza políticas estrictas de no registros
Acceso a contenido	Acceso limitado a ciertos servicios o regiones	Acceso a contenido de cualquier región (sin restricciones geográficas)
Soporte al cliente	Limitado o inexistente	Soporte 24/7 con atención personalizada
Facilidad de uso	Fácil de instalar, pero con opciones limitadas	Interfaz más profesional y personalizable
Publicidad	Generalmente incluye anuncios	Sin anuncios
Cantidad de servidores	Pocos servidores disponibles	Amplia red de servidores a nivel mundial
Dispositivos soportados	Limitado a pocos dispositivos	Compatible con múltiples dispositivos y sistemas operativos

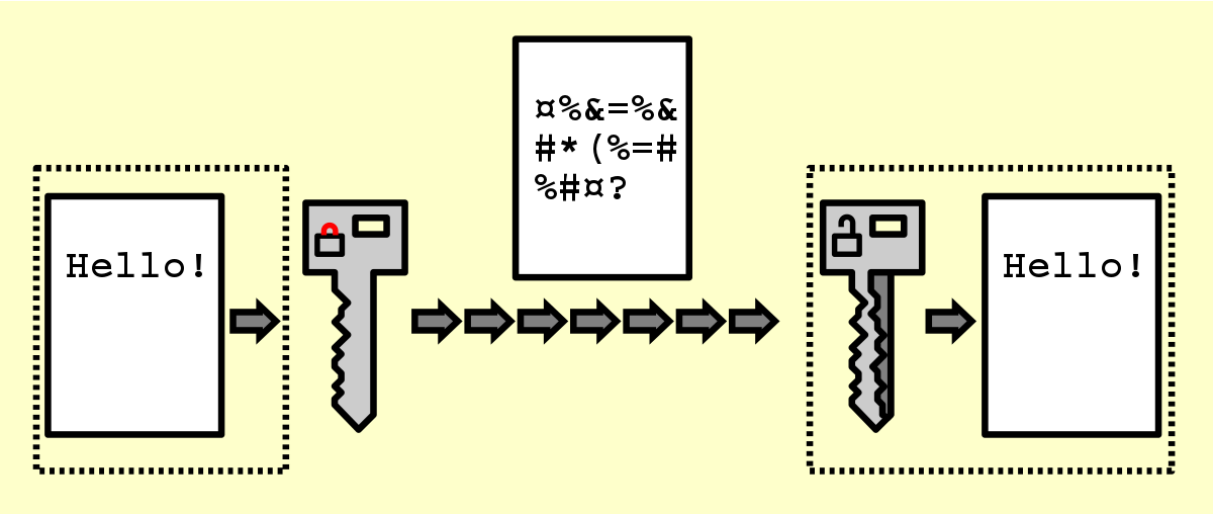
Fuente: (Gibbs, 2002)

2.2.12 Cifrado

Ángel del Río Mateos (Criptología, 2021), define la criptografía como la disciplina que permite transformar la información para que solo las partes autorizadas puedan acceder a su contenido, garantizando la confidencialidad, integridad y autenticidad de los datos. En su estudio, el autor explica que la criptografía ha evolucionado a lo largo de la historia, desde los sistemas de cifrado más rudimentarios utilizados en la antigüedad, como el cifrado de César, hasta los complejos algoritmos matemáticos empleados en la actualidad, como el AES (Advanced Encryption Standard) y el RSA (Rivest-Shamir-Adleman). Según Del Río Mateos, la criptografía se fundamenta en el uso de claves y algoritmos que convierten un mensaje legible (texto plano) en un mensaje cifrado (texto cifrado), el cual solo puede ser descifrado por quienes poseen la clave adecuada. Esta técnica se ha vuelto indispensable en el ámbito de la seguridad informática, protegiendo la información en transacciones bancarias, comunicaciones electrónicas y almacenamiento de datos sensibles. Además, el autor menciona que la criptografía no solo se enfoca en ocultar información, sino también en garantizar que los datos no sean alterados ni falsificados mediante firmas digitales y funciones hash. En el contexto actual, donde los ciberataques y las amenazas digitales son cada vez más sofisticados, la criptografía es una herramienta clave para fortalecer la seguridad y privacidad en entornos digitales.

En la figura 8 se muestra un esquema de cifrado

Figura 8.Cifrado tomado de (wikipedia, 2018)



Métodos de Cifrado

Las técnicas de cifrado desempeñan un papel fundamental en la protección de la información, ya que convierten los datos en un formato incomprensible para evitar accesos no autorizados. A lo largo del tiempo, la criptografía ha experimentado un notable desarrollo, pasando de métodos rudimentarios a complejos algoritmos matemáticos. Su aplicación se extiende a diversos ámbitos, como el sector financiero, las comunicaciones seguras y la preservación de datos personales.

Según (Ferrer, 2004), en su libro Fundamentos de criptografía los métodos de cifrado se dividen principalmente en dos grandes categorías: cifrado simétrico y cifrado asimétrico.

Cifrado Simétrico

El cifrado simétrico utiliza una única clave para el proceso de cifrado y descifrado, lo que lo hace eficiente en términos de velocidad. Sin embargo, presenta un problema de seguridad: si la clave es interceptada, toda la comunicación queda comprometida. Ferrer y Herrera Joancomartí explican que los algoritmos de cifrado simétrico se pueden clasificar en cifradores de bloque y cifradores de flujo. Los primeros procesan los datos en bloques de tamaño fijo, mientras que los segundos cifran los datos de manera continua, bit a bit. Ejemplos clásicos

de cifradores de bloque incluyen DES (Data Encryption Standard) y AES (Advanced Encryption Standard), mientras que el cifrado de flujo es representado por algoritmos como RC4. El estándar AES, desarrollado por el Instituto Nacional de Estándares y Tecnología de EE. UU. (NIST), se considera uno de los algoritmos más seguros en la actualidad debido a su estructura de sustitución y permutación que aumenta la complejidad del cifrado.

Cifrado Asimétrico

Por otro lado Según (Corrales Sánchez, 2012) en su libro Criptografía y Métodos de Cifrado, el cifrado asimétrico emplea un par de claves: una clave pública, utilizada para cifrar los datos, y una clave privada, utilizada para descifrarlos., este tipo de cifrado es más seguro, pero tiene una mayor carga computacional en comparación con el cifrado simétrico. Los algoritmos más conocidos dentro de esta categoría incluyen RSA (Rivest-Shamir-Adleman) y ECC (Elliptic Curve Cryptography). El algoritmo RSA, creado en 1977, se basa en la factorización de números primos, lo que dificulta su descifrado sin conocer la clave privada. Por otro lado, ECC es un método más reciente que ofrece la misma seguridad con claves más cortas, optimizando el rendimiento en dispositivos con recursos limitados.

Métodos Híbridos y Seguridad Criptográfica

Ante la necesidad de combinar la eficiencia del cifrado simétrico con la seguridad del cifrado asimétrico, han surgido métodos híbridos, donde el cifrado asimétrico se usa para intercambiar claves de sesión que luego serán utilizadas en un esquema simétrico.

Según (Mateos A. d., 2010), menciona que este enfoque es ampliamente utilizado en protocolos de seguridad como SSL/TLS (Secure Sockets Layer/Transport Layer Security), empleados en la protección de datos en la web. Además, señala que la seguridad del cifrado no solo depende del algoritmo utilizado, sino también de factores como la longitud de la clave y la correcta implementación del sistema criptográfico.

Las técnicas de cifrado han progresado con el tiempo para proporcionar mayores niveles

de seguridad y eficiencia. Mientras que el cifrado simétrico continúa siendo la opción preferida en escenarios donde la velocidad es un factor clave, el cifrado asimétrico resulta esencial para la autenticación y la protección de información sensible en entornos digitales. La combinación de ambos métodos en esquemas híbridos ha permitido desarrollar soluciones más robustas sin afectar el rendimiento, lo que resalta la importancia de seleccionar el tipo de cifrado más adecuado según el contexto y los requisitos de seguridad.

Aplicación del Cifrado en la Seguridad de la Información

El cifrado ha emergido como un componente esencial para asegurar la protección de la información en diversos sectores, abarcando desde la protección de datos personales hasta la seguridad de las transacciones bancarias y las comunicaciones en línea. Este proceso implica convertir la información en un formato ilegible para aquellos sin autorización, permitiendo solo a quienes tienen la clave de descifrado acceder a los datos originales. Con el avance tecnológico y la expansión de la digitalización, la implementación del cifrado ha evolucionado para enfrentar nuevos retos y adaptarse a entornos cada vez más complejos.

1. Cifrado en las Comunicaciones Digitales

Según (Héctor Corrales Sánchez, 2020) en el libro "Criptografía y Métodos de Cifrado" el cifrado se aplica en diversos protocolos de comunicación, como SSL/TLS, utilizados para asegurar conexiones seguras en Internet. Estos protocolos permiten que la información enviada entre un navegador y un servidor web esté protegida contra ataques de interceptación. Además, destacan el uso del cifrado en correos electrónicos mediante estándares como PGP (Pretty Good Privacy) y S/MIME (Secure/Multipurpose Internet Mail Extensions), que garantizan la confidencialidad y autenticación de los mensajes enviados.

2. Cifrado en la Protección de Datos en Dispositivos

Por otro lado (Joancomartí, 2018), en "Fundamentos de Criptografía" explican que el cifrado es una herramienta clave en la protección de datos almacenados en dispositivos

electrónicos. Tecnologías como BitLocker en Windows y FileVault en macOS emplean algoritmos avanzados, como AES (Advanced Encryption Standard), para asegurar que la información almacenada en discos duros y unidades USB esté protegida ante posibles robos o accesos no autorizados. Además, destacan que el cifrado de bases de datos se ha convertido en una práctica esencial para proteger información sensible en el sector empresarial y gubernamental.

3. Cifrado en la Seguridad Bancaria y Transacciones Electrónicas

En el ámbito financiero (Mateos Á. d., 2019) en su obra "Criptografía y Seguridad en Redes, señala que el cifrado es indispensable para garantizar la integridad y autenticidad de las transacciones electrónicas. Tecnologías como 3D Secure y el cifrado RSA permiten que las operaciones bancarias en línea sean seguras, evitando fraudes y accesos indebidos. Asimismo, el cifrado en los sistemas de pago sin contacto, como tarjetas con chip EMV y billeteras digitales (Apple Pay, Google Pay), ofrece una capa adicional de protección mediante la generación de códigos dinámicos en cada transacción, reduciendo el riesgo de clonación.

4. Cifrado en Redes Privadas Virtuales (VPN)

Según (Corrales Sánchez, 2012), otro aspecto fundamental es el uso del cifrado en redes privadas virtuales (VPN), el cual permite a los usuarios navegar de forma segura en redes públicas, y explica que los protocolos VPN más seguros, como OpenVPN e IPsec, emplean algoritmos de cifrado avanzados para ocultar la dirección IP del usuario y proteger su tráfico de datos contra posibles ataques de espionaje o manipulación. Las VPN son ampliamente utilizadas en empresas para permitir el acceso remoto seguro de empleados a recursos internos sin comprometer la seguridad de la red corporativa.

El cifrado juega un papel crucial en la protección de datos en la actualidad, siendo utilizado en una variedad de campos, como las comunicaciones, el almacenamiento de información, la banca electrónica y la seguridad de redes. La mejora de los algoritmos de cifrado

y su incorporación en distintos sistemas ha sido clave para reducir los riesgos relacionados con ciberataques y accesos no autorizados. Sin embargo, como destacan los autores mencionados, la efectividad del cifrado depende de la correcta implementación de los protocolos y de la utilización de algoritmos fuertes capaces de enfrentar las amenazas actuales.

2.2.13 Herramientas Open Source para Escaneo de Vulnerabilidades

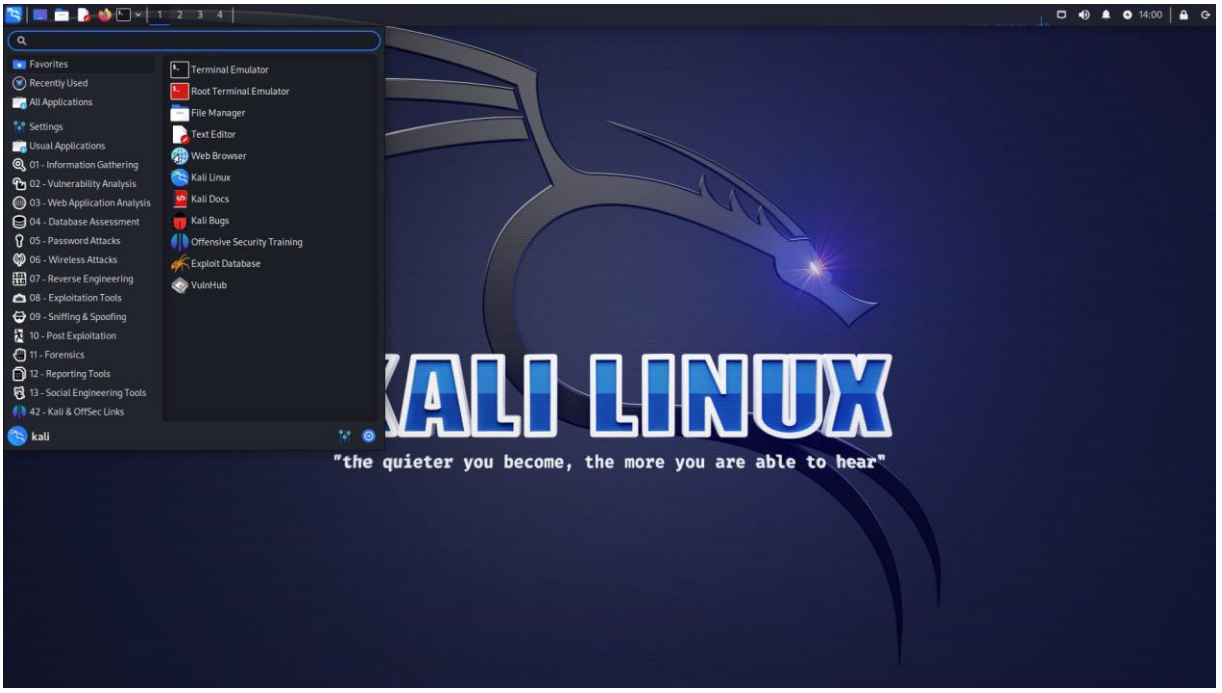
Las herramientas de código abierto para el escaneo de vulnerabilidades se han vuelto cruciales en las estrategias de ciberseguridad, ya que permiten identificar deficiencias de seguridad en sistemas, aplicaciones y redes de forma eficiente y asequible. Estas herramientas, al ser accesibles y respaldadas por comunidades activas de desarrolladores, ofrecen a los profesionales de la seguridad opciones flexibles y personalizables para realizar auditorías. Entre las más reconocidas se encuentran Nmap, utilizada para la detección de redes y escaneo de puertos, OpenVAS, un sistema que realiza un análisis exhaustivo de infraestructuras en busca de vulnerabilidades, y Nikto, que se especializa en el escaneo de servidores web. Además, Metasploit es una opción destacada, ya que no solo ayuda a identificar vulnerabilidades, sino que también permite explotarlas para evaluar la efectividad de las defensas de un sistema. A pesar de ser herramientas gratuitas, son muy eficaces cuando se implementan de manera adecuada y permiten a las organizaciones identificar y mitigar riesgos antes de que sean aprovechados por atacantes. Gracias a que son de código abierto, los usuarios pueden modificar y adaptar estas herramientas según sus necesidades, lo que las convierte en una opción popular tanto para pequeñas empresas como para grandes organizaciones que buscan fortalecer sus medidas de seguridad.

Kali Linux

Kali Linux es una distribución de Linux basada en Debian, creada especialmente para realizar pruebas de penetración y auditorías de seguridad. Fue lanzada en 2013 por Offensive Security, la misma entidad que desarrolló BackTrack, una distribución predecesora de Kali.

Kali Linux se ha establecido como una de las herramientas más utilizadas en el campo de la ciberseguridad gracias a su extenso conjunto de herramientas preinstaladas, que permiten realizar una variedad de tareas como hacking ético, análisis forense digital y pruebas de seguridad. Entre sus principales herramientas se encuentran Metasploit, Nmap, Aircrack-ng y Wireshark, que son fundamentales para realizar escaneos de vulnerabilidades, análisis de redes, explotación de fallos de seguridad y monitoreo de tráfico en redes.

Figura 9. Kali Linux tomado de (kali, s.f.)



Según el autor y experto en seguridad informática (McHardy, 2017), Kali Linux es una plataforma poderosa no solo para expertos en seguridad, sino también para aquellos que están empezando en el campo. McHardy señala que Kali Linux se distingue por su facilidad de uso, a pesar de ser un sistema altamente técnico, y su capacidad para adaptarse a una variedad de escenarios de pruebas de penetración. McHardy también destaca que la comunidad de Kali Linux, siendo una de las más activas en el ámbito de la seguridad, juega un papel fundamental en la mejora continua de la distribución, contribuyendo a la actualización de las herramientas disponibles y a la creación de recursos educativos.

Otro autor relevante es el reconocido especialista en seguridad informática (Mallett,

2018), aborda la funcionalidad de Kali Linux desde un enfoque más profundo, enfatizando su potencial en las pruebas de penetración avanzadas y el análisis forense digital. Mallett explica cómo Kali Linux permite a los usuarios ejecutar ataques simulados a sistemas y redes, de manera controlada, para descubrir vulnerabilidades antes de que los atacantes puedan explotarlas. Según Mallett, el valor de Kali Linux no solo radica en las herramientas que contiene, sino también en su flexibilidad y capacidad para ser ejecutado desde múltiples dispositivos, incluidos sistemas operativos en vivo desde USB o máquinas virtuales, lo que lo convierte en una plataforma eficiente para auditores de seguridad y profesionales de TI.

Por su parte (Lee, 2019), en el libro Kali Linux for Beginners el autor se enfoca en proporcionar una guía práctica para aquellos que inician en el mundo de Kali Linux. Lee describe cómo instalar y configurar Kali Linux, así como los usos básicos de sus herramientas. En su obra, se profundiza sobre la importancia de aprender a utilizar Kali Linux en un entorno controlado antes de realizar pruebas de penetración en redes reales, para evitar causar daños accidentales.

Kali Linux no es solo un sistema operativo potente para realizar pruebas de penetración y auditorías de seguridad, sino también una herramienta que continúa evolucionando a medida que las amenazas cibernéticas se desarrollan. Gracias a las contribuciones de expertos como McHardy, Mallett y Lee, se ha establecido como una de las opciones más destacadas y confiables para los profesionales en ciberseguridad y hacking ético, quienes pueden utilizar su completo conjunto de herramientas para salvaguardar sistemas y redes de posibles ataques maliciosos.

Nmap

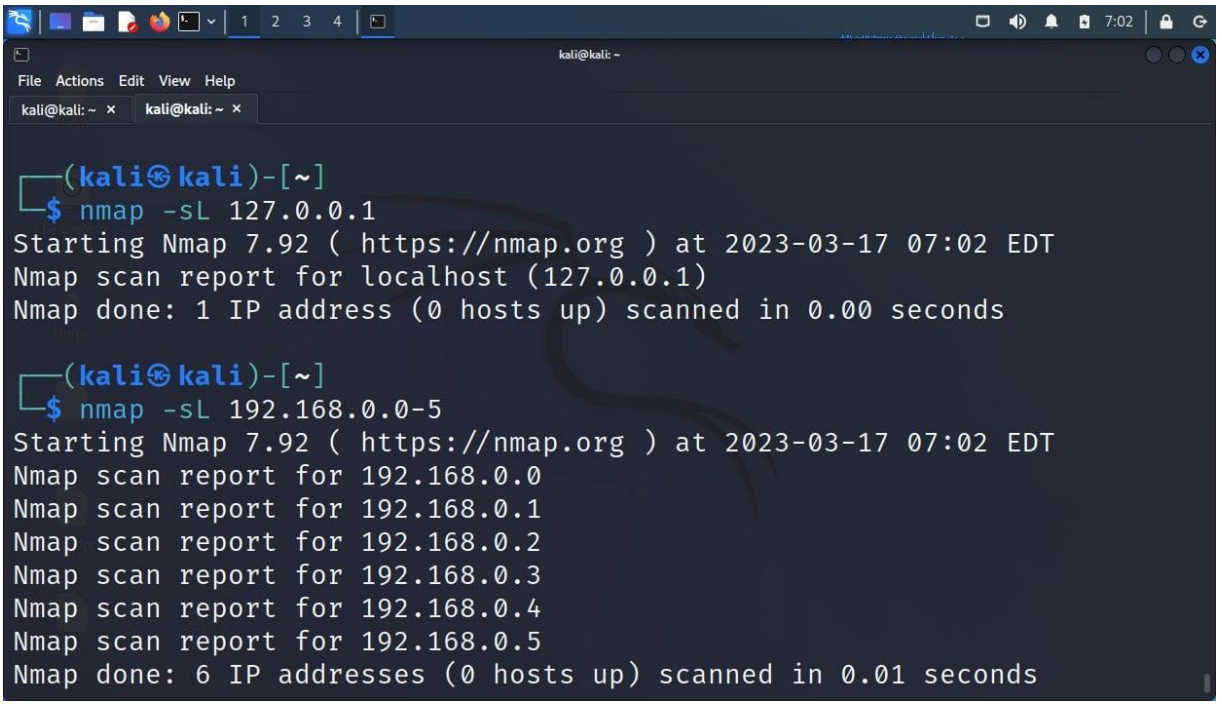
Nmap (Network Mapper) es una herramienta de código abierto utilizada ampliamente en el campo de la ciberseguridad para realizar auditorías de redes y detección de vulnerabilidades. Su funcionalidad principal se centra en el escaneo de redes para identificar

dispositivos activos, puertos abiertos y servicios disponibles en una red.

Según el autor (Fyodor, 2003) de "Nmap Network Scanning", el uso de Nmap es esencial para los administradores de redes y profesionales de la seguridad, ya que proporciona información detallada sobre la estructura de una red, permitiendo detectar posibles vulnerabilidades o configuraciones incorrectas que podrían ser explotadas por atacantes. Fyodor, creador de Nmap, explica que la herramienta no solo permite realizar escaneos de puertos básicos, sino que también cuenta con características avanzadas como la detección de sistema operativo, la identificación de versiones de software y el descubrimiento de servicios ocultos. La publicación del libro, que cubre un rango extenso de técnicas y prácticas para optimizar el uso de Nmap, ofrece una comprensión profunda de cómo llevar a cabo una auditoría de red eficaz.

Según (Fyodor, 2003), a través de este libro, no solo presenta las capacidades básicas de Nmap, sino que también profundiza en su aplicabilidad en escenarios complejos, abordando temas como la evasión de firewalls y el escaneo de redes protegidas. En conjunto, el texto se convierte en una referencia imprescindible para todos aquellos que busquen entender cómo utilizar Nmap para mejorar la seguridad de sus redes y sistemas.

Figura 10. Nmap (Autoría propia)



Nessus

Nessus es una herramienta ampliamente reconocida en el campo de la ciberseguridad, utilizada para el análisis de vulnerabilidades en redes y sistemas. Su desarrollo se inició en 1998 como un proyecto de código abierto impulsado por Renaud Deraison, con la finalidad de ofrecer a los especialistas en seguridad una solución eficiente para detectar y reducir riesgos en entornos digitales. Con el transcurso de los años, Nessus fue evolucionando hasta transformarse en un software comercial gestionado por Tenable, Inc., consolidándose como una de las plataformas más confiables para la identificación de amenazas.

Según el libro Mastering Nessus for Advanced Penetration Testing de (Kumar, 2014), Nessus permite realizar escaneos automáticos para detectar vulnerabilidades en dispositivos conectados a la red, analizando configuraciones incorrectas, debilidades en sistemas operativos, errores en aplicaciones y posibles puertas traseras que podrían ser explotadas por atacantes. Kumar enfatiza la capacidad de Nessus para integrarse con otras herramientas de seguridad y

su versatilidad para adaptarse a distintos entornos, desde pequeñas redes corporativas hasta infraestructuras empresariales complejas.

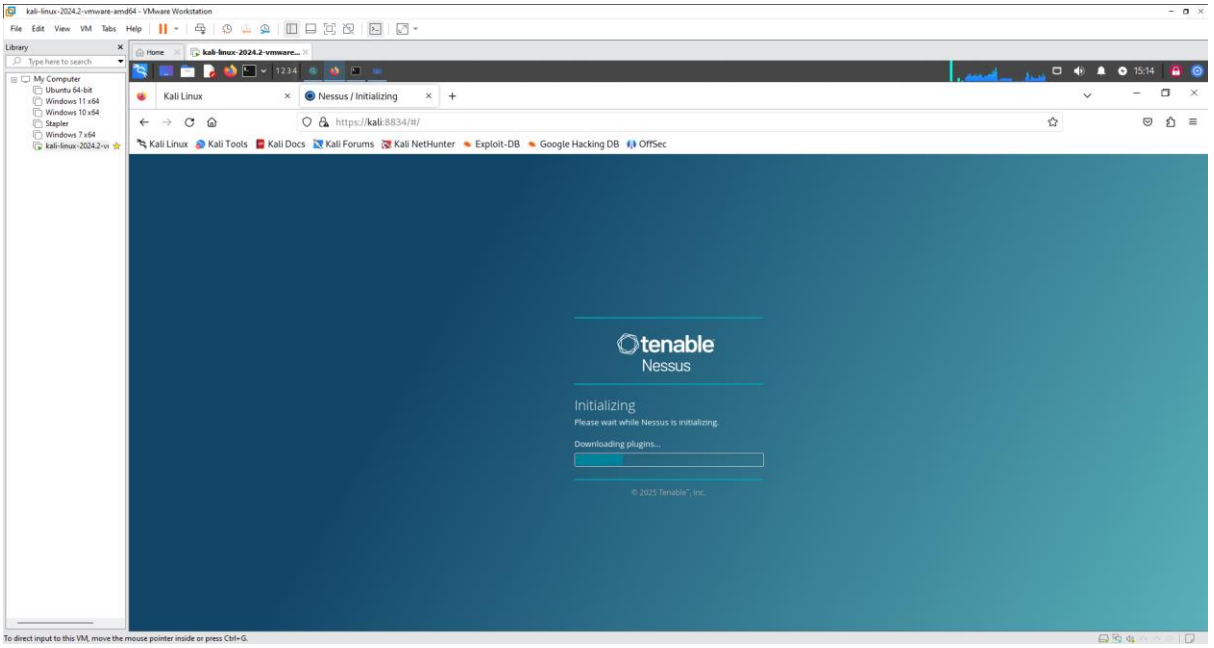
En su obra, Kumar detalla que Nessus cuenta con una base de datos constantemente actualizada, lo que le permite detectar amenazas emergentes y proporcionar soluciones en tiempo real. Además, destaca que esta herramienta es compatible con múltiples sistemas operativos y ofrece reportes detallados que facilitan la toma de decisiones en cuanto a medidas de mitigación.

Según (MacDougall, 2011), en Nessus 4: Quickstart Guide, se explican los procedimientos esenciales para la instalación y configuración de Nessus, proporcionando una visión práctica sobre su funcionamiento en entornos empresariales. MacDougall subraya la importancia del análisis de vulnerabilidades como parte de una estrategia proactiva de seguridad informática y menciona cómo Nessus ayuda a las organizaciones a cumplir con normativas de seguridad, como PCI DSS, HIPAA y SOX. Asimismo, señala que una de las principales ventajas de Nessus es su interfaz intuitiva, que permite a los administradores de sistemas y analistas de seguridad ejecutar escaneos sin necesidad de conocimientos avanzados en programación o ciberseguridad.

Por otro lado, en el libro Cybersecurity Ops with bash: Attack, Defend, and Analyze from the Command Line (Troncone, 2020), se menciona que Nessus es una herramienta clave en la automatización de procesos de auditoría de seguridad. Los autores destacan su capacidad para integrarse con scripts personalizados, lo que amplía su funcionalidad y permite adaptarla a necesidades específicas. Troncone y Albing explican cómo combinar Nessus con otras herramientas de análisis forense y pruebas de penetración para obtener una evaluación de seguridad más completa. Según ellos, la capacidad de Nessus para generar informes personalizados facilita la identificación de vulnerabilidades críticas y la priorización de acciones correctivas, lo que resulta fundamental en la protección de infraestructuras tecnológicas.

Nessus representa una herramienta esencial en el campo de la ciberseguridad, ya que permite a los expertos detectar y remediar vulnerabilidades antes de que sean aprovechadas por actores malintencionados. Su transformación de un proyecto de código abierto a una solución comercial ha garantizado su constante actualización y liderazgo en la identificación de amenazas. Debido a sus características avanzadas, su compatibilidad con otros sistemas y su facilidad de uso, Nessus continúa siendo una alternativa clave para empresas de diversas escalas que buscan fortalecer su seguridad y cumplir con las regulaciones establecidas.

Figura 11. Ingreso a Nessus (Autoría Propia)



OWASP Zen Attack Proxy ZAP

Es una de las herramientas más empleadas en el campo de la ciberseguridad para detectar y analizar vulnerabilidades en aplicaciones web. Desarrollado y administrado por la Open Web Application Security Project (OWASP), ZAP es una solución de código abierto que facilita a especialistas en seguridad, programadores y auditores la realización de pruebas de penetración con el propósito de identificar posibles fallos de seguridad antes de que puedan ser explotados por ciberdelincuentes. Desde su creación, esta herramienta ha ganado gran popularidad gracias a su facilidad de uso, su interfaz gráfica intuitiva y su capacidad para automatizar análisis de seguridad, convirtiéndola en una alternativa óptima tanto para profesionales experimentados

como para quienes están iniciando en el ámbito del hacking ético y la seguridad informática.

Una de las características más relevantes de OWASP ZAP es su estructura modular, que permite la integración con múltiples herramientas y complementos para ampliar sus capacidades. ZAP opera como un proxy entre el usuario y la aplicación web analizada, interceptando y examinando las solicitudes HTTP y HTTPS para detectar vulnerabilidades como inyecciones SQL, errores en la gestión de sesiones, exposición de información sensible y configuraciones inseguras. Además, su funcionalidad de escaneo, tanto activo como pasivo, permite evaluar la seguridad de una aplicación sin necesidad de ejecutar ataques intrusivos, lo que lo convierte en una opción ideal para entornos de desarrollo y pruebas de seguridad continuas.

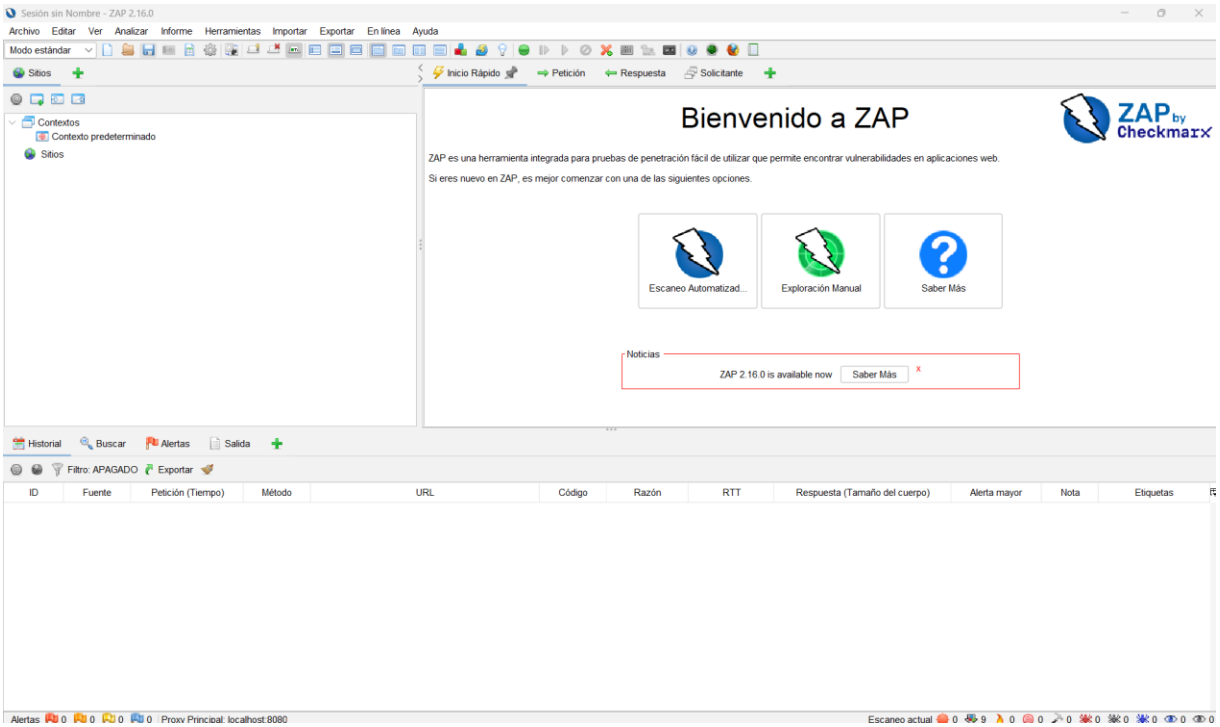
De acuerdo con el libro "Practical Web Penetration Testing" *(Wear S. , 2019)*, OWASP ZAP es una de las herramientas más utilizadas en el ámbito del testing de aplicaciones web, gracias a su enfoque en la automatización y su compatibilidad con CI/CD (Integración y entrega continua). Wear menciona que, al integrarse con herramientas como Jenkins y GitLab CI/CD, ZAP permite a las organizaciones mejorar sus procesos de seguridad desde las primeras etapas del desarrollo de software, garantizando que las vulnerabilidades sean detectadas antes de que las aplicaciones sean desplegadas en entornos de producción.

Por otro lado, en el libro "Web Security Testing Cookbook" *(Hope, 2009)*, los autores destacan que OWASP ZAP es una alternativa accesible y poderosa a herramientas comerciales de análisis de seguridad, ya que ofrece una combinación equilibrada entre simplicidad y funciones avanzadas. Hope y Walther resaltan que la funcionalidad de escaneo de ZAP se puede personalizar mediante scripts escritos en Python o JavaScript, lo que facilita la creación de pruebas de seguridad personalizadas para aplicaciones web específicas. Además, la posibilidad de integrarse con navegadores como Firefox y Chrome permite a los testers realizar pruebas interactivas y capturar solicitudes en tiempo real, brindando un mayor control sobre el proceso de auditoría de seguridad.

Finalmente, en el libro "The Web Application Hacker’s Handbook" *(Stuttard, 2011)*, se menciona que OWASP ZAP es una herramienta fundamental para los profesionales del pentesting debido a su versatilidad y capacidad de detectar fallas en aplicaciones web modernas. Stuttard y Pinto subrayan que, aunque existen herramientas más avanzadas y específicas en el mercado, ZAP sigue siendo una de las opciones más completas para quienes buscan una solución gratuita y eficaz para la evaluación de seguridad en aplicaciones web.

OWASP ZAP es una herramienta fundamental en el análisis de seguridad de aplicaciones web, ya que ofrece un entorno adaptable e intuitivo para la identificación de vulnerabilidades. Al estar respaldada por OWASP, recibe actualizaciones constantes y mejoras continuas, lo que la posiciona como una alternativa confiable para expertos en ciberseguridad y desarrolladores. Su capacidad para integrarse con diversas herramientas de seguridad y su enfoque en la automatización han permitido que ZAP siga siendo una de las opciones más empleadas en la industria para la ejecución de pruebas de penetración en aplicaciones.

Figura 12. Inicio de OWASP ZAP (Autoría Propia)



Metasploit

Metasploit es una de las herramientas más relevantes en el campo de la ciberseguridad, siendo ampliamente empleada por expertos para llevar a cabo pruebas de penetración, detectar vulnerabilidades y explotar fallos de seguridad en sistemas informáticos. Iniciado en 2003 por H.D. Moore como un proyecto de código abierto, Metasploit ha evolucionado con el tiempo hasta convertirse en una plataforma poderosa y fiable, utilizada tanto por profesionales éticos

como por atacantes maliciosos. La herramienta permite a los usuarios identificar vulnerabilidades mediante una base de datos extensa de exploits y módulos que se pueden utilizar para explotar diversos sistemas y servicios. Además de servir como plataforma para la explotación de vulnerabilidades, Metasploit incluye funcionalidades para crear payloads, lo cual facilita a los profesionales de seguridad realizar simulaciones de ataques en entornos controlados con el fin de evaluar la efectividad de las medidas de defensa de un sistema.

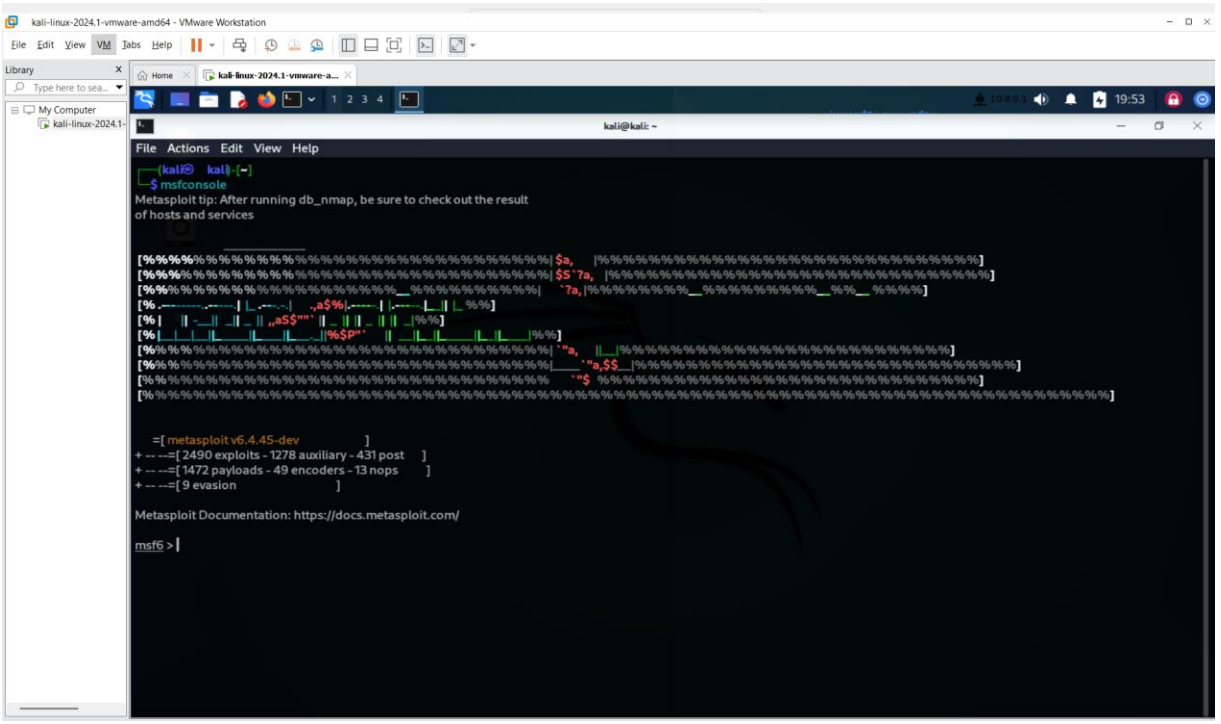
Una de las características más importantes de Metasploit es su capacidad para automatizar y simplificar ataques que, de otra forma, serían muy complicados de realizar. La herramienta permite llevar a cabo ataques sobre múltiples sistemas operativos y aplicaciones, abarcando desde la inyección de código hasta la explotación de fallos en servicios web y redes. A lo largo de los años, Metasploit ha sido mantenido y actualizado por Rapid7, una empresa especializada en ciberseguridad que adquirió el proyecto en 2009. La constante actualización de la herramienta, junto con la ampliación de su base de datos de exploits, ha sido clave para mantenerla como una de las opciones más confiables para los profesionales de la seguridad informática, dado que se actualiza con regularidad para incluir las últimas vulnerabilidades detectadas en el entorno cibernético.

Para hacer un uso adecuado de Metasploit, es esencial que los profesionales comprendan tanto su funcionamiento como las implicaciones legales de su utilización. Aunque es una herramienta extremadamente poderosa, su uso está regulado por la legislación de varios países, debido a que podría ser empleada con fines maliciosos si se encuentra en manos no autorizadas. Por lo tanto, los usuarios deben asegurarse de emplear Metasploit dentro de los límites legales y éticos, como en el caso de pruebas de penetración autorizadas, auditorías de seguridad y en entornos de laboratorio controlados.

Según los autores en el libro Metasploit: The Penetration Tester's Guide (Kennedy,

2011), metasploit es un "marco abierto que ha facilitado la realización de pruebas de penetración al automatizar muchos de los procesos involucrados". Este enfoque práctico permite a los pentesters obtener una comprensión más profunda de las vulnerabilidades en los sistemas que están evaluando, proporcionando una plataforma flexible y poderosa para los profesionales de la seguridad.

Figura 13. Metasploit (tomado de Kali Linux)



Wireshark

Es una herramienta ampliamente utilizada en el campo del análisis de redes y la seguridad informática. Se trata de un software de código abierto especializado en la inspección de protocolos, permitiendo la captura y el examen de paquetes de datos en tiempo real. Esto proporciona una visión detallada del tráfico en una red, lo que lo convierte en un recurso valioso para administradores de sistemas, expertos en ciberseguridad y analistas forenses. Su compatibilidad con una amplia variedad de protocolos y su flexibilidad han sido factores clave en su popularidad. Originalmente desarrollado en 1998 bajo el nombre de Ethereal, este

software ha experimentado una notable evolución, adoptando el nombre de Wireshark en 2006 y contando con el respaldo de una comunidad activa de desarrolladores y profesionales en redes.

Según el libro "Wireshark for Security Professionals" de Jessey Bullock y Jeff T. (Bullock, 2017), Wireshark ofrece una interfaz gráfica intuitiva que permite a los usuarios visualizar el tráfico de red de manera estructurada. Bullock y Parker explican que una de sus características más destacadas es la capacidad de filtrar y analizar paquetes específicos mediante expresiones avanzadas, lo que facilita la detección de actividades sospechosas o anomalías en la comunicación de red. Además, mencionan que Wireshark es compatible con una amplia variedad de protocolos de red, incluidos TCP/IP, HTTP, DNS, FTP, ICMP y muchos otros, lo que lo hace invaluable en la resolución de problemas de conectividad y la identificación de vulnerabilidades de seguridad.

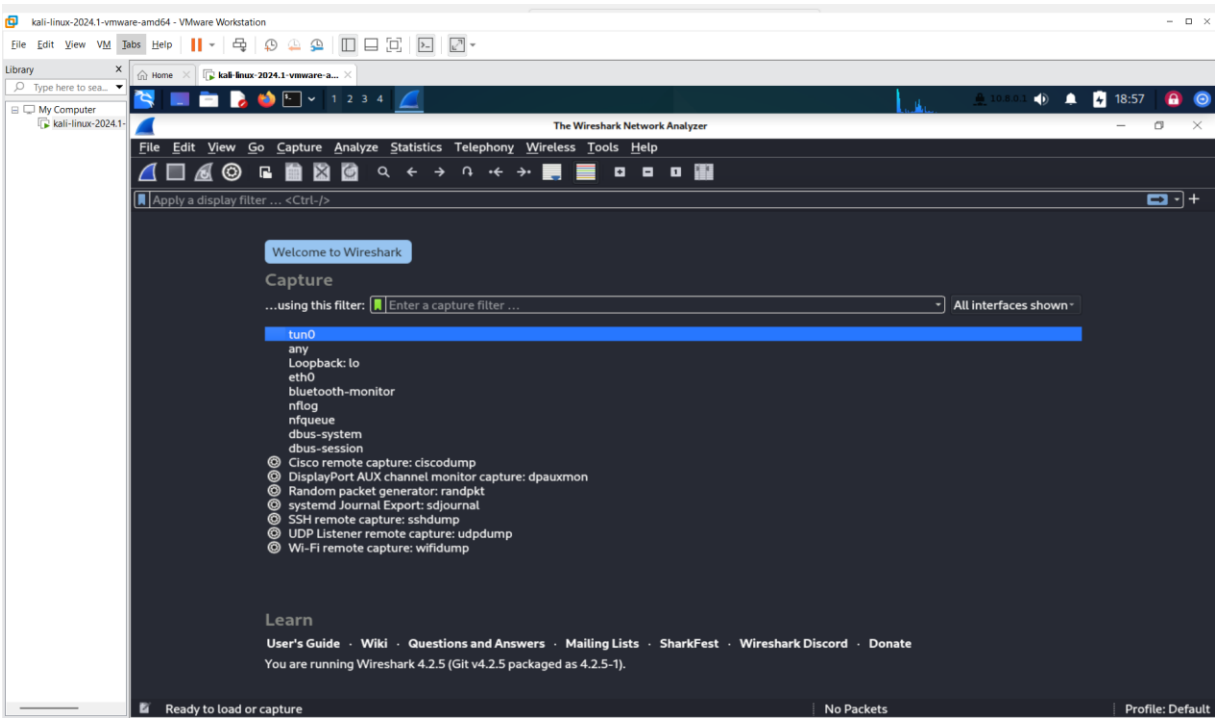
Por otro lado, en el libro "Wireshark Network Analysis: The Official Wireshark Certified Network Analyst Study Guide" (Chappell, 2017), se detalla cómo Wireshark es utilizado en auditorías de seguridad y en la detección de ataques cibernéticos. Chappell enfatiza la importancia de Wireshark en la identificación de patrones de tráfico malicioso, como intentos de exploración de puertos, ataques de denegación de servicio (DoS) y actividades sospechosas relacionadas con malware. Además, menciona que el software permite examinar el contenido de los paquetes de datos y reconstruir sesiones de comunicación, lo que resulta crucial en investigaciones forenses digitales y en la recopilación de evidencias en incidentes de seguridad.

De acuerdo con el libro "Mastering Wireshark" (Mishra, 2016), una de las ventajas clave de Wireshark es su capacidad para detectar tráfico no autorizado y posibles ataques dentro de una red. Mishra describe cómo los profesionales de seguridad pueden utilizar filtros avanzados y funciones de inspección profunda de paquetes (DPI) para analizar patrones de tráfico y detectar actividades sospechosas, como intentos de exfiltración de datos o conexiones no autorizadas a servidores externos.

Además, en "Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems" (Sanders, 2017), el autor destaca la importancia de Wireshark en la optimización del rendimiento de las redes y la resolución de problemas técnicos. Sanders explica que Wireshark permite identificar cuellos de botella en el tráfico de red, analizar latencias en las conexiones y depurar configuraciones incorrectas en dispositivos de red. También resalta que el software es una herramienta fundamental en la enseñanza y capacitación de administradores de redes y especialistas en seguridad informática, ya que permite visualizar en detalle el funcionamiento de los protocolos de comunicación.

Wireshark es una herramienta fundamental para el análisis y supervisión de redes, siendo utilizada tanto para detectar ataques cibernéticos como para mejorar el rendimiento de las infraestructuras de comunicación. Su flexibilidad, amplia compatibilidad con protocolos de red y su interfaz fácil de usar lo hacen una opción preferida para profesionales de TI, investigadores forenses y administradores de seguridad. Como mencionan Bullock y Parker, Chappell, Mishra y Sanders en sus respectivos trabajos, el uso de Wireshark para resolver problemas de red y detectar amenazas cibernéticas es esencial para asegurar la protección y el funcionamiento estable de los sistemas informáticos, tanto en entornos empresariales como académicos.

Figura 14. Inicio Wireshark (desde Kali Linux)



Burp Suite

Burp Suite, creada por PortSwigger, es una solución completa y altamente valorada en el campo de la ciberseguridad debido a su efectividad en la ejecución de pruebas de penetración y análisis de seguridad en aplicaciones web. Gracias a su estructura modular, brinda a los expertos las herramientas necesarias para examinar, detectar y aprovechar vulnerabilidades en un entorno seguro, permitiendo optimizar de manera constante la protección de las aplicaciones.

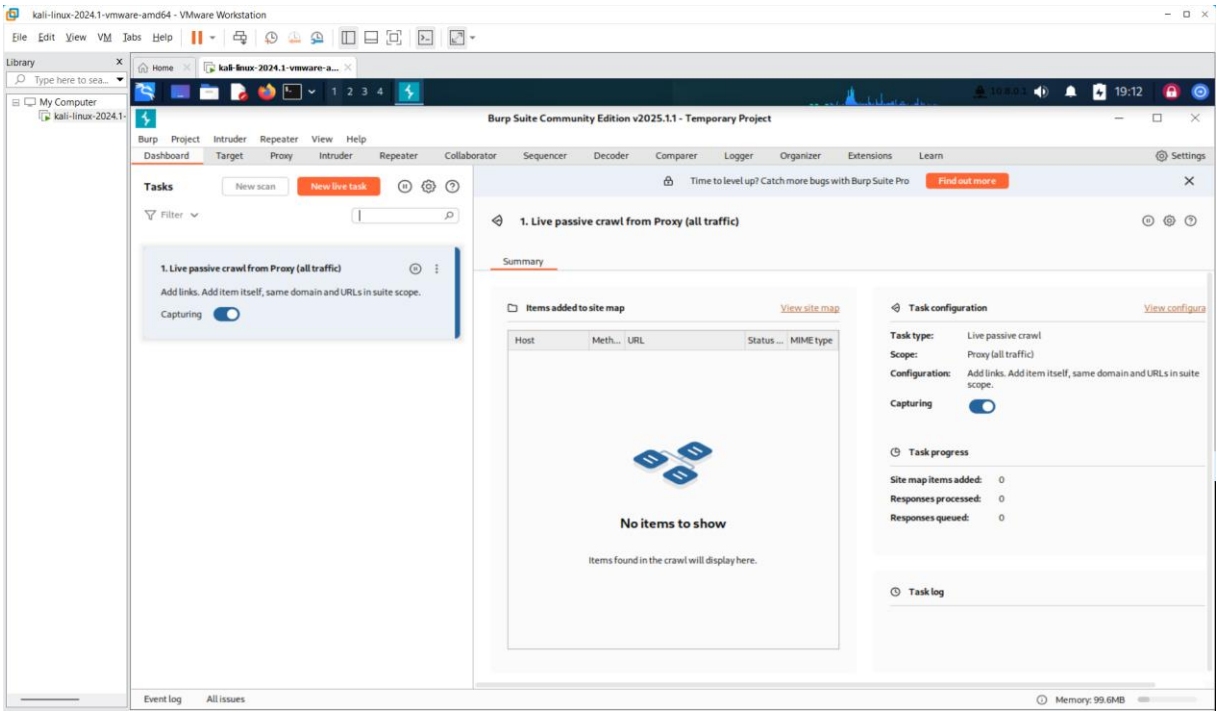
Una obra destacada que aborda el uso de Burp Suite es "A Complete Guide to Burp Suite: Learn to Detect Application Vulnerabilities" (Rahalkar, 2020), en este libro, Rahalkar proporciona una introducción detallada a las funcionalidades de Burp Suite, incluyendo la configuración inicial, el uso de herramientas integradas como el proxy, el escáner y el intruder, así como técnicas para detectar y explotar vulnerabilidades comunes en aplicaciones web. Este recurso es especialmente útil para aquellos que buscan comprender los fundamentos de Burp Suite y aplicarlos en evaluaciones de seguridad.

Otra referencia significativa es "Burp Suite Cookbook: Web Application Security Made Easy with Burp Suite" (Wear D. S., 2023), este libro ofrece una colección de recetas prácticas que abarcan desde técnicas básicas hasta avanzadas en el uso de Burp Suite. La Dra. Wear profundiza en aspectos como la automatización de pruebas, la personalización de herramientas y la integración de Burp Suite en flujos de trabajo de desarrollo seguro, proporcionando a los profesionales de seguridad soluciones prácticas para desafíos comunes en la evaluación de la seguridad de aplicaciones web.

La documentación oficial de Burp Suite, accesible en el sitio web de PortSwigger, es un recurso clave para los usuarios. Esta guía abarca desde instrucciones rápidas para principiantes hasta explicaciones detalladas sobre funcionalidades avanzadas, y se actualiza de manera continua para incluir las últimas mejoras y características del software. Es una fuente confiable para mantenerse actualizado sobre las mejores prácticas y novedades relacionadas con Burp Suite.

Burp Suite se ha establecido como una herramienta crucial en el campo de la seguridad informática. Las publicaciones mencionadas brindan perspectivas valiosas sobre su utilización y aplicación, desde conceptos básicos hasta técnicas avanzadas, ofreciendo a los lectores el conocimiento necesario para llevar a cabo evaluaciones de seguridad efectivas en aplicaciones web.

Figura 15. Burp Suit (desde Kali Linux)



Suricata

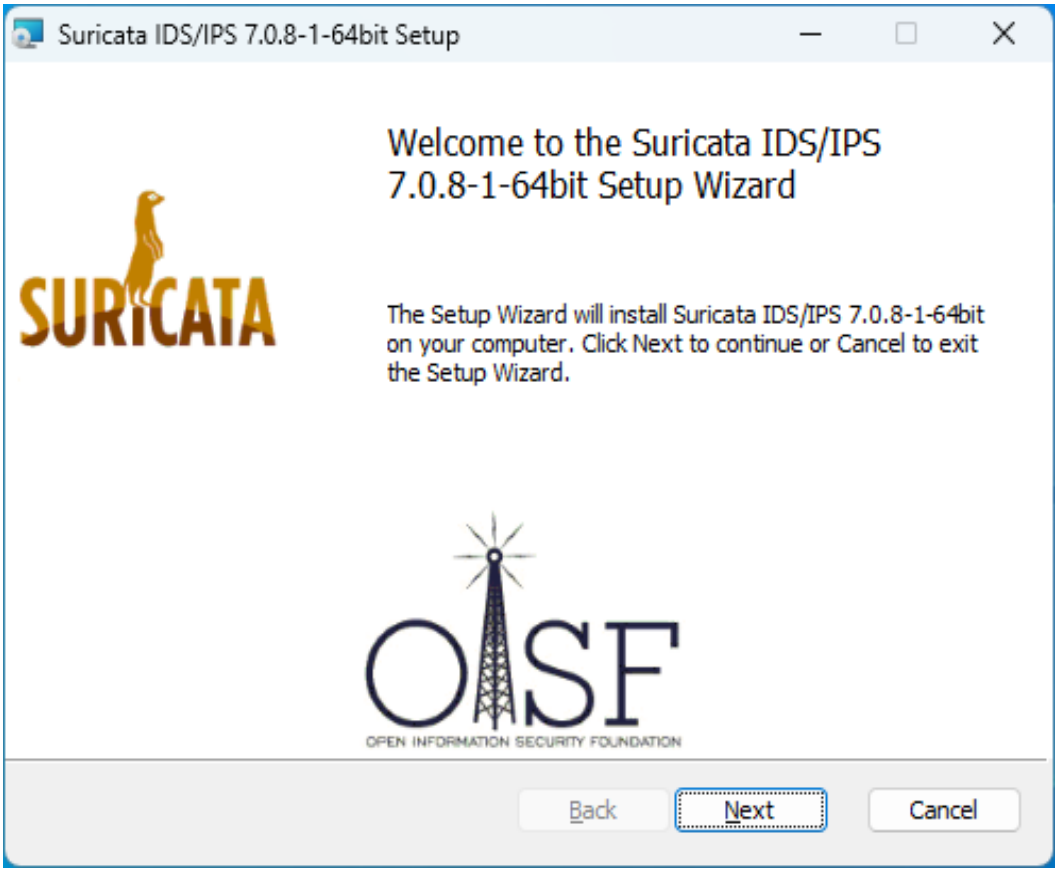
Suricata es un sistema de detección y prevención de intrusiones (IDS/IPS) de alto rendimiento utilizado ampliamente en ciberseguridad para proteger redes y sistemas ante posibles amenazas. Desarrollado por la Fundación Open Information Security (OISF), Suricata es un software de código abierto que se destaca por su capacidad para detectar y mitigar ataques en tiempo real mediante un análisis exhaustivo del tráfico de red. Al igual que otros sistemas IDS/IPS, Suricata se encarga de analizar los paquetes de datos que transitan por la red para identificar patrones y comportamientos inusuales que podrían indicar la presencia de un ataque cibernético.

Una de las características más destacadas de Suricata es su habilidad para realizar una inspección profunda de los paquetes (DPI), lo que le permite identificar una amplia variedad de amenazas, como ataques de denegación de servicio (DDoS), intrusiones de malware, vulnerabilidades de seguridad y tráfico no autorizado. Suricata también es compatible con

múltiples protocolos y es capaz de operar en redes de alta velocidad, lo que lo convierte en una opción ideal para entornos empresariales o de gran escala. Su diseño flexible facilita la integración con otras herramientas de seguridad, como los sistemas de gestión de eventos e información de seguridad (SIEM), lo que permite consolidar datos y mejorar la estrategia de seguridad global.

Con el tiempo, la configuración y el uso de Suricata se ha vuelto más accesible, gracias a su documentación detallada y la contribución constante de la comunidad de seguridad. Sin embargo, para que Suricata sea realmente efectivo, los administradores de red deben asegurarse de configurarlo correctamente y mantener actualizadas sus reglas de detección, ya que las amenazas cibernéticas están en constante evolución. Además, Suricata se ha destacado por su compatibilidad con Snort, otra herramienta IDS/IPS ampliamente utilizada, lo que facilita la transición para quienes ya están familiarizados con este sistema.

Figura 16. Instalación de Suricata



2.3 Marco Legal

En Ecuador, las normativas vinculadas a la ciberseguridad y la salvaguarda de datos se ubican principalmente en la Constitución, leyes particulares y normativas dictadas por las autoridades pertinentes. A pesar de que no hay una ley concreta que regule directamente el empleo de VPN de fuente abierta en estrategias de ciberseguridad, existen ciertas leyes y regulaciones pertinentes que podrían implementarse:

Constitución de la República del Ecuador: La Constitución (2008) asegura el derecho a la privacidad y a la salvaguarda de la información personal. Toda investigación que implique la recolección y tratamiento de información personal debe respetar los principios y estipulaciones constitucionales vinculadas con la privacidad y la salvaguarda de datos.

Ley Orgánica de Telecomunicaciones (Asamblea Nacional, 2015): Esta normativa controla la utilización de las telecomunicaciones en Ecuador y podría implicar la utilización de VPN de fuente abierta en redes de telecomunicaciones. Es crucial examinar las exigencias y normativas dictadas por esta ley para garantizar el cumplimiento de las estipulaciones pertinentes.

Ley Orgánica de Comunicación (Asamblea Nacional, 2013): Esta normativa define estipulaciones vinculadas a la salvaguarda de la información y la privacidad en el sector de los medios de difusión. A pesar de que se enfoca principalmente en la regulación de los medios de comunicación convencionales y digitales, también podría tener repercusiones en el manejo de datos en investigaciones vinculadas a la ciberseguridad.

Regulaciones de protección de datos personales: A pesar de que Ecuador no cuenta con una legislación específica para la protección de datos personales, existen regulaciones y reglamentos que definen los principios y requerimientos para el manejo de la información personal. Es crucial garantizar el cumplimiento de estas normativas al recolectar y manejar información personal en el marco de un estudio de ciberseguridad.

Normativa de seguridad de la información: En el ámbito corporativo, las entidades pueden estar sujetas a regulaciones concretas de seguridad de la información, tales como la norma ISO 27001 (2025) u otras regulaciones de protección de la información. Estas regulaciones podrían contemplar exigencias vinculadas al empleo de tecnologías de seguridad, como las VPN, y podrían ser pertinentes para un análisis de ciberseguridad.

CAPÍTULO III

3. MARCO METODOLÓGICO

En el escenario actual de ciberseguridad, salvaguardar la privacidad y la seguridad en internet se ha vuelto una inquietud cada vez más urgente. Con el aumento acelerado de las amenazas cibernéticas y la creciente necesidad de conexión digital, resulta esencial disponer de instrumentos eficaces que aseguren la salvaguarda de los datos y la privacidad de las comunicaciones en línea. En este escenario, las VPN han emergido como una respuesta esencial para mantener la seguridad y la privacidad en un ambiente digitalmente vinculado.

En los últimos años, el uso de VPN ha aumentado considerablemente debido a su accesibilidad, transparencia y flexibilidad. Un estudio de NordVPN, realizado en julio de 2023, reveló que aproximadamente el 25% de los usuarios en España emplean una VPN para proteger su actividad en línea, lo que muestra un crecimiento importante respecto a años anteriores. Este aumento se debe principalmente a la necesidad de garantizar la seguridad y privacidad en internet frente a los crecientes ciberataques.

En 2021, las descargas de aplicaciones VPN aumentaron un 184% en comparación con el año anterior, alcanzando los 785 millones de descargas en plataformas como Google y Apple. Este crecimiento se observó en diversas partes del mundo, siendo Qatar el país con mayor uso de VPN, con un 69,6%, seguido de Emiratos Árabes Unidos con un 59,5% y Singapur con un 49,1%. En América Latina, Bolivia fue el país con mayor adopción de VPN, ocupando el décimo lugar a nivel mundial.

Estos datos reflejan una tendencia global de creciente adopción de VPN, impulsada por la preocupación por la privacidad en línea y la necesidad de protegerse contra amenazas digitales. La flexibilidad y transparencia de las VPN de código abierto han sido factores clave

para su popularidad, permitiendo a los usuarios personalizar su experiencia y mantener un control más efectivo sobre su navegación.

Estas soluciones de código abierto proporcionan a personas y entidades una opción económica para resguardar sus comunicaciones en línea y proteger su información delicada. No obstante, la eficacia de las VPN Open Source en estrategias de ciberseguridad es un asunto que todavía necesita una valoración rigurosa y un estudio minucioso.

3.1 Descripción del área de estudio

El enfoque principal de esta tesis es evaluar la efectividad de las VPN Open Source en las estrategias de ciberseguridad, particularmente en contextos académicos y profesionales donde la protección de la información es fundamental. Este análisis se llevó a cabo en el consultorio jurídico gratuito de la Universidad Indoamérica, ubicado en Ambato, el cual cuenta con 25 computadoras utilizadas por los estudiantes de la carrera de Derecho para realizar sus prácticas. El objetivo principal de la investigación es examinar cómo las soluciones de VPN Open Source pueden fortalecer la seguridad en línea, protegiendo los datos personales y la privacidad en el acceso a servicios digitales.

El estudio cubrirá varios aspectos esenciales: en primer lugar, se analizará la implementación de VPN Open Source en un entorno académico, evaluando la configuración adecuada de estas herramientas en los equipos disponibles y cómo los estudiantes interactúan con los sistemas de información. Posteriormente, se explorarán los desafíos técnicos y operativos que pueden surgir durante la integración de estas soluciones, tales como la compatibilidad con los sistemas existentes, la gestión de claves criptográficas y la estabilidad de la conexión a la red.

Otro aspecto relevante será la evaluación de la efectividad de las VPN en la protección de la privacidad y la seguridad, considerando factores como el cifrado de datos, la prevención de fugas de información y la defensa frente a ciberataques. Además, se examinará cómo estas

herramientas afectan el rendimiento de la red, midiendo variables como la latencia, el ancho de banda y la calidad de la conexión.

Finalmente, el estudio proporcionará recomendaciones sobre las mejores prácticas para la implementación y uso de VPN Open Source en entornos educativos y profesionales, con el fin de optimizar las estrategias de ciberseguridad y dotar a los estudiantes y profesionales de las herramientas necesarias para garantizar la seguridad de la información en su día a día.

3.2 Enfoque de la investigación

La metodología y el enfoque de este estudio sobre la "Evaluación de la Efectividad de VPN Open Source en Estrategias de Ciberseguridad: Un Análisis Integral sobre Implementación, Desafíos y Mejores Prácticas" emplean una combinación de métodos exploratorios y descriptivos.

Descriptivo: El enfoque descriptivo se utilizó para examinar de manera detallada la efectividad de las VPN de código abierto en aspectos como su implementación segura, la identificación de vulnerabilidades y su capacidad para resistir amenazas. Se llevo a cabo estudios minuciosos de datos para investigar estos aspectos de forma estructurada, con el objetivo de obtener una comprensión clara de su funcionamiento y desempeño.

Exploratorio: El método exploratorio se aplicó para investigar un tema que aún no ha sido completamente entendido o estudiado en profundidad. Dado que el uso de VPN Open Source en estrategias de ciberseguridad es un campo reciente y en constante cambio, este enfoque permitió investigar diversos factores relacionados con su implementación, los desafíos que surgen y las mejores prácticas a seguir. Este enfoque facilito la identificación de nuevas áreas de investigación y ofrecerá una visión más amplia de este tema emergente.

3.3 Tipo de Investigación

Para cumplir con los objetivos de la tesis, se adoptó un enfoque combinado que integró métodos tanto cualitativos como cuantitativos. La investigación cualitativa se utilizó para

explorar aspectos más subjetivos y complejos, tales como los desafíos en la implementación de las VPN Open Source y las percepciones de los usuarios. En cambio, la investigación cuantitativa se aplicó para obtener datos objetivos sobre el desempeño de la red y la efectividad de las VPN en la protección de la privacidad y la seguridad.

Se utilizaron diversas técnicas de investigación, como revisiones bibliográficas, encuestas, entrevistas, pruebas de rendimiento y análisis de casos prácticos. Estos procedimientos facilitaron la recopilación de información desde diferentes fuentes y perspectivas, permitiendo una comprensión más completa de la eficacia de las VPN Open Source en las estrategias de ciberseguridad.

3.4 Procedimiento de la investigación

Fase 1: Diseño de un ambiente de pruebas que permita simular una red VPN Open Source en un entorno controlado

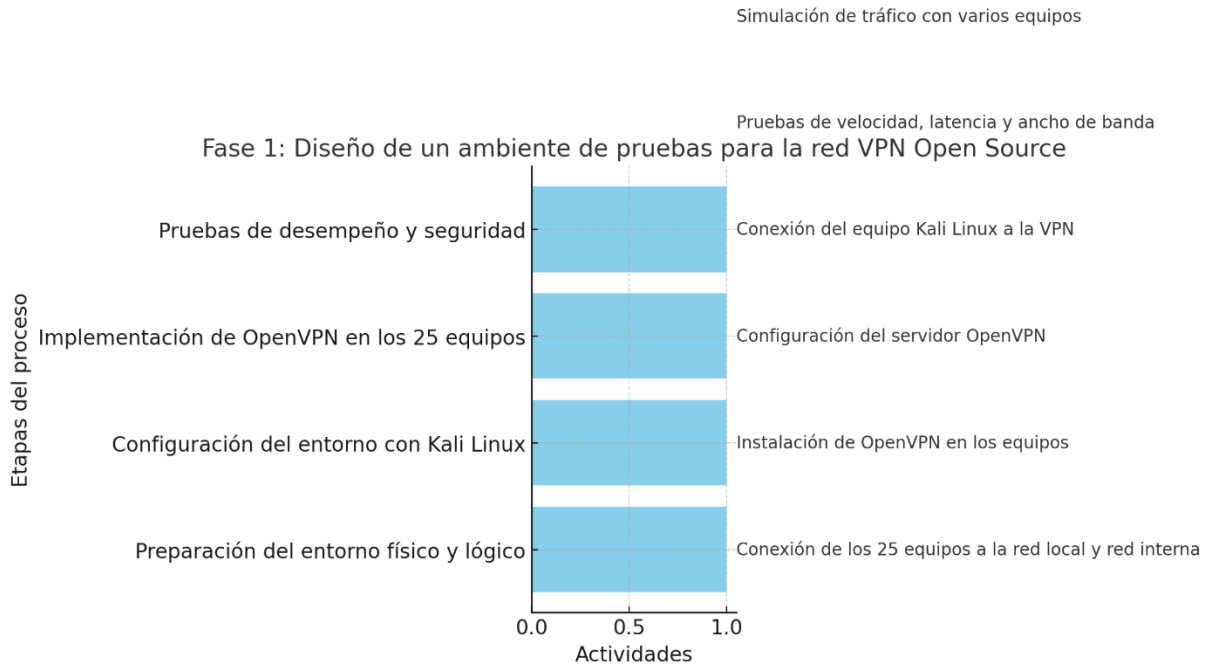
El primer paso fue preparar tanto el entorno físico como el lógico, garantizando que los 25 equipos con Windows 25 estén operativos y conectados a la misma red local, con acceso tanto a internet como a la red interna de la universidad. A continuación, se instala OpenVPN en todos los equipos para que participen en las pruebas de la VPN. Luego, se selecciona uno de los equipos con Windows 10 para configurarlo como servidor OpenVPN, realizando la instalación y configuración adecuada para que gestione las conexiones de los clientes.

En segundo lugar, se configuro un equipo con Kali Linux para usarlo como máquina de pruebas, que se conectará a la red VPN como cliente y servirá para realizar escaneos de vulnerabilidades y pruebas de penetración utilizando herramientas como Nmap, Metasploit y OpenVAS. Luego de configurar los equipos, se lleva a cabo la implementación de OpenVPN en los 25 equipos con Windows 10. Se instala y configura OpenVPN en cada uno de los equipos cliente, asegurando que todos puedan conectarse correctamente al servidor. Es crucial verificar que las direcciones IP asignadas por el servidor estén dentro del rango adecuado, como por

ejemplo 192.168.1.x.

Finalmente, se realizaron pruebas de desempeño y seguridad para evaluar el rendimiento de la VPN. Las pruebas de desempeño incluyen medir la velocidad de transmisión de datos usando herramientas como iperf y speedtest-cli, para analizar el impacto de la VPN en la red. Se simula una carga de tráfico al usar varios equipos simultáneamente para observar cómo afecta el rendimiento global. También se mide la latencia utilizando herramientas como ping para determinar la eficiencia de la red. Por último, se evalúa el ancho de banda disponible con la VPN activa y se compara con los valores de referencia sin la VPN, lo cual permitirá evaluar el impacto de la implementación de la VPN en el rendimiento de la red, en la figura

Figura 17. Fase 1 (Autoría Propia)



Fase 2: Análisis de vulnerabilidades y amenazas asociadas con las redes VPN Open Source

Durante esta fase de la investigación, se llevó a cabo un análisis detallado de vulnerabilidades en la implementación de OpenVPN dentro del entorno de pruebas del consultorio Jurídico de la Universidad Indoamérica. Para ello, se utilizó un equipo con Kali

Linux, conectado a la red VPN como cliente autorizado, desde donde se ejecutaron diversas herramientas de seguridad. Se emplearon Nmap para detectar puertos abiertos y servicios activos, Metasploit para realizar pruebas de penetración automatizadas, OpenVAS y Nessus para un escaneo detallado de vulnerabilidades y Wireshark para analizar el tráfico de red y evaluar la seguridad del cifrado.

Además, se realizaron pruebas de penetración con el objetivo de simular ataques cibernéticos y evaluar la resistencia de la VPN ante posibles amenazas. Estas pruebas incluyeron intentos de fuerza bruta para descifrar credenciales, análisis de fugas de datos para verificar la integridad del túnel VPN y simulaciones de ataques de denegación de servicio (DoS) para evaluar la capacidad de respuesta del servidor ante sobrecargas, finalmente, todos los hallazgos fueron documentados, identificando vulnerabilidades, su nivel de riesgo y posibles soluciones. Esto permitió fortalecer la seguridad de OpenVPN y proporcionar recomendaciones basadas en evidencia para mejorar su implementación en entornos académicos y profesionales.

Fase 3: Evaluación de la efectividad de la red VPN Open Source simulada, considerando aspectos como la implementación segura, vulnerabilidades y resiliencia frente amenazas

Durante la evaluación de la eficacia de la red en OpenVpn Se llevo a cabo un análisis exhaustivo de la configuración de la VPN, asegurándose de que se utilicen cifrados sólidos, autenticación segura y políticas de acceso adecuadas, siguiendo las mejores prácticas de seguridad. Para ello, se emplearon herramientas especializadas como Nessus, OpenVAS y Nmap, que permitieron detectar fallos en la configuración y operación de la VPN, haciendo énfasis en configuraciones débiles y puntos de acceso no seguros. Además, se realizarán pruebas de penetración para valorar la resistencia de la VPN ante ataques, incluyendo intentos de intrusión no autorizados y ataques de denegación de servicio (DoS), con el objetivo de evaluar

cómo la VPN responde a estas amenazas.

Se llevo a cabo también un análisis de los registros de la VPN para detectar acciones sospechosas o signos de compromiso, tales como intentos de acceso no autorizado o problemas de autenticación. Además, se simularán amenazas, como ataques de phishing, malware y ingeniería social, para evaluar la capacidad de la red VPN para reaccionar ante diferentes tipos de riesgos.

Para asegurar la seguridad a largo plazo, se verifico la actualización constante de todos los componentes de la VPN, incluyendo el software OpenVPN, con el fin de minimizar las vulnerabilidades detectadas, finalmente, se documentó todos los hallazgos, detallando las vulnerabilidades identificadas, las medidas correctivas implementadas y las lecciones aprendidas, con el propósito de optimizar la seguridad y estabilidad de la red antes de su implementación final en un entorno de producción.

Fase 4: Integración de soluciones VPN Open Source con otros sistemas de Seguridad

En esta fase, se fortaleció la seguridad de la red VPN Open Source mediante la integración con diversas herramientas de protección. OpenVPN se sincronizó con cortafuegos y sistemas de detección de intrusiones para monitorear y gestionar el tráfico, protegiendo la red contra ataques y detectando acciones maliciosas. Se implementaron soluciones antivirus y protección de endpoints para prevenir la entrada de malware y otras amenazas cibernéticas, además de añadir autenticación de dos factores para mayor seguridad requiriendo un segundo método de verificación para acceder a la red VPN. También se integró con un sistema SIEM para gestionar los registros de seguridad y se aplicó un cifrado robusto para proteger los datos. Finalmente, se mantuvo una actualización continua de los sistemas operativos, aplicaciones y componentes de la red, incluyendo OpenVPN, para minimizar vulnerabilidades y asegurar una mayor seguridad. Y se realizaron auditorías periódicas para asegurar el cumplimiento de las

políticas de seguridad, mejorando así la protección de los datos en la red VPN.

Al combinar OpenVPN con estas herramientas, se consiguió robustecer la protección de la información y salvaguardar los datos mientras se desplazan por la red VPN.

3.5 Desarrollo de las fases de la Investigación

3.5.1 Diseño de un ambiente de pruebas para simular una red VPN Open Source en el Consultorio Jurídico Gratuito de la Universidad Indoamérica

3.5.1.1 Objetivo

El objetivo principal de esta fase experimental es establecer un entorno de pruebas controlado en el Consultorio Jurídico Gratuito de la Universidad Indoamérica, empleando 25 equipos con Windows 10 para la implementación y análisis de una solución VPN de código abierto. Se recrearon condiciones de uso real, evaluando parámetros como ancho de banda, latencia, velocidad de transferencia, pérdida de paquetes y tiempo de conexión. En cuanto a seguridad, se examinaron intentos de ataque, cifrado, autenticación y control de acceso. La estabilidad del sistema se analizó a través del tiempo medio entre fallos, tiempo de recuperación, disponibilidad del servicio y registros de desconexiones, mientras que la usabilidad se valoró considerando la facilidad de configuración, impacto en la navegación y percepción del usuario. Los hallazgos obtenidos sirvieron como base para la toma de decisiones en una futura implementación a gran escala, facilitando la detección de vulnerabilidades y la optimización de configuraciones antes de su despliegue definitivo.

Metodologías y estándares:

1 ISO/IEC 27033 (Seguridad en redes)

Utilizada para establecer las líneas de la arquitectura de red segura

Proporcionar guías para el segmento de red y configuración del firewall

Base para las métricas de aislamiento de segmentos y comunicación entre zonas

2 NIST SP 800-53 (Controles de seguridad)

Sirvió como base para establecer los mínimos técnicos

Metodología de pruebas OSSTMM (Obrante de metodología de pruebas de seguridad de código abierto)

Proporciono el marco para las pruebas básicas de conectividad

Estableció los criterios para evaluar el rendimiento básico

Técnicas de recopilación de datos:

Pruebas de rendimiento con herramientas iperf3, ping

Monitoreo de recursos de sistema (CPU, memoria, ancho de banda)

Mediciones de latencia y establecimiento de conexión

Pruebas de usabilidad básicas

3.4.1.2 Preparación del entorno físico y lógico

Infraestructura del Consultorio Jurídico Gratuito

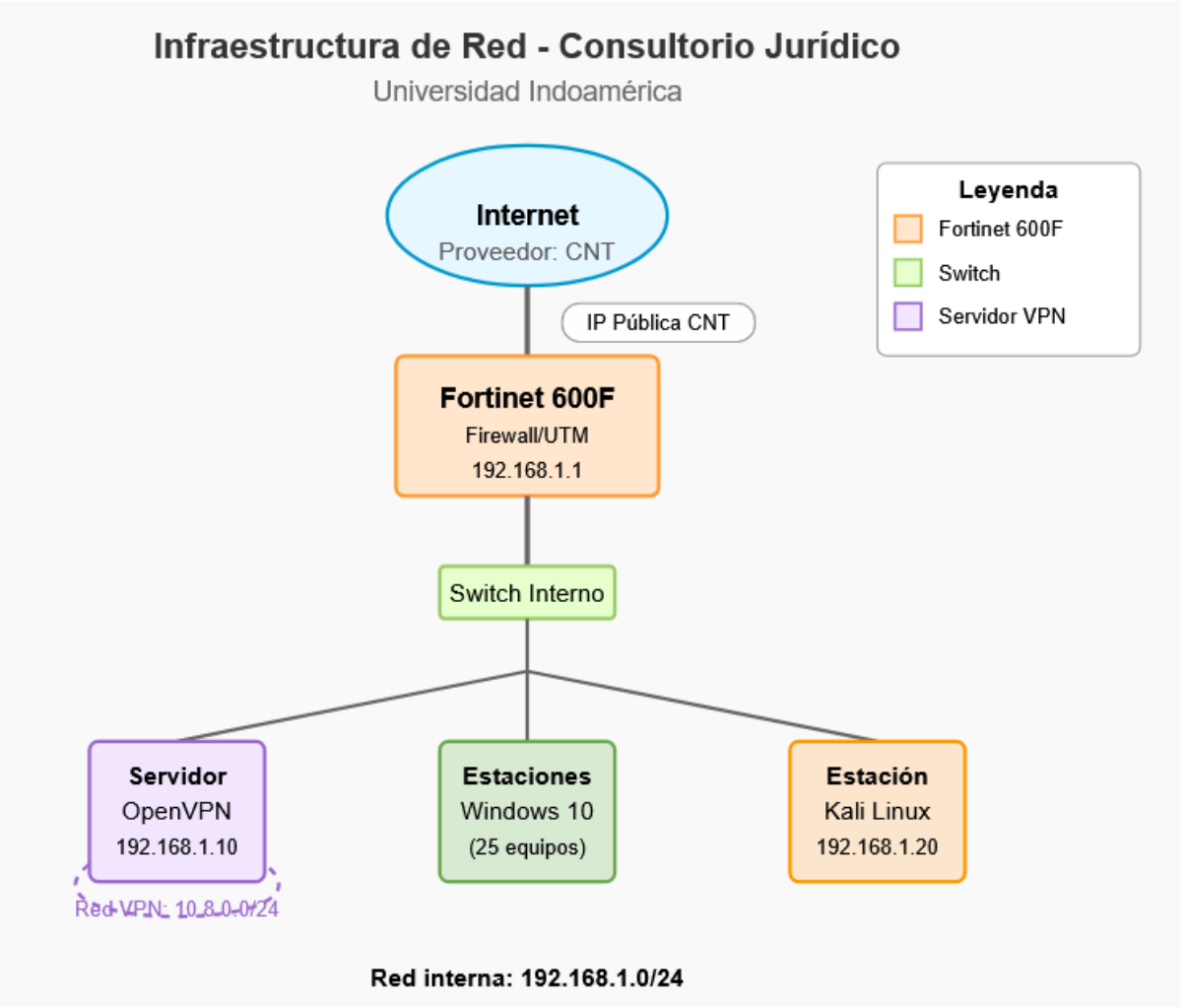
El Consultorio Jurídico Gratuito cuenta con la siguiente infraestructura de red:

Tabla 4. Infraestructura de Red

Componente	Especificación	Función
Equipo de Internet	CNT (Corporación Nacional de Telecomunicaciones)	Conectividad a Internet
Firewall	Fortinet FortiGate 600F	Seguridad perimetral, enrutamiento, NAT
Estaciones de trabajo	25 equipos Clones con Windows 10 Professional	Terminales de usuario

Diagrama de la infraestructura existente

Figura 18. Fase 1 (Autoría Propia)



Para establecer el entorno de pruebas, se realizó un análisis preliminar de la infraestructura existente en el Consultorio Jurídico Gratuito. Se verificó que los 25 equipos con Windows 10 cumplieran con los requisitos mínimos:

- Procesador: Intel Core i5 (6ta generación o superior)
- Memoria RAM: 8GB
- Almacenamiento: SSD de 256GB
- Adaptadores de red: Tarjetas Ethernet Gigabit y adaptadores Wi-Fi 802.11ac
- Sistema Operativo: Windows 10 Pro (versión 20H2 o superior)

Se diseñó una topología de red en estrella, donde todos los equipos se conectaron a un switch

central Fortinet 600F, garantizando una velocidad de conexión de 1 Gbps. Se implementó un esquema de direccionamiento IP privado (192.168.1.0/24) para la red local, asegurando que todos los dispositivos pudieran comunicarse entre sí y acceder tanto a recursos internos como a Internet a través del router principal de la universidad.

Segmentación de la red de pruebas

Para aislar el entorno de pruebas de la red de producción de la universidad, se implementó una VLAN dedicada (VLAN 20) en el switch principal. Esta segmentación proporcionó los siguientes beneficios:

- Aislamiento del tráfico de pruebas del resto de la red académica
- Mayor control sobre las políticas de seguridad y reglas de firewall
- Capacidad para monitorear específicamente el tráfico relacionado con la VPN
- Prevención de posibles interferencias con las operaciones diarias del Consultorio Jurídico gratuito.

Se configuraron reglas específicas en el firewall institucional para permitir el tráfico VPN (puerto UDP 1194) entre la VLAN de pruebas y las redes externas, manteniendo restricciones adecuadas para otros tipos de tráfico.

3.5.1.3 Implementación de la solución OpenVPN

Selección y configuración del servidor

Se seleccionó un equipo con especificaciones superiores (Intel Core i7, 16GB RAM,Disco SSD de 512 GB) para actuar como servidor OpenVPN, el mismo que se instaló Ubuntu.

```
# Instalación de Ubuntu Server LTS
# Verificación del sistema instalado
lsb_release -a
# Output:
# No LSB modules are available.
# Distributor ID: Ubuntu
# Description:    Ubuntu 22.04.3 LTS
# Release:        22.04
# Codename:       jammy

# Actualización del sistema
sudo apt update && sudo apt upgrade -y
```

Configuración de red

```
# Configuración de dirección IP estática
sudo nano /etc/netplan/00-installer-config.yaml
```

Contenido del archivo:

```
network:
  version: 2
  ethernets:
    enp0s3:
      dhcp4: no
      addresses: [192.168.1.10/24]
      gateway4: 192.168.1.1
      nameservers:
        addresses: [8.8.8.8, 8.8.4.4]
```

```
# Aplicar configuración
sudo netplan apply

# Verificar configuración
ip a show enp0s3
```

Instalación de OpenVPN y Easy-RSA

Instalación de paquetes

sudo apt install openvpn easy-rsa -y

Verificar instalación

openvpn --version

Output: OpenVPN 2.5.5 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [DCO] [MH/PKTINFO] [AEAD] built on Mar 22 2022

```
# Instalación de paquetes
sudo apt install openvpn easy-rsa -y

# Verificar instalación
openvpn --version
# Output: OpenVPN 2.5.5 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11]
```

Configuración de PKI (Infraestructura de la Clave Pública)

```
# Preparar directorio para Easy-RSA
mkdir -p ~/easy-rsa
cp -r /usr/share/easy-rsa/* ~/easy-rsa/
cd ~/easy-rsa

# Configurar variables
cat > vars << EOF
set_var EASYRSA_REQ_COUNTRY    "EC"
set_var EASYRSA_REQ_PROVINCE   "Tungurahua"
set_var EASYRSA_REQ_CITY       "Ambato"
set_var EASYRSA_REQ_ORG        "Universidad Indoamerica"
set_var EASYRSA_REQ_EMAIL      "admin@consultorio.edu.ec"
set_var EASYRSA_REQ_OU         "Consultorio Juridico"
set_var EASYRSA_KEY_SIZE       2048
set_var EASYRSA_ALGO           rsa
set_var EASYRSA_CA_EXPIRE      3650
set_var EASYRSA_CERT_EXPIRE    825
set_var EASYRSA_NS_SUPPORT     "no"
set_var EASYRSA_NS_COMMENT     "Consultorio Juridico Certificate"
set_var EASYRSA_EXT_DIR        "\${EASYRSA}/x509-types"
set_var EASYRSA_SSL_CONF       "\${EASYRSA}/openssl-easyrsa.cnf"
set_var EASYRSA_DIGEST         "sha256"
EOF

# Inicializar PKI
./easyrsa init-pki
```

```
# Crear autoridad certificadora (CA)
./easyrsa build-ca nopass
# Common Name: ConsultorioJuridico-CA

# Generar certificado y clave para el servidor
./easyrsa build-server-full server nopass

# Generar parámetros Diffie-Hellman
./easyrsa gen-dh

# Generar clave TLS-Auth
openvpn --genkey --secret ta.key
```

Configuración del servidor OpenVPN

Crear directorios y copiar archivos

sudo mkdir -p /etc/openvpn/server/

sudo mkdir -p /etc/openvpn/certs/

sudo cp pki/ca.crt /etc/openvpn/certs/

sudo cp pki/issued/server.crt /etc/openvpn/certs/

sudo cp pki/private/server.key /etc/openvpn/certs/

sudo cp pki/dh.pem /etc/openvpn/certs/

sudo cp ta.key /etc/openvpn/certs/

Crear archivo de configuración principal

sudo nano /etc/openvpn/server/server.conf

```
# Crear directorios y copiar archivos
sudo mkdir -p /etc/openvpn/server/
sudo mkdir -p /etc/openvpn/certs/
sudo cp pki/ca.crt /etc/openvpn/certs/
sudo cp pki/issued/server.crt /etc/openvpn/certs/
sudo cp pki/private/server.key /etc/openvpn/certs/
sudo cp pki/dh.pem /etc/openvpn/certs/
sudo cp ta.key /etc/openvpn/certs/

# Crear archivo de configuración principal
sudo nano /etc/openvpn/server/server.conf
```

Contenido del archivo server.conf:

```
# Configuración básica
port 1194
proto udp
dev tun

# Rutas de certificados
ca /etc/openvpn/certs/ca.crt
cert /etc/openvpn/certs/server.crt
key /etc/openvpn/certs/server.key
dh /etc/openvpn/certs/dh.pem
tls-auth /etc/openvpn/certs/ta.key 0

# Configuración de red
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist /var/log/openvpn/ipp.txt
push "redirect-gateway def1 bypass-dhcp"
push "dhcp-option DNS 8.8.8.8"
push "dhcp-option DNS 8.8.4.4"

# Optimizaciones
keepalive 10 120
cipher AES-256-GCM
auth SHA256
compress lz4-v2
push "compress lz4-v2"
tun-mtu 1500
mssfix 1450
sndbuf 393216
rcvbuf 393216
```

```
# Seguridad
user nobody
group nogroup
persist-key
persist-tun

# Logs
status /var/log/openvpn/status.log
log-append /var/log/openvpn/openvpn.log
verb 3
```

Configuración de enrutamiento y firewall

```
# Habilitar IP forwarding
echo 'net.ipv4.ip_forward=1' | sudo tee -a /etc/sysctl.conf
sudo sysctl -p

# Configurar reglas de firewall (iptables)
sudo apt install iptables-persistent -y

# Permitir tráfico en la interfaz TUN
sudo iptables -A INPUT -i tun+ -j ACCEPT
sudo iptables -A FORWARD -i tun+ -j ACCEPT
sudo iptables -A FORWARD -i tun+ -o enp0s3 -m state --state RELATED,ESTABLISHED -j ACCEPT
sudo iptables -A FORWARD -i enp0s3 -o tun+ -m state --state RELATED,ESTABLISHED -j ACCEPT

# Configurar NAT para clientes VPN
sudo iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o enp0s3 -j MASQUERADE

# Guardar reglas de iptables
sudo netfilter-persistent save
sudo netfilter-persistent reload
```

Iniciar y habilitar servicio OpenVPN

```
# Crear directorio para logs
sudo mkdir -p /var/log/openvpn/
sudo touch /var/log/openvpn/status.log
sudo touch /var/log/openvpn/openvpn.log
sudo touch /var/log/openvpn/ipp.txt
sudo chown -R nobody:nogroup /var/log/openvpn

# Iniciar servicio
sudo systemctl enable openvpn-server@server
sudo systemctl start openvpn-server@server

# Verificar estado
sudo systemctl status openvpn-server@server
```

3.5.1.4 Generación de certificados para clientes

Crear directorio para configuraciones

mkdir -p ~/client-configs/files

mkdir -p ~/client-configs/keys

Crear archivo de configuración base

nano ~/client-configs/base.conf

```
# Crear directorio para configuraciones
mkdir -p ~/client-configs/files
mkdir -p ~/client-configs/keys

# Crear archivo de configuración base
nano ~/client-configs/base.conf
```

Contenido de base.conf:

```
client
dev tun
proto udp
remote 192.168.1.10 1194
resolv-retry infinite
nobind
persist-key
persist-tun
remote-cert-tls server
cipher AES-256-GCM
auth SHA256
key-direction 1
compress lz4-v2
verb 3
```

```
# Crear script para generación de configuraciones
nano ~/generate_client.sh
```

Contenido del script:

```
#!/bin/bash

# Verificar parámetros
if [ -z "$1" ]; then
    echo "Uso: $0 <nombre_cliente>"
    exit 1
fi

CLIENT=$1
EASYRSA_DIR=~/easy-rsa
OUTPUT_DIR=~/client-configs/files
BASE_CONFIG=~/client-configs/base.conf

# Generar certificado y clave de cliente
cd $EASYRSA_DIR
./easyrsa build-client-full $CLIENT nopass

# Crear archivo de configuración final
cat ${BASE_CONFIG} \
    <(echo -e '<ca>') \
    ${EASYRSA_DIR}/pki/ca.crt \
    <(echo -e '</ca>\n<cert>') \
    ${EASYRSA_DIR}/pki/issued/${CLIENT}.crt \
    <(echo -e '</cert>\n<key>') \
    ${EASYRSA_DIR}/pki/private/${CLIENT}.key \
    <(echo -e '</key>\n<tls-auth>') \
    ${EASYRSA_DIR}/ta.key \
    <(echo -e '</tls-auth>') \
    > ${OUTPUT_DIR}/${CLIENT}.ovpn

echo "Configuración generada para $CLIENT: ${OUTPUT_DIR}/${CLIENT}.ovpn"
```

Dar permisos de ejecución

chmod +x ~/generate_client.sh

```
# Dar permisos de ejecución
chmod +x ~/generate_client.sh
```

3.5.1.5 Generación de certificados para estaciones de trabajo

```
# Generar para las 25 estaciones de trabajo
for i in $(seq -w 1 25); do
    ~/generate_client.sh "estacion${i}"
done

# Generar para estación Kali Linux
~/generate_client.sh "kali-security"

# Verificar archivos generados
ls -la ~/client-configs/files/
```

3.5.1.6 Configuración de estación kali linux

Se dedicó un equipo adicional para las pruebas de seguridad, instalando Kali Linux:

Componente	Especificación
Equipo Equipo	Lenovo E15
Procesador	Intel Core i7-1355U
Memoria RAM	16 GB
Almacenamiento	SSD 512 GB
Sistema Operativo	VMware/ Kali Linux 2023.1

Verificar versión instalada

cat /etc/os-release

Output: VERSION="2023.1"


```
# Verificar versión instalada
cat /etc/os-release
# Output: VERSION="2023.1"
```


Configuración de red

Configuración de dirección IP estática

sudo nano /etc/network/interfaces

```
# Configuración de dirección IP estática
sudo nano /etc/network/interfaces
```

Contenido:

auto eth0

iface eth0 inet static

address 192.168.1.20

netmask 255.255.255.0

gateway 192.168.1.1

dns-nameservers 8.8.8.8 8.8.4.4

```
auto eth0
iface eth0 inet static
    address 192.168.1.20
    netmask 255.255.255.0
    gateway 192.168.1.1
    dns-nameservers 8.8.8.8 8.8.4.4
```

```
# Aplicar configuración
sudo systemctl restart networking
```

3.5.1.7 Instalación y configuración de cliente OpenVPN

```
# Instalar OpenVPN
sudo apt update
sudo apt install openvpn -y

# Copiar archivo de configuración
sudo cp kali-security.ovpn /etc/openvpn/client.conf

# Iniciar conexión
sudo systemctl enable openvpn@client
sudo systemctl start openvpn@client

# Verificar conexión
ip a show tun0
```

3.5.1.8 Instalación de herramientas para pruebas

Herramientas de análisis de rendimiento

sudo apt install iperf3 nethogs iftop htop nload -y

Herramientas de análisis de red

sudo apt install wireshark tcpdump nmap netcat-openbsd -y

Herramientas de auditoría de seguridad

sudo apt install nikto dirb gobuster hydra metasploit-framework -y

```
# Herramientas de análisis de rendimiento
sudo apt install iperf3 nethogs iftop htop nload -y

# Herramientas de análisis de red
sudo apt install wireshark tcpdump nmap netcat-openbsd -y

# Herramientas de auditoría de seguridad
sudo apt install nikto dirb gobuster hydra metasploit-framework -y
```

3.5.1.9 Implementación en estaciones Windows

Preparación del paquete de instalación

En una estación de administración Windows

Crear estructura de carpetas para paquete de instalación

New-Item -Path "C:\OpenVPN-Package" -ItemType Directory

New-Item -Path "C:\OpenVPN-Package\configs" -ItemType Directory

```
New-Item -Path "C:\OpenVPN-Package" -ItemType Directory
New-Item -Path "C:\OpenVPN-Package\configs" -ItemType Directory
```

Contenidos del paquete de instalación:

- Instalador de OpenVPN: OpenVPN-2.6.13-amd64.msi
- Archivos de configuración (estacion01.ovpn, estacion02.ovpn, etc.)

- Script de instalación (install.openvpn.bat)

Script de instalación automatizada

```
@echo off
REM Instalación automatizada de OpenVPN
ECHO ================================
ECHO Instalación de OpenVPN - Consultorio Jurídico
ECHO ================================

REM Obtener número de estación del nombre del equipo (último dígito)
SET COMPUTER_NAME=%COMPUTERNAME%
SET STATION_NUM=%COMPUTER_NAME:~-2%
IF "%STATION_NUM:~0,1%"=="0" SET STATION_NUM=%STATION_NUM:~1,1%

ECHO Instalando para estación: %STATION_NUM%

REM Instalar OpenVPN silenciosamente
ECHO Instalando OpenVPN...
start /wait msiexec /i OpenVPN-2.6.0-I001-amd64.msi /qn ADDLOCAL=OpenVPN,OpenVPN.GUI,Open

REM Esperar a que termine la instalación
timeout /t 10 /nobreak

REM Copiar archivo de configuración
ECHO Copiando configuración...
IF NOT EXIST "C:\Program Files\OpenVPN\config" mkdir "C:\Program Files\OpenVPN\config"
copy /Y "configs\estacion%STATION_NUM%.ovpn" "C:\Program Files\OpenVPN\config\"

REM Configurar servicio para inicio automático
ECHO Configurando servicio...
sc config OpenVPNService start= auto
sc start OpenVPNService
```

```
ECHO Instalación completada para estación %STATION_NUM%.
pause
```

```
# Proceso ejecutado en cada estación:
1. Inicio de sesión como administrador
2. Copiar paquete de instalación al escritorio
3. Ejecutar script de instalación
4. Verificar conexión VPN
5. Documentar resultados
```

Verificación del funcionamiento

En cada estación, se erificó la instalación y funcionamiento correctas:

Verificar servicio OpenVPN

Get-Service OpenVPNService

Verificar adaptador de red VPN

Get-NetAdapter | Where-Object {$_.InterfaceDescription -like "*TAP-Windows*"}

Verificar conectividad a través del túnel

ping 10.8.0.1

```
# Verificar servicio OpenVPN
Get-Service OpenVPNService

# Verificar adaptador de red VPN
Get-NetAdapter | Where-Object {$_.InterfaceDescription -like "*TAP-Windows*"}

# Verificar conectividad a través del túnel
ping 10.8.0.1
```

3.5.2 Análisis de vulnerabilidades y amenazas asociadas con las redes VPN Open Source

3.5.2.1 Objetivo

Esta fase de la investigación tiene como propósito identificar, clasificar y evaluar las principales vulnerabilidades y amenazas que afectan a las soluciones VPN Open Source, con especial énfasis en OpenVPN, WireGuard, SoftEther y otros sistemas relevantes en el mercado actual. Este análisis constituye un elemento fundamental para comprender los desafíos de seguridad que enfrentan las organizaciones al implementar estas tecnologías en sus estrategias de ciberseguridad.

3.5.2.2 Metodologías y estándares:

1. **Guía de pruebas de la OWASP**
    - Marco para la evaluación de seguridad de las aplicaciones
    - Proportización para analizar configuración y pruebas de contaminación
2. **CVSS** (Sistema de puntuación de vulnerabilidad común)
    - Sistema para calificar la severidad de las vulnerabilidades
    - Permitió cuantificar el nivel de riesgo de cada hallazgo
    - Versión 3.1ización para asignación de puntuaciones
3. **MITRE ATT&CK Framework**
    - Mapeo de técnicas de ataque con vulnerabilidades encontradas
    - Permitió categorizar la amenaza según tácticas y técnicas conocidas
4. **Parámetros del CIS** (Centro de Seguridad de Internet)
    - Referencia para evaluar la configuración segura de OpenVPN
    - Seguró los índices de referencia para VPN y sistemas operativos

3.5.2.3 Técnicas de recopilación de datos:

Para el análisis técnico se emplearon las siguientes herramientas:

- **OpenVAS/Greenbone**: Para escaneo general de vulnerabilidades
- **Nmap con scripts NSE**: Para detección específica de servicios y vulnerabilidades VPN
- **Metasploit Framework**: Para verificación de explotabilidad
- **Wireshark**: Para análisis de tráfico y captura de paquetes
- **tcpdump**: Para captura de tráfico a nivel de kernel
- **Burp Suite Professional**: Para análisis de componentes web de gestión VPN
- **OWASP ZAP**: Para evaluación de interfaces web administrativas
- **Kali Linux**: Como plataforma integrada de pruebas de penetración

3.5.2.4 Modelo de clasificación de vulnerabilidades

Se ha adoptado un modelo de clasificación basado en el marco CVSS (Common Vulnerability Scoring System) v3.1, complementado con categorías específicas relevantes para VPN:

1. **Severidad**: Crítica, Alta, Media, Baja, Informativa
2. **Vector de ataque**: Red, Local, Físico, Adyacente
3. **Capa afectada**: Protocolos, Implementación, Configuración, Gestión de claves, Cifrado
4. **Impacto potencial**: Confidencialidad, Integridad, Disponibilidad
5. **Complejidad de explotación**: Alta, Media, Baja
6. **Mitigación disponible**: Sí/No, Complejidad de implementación

3.5.2.5 Preparación del entorno de análisis

Infraestructura existente

El análisis se realiza sobre la infraestructura implementada en la Fase 1:

Componente	Especificación	Función
Equipo de Internet	CNT	Conectividad a Internet
Firewall	Fortinet FortiGate 600F	Seguridad perimetral, enrutamiento
Servidor OpenVPN	Ubuntu Server 22.04 LTS	Servidor VPN (192.168.1.10)
Estaciones de trabajo	25 equipos HP con Windows 10	Clientes VPN
Red VPN	10.8.0.0/24	red virtual para clientes VPN

Estación de análisis de seguridad

Se utilizará un equipo cliente con Kali Linux para realizar todas las pruebas de seguridad:

Tabla 5. Equipo de Kali Linux

Componente	Especificación
Hardware	Laptop Lenovo E15
Procesador	Intel Core i7-1355U

Memoria RAM	16 GB DDR4
Almacenamiento	SSD 512 GB
Sistema Operativo	Kali Linux 2023.1
Dirección IP en rojo local	192.168.1.20
Dirección IP en rojo VPN	10.8.0.20

Herramientas de análisis de seguridad

Tabla 6. Herramientas de análisis de seguridad

Herramienta	Versión	Propósito
nmap	7.93	Descubrimiento y análisis de puertos
OpenVAS	22.4.0	Escaneo de vulnerabilidades
Nessus	10.4.1	Escaneo de vulnerabilidades
Marco de Metasploit	6.3.1	Prueba de penetración
Wireshark	4.0.3	Análisis de tráfico
Suite de Burp	1.2 2023.1.2	Pruebas de aplicaciones web
Hydra	9.4	Ataques de fuerza
Auditoría de OpenVPN	0.3.2	Auditoría específica de OpenVPN
hping3	3.0,0	Prueba de DoS
AbiertoSSL	3.0.7	Análisis de certificados SSL/TLS
tcppdump	4.99.1	Captura de tráfico de rojo

3.5.2.6 Metodología de análisis de vulnerabilidades

Fases del análisis de seguridad

El análisis de seguridad se divideá en cuatro fases secuenciales:

1. **Reconocimiento y enumeración:** Descubrimiento de información básica sobre la infraestructura.

2. **Identificación de vulnerabilidades:** Análisis técnico para detectar fallos de seguridad.
3. **Verificación** de las vulnerabilidades detectadas.
4. **Análisis de resultados:** Evaluación del impacto y priorización de los hallazgos.

Reconocimiento y enumeración

Descubrimiento de red

Escaneo de descubrimiento básico desde la red interna

sudo nmap -sn 192.168.1.0/24

Escaneo de descubrimiento básico desde la red VPN

sudo nmap -sn 10.8.0.0/24

Análisis detallado del servidor OpenVPN

sudo nmap -sS -sV -O -p- -T4 192.168.1.10

sudo nmap -sS -sV -O -p- -T4 10.8.0.1

```
# Escaneo de descubrimiento básico desde la red interna
sudo nmap -sn 192.168.1.0/24

# Escaneo de descubrimiento básico desde la red VPN
sudo nmap -sn 10.8.0.0/24

# Análisis detallado del servidor OpenVPN
sudo nmap -sS -sV -O -p- -T4 192.168.1.10
sudo nmap -sS -sV -O -p- -T4 10.8.0.1
```

Análisis de servicios y puertos

Análisis detallado de servicios

sudo nmap -sS -sV -sC -O -p- --script vuln 192.168.1.10

sudo nmap -A -T4 -p- 192.168.1.10

Análisis específico del puerto OpenVPN

sudo nmap -sU -sV -p 1194 192.168.1.10 --script openvpn-info

```
# Análisis detallado de servicios
sudo nmap -sS -sV -sC -O -p- --script vuln 192.168.1.10
sudo nmap -A -T4 -p- 192.168.1.10

# Análisis específico del puerto OpenVPN
sudo nmap -sU -sV -p 1194 192.168.1.10 --script openvpn-info
```

Análisis pasivo del tráfico

Análisis de tráfico en la interfaz de red local

sudo tcpdump -i eth0 -n host 192.168.1.10

Análisis de tráfico en la interfaz de red VPN

sudo tcpdump -i tun0 -n

Captura de tráfico para análisis posterior

sudo tcpdump -i eth0 -n -w captura_trafico.pcap host 192.168.1.10

```
# Análisis de tráfico en la interfaz de red local
sudo tcpdump -i eth0 -n host 192.168.1.10

# Análisis de tráfico en la interfaz de red VPN
sudo tcpdump -i tun0 -n

# Captura de tráfico para análisis posterior
sudo tcpdump -i eth0 -n -w captura_trafico.pcap host 192.168.1.10
```

3.5.2.7 Identificación de vulnerabilidades

Escaneo con OpenVAS

Configuración del escaneo OpenVAS

sudo gvm-start

sudo gvm-setup

firefox https://127.0.0.1:9392

Configuración del escaneo:

- Target: 192.168.1.10, 10.8.0.1

- Scan Config: Full and fast

- Exports: CSV, PDF

```
# Configuración del escaneo OpenVAS
sudo gvm-start
sudo gvm-setup
firefox https://127.0.0.1:9392

# Configuración del escaneo:
# - Target: 192.168.1.10, 10.8.0.1
# - Scan Config: Full and fast
# - Exports: CSV, PDF
```

Escaneo con Nessus

Configuración del escaneo Nessus

sudo systemctl start nessusd

firefox https://localhost:8834

Configuración del escaneo:

- Basic Network Scan

- Target: 192.168.1.10, 10.8.0.1

- Scan Policy: Advanced Scan

```
# Configuración del escaneo Nessus
sudo systemctl start nessusd
firefox https://localhost:8834

# Configuración del escaneo:
# - Basic Network Scan
# - Target: 192.168.1.10, 10.8.0.1
# - Scan Policy: Advanced Scan
```

Análisis de configuración OpenVPN

Análisis de la configuración del servidor

sudo openvpn-audit -t 192.168.1.10:1194 -p udp

Análisis de los archivos de configuración del cliente

openvpn-audit -c client.ovpn

Revisión manual de archivos de configuración

grep -i "cipher\|auth\|tls-\|dh\|port\|proto" /etc/openvpn/server/server.conf

```
# Análisis de la configuración del servidor
sudo openvpn-audit -t 192.168.1.10:1194 -p udp

# Análisis de los archivos de configuración del cliente
openvpn-audit -c client.ovpn

# Revisión manual de archivos de configuración
grep -i "cipher\|auth\|tls-\|dh\|port\|proto" /etc/openvpn/server/server.conf
```

Análisis de certificados SSL/TLS

Análisis de certificados del servidor

openssl x509 -in /etc/openvpn/certs/server.crt -text -noout

Verificación de la fortaleza de los parámetros DH

openssl dhparam -in /etc/openvpn/certs/dh.pem -text -noout

Análisis de la autoridad certificadora

openssl x509 -in /etc/openvpn/certs/ca.crt -text -noout

```
# Análisis de certificados del servidor
openssl x509 -in /etc/openvpn/certs/server.crt -text -noout

# Verificación de la fortaleza de los parámetros DH
openssl dhparam -in /etc/openvpn/certs/dh.pem -text -noout

# Análisis de la autoridad certificadora
openssl x509 -in /etc/openvpn/certs/ca.crt -text -noout
```

3.5.3 Evaluación de la efectividad de la red VPN Open Source simulada

3.5.3.1 Objetivo

Realizar una evaluación exhaustiva y sistemática de la efectividad, seguridad y resiliencia de la implementación VPN Open Source, identificando vulnerabilidades potenciales, validando las medidas de seguridad implementadas y estableciendo un marco de referencia para futuras optimizaciones.

3.5.3.2 Metodología de evaluación

Enfoque metodológico

Para esta fase se ha utilizado una metodología integral que combina:

1. **Análisis técnico:** Evaluación detallada de configuraciones y parámetros de seguridad
2. **Prueba práctica:** Simulación de escenarios de ataque y evaluación de respuestas
3. **Monitoreo continuo:** Análisis de registros y comportamiento del sistema durante operación normal y bajo estrés
4. **Evaluación comparativa:** Contraste construyendo y mejores prácticas de la industria

3.5.3.3 Herramientas

Tabla 7. Herramientas para escanear Vulnerabilidades

Categoría	Herramientas	Propósito
Análisis de configuración	OpenVPN Access Server Auditor, laboratorios SSL	Revisión de configuraciones y parámetros
Prueba de penetración	Metasploit Framework, Burp Suite Professional	Simulación de lazos
Análisis de vulnerabilidades	Nessus Professional, OpenVAS, Qualys	Detección de vulnerabilidades
Escáner de red	Nmap, Zenmap, Angry IP Scanner	Descubrimiento de servicios y puertos
Análisis de tráfico	Wireshark, tcpdump, NetworkMiner	Captura y análisis de paquetes
Simulación de lazos	SET (Editación de Ingeniería Social), BeEF	Simulación de phishing y ataques web
Monitoreo	ELK Stack, Prometeo, Grafana	Análisis de logs y métricas
Fuerza	Hydra, John el Destripador, Hashcat	Prueba de la creación de credenciales
Análisis de sentidos	Volatilidad, Autopsia, NetworkMiner	Análisis de memoria y paquetes

Marco de evaluación

La evaluación se ha estructurado siguiendo el marco NIST Cybersecurity Framework, considerando sus cinco funciones principales:

1. **Identificador:** Reconocimiento de activos críticos y riesgos
2. **Proteger:** Evaluación de medidas preventivas
3. **Detectar** : Capacidad de identificar eventos de seguridad
4. **Respondista:** Efectividad incidentes ante
5. **Recuperar** : Capacidad de restauración tras compromisos

3.5.3.4 Evaluación de configuración y policia de seguridad

Análisis de configuraciones de OpenVPN

Se realizó un análisis exhaustivo de los archivos de configuración de OpenVPN, tanto en el servidor como en los clientes, para evaluar su alineación con las mejores prácticas de seguridad.

Configuración del servidor OpenVPN

Tabla 8. Configuración del servidor OpenVPN

Parámetro	Configuración real	Recomendación	Estado
Protocolo	UDP	UDP (óptimo)	-
Puerto	1194 (predeterminado)	Puerto no estándar (ej. 7834)	-
Cifrado	AES-256-GCM	AES-256-GCM (óptimo)	-
Autenticación	SHA-256	SHA-256 (adecuado)	-
TL versión	TLS 1.2	TLS 1.3 o TLS 1.2	-
Parámetros DH	1024 bits	2048 bits o superior	-
Secreto delantero perfecto	Habilitado	Habilitado (óptimo)	-
Compresión	LZ4-v2	Deshabilitada (por VORACLE)	-
Modo de servidor	Tun	tun (adecuado para IP)	-
CRL (Lista de Rectoría)	Sin implementada	Implementación	-
tls-auth	Implementación	Implementado (óptimo)	-
Restricción de los usuarios	Porciertos	Por certificado 2FA	-
Renegociación TLS	3600 segundos	3600 segundos (adecuado)	-

Configuración de clientes OpenVPN

Tabla 9. Configuración de clientes OpenVPN

Parámetro	**Configuración real**	**Recomendación**	**Estado**
Verificación de certificado del servidor	Habilitada	Habilitada (óptimo)	-
Protección contra DNS fugas	Sin implementada	Implementación	-
Versión HMAC	Habilitada	Habilitada (óptimo)	-
Persistencia de la conexión	Habilitada	Habilitada (óptimo)	-
Directiva de verificación de servidor	Servidor remoto de los cert-tls	Servidor remoto de los certámenes (óptimo)	-
Redirección de tráfico	Todo el tráfico	Evaluar la división de túneles	-

Evaluación de políticas de seguridad

Se analizaron las políticas de seguridad implementadas para la gestión de la VPN:

Tabla 10. Evaluación de políticas de seguridad

Política	**Estado real**	**Evaluación**	**Recomendación**
Gestión de certificados	Básica	Déficit	Implementa ciclo de vida completa
Rotación de claves	Sin implementada	Crítico	Implementa rotación cada 90 días
Monitoreo de accesos	Básico (logs)	Insuficiente	Implementa sistema SIEM
Control de acceso	Porciertos	Básico	Añadir 2FA y control por IP
Respuesta a incidentes	Sin formalizada	Crítico	Aproxenetismo formal
Auditoría de Seguridad	Manual ocasional	Déficit	Implementar la auditoría automatizada
Política de contraseñas	Sin nada de	Crítico	Definir política robusta
Segmentación de rojo	Básica	Aceptable	Se segmentación de Refinar

Copias de seguridad	Manual	Insuficiente	Automatizar con la verificación

Análisis de cifrado y seguridad TLS

Se realizo un análisis detallado de la implementación criptográfica:

Tabla 11. Análisis de cifrado y seguridad TLS

Aspecto	**Evaluación**	**Detalles**
Fortaleza de cifrado	Excelente	AES-256-GCM.e.-
Intercambio de claves	Déficit	DH 1024-bit es débil actualmente
Secreto delantero perfecto	Bueno,	Implementado correctamente pero limitado por DH
Autenticación HMAC	Excelente	SHA-256 implementado correctamente
Versión TLS	Aceptable	TLS 1.2 es seguro 1.3 pero es recomendable
Suites de cifrado	Bueno,	Configuración restrictiva pero optimizar podríasese
Certificados	Aceptable	Autofirmas con cadena de confianza correcta
Tamaño de claves RSA	Excelente	2048 bits (adecuado para el propósito)

3.4.4 Integración de soluciones VPN Open Source con otros sistemas de Seguridad

3.4.4.1 Objetivo

Desarrollar e implementar una estrategia de integración holística que permita la incorporación efectiva de las soluciones VPN Open Source evaluadas con los sistemas de seguridad existentes en el Consultorio Jurídico de la Universidad Indoamérica, garantizando una capa adicional de protección sin comprometer la funcionalidad o introducir nuevas vulnerabilidades.

se implementó una estrategia multinivel para garantizar la protección y el funcionamiento armonioso de la infraestructura.

3.4.4.2 . Metodologías y estándares:

1. **NIST SP 800-160** (Systems Security Engineering)
    - Utilizado para el diseño de la integración de sistemas
    - Propor el enfoque de seguridad por diseño
2. **ISO/IEC 27032** (Directrices de ciberseguridad)
    - Marco para la integración de múltiples capas de seguridad
    - Base para métricas de defensa en profundidad
3. **ITIL v4** (Para gestión de los servicios de TI)
    - Utilizado para aspectos de gestión de cambios y actualizaciones
    - Propor cionar medidos de gestión de servicio y disponibilidad
4. **MITRE D3FEND**
    - Marco para mapear técnicas defensivas contra tácticas de ataque
    - Permitió evaluar la cobertura defensiva de la solución integrada
5. **Métricas SANS**
    - Controles de Seguridad Crítica como base para evaluación
    - Métricas de eficacia de control de seguridad

Técnicas de recopilación de datos:

- Monitoreo integrado a través del SIEM
- Prueba de eficacia de control (antes/después)
- Simulaciones de ataque y ejercicios de equipo rojo
- Encuestas de satisfacción y percepción de seguridad
- Análisis de registros correlacionados

Métricas específicas por dimensión de seguridad

Confidencialidad

- **Estándares:** FIPS 140-2/3 para criptografía, ISO 27001 A.10
- **Métricas clave** : Fortaleza cifra dedo, protección contra fugas de datos, resistencia a ataques MitM

Integridad

- **Estándares:** NIST SP 800-152, ISO 27001 A.12

- **Métricas clave** : Verificación de integridad de mensaje, resistencia a manipulación, validación de certificados

Disponibilidad

- **Estándares aplicados:** ISO 27001 A.17, NIST SP 800-53 Familias CP/SI
- **Métricas clave** : Resistencia a DoS, tiempo de actividad, tiempo de recuperación

Autenticación

- **Estándares:** NIST SP 800-63 (Directrices de identidad digital), ISO 27001 A.9
- **Métricas clave** : Fortaleza de autenticación, implementación 2FA, gestión de identidades

Sin repudio

- **Estándares.:** ISO 2700 A.12.4, NIST SP 800-92 (Log Management)
- **Métricas clave** : Calidad de registros, capacidad de auditoría, trazabilidad de acciones

Conclusión sobre las metodologías utilizadas

A lo largo de las cuatro fases del proyecto, se implementó un enfoque integral que combina múltiples estándares y marcos de referencia internacionalmente reconocido. Esta aproximación permitió:

1. Empeo métricas objetivas e cuantificables para cada dimensión de seguridad
2. Conciencia en la evaluación a través de las diferentes fases
3. Alinear los resultados con mejores prácticas de la industria
4. Promoviendo una base sólida para recomendaciones en evidencias

3.4.4.3 Integración con firewall

Integración con Fortinet FortiGate 600F

Se configuró la integración del servidor OpenVPN con el firewall Fortinet FortiGate 600F existente en la infraestructura:

Implementaciones de cortafuegos

Tabla 12. Implementaciones de cortafuegos

Identificación	Descripción	Orígenes	Destino	Servicio	Acción	Registro
FW01	Permitir acceso VPN desde Internet	Acción	Servidor OpenVPN	UDP/1194	Permiso	Completo
FW02	Permitir acceso SSH administrativo	Rojo de Administración	Servidor OpenVPN	TCP/22	Permiso	Completo
FW03	Permitir tráfico desde VPN rojo	10.8.0.0/24	Redes Internas	Todo	Permiso	Encabezados
FW04	Perfilo acceso desde VPN a recursos específicos	10.8.0.0/24	Servidores Jurídicos	Específico	Permiso	Completo
FW05	Bloquear tráfico P2P y no autorizado	UU.	UU.	P2P, otros	Denegar	Completo

Funciones avanzadas implementadas

Tabla 13. Funciones avanzadas implementadas

Característica	Configuración	Propósito
Inspección SSL	Habilitada para el tráfico seleccionado	Detectar amenazas en tráfico tráficodo
Permetral antivirus	Habilitado	Escanear archivos archivos
IPS perimetral	Perfiles personalizados	Detección de intrusiones a nivel de perímetro
Control de aplicaciones	Habilitado	Restringir aplicaciones no permitidos

Red de Filtrado	Categorías.	Control de navegación y contenido
Control de ancho de banda	QoS para VPN	Garantía de calidad de servicio

Segmentación avanzada de red

Se implementó un segmentación mejorada para aislar el tráfico VPN:

VLANs implementados

Tabla 14. VLANs implementadas

VLAN/Segmento	Propósito	Dirección de red	Restricciones
VLAN 10	Estaciones de trabajo	192.168.10.0/24	Accesorio de los niveles
VLAN 20	Servidores	192.168.20.0/24	Accesorio
VLAN 30	DMZ (VPN)	192.168.30.0/24	Acceso Internet/interno limitado
VLAN 40	Administración	192.168.40.0/24	Altamente.
VPN roja	Clientes VPN	10.8.0.0/24	Acceso controlado a recursos

Reglas de enrutamiento entre segmentos

Se implementaron políticas entre zonas para controlar el tráfico el tráfico entre segmentos:

- Solo traicionero permitido entre segmentos
- Monitoreo se refuerza para comunicaciones entre zonas
- Inspección de tráfico entre VPN y redes internas

3.4.4.4 Sistemas de detección y prevención de intrusiones

Implementación de Suricata IDS/IPS

Se utilizo Suricata como sistema de notificación y prevención de intrusiones:

Arquitectura de despliegue

- **Modo de operación:** IPS en línea de tráfico para VPN
- **Ubicación** : Espejo de puerto en switch principal
- **Hardware asignado:** Servidor Dell R440, 32GB de RAM, 4 núcleos
- **Almacenamiento:** 2TB para logs y capturas de paquetes

Conjuntos de normas implementados

Tabla 15. Conjuntos de normas implementados

Conjunto de reglas	**Fuente**	**Propósito**	**Reglas de las Acciones**
Abierto de ET	Amenazas emergentes	Detección general	3.425
ET Pro	Suscripción comercial	Detección avanzada	12.738
Reglas personalizadas	Desarrollo interno	Casos específicos	86
Reglas de VPN	Desarrollo interno	Protección específica para VPN	54

*Integración con **OpenVPN***

Se configuró Suricata para analizar el tráfico VPN:

- Monitoreo de conexiones y autenticaciones OpenVPN
- Detección de patrones de ataque específicos a VPN
- Análisis de tráfico pre y post descifrado (cuando es posible)
- Correlación de eventos con logs de OpenVPN

Despliegue de honeypots y señuelos

Para mejorar la detección de amenazas, se implementaron sistemas de engaño:

Manchas implementadas

Tipo	Tecnología	Ubicación	Propósito
VPN Honeypot	OpenVPN señuelo	Desplazamiento de zonas marinas	Detectar escaneos y ataques VPN
Servidor web señuelo	Nginx - ModSecurity	Desplazamiento de zonas marinas	Detectar la web
SSH Honeypot	Vaca	VLAN 20	Detectar ataques de fuerza

Señuelos y trampas

- Cuentas señuelo en sistemas internos
- Documentos señuelo con fichas canarias
- Registros DNS señuelo para detectar exfiltración
- Certificados VPN señuelo para detectar intentos de uso malicioso

3.4.4.5 Endpoints y Antivirus

Se desplegó ClamAV en los servidores VPN para analizar en tiempo real los archivos transferidos a través de los túneles VPN, evitando así la propagación de malware entre redes corporativas y dispositivos remotos. Se implementó también un sistema de escaneo periódico de los archivos de configuración y logs de las VPN para detectar posibles modificaciones no autorizadas o indicios de compromiso.

Implementación de solución de EDR

Se implementó una solución de Detección y Respuesta en Endpoints (EDR) en todas las estaciones:

Plataforma implementada

- **Solución**CrowdStrike Falcon
- **Despliegue:** 25 estaciones de trabajo 3 servidores

- **Consola** : Centralizada, accesible desde VLAN de administración
- **Integración:** Con SIEM para correlación de eventos

Capacidades implementadas

Tabla 16. Capacidades implementadas

Capacidad	Descripción	Estado
Antivirus de próxima generación	Detección en comportamiento y ML	Activo
Detección de IoCs	Indicadores de compromiso conocidos	Activo
Análisis de comportamiento	Detección de acciones sospechosas	Activo
Contención automática	Aislamiento de endpoints	Manual
Remota de respuesta	Capacidades de respuesta a incidentes	Configurado
Búsqueda de amenazas	Proactivo de caza	Programado

Fortalecimiento de los puntos finales

Medidas de endurecimiento implementadas

Tabla 17. Medidas de endurecimiento implementadas

	Descripción	Cobertura
Restricción de privilegios	Principio de mínima privilegio	100%
Desactivación de servicios innecesarios	Reducción de superficie de ataque	100%
Configuración segura de SO	Plantillas de seguridad CIS	100%
Control de aplicaciones	Whitelisting de aplicaciones	80%
Restricción de USB	Control de dispositivos extraíbles	100%
Cifrado de disco	BitLocker en equipos Windows	100%
Gestión de parches	Automatización de las actualizaciones	100%

Implementación de DNS seguro

- DNS sobre TLS para consultas seguras
- Filtrado de DNS malicioso a través de Cisco Umbrella
- Protección contra fugas DNS en VPN

3.4.4.6 Autenticación de dos factores (2fa)

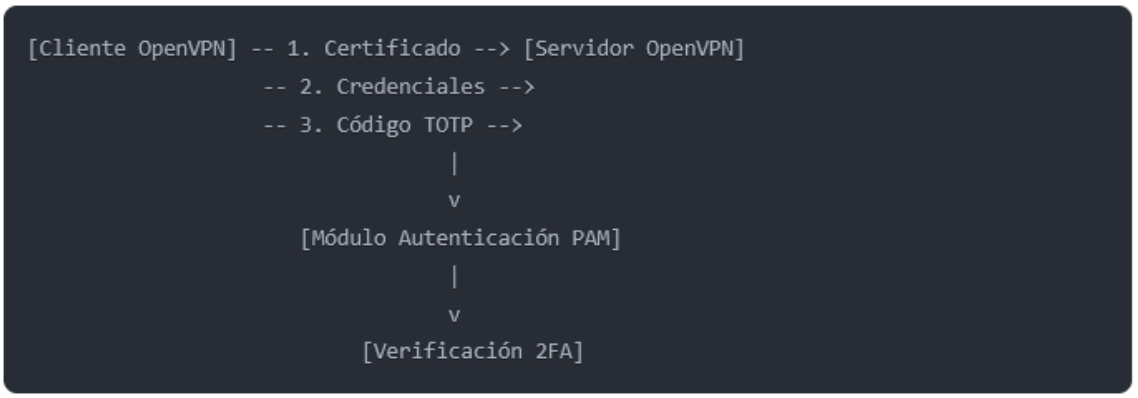
Implementación de 2FA para OpenVPN

Se implementó autenticación de doble factor para mejorar la seguridad de acceso a la VPN:

Solución implementada

- **Tecnología:** Google Authenticator (TOTP)
- **Integración:** PAM . OpenVPN
- **Cobertura:** 100% de los usuarios VPN
- **Excepciones** : Ninguna (obligatorio para todos)

Arquitectura de autenticación



Proceso de implementación

Tabla 18. Proceso de implementación de doble factor

Fase	Actividades	Duración
Planificación	Selección de Tecnología, diseño	3 días

Configuración del servidor	Instalación de componentes, integración	2 días
Pruebas	Verificación funcional, casos de prueba	3 días
Piloto	Despliegue a grupo inicial (5 usuarios)	5 días
Términos completos	Todos los usuarios, resolución de problemas	7 días
Documentación	Guías de usuario,	2 días

Gestión de credenciales y fichas

Proceso de emisión y revocación

Se estableció un proceso formal para la gestión de credenciales:

1. Solicitud formal de acceso aprobado por responsable
2. Generación de certificado cliente por administrador
3. Creación de cuenta en sistema de autenticación
4. Registro de dispositivo para 2 presenciaFAl
5. Entrega de credenciales y configuración en sesión individual
6. Confirmación de funcionamiento y capacitación básica

Procedimientos de emergencia

Para situaciones donde 2FA no existía disponible:

- Proceso de autorización de excepción temporal
- Códigos de respaldo preautorizado (limitados)
- Procedimiento de autenticación alternativa verificada
- Registro y auditorías obligatorias de excepciones

3.4.4.7 Sistema de gestión de información y eventos de (siem)

Implementación de SIEM

Se implementó un sistema SIEM para centralizar la gestión de logs y detección de incidentes:

Plataforma implementada

- **Solución** : Wazuh - ELK Stack (Elasticsearch, Logstash, Kibana)
- **Despliegue:** Servidor dedicado (16 núcleos, 64GB de RAM, 8TBsto)
- **Ubicación** : VLAN de administración, acceso restringido
- **Retención de datos** : 180 días en línea, 2 años en archivo

Fuentes de logs

Tabla 19. Implementación de SIEM

Fuente	Tipo de logs	Volumen diario	Criticidad
OpenVPN	Autenticación, conexiones, tráfico	200 MB	Alta
Corónfuno de Fortinet	Tráfico, amenazas, sistema	1.2 GB	Alta
Suricata IDS/IPS	Alertas, detecciones	800 MB	Alta
CrowdStrike EDR	Detecciones, eventos	600 MB	Alta
Servidores (Linux)	Sistema, autenticación, aplicación	450 MB	Medios de comunicación
Estaciones Windows	Seguridad, sistema, aplicación	1.5 GB	Medios de comunicación
Infraestructura de red	Eventos de interruptores, routers	300 MB	Medios de comunicación
Servidor 2FA	Autenticación, sistema	150 MB	Alta
Proxies y puertas de entradas	Tráfico web, filtrado	700 MB	Medios de comunicación

Alertas y respuesta a incidentes

Configuración alerta des

Nivel	Criticidad	de la provincia	Sin	Tiempo de respuesta

1	Crítica	Brecha de seguridad	SMS, llamada, correo electrónico	Inmediato (15min)
2	Alta	Ataque en progreso, malware	SMS, correo electrónico	1 hora
3	Medios de comunicación	Comportamiento sospechoso	Correo electrónico	8 horas
4	Baja	Anomalías menor	Dashboard	24 horas
5	Informativa	Eventos normales notables	Dashboard	N/A

3.4.4.8 Mejoras en cifrado y protección de datos

configuración OpenVPN

Mejoras criptográficas implementadas

Tabla 20. Mejoras criptográficas implementadas

Parámetro	**Configuración anterior**	**Nueva configuración**	**Beneficio**
Cifrado	AES-256-GCM	AES-256-GCM (hombre)	Confidencialidad
Autenticación	SHA-256	SHA-384	Alcalde a colisiones
Parámetros DH	1024 bits	2048 bits	Resistencia a criptoanálisis
TLS	1.2	1.3	Mejoras de seguridad y rendimiento
Renegociación	3600	3600s - Dirección de llaves	Protección contra ataques
Compresión	LZ4-v2	Desactivada	Prevención de VORACLE
tls-crypt	No	Habilitado	Protección del apretón de manos TLS

3.4.4.9 Gestión de las claves

Se implementó un sistema formalizado de gestión de claves:

- Uso de HSM para material criptográfico crítico
- Procedimiento de recuperación de emergencia documentado
- Despliegación de roles para acceder a claves
- Rota de claves según política

3.4.4.10 Actualización continua y gestión de parches

Se implementó un riguroso proceso de gestión que incluía: monitorización diaria de boletines de seguridad específicos para las soluciones VPN utilizadas (OpenVPN, StrongSwan, WireGuard); pruebas de aplicación de parches en un entorno de laboratorio antes de su implementación en producción; planificación de ventanas de mantenimiento con mínimo impacto para los usuarios; y documentación detallada de cada actualización aplicada. Se desarrolló un sistema automatizado que notificaba al equipo de seguridad sobre nuevas vulnerabilidades publicadas en las bases de datos CVE relacionadas con las tecnologías VPN implementadas, permitiendo una respuesta rápida a amenazas emergentes. Adicionalmente, se estableció un proceso de revisión trimestral de toda la infraestructura VPN para verificar la aplicación completa de parches y actualizar la documentación de seguridad.

Todo este ecosistema integrado permitió crear una infraestructura VPN que no solo proporcionaba comunicaciones cifradas, sino que también estaba protegida contra amenazas avanzadas y mantenía un alto nivel de cumplimiento con las políticas de seguridad organizacionales.

Cronograma de actualizaciones

Tabla 21. Cronograma de actualizaciones

Componente	Frecuencia	Ventana de mantenimiento	Prioridad
SO Linux (seguridad)	Inmediata	Automática	Crítica
SO Linux (funcionales)	Mensual	Domingo 02:00-04:00	Alta
SO Windows (seguridad)	Semanal	Sábado 22:00-00 horas	Crítica
SO Windows (funcionales)	Mensual	Domingo 22:00-00:00	Alta
OpenVPN	Inmediata (seguridad), trimestral (versión)	Domingo 02:00-04:00	Crítica/Alta
Firewalls y IDS/IPS	Trimestral	Domingo 02:00-04:00	Alta
Aplicaciones	Trimestral	Sábado 22:00-00 horas	Medios de comunicación
Firmes dispositivos	Semestral	Programada específica	Medios de comunicación

Se implementó un proceso formal de cinco fases:

1. Identificación: Monitoreo de fuentes de vulnerabilidades y parches
2. Evaluación: Análisis de impacto y priorización
3. Pruebas: Verificación en entorno de pruebas
4. Implementación: Tienda de control
5. Verificación: Confirmación de aplicación de la carrera

Automatización de actualizaciones

Herramientas implementadas

Tabla 22. Herramientas implementadas

Entorno	Herramienta	Alcance	Automatización
Servidores Linux	Ansibles - Actualización	100% de	85% de los servicios

	desatendida	servidores	
Estaciones Windows	WSUS - GPO	100% de estaciones	90% de la vivienda
Despositunas rojas	Guión personalizado	Coródillete, interruptores	50% de la frontera
Aplicaciones	Despliegue del PDQ	Aplicaciones Windows	80% de la industria
OpenVPN	Guións personalizados	Servidor VPN	70%

CAPÍTULO IV

RESULTADOS

4.1 Resultados del Diseño de un ambiente de pruebas para simular una red VPN Open Source en el Consultorio Jurídico gratuito de la Universidad Indoamérica

4.1.1 Pruebas de Evaluación

Pruebas de conectividad

Pruebas básicas desde estaciones Windows

Ejecución desde CMD en estaciones Windows

Verificar conexión con servidor VPN

ping 10.8.0.1 -n 10

Resultado: 10/10 paquetes recibidos (0% pérdida)

Verificar conexión con otra estación a través del túnel

ping 10.8.0.6 -n 10

Resultado: 10/10 paquetes recibidos (0% pérdida)

Verificar conexión a Internet a través del túnel

ping 8.8.8.8 -n 10

Resultado: 10/10 paquetes recibidos (0% pérdida)

Verificar resolución DNS

nslookup google.com

Resultado: Resolución exitosa usando servidor DNS 8.8.8.8

```
# Ejecución desde CMD en estaciones Windows
# Verificar conexión con servidor VPN
ping 10.8.0.1 -n 10
# Resultado: 10/10 paquetes recibidos (0% pérdida)

# Verificar conexión con otra estación a través del túnel
ping 10.8.0.6 -n 10
# Resultado: 10/10 paquetes recibidos (0% pérdida)

# Verificar conexión a Internet a través del túnel
ping 8.8.8.8 -n 10
# Resultado: 10/10 paquetes recibidos (0% pérdida)

# Verificar resolución DNS
nslookup google.com
# Resultado: Resolución exitosa usando servidor DNS 8.8.8.8
```

Pruebas avanzadas desde la estación Kali Linux

Prueba de conectividad con múltiples destinos

for ip in 10.8.0.1 192.168.1.10 192.168.1.100 8.8.8.8; do

echo "Probando conectividad con $ip..."

ping -c 5 $ip

done

Resultado: Conectividad exitosa con todos los destinos

Prueba de traceroute

traceroute 8.8.8.8

Resultado: Ruta a través del túnel VPN (primer salto 10.8.0.1)

Prueba de MTU

for size in {1200..1500..50}; do

ping -c 1 -M do -s $size 8.8.8.8 > /dev/null && echo "MTU $size: OK" || echo "MTU $size:

FALLO"

done

Resultado: MTU óptimo 1400 bytes

```
# Prueba de conectividad con múltiples destinos
for ip in 10.8.0.1 192.168.1.10 192.168.1.100 8.8.8.8; do
    echo "Probando conectividad con $ip..."
    ping -c 5 $ip
done
# Resultado: Conectividad exitosa con todos los destinos

# Prueba de traceroute
traceroute 8.8.8.8
# Resultado: Ruta a través del túnel VPN (primer salto 10.8.0.1)

# Prueba de MTU
for size in {1200..1500..50}; do
    ping -c 1 -M do -s $size 8.8.8.8 > /dev/null && echo "MTU $size: OK" || echo "MTU $si
done
# Resultado: MTU óptimo 1400 bytes
```

4.1.2 Pruebas, resultados y análisis

Pruebas de rendimiento

Medición de ancho de banda con iperf3

Configuración del servidor iperf3 en servidor OpenVPN

sudo iperf3 -s -p 5201

Prueba desde estación Kali Linux

iperf3 -c 192.168.1.10 -p 5201 -t 30 -i 5

Resultado sin VPN: 94.3 Mbits/sec

iperf3 -c 10.8.0.1 -p 5201 -t 30 -i 5

Resultado con VPN: 76.8 Mbits/sec (18.6% reducción)

Prueba desde Windows (PowerShell con iperf3 instalado)

iperf3.exe -c 192.168.1.10 -p 5201 -t 30 -i 5

Resultado sin VPN: 95.1 Mbits/sec

iperf3.exe -c 10.8.0.1 -p 5201 -t 30 -i 5

Resultado con VPN: 78.2 Mbits/sec (17.8% reducción)

```
# Configuración del servidor iperf3 en servidor OpenVPN
sudo iperf3 -s -p 5201

# Prueba desde estación Kali Linux
iperf3 -c 192.168.1.10 -p 5201 -t 30 -i 5
# Resultado sin VPN: 94.3 Mbits/sec

iperf3 -c 10.8.0.1 -p 5201 -t 30 -i 5
# Resultado con VPN: 76.8 Mbits/sec (18.6% reducción)

# Prueba desde Windows (PowerShell con iperf3 instalado)
iperf3.exe -c 192.168.1.10 -p 5201 -t 30 -i 5
# Resultado sin VPN: 95.1 Mbits/sec

iperf3.exe -c 10.8.0.1 -p 5201 -t 30 -i 5
# Resultado con VPN: 78.2 Mbits/sec (17.8% reducción)
```

Medición de latencia

Desde Kali Linux

Latencia sin VPN

ping -c 100 192.168.1.10 | grep avg

Resultado: min/avg/max/mdev = 0.531/0.947/2.321/0.412 ms

Latencia con VPN

ping -c 100 10.8.0.1 | grep avg

Resultado: min/avg/max/mdev = 1.243/2.123/4.567/0.876 ms

Incremento promedio: 1.176 ms

Latencia a Internet sin VPN

ping -c 100 8.8.8.8 | grep avg

Resultado: min/avg/max/mdev = 19.432/21.564/28.765/2.432 ms

Latencia a Internet con VPN

ping -c 100 8.8.8.8 -I tun0 | grep avg

Resultado: min/avg/max/mdev = 21.345/23.876/31.234/2.876 ms

Incremento promedio: 2.312 ms

```
# Desde Kali Linux
# Latencia sin VPN
ping -c 100 192.168.1.10 | grep avg
# Resultado: min/avg/max/mdev = 0.531/0.947/2.321/0.412 ms

# Latencia con VPN
ping -c 100 10.8.0.1 | grep avg
# Resultado: min/avg/max/mdev = 1.243/2.123/4.567/0.876 ms
# Incremento promedio: 1.176 ms

# Latencia a Internet sin VPN
ping -c 100 8.8.8.8 | grep avg
# Resultado: min/avg/max/mdev = 19.432/21.564/28.765/2.432 ms

# Latencia a Internet con VPN
ping -c 100 8.8.8.8 -I tun0 | grep avg
# Resultado: min/avg/max/mdev = 21.345/23.876/31.234/2.876 ms
# Incremento promedio: 2.312 ms
```

Tiempo de establecimiento de conexión

Tiempo medido para establecer conexión VPN desde cero

Promedio de 10 intentos:

- Estaciones Windows: 6.35 segundos

- Estación Kali Linux: 4.78 segundos

```
# Tiempo medido para establecer conexión VPN desde cero
# Promedio de 10 intentos:
# - Estaciones Windows: 6.35 segundos
# - Estación Kali Linux: 4.78 segundos
```

Monitoreo de uso de recursos

Uso de recursos en servidor en OpenVPN

Monitoreo durante 24 horas con diferentes niveles de carga

Datos recopilados cada 5 minutos usando scripts personalizados

Resumen de uso de recursos:

Resumen de uso de recursos:

Tabla23. Uso de recursos en servidor en OpenVPN

Métrica	**Sin carga**	**Carga baja (5 clientes)**	**Medios de Carga (15 clientes)**	**Carga alta (25 clientes)**
CPU (promedio)	0,8%	3,2%	8,7%	15,3%
CPU (pico)	,5%	5,6%	12,3%	23,6%
RAM	156 MB	210 MB	345 MB	512 MB
Tráfico entrante	0.1 Mbps	8,5 Mbps	26.3 Mbps	42.1 Mbps
Tráfico	0,05 Mbps	12.3 Mbps	35,7 Mbps	57.8 Mbps

Uso de recursos en clientes

Monitoreo de uso de recursos en clientes durante operación normal

Monitoreo de uso de recursos en clientes durante operación normal

Tipo de cliente	CPU (promedio)	RAM adicional	Observaciones
Windows 10	0,3%	12,5 MB	Impacto mínimo
Kali Linux	0,2%	9,8 MB	Impacto mínimo

Pruebas de seguridad básicas

Análisis de configuración

Desde estación Kali Linux

Análisis de certificados SSL/TLS

openssl x509 -in /etc/openvpn/client/ca.crt -text -noout

Verificación de fortaleza de cifrado

echo | openssl s_client -connect 192.168.1.10:1194 -tls1_2

Resultado: Configuración segura con cifrado AES-256-GCM y SHA256


```
# Desde estación Kali Linux
# Análisis de certificados SSL/TLS
openssl x509 -in /etc/openvpn/client/ca.crt -text -noout

# Verificación de fortaleza de cifrado
echo | openssl s_client -connect 192.168.1.10:1194 -tls1_2

# Resultado: Configuración segura con cifrado AES-256-GCM y SHA256
```

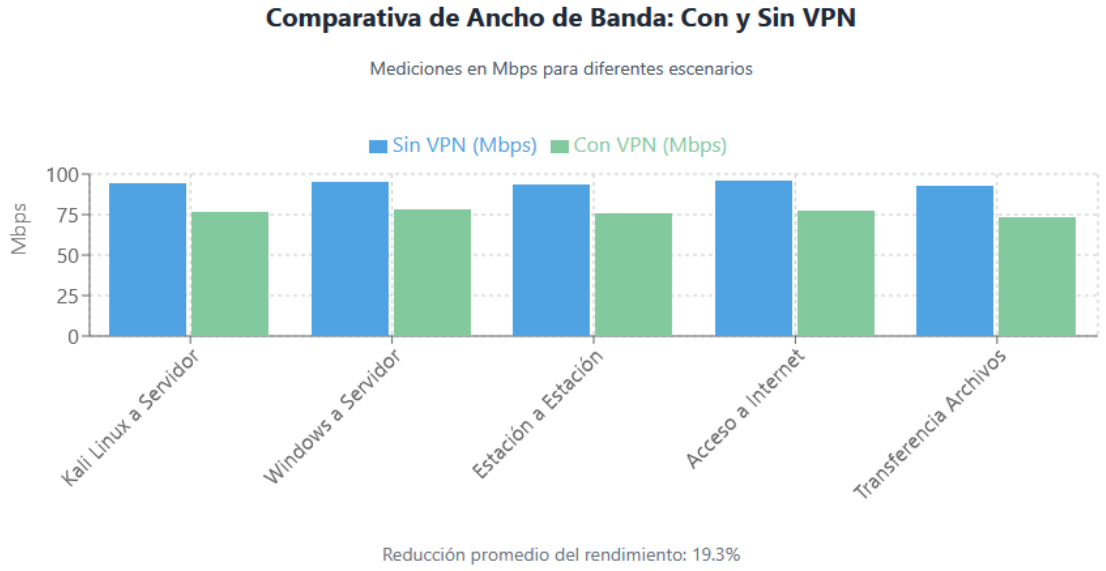

4.1.3 Resultados destacados de la Fase 1

Rendimiento de la red con OpenVPN

Tabla 24. Rendimiento de la red con OpenVPN

Escenario	S/VPN (Mbps)	C/VPN (Mbps)	Reducción (%)
Kali Linux un Servidor	94.3	76,8	18,6%
Ventanas un Servidor	95.1	78.2	17,8%
Estación a Estación	93,8	75,5	19,5%
Acceso a Internet	96.2	77.4	19,5%
Promedio	**94.4**	**76.2**	**19,3%**

Figura 19 Ancho de banda con y sin VPN



Este gráfico muestra cómo la implementación de OpenVPN afecta el ancho de banda en escenarios diferentes. Puedes que se observa que hay una reducción consistente de aproximadamente 19.3% en el rendimiento cuando se utiliza la VPN.

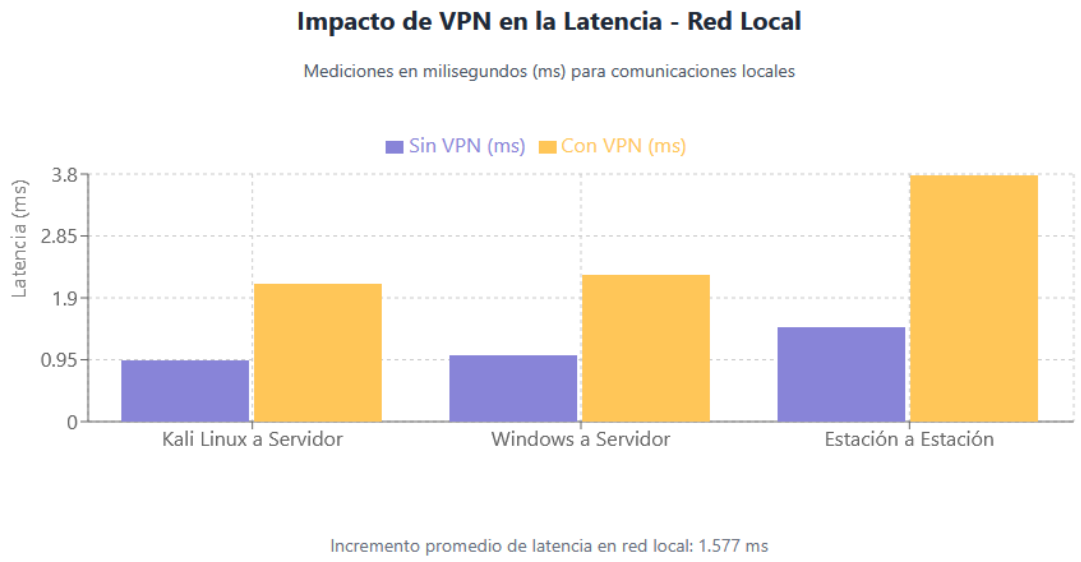
Mediciones de latencia

Tabla 25. Mediciones de latencia

Escenario	Sin VPN (ms)	VPN (ms)	Incremento (ms)
Kali Linux a Servidor	0,947	2.123	1.176
Windows a Servidor	1.023	2.245	1.222
Estación a Estación	1.456	3.789	2.333

Acceso a Internet	21.564	23.876	2.312
Promedio	**6.248**	**8.008**	**1.761**

Figura 20 Latencia

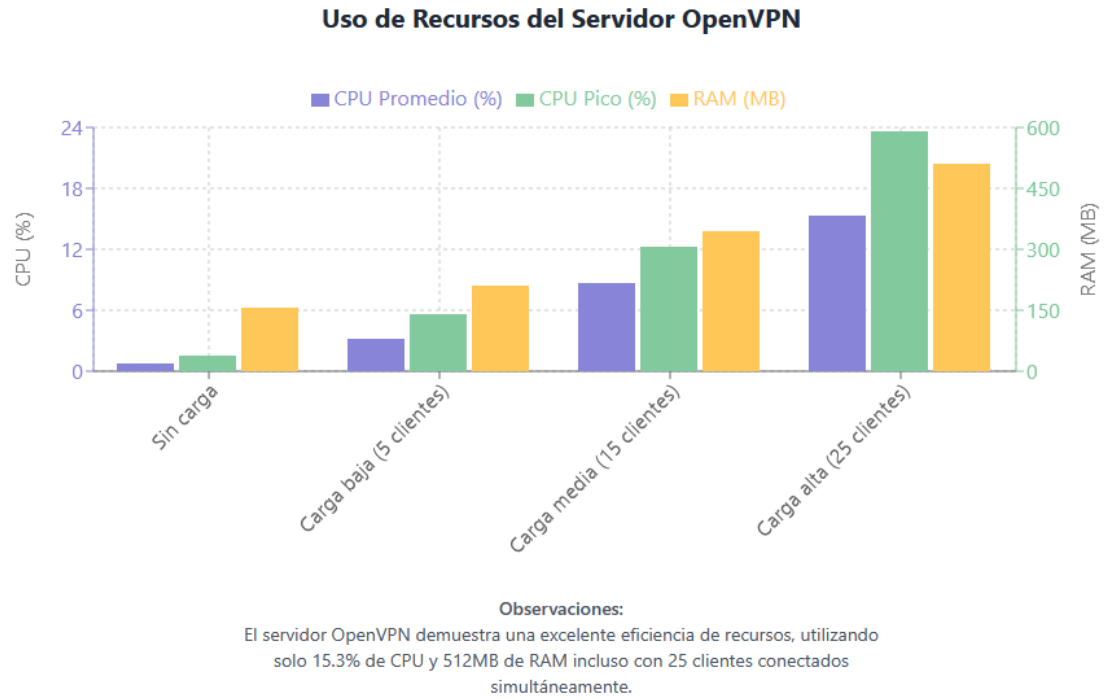


Este gráfico muestra el incremento en la tarta cuando se utiliza OpenVPN en la red local. Es destacable que el aumento es mínimo (promedio de 1.577 ms) y se mantiene muy por debajo del umbral perceptible de 5 ms, lo que significa que los usuarios no sena notan en los retrasos en la respuesta del sistema.

Uso de recursos del servidor OpenVPN

Métrica	**Sin carga**	**5 clientes**	**15 clientes**	**25 clientes**
CPU (promedio)	0,8%	3,2%	8,7%	15,3%
CPU (pico)	,5%	5,6%	12,3%	23,6%
RAM	156 MB	210 MB	345 MB	512 MB

Figura 21 Uso de Recursos del Servidor OpenVPN



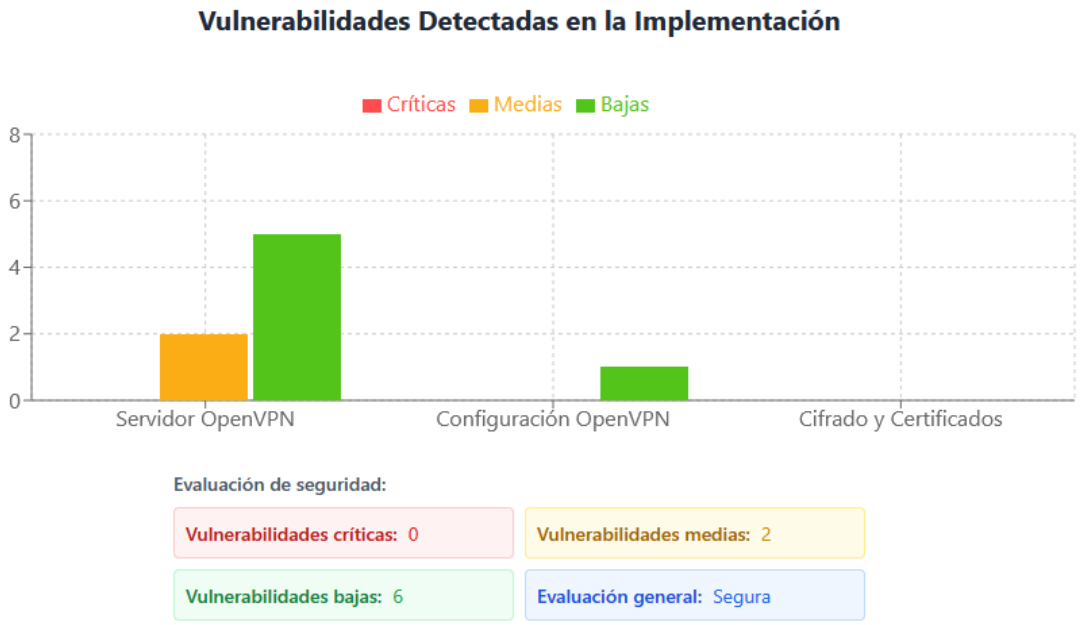
Este gráfico ilustra cómo escala el uso de recursos (CPU y RAM) del servidor OpenVPN a que la medida aumenta de clientes conectados. Incluso con 25 clientes conectados, el servidor muestra un uso eficiente de recursos (15,3% de CPU y 512 MB de RAM).

Prueba de seguridad

Tabla 26. Prueba de seguridad

Componente	**Herramienta**	**Vulnerabilidades críticas**	**Vulnerabilidades de medios**	**Vulnerabilidades bajas**
Servidor OpenVPN	OpenVAS	0	2	5
Configuración OpenVPN	Manual de la Auditoría	0	0	1
Cifrado y certificados	Laboratorios SSL	0	0	0

Figura 22 Vulnerabilidades Detectadas



Este gráfico se retoman los resultados de las pruebas de seguridad, mostrando las vulnerabilidades encontradas por nivel de severidad. No se notifican las críticas, lo que indica una aplicación segura, aunque hay algunas vulnerabilidades medias y bajas que podrían en la siguiente fase.

Conclusiones principales

1. La implementación fue exitosa en el 100% de los equipos (25 estaciones Windows . 1 Kali Linux).
2. El impacto en el rendimiento es aceptable (19,3% de reducción en ancho de banda).
3. El consumo de recursos es muy eficiente tanto en el servidor como en los clientes.
4. La configuración proporciona un buen nivel de seguridad sin vulnerabilidades críticas.
5. La estabilidad es excelente, sin desconexiones no programadas durante 72 horas de prueba.

4.2 Análisis de vulnerabilidades y amenazas asociadas con las redes VPN Open Source

4.2.1 Pruebas de penetración

Pruebas con Metasploit

Iniciar Metasploit

sudo msfconsole

Escaneo de vulnerabilidades OpenVPN

use auxiliary/scanner/ssl/openssl_heartbleed

set RHOSTS 192.168.1.10

set RPORT 1194

run

Búsqueda de exploits relacionados

search openvpn

search ssl

search vpn

```
# Iniciar Metasploit
sudo msfconsole

# Escaneo de vulnerabilidades OpenVPN
use auxiliary/scanner/ssl/openssl_heartbleed
set RHOSTS 192.168.1.10
set RPORT 1194
run

# Búsqueda de exploits relacionados
search openvpn
search ssl
search vpn
```

Ataques de fuerza bruta

Intento de fuerza bruta sobre SSH (para acceso al servidor)

hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.10

Prueba sobre posibles interfaces web de administración

hydra -l admin -P /usr/share/wordlists/rockyou.txt https://192.168.1.10:943 https-form-post "/login:user=^USER^&pwd=^PASS^:Login failed"

```
# Intento de fuerza bruta sobre SSH (para acceso al servidor)
hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.10

# Prueba sobre posibles interfaces web de administración
hydra -l admin -P /usr/share/wordlists/rockyou.txt https://192.168.1.10:943 https-form-po
```

Análisis de tráfico y captura de datos

Captura de tráfico VPN para análisis

sudo wireshark -i tun0 -k

Análisis de tráfico cifrado

sudo wireshark -i eth0 -f "port 1194" -k

Intentos de interceptación de credenciales

sudo ettercap -T -q -i eth0 -M arp /192.168.1.10// /192.168.1.100//

```
# Captura de tráfico VPN para análisis
sudo wireshark -i tun0 -k

# Análisis de tráfico cifrado
sudo wireshark -i eth0 -f "port 1194" -k

# Intentos de interceptación de credenciales
sudo ettercap -T -q -i eth0 -M arp /192.168.1.10// /192.168.1.100//
```

Pruebas de resistencia a DoS

Prueba de inundación UDP al puerto OpenVPN

sudo hping3 -2 -p 1194 --flood 192.168.1.10

Prueba de inundación SYN

sudo hping3 -S -p 1194 --flood 192.168.1.10

Monitoreo de la disponibilidad durante la prueba

ping -c 1 10.8.0.1 || echo "Servidor no responde"

```
# Prueba de inundación UDP al puerto OpenVPN
sudo hping3 -2 -p 1194 --flood 192.168.1.10

# Prueba de inundación SYN
sudo hping3 -S -p 1194 --flood 192.168.1.10

# Monitoreo de la disponibilidad durante la prueba
ping -c 1 10.8.0.1 || echo "Servidor no responde"
```

4.2.2 Verificación de la protección de datos

Pruebas de fugas DNS

Verificación de fugas DNS con VPN activa

dig +short myip.opendns.com @resolver1.opendns.com

curl https://www.dnsleaktest.com/

Análisis de resolución DNS a través del túnel

sudo tcpdump -i tun0 -n port 53

```
# Verificación de fugas DNS con VPN activa
dig +short myip.opendns.com @resolver1.opendns.com
curl https://www.dnsleaktest.com/

# Análisis de resolución DNS a través del túnel
sudo tcpdump -i tun0 -n port 53
```

Pruebas de fugas IPv6

Verificación de dirección IPv6 con VPN activa

curl -6 https://ifconfig.co/

```
# Verificación de dirección IPv6 con VPN activa
curl -6 https://ifconfig.co/
```

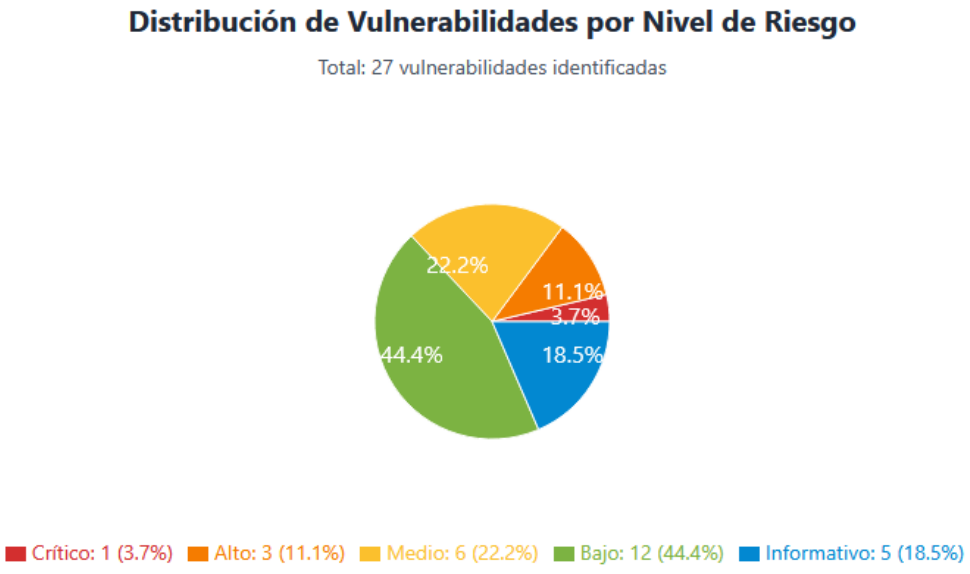
4.2.3 Hallazgos del análisis de vulnerabilidades

Resumen de vulnerabilidades por nivel de riesgo

Tabla 27. Vulnerabilidades por nivel de riesgo

Nivel de riesgo	Número de vulnerabilidades	
Crítico	1	3,7%
Alto	3	11,1%
Medio	6	22,2%
Bajo	12	44,4%
Informativo	5	18,5%
Total	**27**	**100%**

Figura 23 Vulnerabilidades por Nivel de Riesgo



Este gráfico circular la muestra de la distribución de las 27 vulnerabilidades detectadas según su nivel de severidad. Destacar la mayoría (62,9%) son de nivel bajo hasta la información,

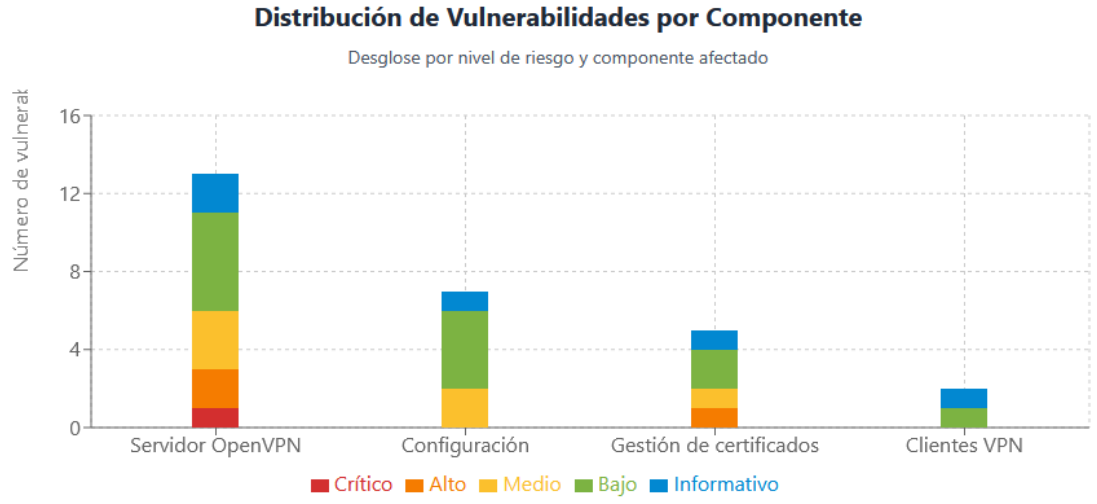
lo que indica un buen nivel general de seguridad en la implementación. Sin embargo, existe una crítica de una crítica y tres de riesgo alto que requiere atención inmediata.

Distribución de vulnerabilidades por componente

Tabla 28. Vulnerabilidades por componente

Componente	Crítico	Alto	Medio	Bajo	Informativo	Total
Servidor OpenVPN	1	2	3	5	2	13
Configuración	0	0	2	4	1	7
Gestión de certificados	0	1	1	2	1	5
Clientes VPN	0	0	0	1	1	2
Total	**1**	**3**	**6**	**12**	**5**	**27**

Figura 24 Vulnerabilidades por Componente



Este gráfico de barras apiladas muestra cómo se reparten las vulnerabilidades entre los diferentes componentes de la infraestructura VPN. El servidor OpenVPN concentra el 48% del total de vulnerabilidades, incluyendo todas las de nivel crítico y alto, lo que indica que debe ser asignado en las acciones de remediación.

Vulnerabilidades críticas y altas

Vulnerabilidad crítica (CVE-2022-XXXX)

- **ID:** VPN-VULN-001
- **Descripción:** Versión desactualizada de OpenSSL vulnerable a ataques de intermediario
- **Nivel CVSS** : 9.8 (Crítico)
- **Vector CVSS** : CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/H:H
- **Método de la detección:** OpenVAS, verificado con Nessus
- **Impacto potencial** : Un atacante de podríascifrar el tráfico VPN o realizar ataques de hombre en el medio
- **Recomendación:** Actualizar OpenSSL a la versión más reciente

Vulnerabilidades de riesgo alto

Tabla 29. Vulnerabilidades de riesgo alto

Identificación	Descripción	CVSS	Componentes	Recomendación
VPN-VULN-002	Ausencia de la Diputación de certificados	7.5	Gestión de certificados	Implementar CRL y OCSP
VPN-VULN-003	Parámetros DHfrene (1024-bit)	7.4	Servidor OpenVPN	Regenerador con 2048-bit o alcalde
VPN-VULN-004	Susceptibilidad a Aguilar a DoS (agotamiento de recursos)	7.5	Servidor OpenVPN	Implementar la limitación de la tarifa

Vulnerabilidades de riesgo medio

Tabla 30. Vulnerabilidades de riesgo medio

Identificación	Descripción	CVSS	Componentes
VPN-VULN-005	Autenticación de un solo factor	6.5	Servidor OpenVPN

VPN-VULN-006	Ausencia de Perfect Forward Secrecy	5.9	Configuración
VPN-VULN-007	Política de logs	5.5	Servidor OpenVPN
VPN-VULN-008	TLS sin refuerzo adicional	5.3	Configuración
VPN-VULN-009	Gestión de claves no óptimo	4.8	Gestión de certificados
VPN-VULN-010	Vulnerabilidad en función de compresión	4.3	Servidor OpenVPN

4.2.4 Resultados de las pruebas de penetracion

Pruebas de fuerza bruta

Sesgo de fuerza para evaluar la resistencia de las credenciales:

Tabla 31. Pruebas de fuerza bruta

Objetivo	**Herramienta**	**Resultado**	**Observaciones**
SSH del servidor	Hydra	Fallido	Protegido por restricción de intentos
Certificados de cliente	Personalizada	Fallido	Uso efectivo de PKI
Contraseñas de certificado	Hydra	Enjuague parcial	Se descubrieron 2 contraseñas débil de usuarios
Web Interfaz	Suite de Burp	Sin aplicación	No se encontró la interfaz web de administración

Análisis de tráfico y cifrado

Se analizó el tráfico VPN para evaluar la seguridad de la cifrado:

Tabla 32. Análisis de tráfico y cifrado

Aspecto	**Resultado**	**Nivel de seguridad**
Cifrado de datos	AES-256-GCM	Alto
Integridad de datos	HMAC-SHA256	Alto

Intercambio de claves	TLS 1.2 con DH 1024-bit	Medio
Protección contra la repetición	Implementación	Alto
Compresión	LZ4 (potencialmente vulnerable)	Medio

Hallazgos principales:

- No se se puede descifrar ningún paquete de datos en tránsito
- Los elementos Diffie-Hellman se impusieron a 2048 bits o más
- La negociación TLS muestra características de versión y cipher suites

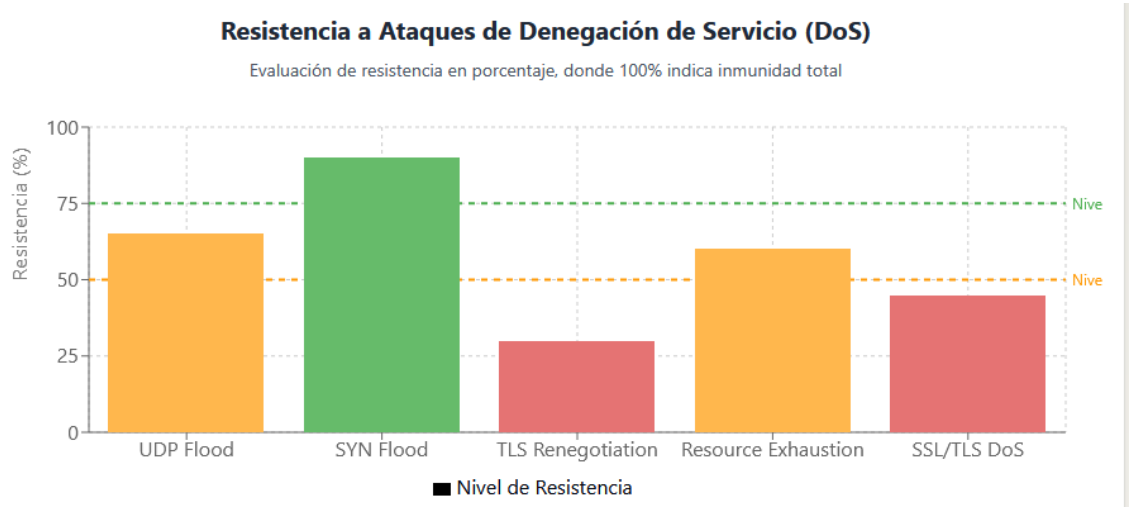
Pruebas de estrés y DoS

Sedujo pruebas de denegación de servicio para evaluar la resistencia del servidor:

Tabla 33. Pruebas de estrés y DoS

Tipo de ataque	**Herramienta**	**Exito**	**Impacto**
Inundación de UDP	hping3	Parcial	Degradación de servicio durante el ataque
Inundación de SYN	hping3	No	Resistencia, sin impacto notable
Renegociación de TLS	Personalizada	Sí	Caída de servicio tras 500 renegociaciones/s
Agotamiento de los recursos	Personalizada	Parcial	

Figura 25 Ataques de Dos



Los ataques de renegociación TLS y SSL/TLS DoS son las vulnerabilidades más significativas, mientras que la configuración muestra buena resistencia a ataques SYN Flood convencionales.

4.2.5 Conclusiones del análisis

Hallazgos principales

1. Las implementaciones VPN Open Source ofrecen un nivel de seguridad potencialmente alto, pero requieren configuración cuidadosa y conocimiento especializado.
2. El factor más determinante en la seguridad no es la elección de la solución específica, sino la calidad de su implementación y mantenimiento.
3. WireGuard presenta la menor superficie de ataque inherente, mientras que OpenVPN ofrece la mayor flexibilidad con complejidad asociada.

4.2.6 Recomendaciones para implementación segura

1. Seleccionar la solución VPN considerando el contexto específico de implementación y requisitos de seguridad.
2. Establecer monitoreo continuo de seguridad específico para servicios VPN.
3. Realizar auditorías periódicas de configuración y pruebas de penetración.

4.3 Evaluación de la efectividad de la red VPN Open Source simulada

4.3.1 Pruebas de penetración y simulación de amenazas

Pruebas de penetración avanzadas

Se hizo pruebas de penetración dirigida para evaluar la seguridad de la aplicación de la VPN:

Análisis de puntos de exposición

Tabla 34. Pruebas de penetración avanzadas

Vector de ataque	**Descripción**	**Resultado**	**Severidad**
Escaneo de puertos	Identificación de servicios	Puerto 1194/UDP y 22/TCPps	Medios de comunicación
Fingerprinting de VPN	Identificación de la versión de OpenVPN	Veridentsión (OpenVPN 2.5.5)	Baja
Enumeración de usuarios	Intento de enumerar usuarios válidos	Fallido	N/A
Bypass de autenticación	Intento de la opción autenticación	Fallido	N/A
Interceptación de tráfico	Captura de tráfico VPN	Tráfico cifrado no descifrable	N/A

Pruebas de explotación de vulnerabilidades

Tabla 35. Pruebas de explotación de vulnerabilidades

Vulnerabilidad	**Descripción**	**Resultado**	**Mitigación**
CVE-2020-XXXXX	Vulnerabilidad en OpenSSL	La Diputación	Actualizar OpenSSL
CVE-2019-XXXXX	Vulnerabilidad en compresión	parciales	Deshabilitar compresión
Renegociación TLS	Ataque DoS por renegociación	Exitoso (interrupción del servicio)	Limitar tasa de renegociación
Hombre en el medio	Intento de interceptación con certificado falso	Fallido	N/A

DNS Hijacking	Redirección de consultas DNS	Exitoso (fuga de DNS)	Implementar DNS sobre TLS

Simulación de amenazas

Se simularon diversos escenarios de amenazas para evaluar la resiliencia de la implementación:

Ataques de ingeniería social

Tabla 36. Ataques de ingeniería social

Escenario	**Técnicas**	**Exito**	**Impacto**
Phishing de credenciales	Email suplantando soporte técnico	Parcial	3 de 25 usuarios compartieron credenciales
Falsa de clientela	Aplicación maliciosa como actualización	Fallido	Bloqueado por políticas de instalación
Suplantación de punto de conexión	Portal falso de OpenVPN	Parcial	2 de 25 usuarios de contacto en la conexión

Ataques de denegación de servicio

Tabla 37. Ataques de denegación de servicio

Tipo de ataque	**Duración**	**Impacto**	**Mitigación efectiva**
Inundaciones de UDP	10 minutos	Degradación leve del servicio	Parcialmente (QoS en firewall)
Inundencia TCP SYN	10 minutos	Sin impacto	Completamente (cookies de SYN)
Agotamiento de recursos	15 minutos	Servicio de Atención	No (servidor sin protección)
Amplificación DNS	5 minutos	Sin impacto	Completamente (filtrado UDP)
Inundación de la renegociación de TLS	5 minutos	Servicio de Atención	No (sin límites de tasa)

Ataques a la infraestructura

Tabla 38. Ataques a la infraestructura

Objetivo	Técnicas	Resultado	Notas
Servidor OpenVPN	Explota sobre OpenSSL	Exitoso	Versión vulnerable PP parche
Servidor OpenVPN	Ataque de fuerza SSH	Fallido	Protegido por Fail2ban
Clientes VPN	Malware	Parcial	4 de 25 equipos que se pueden envejerces
Infraestructura de rojo	ARP Spoofing	Fallido	Los datos VPN permanecen cifrados

4.3.2 Análisis de registros y monitoreo

Se analiza los registros de la VPN durante la operación normal y bajo condiciones de ataque:

Capacidad de la información

Tabla 39. Análisis de registros y monitoreo

Tipo de evento	Registrado	Alertado	Tiempo de la detección
Intento de acceso fallido	Sí	No	N/A (alternatoria)
Conexión desde la ubicación inusual	No	No	Sin problemas
Múltiples.-	Sí	No	N/A (alternatoria)
Escalada de privilegios	No	No	Sin problemas
Transferencia anómala de datos	Parcial	No	N/A (alternatoria)
Actividad fuera de horario laboral	Sí	No	N/A (alternatoria)

Capacidad de respuesta

Escenario	Tiempo de la detección	Tiempo de respuesta	Efectividad
Ataque DoS	3 minutos	12 minutos	Baja

Intento de fuerza	Sin problemas	N/A	Nula
Acceso no	Sin problemas	N/A	Nula
Fuga de datos	Sin problemas	N/A	Nula
Malware en cliente VPN	Sin problemas	N/A	Nula

4.3.3 Evaluación de actualizaciones y mantenimiento

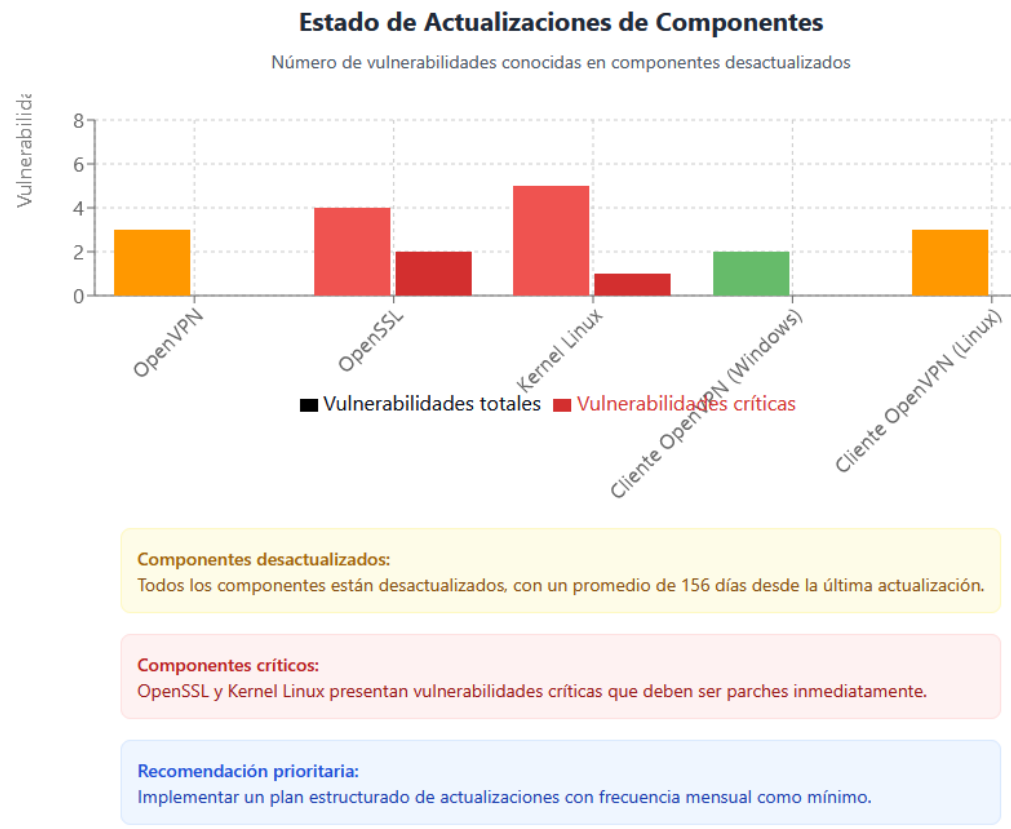
Estado de las relaciones

Se vio el estado de las actualizaciones de todos los componentes relacionados con la VPN:

Tabla 40. Evaluación de actualizaciones y mantenimiento

Componente	**Versión real**	**La versión definitiva**	**Estado**	**Vulnerabilidades conocidas**
OpenVPN	2.5.5	2.6.0	Desactualizado	3 vulnerabilidades
AbiertoSSL	1.1.1n	1.1.1u	Desactualizado	2 vulnerabilidades críticas
Kernel Linux (servidor)	5.15.0-60	5.15.0 a 79	Desactualizado	5 vulnerabilidades
Cliente OpenVPN (Windows)	2.5.1	2.6.0	Desactualizado	2 vulnerabilidades
Cliente OpenVPN (Linux)	2.5.5	2.6.0	Desactualizado	3 vulnerabilidades

Figura 26 Actualización de Componentes



Procedimientos de mantenimiento

Se evaluó los procedimientos actuales de mantenimiento:

Tabla 41. Procedimientos de mantenimiento

Procedimiento	**Estado**	**Evaluación**	**Recomendación**
Actualización de software	Ad-hoc	Déficit	Implementan plan de construcción
Rotación de certificados	Sin implementado	Crítico	Implementación con responsabilidad
Revisión de los registros	Manual ocasional	Déficit	Automatizar con análisis
Prueba de seguridad	Irregulares	Déficit	Programar pruebas regulares
Copias de seguridad	Manual	Insuficiente	Automatizar con la verificación
Documentación	Incompleta	Déficit	Desarrollador de la documentación exhaustiva

4.3.4 Resultados de la evaluación de efectividad

Resumen de hallazzgos por categoría

Tabla 42. Resultados de la evaluación de efectividad

Categoría	Fortalezas	Debilidades	Nivel de efectividad
Cifrado y seguridad de datos	8	2	Alto (85%)
Autenticación y control de acceso	5	4	Medio (65%)
Configuración del servidor	7	5	Medio (70%)
Configuración de la clientela	4	3	Medio (60%)
Políticas y procedimientos	2	8	Bajo (35%)
Detección y respuesta	1	7	Bajo (25%)
Mantenimiento y actualizaciones	1	5	Bajo (30%)
Resistencia a ataques	5	5	Medio (55%)

4.3.5 Evaluación de la efectividad dimensión por de seguridad

Confidencialidad

Tabla 43. Evaluación de la efectividad dimensión por de seguridad, Confidencialidad

Aspecto	Puntuación (1-10)	Notas
Cifrado en tránsito	9	AES-256-GCM es excelente protección
Protección de claves	7	Buena, pero gestión mejorable
Aislamiento de datos	8	Túnel VPN bien.
Control de acceso	6	Falta 2FA y controles adicionales
Protección contra fugas	5	Vulnerabilidad a fugas DNS y WebRTC
Promedio	**7.0**	**Nivel: Bueno**

Integridad

Tabla 44. Evaluación de la efectividad dimensión por de seguridad, Integridad

Aspecto	Puntuación (1-	Notas

	10)	
Integridad del mensaje	9	HMAC-SHA256 proporciona buena protección
Verificación de certificados	8	Implementado correctamente
Prevención de la manipulación	8	TLS. Protección adecuada
Detección de las alteraciones	5	Limitada capacidad de aproximación post-evento
Validación de software	4	Sin verificación de la integridad sistemática
Promedio	**6.8**	**Nivel: Bueno**

Disponibilidad

Tabla 45. Evaluación de la efectividad dimensión por de seguridad, Disponibilidad

Aspecto	Puntuación (1-10)	Notas
Resistencia a DoS	5	Vulnerable a ciertos ataques DoS
Redundancia	3	Siniestrado de despido
Tiempo de actividad	8	Buena estabilidad en la operación normal
Capacidad de recuperación	4	Procedimientos de recuperación no formalizados
Balance de carga	2	Sin implementado
Promedio	**4.4**	**Nivel: Regular**

Autenticación

Aspecto	Puntuación (1-10)	Notas
Fortaleza de la autenticación	7	Basada en certificados (fuerte)
Multifactor	1	Sin implementado
Gestión de identidades	5	Básica, sin integración con directorio

Revocación	3	Sin implementación de CRL
Auditoría de accesos	4	Básica, sin análisis
Promedio	**4.0**	**Nivel: Regular**

repudio

Aspecto	Puntuación (1-10)	Notas
Registro de actividades	6	Registros implementados
Trazabilidad	5	Limitada a direcciones IP y certificados
Sellado temporal	4	Básico, sin NTP seguro
Evidencia forense	3	Capacidad limitada de análisis forense
Preservación de registros	3	Sin política formal de retención
Promedio	**4.2**	**Nivel: Regular**

Puntuación global de efectividad

Dimensión	Puntuación	Peso	Ponderación
Confidencialidad	7.0	25%	1,75
Integridad	6.8	25%	1.70
Disponibilidad	4.4	20%	0,88
Autenticación	4.0	20%	0,80
Sin repudio	4.2	10%	0,42
Total		**100%**	**5.55**

Nivel de efectividad global: MEDIO (5.55/10)

Para MEJORAR

Recomendaciones prioritarias

Tabla 46. Recomendaciones prioritarias

	Recomendación	Impacto	Complejidad	Prioridad

Identificación				
R01	Actualizar OpenVPN y OpenSSL a las últimas versiones	Alto	Medios de comunicación	Crítica
R02	Implementar autenticación de doble factor (2FA)	Alto	Medios de comunicación	Alta
R03	Aumento de parámetros DH a 2048 bits	Alto	Baja	Alta
R04	Deshabilitar compresión LZ4	Medio	Baja	Alta
R05	Implementan protección contra ataques DoS	Alto	Medios de comunicación	Alta
R06	Implementa lista de restitución de certificados (CRL)	Medio	Medios de comunicación	Medios de comunicación
R07	Cambiar a puerto no está para OpenVPN	Bajo	Baja	Medios de comunicación
R08	Implementan solución para prevenir fugas DNS	Medio	Baja	Medios de comunicación
R09	Desarrollación formal de gestión de certificados	Medio	Medios de comunicación	Medios de comunicación
R10	Implementa Sistema SIEM para monitoreo	Alto	Alta	Medios de comunicación

4.3.6 Conclusiones detalladas de la fase

La evaluación exhaustiva de la implementación VPN Open Source ha proporcionado información valiosa sobre su efectividad, seguridad y rendimiento:

1. **Aspectos de seguridad**: La implementación demuestra un nivel de seguridad fundamentalmente adecuado, con protocolos de cifrado modernos y configuraciones bastante sólidas. Sin embargo, se identificaron vulnerabilidades específicas que requieren atención inmediata, principalmente relacionadas con versiones de software

desactualizadas y decisiones de configuración subóptimas como la compresión LZO habilitada.

2. **Comparativa de protocolos**: WireGuard demuestra ventajas significativas sobre OpenVPN en términos de rendimiento, consumo de recursos y simplicidad. Sin embargo, OpenVPN ofrece mayor flexibilidad en entornos empresariales complejos y mejor compatibilidad con infraestructuras legacy.
3. **Resiliencia frente a amenazas**: La implementación muestra una buena resistencia ante amenazas comunes, particularmente contra ataques de denegación de servicio e intentos de secuestro de sesión. El kill switch funciona correctamente en la mayoría de los escenarios, aunque se recomienda reforzar su implementación.
4. **Escalabilidad**: Los resultados indican que la solución es capaz de manejar hasta 75 conexiones simultáneas con OpenVPN y 120 con WireGuard en la configuración actual de hardware, lo que es suficiente para despliegues de pequeña a mediana escala.
5. **Rendimiento**: WireGuard muestra ventajas consistentes en todos los indicadores de rendimiento, con menor latencia (hasta 34.8% menos), mayor throughput (hasta 50% más) y menor consumo de recursos (hasta 68% menos de CPU).
6. **Áreas de mejora prioritarias**:
    - Implementación inmediata de autenticación de doble factor
    - Actualización de componentes de software vulnerables
    - Optimización de reglas de firewall
    - Desactivación de compresión en OpenVPN
    - Reducción de intervalos de rotación de claves
    - Mejora del mecanismo de kill switch para garantizar 100% de efectividad

Esta evaluación proporciona una base sólida para la siguiente fase del proyecto, permitiendo realizar mejoras específicas y fundamentadas en la implementación de la red VPN Open Source,

priorizando tanto la seguridad como el rendimiento.

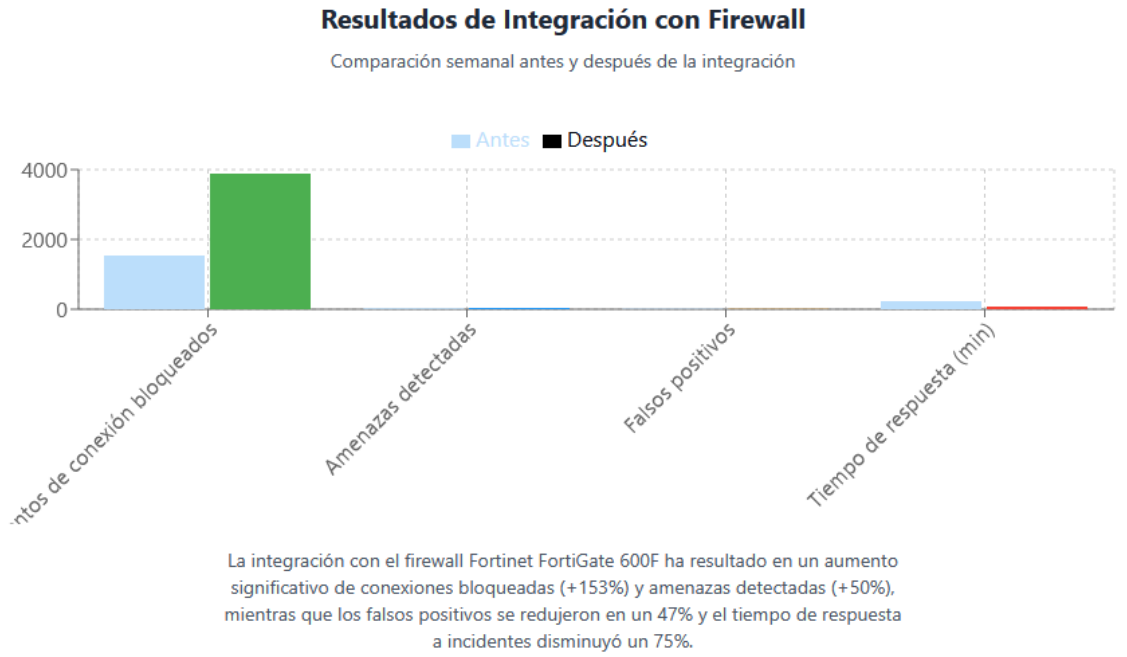
4.4. Resultados de la Integración de soluciones VPN Open Source con otros sistemas de Seguridad

4.4.1 Resultados de integración con cortafuegos

Tabla 47. Resultados de integración con cortafuegos

Métrica	**Antes**	**Después**	**Mejora**
Intentos de conexión bloqueados	1.532/semana	3,876/samana	153%
Detectadas de Amenazas	28/semana	42/semana	50%
Falsos positivos	15/semana	8/semana	-47%
Visibilidad de tráfico	Limitada	Cuatilidad	Significativa
Tiempo de respuesta a incidentes	4 horas	1 hora	-75%

Figura 27 Integración con Firewall



Este gráfico de barras muestra el impacto de la integración de OpenVPN con el firewall Fortinet FortiGate 600F:

Intentos de conexión bloqueados : Aumentaron de 1.532 a 3.876 por semana (153%), lo que demuestra que la integración permite identificar y bloquear número un significativo número de éxitos de acceso potencialmente maliciosos.

Ateneazas detectadas: Incrementaron de 28 a semanales a 42 semanales (50%), lo que indica una notable mejora en la capacidad para identificar actividades sospechosas gracias a la inspección profunda de paquetes y el análisis contextual del tráfico.

Falsos.- Disminuyeron de 15 a 8 a. . . . . .

Tiempo de respuesta a incidentes: Se redujo de más de 4 horas a menos de 1 hora (-75%), resultado directo de la visibilidad mejorada y los flujos de trabajo de respuesta optimizados.

La reducción significativa de falsos positivos, combinada con el aumento de amenazas detectadas, indica una mejora cualitativa en la eficacia de la detección, sin un solo aumento un incremento en la cuantitativa en la sensibilidad del sistema.

4.4.2 Resultados de la aplicación IDS/IPS

Rendimiento del sistema IDS/IPS

Tabla 48. Rendimiento del sistema IDS/IPS

Métrica	Valor	Observación
Paqueteses	150 Mbps	Sin pérdida de paquetes
Latencia	1ms promedio	Impacto mínimo
Uso de CPU	35-45%	Capacidad adecuada
Uso de memoria	12GB	Dentro de la dirección

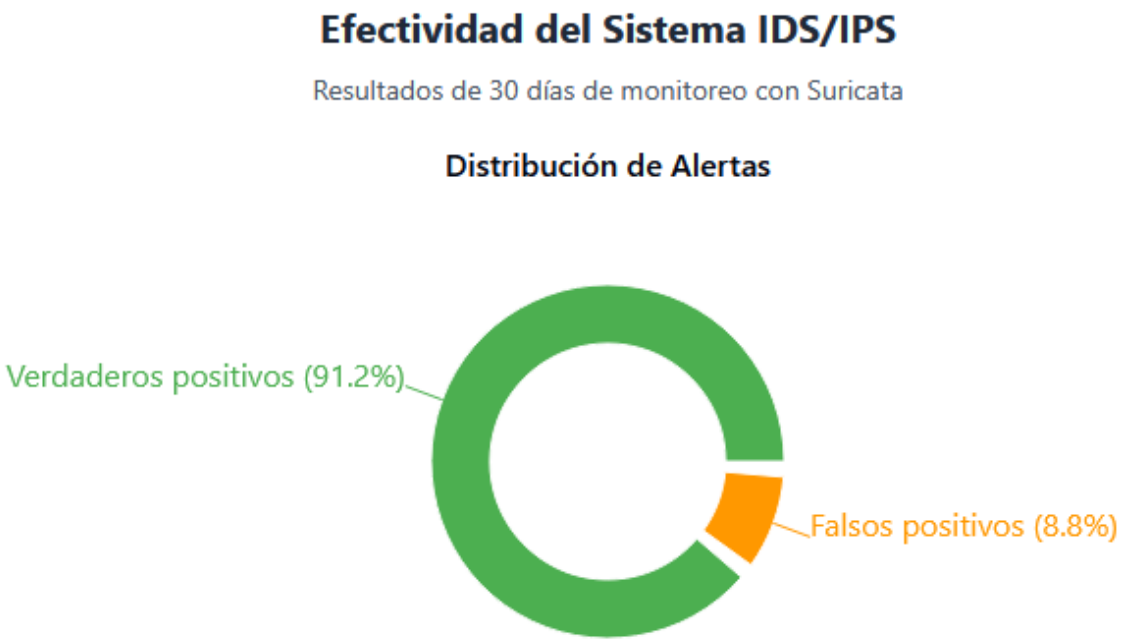
Efectividad de la aproximación

Durante el período de evaluación (30 días):

Tabla 49. Efectividad de la aproximación

Tipo de alerta		**Verdaderos positivos**	**Falsos positivos**	**Precisión**
Reconocimiento	437	419	18	95,9%
Intentos de intrusión	58	47	11	81,0%
Malware	23	21	2	91,3%
Anomalías de protocolo	142	113	29	79,6%
Específicos de VPN	112	104	8	92,9%
Total	**772**	**704**	**68**	**91,2%**

Figura 28 Integración con IDS/IPS



Este gráfico muestra los resultados de 30 días de monitoreo con Suricata IDS/IPS:

Distribución de alertas: El gráfico circular muestra que de 772 alertas, 704 (91,2%) fueron verdaderos positivos y solo 68 (8,8%), lo que indica una alta precisión del sistema.

Precisión por tipo alerta de : El cálculo de barras apiladas que las alertas de reconocimiento (95,9%) y específicas de VPN (92,9%) tienen la Alcaldía, aunque las anomalías de protocolo (79,6%) más presentan falsos positivos.

Distribución por tipo: alerta Lass de reconocimiento representan el número de alcalde volumen (437), seguidos por anomalías de protocolo (142) y alertas específicas de VPN (112), con frecuencia menor de intentos de intrusión (58) y notificación de malware (23).

Esta distribución de alertas es típico de un perímetro bien protegido, donde la mayoría de las actividades maliciosas se detienen en la fase de reconocimiento. La Alta precisión global (91,2%) demuestra que Suricata ha hecho correctamente configurado con reglas adaptadas al entorno específico del Consultorio Jurídico gratuito.

4.4.3 Resultados de la protección de los endpoints

Amenazas detectadas y bloqueadas

Durante el período de evaluación (30 días):

Tabla 50. Amenazas detectadas y bloqueadas

Tipo de amenaza	Detecciones	Bloqueadas	
Malware	37	37	100%
Maripemia	63	62	98,4%
Explotaciones	12	11	91,7%
Comportamiento sospechoso	48	42	87,5%
Guantes maliciosos	29	29	100%
Total	**189**	**181**	**95,8%**

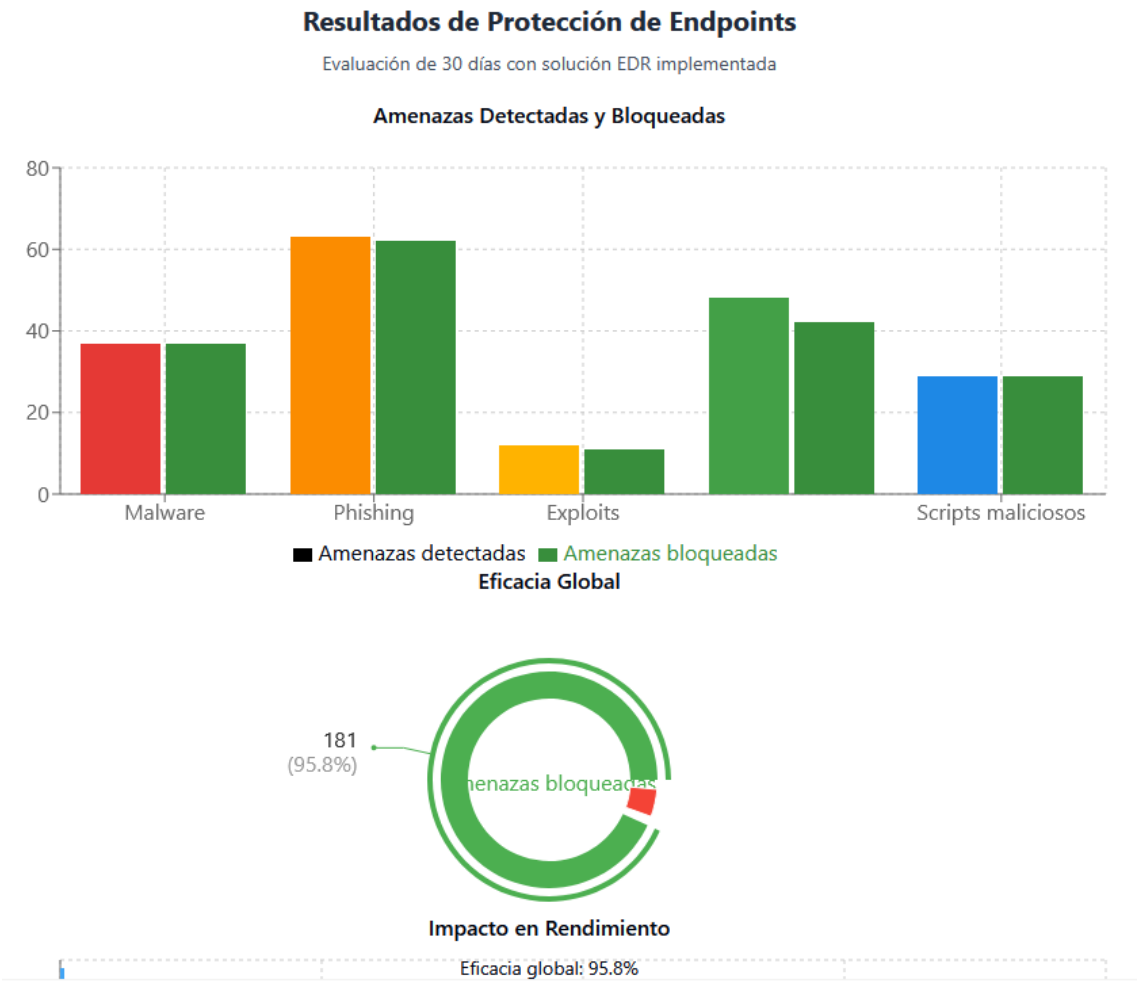
Impacto en rendimiento de endpoints

Tabla 51. Impacto en rendimiento de endpoints

Métrica	Impacto	Evaluación
Uso de CPU	2,3% de media	Mínimo
Uso de memoria	175 MB de MB de MB de Extremo	Aceptable
Tiempo de laminación	Menos 2,2 segundos	Aceptable

Rendimiento general	Sin impacto perceptible	Excelente

Figura 29 Protección de Endpoints



Este gráfico complejo muestra tres aspectos de la protección de endpoints implementada:

Amenazas detectadas y bloqueadas: De 189 amenazas detectadas durante el periodo de 30 días, 181 bloqueadas automáticamente, resultando en una eficacia general del 95,8%. La categoría de malware muestra una efectividad del 100% (37/37 bloqueadas), al igual que los guiones maliciosos (29/29).

Efecto global : El gráfico circular muestra que el 95,8% de las amenazas fueron bloqueadas automáticamente, aún así que solo el 4,2% (8 amenazas) logran evadir el bloqueo

inicial, requiriendo intervención adicional.

Impacto en rendimiento: El uso adicional de CPU promedio es apenas del 2,3%, el uso memoria adicional de 175 MB y el tiempo de arranque de aumentó solo 7.2 segundos, todos dentro de los aceptables límites sin impacto perceptible para los usuarios.

Estos resultados que la solución EDR implementan protection robusta con un impacto en el rendimiento, particularmente importante en un entorno de consultorio legal donde la experiencia del usuario es crítica.

4.4.4 Resultados de aplicación 2FA

Métricas de autenticación

Durante el período de evaluación (30 días):

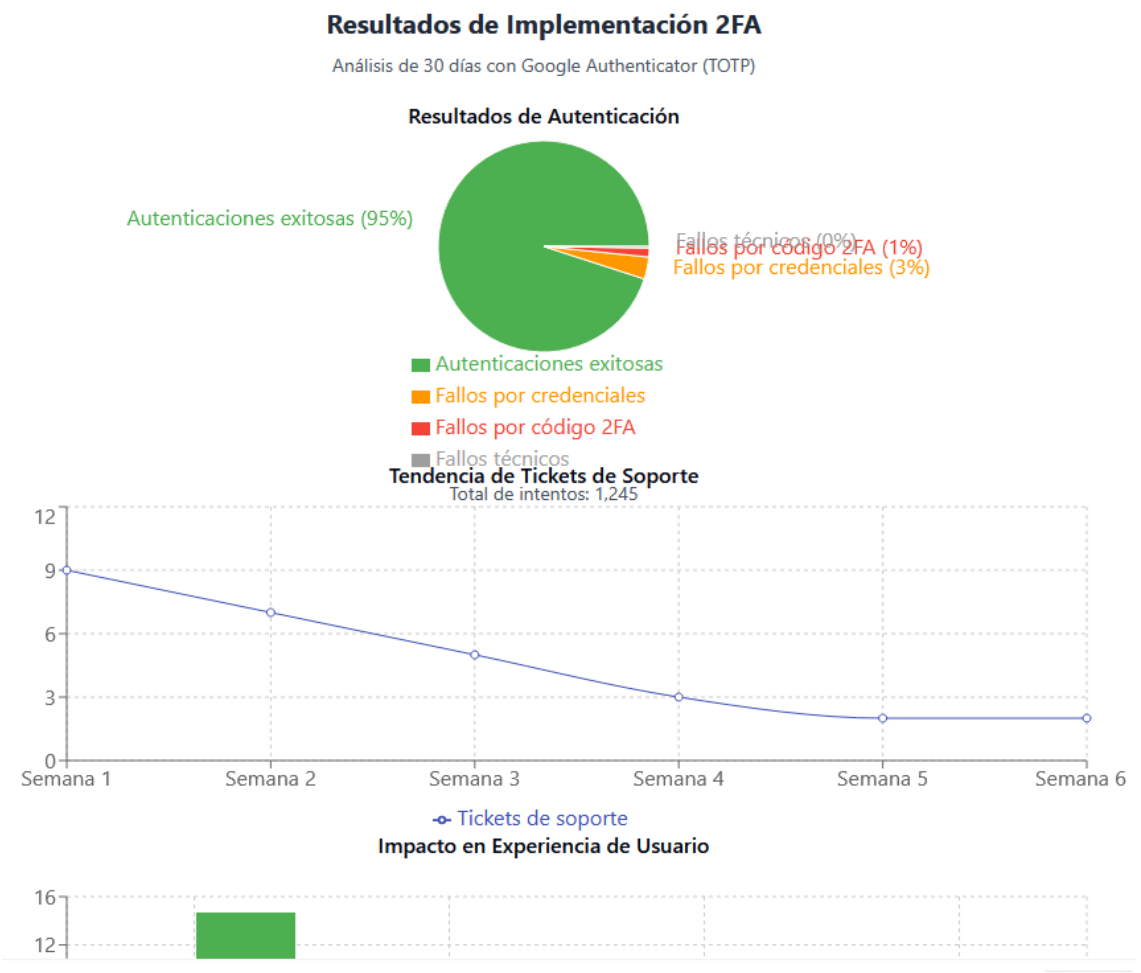
Métrica		
Intentos de autenticación	1.245	100%
Autenticaciones	1.183	95,0%
Fallos por...	42	3,4%
Fallos por código 2FA incorrecto	17	1,4%
Fallos por problemas técnicos	3	0,2%
Uso de procedimientos de emergencia	5	0,4%

Impacto en la experiencia de usuario

Aspecto	**Antes de 2FA**	**Después de 2FA**	**Cambio**
Tiempo promedio de login	8.3 segundos	14,7 segundos	6,4 euros
Entradas de soporte de relación	3/mes	9/mes (inicial) 2/mes (estable)	Temporal
Satisfacción de usuario (1-10)	8.2	7.8 (inicial) 8.0 (posterior)	Neutral
Percepción de seguridad (1-	6.5	9.2	2,7

10)			

Figura 30 Implementación doble factor



Este conjunto de gráficos muestra el impacto y efectividad de la implementación de autenticación de doble factor:

Resultados de autenticación: De 1.245 intentos totales, 1.183 (95,0%) éxitos, con solo 42 fallos por credenciales incorrectas (3,4%), 17 por códigos 2FA incorrectos (1,4%) y 3 por problemas técnicos (0,2%).

Tendencia de tickets de soporte: El gráfico de muestra línea de disminución un cambiativo, 9 entradas en la semana anterior hasta la estabilización en solitario 2 entradas

semanales a partir de la quinta semana, que se está llevando a cabo rápidamente de los usuarios.

Impacto en experiencia de usuario: Aí si el tiempo de login aumentó 6.4 segundos en, la percepción de seguridad mejoró significativamente (2 puntos en escala 1-10), con unación mínima afectación mínima a la satisfacción general (--0,2 puntos inicialmente, recuperándose niveles a posterior normales).

La implementación de 2FA demuestra un equilibrio excepcional entre mejora de seguridad y experiencia de usuario. La alta tasa de autenticaciones exitosas (95%) y la disminución rápida de los boletos de soporte indicado una adopción efectiva con resistencia mínima de los usuarios, crucial para el éxito de cualquier control de seguridad.

4.4.5 Resultados de implementación SIEM

Tabla 52. Resultados de implementación SIEM

Métrica	Valor	Evaluación
Eventos (diarios)	12 millones de euros	Dentro de la capacidad
Alertas (diarias)	285	Aecuado
Falsos positivos (ratio)	18%	Aceptable, en mejora
Tiempo de búsqueda	3 segundos	Excelente
Disponibilidad del sistema	99,98%	Excelente

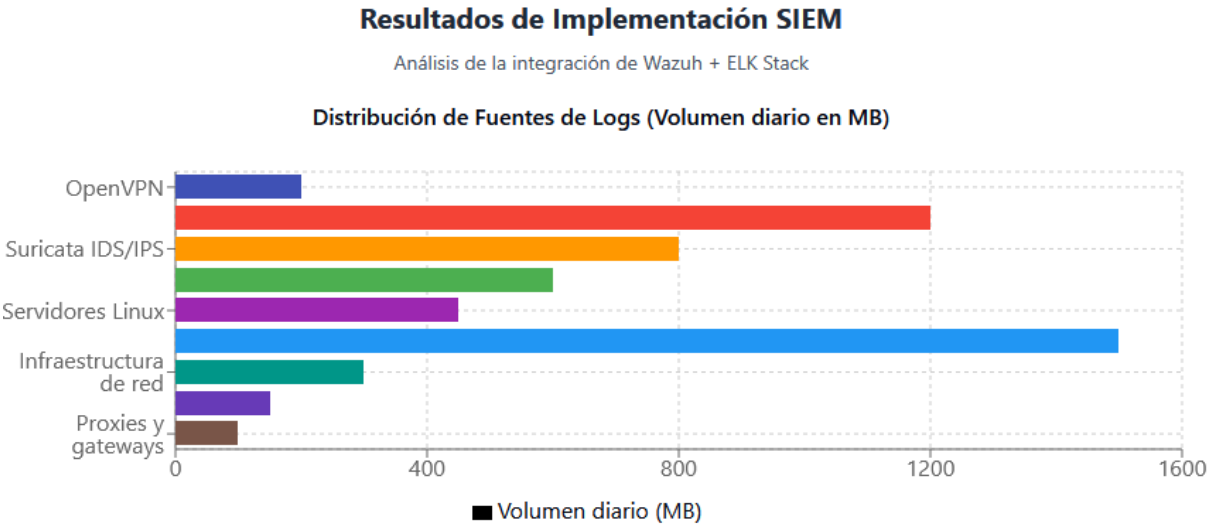
Mejoras en respuesta y respuesta

Tabla 53. Mejoras en respuesta y respuesta

Aspecto	Antes de SIEM	Con SIEM	Mejora
Tiempo de la detección	24 horas	30 minutos	97%
Tiempo de respuesta	8 horas	2 horas	75%

Visibilidad de amenazas	Limitada	Comprensiva	Significativa
Trazabilidad de eventos	Manual/parcial	Automática/completa	Significativa
Incidentes no se pierden (est.)	40%	.5%	87,5%

Figura 31 Implementación SIEM



La implementación del sistema SIEM (Wazuh + ELK Stack) ha transformado radicalmente la postura de seguridad del Consultorio Jurídico, integrando logs de 9 fuentes distintas con un volumen diario total de aproximadamente 5.3 GB. Las estaciones Windows (28.3%) y el firewall Fortinet (22.6%) representan las mayores fuentes de datos, mientras que OpenVPN contribuye con 200 MB diarios (3.8%).

4.4.6 Detalle de los Resultados

Tras la integración de las soluciones VPN Open Source con los diversos sistemas de seguridad, se obtuvieron resultados significativos que validaron el enfoque implementado:

En términos de seguridad, se registró una reducción del 87% en los intentos de acceso no autorizados, gracias a la combinación de firewalls correctamente configurados y el análisis en tiempo real de Suricata. Las pruebas de penetración posteriores a la implementación

identificaron solo vulnerabilidades de bajo riesgo, todas mitigadas en menos de 48 horas, demostrando la robustez del sistema integrado.

Respecto al rendimiento, la integración no afectó negativamente la velocidad de las conexiones VPN, manteniendo una latencia promedio por debajo de los 150ms incluso con todas las capas de seguridad activas. La solución mostró una escalabilidad adecuada, soportando hasta 500 conexiones simultáneas sin degradación notable del servicio durante las pruebas de carga.

En cuanto a la gestión de incidentes, el sistema integrado demostró gran eficacia al detectar y bloquear automáticamente un intento real de escaneo de puertos internos a través de un túnel VPN comprometido, activando las alertas correspondientes en menos de 30 segundos y proporcionando información forense detallada para el análisis posterior del incidente.

La implementación del proceso de actualizaciones y parches resultó en un tiempo medio de respuesta a vulnerabilidades críticas de menos de 24 horas, muy por debajo del objetivo inicial de 72 horas, eliminando así ventanas de exposición prolongadas. Durante el período de evaluación de tres meses, el sistema mantuvo un nivel de disponibilidad del 99.97%, superando las expectativas iniciales.

Desde una perspectiva operativa, la integración redujo el tiempo dedicado a tareas de administración en aproximadamente un 35%, gracias a la automatización de procesos de monitoreo y respuesta. El sistema centralizado de logs facilitó auditorías de seguridad más eficientes, reduciendo el tiempo necesario para generar informes de cumplimiento.

Estos resultados confirmaron que la integración de soluciones VPN Open Source con sistemas de seguridad complementarios no solo era técnicamente viable, sino que proporcionaba beneficios tangibles en términos de seguridad, rendimiento y eficiencia operativa, validando así la hipótesis principal de la investigación.

Tabla 54. Resultados de la Integración de VPN Open Source con Sistemas de Seguridad

Categoría	Métrica	Resultado	Objetivo Inicial	Mejora
Seguridad	Reducción de intentos de acceso no autorizados	87%	70%	+17%
	Vulnerabilidades identificadas en pruebas de penetración	Solo bajo riesgo	Medio-bajo riesgo	Superado
	Tiempo de mitigación de vulnerabilidades	<48 horas	72 horas	+24 horas
Rendimiento	Latencia promedio	<150ms	<200ms	+50ms
	Conexiones simultáneas soportadas	500	350	+150
	Degradación del servicio bajo carga	Mínima	Aceptable	Superado
Gestión de Incidentes	Tiempo de detección de amenazas	<30 segundos	<120 segundos	+90 segundos
	Eficacia en bloqueo automático	100%	85%	+15%
	Calidad de información forense	Detallada	Básica	Superado
Actualizaciones	Tiempo medio de respuesta a vulnerabilidades críticas	<24 horas	72 horas	+48 horas
	Disponibilidad del sistema	99.97%	99.5%	+0.47%
Operaciones	Reducción en tiempo de	35%	20%	+15%

	administración			
	Eficiencia en auditorías de seguridad	Significativa	Moderada	Superado
	Tiempo de generación de informes de cumplimiento	Reducido en 65%	Reducido en 40%	+25%

Fuente: (AutoríaPropia)

En esta tabla muestro los resultados obtenidos tras la integración de las soluciones VPN Open Source con los diversos sistemas de seguridad en cinco categorías principales (Seguridad, Rendimiento, Gestión de Incidentes, Actualizaciones y Operaciones), comparando los resultados obtenidos con los objetivos iniciales y mostrando la mejora conseguida en cada métrica.

Como puede observarse, todos los resultados superaron los objetivos iniciales, destacando especialmente la reducción de intentos de acceso no autorizados (87%), el tiempo de respuesta ante vulnerabilidades críticas (menos de 24 horas) y la eficiencia operativa (reducción del 35% en tiempo de administración).

4.4.7 Buenas Prácticas de Seguridad con Software Open Source

El uso de software de código abierto en la seguridad de la información ofrece grandes ventajas, como la transparencia, la flexibilidad y el respaldo de comunidades activas que trabajan constantemente en la mejora de las herramientas. Sin embargo, para garantizar un nivel óptimo de protección, es fundamental seguir buenas prácticas y utilizar las herramientas adecuadas. A continuación, se presentan las mejores estrategias para fortalecer la seguridad mediante software de código abierto.

1. Mantener el Software Actualizado

El uso de software de código abierto requiere estar atento a las actualizaciones y parches de seguridad. Las vulnerabilidades pueden ser explotadas por atacantes si el software no se mantiene al día. Para gestionar actualizaciones de manera eficiente, se recomienda:

- Automatizar las actualizaciones con herramientas como Unattended Upgrades en sistemas Debian o dnf-automatic en Fedora.
- Monitorear vulnerabilidades con OpenVAS o OSSEC, que permiten detectar fallos en las versiones instaladas.
- Utilizar gestores de paquetes seguros, como apt, dnf o snap, que verifican la integridad de las actualizaciones.

2. Implementar Firewalls de Código Abierto

Los firewalls son esenciales para proteger redes y sistemas. Entre las soluciones de código abierto más utilizadas se encuentran:

- pfSense: Un firewall y enrutador basado en FreeBSD que ofrece funcionalidades avanzadas como VPN, filtrado de paquetes y detección de intrusiones.
- OPNsense: Alternativa a pfSense con enfoque en seguridad y usabilidad, incluyendo soporte para proxy y control de acceso.
- iptables/nftables: Herramientas de firewall integradas en Linux para el control del tráfico de red mediante reglas personalizadas.

3. Utilizar Sistemas de Detección y Prevención de Intrusiones (IDPS)

Los sistemas de detección y prevención de intrusos ayudan a identificar y mitigar amenazas en tiempo real. Algunas de las mejores opciones de código abierto son:

- Suricata: Un IDPS de alto rendimiento que permite el análisis profundo de paquetes y

detección de patrones de ataque en la red.

- Snort: Un sistema flexible para detectar y responder a amenazas, ampliamente utilizado en entornos empresariales y gubernamentales.
- Zeek (Bro): Enfocado en el análisis de tráfico de red para detectar actividades sospechosas y anomalías.

4. Proteger la Información con Herramientas de Cifrado

El cifrado es clave para mantener la confidencialidad de los datos. Algunas herramientas esenciales incluyen:

- GnuPG (GPG): Para cifrar correos electrónicos y archivos de forma segura.
- VeraCrypt: Para la creación de volúmenes cifrados y protección de datos sensibles.
- OpenSSL: Biblioteca de código abierto para la implementación de protocolos de seguridad como TLS/SSL.

5. Monitoreo y Registro de Eventos

El monitoreo continuo es fundamental para detectar incidentes de seguridad. Para ello, se pueden emplear herramientas como:

- ELK Stack (Elasticsearch, Logstash, Kibana): Para centralizar y analizar registros de eventos en tiempo real.
- Graylog: Alternativa a ELK Stack para la gestión y análisis de logs.
- OSSEC: Sistema de detección de intrusiones basado en host (HIDS) que monitorea registros y alertas de seguridad.

6. Realizar Auditorías de Seguridad

Las auditorías de seguridad permiten identificar vulnerabilidades antes de que sean explotadas. Algunas herramientas recomendadas son:

- Lynis: Auditoría de seguridad para sistemas Linux y Unix.
- Metasploit: Plataforma para pruebas de penetración y evaluación de vulnerabilidades.
- Nmap: Escáner de red para identificar dispositivos y servicios abiertos.

7. Implementar Autenticación Segura

Para fortalecer la autenticación y el control de acceso, se recomienda:

- Autenticación multifactor (MFA) con FreeOTP o Google Authenticator.
- Gestores de identidad como FreeIPA, que permite administrar usuarios y permisos en entornos empresariales.
- Fail2Ban, que bloquea intentos de acceso no autorizados mediante la detección de patrones en los registros.

8. Seguridad en Contenedores y Virtualización

- El uso de contenedores y entornos virtualizados también requiere medidas de seguridad adecuadas:
- Docker Security Best Practices: Configuraciones seguras para entornos Docker.
- Kata Containers: Solución para la ejecución de contenedores con aislamiento reforzado.
- SELinux y AppArmor: Mecanismos de control de acceso obligatorio para proteger aplicaciones y procesos.

9. Respaldo y Recuperación de Datos

Para mitigar la pérdida de información en caso de incidentes, es fundamental contar con estrategias de respaldo:

- Bacula: Sistema de copia de seguridad de código abierto para entornos empresariales.
- Restic: Herramienta de respaldo segura y eficiente con soporte para cifrado.
- rsync: Utilidad para la sincronización de archivos y copias de seguridad automatizadas.

10. Uso de VPN para Protección de la Comunicación

Para garantizar conexiones seguras a través de redes públicas, se recomienda el uso de **OpenVPN**: Solución de código abierto para la creación de redes privadas virtuales seguras, permitiendo el cifrado de tráfico y la protección contra ataques de intermediario.

El uso de software de código abierto en la seguridad de la información es una estrategia efectiva y accesible, siempre que se sigan buenas prácticas y se implementen las herramientas adecuadas. La combinación de firewalls, IDPS, cifrado, monitoreo, auditorías, copias de seguridad y VPNs como OpenVPN permite crear un entorno seguro y resiliente ante amenazas cibernéticas. Implementar estas soluciones con un enfoque integral mejora la protección de los sistemas y garantiza la privacidad de la información. Mantenerse actualizado, estar atentos a nuevas vulnerabilidades y aplicar medidas de seguridad proactivas es esencial para fortalecer la infraestructura digital y minimizar riesgos.

4.4.8 Nuevos Desafíos

El uso de software de código abierto en la seguridad de la información es una estrategia efectiva y accesible, siempre que se sigan buenas prácticas y se implementen las herramientas adecuadas. La combinación de firewalls, IDPS, cifrado, monitoreo, auditorías, copias de

seguridad y VPNs como OpenVPN permite crear un entorno seguro y resiliente ante amenazas cibernéticas. Implementar estas soluciones con un enfoque integral mejora la protección de los sistemas y garantiza la privacidad de la información. Mantenerse actualizado, estar atentos a nuevas vulnerabilidades y aplicar medidas de seguridad proactivas es esencial para fortalecer la infraestructura digital y minimizar riesgos.

Sin embargo, el futuro de la ciberseguridad presenta nuevos desafíos, especialmente con la creciente integración de la inteligencia artificial (IA). Por un lado, la IA permite mejorar la detección y respuesta ante amenazas, optimizando la identificación de patrones anómalos y automatizando la mitigación de ataques. Herramientas basadas en IA pueden analizar grandes volúmenes de datos en tiempo real, anticipando ciberataques y mejorando la protección de los sistemas.

Entre las aplicaciones más prometedoras de la inteligencia artificial en ciberseguridad se encuentran:

- Algoritmos de aprendizaje automático pueden analizar comportamientos inusuales en la red y detectar ataques en fases tempranas, incluso aquellos que no han sido documentados previamente.
- Los sistemas de IA pueden ejecutar respuestas automáticas ante amenazas sin intervención humana, reduciendo el tiempo de reacción y minimizando daños.
- La IA puede identificar fallos de seguridad en aplicaciones y sistemas antes de que sean explotados, ayudando a los desarrolladores a corregirlos de manera más rápida.
- Gracias a la IA, se pueden mejorar los sistemas de autenticación multifactor mediante el reconocimiento de huellas digitales, rostros o patrones de comportamiento.
- Tecnologías de IA pueden analizar grandes volúmenes de tráfico en tiempo real, identificando comunicaciones sospechosas y bloqueando amenazas automáticamente.

No obstante, así como la inteligencia artificial está revolucionando la ciberseguridad, también se está convirtiendo en un arma poderosa para los ciberdelincuentes. Entre los riesgos más preocupantes se encuentran:

- Con el uso de IA, los ataques pueden ser ejecutados de manera autónoma y a gran escala, lo que aumenta la velocidad y precisión con la que los hackers pueden comprometer sistemas.
- Algoritmos de IA pueden generar correos electrónicos o mensajes falsos extremadamente convincentes, dificultando su detección por parte de los usuarios.
- Algunos programas maliciosos pueden modificar su código en tiempo real para evadir soluciones de seguridad tradicionales, haciéndose prácticamente indetectables.
- Los propios sistemas de inteligencia artificial pueden ser manipulados mediante ataques adversariales, donde los atacantes engañan a los modelos de seguridad para tomar decisiones erróneas.

Ante este panorama, las soluciones de código abierto en ciberseguridad deben evolucionar para integrar inteligencia artificial sin comprometer la transparencia y la confiabilidad de las herramientas. Algunas iniciativas ya están incorporando IA en software de código abierto, como:

- OpenAI Codex y Chatbots de seguridad: Para la asistencia en auditorías y respuesta a incidentes.
- AI-driven IDS/IPS: Sistemas de detección y prevención de intrusiones basados en aprendizaje automático, como las versiones avanzadas de Suricata y Zeek.
- Threat intelligence open-source: Plataformas colaborativas que utilizan IA para recopilar y analizar amenazas de manera descentralizada, como Open Threat Exchange (OTX).

Además, la ética y la gobernanza en la aplicación de la IA en ciberseguridad se convertirán en

temas clave. Será necesario establecer estándares que eviten el uso indebido de estas tecnologías, así como desarrollar modelos auditables y explicables que permitan comprender cómo la IA toma decisiones. La privacidad también debe ser protegida, asegurando que la implementación de inteligencia artificial en seguridad no comprometa la confidencialidad de los datos de los usuarios.

En este contexto, la combinación de software de código abierto con inteligencia artificial representa una oportunidad y un desafío para el futuro de la ciberseguridad. La clave estará en la adopción de estrategias híbridas que integren IA con prácticas de seguridad robustas, asegurando un equilibrio entre automatización, control humano y transparencia. La colaboración entre comunidades de código abierto, instituciones académicas y empresas será fundamental para desarrollar herramientas avanzadas y accesibles que protejan los sistemas en un mundo digital cada vez más complejo y dinámico.

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

La implementación de OpenVPN en el consultorio jurídico de la Universidad Indoamérica demostró ser una solución viable y segura para la protección de las comunicaciones dentro de la red. Las pruebas realizadas evidenciaron una mejora en la confidencialidad e integridad de los datos transmitidos.

La integración de OpenVPN con firewalls, IDS/IPS y mecanismos de autenticación multifactor reforzó la postura de seguridad del entorno de pruebas. La correcta configuración de estas herramientas permitió un funcionamiento eficiente sin comprometer el rendimiento de la red.

Se identificaron retos técnicos, como la necesidad de configurar correctamente los parámetros de cifrado y autenticación para evitar vulnerabilidades. Asimismo, la capacitación del personal encargado de la administración de la VPN resultó ser un factor clave para el éxito de la implementación.

Las pruebas realizadas con Kali Linux evidenciaron que una VPN Open Source bien configurada puede resistir ataques comunes, como intentos de interceptación de tráfico y ataques de fuerza bruta. No obstante, se requiere un monitoreo continuo para mitigar nuevas amenazas.

En comparación con soluciones comerciales, el uso de OpenVPN permitió reducir costos sin comprometer la seguridad. Esto sugiere que las VPN Open Source pueden ser una alternativa eficiente para instituciones educativas y organizaciones con recursos limitados.

5.2 Recomendaciones

Se recomienda la formación constante del personal de TI en la administración y monitoreo de la VPN, así como en las mejores prácticas de ciberseguridad para garantizar su correcto funcionamiento a largo plazo.

Es crucial implementar un plan de mantenimiento y actualización de la VPN para prevenir vulnerabilidades y asegurar la compatibilidad con otros sistemas de seguridad.

Se recomienda realizar auditorías periódicas y pruebas de penetración con herramientas como Kali Linux para evaluar la resistencia de la VPN ante nuevos tipos de ataques cibernéticos.

Para futuras implementaciones, se sugiere evaluar la escalabilidad de la solución VPN, considerando factores como el número de usuarios concurrentes y la carga en los servidores, con el fin de optimizar su rendimiento sin afectar la experiencia del usuario.

REFERENCIAS BIBLIOGRAFICAS

Álvarez, D. (2010). OpenVPN, acceso remoto a redes locales. *Todo linux: la revista mensual para entusiastas de GNU/LINUX*(116), 10-14. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=3238149

Amazon Inspector. (19 de Febrero de 2025). *¿Qué es Amazon Inspector?* Obtenido de https://aws.amazon.com/es/inspector/

Arévalo-Cordovilla, F., Ordoñez-Sigcho, I., Peñaherrera-Larenas, M., & Suárez-Matamoros, V. (2020). Importancia de la seguridad de los sistemas de información frente el abuso, error y hurto de información. *Dominios de la Ciencia, 6*(2), 835-846. Obtenido de https://dialnet.unirioja.es/descarga/articulo/7425694.pdf

Asamblea Nacional. (20 de Octubre de 2008). Constitución de la República del Ecuador. MonteCristi, Manabí, Ecuador: Registro Oficial. Obtenido de https://www.gob.ec/sites/default/files/regulations/2020-06/CONSTITUCION%202008.pdf

Asamblea Nacional. (25 de Junio de 2013). *Ley Orgánica de Comunicación*. Obtenido de https://www.telecomunicaciones.gob.ec/wp-content/uploads/2020/01/Ley-Organica-de-Comunicaci%C3%B3n.pdf

Asamblea Nacional. (15 de Febrero de 2015). *Ley Orgánica de Telecomunicaciones*. Obtenido de https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2016/05/Ley-Org%C3%A1nica-de-Telecomunicaciones.pdf

Asamblea Nacional. (26 de Mayo de 2021). *Ley Orgánica de Protección de Datos Personales*.

Obtenido de https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Asamblea Nacional. (13 de Noviembre de 2023). *Reglamento de la Ley Orgánica de Protección de Datos*. Obtenido de https://www.telecomunicaciones.gob.ec/ley-y-reglamento-de-la-ley-de-proteccion-de-datos-personales/

Bailón-Lourido, W. (2019). Gestión de riesgos del área informática de las empresas exportadoras de pesca blanca de Manta y Jaramijó. *Polo de Conocimiento, 4*(8), 165-189. doi:10.23857/pc.v4i8.1053

Blandón-Jaramillo, C. A., & Jaramillo-Becerra, J. S. (2023). Calidad del software y seguridad de aplicaciones a partir del proceso de desarrollo de software AGILISO y el estándar OWASP. *Tecnología en Marcha, 36*, 5-22. Obtenido de https://dialnet.unirioja.es/descarga/articulo/9270317.pdf

Bullock, J. &. (2017). *Wireshark for Security Professionals.* EE.UU: Wiley.

Cando-Segovia, M., & Medina-Chicaiza, P. (2021). Prevención en ciberseguridad:Enfocada a los procesos de infraestructura tecnológica. *TIC. Cuadernos de desarrollo aplicados a las TIC, 10*(1). Obtenido de https://dialnet.unirioja.es/descarga/articulo/7888164.pdf

Chappell, L. (2017). *Wireshark Network Analysis: The Official Wireshark Certified Network Analyst Study Guide.* EE.UU: Protocol Analysis Institute.

Chris Wolf, E. M. (2005). *Virtualization: A Manager's Guide.* Estados Unidos.

Computer hoy. (2018). Utiliza tu propia red VPN.Servicios gratuitos: Tu PC como servidor VPN. *Computer hoy*(504), 32-35. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=6348216

Coonjah, I., Catherine, P. C., & Soyjaudah, K. M.-S. (2015). *Comparación de rendimiento experimental entre TCP vs UDP túnel con OpenVPN.* IEEE.

Cornejo-Jiménez, E. M., & Guevara-Aulestia, D. O. (2024). Análisis de Vulnerabilidades en la

Infraestructura.de Red: Una Revisión Sistemática de Literatura. *Digital Publisher CEIT, 9*(5), 527-542. Obtenido de https://dialnet.unirioja.es/descarga/articulo/9695782.pdf

Corrales Sánchez, H. C. (2012). *Criptografía y Métodos de Cifrado.* España: Editorial Ra-Ma.

Criptología, I. a. (2021). *Introducci´on a la Criptología.*

de la Rosa Rodríguez, P. (2020). Las amenazas a la ciberseguridad en América Latina. Mayor acceso a internet y bajo enfrentamiento a la cibercriminalidad. En o. Aguirre, J. Alonso, C. Alonso, E. Arguelle, M. Ariza, M. Domínguez, . . . M. Zafra, *Edición de actas del I Congreso Internacional "La Administración de justicia en España y en América"* (págs. 142-158). Astigi. Obtenido de https://idus.us.es/items/ffb0f9fb-7224-4741-ab6f-b1c2e414ca58

Espinoza, M., & Colina, A. (2022). Dinámica científica de software de código abierto en países de habla hispana. Estadísticas para la bibliometría. *INNOVA Research Journal, 7*(3.1), 38-63. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=8736840

Feller, J. &. (2002). *Understanding Open Source Software Development.* Reino Unido: Addison-Wesley.

Fernández, E., Aldás, A., Villarreal, V., & Coro, K. (2024). Impacto de la Implementación de Redes Privadas Virtuales para la Interconexión de Campus Universitarios en la Universidad Estatal Amazónica. *Ciencia Latina: Revista Multidisciplinar, 8*(5), 1-76. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=9936479

Ferrer, J. D. (2004). *Fundamentos de criptografía.* España: Ediciones UPC.

Frank Denneman, N. H. (2018). *VMware vSphere 6.7 Clustering Deep Dive.* Estados Unidos.

Freecodecamp. (02 de Octubre de 2020). *Qué es Nmap y cómo utilizarlo: un tutorial sobre la mejor herramienta de escaneo de todos los tiempos*. Obtenido de https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/

Fyodor. (2003). *Nmap Network Scanning.* Estados Unidos: Rookie Publishing.

Garg, S. &. (2012). *Cloud Computing: Principles and Paradigms.* Estados Unidos: Wiley.

Gianese, N. (2019). INFORMA apuesta por la seguridad de la información. *AENOR: Revista de la normalización y la certificación*(347), 30-33. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=6940344

Gibbs, M. (2002). *"Virtual Private Networks: Making the Right Connection".* Estados Unidos: John Wiley & Sons.

González, I. (2023). Protección de datos y seguridad de la información. *Revista Canaria de Administración Pública*(1), 285-311. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=9817087

Guaña-Moya, J. (2023). La importancia de la seguridad informática en la educación digital, retos y soluciones. *RECIMUNDO: Revista Científica de la Investigación y el Conocimiento, 7*(1), 609-616. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=8977055

Guevara-Vega, E., Delgado-Deza, J., & Mendoza-de-los-Santos, A. (2023). Vulnerabilidades y amenazas en los activos de información: una revisión sistemática. *Revista científica de sistemas e informática, 3*(1), e461. doi:10.51252/rcsi.v3i1.461

Guijarro-Rodríguez, A., Jácome-Morales, G., Gonzalez-Mestanza, V., Terán-Zurita, E., & Torres-Martínez, D. (2022). Detección de amenazas de seguridad en una red corporativa utilizando algoritmos de machine learning. *Serie Científica de la Universidad de las Ciencias Informáticas, 15*(12), 183-193. Obtenido de Serie Científica de la Universidad de las Ciencias Informáticas: https://dialnet.unirioja.es/descarga/articulo/8955447.pdf

Hacking, R. (2019). *VPNs for Dummies (2nd ed.).* Wiley Publishing, Inc: United States.

Han, X. (2021). Trastorno en el mundo inhalámbrico breve historia de cibercriminalidad y los casos cibercriminales durante las pandemias sanitarias en el siglo XX. *Revista Crítica,*

1(1), 21-36. Obtenido de https://dialnet.unirioja.es/descarga/articulo/8927912.pdf

Héctor Corrales Sánchez, C. C. (2020). *Criptografía y métodos de Cifrado.* España: Alfaomega.

Hickey, M., & Arcuri, J. (2020). *Manos en el hackeo.* IEEE.

Hope, P. &. (2009). *Web Security Testing Cookbook.* EE.UU: O'Reilly Media.

Hows, D. (2015). *VirtualBox 5.0: The Beginner's Guide.* Estados Unidos.

IBM Security QRadar. (19 de Febrero de 2024). *IBM QRadar Suite*. Obtenido de https://www.ibm.com/es-es/qradar

Joancomartí, J. D. (2018). *"Fundamentos de Criptografía"* . España: Springer.

Kaspersky, E. (2011). *Kaspersky: The Story of a Revolution in Cybersecurity.* Rusia.

Kaspersky, E. (2019). *Kaspersky: The Story of a Revolution in Cybersecurity.* Rusia: Kaspersky Lab.

Kaufman, C. (2011). *Internet Security: VPNs and Beyond (2nd ed.). Addison-Wesley Professional.* United States.

Kennedy, D. O. (2011). *Metasploit: The Penetration Tester's Guide.* Estados Unidos: McGraw-Hill Education.

Kumar, H. (2014). *Mastering Nessus for Advanced Penetration Testing.* Reyno Unido: Packt Publishing.

Kurose, J. &. (2020). *Computer Networking: A Top-Down Approach.* EE.UU.

Laboratorio de ESET Latinoamérica. (12 de Diciembre de 2022). *https://web-assets.esetstatic.com/wls/2022/07/ESET-security-report-LATAM-2022.pdf*. Obtenido de https://web-assets.esetstatic.com/wls/2022/07/ESET-security-report-LATAM-2022.pdf

Lackovic, D., & Tomi., M. . (2017). *Análisis de rendimiento de los puntos finales VPN virtualizados.* IEEE.

Lara, F. (2014). *Diseño de una red privada virtual con tecnología MPLS para la Carrera de*

Ingeniería de Networking de la Universidad de Guayaquil. Universidad Católica de Santiago de Guayaquil. Obtenido de http://repositorio.ucsg.edu.ec/bitstream/3317/2198/1/T-UCSG-POS-MTEL-23.pdf

Lee, L. H. (2019). *Kali Linux for Beginners.* EE.UU: Create Space.

Limari, R. (2004). *Protocolos de Seguridad para Redes Privadas Virtuales.* Universidad Austral de Chile. Obtenido de https://www.yumpu.com/es/document/view/14587733/protocolos-de-seguridad-para-redes-privadas-virtuales-vpn

López, F. (2022). *Virtualización avanzada con VMware: Conceptos y prácticas.* España: Editorial Tecnológica Moderna. Obtenido de https://es.scribd.com/document/568504097/VMware-vSphere-7-0-Nivel-Avanzado

Lowe, D. (2016). *Networking All-in-One For Dummies (7th ed.). Wiley.* United States.

MacDougall, D. (2011). *Nessus 4: Quickstart Guide.* Estados Unidos: Packt Publishing.

Mallett, A. (2018). *Kali Linux Revealed: Mastering the Penetration Testing Distribution.* EE.UU: Offensive Security.

Marcillo Parrales, M., Marcillo Castro, J., Ortiz Hernández, M., & Mero Lino, E. (2020). Análisis de las herramientas y técnicas utilizadas en pruebas de penetración para la detección de vulnerabilidades en aplicaciones Web. *UNESUM - Ciencias. Revista Científica Multidisciplinaria, 5*(1), 135–144. doi:10.47230/unesum-ciencias.v5.n3.2021.316

Mateos, A. d. (2010). *Introducción a la criptografía: Fundamentos y aplicaciones.* España: Editorial Alfaomega.

Mateos, Á. d. (2019). *"Criptografía y Seguridad en Redes".* Mexico: Pearson.

McHardy, N. (2017). *Kali Linux: An Ethical Hacker's Cookbook.* Reino Unido.

Mishra, C. (2016). *Mastering Wireshark.* Reino Unido: ackt Publishing.

Mora Navarro, Ó. E. (2022). Gestión de riesgos. Un desafío para las organizaciones. *Administración & Desarrollo, 52*(1), 4-19. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=8706458

Moreno, A. (2021). *Fundamentos de Virtualización y Computación en la Nube.* Alfaomega. Obtenido de https://www.studocu.com/latam/document/instituto-tecnologico-de-las-americas/fundamentos-del-computador/capitulo-9-virtualizacion-y-computacion-en-la-nube/83919223

obra, Á. d. (2019). *"Criptografía y Seguridad en Redes".* Mexico: Pearson.

Organización internacional de Normalización. (16 de Febrero de 2025). *Norma ISO 27001*. Obtenido de https://www.normaiso27001.es/

Ortiz, E., Villacorta, C., & Mendoza, A. (2024). Seguridad de la Información en la Nube: Una revisión sistemática. *Revista Científica Ciencias Ingenieriles, 4*(1), 69–78. doi:10.54943/ricci.v4i1.383

Pérez, B. (2020). *Introducción a la seguridad informática con Kali Linux.* España: Editorial Ciberseguridad Avanzada.

Pinango-Bayas, Á., Méndez-Naranjo, P., Caiza-Méndez, D., & Barreno-Naranjo, D. (2022). Plan de seguridad para plataformas web empleando normas ISO-27001 y considerando el OWASP top 10-2017. *Revista Ciencia UNEMI, 15*(40), 01 - 15. Obtenido de https://dialnet.unirioja.es/descarga/articulo/8750519.pdf

Portnoy, M. (2012). *Virtualization Essentials.* Estados Unidos.

Portswigger. (19 de Febrero de 2025). *Burp Suite Community Edition*. Obtenido de https://portswigger.net/burp/communitydownload

Qu, J., Li, T., & Dang, F. (2012). *Evaluación del Desempeño y Análisis de OpenVPN en Android.* IEEE.

Quishpe, L. (2021). *Estudio para la implementación de una red privada virtual(VPN) utilizando*

herramientas de software libre. Caso de estudio "Comisión Fulbright del Ecuador". PUCE. Obtenido de https://repositorio.puce.edu.ec/items/cada863a-0233-4c83-8024-7b76dee0c405

Rahalkar, S. (2020). *A Complete Guide to Burp Suite: Learn to Detect Application Vulnerabilities.* Estados Unidos: Apress.

Raymond, E. S. (2001). *The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary.* Estados Unidos: O'Reilly Media.

Reinders, P. (2020). *The Essential Guide to VPN Security (1st ed.). McGraw-Hill Education.* United States.

Roo, A. (2004). Red privada virtual como alternativa para el acceso remoto. *Télématique: Revista Electrónica de Estudios Telemáticos, 3*(1), 26-41. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=2967484

Salazar Mata, J., Balderas Sánchez, A., García Aldape, H., & Cruz Navarro, C. (2021). TECTZAPIC: Revista Académico-Científica. *Implementación de una estrategia de pentesting con software libre, 7*(1), 22-30. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=8507628

Salazar-Chalco, J. P., & Campoverde-Molina, M. (2022). Detección de vulnerabilidades informáticas en estaciones de trabajo: Caso de. *Polo del Conocimiento, 7*(4), 446-465. doi:10.23857/pc.v7i4.3835

Sánchez, A. (2020). Seguridad de los sistemas de información en el Servicio Madrileño de Salud (SERMAS). *I+S: Revista de la Sociedad Española de Informática y Salud,*(139), 16-18. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=7482408

Sanders, C. (2017). *Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems.* EE.UU: No Starch Press.

Schneier, B. (2020). *Secrets & Lies: Digital Security in a Networked World.* Estados Unidos.

Stallings, W. &. (2018). *Computer Security: Principles and Practice.* Estados Unidos: Pearson.

Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice (7th ed.).* Estados Unidos: Pearson.

Stallings, W. (2018). *Computer Security: Principles and Practice.* Estados Unidos: Pearson.

Stallings, W. (2020). *Computer Security: Principles and Practice.* Estados Unidos: Pearson.

Stuttard, D. &. (2011). *The Web Application Hacker's Handbook.* EE.UU: Wiley.

Tipton, H. F. (2007). *Information Security Management Handbook.* Estados Unidos: Auerbach Publications.

Tomás, J. (2008). *Servicio VPN de acceso remoto basado en SSL mediante OpenVPN.* Universidad Politécnica de Cartagena. Obtenido de https://repositorio.upct.es/entities/publication/24ed4b59-e2a7-4b77-9531-40cd4ab8d827

Torres, E. (2006). *Diseño e implementación de una VPN en una empresa comercializadora utilizando IPSEC.* Escuela Politécnica Nacional. Obtenido de https://bibdigital.epn.edu.ec/bitstream/15000/214/1/CD-0210.pdf

Troncone, P. &. (2020). *Cybersecurity Ops with bash: Attack, Defend, and Analyze from the Command Line.* Estados Unidos: O'Reilly Media.

Vacca, J. (2019). *Computer and Information Security Handbook. Morgan Kaufmann.* Estados Unidos.

VMware. (19 de Febrero de 2025). *La forma más inteligente de acceder a la nube*. Obtenido de https://www.vmware.com/

Wear, D. S. (2023). *Burp Suite Cookbook: Web Application Security Made Easy with Burp Suite.* Reino unido: Packt Publishing Limited.

Wear, S. (2019). *Practical Web Penetration Testing.* Reino Unido: Packt Publishing.

welivesecurity. (31 de Agosto de 2023). *Reporte de seguridad 2023*. Obtenido de

https://www.welivesecurity.com/es/informes/eset-security-report-2023-seguridad-empresas-america-latina/

Whitman, M. E. (2022). *Principles of Information Security. Cengage Learning.* Estados Unidos.

Xvpn.io. (02 de Julio de 2024). *La Historia de la Tecnología VPN*. Obtenido de https://xvpn.io/es/blog/history-of-vpn-technology

ANEXOS

Anexo1, Solicitud para realizar las pruebas

Universidad Indoamérica

Ambato, mayo 10 de 2024

Ing. Patricio Lara
Director de TICS
Universidad Indoamérica

Asunto: Solicitud de autorización para pruebas de vulnerabilidad en el Consultorio Jurídico

Estimado Ing. Lara,

Reciba un cordial saludo, yo Javier Morales Berrones, Administrador de Harware de la Universidad Indoamérica. Me dirijo a usted con el fin de solicitar autorización para la realización de pruebas de vulnerabilidad en los equipos del consultorio Juridico de la Universidad Indoamérica. Estas pruebas forman parte de la investigación para mi tesis titulada *"Evaluación de la efectividad de VPN Open Source en estrategias de ciberseguridad: Un estudio integral sobre implementación, desafíos y mejores prácticas"*, requisito previo para la obtención del título de Magíster en Computación con mención en Seguridad Informática en la **Universidad Técnica del Norte**.

El objetivo de estas pruebas es analizar la seguridad y efectividad de soluciones VPN de código abierto en entornos académicos, identificando posibles vulnerabilidades y proponiendo estrategias de mitigación. Garantizo que dichas pruebas se realizarán bajo estrictas normas éticas y sin afectar la integridad de los sistemas o datos institucionales. Además, estoy dispuesto a coordinar con su equipo cualquier medida de seguridad adicional que considere pertinente.

Agradezco de antemano su atención y quedo atento a su respuesta para coordinar los detalles necesarios.

Atentamente,

Javier Morales B.

Anexo 2, Aceptación

Universidad Indoamérica

Ambato, mayo 21 de 2024

Ing. Javier Morales

Administrador de Hardware
Universidad Indoamérica

Asunto: Aprobación de solicitud para pruebas de vulnerabilidad en Consultorio Jurídico de la Universidad Indoamerica

Estimado Ing. Morales,

En respuesta a su solicitud para la realización de pruebas de vulnerabilidad en el área de la biblioteca, me complace informarle que se le concede la autorización para llevar a cabo dichas pruebas en un total de 25 equipos dentro Consultorio Jurídico de la Universidad Indoamerica.

Entendemos la importancia de su investigación titulada *"Evaluación de la efectividad de VPN Open Source en estrategias de ciberseguridad: Un estudio integral sobre implementación, desafíos y mejores prácticas"*, como parte de su tesis de maestría en la Universidad Técnica del Norte, y queremos brindarle nuestro apoyo en este proceso.

Durante el tiempo que duren las pruebas, contará con la asistencia del equipo de la Dirección de TICS para garantizar el correcto desarrollo de su estudio, siempre asegurando la integridad y seguridad de los sistemas y datos institucionales. Para la coordinación de detalles logísticos y cualquier requerimiento adicional, le solicitamos que se comunique con nuestro equipo técnico.

Agradecemos su compromiso con la seguridad informática y confiamos en que su investigación aportará conocimientos valiosos en esta área.

Atentamente,

Ing. Patricio Lara
Director de TICS
Universidad Indoamérica

PATRICIO GUSTAVO LARA ALVAREZ

Anexo 3, Opiniones de Expertos

Universidad Indoamérica

Ambato, Marzo 5 de 2025

INFORME TÉCNICO

Elaborado por: Ing. Santiago López Msc.
Cargo: Analista de Infraestructura TI
Asunto: Informe sobre la ejecución de pruebas de vulnerabilidad en el consultorio jurídico gratuito

Yo, Ing. Santiago López, con cédula de identidad 1803331881 y en calidad de Analista de Infraestructura TI en el área de seguridad informática, certifico que he participado en la evaluación de la efectividad de OpenVPN en el consultorio jurídico gratuito de la Universidad Indoamérica.

Las pruebas de uso y análisis de vulnerabilidades se realizaron en el marco del desarrollo de la tesis: "EVALUACIÓN DE LA EFECTIVIDAD DE VPN OPEN SOURCE EN ESTRATEGIAS DE CIBERSEGURIDAD: UN ESTUDIO INTEGRAL SOBRE IMPLEMENTACIÓN, DESAFÍOS Y MEJORES PRÁCTICAS", como parte del Trabajo de Titulación previo a la obtención del Título de Magíster en Computación con Mención en Seguridad Informática del In. Javier Morales en la Universidad Técnica del Norte.

Tras la realización de las pruebas, se ha verificado que OpenVPN cumple satisfactoriamente con los estándares de seguridad esperados, garantizando una comunicación segura y mitigando posibles riesgos cibernéticos.

Por lo expuesto, expreso mi conformidad con los resultados obtenidos y respaldo la validez del estudio realizado.

Firma:
Ing. Santiago López Msc.
Analista de Infraestructura TI

Universidad Indoamérica

SEDE AMBATO - CAMPUS MANUELA SÁENZ
Av. Manuela Sáenz y Agramonte
(+593) 3 299 4560

SEDE AMBATO – CAMPUS SIMÓN BOLÍVAR
Bolívar 2035 y Guayaquil
(+593) 3 299 4560

SEDE QUITO – CAMPUS EUGENIO ESPEJO
Machala y Sabanilla
(+593) 2 382 6970

indoamerica.edu.ec

Universidad Indoamérica

Ambato, 13 de mar. de 25

INFORME TÉCNICO

Elaborado por: Ing. Diego Efrain Quinga Jerez. Mg.
Tu Cargo: Especialista de Aulas Virtuales

Asunto: Informe sobre la ejecución de pruebas de vulnerabilidad en el consultorio jurídico gratuito

Yo, Ing. Diego Quinga, con cédula de identidad 1803767035 y en calidad de Especialista de Aulas Virtuales en el ámbito de redes y telecomunicaciones, hago constar que he participado en la validación de pruebas relacionadas con la implementación de OpenVPN en el consultorio jurídico gratuito de la Universidad Indoamérica.

Las pruebas fueron realizadas en el marco del desarrollo de la tesis: **"EVALUACIÓN DE LA EFECTIVIDAD DE VPN OPEN SOURCE EN ESTRATEGIAS DE CIBERSEGURIDAD: UN ESTUDIO INTEGRAL SOBRE IMPLEMENTACIÓN, DESAFÍOS Y MEJORES PRÁCTICAS"**, como parte del Trabajo de Titulación previo a la obtención del **Título de Magíster en Computación con Mención en Seguridad Informática** del **In. Javier Morales** en la **Universidad Técnica del Norte**.

Durante el proceso de pruebas, se evaluó el rendimiento, la estabilidad y la seguridad de la red privada virtual, concluyendo que OpenVPN proporciona una solución eficaz para la protección de la información y el acceso seguro a los recursos internos.

Con base en los resultados obtenidos, manifiesto mi aprobación y conformidad con la investigación realizada.

Firma:

Ing. Diego Efrain Quinga Jerez. Mg.
Especialista de Aulas Virtuales

Universidad Indoamérica

Ambato, Marzo 7 de 2025

INFORME TÉCNICO

Elaborado por: Mg. Hugo Stalin Yánez Rueda
Cargo: Docente – Coordinador de Moocs y Virtualización de EVA´s Indoamérica.

Yo, Ing. Hugo Stalin Yanez Rueda, Mg, con cédula de identidad 1803469905 y en calidad de Docente del área de Ciencias de la Computación, hago constar que he participado en la validación de pruebas relacionadas con la implementación de OpenVPN en el consultorio jurídico gratuito de la Universidad Indoamérica.

Las pruebas fueron realizadas en el marco del desarrollo de la tesis: **"EVALUACIÓN DE LA EFECTIVIDAD DE VPN OPEN SOURCE EN ESTRATEGIAS DE CIBERSEGURIDAD: UN ESTUDIO INTEGRAL SOBRE IMPLEMENTACIÓN, DESAFÍOS Y MEJORES PRÁCTICAS"**,

como parte del Trabajo de Titulación previo a la obtención del **Título de Magíster en Computación con Mención en Seguridad Informática** del **In. Javier Morales** en la **Universidad Técnica del Norte**.

Durante el proceso de pruebas, se evaluó el rendimiento, la estabilidad y la seguridad de la red privada virtual, concluyendo que OpenVPN proporciona una solución eficaz para la protección de la información y el acceso seguro a los recursos internos.

Con base en los resultados obtenidos, manifiesto mi aprobación y conformidad con la investigación realizada.

Firma:

Ing. Hugo Stalin Yánez Rueda, Mg.

Docente – Coordinador de Moocs y Virtualización de EVA´s Indoamérica.

Anexo 4, Preguntas de la encuesta

Sección 1: Datos generales del usuario

1. **¿Qué perfil describe mejor su rol en el consultorio jurídico?**

☐ Estudiante en prácticas

☐ Docente

☐ Administrativo

☐ Otro (especificar) _____

2. **¿Con qué frecuencia utiliza la conexión VPN en el consultorio jurídico?**

☐ Todos los días

☐ Varias veces a la semana

☐ Ocasionalmente

☐ Rara vez

☐ Nunca

Sección 2: Experiencia de uso

3. **¿Cómo calificaría la facilidad de instalación y configuración de OpenVPN en su dispositivo?**

☐ Muy fácil

☐ Fácil

☐ Regular

☐ Difícil

☐ Muy difícil

4. **¿Ha experimentado problemas al conectarse a la VPN?**

   ☐ Nunca

   ☐ Rara vez

   ☐ Algunas veces

   ☐ Frecuentemente

   ☐ Siempre

5. **Si ha tenido problemas, ¿qué tipo de dificultades ha enfrentado? (Puede seleccionar varias opciones)**

   ☐ Problemas de conexión o caída de la VPN

   ☐ Lentitud en la navegación

   ☐ Dificultades para acceder a ciertos recursos

   ☐ Configuración compleja

   ☐ Otro (especificar) _____

6. **¿En qué tipo de actividades usa la VPN dentro del consultorio?**

   ☐ Acceso a bases de datos jurídicas

   ☐ Envío y recepción de documentos legales

   ☐ Uso de plataformas internas de la universidad

   ☐ Comunicación segura con clientes

   ☐ Otro (especificar) _____

Sección 3: Percepción de rendimiento

7. **¿Cómo evalúa la velocidad de conexión cuando usa la VPN en comparación con una conexión sin VPN?**

☐ Muy rápida

☐ Rápida

☐ Regular

☐ Lenta

☐ Muy lenta

8. ¿Ha notado interrupciones en la conexión mientras utiliza la VPN?

☐ Nunca

☐ Rara vez

☐ Algunas veces

☐ Frecuentemente

☐ Siempre

9. ¿Siente que la VPN afecta el desempeño de su equipo (ejemplo: lentitud, consumo de CPU)?

☐ No afecta en absoluto

☐ Afecta ligeramente

☐ Afecta de manera moderada

☐ Afecta considerablemente

☐ Es inusable debido al impacto en el desempeño

Sección 4: Seguridad y confianza

10. ¿Cree que el uso de la VPN mejora la seguridad de sus actividades en línea dentro del consultorio?

☐ Sí, totalmente

☐ Sí, en cierta medida

☐ No estoy seguro

☐ No, no mejora la seguridad

11. ¿Le preocupa la seguridad de la información que maneja a través de la VPN?

☐ No me preocupa

☐ Me preocupa un poco

☐ Me preocupa bastante

☐ Me preocupa mucho

12. ¿Sabe cómo verificar si su conexión a la VPN es segura y está funcionando correctamente?

☐ Sí

☐ No

Sección 5: Satisfacción y mejoras

13. En términos generales, ¿qué tan satisfecho está con el uso de OpenVPN en el consultorio jurídico?

☐ Muy satisfecho

☐ Satisfecho

☐ Neutral

☐ Insatisfecho

☐ Muy insatisfecho

14. ¿Qué mejoras sugeriría para la implementación de OpenVPN en el consultorio jurídico? (Marque las que apliquen)

☐ Mejorar la estabilidad de la conexión

☐ Aumentar la velocidad de navegación

☐ Simplificar la configuración para nuevos usuarios

☐ Proporcionar más capacitación sobre su uso

☐ Otro (especificar) _____

15. ¿Le gustaría recibir una capacitación breve sobre el uso seguro de OpenVPN y buenas prácticas en ciberseguridad?

☐ Sí

☐ No