Universidad Nacional Federico Villarreal

VRIN | VICERRECTORADO DE INVESTIGACIÓN

FACULTAD DE INGENIERÍA ELECTRÓNICA E INFORMÁTICA

DISEÑO DE UNA CABECERA VPN PARA MEJORAR LA CALIDAD DE COMUNICACIÓN EN LAS TIENDAS DE UNA EMPRESA DE LOTERÍAS Y APUESTAS DEPORTIVAS EN CERCADO DE LIMA

Línea de investigación:
Sistemas de información y optimización

Tesis para optar el Título Profesional de Ingeniero de Telecomunicaciones

Autor

Rios Tomanguillo, Jorge Alejandro

Asesor

Pastor Castillo, José Enrique

ORCID: 0009-0002-7030-9268

Jurado

Flores Masias, Edward Jose

Peña Carrillo, Cesar Serapio

Rosales Fernandez, Jose Hilarion

Pastor Castillo, José Enrique

Lima - Perú

2025

DISEÑO DE UNA CABECERA VPN PARA MEJORAR LA CALIDAD DE COMUNICACIÓN EN LAS TIENDAS DE UNA EMPRESA DE LOTERÍAS Y APUESTAS DEPORTIVAS EN CERCADO DE LIMA

INFORME DE ORIGINALIDAD

5%	4%	1%	1%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	Submitted to Pontificia Universidad Catolica del Peru Trabajo del estudiante	1%
2	Submitted to Universidad Catolica de Trujillo Trabajo del estudiante	<1%
3	dokumen.pub Fuente de Internet	<1%
4	www.nutricionhospitalaria.org Fuente de Internet	<1%
5	rraae.cedia.edu.ec Fuente de Internet	<1%
6	www.grafiati.com Fuente de Internet	<1%
7	www.researchgate.net Fuente de Internet	<1%
8	www.scribd.com Fuente de Internet	<1%
9	prezi.com Fuente de Internet	<1%
10	Sullca Quispe, Jacquelin. "Entorno familiar y su relación con el comportamiento de los alumnos del CEBA Avanzado del Colegio Mateo Pumacahua, Sicuani-2023",	<1%

Universidad Nacional Federico Villarreal

VRIN | VICERRECTORADO DE INVESTIGACIÓN

FACULTAD DE INGENIERÍA ELECTRÓNICA E INFORMÁTICA

DISEÑO DE UNA CABECERA VPN PARA MEJORAR LA CALIDAD DE COMUNICACIÓN EN LAS TIENDAS DE UNA EMPRESA DE LOTERÍAS Y APUESTAS DEPORTIVAS EN CERCADO DE LIMA

Línea de investigación:

Sistemas de información y optimización

Tesis para optar el Título Profesional de Ingeniero de Telecomunicaciones

Autor:

Rios Tomanguillo, Jorge Alejandro

Asesor:

Pastor Castillo, José Enrique

ORCID: 0009-0002-7030-9268

Jurado:

Flores Masias, Edward Jose

Peña Carrillo, Cesar Serapio

Rosales Fernandez, Jose Hilarion

Pastor Castillo, José Enrique

Lima – Perú

2025

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

La presente investigación tuvo como propósito implementar una cabecera VPN con la intención de mejorar la comunicación entre los distintos puntos de venta de una empresa dedicada al rubro de loterías y apuestas deportivas. El estudio se desarrolló bajo un enfoque mixto, empleando un diseño pre experimental que combinó la aplicación de encuestas con la observación directa a un grupo de 40 trabajadores. Los resultados obtenidos evidenciaron cambios positivos, pues el desempeño operativo alcanzó un incremento significativo en su promedio, pasando de 21,05 a 35,28, lo que permitió constatar una mayor eficiencia y homogeneidad en los procesos internos. Por otro lado, el tiempo de respuesta del sistema también se redujo de manera considerable, bajando de 9,11 a 1,22 minutos, una mejora que supera el 85 %. Ambos resultados fueron respaldados por análisis estadísticos, con un nivel de significancia de p = 0,00. Con base en estos hallazgos, se concluyó que el diseño e implementación de la cabecera VPN, construida con dispositivos FortiGate en alta disponibilidad, permitió optimizar la conectividad, reducir la latencia en las operaciones y mejorar de forma concreta el rendimiento de los puntos de venta, generando beneficios reales para la dinámica operativa de la empresa.

Palabras clave: cabecera VPN, desempeño operativo, tiempo de respuesta.

ABSTRACT

The purpose of this research was to develop a VPN headend to improve communication between the points of sale of a company dedicated to lotteries and sports betting. For this purpose, we worked under a mixed approach and applied a pre-experimental design, using both surveys and direct observation to a total of 40 workers. The data collected showed significant improvements after implementation. Operational performance showed a significant increase in its average score, from 21.05 to 35.28, reflecting more efficient and consistent processes. On the other hand, the system's response time was also considerably reduced, dropping from 9.11 to 1.22 minutes, an improvement of more than 85%. Both results were supported by statistical analysis, with a significance level of $p = 0.00$. Based on these findings, it was concluded that the design and implementation of the VPN headend, built with FortiGate devices in high availability, allowed optimizing connectivity, reducing latency in operations and concretely improving point-of-sale performance, generating real benefits for the company's operational dynamics.

Keywords: VPN headend, operational performance, response time.

I. INTRODUCCIÓN

Representa un eje clave la gestión documental como parte de la operatividad de cualquier entidad, ya que los documentos no solo sirven como evidencia de las acciones, sino que también contienen información valiosa para la toma de decisiones. Aunque la gestión documental ha evolucionado significativamente a lo largo de la historia, desde métodos manuales hasta sistemas informáticos avanzados, su implementación sigue siendo un desafío en muchas entidades, especialmente en el sector público peruano.

A nivel nacional, a pesar de los esfuerzos por modernizar el sistema documental a través de iniciativas como el Modelo de Gestión Documental y la Plataforma Digital de Gestión Documental, persisten deficiencias significativas. La falta de un sistema integral y la dispersión en el manejo de archivos han generado problemas como la desorganización, el extravío de datos y los retrasos en los trámites, lo que repercute directamente en la eficiencia operativa.

Esta investigación, en este contexto, tiene por objetivo determinar la influencia de la administración documental en la gestión de archivos del Seguro Social de Salud (EsSalud) durante el año 2022. Para ello, se ha evaluado cómo los servidores de la institución manejan la información, identificando las causas subyacentes de los problemas existentes. Por lo tanto, el objetivo es proponer estrategias y recomendaciones que optimicen el acceso, el orden y la conservación de los registros documentales.

El estudio se justifica desde un enfoque teórico, ya que busca diagnosticar la situación en el Archivo Central de EsSalud utilizando instrumentos de investigación que podrían servir de modelo para otras instituciones. Asimismo, en el ámbito metodológico, se analiza la relación entre ambas variables para comprobar el grado de conocimiento de los funcionarios y su impacto en la calidad del servicio. Finalmente, este trabajo aspira a contribuir al establecimiento de políticas y procedimientos que mejoren el desempeño personal y

profesional de los servidores, lo que permitirá una atención más eficiente a la población asegurada.

1.1. Descripción y formulación del problema

El acelerado progreso de la tecnología ha llevado a muchas empresas a enfocarse en la expansión internacional, lo que exige contar con una infraestructura tecnológica rápida, segura y confiable. A medida que el internet ha crecido, las organizaciones han recurrido a él como medio para conectar sus diferentes oficinas, utilizando redes privadas virtuales (VPN) para satisfacer las necesidades de sus ubicaciones remotas (Salazar, 2018).

En el Perú, muchas empresas buscan crecer con rapidez frente a un mercado cada vez más competitivo y marcado por la transformación digital. Para lograrlo, resulta necesario incorporar herramientas tecnológicas que faciliten la mejora en las ventas y, al mismo tiempo, permitan ofrecer una mejor experiencia a sus clientes (Diario El Peruano, 2024). En el sector de loterías y apuestas deportivas, el reto fue aún más complejo, ya que las empresas de este rubro intentaron expandirse a nivel nacional, llegando a diferentes regiones del país con diversos formatos. Sin embargo, dicho proceso de crecimiento enfrentó múltiples dificultades de carácter tecnológico, logístico y operativo, lo que limitó tanto su avance como la posibilidad de garantizar una experiencia adecuada a los clientes (Padilla y Barrionuevo, 2023).

En los últimos años, esta empresa de loterías y apuestas emprendió una expansión que le permitió alcanzar más de cuatro mil puntos de venta en todo el país. Este crecimiento trajo consigo la necesidad de disponer de una conectividad más rápida, segura y confiable, indispensable para mejorar la atención a sus clientes. En el desarrollo de este proceso aparecieron dificultades con las conexiones inalámbricas utilizadas para enlazar los puntos de venta con los servicios centralizados, lo que terminó afectando la infraestructura de comunicación de la empresa. Ante esta situación, el área de Infraestructura y Comunicaciones se vio en la obligación de explorar distintas alternativas para mejorar el uso de sus recursos, y

dentro de ese análisis consideró la instalación de una VPN como una salida viable para enfrentar dichas limitaciones. Las VPN ofrecieron ventajas relevantes al permitir la conexión de diferentes puntos a través de redes públicas de manera segura y eficiente. Entre sus principales aportes destacaron el aumento de la seguridad, la posibilidad de escalar sin dificultad y la reducción de costos. Sin embargo, pese a estos beneficios, también fue necesario atender los problemas de conectividad y asegurar que la comunicación se mantuviera estable y protegida, de modo que acompañara el crecimiento de la empresa sin generar un incremento considerable en los gastos operativos.

En una red que integra a más de 4000 puntos de venta en todo el país, mantener una buena calidad de comunicación es fundamental para que las operaciones se desarrollen sin contratiempos. Aun así, durante las horas de mayor demanda, se ha notado una caída en la conectividad que llega a afectar hasta al 15% de los puntos. Cuando esto ocurre, muchas tareas se ven interrumpidas: no se pueden validar operaciones, la emisión de comprobantes se detiene y la sincronización con los sistemas centrales simplemente no ocurre. El problema de fondo es que la red no está preparada para afrontar estos escenarios, ya que no cuenta con mecanismos que garanticen estabilidad ni tolerancia ante fallos. Esta situación, además de generar retrasos, afecta directamente la continuidad operativa.

La red actual viene mostrando un rendimiento por debajo de lo esperado. En promedio, solo alcanza un 97.2% de disponibilidad al mes, lo que se traduce en más de 20 horas sin servicio, muy por encima del límite aceptable de 43 minutos que se considera estándar en el sector. Esta diferencia no es menor, ya que cada interrupción afecta directamente el trabajo en los puntos de venta, sobre todo cuando hay mayor carga operativa. Las caídas del sistema no solo complican la atención, sino que también generan pérdidas económicas y desgastan la experiencia del cliente. Está claro que se necesita una red mucho más sólida, que esté preparada para sostenerse activa y estable, incluso en los momentos más exigentes.

Cuando un sistema depende de muchos puntos distribuidos, cada segunda cuenta. Últimamente, se ha notado que los tiempos de respuesta durante las horas pico están siendo excesivos: en varios casos superan los tres minutos, algo muy lejos del ideal de 100 milisegundos que se necesita para que las operaciones en tiempo real fluyan sin problemas. Este retraso no es solo un dato técnico, se siente directamente en el día a día. Afecta acciones básicas como validar una apuesta, emitir un comprobante o realizar un pago al instante. Y cuando estas demoras se repiten, los puntos de atención se congestionan, el servicio se vuelve lento y la experiencia del usuario empieza a deteriorarse.

En redes distribuidas, la seguridad debería ser una prioridad, pero en muchos casos aún queda en segundo plano. Hoy se sabe que cerca del 70% de los puntos de venta siguen trabajando conectados a redes públicas y sin ningún tipo de cifrado. Esto representa un riesgo real, ya que cualquier dato que se transmite como información personal, credenciales o registros de transacciones puede ser interceptado o manipulado con facilidad. Ya se han visto consecuencias concretas. En 2021, una lotería nacional sufrió un ataque en el que se filtraron más de 3 GB de datos confidenciales, todo por no contar con las medidas de seguridad necesarias. Situaciones como esa confirman que no se puede seguir operando con redes expuestas.

1.1.1. Formulación del problema

Problema general

¿Cómo el diseño de una cabecera VPN puede mejorar la calidad de comunicación en los puntos de venta de una empresa de loterías y apuestas deportivas?

Problemas específicos

a. ¿Cómo influye el diseño de la cabecera VPN en la calidad de comunicación en los puntos de venta de la empresa de loterías y apuestas deportivas?

b. ¿De qué manera la cabecera VPN puede contribuir a mejorar el desempeño operativo en los puntos de venta de una empresa de loterías y apuestas deportivas?

c. ¿Cómo puede la cabecera VPN optimizar el tiempo de respuesta en los puntos de venta de una empresa de loterías y apuestas deportivas?

1.2. Antecedentes

1.2.1. Antecedentes internacionales

Según Blancaflor et al. (2024) en su artículo Un análisis comparativo de las aplicaciones VPN y sus capacidades de seguridad frente a problemas de seguridad, este estudio se enfocó en evaluar el interés de los usuarios por los servicios de VPN, además de investigar su confianza y comprensión sobre la seguridad y privacidad que proporcionan los distintos proveedores de VPN. Para ello, se realizaron encuestas a usuarios con el fin de medir su familiaridad con estas tecnologías y su percepción sobre posibles vulnerabilidades. Los resultados indicaron que los usuarios comprenden bien el funcionamiento de los VPN y sus servicios, pero también reconocen que pueden existir fallas de seguridad que los hackers podrían explotar. En conclusión, el estudio subraya la necesidad de fortalecer la seguridad de los VPN debido a la creciente inquietud de los usuarios respecto a posibles riesgos.

Wu et al. (2024) en su artículo dominado RT-CBCH: Identificación de tráfico de VPN en tiempo real basado en datos muestreados en redes de alta velocidad, este artículo presenta un método llamado RT-CBCH para identificar servicios de tráfico VPN en tiempo real, con el objetivo de mejorar la gestión de redes al reconocer el tráfico VPN de manera eficiente en entornos de alta velocidad. El enfoque se basa en el uso de características de tráfico que se mantienen después del muestreo, junto con una estructura de procesamiento rápido que emplea un filtro Counting Bloom y una tabla hash encadenada (CBCH) para reducir el uso de recursos. Los experimentos demuestran que, con un muestreo de 1/256, el método puede procesar 900 segundos de tráfico en 23.63 segundos, alcanzando una precisión del 90% en la identificación

de servicios y más del 99% en la detección del proxy V2Ray. La conclusión resalta que RT-CBCH es capaz de identificar el tráfico de manera precisa y estable, con un consumo mínimo de recursos en tiempo real.

Fassl et al. (2023) cuya investigación fue Investigación del folclore de seguridad: un estudio de caso sobre el fenómeno Tor sobre VPN, el estudio tuvo como finalidad analizar el fenómeno conocido como “Tor sobre VPN”, considerado una práctica de seguridad basada en consejos no verificados. Para ello, se emplearon tres enfoques complementarios. Primero, se revisó el tráfico real de Tor, identificando una prevalencia del 6,23%. Luego, se aplicaron encuestas que reflejaron la intención de los usuarios de protegerse de la red Tor o reforzar su seguridad general. Después, se evaluaron fuentes en línea, donde se observó la influencia de normas sociales y la facilidad de uso por encima de las creencias sobre los efectos de la práctica. Finalmente, el estudio concluyó que es necesario mejorar la comunicación de las recomendaciones de seguridad para disminuir la desinformación y los malentendidos.

Fayoumi et al (2022) en su artículo llamado Clasificación del tráfico de redes VPN y no VPN mediante funciones relacionadas con el tiempo, este estudio se centró en optimizar la clasificación del tráfico de red entre tráfico VPN y no VPN, enfrentando los retos que el cifrado plantea para la calidad del servicio y la seguridad en redes. La metodología empleó dos modelos de aprendizaje automático que clasificaron el tráfico utilizando características estadísticas, el análisis de correlación de Pearson y un algoritmo genético, con el fin de seleccionar las características más importantes. Los resultados indicaron que el modelo más eficaz alcanzó una precisión superior al 95.02%, con tiempos de predicción por paquete en microsegundos, y solo una reducción del 2.37% en comparación con métodos puramente estadísticos. La conclusión subraya que estos modelos tienen un gran potencial para el desarrollo de herramientas de análisis de tráfico en tiempo real de manera eficiente.

Quintana y Gallardo (2022) en su tesis denominada Diseño de una red VPN full mesh para mejorar la comunicación y seguridad en una empresa metalmecánica de Lima – 2021, esta tesis tuvo como propósito diseñar una red de comunicación VPN FULL MESH en una empresa metalmecánica para resolver los inconvenientes de conectividad que enfrentaban los usuarios al conectarse mediante una VPN cliente-servidor entre las sucursales y la sede principal. Para abordar este problema, se definieron los requerimientos de inversión para el mantenimiento y renovación de la solución, sirviendo como base para evaluar alternativas tecnológicas. Se revisaron tres alternativas tanto en el aspecto técnico como en el económico: la compra de un firewall, el uso de software libre y el alquiler de servicios VPN mediante un proveedor de Internet. Tras la comparación de estas opciones, se identificó que la más conveniente era la implementación de software libre. Esta elección permitió resolver los problemas de conectividad con una inversión reducida. Además, brindó flexibilidad y posibilidades de crecimiento a futuro. De esta forma, la empresa consiguió una solución eficiente y de bajo costo para sus necesidades de comunicación.

Luna y Zeta (2021) en su investigación Implementación de redes VPN MIKROTIK para los servidores entre ciudades de Lima y Pisco, tuvo como finalidad mostrar la efectividad de las conexiones VPN de acceso remoto cuando se utilizan equipos Mikrotik, conocidos por brindar seguridad en la transmisión de datos en empresas de distintos tamaños. Para ello, se implementaron y supervisaron dichas conexiones, lo que permitió a los especialistas analizar su rendimiento y nivel de protección con ayuda de herramientas de monitoreo. Los resultados evidenciaron que el uso de Mikrotik en las VPN refuerza la privacidad del tráfico de datos, previene accesos no autorizados y disminuye el riesgo de pérdida de información. En conclusión, con las exigencias impuestas por la nueva normalidad, estas soluciones se volvieron esenciales para asegurar el acceso remoto a servidores y aplicaciones, permitiendo a

los trabajadores mantener su productividad desde casa y optimizando los recursos de las empresas.

Lazarte y Silva (2022) en su tesis Diseño de una red privada virtual (VPN) basada en software libre para la mejora de la seguridad de la información de la jurisdicción de la dirección de redes integradas de salud Lima Centro, el objetivo de mejorar la seguridad en los centros de salud gestionados por la DIRIS Lima Centro. Actualmente, estos establecimientos enfrentan desafíos como el acceso a sitios web no autorizados, la instalación de software ajeno al ámbito laboral y la pérdida de datos por la desactivación de antivirus. La metodología consiste en conectar los centros de salud con la sede administrativa a través de una VPN que integre Active Directory y un firewall en Linux (Squid), con el fin de garantizar una gestión segura de la información. Se espera que los resultados mejoren la protección de datos y el control de los sistemas de salud. En resumen, la implementación de esta VPN proporcionará una mayor seguridad y optimizará la administración de los recursos tecnológicos en la institución.

Malque (2024) en su tesis denominado “Migración de las telecomunicaciones a una red propia de fibra óptica para mejorar la gestión y control de los servicios en una empresa transmisora eléctrica” este informe refleja una experiencia profesional en la que, como parte del equipo de Telecomunicaciones de CLARO PERÚ, se trabajó para que una empresa transmisora eléctrica pudiera gestionar y controlar las comunicaciones de sus subestaciones en el norte del Perú. El objetivo fue migrar sus servicios a una red propia de fibra óptica, lo que implicó un análisis previo para determinar qué servicios requerían esta transición, además de la compra e instalación de equipos de telecomunicaciones para llevar la información a los centros de control en Lima. Gracias a este esfuerzo, se implementó una solución eficiente que fortaleció la autonomía y la capacidad operativa de la empresa transmisora. Este proyecto subraya el valor de invertir en redes propias para optimizar comunicaciones en sectores clave, garantizando mejores resultados y mayor sostenibilidad

Conche (2021) en su tesis titulada “La red dorsal nacional de fibra óptica y su influencia en el servicio de internet en el Perú”, esta investigación explora cómo la Red Dorsal Nacional de Fibra Óptica ha impactado en el servicio de internet en el Perú, buscando determinar su influencia en la infraestructura y cobertura a nivel nacional. Para ello, se utilizó un enfoque descriptivo y explicativo, con un diseño experimental-longitudinal y una muestra censal basada en datos nacionales. Los resultados revelan un impacto positivo: desde su implementación, la cantidad de fibra óptica desplegada creció un 91.71% entre 2015 y 2016, y continuó aumentando un 14.46% hasta 2020. En términos de cobertura, el número de líneas móviles mostró un crecimiento del 10.17% entre 2015 y 2016, con un incremento sostenido del 11.75% hasta 2018, aunque posteriormente registró una ligera caída del 6.66% hacia 2020. En conclusión, la Red Dorsal ha sido clave para fortalecer la infraestructura y expandir el alcance del servicio de internet en el país, impulsando su desarrollo tecnológico.

1.3. Objetivos

Objetivo general

Diseñar una cabecera VPN para mejorar el servicio de comunicación en los puntos de venta de una empresa de loterías y apuestas deportivas.

Objetivos específicos

a. Desarrollar el diseño de la cabecera VPN para mejorar la calidad de comunicación en los puntos de venta de la empresa de loterías y apuestas deportivas.

b. Mejorar el desempeño operativo con la cabecera VPN en los puntos de venta de una empresa de loterías y apuestas deportivas.

c. Mejorar el tiempo de respuesta con la cabecera VPN en los puntos de venta de una empresa de loterías y apuestas deportivas.

1.4. Justificación

La investigación se justifica por la necesidad de diseñar una cabecera VPN que mejore la seguridad y la calidad de comunicación en los puntos de venta de la empresa de loterías y apuestas deportivas. Este diseño contribuyó a optimizar la protección de datos y la eficiencia en las comunicaciones, lo cual fue crucial para las operaciones diarias y el bienestar de los colaboradores, mejorando así la calidad del servicio prestado. La investigación se enfocará en los puntos de venta de la empresa en Cercado de Lima, lo que limita la aplicabilidad de los resultados a otras zonas. Además, se trabajará con los datos disponibles y las entrevistas a los colaboradores de estas tiendas, lo que puede restringir la amplitud del análisis en otros aspectos tecnológicos u operativos.

1.4.1. Justificación práctica

El presente trabajo de investigación se basó en emplear la tecnología de red “Virtual Private Network” (VPN), “con la finalidad de mejorar la confidencialidad del intercambio de información” Con lo que se mejoró el servicio de comunicación en los puntos de venta.

1.4.2. Justificación tecnológica

Las redes VPN utilizaron varios protocolos de seguridad para la transmisión de datos, entre los que destacan 3DES (Triple data encryption Estándar) el cual cumple la función de encriptar la información a tranferir y el protocolo IPSec (IP Security) para manejo de los túneles de conexión.

1.4.3. Justificación metodológica

La elección de una metodología mixta para este estudio fue basada en la necesidad de abordar tanto los aspectos técnicos como humanos del impacto del diseño de la cabecera VPN en la calidad de comunicación y seguridad en los puntos de venta de una empresa de loterías y apuestas deportivas.

El enfoque cuantitativo fue adecuado para evaluar de manera objetiva las mejoras relacionadas con la implementación de la cabecera VPN, permitiendo medir cómo afectó a la comunicación interna, la estabilidad de la red y la eficiencia operativa en los puntos de venta. Este enfoque buscó obtener información clara y comprobable que respaldara de manera objetiva las mejoras tecnológicas planteada.

El enfoque cualitativo facilitó comprender la manera en que los colaboradores percibieron los cambios en la comunicación y cómo estos influyeron en su rutina laboral. Mediante las entrevistas se identificaron tanto los aspectos positivos como las dificultades mencionadas, lo que permitió obtener una apreciación más real y cercana del efecto generado por la implementación de la cabecera VPN.

La aplicación de ambos enfoques permitió que la investigación se desarrollara de manera más completa, integrando tanto la parte técnica como la visión de los trabajadores involucrados. Esta combinación facilitó una comprensión más cercana de los efectos que tuvo la implementación de la cabecera VPN dentro de la empresa, ofreciendo un panorama equilibrado entre lo funcional y lo experiencial.

1.5. Hipótesis

Hipótesis general

El diseño de una cabecera VPN mejora la calidad de comunicación en los puntos de venta de una empresa de loterías y apuestas deportivas.

Hipótesis específicas

a. El diseño adecuado de la cabecera VPN mejorará significativamente la calidad de la comunicación en los puntos de venta de la empresa de loterías y apuestas deportivas.

b. El diseño de la cabecera VPN incrementa el desempeño operativo de los puntos de venta de la empresa de loterías y apuestas deportivas.

c. El diseño de la cabecera VPN mejora el tiempo de respuesta en los puntos de venta de una empresa de loterías y apuestas deportivas.

II. MARCO TEÓRICO

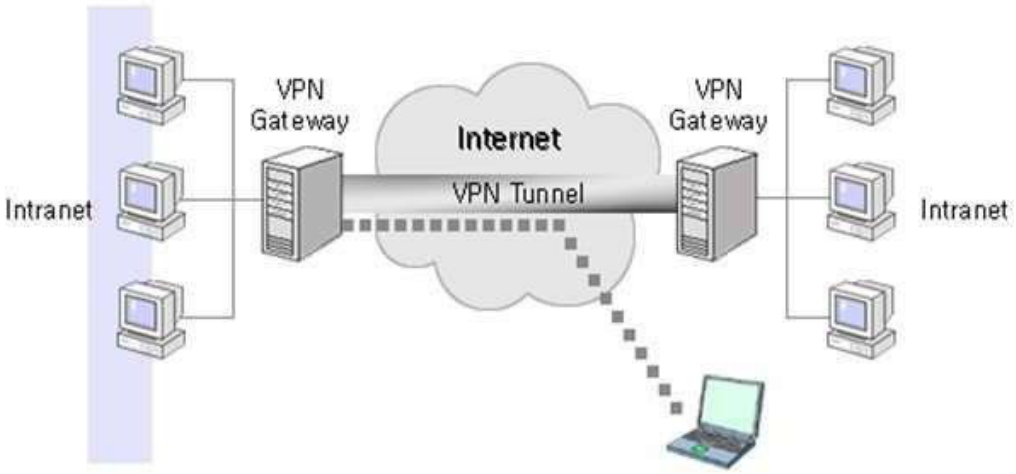
2.1. Bases teóricas sobre el tema de investigación

2.1.1. Red privada virtual (VPN)

Una red VPN brinda seguridad al momento de compartir información entre puntos de venta que se encuentran en diferentes lugares. Lo logra al crear conexiones cifradas que viajan por internet, una red que es pública. Gracias a esto, los datos pueden enviarse sin ser vistos ni modificados, lo que asegura que la información se mantenga protegida durante todo el proceso.

Figura 1

Red privada virtual.



2.1.2. Ventajas de implementación VPN

Ofrece numerosas ventajas, entre ellas la integridad, confidencialidad y encriptación de los datos. En ese sentido, la integridad garantiza que la información enviada no sea modificada durante su recorrido, de modo que el mensaje llegue al destinatario tal como fue transmitido, sin alteraciones. Asimismo, la confidencialidad permite que solo las personas autorizadas puedan acceder a la información dentro de la VPN, ya que los datos son protegidos mediante

métodos de encriptación que los convierten en códigos difíciles de interpretar para terceros no autorizados.

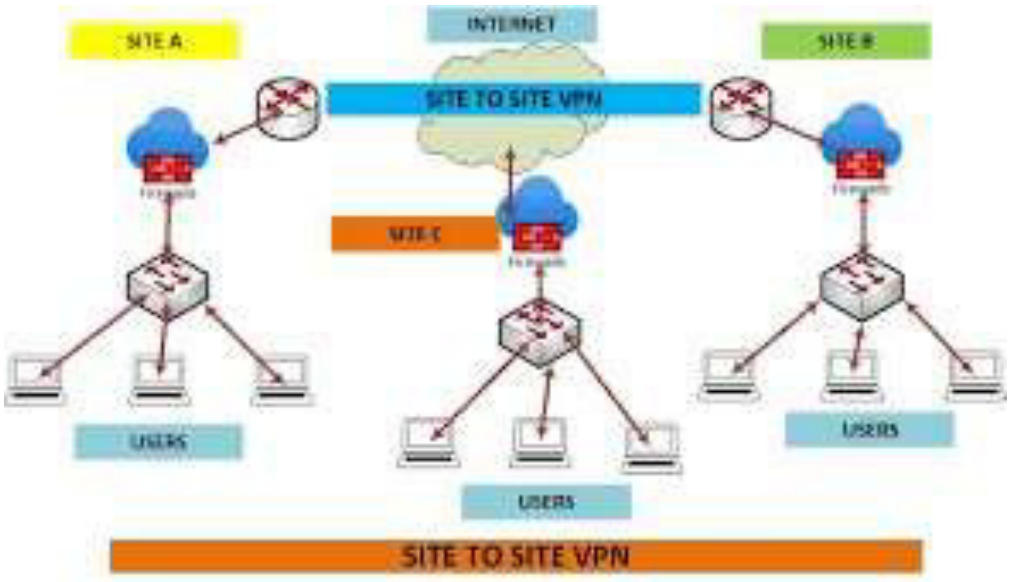
Además, esta herramienta contribuye al ahorro de costos y resulta de fácil uso para los usuarios. Del mismo modo, facilita la comunicación entre personas u oficinas ubicadas en distintos lugares, permitiendo que puedan conectarse de manera eficiente sin importar la distancia que las separe.

2.1.3. Tipos de VPN

2.1.3.1. VPN Sitio a Sitio. Este tipo de VPN conecta las oficinas que están en diferentes lugares con la oficina central de la empresa. En la sede principal, un servidor o firewall siempre está conectado a Internet y recibe las conexiones que vienen de los puntos de venta. Luego, crea un túnel seguro para que la comunicación funcione bien. Tanto la oficina principal como las sucursales usan conexiones de banda ancha que les brinda su proveedor local, lo que permite ahorrar dinero porque no necesitan enlaces especiales que suelen ser más costosos.

Figura 2

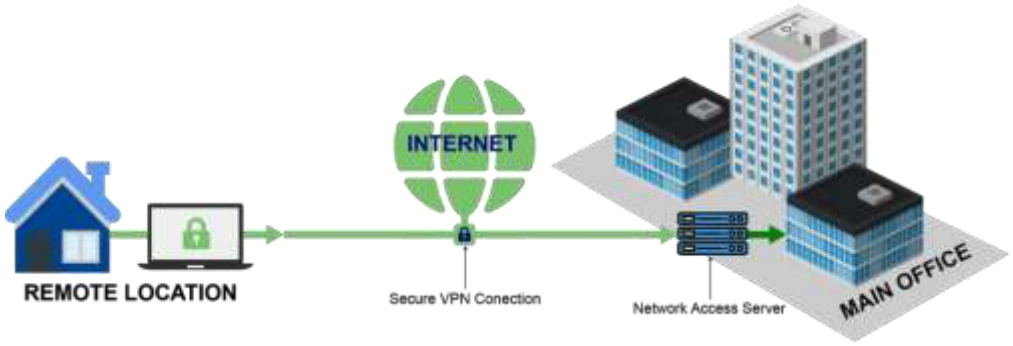
VPN sitio a sitio.



2.1.3.2. VPN de acceso remoto. Este tipo de VPN es utilizado por la mayoría de las empresas, con la finalidad de conectar a los trabajadores y/o proveedores con las sedes principales y remotas de las empresas, utilizando Internet como medio de acceso, donde luego de la autenticación, podrán trabajar como si estuvieran en una red local de la empresa.

Figura 3

VPN de acceso remoto.



2.2. Multi Protocolo Layer Switching (Mpls)

Es una tecnología que desarrolló el grupo IETF para que las redes IP puedan funcionar mejor. La idea es que, aunque estas redes no siempre mantienen una conexión constante, puedan tener algunas ventajas de las redes que sí lo hacen.

Cuando un paquete de datos viaja por una red IP tradicional, cada router por donde pasa revisa a dónde debe ir y otros detalles. La ruta que sigue puede cambiar según lo que sabe cada router en ese momento, pero como no se puede predecir exactamente, es complicado garantizar que el servicio sea siempre igual de bueno. Además, los routers necesitan buscar en sus listas para saber por dónde enviar el paquete, y cuanto más grande sea esa lista, más tiempo tardan en hacerlo.

MPLS funciona haciendo que cada nodo, ya sea un router o un switch, asigne una pequeña etiqueta a cada elemento en su tabla y se la pase a los nodos que tiene cerca. Esa

etiqueta, que es un código corto, va dentro del paquete y sirve para identificar grupos de paquetes que viajan juntos por la misma ruta, aunque terminen en lugares distintos. La etiqueta en MPLS es un pequeño código que solo tiene importancia dentro de cada nodo y sirve para relacionar el tráfico con un grupo específico de paquetes, conocido como FEC. Esta etiqueta se asigna tomando en cuenta la dirección del paquete, el tipo de servicio, si pertenece a una VPN u otros criterios. Cuando MPLS se usa como una solución IP de nivel 3, que es lo más común, esta etiqueta se añade al comienzo del paquete. La cabecera de MPLS tiene un tamaño de 4 bytes y está compuesta por varios campos:

- Label (20 bits). El valor que tiene la etiqueta MPLS se entiende solo dentro del nodo donde se aplica. Esa etiqueta es la que guía al paquete para saber a dónde debe ir después.
- CoS (3 bits). Este campo sirve para que los dispositivos que reciben el paquete sepan cómo tratarlo, decidiendo qué paquetes priorizar y cómo organizarlos. Así, es posible diferenciar los tipos de tráfico y dar un mejor rendimiento a algunos frente a otros
- Stack (1 bit). Este bit indica si hay más etiquetas MPLS apiladas una encima de la otra. El nodo siempre procesa la etiqueta que está en la parte superior de la pila. Esto resulta útil cuando una red MPLS tiene que atravesar otra red MPLS de un proveedor o entidad diferente; así, al salir de esa red externa, el paquete sigue funcionando con MPLS sin que se note la diferencia.

2.2.1. Principales ventajas de MPLS

Entre las principales ventajas de MPLS se encuentra que los paquetes pueden conmutarse con mayor rapidez, debido a que el proceso se realiza mediante etiquetas y no únicamente a partir de las direcciones IP de destino. Asimismo, permite implementar redes en las que los clientes cuentan con un espacio independiente, conocidas como MPLS-VPN, lo que favorece una mejor organización y separación del tráfico.

Además, MPLS tiene la capacidad de trabajar con distintos protocolos, tanto en el nivel superior, como ocurre en L3, como en el nivel inferior, mediante PWE3. Del mismo modo, facilita el control de la calidad del servicio (QoS) a través de la marcación de paquetes, permitiendo priorizar determinados tipos de tráfico según las necesidades de la red.

Por otra parte, para establecer una nueva VPN solo se requiere configurar el circuito de acceso y el enrutamiento correspondiente. A ello se suma que MPLS facilita el uso de la ingeniería de tráfico (TE) y permite aprovechar de manera más eficiente el ancho de banda en los accesos, especialmente mediante una malla virtual completa.

2.2.2. Términos principales utilizados en MPLS

En una red MPLS se emplean diversos términos técnicos que permiten comprender su funcionamiento básico. En primer lugar, el LSR es el router encargado de revisar las etiquetas de los paquetes para determinar su envío dentro de la red. Asimismo, el Edge LSR o LER se ubica en los extremos de la red MPLS y cumple la función de agregar etiquetas cuando el tráfico ingresa, así como retirarlas cuando los paquetes salen hacia otra red. De igual manera, el LDP permite el intercambio de etiquetas entre los equipos mediante sesiones TCP, mientras que el TDP cumple una función similar, aunque corresponde a una tecnología propia de Cisco (Núñez et al., 2026).

Por otro lado, la LIB constituye la base de información donde se registran las etiquetas y las interfaces asociadas a los destinos. Además, la FEC agrupa paquetes con características similares para que sigan una misma ruta dentro de la red. En ese sentido, el LSP representa el camino unidireccional por donde circulan dichos paquetes etiquetados. Finalmente, la ingeniería de tráfico permite administrar y orientar el flujo de datos para aprovechar mejor los recursos de la red y mejorar su rendimiento (Núñez et al., 2026).

2.2.3. Componentes físicos

Dentro de MPLS, uno de los componentes físicos principales es el Label Switch Router o LSR, entendido como el router o switch capaz de distribuir etiquetas y reenviar paquetes a partir de ellas. Según su función y ubicación en la red, estos equipos pueden clasificarse como LSR de borde, ATM-LSR o ATM Edge-LSR, lo que permite diferenciar el papel que cumplen dentro del dominio MPLS (Carletto, 2022).

En ese sentido, el Edge-LSR se ubica en los límites de la red MPLS y se encarga de gestionar las etiquetas de los paquetes que ingresan y salen de ella. Cuando el tráfico entra al dominio MPLS, este equipo añade una etiqueta para facilitar su encaminamiento; mientras que, al salir de la red, retira dicha etiqueta para que el paquete continúe su recorrido hacia el destino correspondiente. Asimismo, cuando el LSR se conecta con dispositivos que no utilizan MPLS, cumple una función de borde; pero si se vincula con equipos ATM-LSR mediante interfaces MPLS, puede considerarse un ATM Edge-LSR (Carletto, 2022).

Por su parte, el ATM-LSR corresponde a un switch ATM que ha sido adaptado para operar como un LSR dentro de una red MPLS. Este equipo participa en el control del enrutamiento IP y en la asignación de etiquetas, aunque para el reenvío de paquetes utiliza la conmutación de celdas propia de la tecnología ATM. Por ello, un switch ATM tradicional puede convertirse en un ATM-LSR mediante la actualización del software de su componente de control, permitiendo su integración al funcionamiento de una red MPLS (Carletto, 2022).

III. MÉTODO

3.1. Tipo de investigación

En el proyecto, se recurrió a un enfoque mixto para analizar el impacto de la cabecera VPN en los puntos de venta. La aplicación del enfoque cuantitativo permitió recopilar datos expresados en números y evaluar los tiempos de respuesta que se presentaron después de la implementación, lo que ofreció resultados comprensibles y verificables. Hernández Sampieri (2018), señala que, esta metodología permite verificar hipótesis a partir del análisis de datos numéricos y técnicas estadísticas, lo que brinda un respaldo objetivo para interpretar los resultados obtenidos con la incorporación de la tecnología. Del mismo modo, el uso del enfoque cualitativo hizo posible conocer con mayor profundidad la percepción de los trabajadores frente a los cambios en la comunicación y comprender cómo la implementación de la cabecera VPN influyó en el desarrollo de sus actividades diarias.

El estudio se realizó con un enfoque aplicado, ya que estuvo dirigido a atender una necesidad concreta dentro de la empresa de loterías y apuestas deportivas. Su finalidad principal no fue elaborar nueva teoría, sino optimizar un proceso operativo a través de la implementación de una cabecera VPN. Este tipo de investigación busca ofrecer soluciones prácticas basadas en conocimientos científicos previamente adquiridos (Hernández, 2018). En este caso, el estudio no solo permitió identificar la problemática existente, sino que también planteó una alternativa diseñada.

Se realizó bajo un enfoque descriptivo, ya que buscó explicar los cambios ocurridos en el servicio de comunicación luego de la intervención, tomando en cuenta la disponibilidad y los tiempos de respuesta.

Este tipo de investigación permite describir con detalle las características de los procesos, personas o fenómenos estudiados (Hernández et al., 2014). En este caso, el análisis se centró en mostrar las mejoras alcanzadas tras la implementación de la VPN.

El diseño elegido fue pre-experimental, porque se midió el efecto de la implementación de la cabecera VPN sin un grupo de control. Un diseño pre-experimental se caracteriza por no incluir un grupo control, lo que limita la posibilidad de establecer con certeza una relación causa-efecto. Sin embargo, este tipo de diseño es útil cuando se busca una primera aproximación al impacto de una intervención (Hernández, 2018), como en este caso, donde se compararán los resultados antes y después de la instalación de la cabecera VPN para evaluar mejoras iniciales.

3.2. Ámbito temporal y espacial

El presente trabajo de investigación tomó aproximadamente entre 4 y 9 meses para su organización y recopilación de datos. Este periodo contempló todas las fases del proyecto, que fueron desde la planificación inicial hasta la instalación de la cabecera VPN y la revisión de sus efectos en la comunicación entre los puntos de venta. Se diseñó un cronograma de actividades en el que se incluyó la recopilación de información sobre la disponibilidad de la conexión y los tiempos de respuesta, además del análisis de esos datos. Al cierre del proceso, se expusieron los resultados, lo que permitió comprender con claridad los beneficios obtenidos con la implementación.

3.3. Variables

3.3.1. Definición conceptual de la variable: Cabecera VPN

Herramienta que brinda la posibilidad de acceder a los recursos de una organización de manera remota mediante una conexión cifrada y segura. Su funcionamiento se basa en protocolos que protegen la información y aseguran la confidencialidad de los datos, creando un canal confiable incluso cuando se navega en redes públicas o poco seguras (La Universidad en Internet [UNIR], 2021).

3.3.2. Definición operacional de la variable: Cabecera VPN

La configuración de una red privada virtual permite que los usuarios accedan de forma segura a los sistemas de la organización. Este proceso incluye la forma en que la red realiza su funcionamiento, la implementación de estrategias de protección ante posibles amenazas y la salvaguarda de la información, asegurando su confidencialidad e integridad por medio de mecanismos de autenticación y verificación de datos.

3.3.3. Definición conceptual de la variable: Sistema de comunicación

El desarrollo de los servicios de comunicación ha hecho posible que el acceso a redes y sistemas se lleve a cabo con mayor seguridad y privacidad, lo que permite una transmisión de información más rápida y confiable. A su vez, estos avances han favorecido el incremento de la productividad, ya que facilitan un flujo continuo y eficiente de datos en tiempo real (Organismo Supervisor de Inversión Privada en Telecomunicaciones [OSIPTEL], 2023).

3.3.4. Definición operacional de la variable: Sistema de comunicación

La capacidad de la red para asegurar el intercambio de información se evaluó a partir de dos criterios fundamentales: la disponibilidad, entendida como la continuidad en el acceso, y el tiempo de respuesta, vinculado con la rapidez con que se transmiten y reciben los datos.

3.4. Población y muestra

Esta población estuvo conformada por 40 trabajadores de la empresa de loterías y apuestas deportivas, quienes tienen experiencia directa en el uso de los sistemas de comunicación. Definir de manera precisa la población es importante para garantizar la validez y la representatividad de los resultados. Esta delimitación también permite establecer comparaciones con otros estudios y aporta a la generación de mejoras en el sector (Hernández y Mendoza, 2018).

La muestra utilizada en la investigación estuvo integrada por los mismos 40 trabajadores que conformaron la población, lo que permitió evitar sesgos y garantizar que las

opiniones de todos los participantes fueran consideradas. Contar con una muestra representativa es fundamental para mantener la validez de los resultados y facilitar la generalización de los hallazgos obtenidos (Hernández y Mendoza, 2023).

Se llevó a cabo un muestreo no probabilístico de carácter intencional, eligiendo a 40 trabajadores que desempeñan un papel importante en los procesos de comunicación de la empresa de loterías y apuestas deportivas. Esta selección hizo posible incluir a quienes resultan determinantes para analizar la efectividad de la cabecera VPN. Este tipo de muestreo permite obtener información más significativa al enfocarse en las personas con mayor relación con el objeto de estudio (Hernández y Mendoza, 2018).

3.5. Instrumentos

La investigación tuvo como fuente principal de información la observación directa del desempeño de los trabajadores en los diferentes puntos de venta de la empresa de loterías y apuestas deportivas, lo que permitió obtener una apreciación más precisa sobre su labor. Asimismo, se llevó a cabo una encuesta dirigida a la muestra de 40 empleados, con el objetivo de evaluar factores relacionados con la disponibilidad, los tiempos de respuesta y la efectividad de la cabecera VPN. Esta técnica fue utilizada para recopilar información relacionada con los indicadores establecidos en la investigación, con el objetivo de examinar el efecto que tuvo la implementación de la cabecera VPN en la comunicación interna entre los diversos puntos de venta.

3.6. Procedimientos

El enfoque de esta investigación inició con la selección deliberada de una muestra compuesta por 40 trabajadores de la empresa de loterías y apuestas deportivas, quienes desempeñan un papel clave en la evaluación de la comunicación en los distintos puntos de venta. En la fase de recopilación de datos, se crearon herramientas que incluyeron una guía para la observación directa y una encuesta dirigida a medir la disponibilidad y los tiempos de

respuesta relacionados con la cabecera VPN. Durante la observación directa, se documentó el rendimiento de los trabajadores y las interacciones en los diversos puntos de venta, mientras que la encuesta permitió obtener información sobre la efectividad de la cabecera VPN utilizando indicadores específicos. Tras esta etapa de recopilación, se procedió a la implementación de la cabecera VPN, que implica la instalación y configuración del equipo necesario para establecer una red privada virtual, así como realizar pruebas de conexión para garantizar su correcto funcionamiento. Posteriormente, se realizaron más observaciones y encuestas para evaluar el impacto de la cabecera VPN en la comunicación. Los datos obtenidos fueron analizados mediante métodos estadísticos en el programa SPSS, lo que permitió comprender el efecto de la implementación en la disponibilidad y los tiempos de respuesta de los servicios hacia los puntos de venta, finalizando con un informe que presente las conclusiones y recomendaciones derivadas de los hallazgos de la investigación.

3.7. Análisis de datos

Un aspecto fundamental de este trabajo fue analizar los datos recogidos, ya que permitió entender si la cabecera VPN realmente ayudó a mejorar el funcionamiento en los puntos de venta de la empresa de loterías y apuestas deportivas. Para hacer esto, se utilizó el programa SPSS, que facilitó la organización y el análisis de la información obtenida mediante encuestas y observaciones directas en el lugar de trabajo. A partir de este proceso, fue posible notar ciertos comportamientos y relaciones entre los datos, lo que ayudó a identificar cómo afectó la implementación de la VPN en aspectos como la estabilidad del servicio y los tiempos de respuesta. Para que los resultados de esta investigación tuvieran sentido y pudieran respaldar las conclusiones, fue necesario analizar los datos con mucho cuidado. Este paso ayudó no solo a confirmar que la información era confiable, sino también a dar una base sólida a las recomendaciones propuestas. Gracias a ese análisis, se pudo entender mejor de qué manera los

cambios en la infraestructura de comunicación ayudaron a que el sistema funcionara de forma más eficiente y a que los clientes se sintieran más satisfechos con el servicio.

3.8. Consideraciones éticas

En este estudio se tuvo mucho cuidado con el manejo ético, sobre todo pensando en proteger a las personas que participaron. Antes de comenzar, a los empleados se les explicó claramente en qué consistía la investigación, qué se iba a hacer y que podían decidir no seguir en cualquier momento si así lo querían. Solo después de entender todo eso, aceptaron participar. Además, se cuidó que la información que compartieron se manejara con total discreción. Para evitar que alguien pudiera ser identificado, los datos se trataron de forma anónima y no se compartió nada sin su permiso. Se tuvo mucho cuidado en cómo se recogieron los datos, siempre siendo honestos y claros con todo lo que se anotó. Se hizo el esfuerzo para que nadie se sintiera mal o incómodo durante el proceso, usando maneras que fueran adecuadas para eso. También se respetó que cada persona tiene una forma de ser diferente, tanto en cultura como en su forma de vida, y se les trató a todos con respeto, sin hacer diferencias ni discriminarlos.

IV. RESULTADOS

Para el diseño de la cabecera VPN para mejorar la calidad de comunicación en los puntos de venta de la empresa de loterías y apuestas deportivas, se realizó de la siguiente manera. Se ha considerado como parte de la solución, el despliegue de la plataforma FortiGate 1101E en alta disponibilidad (Primario-Secundario) para el establecimiento de una VPN IPSec-Dialup entre los puntos de venta y la red central. De esta manera se podrá establecer túneles con métodos de autenticación y encriptación más robustos y seguros para proteger las transacciones que se realizan.

4.1. Solución de ciberseguridad perimeral

Dos (02) equipos de Seguridad FortiGate FGT 1101E, los cuales cuentan con licenciamiento y soporte del fabricante por 48 meses.

Figura 4

Equipo primario

Figura 5

Licencia de información

4.1.1. Arquitectura propuesta

La solución propuesta por Entel Cyber Secure, enfocada en mantener la disponibilidad y la productividad de las sedes remotas o puntos de venta (2000), se propuso realizar la instalación en paralelo, lo cual fue validado en un ambiente de pruebas realizadas en conjunto con el cliente.

A continuación, se brinda la arquitectura provisional y final de la solución:

Figura 6

Arquitectura provisional.

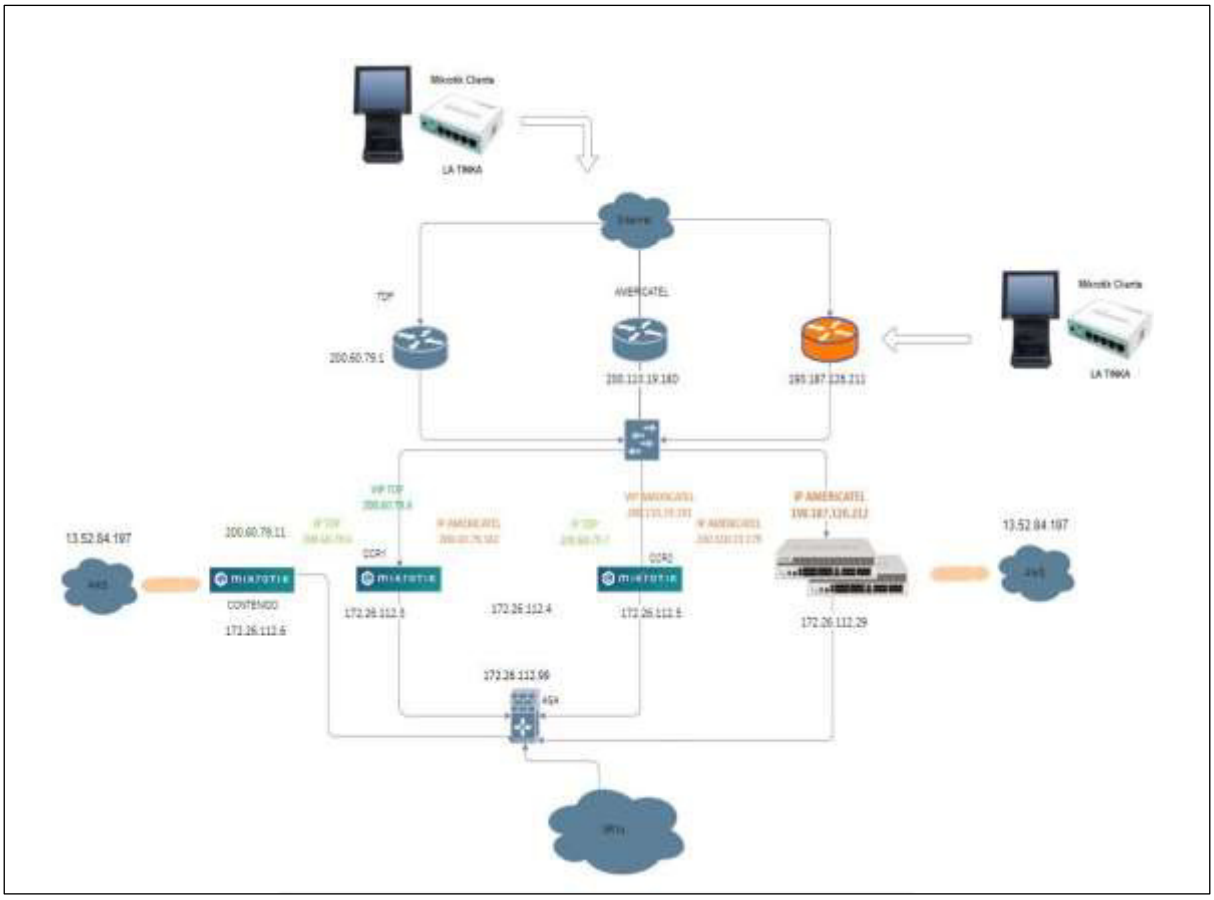
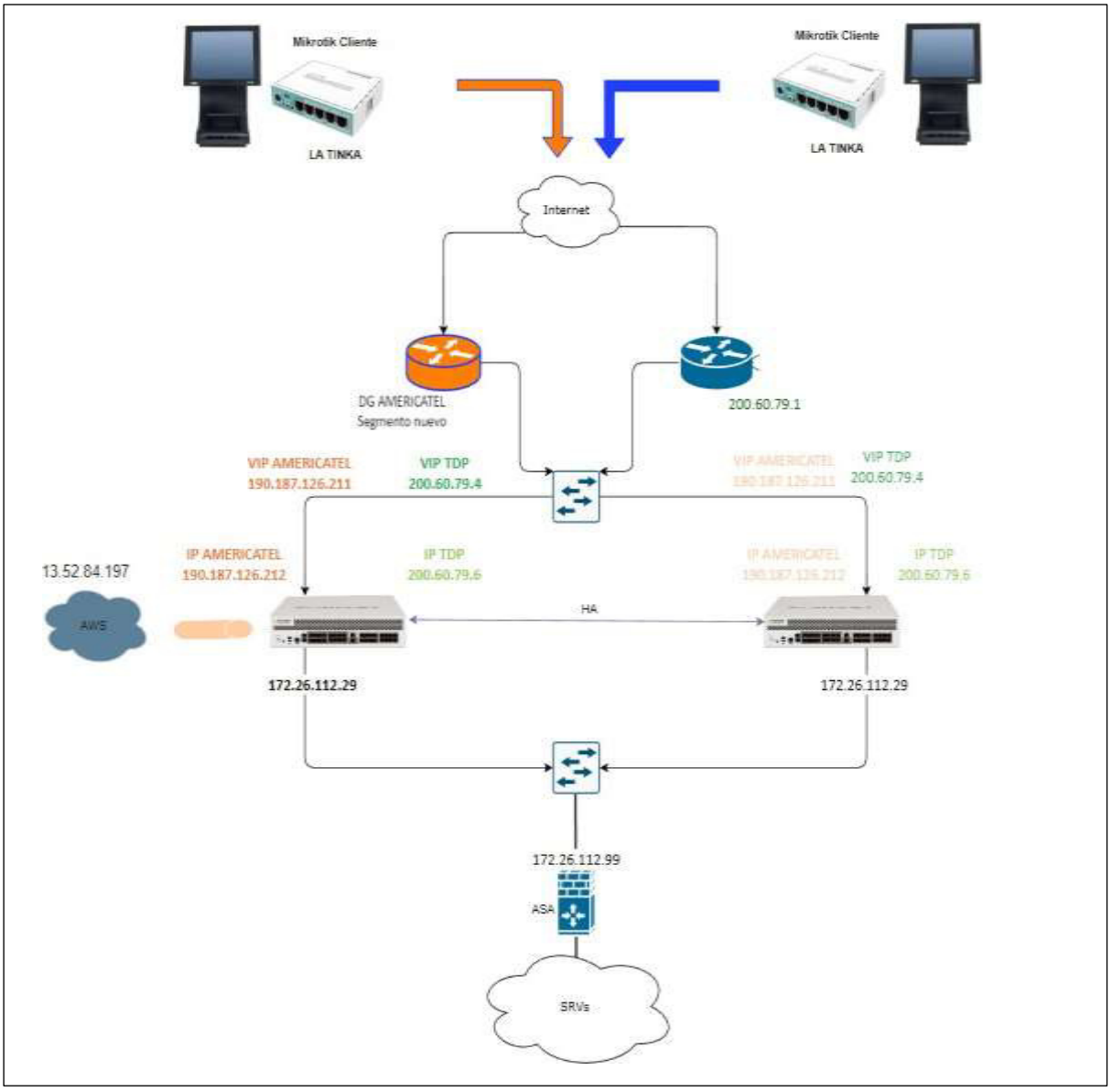


Figura 7

Arquitectura final.



4.2. Configuración del sistema

Figura 8

Información general equipo primario.

Figura 9

Información general del equipo secundario.

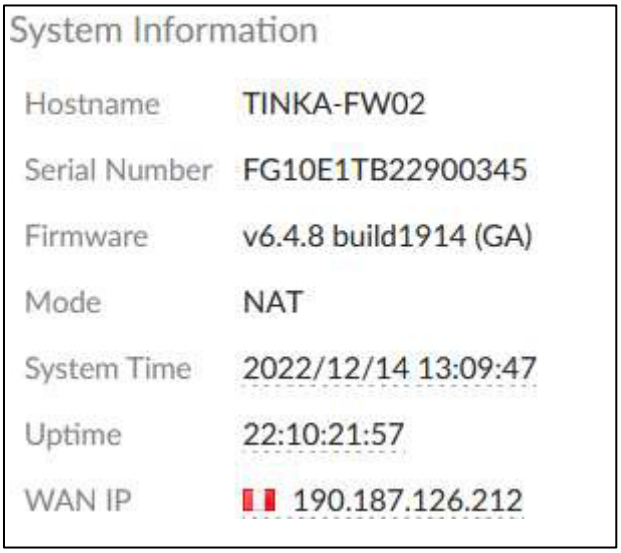


Figura 10

Licenciamiento.

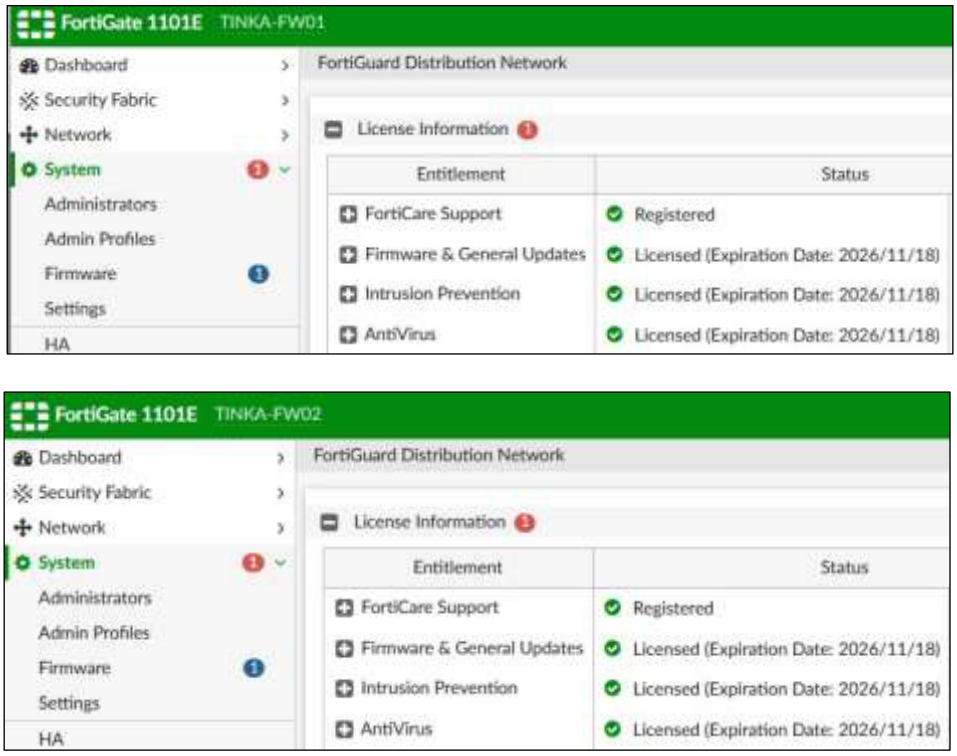
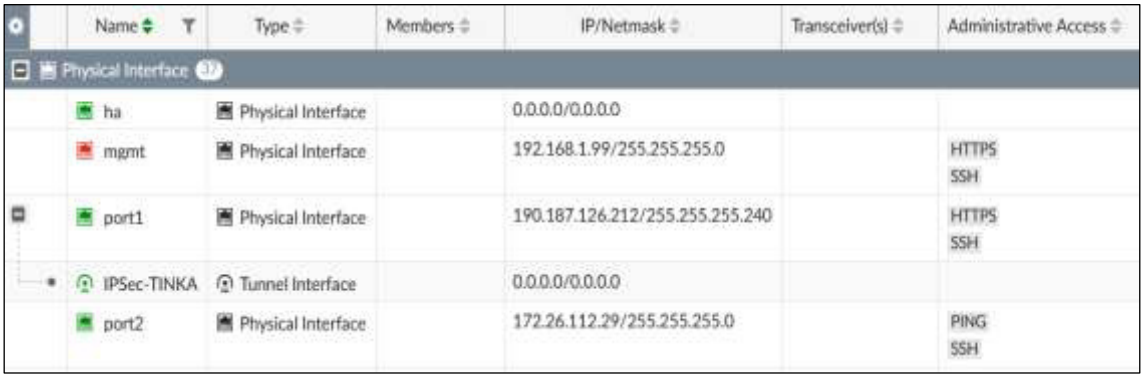


Figura 11

Interfaces.



En cuanto a la conexión a Internet, se configuró la interfaz port1 con la dirección IP 190.187.126.212/29, la cual permitirá establecer las conexiones remotas hacia el equipo

FortiGate 1101. Asimismo, sobre este enlace se encuentra implementada la VPN IPSec Dialup, destinada a facilitar el acceso remoto seguro al equipo.

Por otro lado, respecto a la red LAN, se configuró la interfaz port2 con la dirección IP 172.26.112.29/24, proporcionada por el cliente. Esta subred cumple la función de servir como vía de comunicación hacia el equipo ASA-FirePower, permitiendo la integración y el tránsito de datos entre los dispositivos involucrados en la infraestructura de red.

Figura 12

Rutas configuradas.

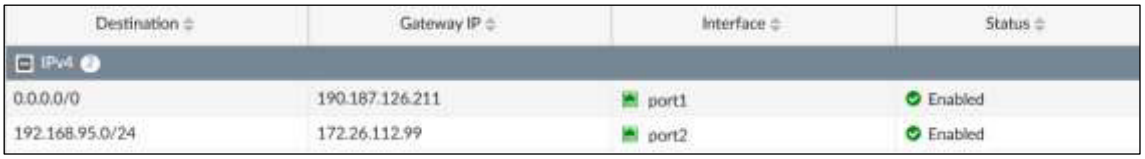
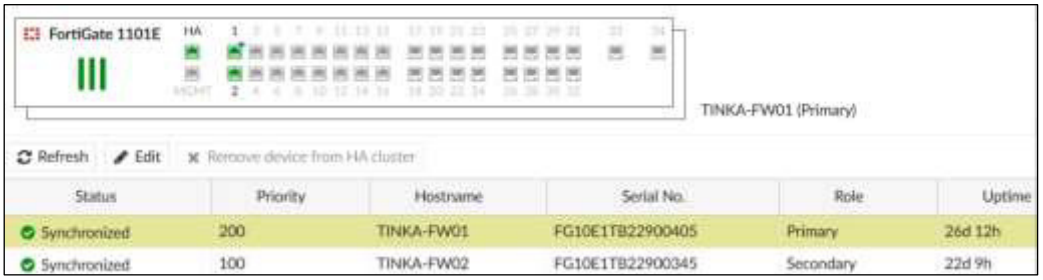


Figura 13

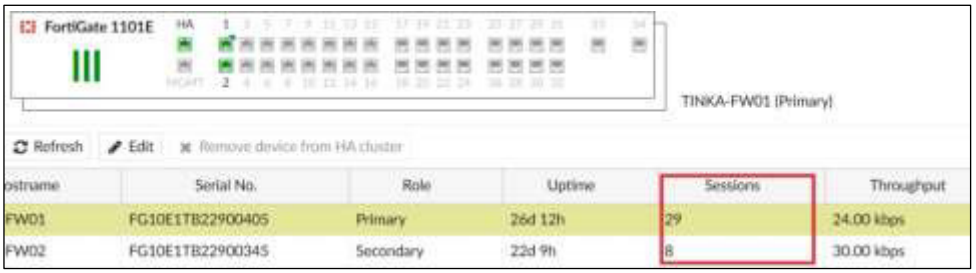
Disponibilidad.



Redundancia entre equipos desplegada en Primario y Secundario, esto se refiere a la prioridad que se estableció a los equipos, ambos equipos replican sesiones, lo que indica que al fallar uno de ellos, las conexiones no vuelven a negociar y la perdida de conectividad es imperceptible en un 99.95%.

Figura 14

Sesiones replicadas.



4.2.1. Perfiles de seguridad

El equipo FortiGate tiene configurado el siguiente perfil de antivirus el cual se encuentra aplicado en cada uno de las políticas de seguridad.

Figura 15

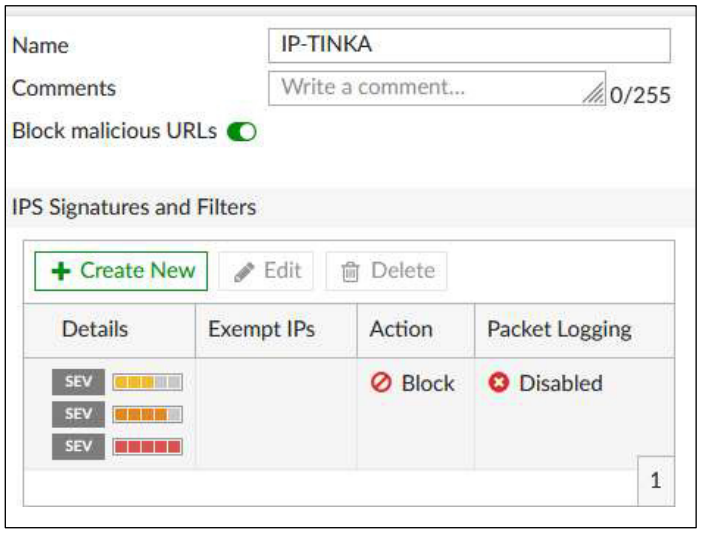
Antivirus.

4.2.2. Intrusion prevention

El equipo FortiGate tiene configurado el siguiente perfil de protección contra intrusos.

Figura 16

Configuración de protección.



4.2.3. Objetos de seguridad

El equipo FortiGate puede clasificar y ordenar objetos asociando a los diferentes recursos de la RED, de esta manera la administración es mucho más precisa.

Figura 17

Address.

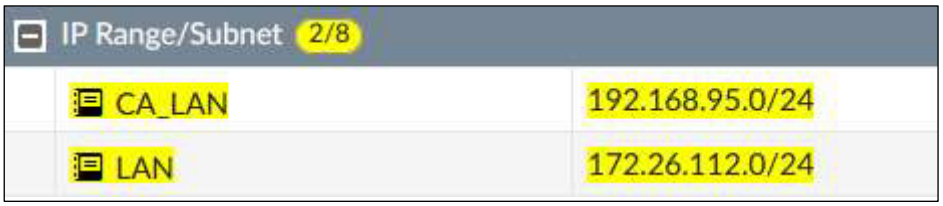
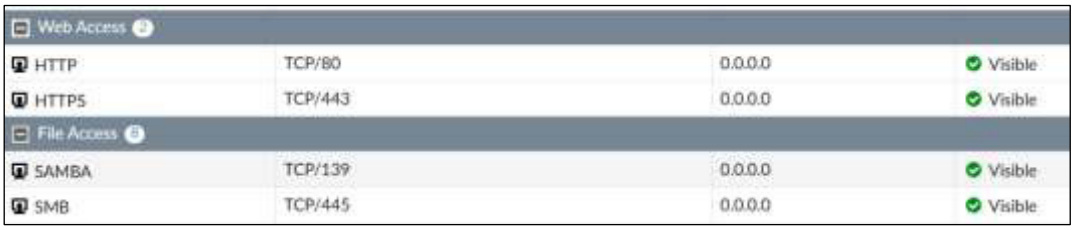


Figura 18

Services.



4.2.4. Políticas de seguridad

Se crearon las siguientes políticas de seguridad IPSec, los cuales son utilizadas para establecer los permisos de navegación hacia los servicios internos brindados por la organización La Tinka.

Figura 19

Política de entrada.

Figura 20

Política de salida.

4.2.5. Configuración VPN IPSEC

Según el diseño aprobado por La Tinka, se procedió a configurar una conexión VPN IPSec, en reemplazo al servicio L2TP, la cual es utilizada para establecer los permisos de navegación hacia los servicios internos brindados por la organización La Tinka.

Figura 21

Configuración de VPN.

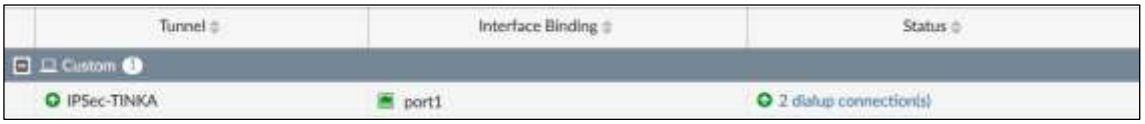
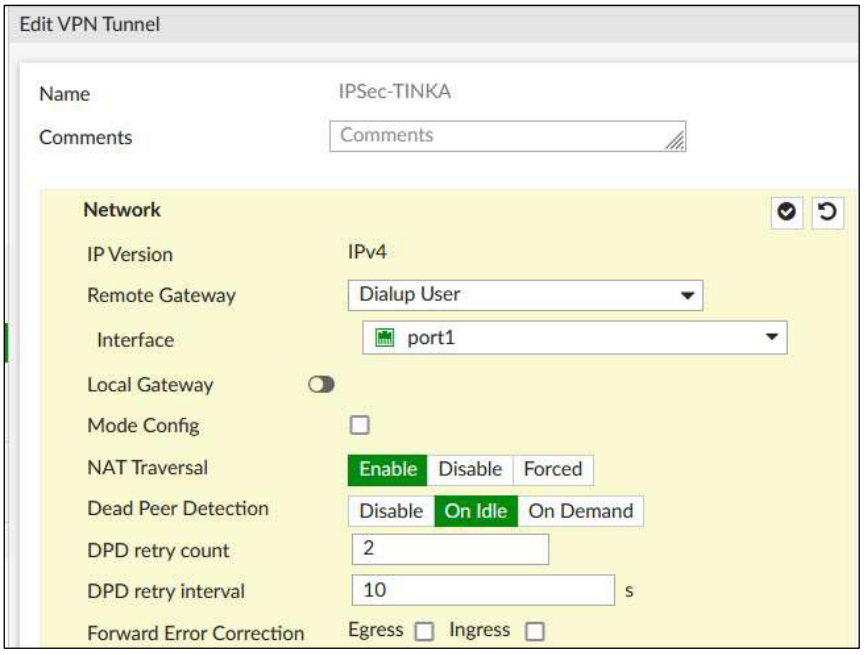


Figura 22

Configuración fase 1.




Authentication
Method
Pre-shared Key
Pre-shared Key
IKE
Version
1
2
Mode
Aggressive
Main (ID protection)
Peer Options
Accept Types
Any peer ID

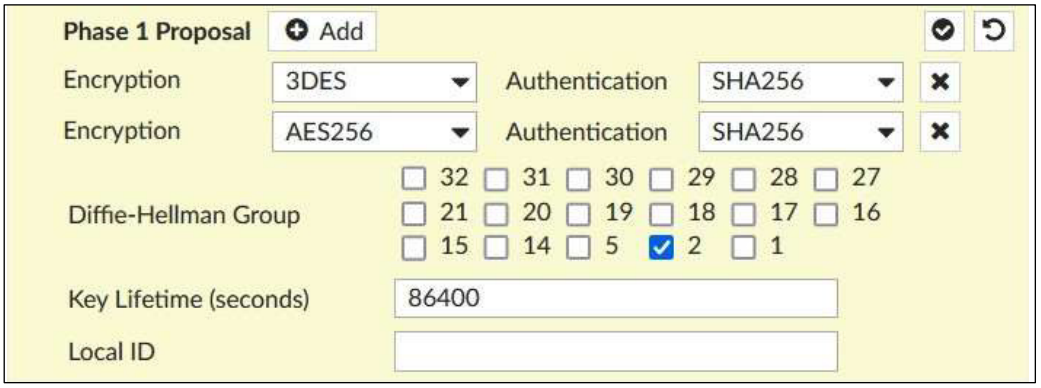
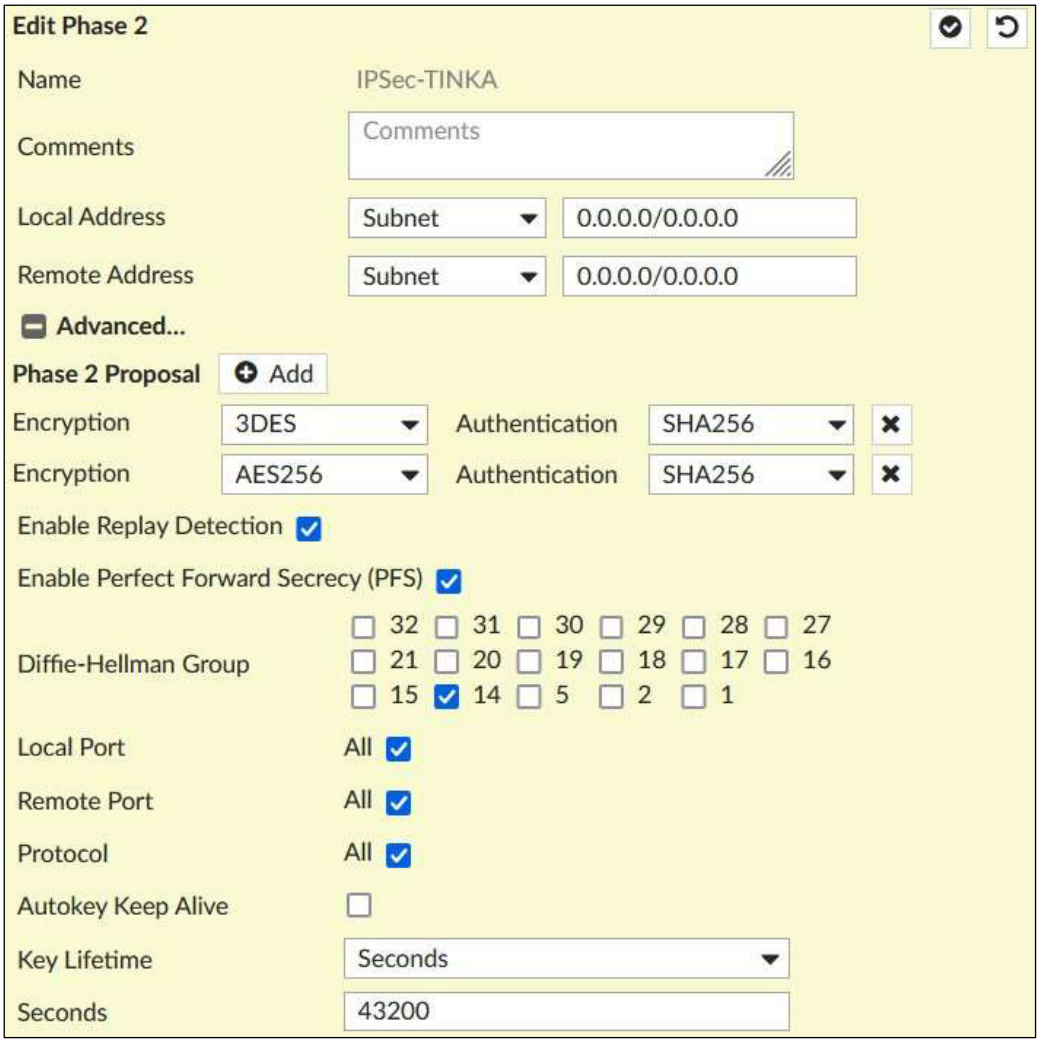

Phase 1 Proposal
Add
Encryption
3DES
Authentication
SHA256
Encryption
AES256
Authentication
SHA256
Diffie-Hellman Group
32 31 30 29 28 27
21 20 19 18 17 16
15 14 5 2 1
Key Lifetime (seconds)
86400
Local ID

Figura 23

Configuración fase 2.



4.3. Pruebas de alta disponibilidad

4.3.1. Alta disponibilidad equipo Fortigate 1101e

Según el diseño aprobado por La Tinka, se procedió a configurar una conexión VPN IPSec en reemplazo del servicio L2TP, la cual es utilizada para establecer los permisos de navegación hacia los servicios internos brindados por la organización La Tinka. Asimismo, se realizó la ejecución del cambio de roles, conocido como failover.

Figura 24

Equipo Tinka-FW02 toma rol primario.

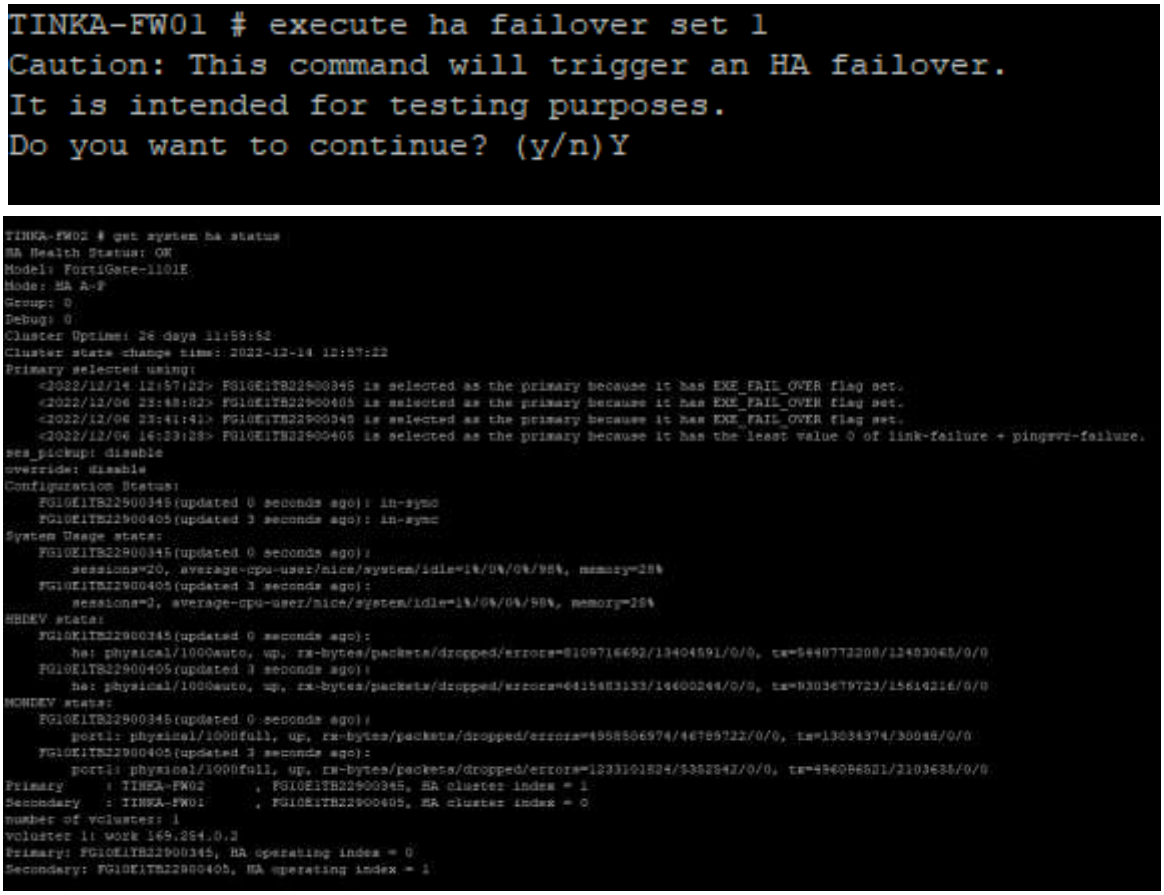


Figura 25

Equipo Tinka-FW02 toma rol secundario.

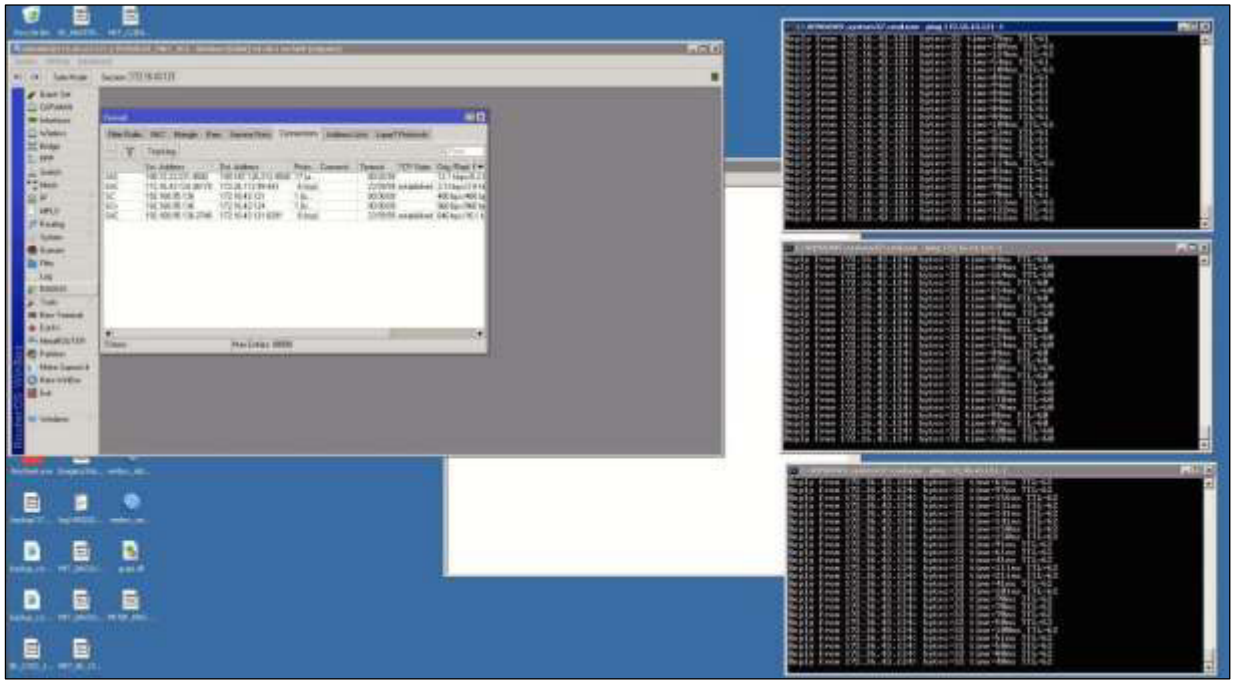
4.4. Pruebas transaccionales Tinka

4.4.1. Pruebas de conectividad

Según el diseño aprobado por La Tinka, las conexiones deberán pasar sin ningún tipo de enmascaramiento, de manera que la comunicación pueda visualizarse con las direcciones IP originales de cada uno de los dispositivos. Asimismo, se realizaron las pruebas de conexión utilizando el segmento de origen 192.168.95.0/24, luego del establecimiento del túnel a través del equipo FortiGate.

Figura 26

Pruebas de conexión.



La dirección IP de origen utilizada para las pruebas fue 192.168.95.136; asimismo, las direcciones IP de destino consideradas fueron 172.16.43.121, 172.16.43.124 y 172.36.43.121, con la finalidad de validar la comunicación hacia los servicios correspondientes a través del túnel establecido.

4.4.2. Pruebas transaccionales

Se realizaron las pruebas de transacciones utilizando el segmento de origen 192.168.43.136/29, luego del establecimiento del túnel a través del equipo FortiGate. Asimismo, para la validación correspondiente, se efectuó el inicio de sesión con el Usuario 1.

Figura 27

Inicio de sesión: Usuario 1.

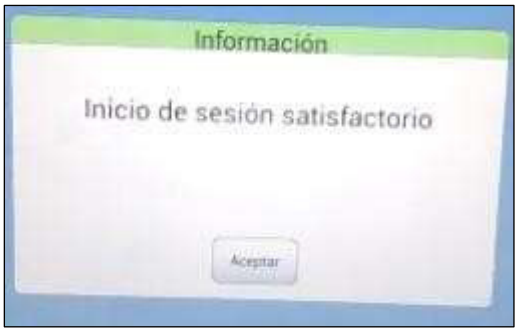


Figura 28

Visualización de juego Tinka.

Figura 29

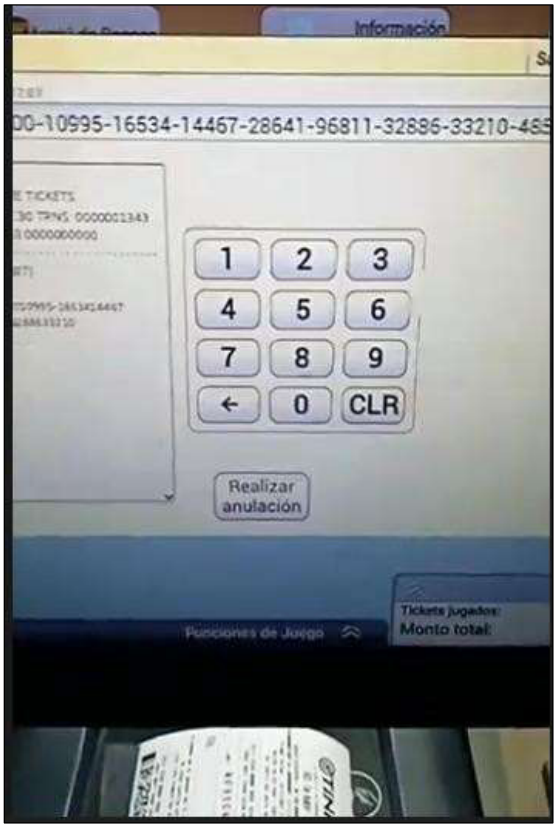
Elección de juego al azar.

Figura 30

Impresión de boleto con jugada realizada.

Figura 31

Anulación de transacción.



Como parte de las pruebas de conectividad, se ejecutó el cambio de roles o failover de la alta disponibilidad de los equipos FortiGate.

Figura 32

Cambios de failover.

```
TINKA-FW01 # execute ha failover set 1
Caution: This command will trigger an HA failover.
It is intended for testing purposes.
Do you want to continue? (y/n)Y
```

El equipo TINKA-FW02 tomo el rol primario, en este estado inicia a administrar los paquetes de las conexiones ya establecidas en el equipo TINKA-FW01.

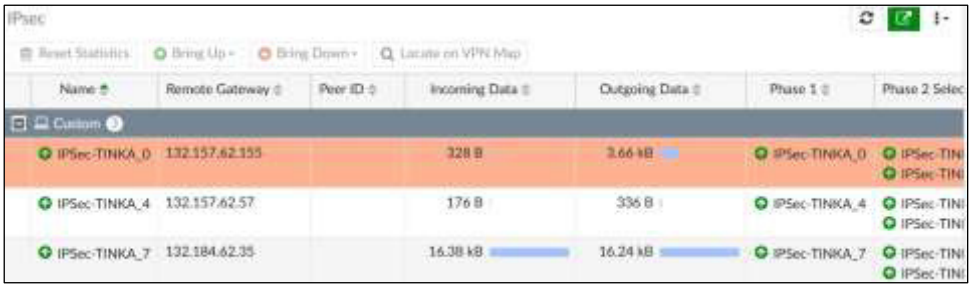
Figura 33

Administración de los paquetes de las conexiones.

```
TINKA-FW01 # get system ha status
HA Health Status: OK
Model: FortiGate-1101E
Mode: HA A-P
Group: 0
Debug: 0
Cluster Uptime: 26 days 12:4:33
Cluster state change time: 2022-12-14 13:18:37
Primary selected using:
    <2022/12/14 13:18:37> FG10E1TB22900405 is selected as the primary because it has the largest value of uptime.
    <2022/12/14 12:57:22> FG10E1TB22900345 is selected as the primary because it has EXE_FAIL_OVER flag set.
    <2022/12/06 23:48:02> FG10E1TB22900405 is selected as the primary because it has the largest value of uptime.
    <2022/12/06 23:41:41> FG10E1TB22900345 is selected as the primary because it has EXE_FAIL_OVER flag set.
ses_pickup: disable
override: disable
Configuration Status:
    FG10E1TB22900405(updated 4 seconds ago): in-sync
    FG10E1TB22900345(updated 1 seconds ago): in-sync
System Usage stats:
    FG10E1TB22900405(updated 4 seconds ago):
        sessions=18, average-cpu-user/nice/system/idle=1%/0%/0%/98%, memory=28%
    FG10E1TB22900345(updated 1 seconds ago):
        sessions=9, average-cpu-user/nice/system/idle=1%/0%/0%/98%, memory=28%
HBDEV stats:
    FG10E1TB22900405(updated 4 seconds ago):
        ha: physical/1000auto, up, rx-bytes/packets/dropped/errors=6416577247/14604143/0/0, tx=5304670023/15617868/0/0
    FG10E1TB22900345(updated 1 seconds ago):
        ha: physical/1000auto, up, rx-bytes/packets/dropped/errors=8110704645/13408235/0/0, tx=5449850263/12496846/0/0
MONDEV stats:
    FG10E1TB22900405(updated 4 seconds ago):
        port1: physical/1000full, up, rx-bytes/packets/dropped/errors=1233742005/5354269/0/0, tx=496481704/2104855/0/0
    FG10E1TB22900345(updated 1 seconds ago):
        port1: physical/1000full, up, rx-bytes/packets/dropped/errors=4959300619/46792486/0/0, tx=14078174/32411/0/0
Primary      : TINKA-FW01       , FG10E1TB22900405, HA cluster index = 0
Secondary    : TINKA-FW02       , FG10E1TB22900345, HA cluster index = 1
number of vcluster: 1
vcluster 1: work 169.254.0.1
Primary: FG10E1TB22900405, HA operating index = 0
Secondary: FG10E1TB22900345, HA operating index = 1
```

Figura 34

Visualización de túneles conectados continuamente.



Se procedió a ejecutar una jugada nueva:

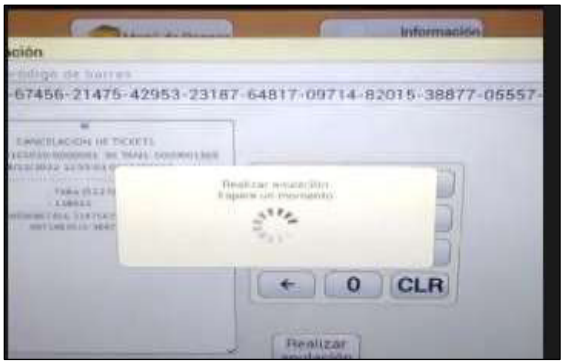
Figura 35

Nueva jugada.

Asimismo, se ejecutó la anulación de la misma:

Figura 36

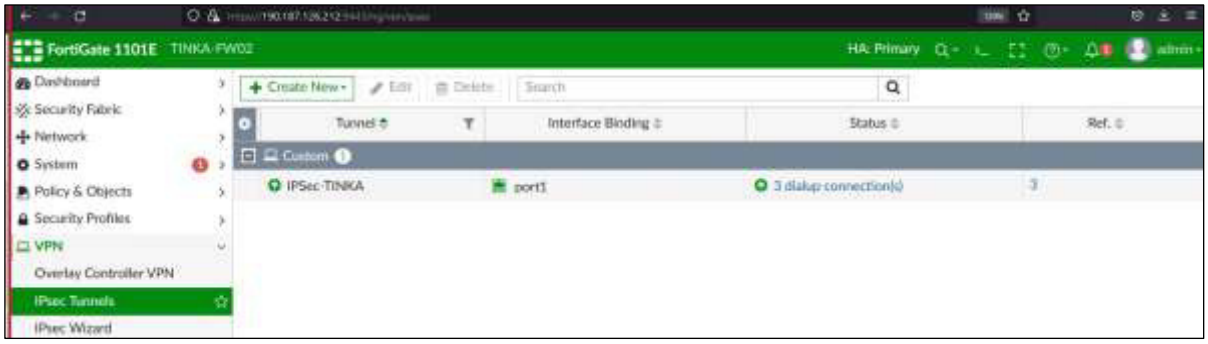
Anulación de la jugada.



Visualización de equipo Firewall TINKA-FW02 post-pruebas realizadas:

Figura 37

Post pruebas realizadas de Firewall.



El contador de KB de la conexión TINKA-7 ha aumentado posterior a la transacción realizada:

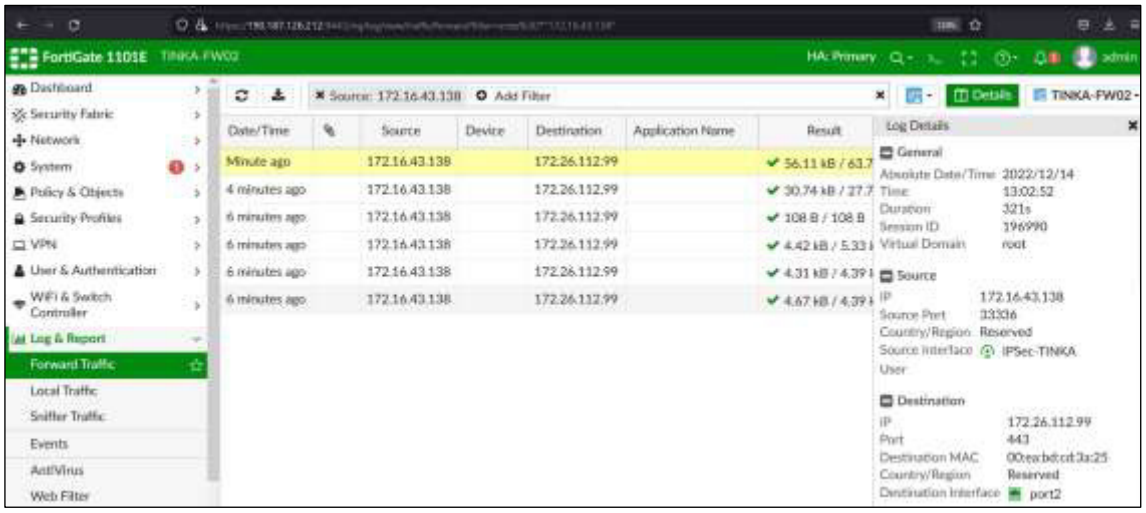
Figura 38

Aumento posterior a la transacción.

Logs visualizados referenciado al tráfico de la transacción realizada:

Figura 39

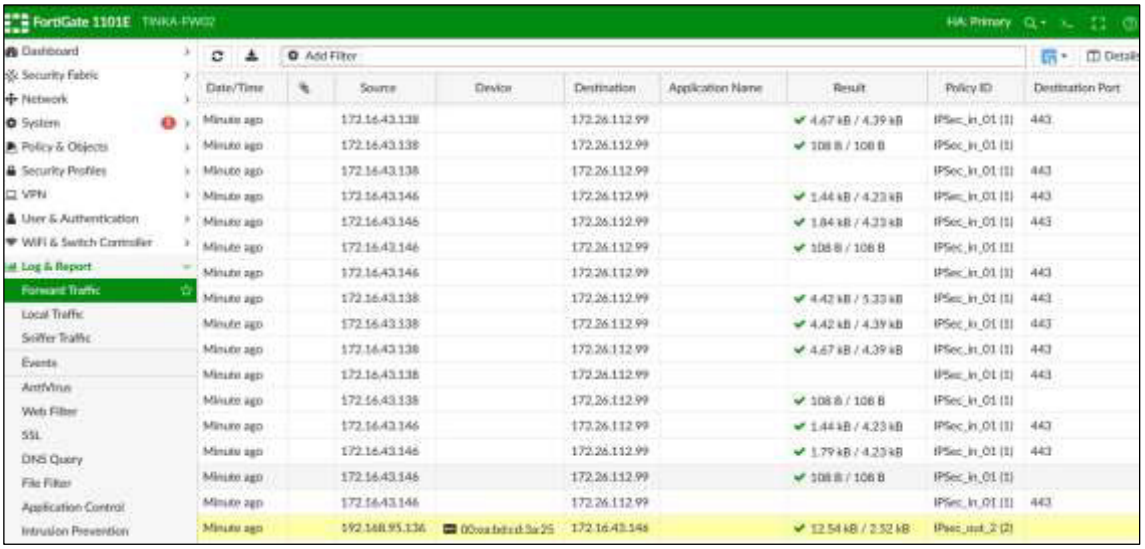
Transacción realizada.



Se confirma que el tráfico es simétrico y la comunicación se mantiene en ambos sentidos:

Figura 40

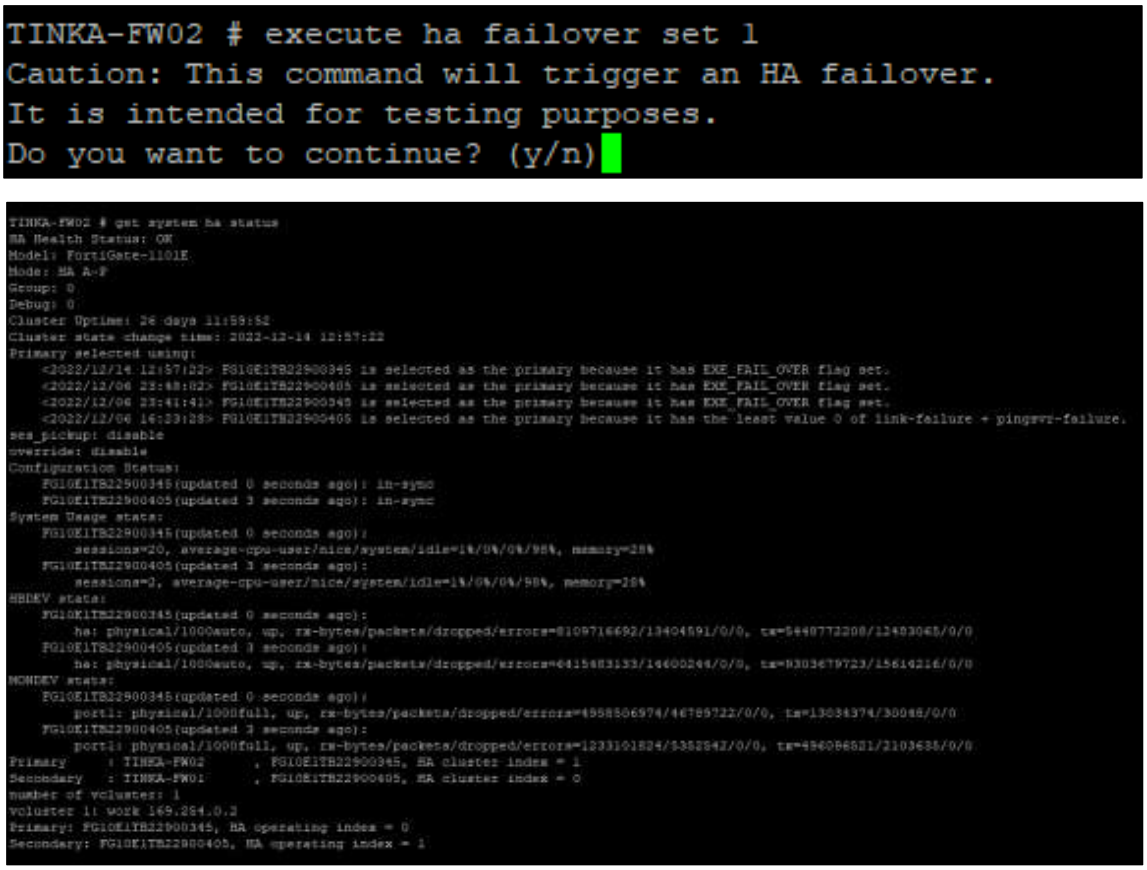
Tráfico simétrico.



Al culminar con las pruebas de transacciones con el equipo TINKA-FW02, se realizó el procedimiento de failover para que solución retorne al estado inicial de las pruebas:

Figura 41

Tráfico simétrico.



4.5. Monitoreo de recursos fortigate

Durante las pruebas de alta disponibilidad, se realizó el monitoreo de los recursos físicos de los equipos FortiGate. Cabe indicar que el estado actual corresponde a un ambiente de pruebas, por lo que no resulta representativo del escenario final. En ese contexto, se verificó el equipo Tinka-FW01, considerando el comportamiento de la CPU y la memoria.

Figura 42

Monitoreo de recursos Fortigate.

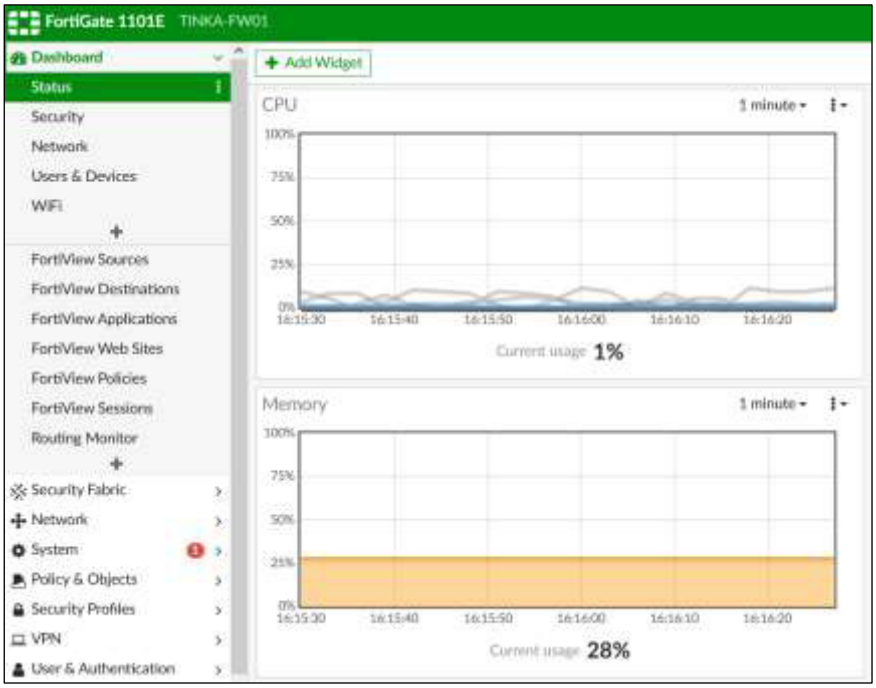


Figura 43

Sesiones.

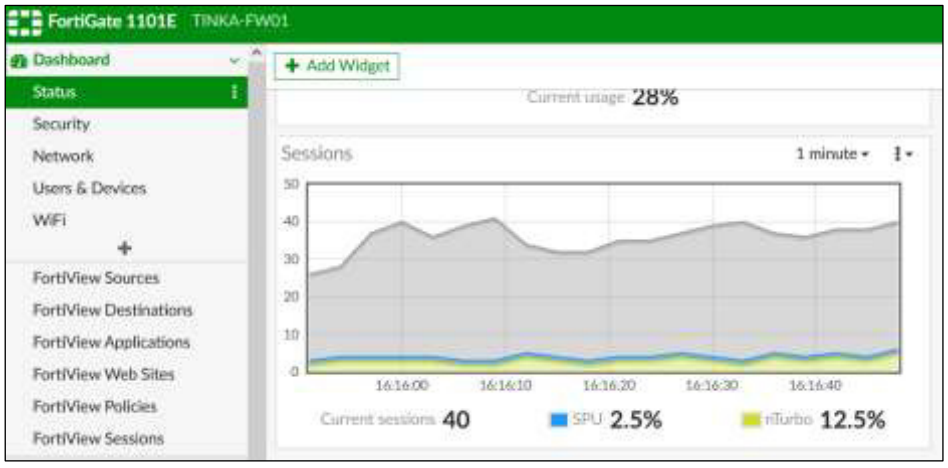
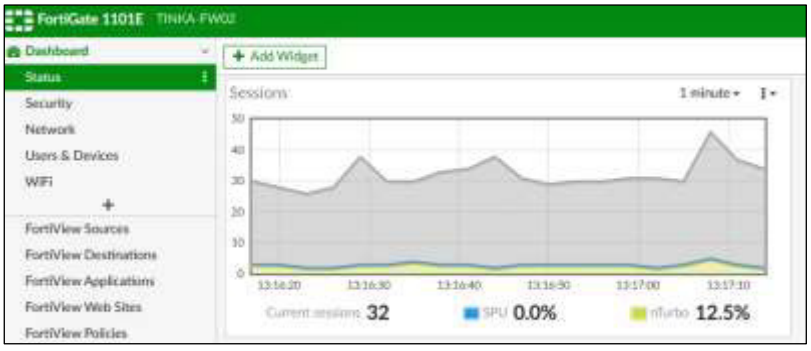


Figura 44

Tinka-FW02.

Figura 45

Sesiones.



4.6. Análisis descriptivo

Durante el desarrollo del estudio, se optó por iniciar el análisis de los datos mediante un enfoque descriptivo. Esta decisión permitió examinar de forma ordenada cada uno de los indicadores recopilados, con el objetivo de obtener una visión clara y general del conjunto de información.

Tabla 1

Análisis descriptivo del desempeño operativo.

	n	Mín.	Máx.	Media	Desv. Estándar
Pre Test	40	13,00	27,00	21,05	3,113
Post Test	40	31,00	40,00	35,28	2,386

A partir de la comparación entre los resultados obtenidos en el pre test y el post test, fue posible notar una mejora significativa en el desempeño operativo. Inicialmente los puntajes estaban entre 13 y 27, con un promedio de 21,05 y una desviación estándar de 3,113. Esto

indicaba un nivel medio de desempeño y cierta variación en los resultados. Después de aplicar la cabecera VPN, los puntajes subieron y se ubicaron entre 31 y 40, con un promedio de 35,28 y una desviación estándar más baja, de 2,386. Esta mejora mostró que la comunicación entre las tiendas fue más fluida, lo que a su vez ayudó a que las operaciones fueran más eficientes y los resultados más uniformes.

Tabla 2

Análisis descriptivo del tiempo de respuesta.

	n	Mín.	Máx.	Media	Desv. Estándar
Pre Test	9	5,00	12,00	9,11	2,315
Post Test	9	1,00	2,00	1,22	0,441

Lo que más se notó después de poner la cabecera VPN fue el tiempo que tardaba el sistema en responder. Antes, según los datos del pre test, ese tiempo iba de 5 a 12 minutos, con un promedio de 9,11 y mucha variación. Eso quería decir que la respuesta era lenta y no muy constante. Pero una vez que se implementó la cabecera, los resultados cambiaron mucho. En el post test, los tiempos bajaron a entre 1 y 2 minutos, con un promedio de 1,22 y casi sin variación. Esto dejó claro que la comunicación entre las tiendas mejoró bastante, con respuestas mucho más rápidas y parecidas entre sí después del cambio.

4.7. Análisis inferencial

Antes de hacer la prueba de hipótesis, primero se revisó si los datos tenían una distribución normal. Para eso, se eligió la prueba de Shapiro-Wilk, que es buena para cuando el número de datos es pequeño, menos de 50.

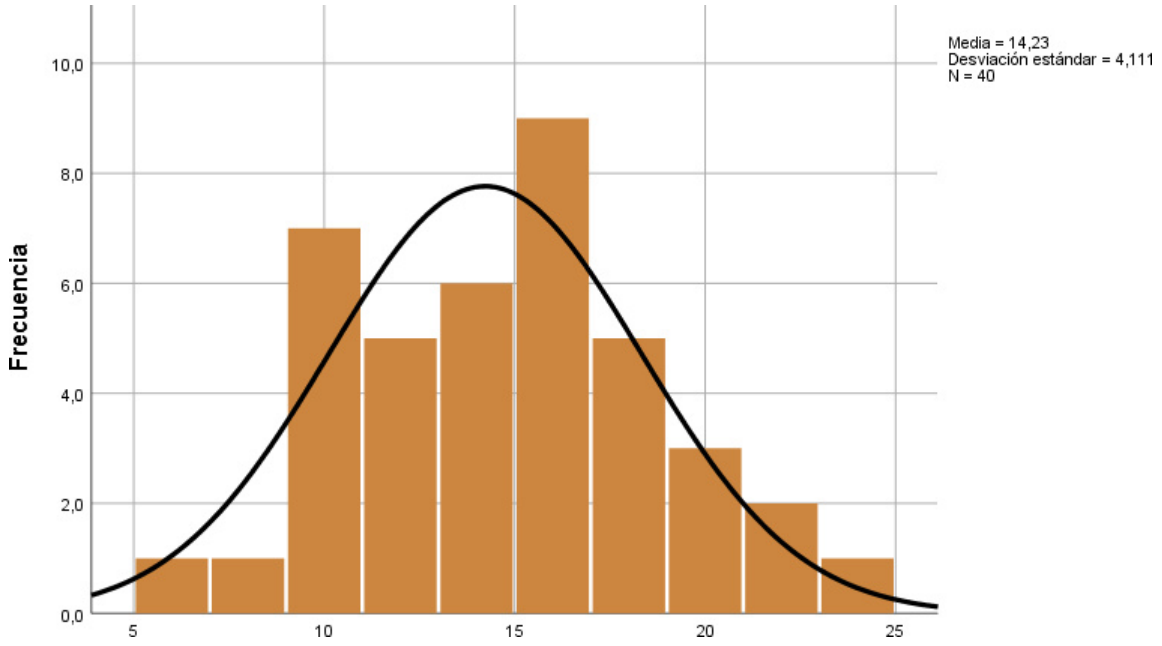
Tabla 3

Prueba de Shapiro – Wilk para desempeño operativo.

	Shapiro - Wilk		
	Estadístico	gl	Sig.
Antes – Después	0,976	40	0,549

Figura 46

Gráfica para desempeño operativo.



Al realizar la prueba de normalidad Shapiro-Wilk sobre el desempeño operativo, se obtuvo un valor de significancia de 0,549, considerando un total de 40 casos. Dado que el valor de significancia fue superior a 0,05, se concluyó que los datos siguen una distribución normal. Esto abrió la posibilidad de emplear pruebas paramétricas en el análisis. Así, se decidió utilizar la prueba t de Student para muestras relacionadas al comparar los resultados previos y posteriores a la implementación del diseño de la cabecera VPN, ya que los datos cumplían con los requisitos de normalidad necesarios para su uso.

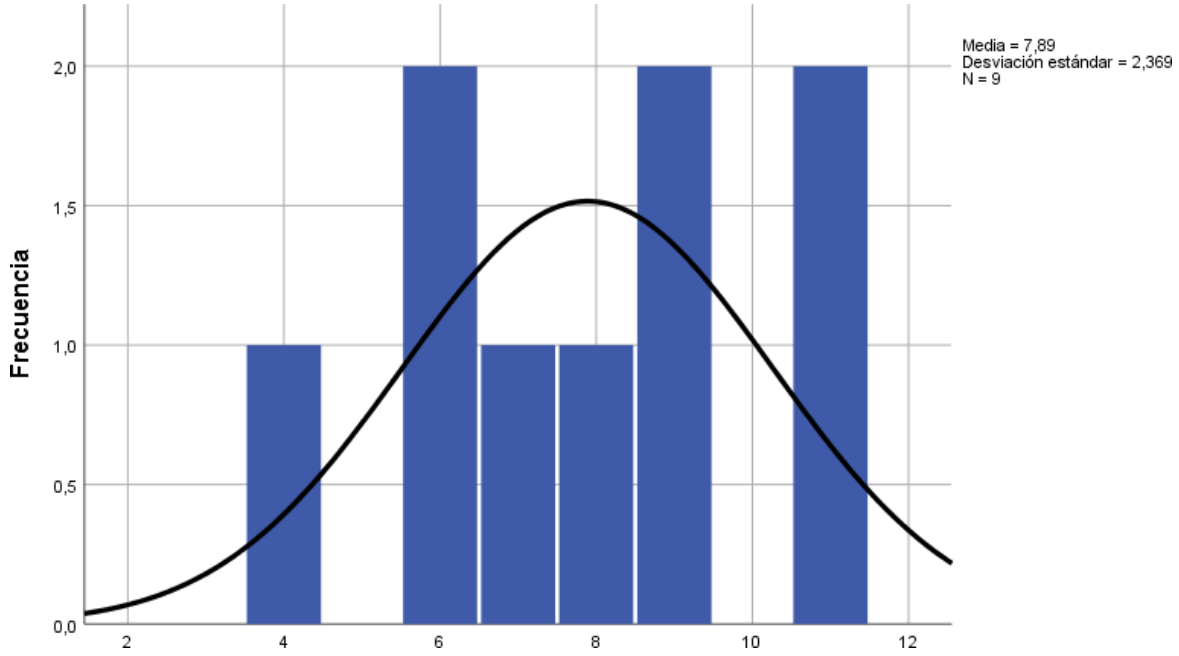
Tabla 4

Prueba de Shapiro – Wilk para tiempo de respuesta.

	Shapiro - Wilk		
	Estadístico	gl	Sig.
Antes – Después	0,949	40	0,679

Figura 47

Gráfica para tiempo de respuesta.



Al evaluar el tiempo de respuesta, se realizó la prueba de normalidad Shapiro-Wilk, la cual arrojó un valor de significancia de 0,679, basado en una muestra de 9 casos. Dado que el valor de significancia fue mayor a 0,05, se concluyó que los datos no muestran desviaciones significativas de una distribución normal. Esto permitió confirmar que se cumplía con el supuesto de normalidad, lo que a su vez justificó el uso de una prueba paramétrica. Por lo tanto,

se optó por la prueba t de Student para muestras relacionadas, con el fin de comparar los tiempos de respuesta antes y después de la implementación del diseño de la cabecera VPN.

4.8. Contrastación de hipótesis

Una vez que se haya verificado si los datos siguen una distribución normal mediante las pruebas estadísticas correspondientes, se elegirá la prueba adecuada para evaluar las hipótesis planteadas. Si los datos son normales, se utilizará la prueba t de Student para muestras relacionadas. Sin embargo, si no se cumple con la normalidad, se recurrirá a la prueba no paramétrica de Wilcoxon. En ambos casos, se fijó un nivel de significancia del 5 % (0,05) para decidir si se acepta o se rechaza la hipótesis.

4.8.1. Desempeño operativo

Ho: El diseño de la cabecera VPN no mejora el desempeño operativo en los puntos de venta de una empresa de loterías y apuestas deportivas.

H1: El diseño de la cabecera VPN mejora el desempeño operativo en los puntos de venta de una empresa de loterías y apuestas deportivas

Tabla 5

Prueba T-Student para el desempeño operativo.

	Desviación	**Desv. Error promedio**	**95% De intervalo de confianza de la diferencia**		**t**	**gl**	**Sig. (bilateral)**
			Inferior	**Superior**			
Pre Test - Post Test	4,11	0,650	-15,54	-12,91	-21,88	39	0,00

El análisis realizado mediante la prueba t de Student mostró un valor de significancia bilateral de 0,00, lo cual evidencia una diferencia significativa entre los resultados obtenidos antes y después de la implementación. Al ser este valor menor al nivel de significancia definido

(0,05), se descarta la hipótesis nula y se da respaldo a la hipótesis alternativa. Esto permite afirmar que la introducción del diseño de la cabecera VPN tuvo un efecto favorable en el desempeño operativo de los puntos de venta de la empresa de loterías y apuestas deportivas, en línea con lo que también se reflejó en los datos descriptivos.

4.8.2. Tiempo de respuesta

Ho El diseño de la cabecera VPN no mejora el tiempo de respuesta en los puntos de venta de una empresa de loterías y apuestas deportivas.

H1: El diseño de la cabecera VPN mejora el tiempo de respuesta en los puntos de venta de una empresa de loterías y apuestas deportivas

Tabla 6

Prueba T-Student para el tiempo de respuesta.

	Desviación	**Desv. Error promedio**	**95% De intervalo de confianza de la diferencia**		**t**	**gl**	**Sig. (bilateral)**
			Inferior	**Superior**			
Pre Test - Post Test	2,37	0,790	6,09	9,71	9,99	8	0,00

Al analizar los tiempos de respuesta antes y después de la implementación del diseño de la cabecera VPN, se encontró que el valor de significancia fue muy bajo, lo que indica una diferencia real y notable. Por esta razón, se descartó la idea de que no hubiera cambios y se confirmó que la mejora en los tiempos de respuesta fue significativa. Esto demuestra que la solución aplicada logró optimizar la comunicación en los puntos de venta, facilitando procesos más ágiles y eficientes en la empresa de loterías y apuestas deportivas.

V. DISCUSIÓN DE RESULTADOS

Se optó por rediseñar la cabecera VPN utilizando dispositivos FortiGate 1101E, incorporando además un esquema de alta disponibilidad para garantizar estabilidad ante cualquier eventualidad. Esta nueva solución reemplazó el antiguo modelo basado en L2TP, que ya presentaba limitaciones en cuanto a seguridad y rendimiento. Con el diseño de la VPN, fue posible mejorar aspectos clave como la autenticación, el cifrado de la información y la integridad de los datos transmitidos. No se trató solo de cambiar la tecnología, sino de asegurar que el nuevo sistema realmente respondiera a las necesidades operativas. Por eso, se realizaron diversas pruebas: desde simulaciones de fallos hasta análisis de replicación de sesiones y monitoreo del desempeño general. Los resultados fueron positivos, confirmando una disponibilidad del servicio del 99.95%, lo cual representó un avance considerable frente al modelo anterior.

Luego de aplicar los cambios en la infraestructura de red, se notó una mejora clara en el desempeño general. Antes de la implementación del nuevo diseño de la cabecera VPN, las evaluaciones iniciales reflejaban un rendimiento moderado: la media fue de 21,05, con resultados que variaron entre 13,00 y 27,00, y una desviación estándar de 3,113. Estos valores mostraban no solo un nivel bajo de eficiencia, sino también diferencias importantes entre los distintos puntos evaluados. Tras la intervención, los resultados del postest evidenciaron un avance notable. La media aumentó a 35,28, con un rango más alto y concentrado, entre 31,00 y 40,00, y una desviación estándar reducida a 2,386. Esta disminución en la variabilidad indicó una mayor estabilidad y uniformidad en el rendimiento, algo que no se había observado con la estructura anterior. La prueba t de Student validó estadísticamente esta mejora, con un valor de $p = 0,00$ que confirmó la existencia de una diferencia significativa entre ambos escenarios. Aunque los estudios revisados no presentaron cifras directamente comparables, varios coincidieron en aspectos clave. Por ejemplo, Blancaflor et al. (2024) destacaron que, si bien

los usuarios entienden cada vez mejor el funcionamiento de las VPN, aún hay inquietudes sobre su fiabilidad. Señalaron que muchas de esas fallas están relacionadas con debilidades estructurales en el diseño o en la gestión de los recursos de red. En contraste, la solución adoptada en esta investigación, basada en dispositivos FortiGate 1101E y una arquitectura con alta disponibilidad, demostró cómo una infraestructura bien diseñada puede mejorar de manera tangible el rendimiento y reducir esos puntos débiles. Por otro lado, Quintana y Gallardo (2022) compartieron una experiencia similar, en la que el rediseño de una VPN full mesh en una empresa del sector metalmecánico les permitió superar múltiples problemas de conectividad y mejorar la eficiencia de su operación. Este tipo de resultados contribuyó a reforzar la validez de lo observado en el presente estudio, destacando la importancia de tomar decisiones técnicas estratégicas y bien fundamentadas

A raíz del diseño de la nueva cabecera VPN, se produjo una mejora evidente en los tiempos de respuesta del sistema. Durante la evaluación previa, los registros mostraban una respuesta lenta y poco consistente: los valores variaban entre 5,00 y 12,00 minutos, con una media de 9,11 minutos y una desviación estándar de 2,315. Estos resultados reflejaban las limitaciones que enfrentaban los puntos de venta en sus operaciones diarias. Después del cambio, la diferencia fue notoria. En la etapa posterior, los tiempos se redujeron drásticamente, ubicándose entre 1,00 y 2,00 minutos. La media bajó a 1,22 minutos y la desviación estándar se redujo a solo 0,441, lo que no solo indicó mayor velocidad, sino también una respuesta más uniforme. Esta mejora, superior al 86% en promedio, tuvo un impacto directo en la eficiencia operativa. La prueba t de Student confirmó la relevancia de este cambio, arrojando un valor de $p = 0,00$ que validó estadísticamente la diferencia entre ambos escenarios. Aunque no se encontraron estudios que trabajaran exactamente con los mismos parámetros temporales, algunos antecedentes ayudaron a contextualizar los hallazgos. El trabajo de Wu et al. (2024), por ejemplo, presentó un modelo capaz de procesar grandes volúmenes de tráfico en pocos

segundos, con resultados muy precisos en la identificación de servicios y detección de proxies. Aunque su enfoque fue distinto, destacó la importancia de mejorar el rendimiento en tiempo real, algo que también se logró en esta experiencia. Por otro lado, Malque (2024) mostró cómo la migración a una red de fibra óptica propia permitió a una empresa eléctrica optimizar sus tiempos de respuesta y su capacidad de control. Ambos casos, aunque diferentes en naturaleza, reforzaron una idea en común: cuando se invierte en infraestructura de red adecuada, los resultados no tardan en reflejarse en la eficiencia del servicio.

VI. CONCLUSIONES

- Con el diseño de la cabecera VPN utilizando dispositivos FortiGate 1101E y la configuración de alta disponibilidad, junto con la conexión IPsec Dialup, se logró establecer una infraestructura de red mucho más segura y eficiente para los puntos de venta de la empresa de loterías y apuestas deportivas. La correcta implementación de perfiles de seguridad, rutas optimizadas y mecanismos de failover no solo proporcionó mayor seguridad, sino que también permitió garantizar una operación continua y estable entre las tiendas, mejorando así la calidad de la comunicación.
- Después del diseño de la nueva solución tecnológica, el desempeño operativo de los puntos de venta mejoró notablemente. Los puntajes aumentaron considerablemente, pasando de una media de 21,05 en la evaluación inicial a 35,28 en la evaluación posterior, lo que indica un avance significativo en la eficiencia operativa. Este cambio fue respaldado por la prueba estadística, que mostró un valor de $p = 0,00$, confirmando que la solución implementada tuvo un impacto directo en la optimización de los procesos internos y ayudó a reducir la variabilidad en el rendimiento entre las distintas ubicaciones.
- Se pudo observar una notable mejora en los tiempos de respuesta tras el diseño de la cabecera VPN. Antes de la intervención, el tiempo promedio era de 9,11 minutos, pero después de la implementación, la media se redujo a 1,22 minutos, lo que representó una disminución de más del 86%. Este cambio, respaldado por una significancia estadística de $p = 0,00$, confirma que la solución aplicada optimizó considerablemente la velocidad de atención en los puntos de venta, lo que a su vez contribuyó a una mayor eficiencia operativa y una experiencia mucho más ágil para los usuarios.

VII. RECOMENDACIONES

- Es recomendable realizar un mantenimiento periódico de los dispositivos FortiGate utilizados en la cabecera VPN, asegurándose de actualizarlos regularmente y renovar las licencias de seguridad necesarias. Además, se sugiere llevar un monitoreo constante del rendimiento de la red y aplicar los parches de seguridad correspondientes para prevenir cualquier posible vulnerabilidad que pudiera afectar la comunicación entre los puntos de venta.
- Para continuar mejorando el desempeño operativo, sería recomendable expandir el diseño de la cabecera VPN a las nuevas sedes o puntos de venta que se sumen en el futuro. También es fundamental ofrecer capacitación continua al personal técnico encargado del mantenimiento de la red. Además, la implementación de indicadores de desempeño permanentes permitiría evaluar y gestionar la eficiencia operativa de manera constante.
- Con el fin de mantener un buen desempeño, se recomienda utilizar herramientas de monitoreo en tiempo real para el tiempo de respuesta, lo que permitirá identificar rápidamente cualquier cuello de botella o interrupción. También sería útil realizar auditorías periódicas del tráfico VPN para garantizar que la velocidad de respuesta se mantenga constante, incluso durante picos de alta demanda o cuando el número de usuarios conectados crezca.

VIII. REFERENCIAS

Blancaflor, E., Armado, J., Cabral, C., Laurenio, E., y Salanguste, J. (2024). Un análisis comparativo de las aplicaciones VPN y sus capacidades de seguridad frente a problemas de seguridad. En *Signals and Communication Technology* (pp. 73-82). Springer. https://doi.org/10.1007/978-3-031-47100-1_7

Carletto, J. (2022). *Optimización de tráfico en redes multiservicios aplicando técnicas heurísticas.* [Tesis de maestría, Universidad Nacional de La Plata]. Repositorio Institucional UNLP. https://sedici.unlp.edu.ar/handle/10915/147414

Conche, H. (2021). *La red dorsal nacional de fibra óptica y su influencia en el servicio de internet en el Perú* [Tesis de pregrado, Universidad Nacional Federico Villarreal]. Repositorio Institucional UNFV. https://goo.su/NmWm5

Diario El Peruano. (24 de septiembre de 2024). Transformación digital: 72% de las empresas en el Perú comenzará este proceso en el 2024. *El Peruano*. https://goo.su/l8zU8oX

Fassl, M., Ponticello, A., Dabrowski, A., y Krombholz, K. (2023). Investigación del folclore de seguridad: un estudio de caso sobre el fenómeno Tor sobre VPN. *Proceedings of the ACM on Human-Computer Interaction*, *7*, 1-26. https://doi.org/10.1145/3610193

Fayoumi, M., Fawareh, M., y Nashwan, S. (2022). Clasificación del tráfico de redes VPN y no VPN mediante funciones relacionadas con el tiempo. *Computers, Materials and Continua*, *72*(2), 3091-3111. https://doi.org/10.32604/cmc.2022.025103

Hernández, R. (2018). *Metodología de la investigación: las rutas cuantitativa, cualitativa y mixta.* McGraw Hill.

Hernández, R. y Mendoza, C. (2023). *Metodología de la investigación, las rutas cuantitativa, cualitativa y mixta.* McGraw-Hill Interamericana Editores.

Hernández, R., Fernández, C. y Baptista, P. (2014). *Metodología de la investigación.* Mcgraw-hill

La Universidad en Internet. (2021). ¿Qué es una VPN?: funciones, tipos e importancia. *UNIR Revista*. https://www.unir.net/ingenieria/revista/que-es-vpn/

Lazarte, D., y Silva, G. (2022). *Diseño de una red privada virtual (VPN) basada en software libre para la mejora de la seguridad de la información de la jurisdicción de la dirección de redes integradas de salud Lima Centro* [Tesis de pregrado, Universidad César Vallejo]. Repositorio Institucional UCV. https://repositorio.ucv.edu.pe/handle/20.500.12692/92270

Luna, A., y Zeta, C. (2021). *Implementación de redes VPN MIKROTIK para los servidores entre ciudades de Lima y Pisco* [Tesis de pregrado, Universidad César Vallejo]. Repositorio Institucional UCV. https://repositorio.ucv.edu.pe/handle/20.500.12692/82658

Malque, A. (2024). *Migración de las telecomunicaciones a una red propia de fibra óptica para mejorar la gestión y control de los servicios en una empresa transmisora eléctrica* [Tesis de pregrado, Universidad Nacional Federico Villarreal]. Repositorio Institucional UNFV. https://goo.su/NF0fsIq

Núñez, D., Espinoza, J., Pérez, F. y Rodríguez, G. (2026). A Comparison of Technologies for Layer 2 Network Extension over IP: EoIP vs. VxLAN. *Journal of Computer Science & Technology, 26*(1), e05. https://doi.org/10.24215/16666038.26.e05

Organismo Supervisor de Inversión Privada en Telecomunicaciones - OSIPTEL. (2023). *La ruta de la conectividad en el Perú*. https://goo.su/vrHkG3

Padilla, E., y Barrionuevo, B. (2023). *Propuesta de plan de marketing para desarrollar oportunidades de crecimiento para las loterías de la empresa LA TINKA S.A.* [Tesis de pregrado, Universidad Peruana de Ciencias Aplicadas]. Repositorio Institucional UPC. https://goo.su/NjGGC

Quintana, J., y Gallardo, E. (2022). *Diseño de una red VPN full mesh para mejorar la comunicación y seguridad en una empresa metalmecánica de Lima - 2021* [Tesis de pregrado, Universidad Tecnológica del Perú]. Repositorio Institucional UTP. https://repositorio.utp.edu.pe/handle/20.500.12867/6572

Salazar, J. (2018). *Cambio Tecnológico acelerado e impactos en el mundo del trabajo: ¿qué hacer?* OIT para América Latina y Caribe. https://acortar.link/QlAIuc

Wu, H., Liu, Y., Cheng, G., y Hu, X. (2024). RT-CBCH: Identificación de tráfico de VPN en tiempo real basado en datos muestreados en redes de alta velocidad. *IEEE Transactions on Network and Service Management*, *21*(1), 88-107. https://doi.org/10.1109/TNSM.2023.3286446

IX. ANEXOS

Anexo A: Matriz de Consistencia:
Título: Diseño de una cabecera VPN para mejorar la calidad de comunicación en las tiendas de una empresa de loterías y apuestas deportivas en Cercado de Lima

PROBLEMA	OBJETIVO	HIPÓTESIS	VARIABLES	DIMENSIONES	INDICADORES	INSTRUMENTO	METODOLOGÍA
Problema General ¿Cómo el diseño de una cabecera VPN puede mejorar la calidad de comunicación en los puntos de venta de una empresa de loterías y apuestas deportivas? **Problemas Específicos** Problema específico 1: ¿Cómo influye el diseño de la cabecera VPN en la calidad de comunicación en los puntos de venta de la empresa de loterías y apuestas deportivas? Problema específico 2: ¿De qué manera la cabecera VPN puede contribuir a mejorar el desempeño operativo en los puntos de venta de una empresa de loterías y apuestas deportivas? Problema específico 3: ¿Cómo puede la cabecera VPN optimizar el tiempo de respuesta en los puntos de venta de una empresa de	**Objetivo general** Diseñar una cabecera VPN para mejorar la calidad de comunicación en los puntos de venta de una empresa de loterías y apuestas deportivas. **Objetivos Específicos** Objetivo específico 1: Desarrollar el diseño de la cabecera VPN para mejorar la calidad de comunicación en los puntos de venta de la empresa de loterías y apuestas deportivas. Objetivo específico 2: Mejorar el desempeño operativo con la cabecera VPN en los puntos de venta de una empresa de loterías y apuestas deportivas. Objetivo específico 3: Mejorar el tiempo de respuesta con la cabecera VPN en los puntos de venta de una empresa de loterías y apuestas deportivas.	**Hipótesis General** El diseño de una cabecera VPN mejora la calidad de comunicación en los puntos de venta de una empresa de loterías y apuestas deportivas. **Hipótesis específicas** Hipótesis específica 1: El diseño adecuado de la cabecera VPN mejorará significativamente la calidad de la comunicación en los puntos de venta de la empresa de loterías y apuestas deportivas. Hipótesis específica 2: El diseño de la cabecera VPN incrementa el desempeño operativo de los puntos de venta de la empresa de loterías y apuestas deportivas. Hipótesis específica 3: El diseño de la cabecera VPN mejora el tiempo de respuesta en los puntos de venta de una empresa de loterías y apuestas	**Variable Independiente: Cabecera VPN** Herramienta que permite establecer una conexión segura y encriptada a través de Internet, facilitando el acceso remoto a los recursos de una organización. Utiliza protocolos que garantizan la privacidad y protección de los datos, creando un canal seguro en redes no confiables (La Universidad en Internet, 2021)	Desempeño operativo	• Seguridad • Calidad de servicio • Experiencia del colaborador	Documentación técnica y software de diseño. Observación. Encuesta	**Enfoque**: mixto **Tipo: Aplicada** **Diseño**: Pre-experimental. **Nivel:** Descriptivo **Población:** 40 trabajadores **Muestra:** 40 trabajadores **Técnica.** Ficha de registro **Instrumentos.** Observación, encuesta
			Variable dependiente: Calidad de comunicación El avance de los servicios de	Tiempo de respuesta	• Percepción de rapidez		

loterías y apuestas deportivas?		deportivas.	comunicación permite un acceso seguro y privado a redes y sistemas, facilitando la transferencia rápida y eficiente de información. Además, estas conexiones optimizan la productividad al permitir un intercambio fluido de información en tiempo real (OSIPTEL, 2023)				

Anexo B: Instrumentos

Encuesta para medir el nivel de funcionalidad, usabilidad y seguridad del sistema web

Instrucciones:

Este formulario es confidencial. Por favor, responda honestamente. Lea cada ítem cuidadosamente. Cada uno presenta cinco opciones de respuesta. Marque con una "X" la opción que corresponda a su elección.

El significado de cada número es:

1 = Muy insatisfecho (MS)

2 = Insatisfecho (S)

3 = Neutro (N)

4 = Satisfecho (I)

5 = Muy satisfecho (MI)

Dimensiones	INDICADORES / ÍTEMS	1	2	3	4	5
Seguridad	1. ¿Qué tan seguro(a) se siente al transmitir información a través de la VPN en el local?					
	2. ¿Qué tan satisfecho(a) está con las políticas de seguridad aplicadas a través de la VPN para proteger los datos transmitidos en el local?					
	3. ¿La VPN le proporciona notificaciones o alertas claras en caso de riesgos de seguridad?					
Calidad de servicio	4. ¿Qué tan satisfecho está con la velocidad de conexión de la VPN durante el uso diario?					
	5. ¿Cómo evalúa la capacidad de la VPN para manejar múltiples usuarios simultáneamente sin afectar el rendimiento?					
	6. ¿Qué tan satisfecho está con la reducción de interrupciones o caídas en la conexión al usar la VPN?					
Experiencia del colaborador	7. ¿Cómo calificaría la integración de la VPN con las herramientas necesarias para su trabajo?					
	8. ¿Qué tan cómodo se siente usando la VPN para realizar sus tareas de manera eficiente?					
	9. ¿Qué tan satisfecho está con la capacitación recibida para comprender y utilizar la VPN?					

Anexo C: Ficha de registro N° 01: Tiempo de respuesta

<table>
<tr><td colspan="5">Ficha de registro del indicador: Tiempo promedio de respuesta</td></tr>
<tr><td colspan="2">Investigador:</td><td colspan="3"></td></tr>
<tr><td colspan="2">Tiempo</td><td colspan="2">PRETEST</td><td>POSTEST</td></tr>
<tr><td colspan="2">Empresa:</td><td colspan="3">Empresa de loterías y apuestas deportivas</td></tr>
<tr><td colspan="2">Formula</td><td colspan="3">$TPC = \frac{\sum_i^n TRi}{n}$
Donde:
TRi: Tiempo de respuesta registrado para cada prueba
N: Número total de pruebas</td></tr>
<tr><td rowspan="2">N°</td><td rowspan="2">Fecha</td><td colspan="2">Rango de tiempo</td><td rowspan="2">Tiempo de Respuesta</td></tr>
<tr><td>Tiempo de inicio (minuto)</td><td>Tiempo final (minuto)</td></tr>
<tr><td>1</td><td></td><td></td><td></td><td></td></tr>
<tr><td>2</td><td></td><td></td><td></td><td></td></tr>
<tr><td>3</td><td></td><td></td><td></td><td></td></tr>
<tr><td>4</td><td></td><td></td><td></td><td></td></tr>
<tr><td>5</td><td></td><td></td><td></td><td></td></tr>
<tr><td>6</td><td></td><td></td><td></td><td></td></tr>
<tr><td>7</td><td></td><td></td><td></td><td></td></tr>
<tr><td>8</td><td></td><td></td><td></td><td></td></tr>
<tr><td>9</td><td></td><td></td><td></td><td></td></tr>
<tr><td>10</td><td></td><td></td><td></td><td></td></tr>
<tr><td>11</td><td></td><td></td><td></td><td></td></tr>
<tr><td>12</td><td></td><td></td><td></td><td></td></tr>
<tr><td>13</td><td></td><td></td><td></td><td></td></tr>
<tr><td>14</td><td></td><td></td><td></td><td></td></tr>
<tr><td>15</td><td></td><td></td><td></td><td></td></tr>
<tr><td>16</td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="4">Promedio</td><td></td></tr>
</table>