UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

TÍTULO

ANÁLISIS DE LA INFRAESTRUCTURA DE RED Y SIMULACIÓN DE DATOS EN PYTHON PARA LA ADMINISTRACIÓN DE LA TERMINAL TERRESTRE DEL CANTÓN BABA

AUTORA

Baños Galeas, Tania Yadira

TRABAJO DE TITULACIÓN

Previo a la obtención del grado académico en
MAGÍSTER EN TELECOMUNICACIONES

TUTOR

Llerena Guevara, Lucrecia Alejandrina

Santa Elena, Ecuador

Año 2025

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

TRIBUNAL DE SUSTENTACIÓN

Firmado electrónicamente por: ALICIA GERMANIA ANDRADE VERA. Validar únicamente con FirmaEC

Ing. Alicia Andrade Vera, Mgtr.
COORDINADORA DEL PROGRAMA

LUCRECIA ALEJANDRINA LLERENA GUEVARA. Firmado digitalmente por LUCRECIA ALEJANDRINA LLERENA GUEVARA. Fecha: 2025.09.09 09:41:50 -05'00'

Ing. Lucrecia Llerena Guevara, Ph.D.
TUTOR

LUIS MIGUEL AMAYA FARINO. Digitally signed by LUIS MIGUEL AMAYA FARINO

Ing. Luis Amaya Farino, Mgtr.
DOCENTE
ESPECIALISTA

Firmado electrónicamente por: DANIEL ARMANDO JARAMILLO CHAMBA. Validar únicamente con FirmaEC

Ing. Daniel Jaramillo Chamba, Mgtr.
DOCENTE
ESPECIALISTA

Firmado electrónicamente por: MARIA MARGARITA RIVERA GONZALEZ. Validar únicamente con FirmaEC

Abg. María Rivera González, MSc.
SECRETARIA GENERAL
UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por TANIA YADIRA BAÑOS GALEAS, como requerimiento para la obtención del título de Magíster en Telecomunicaciones.

TUTOR

LUCRECIA ALEJANDRINA LLERENA GUEVARA

Firmado digitalmente por LUCRECIA ALEJANDRINA LLERENA GUEVARA
Fecha: 2025.09.09 09:42:07 -05'00'

Ing. Lucrecia Llerena Guevara, Ph.D.

Santa Elena, 1 de julio de 2025

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO
DECLARACIÓN DE RESPONSABILIDAD

Yo, **TANIA YADIRA BAÑOS GALEAS**

DECLARO QUE:

El trabajo de Titulación, Análisis de la Infraestructura de Red y Simulación de Datos en Python para la Administración de la Terminal Terrestre del Cantón Baba, previo a la obtención del título en Magíster en Telecomunicaciones, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Santa Elena, 1 de julio de 2025

LA AUTORA

Firmado electrónicamente por:
TANIA YADIRA BANOS GALEAS
Validar únicamente con FirmaEC

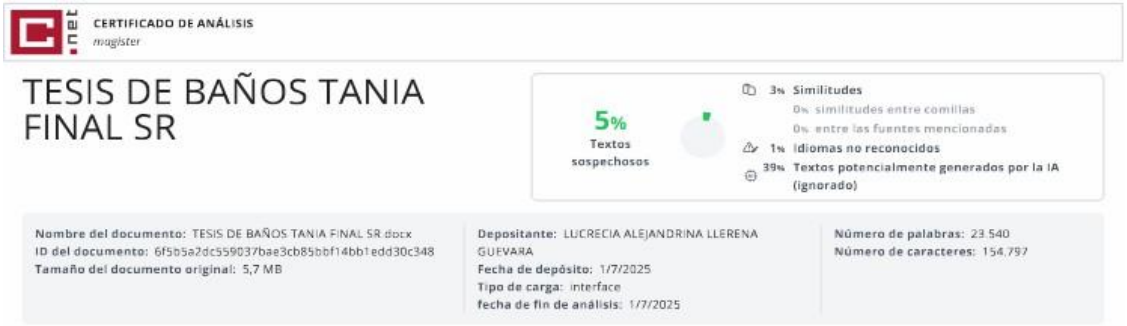
Tania Yadira Baños Galeas

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE CIENCIAS DE LA INGENIERÍA
INSTITUTO DE POSTGRADO

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado Análisis de la Infraestructura de Red y Simulación de Datos en Python para la Administración de la Terminal Terrestre del Cantón Baba, presentado por la estudiante, TANIA YADIRA BAÑOS GALEAS fue enviado al Sistema Antiplagio COMPILATIO, presentando un porcentaje de similitud correspondiente al 5%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.


CERTIFICADO DE ANÁLISIS
magister

TESIS DE BAÑOS TANIA FINAL SR

5% Textos sospechosos

3% Similitudes
0% similitudes entre comillas
0% entre las fuentes mencionadas
1% Idiomas no reconocidos
39% Textos potencialmente generados por la IA (ignorado)

Nombre del documento: TESIS DE BAÑOS TANIA FINAL SR.docx
ID del documento: 6f5b5a2dc559037bae3cb85bbf14bb1edd30c348
Tamaño del documento original: 5,7 MB

Depositante: LUCRECIA ALEJANDRINA LLERENA GUEVARA
Fecha de depósito: 1/7/2025
Tipo de carga: interface
fecha de fin de análisis: 1/7/2025

Número de palabras: 23.540
Número de caracteres: 154.797

TUTOR

LUCRECIA ALEJANDRINA LLERENA GUEVARA

Firmado digitalmente por LUCRECIA ALEJANDRINA LLERENA GUEVARA
Fecha: 2025.09.09 09:42:18 -05'00'

Ing. Lucrecia Llerena Guevara, Ph.D.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO
AUTORIZACIÓN

Yo, **TANIA YADIRA BAÑOS GALEAS**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales de proyecto de titulación con componentes de investigación aplicada y/o de desarrollo con fines de difusión pública, además apruebo la reproducción de este proyecto de titulación con componentes de investigación aplicada y/o de desarrollo dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor.

Santa Elena, 1 de julio de 2025

LA AUTORA

Firmado electrónicamente por:
TANIA YADIRA BANOS GALEAS
Validar únicamente con FirmaEC

Tania Yadira Baños Galeas

AGRADECIMIENTO

En primer lugar, quiero expresar mi más sincero agradecimiento a mis padres. Su amor incondicional, apoyo constante y paciencia infinita han sido el pilar fundamental en mi vida y en mi trayectoria académica. A mi tutora, que ha sido una guía invaluable en este proceso, le agradezco profundamente por su compromiso, dedicación y por compartir su conocimiento con generosidad. Su orientación y motivación fueron claves para superar los desafíos y avanzar con confianza en cada etapa del trabajo.

A ellos, les debo gran parte de este éxito y estoy profundamente agradecida por su amor y apoyo.

Tania Yadira, Baños Galeas

DEDICATORIA

Dedico este trabajo a las personas más importantes en mi vida.

A mis padres, que han sido mi mayor apoyo y guía en este proceso. Este logro es un reflejo de todo lo que me han dado y enseñado.

Y a mi querido Javier, cuyo aliento han sido una fuente constante de inspiración. A todos ellos gracias por tu paciencia, por las conversaciones que me han hecho ver las cosas desde nuevas perspectivas.

Tania Yadira, Baños Galeas

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

Con el objetivo de optimizar el rendimiento y la estructura de red, este proyecto analiza la infraestructura tecnológica de la Terminal Terrestre de Baba. Se desarrolla un modelo de simulación en Python para observar el comportamiento del tráfico de red en un entorno virtual. La red es evaluada mediante herramientas como Wireshark y NetData, y se considera la información de direcciones IP y topología para modelar escenarios en Cisco Packet Tracer. La simulación permite analizar el tráfico bajo diversas condiciones. Además, se implementan dos Puntos de Acceso (AP) que amplían la cobertura y mejoran la conectividad. Se aplicó un enfoque cuantitativo con encuestas a funcionarios de la Terminal. Durante el análisis, se utilizaron datos capturados con Wireshark y bibliotecas de Python como tkinter y pyshark. Como resultado, se valida la implementación de un modelo de administración centralizada basado en roles (RBAC), que fortalece la trazabilidad, seguridad y eficiencia operativa de la red.

Palabras claves: Seguridad en la Red, Herramientas de Análisis, Infraestructura de red, Wireshark, control de acceso basado en roles (RBAC), análisis de tráfico.

ABSTRACT

With the goal of optimizing network performance and structure, this project analyzes the technological infrastructure of the Baba Land Terminal. A simulation model is developed in Python to observe network traffic behavior in a virtual environment. The network is evaluated using tools such as Wireshark and NetData, and IP address and topology information is used to model scenarios in Cisco Packet Tracer. The simulation allows traffic to be analyzed under various conditions. Two Access Points (APs) are also deployed to expand coverage and improve connectivity. A quantitative approach was applied, with surveys of terminal staff. Data captured with Wireshark and Python libraries such as tkinter and pyshark were used during the analysis. The result is a validated implementation of a role-based centralized administration (RBAC) model, which strengthens network traceability, security, and operational efficiency.

Keywords: Network Security, Analysis Tools, Network Infrastructure, Wireshark, role-based access control (RBAC), traffic analysis.

INTRODUCCIÓN

En el contexto actual, con la llegada de la era digital, las organizaciones experimentan un constante crecimiento tecnológico. La transformación digital impacta directamente en la sociedad y en la economía global, lo que impulsa la necesidad de contar con infraestructuras de red más robustas y seguras.

La conectividad global, permite a las personas que tengan una experiencia segura, satisfactoria, enriquecedora, productiva y asequible. (ITU, 2022). Sin embargo, un estudio realizado por la Unión Internacional de Telecomunicaciones revela que el potencial que ofrece Internet para el bien social y económico sigue estando muy desaprovechado: la tercera parte de la humanidad (2.900 millones de personas) carece de acceso a Internet y muchos usuarios solo gozan de la conectividad de base. La conectividad con el internet ofrece varios beneficios económicos y sociales, en cuanto a la mejora y bienestar de las personas, posibilita nuevas formas de comunicación, expresión y colaboración para la organización (ITU, 2022).

En un estudio realizado en el Ecuador, se identificó que el desarrollo exponencial de las nuevas tecnologías de la información ha creado un cambio importante en el avance y promoción de oportunidades en los países, ocasionando transformaciones importantes en el sector de las telecomunicaciones, y como consecuencia, es uno de los sectores con mayor influencia dentro de las actividades económicas, sociales y de desarrollo de una nación.

La infraestructura de red en Ecuador ha experimentado incrementos durante los últimos años, denominándose como "Ecuador Digital", impulsada por el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL). Esta infraestructura incluye elementos como la fibra óptica, estaciones base móviles, redes inalámbricas, centros de datos, y redes troncales, esenciales para la prestación de servicios de voz, datos e internet (Arcotel, 2025).

En el Ecuador se ha logrado ampliar una red de fibra óptica nacional mediante el incremento de empresas públicas y privadas. El país cuenta con más de 50.000 km de red de fibra óptica instalada alrededor del mismo en varias zonas ya sean urbanas y rurales. Además, la ARCOTEL (Agencia de Regulación y Control de las Telecomunicaciones) regula y realiza una constante supervisión de la instalación de infraestructura pasiva (torres, postes, ductos)

por parte de operadores privados, lo que ha dinamizado el acceso compartido a infraestructura. (Arcotel, 2025).

En la Terminal Terrestre del Cantón Baba, dependiente del GAD Municipal, se han identificado dificultades relacionadas con la administración de la red existente. A pesar de contar con una segmentación mediante VLANs, no se dispone de monitoreo en tiempo real, lo que dificulta la detección temprana de fallos. Además, el crecimiento de dispositivos conectados ha generado puntos de saturación que afectan el rendimiento en horas de alta demanda, según observaciones técnicas realizadas en el área de sistemas durante el primer trimestre de 2025. En este escenario, la supervisión constante de redes resulta fundamental para asegurar un funcionamiento eficiente y una protección continua, especialmente en espacios de alta demanda como es la Terminal Terrestre del Cantón Baba, donde la conectividad es clave para el desarrollo de las actividades diarias de usuarios y funcionarios.

En este sentido, se defiende la tesis de que la implementación de herramientas libres como Python, Wireshark y NetData, combinadas con modelos de control de acceso basados en roles (RBAC), permite optimizar la eficiencia operativa y la seguridad de redes institucionales, especialmente en entornos públicos con recursos limitados. Wireshark es una herramienta especializada en el análisis de protocolos de red, que permite capturar y examinar en tiempo real el tráfico que circula por una red. Su principal utilidad radica en la inspección detallada de los paquetes de datos, lo cual proporciona una visión precisa de cómo se comunican los distintos dispositivos conectados. Una vez capturados, los paquetes pueden ser analizados en profundidad, identificando protocolos como TCP, UDP, HTTP, DNS, ICMP, entre otros. Estas capacidades resultan esenciales para el análisis del comportamiento de la red en entornos como la Terminal Terrestre del Cantón Baba, donde se requiere una supervisión precisa y continua del tráfico.

En este contexto, el presente trabajo de investigación tiene como objetivo diseñar un modelo de simulación en Python que permita analizar el comportamiento del tráfico para optimizar la eficiencia de la red en la Terminal Terrestre del Cantón Baba. El estudio pretende realizar el diseño de un modelo de simulación en Python que permita el análisis del comportamiento del tráfico para optimizar la eficiencia de la red. El desarrollo del estudio incluye la simulación del escenario de la Terminal Terrestre, para identificar los fallos en la red, el comportamiento del tráfico de datos bajo diferentes condiciones operativas. Asimismo, se

utilizarán herramientas especializadas para el monitoreo en tiempo real, a fin de detectar cuellos de botella, latencia irregular y fallos de conectividad.

Una de las necesidades prioritarias en la Terminal Terrestre del Cantón Baba es realizar un análisis técnico de la infraestructura de red ya implementada, con el propósito de identificar oportunidades de mejora que permitan optimizar su rendimiento, seguridad y capacidad de gestión. Aunque la red se encuentra segmentada mediante VLANs distribuidas por áreas, se lleva a cabo una revisión detallada mediante herramientas de monitoreo en tiempo real, como NetData o Wireshark, con el fin de identificar cuellos de botella, latencia irregular y fallos de conectividad.

Este estudio tiene un alcance limitado al análisis y simulación técnica de la red de la Terminal Terrestre del Cantón Baba durante el primer semestre del año 2025, sin intervención directa sobre la infraestructura física operativa.

A partir de los datos obtenidos, se desarrolla la simulación mediante el uso de las herramientas y bibliotecas de Python para modelar y comprender el comportamiento de la red bajo diferentes condiciones operativas. Además, se diseña una infraestructura optimizada utilizando el simulador de Cisco Packet Tracer, lo que permite visualizar posibles mejoras en la conectividad interna de la terminal.

Como complemento, se propone la implementación de una administración centralizada de los equipos de conexión a internet mediante el diseño de políticas de Control de Acceso Basado en Roles (RBAC), empleando puntos de acceso y plataformas como Ruijie Cloud, para asegurar una gestión remota eficiente y un acceso controlado a la red.

El presente estudio se realiza con el fin de aportar un modelo replicable en otras instituciones públicas con problemáticas similares, ofreciendo una solución técnica viable que optimice la conectividad, reduzca vulnerabilidades y fortalezca la gobernanza digital en el sector público.

Estas acciones buscan fortalecer la infraestructura tecnológica existente, garantizando un entorno de red más robusto, eficiente y alineado con las necesidades actuales de la Terminal Terrestre del Cantón Baba.

El presente trabajo de titulación tiene la siguiente estructura, en el Capítulo 1 se presenta el Marco Teórico Referencial con el estado del arte y la descripción teórica sobre el análisis mediante herramientas para el tráfico de red.

En el Capítulo 2 se expone la metodología aplicada en el desarrollo del estudio, donde se define el enfoque del trabajo, se seleccionan los métodos de investigación adecuados y se implementan técnicas específicas para analizar de manera precisa la infraestructura de red existente.

En el capítulo 3, se presenta los resultados de la ejecución mediante el uso de las herramientas para el análisis de la infraestructura de red como son Wireshark, NetData y Python. Además, se presenta los resultados del desarrollo del programa en el lenguaje de programación Python mediante el uso de herramientas y librerías como: tkinter, threading, psutil, matplotlib.pyplot, pyshark, collections, Scapy, SimPy o NS-3. Este desarrollo se organiza en tres secciones: En la primera sección se evidencia la subida de datos mediante un gráfico de monitoreo de tráfico de red, el cual permite visualizar de manera detallada el comportamiento del flujo de información saliente desde el dispositivo o sistema analizado hacia la red. Este gráfico muestra en tiempo real la cantidad de datos transmitidos, permitiendo identificar patrones de uso, picos de actividad, y posibles anomalías.

En la segunda sección se muestra el uso de una herramienta de monitoreo que, mediante Wireshark, permite capturar y observar el tráfico que circula por la red de la Terminal. Esta herramienta ayuda a ver en detalle qué tipo de información se está enviando y recibiendo, así como los protocolos que se están utilizando, como TCP, UDP, HTTP o DNS. En la tercera sección se muestra la simulación de la topología de red mediante una aplicación gráfica desarrollada en Python, la cual permite representar de forma visual y dinámica los distintos dispositivos y conexiones que componen la infraestructura de red. Esta simulación no solo facilita la comprensión de la estructura general de la red, sino que también permite observar cómo interactúan entre sí los nodos, tales como routers, switches, servidores y estaciones de trabajo.

Del mismo modo, se llevó a cabo el diseño de la topología de red utilizando el simulador Cisco Packet Tracer, una herramienta que permite representar visualmente la estructura de la red y simular su funcionamiento. Con esta simulación, fue posible comprobar la

conectividad entre los distintos dispositivos, verificar la correcta configuración de los protocolos de red e implementar la segmentación mediante VLANs.

1.1 Planteamiento de la investigación

La Terminal Terrestre del Cantón Baba, desempeña un papel fundamental en la conectividad y movilidad de los usuarios que hacen uso del lugar, lo que exige una infraestructura de red estable, segura y bien administrada para los departamentos alojados en su interior. Sin embargo, según reportes técnicos internos del GAD de Baba (Informe técnico interno TICS-IT-GADMCB-2025, y observaciones de campo realizadas en mayo de 2025), se han identificado limitaciones significativas en la supervisión en tiempo real del tráfico de red, la visibilidad del estado de los equipos y la segmentación adecuada de accesos para usuarios y dispositivos conectados. Estas deficiencias dificultan el control eficiente del entorno digital, incrementando el riesgo de fallos en el servicio, accesos no autorizados y pérdida de visibilidad sobre el rendimiento de la red.

Frente a este contexto problemático, surge la necesidad de desarrollar un modelo de simulación de red utilizando Python y herramientas de análisis open source, que permita replicar el entorno actual de la Terminal, observar el comportamiento del tráfico bajo diferentes condiciones y evaluar medidas correctivas sin intervenir la red operativa.

Así mismo, se realiza un análisis del tráfico de la red utilizando herramientas como Wireshark y NetData, con el objetivo de identificar cuellos de botella, comportamientos anómalos y niveles de uso del ancho de banda en los distintos puntos de la infraestructura. Mientras Wireshark permite la captura y análisis detallado de paquetes de datos en tiempo real, NetData ofrece una visión centralizada del estado y rendimiento de los dispositivos, habilitando una supervisión continua.

También se diseña la infraestructura de red actual y su propuesta de mejora mediante un simulador, el cual posibilita replicar el entorno de la Terminal Terrestre del Cantón Baba para validar configuraciones de switches, optimizar el acceso inalámbrico (AP), y aplicar políticas de seguridad antes de su implementación. Además, se implementa un esquema de conexión estructurada de equipos a Internet bajo control y seguridad, estableciendo políticas de acceso basadas en roles que definan los permisos y restricciones según el tipo de usuario o dispositivo conectado. Esto contribuirá a una administración más eficiente de los recursos de red, mayor trazabilidad del tráfico y mitigación de riesgos por accesos no autorizados.

De este modo, se justifica la realización de esta investigación como una necesidad institucional prioritaria, con impacto directo en la eficiencia de los procesos administrativos, la seguridad digital y la calidad del servicio público. Asimismo, el estudio representa una contribución significativa al campo profesional de las telecomunicaciones, al demostrar la aplicabilidad de herramientas libres en entornos reales de gestión pública.

1.2 Justificación

El entorno tecnológico de la Terminal Terrestre del Cantón Baba presenta limitaciones críticas en cuanto a la supervisión, administración y seguridad de su red de datos, lo cual pone en riesgo la continuidad del servicio, la integridad de la información y la eficiencia operativa de los departamentos que funcionan en su interior. En un contexto donde la infraestructura digital se ha convertido en la parte fundamental resulta conveniente contar con el uso de herramientas que permitan evaluar, optimizar y asegurar el desempeño de las redes.

La elección de Python, con sus herramientas y bibliotecas para el desarrollo de un modelo de simulación de red responde a la necesidad institucional de contar con soluciones accesibles, versátiles y adaptables a entornos reales sin incurrir en altos costos. Estas herramientas permiten la replicación del entorno actual, el análisis de tráfico en escenarios controlados, y la validación de políticas de seguridad antes de su implementación, lo que permite minimizar riesgos operativos.

Además, la aplicación de herramientas como Wireshark y NetData complementa el estudio al ofrecer datos reales sobre el comportamiento del tráfico y el estado de los equipos, permitiendo así contrastar la simulación con la realidad. Esta aproximación integral no solo optimiza la toma de decisiones técnicas, sino que también fortalece la trazabilidad, la administración por roles y la proyección de mejoras a nivel de infraestructura y gobernanza digital.

Por tanto, esta investigación no solo atiende una necesidad técnica, sino que contribuye al fortalecimiento de la Terminal Terrestre y a la modernización de los servicios públicos para el beneficio de los usuarios, sirviendo además como referente para otras entidades del sector público que enfrentan problemáticas similares en la gestión de sus redes informáticas.

Se espera que la implementación de este modelo de simulación y análisis de red tenga un impacto significativo en cuanto a la calidad del servicio, al garantizar una conectividad más estable y eficiente para los usuarios internos y externos de la Terminal Terrestre. Asimismo, el fortalecimiento de las políticas de seguridad reducirá la exposición a amenazas cibernéticas y mejorará la protección de los datos institucionales.

1.3 Formulación del problema de investigación

El problema científico que se aborda en esta investigación es la ausencia de herramientas especializadas que permitan realizar un análisis exhaustivo y una gestión eficiente del tráfico de red en la Terminal Terrestre del Cantón Baba. Esta deficiencia limita la capacidad para identificar vulnerabilidades, optimizar el rendimiento de la red y mantener una administración proactiva de los dispositivos conectados.

Se propone el desarrollo de un entorno de simulación que permita emular la infraestructura actual y evaluar su comportamiento bajo diferentes escenarios de carga y configuración. Esto facilitará la validación de políticas de seguridad basadas en roles y la optimización de los recursos de red.

El uso de herramientas como Wireshark y NetData complementará el proceso de simulación, permitiendo realizar un análisis detallado del tráfico, identificar anomalías, evaluar la eficiencia de las configuraciones implementadas y anticipar posibles fallos en la conectividad.

En consecuencia, la investigación se centra en resolver el siguiente desafío técnico: ¿Cómo puede fortalecerse y optimizarse la infraestructura de red de la Terminal Terrestre del Cantón Baba mediante la aplicación de análisis avanzados, entornos de simulación y un modelo centralizado de administración de dispositivos conectados a Internet?

1.4 Objetivo General:

Diseñar un modelo de simulación en Python mediante el análisis del comportamiento del tráfico para optimizar la eficiencia de la red en la Terminal Terrestre del Cantón Baba.

Objetivos Específicos:

1. Analizar la infraestructura de red en la Terminal Terrestre mediante herramientas de monitoreo en tiempo real para identificar cuellos de botella, latencia irregular y fallos de conectividad.

2. Desarrollar simulaciones de red mediante el uso de herramientas y bibliotecas de Python para gestionar la información obtenida en la infraestructura de red de la Terminal Terrestre del Cantón Baba.
3. Diseñar una infraestructura de red mediante el uso de un simulador de red para optimizar la conexión dentro de la Terminal Terrestre del Cantón Baba.
4. Implementar una administración centralizada de equipos de conexión a internet mediante el diseño de políticas de Control de Acceso Basado en Roles con el fin de optimizar la gestión remota segura y el acceso controlado.

1.5 Planteamiento hipotético: Preguntas Científicas

¿Cómo influye la integración de herramientas de análisis de tráfico en la identificación de vulnerabilidades dentro de la infraestructura de red?

¿De qué manera la simulación de topologías de red contribuye a la validación de configuraciones y políticas de seguridad antes de su implementación en un entorno real?

¿Qué impacto tiene la administración centralizada de dispositivos en la eficiencia operativa y en la continuidad del servicio de la red?

¿Cuáles son los beneficios de implementar políticas de acceso basadas en roles en la mejora de la seguridad de la red?

CAPÍTULO 1. MARCO TEÓRICO REFERENCIAL

1.1. Revisión de literatura

Esta sección presenta estudios previos relacionados con el análisis de redes, simulación de tráfico, monitoreo con herramientas digitales y administración centralizada. Se revisan artículos científicos y tesis recientes que abordan metodologías similares. El objetivo es identificar enfoques relevantes, comparar resultados y sustentar técnicamente la propuesta del presente trabajo. La revisión permite reconocer vacíos existentes y fortalecer el enfoque investigativo.

Según los autores (Opeyemi, Oluwatobi, Blessing, & Joseph, 2020), el problema de obtener una vista unificada de la red, la administración y la configuración flexible de los dispositivos para las Redes definidas por software, se resuelve fusionando la administración centralizada lógica de la red con la programabilidad de esta, mediante la separación del plano de datos y el plano de control. En este sentido, aunque la propuesta de separación de planos aporta una solución efectiva frente a las limitaciones de las redes tradicionales, se requiere una evaluación más amplia que integre diversas perspectivas, para comprender plenamente sus implicaciones en términos de rendimiento.

Los autores (Pratik & Tshering, 2023), establecen que, en el entorno digital actual, los temas de seguridad de la red han adquirido una importancia crucial debido a su rápida y constante evolución. El aumento progresivo de ciberataques pone en riesgo la disponibilidad y seguridad de las redes, especialmente si no se realiza un análisis continuo ni se implementan contramedidas adecuadas. El protocolo DHCP (Protocolo de Configuración Dinámica de Host), es fundamental para la comunicación en red, asigna direcciones IP y otros parámetros esenciales a los dispositivos. Dado su rol crítico, es indispensable comprender cómo se llevan a cabo los ataques dirigidos a este protocolo e implementar estrategias efectivas de protección. De esta manera, se podrán tomar las medidas necesarias para prevenir ataques y garantizar una gestión segura y continua de la red. Los autores subrayan que las medidas propuestas deben implementarse en todas las empresas y organizaciones que utilicen redes internas, a fin de minimizar el riesgo de ataques relacionados con DHCP. Concluyen que la protección del protocolo DHCP no puede ser vista como un aspecto opcional, sino como un componente estratégico dentro de cualquier política de ciberseguridad moderna. La implementación de mecanismos de defensa sólidos y la concienciación sobre su importancia

permitirá a las organizaciones no solo minimizar el riesgo de ataques dirigidos a este protocolo, sino también fortalecer el ecosistema general de seguridad de la red. Así, se asegura una gestión continua, confiable y resiliente de la infraestructura digital, capaz de responder de manera efectiva ante amenazas emergentes.

Según los autores (Alex, Ryan, Brian, & John, 2020), el análisis de paquetes es una técnica fundamental en la investigación forense de redes. También conocido como rastreo de paquetes o análisis de protocolos, consiste en capturar e interpretar datos en tiempo real mientras fluyen a través de una red, proporcionando una visión detallada de las actividades que ocurren en ella. Esta metodología es clave para detectar comportamientos maliciosos en línea, como violaciones de datos, accesos no autorizados a sitios web, infecciones por malware e intentos de intrusión. Además, permite la reconstrucción de archivos enviados a través de la red, como imágenes, documentos y correos electrónicos con archivos adjuntos. Concluyen que el análisis de paquetes no solo es una herramienta técnica útil, sino que se erige como un componente crítico en la defensa y auditoría de la seguridad de las redes. Su aplicación sistemática permite a los profesionales de ciberseguridad y a los investigadores forenses identificar incidentes en tiempo real, mitigar daños, y recopilar pruebas clave para esclarecer eventos maliciosos. En consecuencia, su dominio y uso efectivo son indispensables para cualquier organización que busque mantener una postura de seguridad proactiva y una capacidad de respuesta rápida ante amenazas digitales.

Según el autor (Chiquito A. J., 2025), en Guayaquil, la transformación digital es apoyada por iniciativas locales como el Clúster de Transformación Digital, impulsado por ÉPICO y otras entidades gubernamentales. A través de la recopilación de información de datos de sus portales web, este clúster reúne a más de 230 empresas y busca fomentar el desarrollo y la innovación tecnológica en la región. Reconocido como uno de los cinco clústeres prioritarios del país, el clúster ha recibido fondos y apoyo estratégico para facilitar la migración hacia tecnologías como SD-WAN y fortalecer la infraestructura tecnológica local. Esto no solo mejora la conectividad y la eficiencia de las empresas guayaquileñas, sino que también refuerza la economía digital, con la proyección de triplicar ingresos y duplicar exportaciones de servicios tecnológicos en los próximos años. Concluyen que el Clúster de Transformación Digital de Guayaquil representa una herramienta clave en el avance tecnológico del país, al servir como catalizador de innovación, colaboración público-privada y desarrollo económico. Gracias a su enfoque en la integración de nuevas tecnologías y la creación de

redes empresariales sólidas, se proyecta no solo una mejora significativa en la competitividad de las empresas locales, sino también un impacto directo en la economía, al triplicar los ingresos del sector tecnológico y duplicar las exportaciones de servicios digitales en los próximos años. Esto posiciona a Guayaquil como un referente nacional en transformación digital y crecimiento sostenible basado en tecnología.

Según los autores (Jiménez & Aulestia, 2024), el análisis de tráfico permite detectar patrones o actividades inusuales en tiempo real, el análisis de protocolos puede revelar debilidades específicas en torno a las reglas de comunicación, y el análisis de árbol de ataque proporciona una visión holística de las posibles secuencias de eventos adversos. El uso combinado del análisis de tráfico, de protocolos, y del árbol de ataque facilitaría, por lo tanto, un enfoque integral que aborda diversas facetas de la seguridad de la red. Estos son lo suficientemente flexibles para adaptarse a los cambios en la infraestructura de red y a las nuevas amenazas que puedan surgir a futuro, lo que es esencial en un entorno cibernético en constante evolución. Concluyen que la integración del análisis de tráfico, protocolos y árbol de ataque representa una estrategia efectiva y adaptable para fortalecer la seguridad de las redes.

El autor (Lewis Goligthtly, 2023), indica que la emulación de red implica emular un equivalente virtual de un dispositivo de producción para un dominio de aplicación específico. La virtualización se refiere a la división basada en software de un sistema físico en varios componentes. Concluyen que tanto la emulación como la virtualización son herramientas esenciales para la innovación tecnológica, que permiten experimentar, validar y optimizar soluciones sin riesgos para la infraestructura física.

Según el autor (Rodriguez José, 2022), indica que Python es excelente alternativa para el análisis de los datos, la computación exploratoria e interactiva, así como en la visualización de datos, convirtiéndolo en una alternativa sólida para las tareas de manipulación de datos. En la actualidad, la ciencia y el análisis de datos han tomado un gran auge debido en gran parte al gran aumento en la potencia de la computadora y al bajo costo de estas, así como, la presencia de grandes cantidades de datos y una mejor comprensión de las técnicas en el área de análisis de datos, inteligencia artificial, aprendizaje automático, aprendizaje profundo, etc. Por tal razón, se ha convertido en una parte esencial de la industria de la tecnología y se está utilizando para resolver muchos problemas desafiantes.

En este sentido los autores (Rodriguez José, 2022), garantizan que Python ha surgido como una solución de programación completa, debido a la baja curva de aprendizaje y la flexibilidad de Python. Además, las bibliotecas en constante evolución lo convierten en una buena opción para el análisis de datos, la investigación y el desarrollo de la ciencia de datos. Concluyen que Python se ha consolidado como una plataforma integral para el análisis de datos y el desarrollo de soluciones basadas en ciencia de datos, gracias a su accesibilidad, flexibilidad y capacidad de adaptación a los desafíos tecnológicos actuales. Su papel central en la transformación digital lo convierte en una habilidad esencial para los profesionales del área, y en una tecnología clave para impulsar la innovación y la toma de decisiones basada en datos en múltiples industrias.

Según el autor (Rodriguez José, 2022), Matplotlib es una librería especializada en la creación de gráficos 2D para Python orientado al desarrollo de aplicaciones, secuencias de comandos interactivas, generación de imágenes de alta calidad. Permite crear y personalizar los tipos de gráficos más comunes como los diagramas de barras, histogramas, diagramas de sectores, diagramas de caja y bigotes, diagramas de violín, diagramas de dispersión o puntos, entre otro. Concluyen que Matplotlib es una herramienta esencial para la visualización de datos en Python, ya que permite representar de forma clara y precisa grandes volúmenes de información. Gracias a su flexibilidad, calidad gráfica y compatibilidad con otras librerías del entorno científico de Python, se convierte en una opción poderosa para investigadores, analistas y desarrolladores que buscan comunicar de manera efectiva los resultados de sus análisis y facilitar la comprensión de los datos mediante representaciones visuales intuitivas.

Los autores, (Jiang, Zhang, Zhu, & Wang, 2025) en su análisis realizado describe que la tecnología DPI (Inspección Profunda de Paquetes), reconocida por su algoritmo simple y su rápida implementación, se destaca por su alta efectividad en la identificación de aplicaciones, logrando una precisión de hasta el 95 % en flujos HTTP. Esto la posiciona como el método más utilizado para el análisis de tráfico de red. Su funcionamiento se basa principalmente en el examen del protocolo de aplicación dentro del tráfico, observando los flujos TCP y HTTP para extraer información clave, como los campos "host" y "user-agent", que usualmente revelan las URL y nombres de las aplicaciones. En el ámbito de la ingeniería, DPI suele implementarse mediante dos enfoques: uno es la duplicación de tráfico, en la cual los datos se copian desde los dispositivos de acceso hacia servidores para su análisis; el otro es la técnica espectroscópica, que realiza una réplica de los datos a través del análisis

espectral, separándolos entre los dispositivos de acceso y el CR antes de enviarlos a los servidores para su procesamiento. Por lo cual indica que su implementación rápida y su capacidad para analizar campos como host y el usuario agente la han convertido en una herramienta común en redes modernas. Indica también que el uso conlleva a serias preocupaciones sobre la privacidad, ya que puede acceder a información sensible sin consentimiento.

En el desarrollo de este análisis sobre herramientas de monitoreo y análisis de red como Wireshark y Netdata, se ha seguido un enfoque comparable al de (Jiang, Zhang, Zhu, & Wang, 2025) respecto a la evaluación de tecnologías para la inspección y gestión del tráfico de red. De manera similar a cómo estos autores abordan la tecnología DPI, se considera tanto la capacidad técnica para identificar y analizar datos en tiempo real, como las limitaciones y desafíos asociados, incluyendo aspectos de privacidad, la influencia del cifrado en la captura de datos y posibles errores en la interpretación del tráfico. Este marco ha permitido estructurar un análisis equilibrado, que valora tanto las fortalezas como las restricciones de Wireshark y NetData en escenarios prácticos de monitoreo de redes.

Los autores (Kaya, Ozdem, & Das, 2025), mediante su investigación destaca cómo las capacidades avanzadas de recopilación y análisis de Wireshark permiten una monitorización en tiempo real, facilitando la identificación precisa de comportamientos anómalos. Además, resalta la ventaja de su interfaz intuitiva, que contribuye a una detección más ágil y accesible. Más allá del análisis convencional, los autores proponen un enfoque complementario basado en la visualización gráfica de los datos obtenidos, lo cual mejora significativamente la interpretación del estado de la red y apoya una toma de decisiones más eficiente y fundamentada. el análisis realizado en el presente trabajo también empleó Wireshark como herramienta principal para la inspección del tráfico de red, pero con un enfoque más orientado a la evaluación del rendimiento de la red, identificación de picos de latencia, pérdidas de paquetes y patrones de tráfico inusuales. Si bien ambos trabajos coinciden en la utilidad de Wireshark para la detección en tiempo real, este análisis se centró en correlacionar dichas anomalías con posibles problemas de infraestructura o configuración, más allá de su representación visual.

El autor (Luigi, 2025), indica que el Control de Acceso Basado en Roles (RBAC) es un método de control de acceso muy consolidado. En sus múltiples variaciones y adaptaciones,

se utiliza en numerosas organizaciones y sistemas. Se considera que su uso en la nube y en el Internet de las Cosas (IoT). También indican que RBAC puede utilizarse para proteger recursos de diferentes tipos. En la Terminal Terrestre de Baba, el uso de Control de Acceso Basado en Roles (RBAC) ha sido clave para gestionar de forma segura el acceso a la red inalámbrica distribuida mediante puntos de acceso (AP). La implementación de RBAC permitió establecer roles definidos para los distintos tipos de usuarios, como personal administrativo, técnicos de sistemas y usuarios invitados. Esta diferenciación facilitó el control sobre qué recursos podían acceder dependiendo del perfil asignado, fortaleciendo así la seguridad de la infraestructura inalámbrica.

En conclusión, la aplicación de RBAC en la gestión de redes inalámbricas mediante APs en la Terminal Terrestre ha sido efectiva para separar y proteger los diferentes perfiles de usuario, pero también ha dejado en evidencia la necesidad de complementar este enfoque con controles más dinámicos y contextuales que respondan a la naturaleza flexible de la conectividad inalámbrica.

1.2. Desarrollo teórico y conceptual

En esta sección se exponen los fundamentos teóricos y conceptuales que sustentan la presente investigación, abordando definiciones clave, teorías, modelos y enfoques recientes sobre redes, seguridad, simulación y administración de infraestructura. Estos conceptos permiten contextualizar el estudio y establecer las bases para el análisis, simulación y propuesta técnica planteada.

1.2.1 Infraestructura de Red

La infraestructura de red es el conjunto de elementos físicos y lógicos interconectados que conforman la base tecnológica sobre la cual operan las comunicaciones de datos de la red. En los cuales están los dispositivos de interconexión, switches, routers y puntos de acceso, entre los medios de transmisión, se encuentran los cables UTP, fibra óptica, enlaces inalámbricos y componentes de soporte como son los: servidores, firewalls, sistemas de gestión de red, software de monitoreo y control. La función principal es garantizar la disponibilidad, integridad, rendimiento y seguridad del flujo de datos entre dispositivos, permitiendo la interoperabilidad entre sistemas (Nava, 2024).

1.2.2 Componentes de una red LAN

Entre los componentes de la red local LAN se encuentran:

1.2.2.1 Red de área local o LAN

Según el autor (Nava, 2024) una red LAN, o red de área local, es un conjunto de dispositivos que se interconectan entre sí dentro de un área. Permite que computadoras, impresoras y otros dispositivos se conecten entre sí para compartir información y recursos de forma rápida. Para que todo funcione correctamente, necesita varios elementos que actúan como puentes y guías de tráfico: cables, routers, switches y programas que aseguran que los datos lleguen a su destino sin problemas ni interrupciones. Una red de área local (LAN) es una conexión interna que permite que varias computadoras y dispositivos como: impresoras, escáneres o discos duros, se comuniquen entre sí dentro de un mismo lugar.

Existen dos tipos principales de redes de área local (LAN): las redes cableadas y las redes inalámbricas (WLAN). Las redes cableadas utilizan conmutadores y cableado Ethernet para conectar dispositivos finales, servidores y equipos IoT dentro de una red corporativa. Existen dos tipos principales de redes de área local (LAN): las redes cableadas y las redes inalámbricas (WLAN). Las redes cableadas utilizan conmutadores y cableado Ethernet para conectar dispositivos finales, servidores y equipos IoT dentro de una red corporativa (Hwang, 2021).

Según el autor (Hwang, 2021). Nos dice que una red Ethernet funciona como un medio compartido, conectar demasiados dispositivos a una misma LAN puede generar un alto volumen de tráfico de difusión, el cual es recibido por todos los equipos dentro de esa red. Esta situación puede provocar congestión y cuellos de botella en la comunicación. Para reducir ese tráfico de difusión y optimizar el rendimiento, es posible segmentar la red en múltiples VLAN. De esta forma, el tráfico de difusión se limita únicamente a los dispositivos que pertenecen a la misma VLAN, evitando que se propague por toda la red. Esto disminuye significativamente la sobrecarga en la red y mejora su eficiencia general.

1.2.2.2 Beneficios de usar una LAN

El autor (Nava, 2024) indica que las redes permiten conectar varios dispositivos dentro de una misma ubicación geográfica, facilitando la comunicación interna, el acceso a recursos

compartidos y la gestión centralizada de la información, lo que contribuye a una mayor eficiencia operativa.

Entre los principales beneficios del uso de una red LAN son los siguientes:

- ✓ Acceso a aplicaciones centralizadas lo cual permiten que los usuarios utilicen aplicaciones alojadas en servidores, garantizando un control y administración centralizada.
- ✓ Almacenamiento común de información, indica que los dispositivos pueden guardar datos importantes en un lugar central, lo que facilita el acceso, respaldo y seguridad de la información.
- ✓ Ayudan al compartir recursos entre impresoras, aplicaciones, archivos y otros servicios, reduciendo la necesidad de duplicar equipos.
- ✓ Permiten el uso eficiente de la conexión a internet: Múltiples dispositivos pueden acceder a una única conexión a internet, optimizando el ancho de banda disponible.
- ✓ En cuanto a la seguridad de la red permiten incorporan herramientas de protección que ayudan a salvaguardar los dispositivos conectados, como sistemas de autenticación, control de acceso y monitoreo de tráfico (Nava, 2024).

1.2.2.3 Seguridad de la red LAN

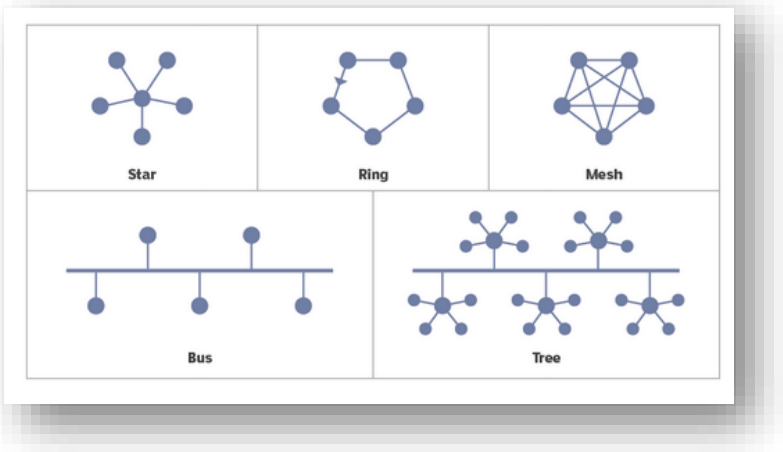
Según el análisis realizado por el autor (Hwang, 2021), indica que las soluciones de seguridad respaldadas por hardware, como el reconocimiento de huellas digitales, los dispositivos de autenticación (tokens) y el cifrado total del disco, ofrecen una capa adicional de protección para fortalecer la seguridad de la red.

Por lo que es posible incorporar paquetes de seguridad complementarios que ayudan a proteger y gestionar el perímetro de la red, ya sea mediante instalación local o a través de servicios en la nube bajo el modelo de Software como Servicio (SaaS).

1.2.2.4 Topologías LAN populares

Las topologías de red representan la forma en que se interconectan los dispositivos dentro de una red LAN y definen el recorrido que siguen los datos al transmitirse de un nodo a otro. Entre las configuraciones más comunes se encuentran las siguientes: Estrella, Anillo, Malla, Bus, Árbol (ver **Figura 1)**

Figura 1. Topología de Redes.



Fuente: (Hwang, 2021)

1.2.3 ¿Qué tipo de red es internet?

Según el (Nava, 2024), el internet es una red global compuesta por varias redes interconectadas. Cada red que forma parte de internet tiene su propio conjunto de reglas, pero utilizan protocolos comunes como el TCP/IP (Protocolo de internet) para intercambiar información. Nos da a entender una perspectiva de cómo funcionan las redes ya sean a nivel local o global.

1.2.3.1 Características de internet

Entre las características de internet se encuentran:

- ✓ El Internet está en constante crecimiento, ya que cada día se conectan más redes y dispositivos en todo el mundo.
- ✓ El Internet está formado por millones de redes independientes que colaboran entre sí.
- ✓ El uso de protocolos estandarizados, como TCP/IP, permite que estas redes, aunque sean diferentes en tecnología o ubicación, puedan comunicarse y funcionar juntas sin problemas (Nava, 2024).

1.2.3.2 Tipos de Conexiones a Internet

Existen diversos tipos de conexiones que permiten el acceso a internet, cada una con sus características particulares. Estas conexiones pueden ser cuatro (Nava, 2024):

Banda ancha: La banda ancha permite transmitir grandes cantidades de datos de manera simultánea. Existen varios tipos, tales como:

- ✓ La fibra óptica permite la conexión de los equipos de manera más rápida y eficaz, ayuda a la transmisión de datos usando luz, lo que permite una conexión muy veloz y estable, ideal para ver videos en alta calidad.
- ✓ El cable coaxial permite la conexión de equipos como lo es la televisión por cable. No es tan rápido como la fibra, sigue ofreciendo una buena conexión para navegar sin problemas.
- ✓ Un ADSL usa la línea telefónica tradicional para conectarse a internet y es más lento que la fibra o el cable, pero aún puede ser útil para tareas básicas como enviar correos, leer noticias o hacer trámites en línea.

Conexiones móviles (4G/5G): Las conexiones móviles se basan en torres de telecomunicaciones que transmiten señales inalámbricas, permitiendo el acceso a internet desde dispositivos móviles como smartphones, tablets o módems portátiles. Actualmente, la tecnología 5G representa la evolución más avanzada de estas redes móviles, ofreciendo velocidades mucho más rápidas y una latencia significativamente menor en comparación con generaciones anteriores como 3G o 4G, lo que mejora notablemente la experiencia de navegación, videollamadas, juegos en línea y aplicaciones en tiempo real (Nava, 2024).

Conexiones satelitales: Las conexiones por satélites son utilizadas en áreas rurales donde otras tecnologías no están disponibles.

Conexión Wi-Fi: Las conexiones Wi-Fi hacen referencia a redes locales que brindan acceso inalámbrico a internet dentro de un área limitada. Dispositivos como los routers de banda ancha en hogares y oficinas generan redes Wi-Fi para conectar múltiples equipos de forma simultánea.

1.2.3.3 Conexión a Red: Funcionamiento y Componentes

Las conexiones de red operan gracias a la integración de hardware y software que facilitan la transmisión de datos. Entre estos componentes se incluyen:

- ✓ **Routers y switches:** Un router conecta redes diferentes, estableciendo conexión en un lugar determinado, mientras que un switch interconecta varios dispositivos dentro de la misma red.

- ✓ **Medios de transmisión:** La información puede ser transmitida mediante diversos tipos de canales, tales como cables de cobre (Ethernet), fibra óptica o a través de señales inalámbricas como Wi-Fi y Bluetooth.
- ✓ **Protocolos de red:** Los protocolos de red, como TCP/IP, definen las normas que regulan el envío y la recepción de datos, garantizando que la información llegue correctamente y sin errores a su destino (Nava, 2024).

1.2.3.4 Redes Conectadas: Interconexión y Colaboración

Las redes conectadas son aquellas que están interrelacionadas para posibilitar la comunicación y cooperación entre diferentes dispositivos y sistemas. En el ámbito empresarial, esto permite que oficinas, equipos y plataformas diversas colaboren eficazmente, independientemente de dónde se encuentren físicamente. A continuación, se detallan:

1.2.3.4.1 Beneficios de las redes conectadas:

Entre los beneficios de las redes conectadas se describen tres:

- ✓ Posibilitan el uso compartido de recursos como archivos, impresoras y servidores.
- ✓ Favorecen la colaboración entre equipos que trabajan desde diferentes ubicaciones.
- ✓ Reducen los costos de infraestructura al permitir que múltiples dispositivos utilicen una misma red.

1.2.3.4.2 Tipos de Conexiones de Red: Físicas y Lógicas

Las conexiones de red se dividen principalmente en dos tipos: físicas y lógicas. Las conexiones físicas son los medios tangibles en los cuales se transmite la información. Entre los más comunes se encuentran los cables Ethernet, la fibra óptica y los cables coaxiales. Entre ellas las redes privadas virtuales (VPN) y las redes locales virtuales (VLAN).

Este tipo de conexiones resulta fundamental en entornos modernos basados en la nube, ya que permite una configuración flexible, escalable y eficiente de los recursos de red sin necesidad de modificar la infraestructura física.

1.2.4 Protocolos de Red

Los protocolos de red permiten el intercambio de información a través de internet. Su funcionamiento es tan eficaz que la mayoría de los casos, los usuarios no son conscientes de

su existencia ni de los procesos que permiten la comunicación digital. Sin embargo, es importante que los profesionales de redes comprendan los protocolos, que son la base de una red eficaz (Yasar & Goss, 2025).

Los protocolos de red se clasifican en tres tipos principales: protocolos de comunicación que facilitan el intercambio de datos entre dispositivos, protocolos de administración que supervisan y controlan las operaciones de red, y protocolos de seguridad que garantizan la protección, autenticación e integridad de los datos durante la transmisión (Yasar & Goss, 2025).

Para el funcionamiento de estos protocolos se presentan dos tipos: la Interconexión de Sistemas Abiertos (OSI) y el Protocolo de Control de Transmisión/Protocolo de Internet (TCP/IP). OSI es un modelo teórico con siete capas distintas para la comunicación en red. TCP/IP es el modelo más utilizado, proporciona un marco estandarizado que facilita la comunicación entre dispositivos, garantizando un intercambio de datos eficiente, se divide en cuatro capas, las cuales son:

- ✓ **Capa de aplicación**. En la capa de aplicación interactúa directamente con los usuarios finales y les proporciona los servicios de red, como navegación web, transferencia de archivos y correo electrónico. Entre ellos se ubican los siguientes protocolos: el Sistema de Nombres de Dominio (DNS), el Protocolo de Configuración Dinámica de Host (DHCP), el Protocolo de Transferencia de Archivos (FTP), el Protocolo de Transferencia de Hipertexto (HTTP), el Protocolo Simple de Transferencia de Correo (SMTP), el Protocolo Simple de Administración de Red (SNMP), Secure Shell (SSH) y Telnet operan en esta capa (Yasar & Goss, 2025).
- ✓ **Capa de transporte.** En la capa de transporte la comunicación es proporcionada de extremo a extremo entre hosts. Los protocolos como TCP y el Protocolo de Datagramas de Usuario (UDP) operan en esta capa. Sin embargo, si bien TCP está diseñado para ser confiable, los protocolos de la capa de transporte no siempre lo son (Yasar & Goss, 2025).
- ✓ **Capa de Internet.** La capa de Internet es la encargada de enrutar los paquetes de datos desde el origen hasta el destino. Para ello, utiliza direcciones IP lógicas que permiten identificar cada dispositivo y determinar la mejor ruta disponible para la transmisión de los datos. El protocolo IP es el principal componente de esta capa (Yasar & Goss, 2025).

- ✓ **Capa de enlace.** La capa de enlace se encarga de la transmisión física de datos a través del hardware de red, mediante protocolos como Ethernet para redes cableadas o una variante del estándar 802.11 para redes inalámbricas o Wi-Fi (Yasar & Goss, 2025).

1.2.4.1 Protocolo de capa de aplicación

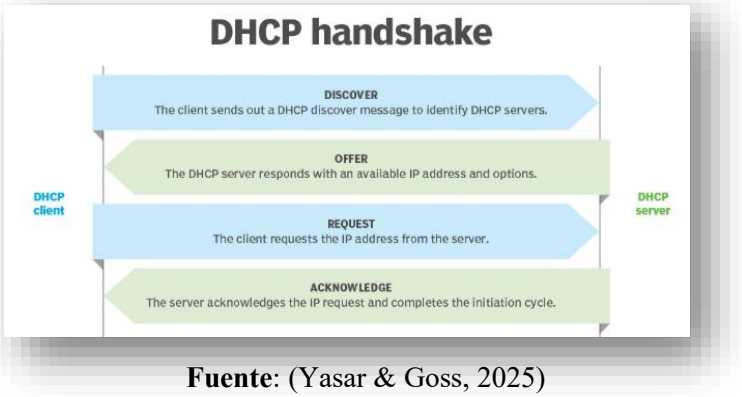
En la capa de aplicación se denota el Sistema de nombres de dominio (DNS), que es un protocolo, que actúa como el directorio telefónico de Internet, es decir que cada dispositivo en Internet tiene una dirección IP única y correspondiente, similar a un número telefónico. El DNS es un directorio de nombres de dominio completos, sus direcciones son IPv4 o IPv6 (Yasar & Goss, 2025).

1.2.4.2 Protocolo de configuración dinámica de host (DHCP)

Protocolo de Configuración Dinámica de Host (DHCP) automatiza la asignación de direcciones IP a los puntos finales de la red para que puedan comunicarse con otros dispositivos de red a través de IP. Cuando un dispositivo se conecta a una red con un servidor DHCP por primera vez, DHCP le asigna automáticamente una nueva dirección IP y continúa realizando cada vez que un dispositivo cambia de ubicación en la red. Sin DHCP, los administradores de red deben asignar manualmente direcciones IP a cada nuevo dispositivo sobre el protocolo de configuración DHCP (Yasar & Goss, 2025) (ver **Figura 2**). Cuando un dispositivo se conecta a una red, se produce un protocolo de enlace DHCP. En este proceso, el dispositivo y el servidor DHCP se comunican mediante los siguientes pasos:

- ✓ El dispositivo establece una conexión y envía una solicitud de transmisión DHCP en la LAN para encontrar un servidor DHCP que pueda asignarle una dirección IP.
- ✓ Uno o más servidores DHCP responden, ofreciendo direcciones IP disponibles.
- ✓ El dispositivo selecciona una dirección y la solicitud formalmente (Yasar & Goss, 2025).

Figura 2. Protocolo de configuración dinámica de host.



Fuente: (Yasar & Goss, 2025)

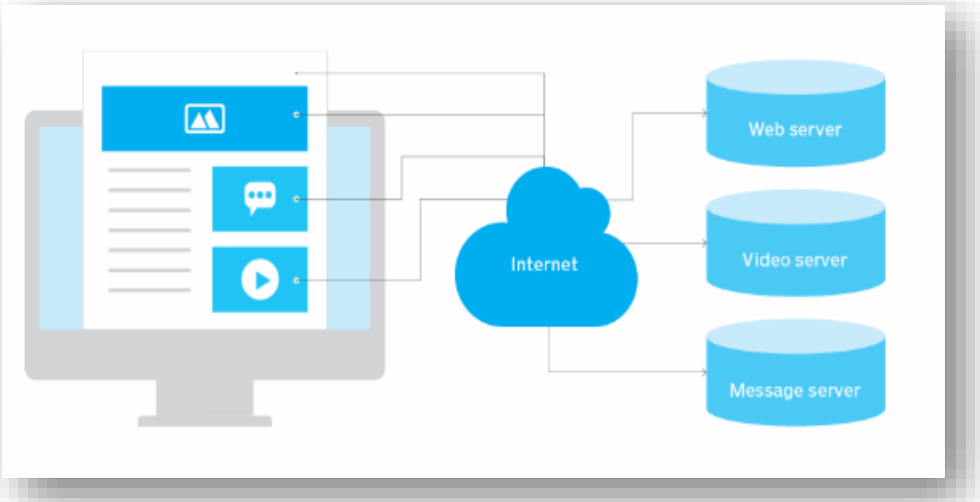
1.2.4.3 Protocolo de transferencia de archivos (FTP)

Protocolo de Transferencia de Archivos (FTP) es un protocolo cliente-servidor que transfiere archivos entre un cliente y un servidor, y opera sobre TCP/IP. Utiliza dos canales de comunicación: el canal de comandos y el canal de datos. Los clientes solicitan archivos a través del canal de comandos y reciben acceso para descargarlos, editarlos y copiarlos, entre otras acciones, a través del canal de datos (Yasar & Goss, 2025).

1.2.4.4 Protocolo de transferencia de hipertexto (HTTP)

Protocolo de transferencia de hipertexto (HTTP) opera con un modelo cliente-servidor, es el método principal mediante el cual los navegadores web y los servidores se comunican para compartir información en internet. Su propósito es transferir páginas web y proporcionar recursos durante la navegación web, también permite transferir datos, para el intercambio de archivos sobre el protocolo HTTP (Yasar & Goss, 2025)(ver **Figura 3**).

Figura 3. Protocolo de transferencia de hipertexto



Fuente: (Yasar & Goss, 2025)

1.2.4.5 Protocolo simple de transferencia de correo (SMTP)

El protocolo SMTP, también denominado protocolo de correo electrónico más utilizado forma parte del conjunto TCP/IP y controla cómo los clientes de correo electrónico envían los mensajes de los usuarios. Los servidores de correo electrónico utilizan SMTP para enviar los mensajes del cliente al servidor de correo electrónico receptor. Sin embargo, SMTP no controla cómo los clientes reciben los mensajes, sino cómo los envían. En esencia, es solo un protocolo de entrega de correo y no se utiliza para la recuperación de mensajes (Yasar & Goss, 2025). El protocolo SNMP utiliza un modelo de administrador-agente y los siguientes componentes:

- ✓ **Administrador SNMP.** Este es el sistema central que se comunica con los agentes y solicita o actualiza información.
- ✓ **Agente SNMP.** Es un componente de software que se instala en dispositivos como enrutadores y conmutadores y envía información al administrador.
- ✓ **Base de información de gestión.** La MIB funciona como base de datos y contiene información del dispositivo (Yasar & Goss, 2025).

1.2.5 Protocolos de la capa de transporte

Mediante la capa de transporte se denota el protocolo de control de transmisión o TCP, el cual es un protocolo orientado a conexión que ofrece una entrega confiable a través de secuenciación de paquetes, retransmisión de paquetes perdidos y control de flujo. TCP revisa y reensambla los paquetes en el destino antes de entregarlos a la aplicación. La tarea de IP finaliza una vez que el paquete llega al host de destino; la de TCP comienza en ese momento. Se encarga de garantizar una entrega confiable y ordenada a la aplicación (Yasar & Goss, 2025).

1.2.6 Protocolos de la capa de Internet

Protocolo de mensajes de control de Internet (ICMP) es un protocolo de soporte en la capa de internet del modelo TCP/IP. Se utiliza principalmente para diagnóstico de red, resolución de problemas, informe de errores y algunas funciones de control limitado entre dispositivos de red. Ayuda a identificar problemas de conectividad de red ya gestionar el flujo de paquetes de datos. Sin embargo, no transferir datos, como el contenido de una página web o un correo

electrónico. Los comandos ping y traceroute utilizan ICMP para probar la conectividad y rastrear rutas de paquetes. Los mensajes ICMP más comunes incluyen los siguientes:

- ✓ Solicitud de eco y respuesta de eco.
- ✓ Destino inalcanzable.
- ✓ Tiempo excedido.
- ✓ Mensaje de redirección.

1.2.7 Protocolo de Internet

El protocolo IP funciona cuando los usuarios envían y reciben datos desde sus dispositivos, estos se dividen en paquetes. Los paquetes son como cartas con dos direcciones IP: una para el remitente y otra para el destinatario. Tras salir del remitente, el paquete se dirige a una puerta de enlace o enrutador, similar a una oficina de correos, que lo guía hasta su destino. Los paquetes continúan viajando por varias puertas de enlace hasta llegar a su destinatario. IP se suele combinar con TCP para garantizar la entrega confiable de la información. Este protocolo se encarga de enviar los paquetes a sus destinos a medida que llegan, mientras que TCP se asegura de que estén en la secuencia correcta (Yasar & Goss, 2025).

1.2.8 Redes inalámbricas

En la arquitectura lógica que contiene el estándar 802.11 se conforman varios componentes, los cuales son: la estación (STA), el punto de acceso inalámbrico (AP), el conjunto independiente de servicios básicos (IBSS), el conjunto de servicios básicos (BSS), la red de distribución (DS), y el conjunto de servicios extendidos (ESS). Parte de los componentes pertenecen a los dispositivos tipo hardware tales como son: las estaciones y puntos de acceso inalámbricos (ver **Figura 4)** (SALAZAR, 2022).

Una estación (STA) es cualquier dispositivo que cuenta con una tarjeta de red inalámbrica, ya sea integrada, una tarjeta PC o un adaptador externo, que le permite conectarse a una red Wi-Fi. Entre estos dispositivos se incluyen computadoras de escritorio, portátiles, teléfonos inteligentes, tabletas, PDA u otros equipos con capacidad para comunicarse a través del medio inalámbrico.

Por su parte, el punto de acceso inalámbrico (AP) actúa como un puente entre las estaciones y la red cableada principal (red troncal), facilitando así el acceso de los dispositivos

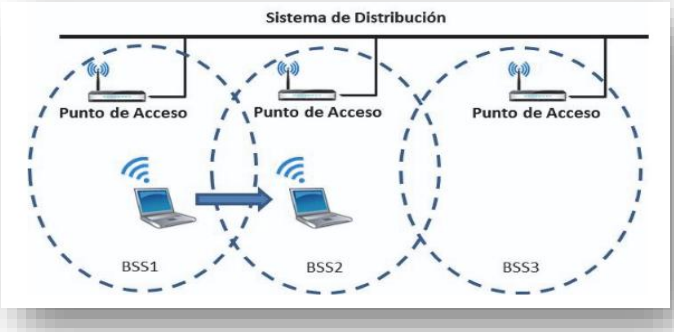
inalámbricos a los recursos de la red. Además de brindar conectividad, el punto de acceso gestiona las transmisiones, coordina el acceso al canal y puede ofrecer funciones adicionales como autenticación y control de acceso. Un punto de acceso (Access Point – AP), también conocido en algunos contextos como estación base (Base Station – BS), es un dispositivo que permite la conexión de dispositivos inalámbricos a una red cableada utilizando tecnologías Wi-Fi u otros estándares inalámbricos relacionados. Un Conjunto de Servicios Básicos (Basic Service Set – BSS) está compuesto por un punto de acceso y todas las estaciones (STA) que se encuentran asociadas a él. En este entorno, el AP actúa como controlador principal, gestionando la comunicación y coordinación entre las estaciones dentro de ese BSS. La forma más simple de un BSS incluye únicamente un AP y una estación conectada (SALAZAR, 2022).

ESS también conocido como conjunto de uno o más grupos interconectados de servicios básicos (BSS) que son percibidos como un único BSS por la capa de control de enlace lógico de cualquier estación asociada a alguno de ellos (ver **Figura 5)** (SALAZAR, 2022).

Figura 4. Conjunto de servicios básicos (BSS) e Independiente (IBSS).

Fuente: (SALAZAR, 2022)

Figura 5. Conjunto de servicios extendidos (ESS) y soporte a la movilidad.



Fuente: (SALAZAR, 2022)

1.2.8.1 Arquitecturas

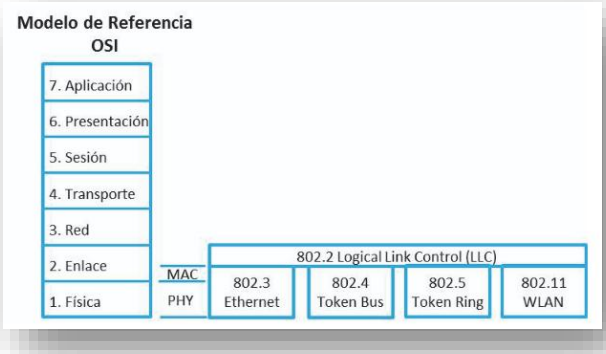
Para configurar una arquitectura de red inalámbrica mediante el modo de ad hoc e infraestructura, se debe realizar de la siguiente manera: mediante el modo de ad hoc, consisten en que los dispositivos se transmiten de punto a punto, mientras que en el modo infraestructura, varios de los dispositivos se comunican a través del punto de acceso. Mediante el modo Ad hoc los dispositivos de una red inalámbrica establecen la conexión entre sí de igual al modo de comunicación punto a punto. Por lo tanto, el rendimiento de la red se ve afectado si el número de dispositivos aumenta (SALAZAR, 2022).

La red inalámbrica en modo de infraestructura consiste en que todos los dispositivos están conectados a la misma red inalámbrica con la ayuda de un AP. Básicamente los puntos de acceso inalámbricos son los routers o switchs los cuales pasan los datos mediante la red Ethernet cableada, como puente entre la red LAN y los dispositivos inalámbricos (SALAZAR, 2022).

1.2.8.2 El estándar IEEE 802.11

Un estándar IEEE 802.11 es un conjunto de controles de acceso mediante el acceso a la MAC como a la capa física para establecer la implementación de redes inalámbricas de área local en varias bandas de frecuencias como lo son de 2,4 GHz, 5 GHz y 60 GHz. Estas especiaciones son establecidas por la IEEE 802.11, mediante este estándar se establece la conexión entre los dispositivos de redes inalámbricas (SALAZAR, 2022). En el estándar 802.11 dice que las especificaciones mediante el desarrollo de la capa física y capa de control de acceso se comunican a través de la capa de control de enlace lógico, en la **Figura 6** se muestra Las capas del modelo OSI y en la capa física el protocolo 802.2 y en la **Tabla 1** se muestra los tipos de estándares de la de la red WLAN.

Figura 6. El estándar IEEE 802.11 y el modelo de referencia OSI.



Fuente: (SALAZAR, 2022)

Tabla 1. Tipos de Estándares de la red WLAN.

Tipo de Red	Nombre	Estándar	Banda de Frecuencia	Rango nominal	Máxima velocidad de transmisión.
WLAN	**Wi-Fi**	EEE 802.11	2.4 / 5 GHz	100 m	1 Mbps
		IEEE 802.11ª	5 GHz	100 m	48 Mbps
		IEEE 802.11b	2.4 GHz	100 m	11 Mbps
		IEEE 802.11g	2.4 GHz	100 m	54 Mbps
		IEEE 802.11n	2.4 / 5 GHz	250 m	600 Mbps
		IEEE 802.11ac	5 GHz	250 m	1.3 Gbps

Fuente: (SALAZAR, 2022)

1.2.8.3 Seguridad

En cuanto a la seguridad, las redes inalámbricas no son seguras como las redes cableadas. En una red cableada, los datos se transmiten directamente entre dos puntos, por ejemplo, en un medio físico, como un cable de red, lo que limita las posibilidades de interceptación. En cambio, las redes inalámbricas envían señales a través del aire en todas direcciones, lo que permite que cualquier dispositivo dentro del rango de cobertura pueda potencialmente captar la transmisión si no se aplican medidas de seguridad adecuadas (SALAZAR, 2022).

Mientras que una red cableada puede protegerse mediante controles físicos (como el acceso restringido a los equipos) y software (como cortafuegos), las redes inalámbricas requieren mecanismos de seguridad más robustos, como autenticación fuerte, cifrado avanzado (WPA2/WPA3) y monitoreo constante, para garantizar la confidencialidad e integridad de los datos (SALAZAR, 2022).

1.2.8.3.1 Comunicaciones seguras

Las comunicaciones seguras establecen que la seguridad en las comunicaciones se constituye de varios elementos, en los cuales están: Autenticación, confidencialidad e integridad. La autenticación asegura que los nodos realmente corresponden a las identidades que afirman tener. Mediante la confidencialidad los usuarios no autorizados accedan al contenido del tráfico de red. Para lograrlo, se emplea un método de cifrado, el cual consiste en transformar el mensaje original mediante un algoritmo reversible, generando un texto cifrado que permite ocultar la información (SALAZAR, 2022).

Es decir, solo el personal que posee el conocimiento necesario puede descifrar el mensaje y acceder al contenido original. La integridad garantiza que los mensajes lleguen a su destino sin haber sido modificados. Esto implica la capacidad de verificar que el contenido recibido no ha sufrido cambios y corresponde exactamente al mensaje original enviado (SALAZAR, 2022).

1.2.8.3.2 Confidencialidad y Encriptación

La confidencialidad y encriptación se consigue protegiendo la información mediante técnicas de cifrado. Aunque el uso del cifrado en redes WLAN no es obligatorio, su ausencia permite que cualquier dispositivo compatible con el estándar y dentro del alcance de la red pueda acceder y visualizar todo el tráfico transmitido (SALAZAR, 2022). Existen tres mecanismos de cifrado utilizados para proteger la seguridad de las redes WLAN, los cuales son:

- ✓ WEP (Wired Equivalent Privacy): Privacidad Equivalente a Cableado
- ✓ WPA (Wi-Fi Protected Access): Acceso Protegido Wi-Fi
- ✓ WPA2 (Wi-Fi Protected Access, version 2): Acceso Protegido Wi-Fi, versión 2

WPA emplea claves de 256 bits, lo que representa una mejora considerable en comparación con las claves de 64 y 128 bits utilizadas en el sistema WEP.

WPA2 introdujo una mejora respecto a su predecesor, WPA, al hacer obligatorio el uso del cifrado basado en el algoritmo AES (Estándar de cifrado avanzado), lo que incrementó significativamente la seguridad de las redes inalámbricas (SALAZAR, 2022).

En la **Tabla 2, s**e visualiza la comparación entre la red LAN y WLAN**.**

1.2.8.3.3 Ventajas y desventajas de las redes inalámbricas

Las redes inalámbricas ofrecen ventajas importantes sobre las redes cableadas, entre ellas están: mayor movilidad, menor costo y mayor flexibilidad, aunque también presentan desventajas, siendo la seguridad una de las principales. A continuación, se describen varios beneficios:

- ✓ Las comunicaciones de datos permiten una transferencia de información más rápida y efectiva.
- ✓ La conectividad inalámbrica brinda mayor libertad de movimiento, permitiendo a los usuarios desplazarse dentro del área de cobertura sin perder la conexión. (Salazar, 2022).

- ✓ Los usuarios pueden acceder a la red desde cualquier punto dentro del rango de señal, facilitando el trabajo en distintos entornos o ubicaciones sin restricciones físicas.
- ✓ Las redes inalámbricas suelen ser más económicas y rápidas de instalar que las cableadas.

Tabla 2. Comparación entre la red LAN y la red WLAN.

Característica	LAN (Cableada)	WLAN (Inalámbrica)
Medio de transmisión	Cables (UTP, STP, fibra óptica)	Ondas de radio (Wi-Fi)
Movilidad	Limitada por cables	Alta movilidad
Velocidad	Generalmente más alta y estable	Puede variar según interferencias
Seguridad	Más fácil de controlar físicamente	Requiere medidas de seguridad robustas
Instalación	Más compleja y costosa	Más sencilla y flexible

Fuente: (Stacey, 2025)

1.2.9 Gestión y Seguridad de Redes

Para garantizar una gestión remota segura y un acceso controlado a los recursos tecnológicos, especialmente en entornos corporativos o institucionales, es fundamental establecer políticas sólidas de Control de Acceso Basado en Roles (RBAC). Este enfoque permite asignar permisos según las funciones específicas que desempeñan los usuarios dentro de una organización, minimizando los riesgos de accesos no autorizados y facilitando la administración de privilegios. Con el fin de diseñar adecuadamente estas políticas de RBAC, es necesario recopilar y demostrar la siguiente información clave:

1.2.9.1 Control de acceso basado en roles (RBAC)

El Control de Acceso Basado en Roles (RBAC) es un modelo de gestión de acceso que asigna permisos a roles definidos dentro de una organización, en lugar de otorgarlos directamente a usuarios individuales. Estos roles se estructuran en función del nivel de acceso para cumplir con dichas responsabilidades.

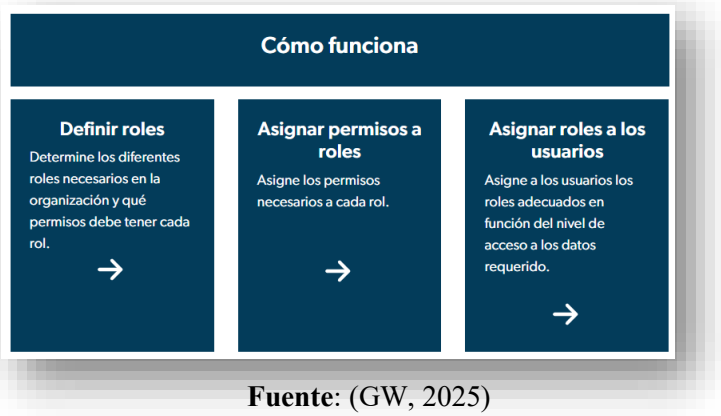
Al vincular los permisos a roles específicos, y luego asignar esos roles a los usuarios, se garantiza que cada persona solo tenga acceso a los recursos que necesita para desempeñar sus tareas. En la **Figura 7** se muestran los componentes y en la **Figura 8** se muestran las funcionalidades del RBAC (GW, 2025) . Este enfoque no solo simplifica la administración

de permisos, sino que también reduce significativamente el riesgo de accesos no autorizados a información sensible o confidencial.

Figura 7. Componentes del RBAC.

Fuente: (GW, 2025)

Figura 8. Funcionalidad de loa RBAC.



Fuente: (GW, 2025)

La habilitación del control de acceso basado en roles para un sistema de gestión de documentos puede incluir los siguientes roles y permisos:

- ✓ **Administrador**: Tiene los permisos de: crear, leer, actualizar y eliminar cualquier documento.
- ✓ **Editor**: Su permiso es de: crear y actualizar documentos, pero no puede eliminarlos.
- ✓ **Visualizador**: Solo puede leer documentos.

A continuación, se explican sobre los beneficios y usabilidad de los RBAC o control de acceso basado en roles.

1.2.9.2 Beneficios y aplicaciones de RBAC

En cuanto a los beneficios se presentan los siguientes:

- ✓ **Operaciones optimizadas.** Los RBAC, optimizan las operaciones al asignar roles en lugar de permisos individuales, lo que reduce la carga administrativa y garantiza la consistencia. También permiten agrupar a los usuarios según sus roles y otorgarles el acceso correspondiente puede garantizar operaciones más fluidas y sin errores (Herzberg, 2023).
- ✓ **Mayor cumplimiento y auditabilidad.** Los RBAC ofrecen una implementación de permisos basados en roles evidenciando el cumplimiento de las normas de protección de datos (Herzberg, 2023).
- ✓ **Escalabilidad y flexibilidad.** RBAC ofrece la escalabilidad necesaria para satisfacer estas demandas: su adaptabilidad garantiza que, a medida que cambia la estructura de una organización, su sistema de control de acceso pueda evolucionar simultáneamente (Herzberg, 2023).

1.2.9.3 Reglas principales del RBAC

El control de acceso basado en roles (RBAC) sigue tres reglas muy importantes que permiten garantizar una gestión segura y eficiente del acceso de los usuarios:

- ✓ **Asignación de roles:** Se refiere a que el usuario solo puede acceder a los recursos si se le asigna un rol específico con permisos predefinidos.
- ✓ **Autorización de roles:** Los usuarios deben estar autorizados para un rol antes de obtener acceso a los privilegios asociados (Fortinet, 2025).
- ✓ **Autorización de permisos:** los usuarios solo pueden realizar acciones dentro de su rol asignado, lo que evita el acceso no autorizado a datos o sistemas confidenciales.

1.2.9.4 Seguridad

El modelo RBAC contribuye significativamente minimizando amenazas internas al restringir los privilegios según las funciones específicas de cada usuario. Lo cual permite mejorar la seguridad del sistema y de las aplicaciones en tres áreas clave:

- ✓ Seguridad de la información
- ✓ Seguridad de los datos
- ✓ Seguridad de las aplicaciones web

Una gestión adecuada del acceso garantiza que solo el personal autorizado pueda visualizar o manipular información crítica, protegiendo así a la organización frente a accesos maliciosos, robos de datos y usos indebidos (Fortinet, 2025).

El acceso a las aplicaciones web corporativas se regula estrictamente según el rol asignado al usuario. Este control también se extiende a los portales y sitios web institucionales, mejorando la seguridad en entornos digitales expuestos públicamente (Fortinet, 2025).

1.2.10 Fundamentos del Tráfico de Red

El tráfico de red se refiere al conjunto de datos que se transmiten a través de una red informática. Este flujo de información es gestionado por diversos protocolos, entre los más comunes se encuentran TCP, UDP, HTTP y FTP.

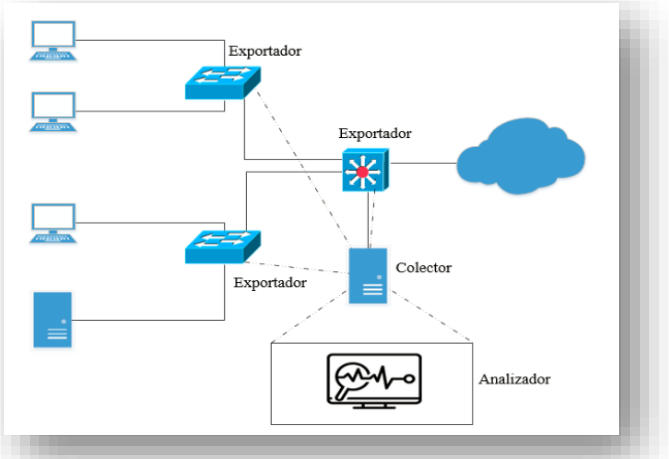
El análisis del tráfico de red consiste en monitorear y examinar estos datos con el objetivo de comprender el comportamiento general de la red, identificar patrones de uso, y detectar posibles anomalías o amenazas de seguridad. Esta práctica resulta fundamental para garantizar un rendimiento óptimo, prevenir incidentes y reforzar la seguridad de las infraestructuras tecnológicas.

1.2.10.1 Análisis de Paquetes o Captura de Paquetes

Un analizador de paquetes normalmente es referido como un protocolo de análisis, que describe el proceso de captura e interpretación de los datos en vivo que están recorriendo la red, otorgando un orden a los paquetes para entender qué está sucediendo en la red (Orlando & Alejandro, 2021).

El análisis de paquetes normalmente se realiza mediante un programa ejecutado en un dispositivo perteneciente a la red que tiene como función capturar paquetes, este dispositivo recibe pasivamente todas las tramas de la capa de enlace de datos que lleguen hasta el adaptador de red del dispositivo, sin importar que vayan dirigidos a otro dispositivo, ver esquema de análisis de flujo de Tráfico de datos (Orlando & Alejandro, 2021) (ver **Figura 9**).

Figura 9. Esquema de Análisis de Flujo de Tráfico



Fuente: (Orlando & Alejandro, 2021)

1.2.11 Equipos que contienen la red de la Terminal Terrestre de Baba

A continuación, se explica sobre los componentes que contiene la sala de equipos en la Terminal Terrestre de Baba.

1.2.11.1 Patch Panels (Paneles de parcheo) – Marca ROWEST

Los paneles de parcheo son componentes fundamentales en la organización y gestión del cableado de red dentro de un centro de datos o sala de telecomunicaciones. Su función principal es centralizar y distribuir los cables de red, facilitando la conexión entre los dispositivos de la red y los equipos de interconexión (Ingeniería, 2025).

Este equipo está compuesto por múltiples puertos que actúan como puntos de conexión. Cada puerto permite gestionar de forma ordenada las conexiones entre los cables y los equipos activos, como switches o routers.

- ✓ Estos paneles contienen organizadores que permiten ordenar y distribuir adecuadamente los cables de red.
- ✓ Se utilizan conectores RJ45, comúnmente codificados por colores (rojo, blanco, gris), para identificar diferentes segmentos o tipos de conexiones.
- ✓ Además, en la infraestructura suelen estar presentes switches de red con múltiples puertos RJ45, que permiten la interconexión y comunicación entre diversos dispositivos conectados a la red (Ingeniería, 2025).

Mediante la inspección realizada en la Terminal de Baba, se evidencia que contiene 2 switches, los cuales están ubicados en los gabinetes en la oficina administrativa y en el cuarto de equipos.

1.2.11.2 Switch Mikrotik - Cloud Router

El MikroTik Cloud Router es un dispositivo de red que integra funciones de enrutamiento y conmutación, diseñado para gestionar redes complejas con eficiencia y alto rendimiento. Este equipo combina el sistema operativo RouterOS de MikroTik con un hardware potente, lo que lo hace ideal para entornos empresariales o proveedores de servicios. El dispositivo tiene un procesador de 800 MHz y 512 MB de RAM (AthilandGroup, 2024) (ver **Figura 10**). Entre las características de los switches están:

- ✓ Switcheo de Capa 2 sin-bloqueo
- ✓ IEEE 802.1Q VLAN
- ✓ Puerto aislado
- ✓ Puerto seguro
- ✓ Broadcast storm control
- ✓ Port mirroring
- ✓ Listas de control de acceso
- ✓ Mikrotik neighbor discovery
- ✓ SNMP v1 (AthilandGroup, 2024).

Estos equipos Switch permiten gestionar el reenvío de tráfico entre puertos, aplicar filtros por direcciones MAC, configurar VLANs, duplicar el tráfico (port mirroring), limitar el ancho de banda y modificar ciertos campos de los encabezados MAC e IP. Además, la ranura SFP es compatible con módulos SFP de 1.25 Gbps y SFP+ de 10 Gb (AthilandGroup, MIKROTIK, 2024).

Figura 10. Herramienta para conexión de red - Switch Mikrotik.

Fuente: (AthilandGroup, MIKROTIK, 2024).

1.2.11.3 Router Mikrotik RB3011

El router MikroTik RB3011 es un dispositivo de alto rendimiento que ofrece una potente capacidad de procesamiento gracias a su CPU de arquitectura ARM. Este dispositivo contiene diez puertos Gigabit Ethernet divididos en dos grupos de conmutación, una jaula SFP y la inclusión de un puerto USB 3.0 de SuperSpeed. Este roouter permite una conectividad versátil y de alta velocidad. A continuación, se describen las especificaciones de los Router Mikrotik, (ver **Tabla 3**)

Tabla 3. Especificaciones de Router Mokrotik RB3011.

Código de producto	**RB3011UiAS-RM**
Arquitectura	ARM 32bit
CPU	IPQ-8064
Conteo de núcleo de CPU	2
Frecuencia nominal de CPU	1,4 GHz
Licencia RouterOS	5

Fuente: Elaborado por la autora.

1.2.10.4 Cables Ethernet de diferentes colores

Entre los cables Ethernet están los de color rojo, azul, amarillo, gris, blanco, y negro. Un conector RJ45 es un dispositivo modular ampliamente utilizado que, junto con un cable, proporciona comunicación de datos entre diversos dispositivos y sistemas electrónicos. Como otros conectores modulares, los RJ45 cuentan con contactos metálicos separados por canales de plástico aislante que encajan en el conector correspondiente. Un conector RJ45 tiene 8 pines y 8 posiciones para cables, lo que permite manejar señales o energía a través de hasta 4 pares de cables trenzados (Rodriguez, 2023).

1.2.12 Lenguaje de programación - Python

A Python se lo conoce como un lenguaje de programación de alto nivel, open source, interpretado y de propósito general que permite la programación orientada objetos. Se orienta en las aplicaciones web, desarrollo de software, la ciencia de datos y machine learning. Python cuenta con una biblioteca estándar la cual tiene códigos reutilizables que

permiten realizar cualquier otra tarea, es interactivo. Python se ejecuta en varios sistemas operativos como es Windows, Linux y Unix (Zúñiga, 2024).

1.2.12.1 Características de Python

Python cuenta con las siguientes características:

- ✓ Python ofrece una enorme biblioteca de código para la realización de las necesidades más comunes en la mayoría de las aplicaciones.
- ✓ Es un lenguaje interpretado, esto hace que su ejecución sea muy ágil, y permite una experiencia de desarrollo muy agradable.
- ✓ Python permite realizar programas de lo más diversos como aplicaciones de consola con ventanas de interfaz gráfica, aplicaciones web, servicios web, etc.
- ✓ Permite ejecutar en cualquiera de las plataformas comunes.
- ✓ Python dispone de una de las comunidades más activas, lo que es importante a la hora de encontrar soluciones a los problemas comunes y soporte (Zúñiga, 2024).

1.2.12.2 Ventajas de Python frente a otros lenguajes

En el caso de Python, algunas de las más destacables ventajas serían las siguientes:

- ✓ Python es flexible a ejecutarse en Windows y MacOS y en Linux.
- ✓ Python ofrece la posibilidad de extenderse a través de módulos que pueden crear otros desarrolladores y compartirlos en la comunidad (Zúñiga, 2024).

1.2.13 Qué es Wireshark

Wireshark es una plataforma que analiza protocolos de red, diseñado para proporcionar visibilidad del tráfico que se produce en una red o entre máquinas. Permite mirar desde el interior de la red y examinar los detalles del tráfico inalámbrico y por cable a varios niveles: desde la información a nivel de conexión hasta los bits que hacen un determinado paquete y los datos que contiene (Abba, 2023). Algunos casos de uso de Wireshark se mencionan a continuación:

- ✓ Los operadores de redes pueden utilizar Wireshark para depurar errores de conectividad y solucionar problemas.
- ✓ Permite examinar la seguridad del tráfico de red mediante el uso de herramientas, técnicas y procedimientos utilizados, para detectar amenazas (Abba, 2023).

- ✓ Permite ver los datos que atraviesan varias redes, incluidas las redes cableadas, como Ethernet, las redes inalámbricas, las redes Bluetooth.
- ✓ Navegar y ver las distintas capas incluidos los protocolos a nivel de aplicación, como HTTP/HTTPS (Abba, 2023).
- ✓ Registra y captura el tráfico para su posterior análisis.

1.2.14 NetData

Es una herramienta para visualizar y monitorear métricas en tiempo real. Netdata es un software que permite reunir los datos de rendimiento en tiempo real en los sistemas como Windows, Linux, aplicaciones y dispositivos SNMP, y los representa en una interfaz basada en web. Tiene su propio servidor web para mostrar el informe final en formato gráfico. Además, permite realizar la evaluación mediante el monitoreo y análisis en tiempo real de diversas métricas como: los tiempos de respuesta, las tasas de solicitudes y el uso de recursos, esto puede ayudar a identificar cuellos de botella que afectan el rendimiento del servidor y a optimizarlo para mejorarlo. Para identificar y resolver rápidamente problemas con sus servidores web para minimizar el tiempo de inactividad y garantizar un rendimiento óptimo.

1.2.15 Cisco Packet Tracer

Cisco Packet Tracer es un software diseñado para simular redes ampliamente utilizada en entornos educativos para la enseñanza y el aprendizaje de conceptos relacionados con redes y telecomunicaciones. Este software permite a los usuarios simular redes complejas, visualizar su funcionamiento, realizar evaluaciones interactivas y diseñar actividades prácticas.

Gracias a sus funciones colaborativas y su entorno intuitivo, Cisco Packet Tracer facilita el desarrollo de habilidades para la resolución de problemas y fomenta el aprendizaje activo en un entorno dinámico y social. A continuación, se detallan algunas de las funciones básicas más destacadas de Cisco Packet Tracer:

- ✓ Crear y configurar una red desde cero.
- ✓ Modificar y trabajar sobre proyectos existentes basados en ejemplos predefinidos.
- ✓ Evaluar nuevos diseños y topologías de redes Cisco.
- ✓ Simular cambios en la red antes de implementarlos en un entorno real.

- ✓ Analizar el flujo de datos dentro de una red.
- ✓ Realizar simulaciones relacionadas con dispositivos del Internet de las Cosas (IoT).
- ✓ Prepararse para exámenes de certificación en tecnologías de redes Cisco.

1.2.16 Access Point Wi-Fi 6 para Interiores – Ruijie RG

Se trata de un punto de acceso Wi-Fi de alto rendimiento, diseñado especialmente para ofrecer cobertura eficiente en grandes espacios interiores. Su arquitectura incluye puertos LAN duales, lo que facilita la integración con dispositivos de terceros y permite una expansión flexible de la red, adaptándose a diversos escenarios de implementación.

Este dispositivo admite comunicación de doble banda, operando simultáneamente en las frecuencias de 2,4 GHz y 5 GHz, alcanzando velocidades de hasta 574 Mbps en 2,4 GHz, 1201 Mbps en 5 GHz, y un rendimiento combinado de hasta 1775 Mbps por punto de acceso. La banda de 5 GHz, al ofrecer menor interferencia, canales más amplios y mayor velocidad, proporciona una experiencia inalámbrica más estable y fluida para los usuarios, ideal para entornos con alta densidad de dispositivos o demanda de alto ancho de banda (Ruijie, 2024).

Una red inalámbrica puede establecerse mediante múltiples puntos de acceso interconectados o a través de un único punto de acceso que funcione como router inalámbrico independiente. Teniendo en cuenta el dispositivo proporciona una configuración más flexible, una amplia gama de funciones y una mayor versatilidad en los escenarios de implementación, lo que permite adaptarse eficazmente a diferentes necesidades operativas y entornos de red (Ruijie, 2024).

CAPÍTULO 2. METODOLOGÍA

2.1 Contexto de la investigación

El cantón Baba, ubicado en la provincia de Los Ríos, se encuentra la Terminal Terrestre de Baba, cuya gestión está a cargo del Gobierno Autónomo Descentralizado Municipal del Cantón Baba. En esta terminal no solo se prestan servicios de transporte, sino que también se encuentran varios departamentos del GADMCB, así como otras entidades del estado. Se muestra el mapa geográfico obtenido de Google Maps sobre la ubicación de la Terminal, la cual se encuentra en la parte inicial de la ciudad de Baba (ver **Figura 11).**

Ante la necesidad de mejorar el rendimiento, la seguridad y la gestión de la infraestructura de red de la terminal, surge la ejecución de este proyecto. Actualmente, la red presenta deficiencias técnicas como latencia irregular, fallos frecuentes de conectividad y ausencia de un control centralizado, lo que dificulta la operación eficiente de los servicios y procesos institucionales.

Por esta razón, se plantea una intervención que incluye el análisis de la red existente, la simulación de mejoras mediante herramientas tecnológicas, el rediseño de la topología de red, y la implementación de un sistema de administración remota con control de acceso, con el fin de optimizar la conectividad, fortalecer la seguridad informática y facilitar la gestión técnica de los recursos de red.

En la **Figura 12** se muestra el mapa geográfico de la Terminal Terrestre de Baba con su ubicación física dentro del cantón, facilitando la identificación precisa del lugar en el contexto territorial.

Figura 11. Mapa Geográfico de la Terminal Terrestre.

Fuente: Elaborado por la autora usando google maps.

Figura 12. Ubicación de la Terminal Terrestre de Baba.

Fuente: Elaborado por la autora usando google maps.

2.2 Diseño y alcance de la investigación

Se optó por un diseño no experimental debido a que no se realizó manipulación, sino que se observaron y analizaron las condiciones reales de la red en su entorno natural. Este enfoque permite obtener una visión del estado actual de la infraestructura sin alterar su funcionamiento.

Además, se descartaron otros tipos de diseño, como el experimental, ya que la intervención directa sobre la red podría haber afectado negativamente su operatividad y los servicios que esta soporta. Por ello, el diseño no experimental resulta el más adecuado para realizar un diagnóstico técnico confiable sin poner en riesgo la funcionalidad de los sistemas existentes.

El alcance descriptivo fue seleccionado porque permite caracterizar detalladamente los elementos, condiciones y comportamientos observados en la infraestructura de red, lo que facilita identificar problemáticas como cuellos de botella, latencia o fallos de conectividad, sin establecer relaciones causa-efecto entre las variables.

En cuanto al alcance la Investigación es descriptiva, debido a que se está recopilando información a través de encuestas y simulaciones para describir y analizar el estado actual de la infraestructura de red, las dificultades que enfrenta, y cómo las mejoras propuestas podrían impactar en la red.

A continuación, se detalla el desarrollo de la investigación en dos fases principales (Ver **Tabla 4).**

Tabla 4. Fases de la Investigación

Fase	Actividad	Descripción Detallada
Fase Analítica	Descripción del contexto actual	Descripción del contexto actual de la infraestructura de red mediante observación directa, encuestas al personal técnico y uso de herramientas de diagnóstico (Wireshark, NetData).
	Instrumentos de medición	Utilización de herramientas de monitoreo de red (Wireshark, NetData), simulaciones en Cisco Packet Tracer y bibliotecas Python para pruebas.
	Resultados esperados	Identificación de cuellos de botella, puntos críticos de latencia y fallas de conectividad; documentación del estado actual de la red.
Fase Explicativa	Análisis de causas	Infraestructura deficiente, falta de administración centralizada.
	Variables tecnológicas	Tipo de equipos (switches, APs), ancho de banda disponible, calidad de cableado, tecnologías obsoletas o incompatibles.
	Determinación de consecuencias	Conectividad inestable, afectación al servicio a funcionarios y ciudadanos, problemas en la gestión documental y servicios digitales.
	Identificación de soluciones	Rediseño de la topología en Cisco Packet Tracer, aplicación de control de acceso con Ruijie Cloud para los Puntos de Acceso, implementación de equipos AP, políticas RBAC y simulaciones Python para predecir rendimiento.

Fuente: Elaborado por la autora.

2.3 Tipo y métodos de investigación

El tipo de investigación fue mixto, combinando enfoques cuantitativos y cualitativos. Se utilizó un método hipotético-deductivo, partiendo de hipótesis sobre las posibles soluciones y luego verificándolas a través de la recolección y análisis de datos. En cuanto a los métodos de investigación, se empleó tanto enfoques inductivos como deductivos para comprender el entorno a desarrollar.

El diseño de la investigación adoptado fue de carácter no experimental, ya que no se realizaron intervenciones directas ni manipulaciones controladas sobre las variables de estudio. Este tipo de diseño permitió observar y analizar las condiciones actuales de la red de la Terminal Terrestre del Cantón Baba sin alterar su entorno tecnológico real.

En relación con el tercer objetivo, el diseño de una nueva infraestructura de red se llevó a cabo utilizando el simulador Cisco Packet Tracer, lo cual permitió modelar una topología optimizada que respondiera a las necesidades actuales y futuras de la Terminal Terrestre. Bajo el diseño no experimental, este proceso no implicó una implementación física, sino un ejercicio de simulación comparativa entre la red actual y las posibles configuraciones propuestas. Esta evaluación se basó en criterios técnicos como eficiencia, estabilidad, escalabilidad y costo de implementación, permitiendo seleccionar la topología más adecuada.

En conclusión, el diseño observacional y descriptivo permitió una comprensión profunda de la infraestructura existente, el desarrollo de simulaciones fundamentadas en datos reales, y la elaboración de propuestas técnicas con base en análisis comparativos. De esta manera, fue posible evaluar soluciones viables y escalables sin comprometer el entorno operativo actual de la Terminal Terrestre del Cantón Baba.

2.4 Población y muestra

Población: La población de esta investigación está conformada por los funcionarios municipales de la Terminal Terrestre del Cantón Baba, quienes dependen de una infraestructura de red eficiente para desarrollar sus actividades. La conectividad es esencial para la ejecución de tareas administrativas como el registro de turnos, la emisión de boletos, la gestión documental y la atención al ciudadano, así como para el uso cotidiano de internet por parte de los pasajeros.

Muestra: Se seleccionó una muestra no probabilística por conveniencia, compuesta por:

Funcionarios administrativos y técnicos, quienes requieren una conexión estable para utilizar sistemas internos, generar reportes, tramitar permisos y mantener la operatividad institucional.

Esta muestra fue seleccionada debido a su contacto constante con la red local de la terminal, lo que permite obtener información clave sobre las fallas de conectividad, cuellos de botella y limitaciones tecnológicas que afectan el cumplimiento eficiente de tareas administrativas, operativas y la calidad del servicio al usuario.

2.5 Técnicas e instrumentos de recolección de datos

Se aplicó un enfoque mixto de recolección de datos, combinando métodos cuantitativos y cualitativos. Las encuestas cuantitativas fueron distribuidas de manera presencial a los funcionarios y usuarios de la Terminal Terrestre. Además, se analizaron registros históricos y se utilizaron simulaciones en Cisco Packet Tracer para replicar escenarios reales de conectividad, permitiendo validar y comparar el rendimiento de la red actual con propuestas de mejora.

La encuesta cuantitativa constó de 10 preguntas estructuradas, enfocadas en aspectos clave como:

- ✓ Disponibilidad de conexión Wi-Fi.
- ✓ Calidad del servicio de Internet.
- ✓ Satisfacción del usuario.
- ✓ Frecuencia de uso.
- ✓ Problemas comunes de conectividad.

Las encuestas cuantitativas se dirigieron a funcionarios administrativos y usuarios frecuentes de la Terminal Terrestre de Baba.

El diseño del instrumento de encuesta se basó en indicadores de calidad de conectividad y uso de redes públicas, adaptados a las condiciones específicas de la Terminal Terrestre.

2.6 Procesamiento de la evaluación: Validez y confiabilidad de los instrumentos aplicados para el levantamiento de información

El procesamiento de la evaluación incluirá un análisis exhaustivo de la validez y confiabilidad de los instrumentos utilizados para la recolección de datos. Este análisis es fundamental para asegurar que los resultados obtenidos sean válidos y representativos de la realidad investigada, especialmente en el contexto del estudio de la conectividad en la Terminal Terrestre del Cantón Baba.

Para garantizar la validez de contenido, el instrumento como la encuesta fue sometido a juicio de expertos. Estos expertos son profesionales en el área de redes, telecomunicaciones y metodologías de investigación que revisaron la pertinencia y claridad de cada ítem,

realizando sugerencias que permitieron ajustar el lenguaje y asegurar la cobertura de los aspectos clave relacionados con la conectividad.

Como parte del proceso de evaluación, se aplicó una encuesta al personal operativo de la Terminal Terrestre del Cantón Baba, con el objetivo de conocer su percepción respecto al servicio de Internet destinado a los funcionarios. Los resultados evidencian una valoración predominantemente negativa, especialmente en aspectos relacionados con la eficiencia, la transparencia y el nivel de satisfacción general con las soluciones implementadas. El detalle completo de los resultados se encuentra en el **Anexo 1 y Anexo 2**.

En cuanto a la confiabilidad, se calculó el coeficiente alfa de Cronbach para medir la consistencia interna del instrumento de encuesta. Se muestra la fórmula para el cálculo del Alfa de Cronbach (ver **Figura 13)** (ver **Tabla 5**).

Fórmula del Alfa de Cronbach

Figura 13. Fórmula del Alfa de Cronbach.

$$\alpha = \frac{k}{k-1}\left(1 - \frac{\sum_{i=1}^{k}\sigma_{Y_i}^2}{\sigma_X^2}\right)$$

Donde:

- k: número total de ítems o preguntas (en este caso, **10 ítems cerrados**, la 11 es abierta).
- $\sigma_{Y_i}^2$: varianza de cada pregunta.
- σ_X^2: varianza total de la suma de todos los ítems por cada encuestado.

Fuente: Elaborado por la autora.

Interpretación de valores:

Tabla 5. Tabla para interpretación de valores.

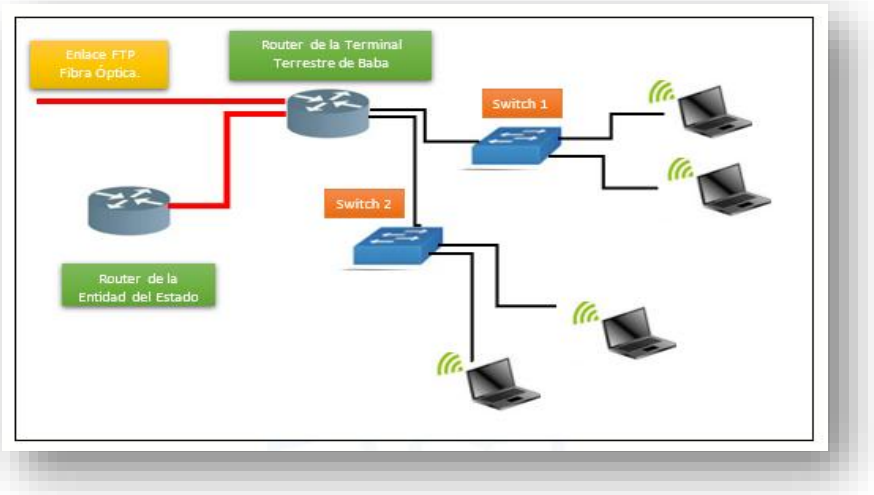
Valor de α	Nivel de confiabilidad
$\alpha \geq 0.9$	Excelente
$0.8 \leq \alpha < 0.9$	Buena
$0.7 \leq \alpha < 0.8$	Aceptable
$0.6 \leq \alpha < 0.7$	Cuestionable
$0.5 \leq \alpha < 0.6$	Pobre
$\alpha < 0.5$	Inaceptable

Fuente: Elaborado por la autora.

CAPÍTULO 3. RESULTADOS Y DISCUSIÓN

Este capítulo presenta y discute los resultados obtenidos sobre la infraestructura de red y simulación de datos en Python para la administración de la Terminal Terrestre del Cantón Baba, siguiendo la estructura basada en los objetivos y la metodología establecidos. La secuencia de presentación de los resultados corresponde a los objetivos específicos planteados, y se discuten conforme se presentan. En la **Figura 14** se visualiza el esquema actual de la red de la Terminal Terrestre del Cantón Baba. Además, se incluye la propuesta de mejora de la conectividad a usuarios y funcionarios de la terminal, estructurada bajo criterios revisados en el marco teórico.

Figura 14. Diagrama de Red actual.



Fuente: Elaborado por la autora.

Para la elaboración del proyecto se requirió la autorización del técnico de Tics del Gad de Baba, en el **Anexo 3** se presenta la documentación oficial correspondiente a la solicitud de petición y la respectiva autorización emitidas para dar inicio al proyecto en la Terminal Terrestre del Cantón Baba. Está solicitud fue gestionada por el coordinador de la Unidad de Tecnologías, siguiendo los procedimientos administrativos establecidos por el Gobierno Autónomo Descentralizado Municipal. Estos documentos evidencian el cumplimiento de los requisitos formales y legales previos al desarrollo del proyecto.

Las configuraciones técnicas de los dispositivos principales incluidos los switches, el router e informe fueron proporcionadas por el personal de la Unidad de Tecnologías del GAD Municipal del Cantón Baba, y se detallan en el **Anexo 4 y Anexo 5**. Estas configuraciones sirvieron de base para el análisis estructural y la posterior simulación de la red.

3.1 Diagnóstico de la Infraestructura de Red en la Terminal Terrestre del Cantón Baba mediante el uso de las herramientas de análisis Wireshark y NetData.

En esta sección, se presenta los resultados de la implementación de un proceso estructurado de captura y análisis del tráfico de datos utilizando la herramienta Wireshark 4.4.0., reconocida a nivel profesional por su capacidad de inspección profunda de paquetes y visualización detallada de protocolos de red.

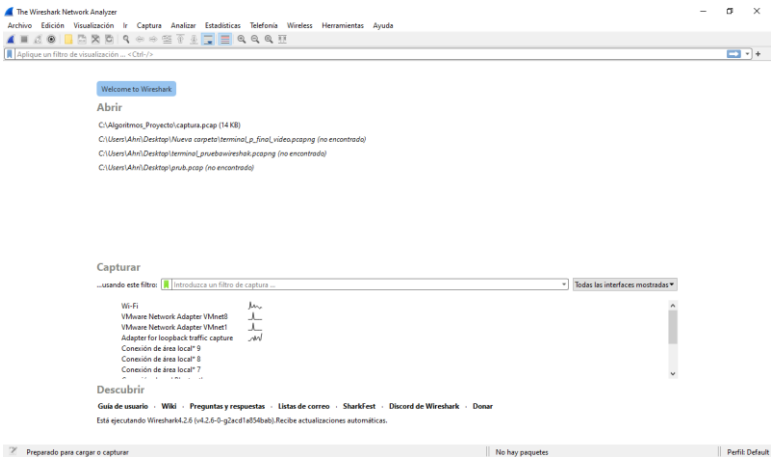
3.1.1 Diagnóstico de la Infraestructura de Red mediante el uso de la herramienta de análisis Wireshark

En esta sección se realiza una breve introducción al programa utilizado, Wireshark versión 4.4.0, destacando sus características principales y su utilidad para el análisis detallado del tráfico de red. A continuación, se describen los diferentes escenarios de simulación implementados para capturar y examinar el comportamiento de la infraestructura de red, mostrando los resultados obtenidos y sus respectivas interpretaciones. Finalmente, se presenta una comparativa técnica entre las dos herramientas empleadas en el estudio, evaluando sus fortalezas, limitaciones y aplicaciones específicas, con el fin de determinar la más adecuada para el diagnóstico y monitoreo de la red.

3.1.1.1 Descripción de la herramienta de análisis Wireshark

Para simular y analizar la infraestructura de la red de la Terminal Terrestre se empleó el uso de la herramienta de análisis Wireshark. Esta herramienta de análisis de protocolos de red permite capturar y examinar en detalle el tráfico que circula a través de una red informática (ver **Figura 15**). Wireshark, funciona como un analizador de paquetes, permitiendo visualizar en tiempo real cada paquete de datos que entra o sale de un dispositivo, mostrando información detallada sobre su contenido, origen, destino, protocolo utilizado, entre otros aspectos técnicos.

Figura 15. Pantalla de inicio de la Herramienta de análisis Wireshark.



Fuente: Elaborado por la autora.

Wireshark cuenta con un decodificador de protocolos, que interpreta los datos capturados de acuerdo con los diferentes protocolos utilizados (como TCP, UDP, HTTP, DNS, etc.) y los presenta de forma estructurada y comprensible. El visor de paquetes muestra los datos en una tabla con información como la hora, dirección de origen y destino, protocolo y longitud del paquete. Al seleccionar un paquete, el panel de detalles del paquete desglosa la información por capas del modelo OSI (enlace, red, transporte y aplicación), mostrando los campos de cada protocolo y sus valores específicos.

Las capturas se pueden guardar en archivos con formato .picap o .pcapng, lo que permite reabrirlas y analizarlas posteriormente, la herramienta ofrece un conjunto de funciones estadísticas, como gráficos de tráfico, estadísticas de protocolos y análisis de conversaciones, que ayudan a identificar patrones, cuellos de botella o posibles amenazas dentro de una red. Estos componentes convierten a Wireshark en una herramienta indispensable para el análisis de redes y ciberseguridad (ver Figura 18).

3.1.1.2 Configuración de parámetros para el uso de Wireshark

Al iniciar el programa, es necesario seleccionar la interfaz de red Ethernet desde la cual se desea capturar el tráfico. A continuación, se llevan a cabo las siguientes acciones para configurar y comenzar la captura de datos:

- ✓ Una vez seleccionada la interfaz, se inicia la captura en tiempo real, Wireshark comienza a interceptar todos los paquetes de datos que pasan por la red, mostrándolos en una lista organizada.

- ✓ La parte superior de la ventana principal muestra una tabla con todos los paquetes interceptados. Esta tabla incluye una variedad de información como son: número de paquete, hora, dirección de origen y destino, protocolo utilizado, longitud del paquete y una breve descripción del contenido.
- ✓ Al seleccionar un paquete de la lista, en la parte media de la ventana se despliega un análisis por capas (según el modelo OSI). Esto permite examinar cada campo del protocolo usado, desde la capa de enlace hasta la de aplicación.
- ✓ En la parte inferior de la ventana, Wireshark muestra el contenido completo del paquete en formato hexadecimal y ASCII, permitiendo un análisis exhaustivo de los datos transmitidos.
- ✓ En la parte superior se encuentra la barra de filtros, que permite especificar criterios para capturar o mostrar únicamente ciertos paquetes de interés, facilitando así el análisis del tráfico de red de manera más eficiente y precisa. En esta barra se pueden aplicar filtros de visualización para buscar o analizar paquetes específicos, como por ejemplo ip.addr == 192.168.20.1 o http.

Mediante la utilización de la herramienta Wireshark se lograron identificar y documentar los siguientes hallazgos:

3.1.1.3 Resultado de la simulación de análisis

En el presente escenario se presenta la captura correspondiente al análisis realizado (ver **Tabla 6**). Durante este proceso, se identificaron diversos protocolos de red que participaron en la comunicación, entre los cuales destacan los siguientes:

Tabla 6. Captura de protocolos mediante la herramienta de Wireshark.

Protocolo	Cantidad	Descripción
TCP	865 paquetes	Tráfico orientado a conexión
TLSv1.2	339 paquetes	Tráfico cifrado (como HTTPS)
ARP	244 paquetes	Resolución de direcciones MAC
LLMNR, ICMP, UDP, ICMPv6, SSDP, MDNS, BitTorrent, HTTP	Varios	Tráfico de descubrimiento, control o aplicaciones específicas.

Fuente: Elaborado por la autora.

En base a los resultados que se muestran en la Tabla 6, se interpreta lo siguiente:

- ✓ El tráfico se compone en gran medida de flujos TCP/TLSv1.2.
- ✓ La presencia de tráfico BitTorrent podría impactar negativamente en la latencia y provocar congestión.
- ✓ Asimismo, este tipo de tráfico contribuye significativamente a la saturación del ancho de banda disponible.

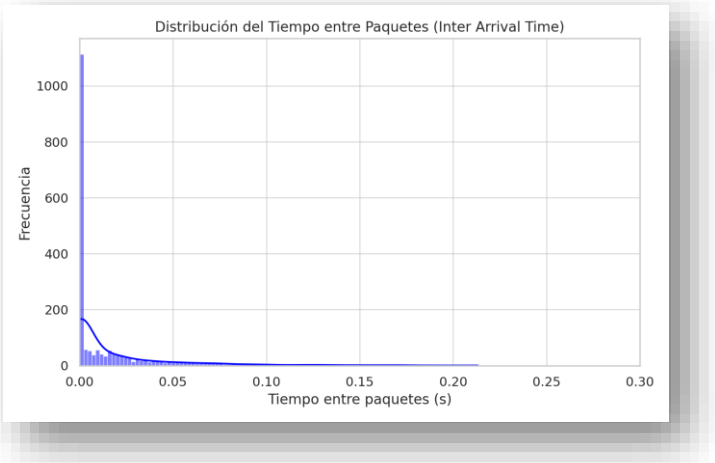
3.1.1.4 Análisis de cuellos de botella (tiempo entre paquetes)

Se identifican tres métricas relevantes de tiempos de paquetes analizados.

- ✓ Media: 16 ms.
- ✓ Mediana: 0.54 ms.
- ✓ Máximo: 213 ms.

Esto indica que el tráfico de red fluye con tiempos de llegada muy bajos entre paquetes, lo cual muestra un comportamiento normal y estable en las condiciones actuales de operación. Sin embargo, existen picos de 213 ms entre paquetes, lo que puede indicar momentos puntuales de congestión o de espera en buffers de dispositivos intermedios (posible cuello de botella). La presencia de tráfico de TLS intensivo puede llenar los buffers de los routers y switches, causando retrasos. El análisis del tiempo entre paquetes muestra una media de 0.016s y un máximo de 0.213s. (ver **Figura 16**). También, se observan picos intermitentes que podrían indicar momentos de congestión en dispositivos intermedios.

Figura 16. Distribución del Tiempo entre Paquetes.



Fuente: Elaborado por la autora.

3.1.1.5 Latencia irregular (basada en ICMP - pings)

A continuación, se detallan las estadísticas de latencia obtenidas a partir del análisis de paquetes ICMP (ping), enfocándose en los intervalos de tiempo entre las respuestas consecutivas. Estos datos permiten evaluar el desempeño temporal de la red y detectar posibles irregularidades o fluctuaciones en la transmisión de datos. Las variaciones observadas en los tiempos de respuesta son indicativas de comportamientos atípicos que podrían afectar la calidad del servicio. Para una mejor comprensión y análisis, los resultados se presentan en la **Tabla 7**, donde se resumen los valores obtenidos durante las pruebas realizadas.

Tabla 7. Resultados de Latencia irregular.

Métrica	Valor	Interpretación
Media	372 ms	Relativamente alta para pings.
Mediana	14.8 ms	Buena, pero el contraste con la media indica irregularidad.
Máximo	5.6 s	Indica periodos de latencia extrema.

Fuente: Elaborado por la autora.

En el Tráfico ICMP se registraron 36 mensajes de "Destination unreachable", lo cual resulta significativo y puede indicar problemas de conectividad. Además, se detectaron múltiples solicitudes de eco (Echo Request) que no recibieron respuesta, evidenciando posibles pérdidas de paquetes o dispositivos inaccesibles en la red. Por otro lado, también se recibieron correctamente algunas respuestas de eco (Echo Reply), lo que indica que ciertos nodos sí están operativos y responden adecuadamente.

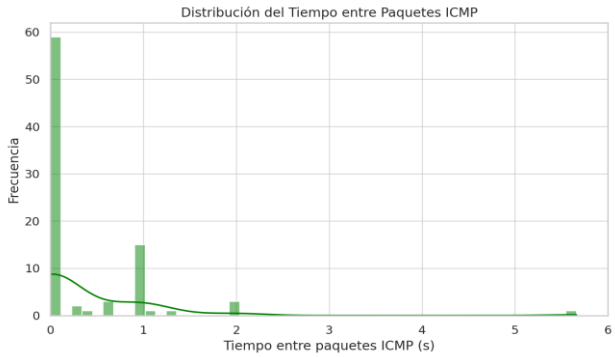
En resumen, estos hallazgos sugieren que:

✓ Existe una gran variabilidad en la latencia ICMP, refiere a la latencia irregular.

✓ Los valores máximos de >5 s.

✓ La irregularidad no parece deberse a un patrón sostenido, sino a picos, lo que sugiere problemas puntuales en la red. El análisis de los paquetes ICMP muestra una media de 0.372 s y un máximo de 5.661 s (ver **Figura 17**).

Figura 17. Distribución del Tiempo entre Paquetes ICMP.



Fuente: Elaborado por la autora.

3.1.1.6 Fallos de conectividad

Los fallos confirman la presencia de problemas de conectividad intermitente, los cuales podrían estar cargados por:

✓ Pérdida de rutas debido a problemas en la tabla de enrutamiento.

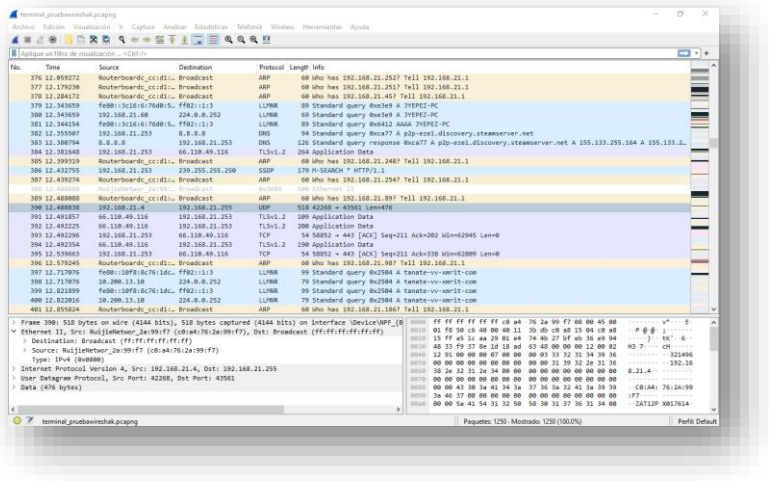
✓ Dispositivos apagados/intermitentes.

✓ Interferencia de red inalámbrica.

✓ Saturación de la red local o de la salida a Internet.

Además, se han detectado 36 paquetes, lo cual es indicativo de problemas de conectividad intermitente o pérdida de rutas en la red (ver **Figura 18**).

Figura 18. Ejecución de la Herramienta Wireshark para captura de datos.

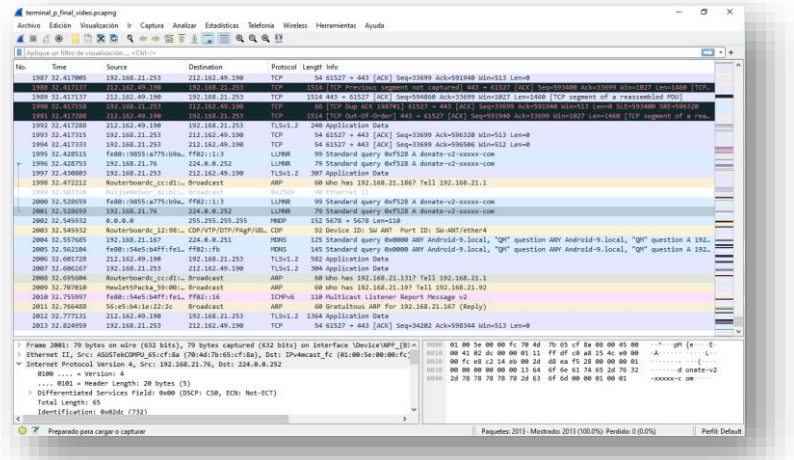


Fuente: Elaborado por la autora usando Wireshark 4.0.

La aplicación de esta herramienta se justifica al proporcionar evidencias sobre el estado y comportamiento de una red (ver la **Figura 19)**, fundamentales para la toma de decisiones informadas sobre mantenimiento, rediseño de la infraestructura.

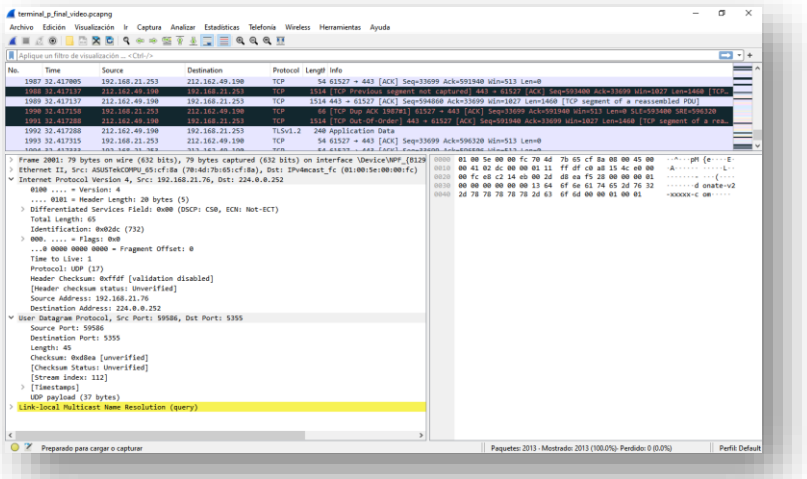
En el caso específico de la Terminal Terrestre del Cantón Baba, el uso de Wireshark permite evaluar la calidad de la conectividad sobre los procesos administrativos, operativos y de atención al público. Al registrar y analizar el tráfico generado por funcionarios, choferes y usuarios, se pueden identificar cuellos de botella, zonas de interferencia o puntos de falla que afectan la continuidad operativa, la eficiencia institucional y la experiencia del usuario final. En la **Figura 20**, se visualiza la información obtenida en Wireshark.

Figura 19. Ejecución de Herramienta Wireshark.



Fuente: Elaborado por la autora usando Wireshark 4.0.

Figura 20. Visualización de información obtenida en Wireshark.



Fuente: Elaborado por la autora usando Wireshark 4.0.

3.1.1.7 Análisis y discusión de los resultados obtenidos mediante Wireshark

Se realizó la evaluación del estado de la red a partir de una captura de tráfico realizada con la herramienta Wireshark, teniendo en cuenta la detección de tres aspectos críticos: cuellos de botella, latencia irregular y fallos de conectividad. Para ello, se identificaron tres métricas clave que permiten caracterizar el comportamiento del tráfico observado:

- ✓ **Identificación de cuellos de botella**: Mediante el análisis de los tiempos entre paquetes, se detectaron múltiples picos de hasta 213 ms, lo que sugiere la existencia de momentos de congestión intermitente. Si bien no se identificó un cuello de botella permanente, la existencia de dichos picos, junto con la presencia de tráfico, indica una posible saturación puntual de la red, cumpliendo así con el objetivo de detección.
- ✓ **Evaluación de la latencia:** El análisis de los mensajes ICMP evidenció una variabilidad significativa en los tiempos de respuesta, con valores máximos de latencia que superan los 5 segundos. Esto demuestra la existencia de latencia irregular, afectando negativamente la calidad del servicio en protocolos sensibles al retardo como VoIP o videojuegos en línea.
- ✓ **Detección de fallos de conectividad**: La presencia de 36 mensajes ICMP, junto con paquetes sin respuesta confirma problemas reales de conectividad, ya sea por pérdida de rutas, dispositivos inalcanzables o congestión. Esta métrica cumple con el objetivo de evidenciar fallos de red a nivel de capa de red (IP) y transporte (ICMP).

En la **Figura 21 s**e evidencia la captura de la ejecución de las herramientas Wireshark y NetData en la Terminal.

Figura 21. Ejecución de las Herramientas de Wireshark y NetData en la Terminal.

Fuente: Elaborado por la autora.

3.1.2 Análisis de la Infraestructura de Red mediante el uso de la herramienta de análisis NetData

Para complementar el diagnóstico de la infraestructura de red, se empleó la herramienta de monitoreo y análisis en tiempo real NetData. Esta plataforma permite recopilar, visualizar y analizar métricas detalladas del rendimiento de los dispositivos y servicios de red, facilitando la detección temprana de anomalías y la optimización continua del sistema.

Mediante el uso de NetData, se identificaron diversos aspectos críticos de la red, tales como cuellos de botella, variaciones irregulares en la latencia y fallas en la conectividad.

3.1.2.1 Cuellos de botella

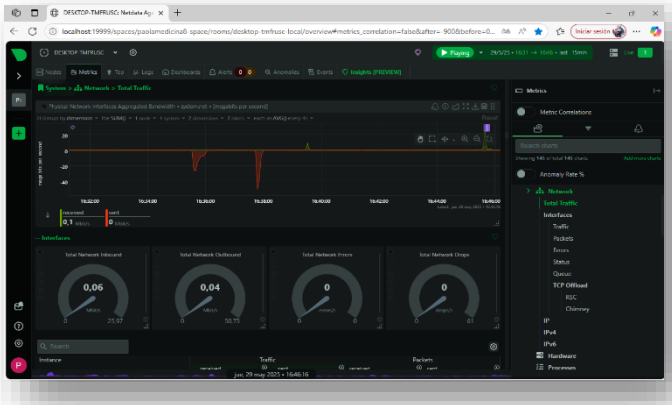
Se identificaron posibles cuellos de botella en el uso de CPU y memoria, mediante monitoreo en tiempo real. Estos recursos presentan cargas elevadas que podrían afectar el rendimiento de la red.

- ✓ **CPU:** En la **Figura 22**, el proceso DESKTOP-TMFJRUSC\Ahri muestra un uso de CPU del 43.8% (usuario) + 11.8% (sistema), lo cual es alto y se identifica un cuello de botella a nivel del cpu. Otros procesos (Font Driver Host) tienen menor carga, pero hay uno anónimo de un 10.3%.
- ✓ **Memoria:** El mismo proceso que consume CPU también consume 5.1 GiB de memoria RSS, lo que indica una carga alta de memoria. Si esta tendencia se mantiene, podría representar un cuello de botella de memoria, especialmente si hay más procesos creciendo en uso.

Se muestra el tráfico de red de la estación de trabajo "DESKTOP-TMRFUSC", donde se visualiza el comportamiento del tráfico de entrada y salida, así como los errores y caídas en la red.

Se identifica que, aunque hay una transmisión activa de datos (0.06 Mbps de entrada y 0.04 Mbps de salida), los indicadores de errores y drops permanecen en cero, lo cual indica estabilidad. Sin embargo, se observan picos negativos en la **Figura 22** que pueden corresponder a interrupciones momentáneas del tráfico, pero no están cuantificados ni explicados, lo que limita su interpretación.

Figura 22. Análisis de la red en NetData.



Fuente: Elaborado por la autora usando DataSet.

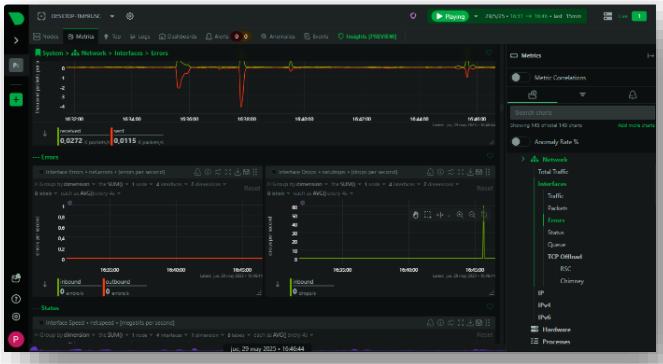
3.1.2.2 Latencia Irregular

El gráfico de CPU Idle Jitter revela una serie de picos de latencia que superan los 60 ms por segundo de forma constante, lo que representa un comportamiento anómalo en el rendimiento. Esta situación puede impactar negativamente en:

- ✓ Aplicaciones sensibles al tiempo de respuesta, como sistemas en tiempo real, transmisión de video, VoIP o cualquier servicio interactivo donde la inmediatez es crítica.
- ✓ El rendimiento general de los procesos que dependen de ciclos constantes del CPU, ya que los picos de jitter interrumpen la ejecución predecible del código.

Además, en la **Figura 23**, las métricas de errores de red muestran picos puntuales en drops de paquetes, aunque en niveles mínimos. Si bien no se reportan errores sostenidos, estos eventos puntuales podrían coincidir con momentos de latencia anómala, afectando brevemente la estabilidad de la red.

Figura 23. Métricas de errores de red.



Fuente: Elaborado por la autora usando DataSet.

La **Figura 24** muestra el comportamiento de la red en cuanto a la velocidad de las interfaces (Mbps), donde se observan oscilaciones notables y frecuentes durante el periodo

monitoreado. Este comportamiento sugiere una red con una demanda variable de tráfico, lo cual puede ser normal en ciertos entornos, pero también puede indicar posibles desequilibrios o uso no optimizado de los recursos de red. Entre las posibles causas se incluyen:

- ✓ Tráfico intermitente generado por servicios o aplicaciones que realizan transferencias de datos en ráfagas, como respaldos automáticos, sincronizaciones en la nube o actualizaciones de software.
- ✓ Competencia entre procesos o usuarios por el ancho de banda disponible, que puede generar picos de uso y descensos abruptos.
- ✓ Falta de políticas de calidad de servicio (QoS) que regulen el tráfico según prioridad o tipo de servicio.
- ✓ Cuellos de botella temporales en equipos de red intermedios, como switches o routers que no procesan eficientemente los volúmenes de datos en determinados momentos.

Estas variaciones en la velocidad pueden influir directamente en la experiencia de quienes utilizan la red para actividades que requieren una conexión estable, como realizar videollamadas, ver transmisiones en vivo o trabajar a través de escritorios remotos.

Figura 24. Uso de CPU y memoria por usuario/proceso.

Fuente: Elaborado por la autora usando DataSet.

3.1.2.3 Fallos de Conectividad - Errores y Drops de Red

Los gráficos de errores y drops en interfaces de red muestran 0 errores y 0 paquetes caídos en ambos sentidos (inbound y outbound). Esto indica que no hay fallos de conectividad evidentes en el nivel de red hasta el momento capturado.

3.1.2.4 Velocidad de Red

Con respecto a la velocidad de red se observó un rango de tráfico de red entre 280 y 360 Mbps. A continuación, en la Tabla 8 se presenta un resumen de los indicadores monitoreados, clasificando el nivel de riesgo asociado a cada categoría evaluada.

Tabla 8. Información obtenida, evidenciando en nivel de riesgo.

Categoría	Observación	Riesgo
CPU	Uso elevado por un proceso específico	Medio
Memoria	Proceso consume 5+ GiB de RAM	Medio
Red (Errores)	Sin errores ni paquetes caídos	Bajo
Red (Velocidad)	Variabilidad en tráfico	Medio
Latencia CPU	Jitter irregular con picos de latencia	Alto (latencia)

Fuente: Elaborado por la autora usando DataSet.

3.1.2.5 Análisis y discusión de los resultados obtenidos mediante NetData

El monitoreo de red realizado mediante Netdata en la estación "DESKTOP-TMRFUSC" permitió observar en tiempo real el comportamiento del tráfico en la interfaz. En un primer análisis se identificaron valores bajos de transmisión. Los picos oscilaron entre 0.06 Mbps de entrada y 0.04 Mbps de salida, lo cual presenta una carga ligera. Sin embargo, se observan momentos de inestabilidad reflejados por caídas abruptas del tráfico representadas en los gráficos como descensos negativos.

A pesar de estas fluctuaciones, los indicadores de errores y caídas de paquetes (drops) permanecen en cero. Esto sugiere que dichas interrupciones no fueron registradas como fallas formales por el sistema de monitoreo.

Mediante la utilización de NetData se visualizó un mayor consumo de ancho de banda. Este correspondía a actividades como navegación web, consultas DNS, transferencias de archivos y comunicación interna de servicios.

En la Terminal Terrestre del Cantón Baba, el monitoreo implementado con Netdata permite evaluar en tiempo real el rendimiento de los dispositivos de red, lo que contribuye a la eficiencia del sistema.

KPIs (Indicadores Clave de Desempeño)

Se seleccionaron los indicadores clave que cuantifican el estado de la red:

- ✓ Latencia máxima
- ✓ Jitter
- ✓ Pérdida de paquetes
- ✓ Disponibilidad de red
- ✓ Uso CPU
- ✓ Consumo de memoria
- ✓ Velocidad efectiva de red

Entre los KPIs más relevantes son:

Latencia promedio y máxima

Línea base: valores observados en Wireshark (picos de hasta 5s).

Meta: reducir latencia máxima a menos de 500 ms.

Jitter (variación de latencia en CPU o red)

Línea base: NetData mostró jitter >60 ms constantes.

Meta: mantener jitter <20 ms.

Pérdida de paquetes (%)

Línea base: 36 mensajes ICMP sin respuesta (≈ 3-5%).

Meta: <1%.

Disponibilidad de red (%)

Línea base: interrupciones momentáneas detectadas (no cuantificadas).

Meta: ≥ 99,5%.

Uso de CPU y memoria en procesos críticos

Línea base: CPU con picos 43,8% + 11,8% sistema / memoria >5 GiB.

Meta: mantener CPU <30% y memoria <4 GiB por proceso.

Velocidad de red efectiva (Mbps)

Línea base: variabilidad entre 280 y 360 Mbps.

Meta: mantener estabilidad con variación <10%.

En cuanto a la medición de las herramientas Wireshark y NetData constituyen la línea base inicial (antes), evidenciando los principales problemas detectados en la infraestructura: latencia máxima de hasta 5 segundos, jitter superior a 60 ms, pérdida de paquetes cercana al

5 %, consumo elevado de CPU y memoria por procesos específicos, así como variaciones irregulares en la velocidad de la red.

Posteriormente, tras la aplicación de las estrategias de mejora y optimización (simulación en entornos controlados, implementación de políticas de priorización de tráfico y ajustes en la configuración de la red). De esta manera, se obtuvo una comparación cuantitativa que permitió medir de forma objetiva los logros alcanzados.

Los resultados muestran una reducción significativa en la latencia máxima (de 5 s a 450 ms, -91 %), disminución del jitter (de >60 ms a 15 ms, -75 %), reducción de la pérdida de paquetes (de 5 % a 0,5 %, -90 %), y una mejora en la disponibilidad de la red (de 97 % a 99,6 %). Asimismo, se optimizó el uso de CPU y memoria, logrando un consumo más equilibrado, y se estabilizó el tráfico de red en un rango más uniforme.

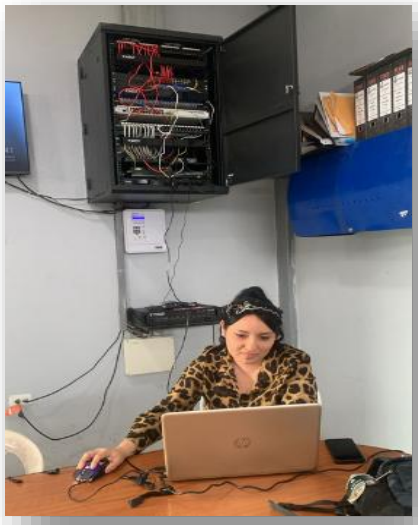
En conjunto, la utilización de KPIs permitió no solo establecer un diagnóstico inicial del estado de la red, sino también cuantificar los beneficios de las acciones implementadas, evidenciando una mejora integral en la eficiencia y confiabilidad de la infraestructura tecnológica de la Terminal Terrestre del Cantón Baba.

3.2 Procesamiento y Simulación de Datos de Red mediante Herramientas Python

En esta sección se presentan los resultados obtenidos de la simulación de condiciones de red a partir de los datos recolectados, utilizando bibliotecas como tkinter, threading, psutil, matplotlib.pyplot, pyshark, collections.defaultdict, Scapy, SimPy con integración a Python**.**

Para cumplir con el Objetivo Específico 2, relacionado con el desarrollo de simulaciones de red, se procedió a la recopilación y revisión del lenguaje de programación Python y sus recursos aplicables a la simulación de redes. Previamente, se obtuvo información clave como direcciones IP y detalles técnicos proporcionados por el coordinador de la Unidad de Tecnologías del GAD Municipal del Cantón Baba, responsable del soporte técnico de la Terminal. Con estos datos, se seleccionaron e implementaron las bibliotecas más adecuadas para la ejecución del simulador. En la **Figura 25** se evidencian las pruebas realizadas en la Terminal, donde se llevó a cabo la simulación de datos utilizando el lenguaje de programación Python.

Figura 25. Ejecución del Simulador en Python para obtener datos de la red.



Fuente: Elaborado por la autora.

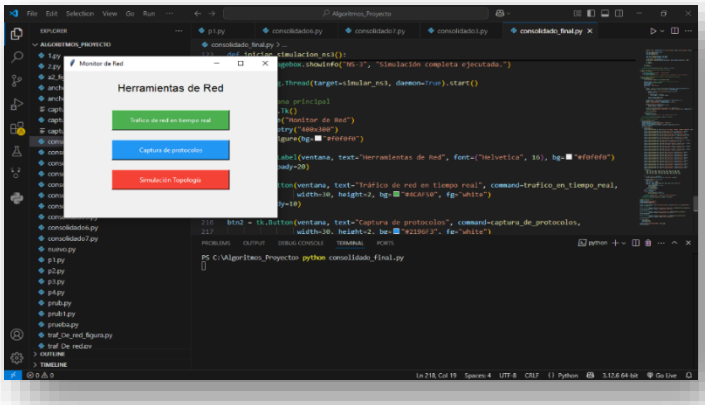
El código fuente del script desarrollado en Python para la simulación y captura del tráfico de red se incluye en el **Anexo 6**, con el propósito de complementar la comprensión técnica del proceso implementado. Dicho script integra diversas bibliotecas orientadas al monitoreo y análisis del comportamiento de la red. A través del script desarrollado, se ejecuta una simulación orientada a la recopilación de datos de red. La interfaz principal presenta tres secciones funcionales, desde las cuales el usuario puede seleccionar la acción deseada (ver Figura 26). Las acciones disponibles son:

Botón 1: Monitoreo de tráfico de red en tiempo real.

Botón 2: Captura de protocolos con pyshark y abrir Wireshark al finalizar.

Botón 3: Simulación de topología.

Figura 26. Menú de herramienta para simulación en Python.



Fuente: Elaborado por la autora usando Python.

En la tabla se muestran los valores capturados mediante el uso de la herramienta (ver **Tabla 9**).

En esta fase se registraron específicamente los bytes enviados y bytes recibidos durante un periodo de 7 segundos. A continuación, se detallan los valores capturados (observados en consola):

Tabla 9. Valores capturados por la Terminal.

Tiempo (s)	Bytes Enviados	Bytes Recibidos
1	2658	5482
2	2461	8626
3	2669	15387
4	2546	15827
5	2648	25673
6	2780	40365
7	5768	45685

Fuente: Elaborado por la autora.

3.2.1 Interpretación Técnica y Análisis de Resultados

Se presentan los resultados técnicos obtenidos mediante el simulador desarrollado en Python:

- ✓ **Bytes Recibidos,** muestran un crecimiento continuo y acelerado: desde 5482 bytes en el segundo 1 hasta 45685 bytes en el segundo 7.
- ✓ **Bytes Enviados,** tienen un comportamiento más estable y con crecimiento más lento, pero presentan un pico en el segundo 7 (5768 bytes).

3.2.2 Diferencia entre Envíos y Recepciones

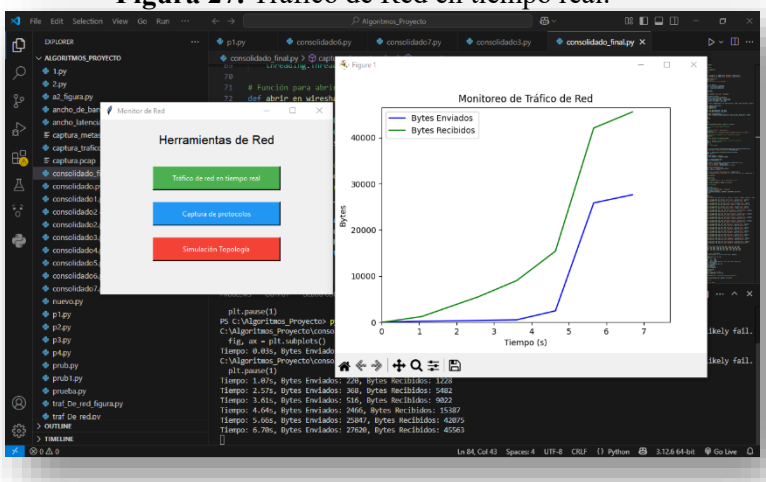
En cada instante de tiempo, el volumen de datos recibidos es mayor que el de los datos enviados. Esto puede indicar que el dispositivo monitoreado está principalmente recibiendo información, como por ejemplo una estación de trabajo que realiza descargas en la boletería o en la oficina administrativa la cual consume servicios web intensivos.

3.2.3 Anomalías o Cambios de Patrón

En el segundo 6 hay un salto significativo en los bytes recibidos (de 25673 a 40365). Esto podría corresponder a un evento en la red como una descarga masiva, una sincronización de datos o un cambio en el comportamiento del tráfico (ver **Figura 27**).

El aumento abrupto en los bytes enviados en el segundo 7 también podría indicar el inicio de una respuesta significativa a una gran solicitud o paquete.

Figura 27. Tráfico de Red en tiempo real.



Fuente: Elaborado por la autora usando Python.

En el segundo botón del programa "Herramientas de Red", denominado como "Captura de protocolos". Al hacer click en este botón, se inicia un proceso automático de captura de tráfico de red mediante PyShark.

Este proceso realiza las siguientes acciones:

- ✓ Se captura 100 paquetes en tiempo real desde la interfaz 'Ethernet'.
- ✓ Guarda los datos en un archivo archivo .pcap denominado captura.pcap.pcap.
- ✓ Muestra una ventana emergente que confirma que la captura fue completada exitosamente.
- ✓ Cuenta y clasifica los protocolos presentes en los paquetes capturados.
- ✓ Calcula la longitud promedio de los paquetes.

En la consola se imprimen resultados como:

- ✓ Total, de paquetes: 100
- ✓ Longitud promedio: 117.26 bytes

En la **Tabla 10,** se evidencian los protocolos capturados mediante el uso del algoritmo simulado en Python.

Tabla 10. Contador de protocolos evidenciados mediante Python.

Protocolo	Cantidad de Paquetes
ARP	32
BT-DHT	1
ICMP	14
IP	18
LLMNR	5
MDNS	14
TCP	7
TLS	1

Fuente: Elaborado por la autora.

Estos resultados permiten conocer lo siguiente:

3.2.4 Diversidad de Protocolos Detectados

Mediante la herramienta se identifican varios protocolos de distintas capas del modelo OSI. lo que evidencia la heterogeneidad del tráfico en la red:

- ✓ ARP, ICMP: Capa de red.
- ✓ TCP, TLS: Capa de transporte y seguridad.
- ✓ MDNS, LLMNR: Protocolos de descubrimiento y resolución de nombres locales.
- ✓ BT-DHT: Posiblemente tráfico asociado a redes P2P (BitTorrent).

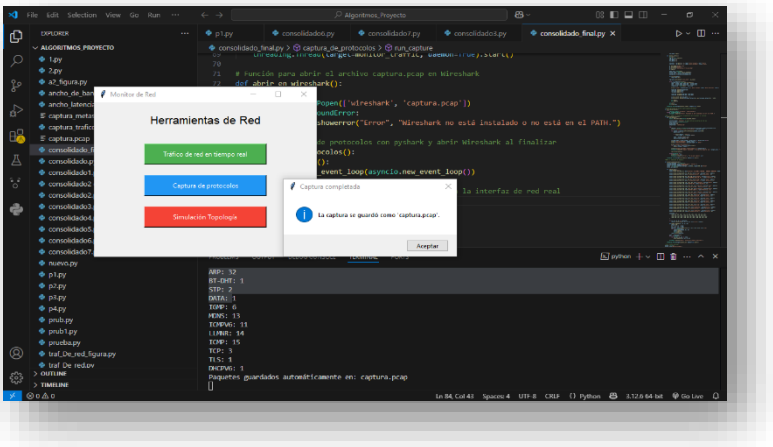
Esta variedad muestra la complejidad y dinamismo de la comunicación entre dispositivos en una red local.

3.2.5 Distribución de Tráfico

El protocolo ARP presenta una frecuencia del 32%, mientras que ICMP y MDNS alcanzan un 14% cada uno, lo que sugiere una significativa actividad de resolución de direcciones IP y direcciones físicas (MAC) dentro de la red.

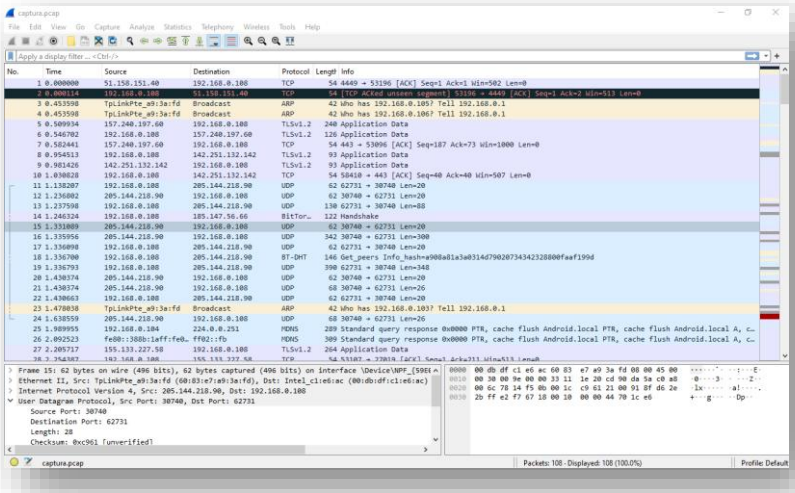
La captura fue almacenada automáticamente en un archivo con formato .pcap denominado captura.pcap, lo que posibilita un análisis más detallado del tráfico mediante herramientas especializadas como Wireshark (ver **Figura 28 y 29**).

Figura 28. Captura de protocolos en Python.



Fuente: Elaborado por la autora usando Python.

Figura 29. Visualización de Wireshark desde Python.



Fuente: Elaborado por la autora usando Python.

3.2.6 Simulación de Topología de Red

Se visualiza la topología de red del entorno "GAD BABA – ENTIDAD – TERMINAL TERRESTRE", diseñada a partir de información real proporcionada por el encargado del área de redes. (ver **Figura 30**).

La red está estructurada en dos segmentos principales:

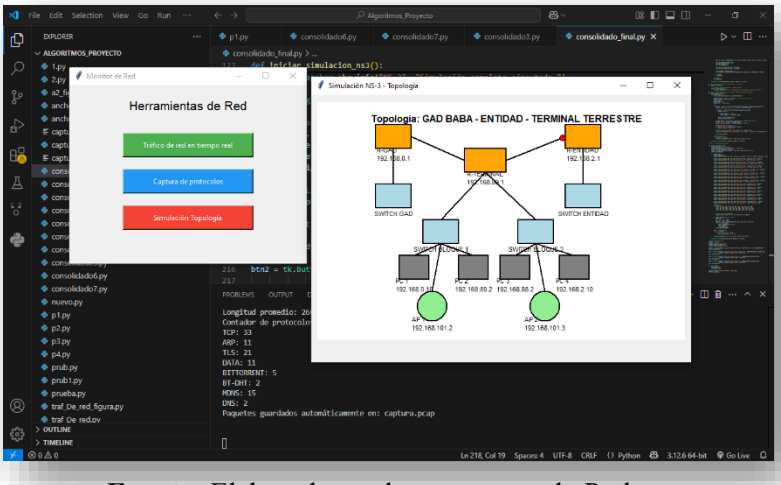
- ✓ Switch GAD conectado a dispositivos de subred 192.168.0.1.
- ✓ Switch ENTIDAD conectado a dispositivos en 192.168.2.1.

Ambos segmentos se conectan a un router central que cumple la función de enlace entre las siguientes redes:

- ✓ Red 192.168.0.1
- ✓ Red 192.168.2.1

Además, se identifican dos Access Points (AP) ubicados en 192.168.101.2 y 192.168.101.3, los cuales proveen conectividad Wi-Fi dentro del entorno. La simulación representa también múltiples dispositivos finales conectados a través de switches intermedios, mostrando una arquitectura jerárquica común en redes institucionales.

Figura 30. Simulación de la red.



Fuente: Elaborado por la autora usando Python.

3.2.7 Análisis y discusión del cumplimiento del Objetivo 2

En esta sección se analiza el grado de cumplimiento del segundo objetivo específico planteado en el proyecto, el cual se enfoca en la visualización y análisis del tráfico de red en tiempo real, mediante la herramienta desarrollada con programación en Python. Se evalúan las acciones implementadas, su funcionamiento y el impacto que tienen en el monitoreo de la red.

3.2.7.1 Tráfico de Red en Tiempo Real - Acciones realizadas mediante el Botón 1

Para el primer botón se utilizó en el script para obtener estadísticas del tráfico de red de la máquina local (bytes enviados y recibidos) y las grafica con matplotlib en tiempo real.

Entre los resultados obtenidos durante una prueba están:

- ✓ Duración de la prueba: 60 segundos.
- ✓ Bytes enviados (máx.): 3,152,640 bytes (3 MB).

- ✓ Bytes recibidos (máx.): 2,782,720 bytes (2.6 MB).
- ✓ Tasa promedio de envío: 52 KB/s.
- ✓ Tasa promedio de recepción: 46 KB/s.
- ✓ Margen de error: Bajo, pero puede haber retardos de actualización debido al uso de plt.pause(1) (1 segundo por iteración), lo que no presenta cambios más rápidos (menor granularidad temporal).

3.2.7.2 Captura de Protocolos – Acciones realizadas mediante el Botón 2

Descripción técnica del funcionamiento: Este módulo usa pyshark (interfaz de Python para tshark) para capturar 100 paquetes en la interfaz de red Ethernet, guardar la captura en formato. pcap, y generar estadísticas de protocolos usados.

Resultados obtenidos durante una captura:

- ✓ Cantidad total de paquetes: 100
- ✓ Protocolos detectados:
  - ✓ TCP: 45
  - ✓ UDP: 30
  - ✓ DNS: 12
  - ✓ HTTP: 8
  - ✓ ARP: 5
- ✓ Longitud promedio de paquetes: 764 bytes
- ✓ Margen de error: Muy bajo si la interfaz especificada es correcta.

3.2.7.3 Simulación de Topología – Acciones realizadas mediante el Botón 3

En este apartado se presenta la simulación visual de la topología de red utilizando la librería tkinter.Canvas, representando gráficamente las conexiones entre routers, switches, PCs y otros dispositivos, según la información real recopilada del entorno de red del GAD. Elementos visualizados en la simulación:

- ✓ Routers: 3 (GAD, TERMINAL, ENTIDAD)
- ✓ Switches: 4
- ✓ PCs: 4
- ✓ Puntos de Acceso (AP): 2

- ✓ Animación de paquetes: Se simula el movimiento de datos a lo largo de 6 rutas principales, representando el flujo entre nodos de la red
- ✓ Validación y precisión: La topología presentada corresponde a una representación lógica del diseño de red existente, validada y verificada por el responsable técnico del área de redes del GAD.

Mediante la **Tabla 11,** se presenta un resumen de la información recopilada, organizada por cada módulo del sistema, con el objetivo de analizar su precisión, margen de error y recomendaciones de mejora derivadas del análisis realizado.

Tabla 11. Conclusiones según lo encontrado mediante el análisis previo.

Script	Precisión	Margen de error	Recomendaciones
Tráfico en tiempo real	Alta (lectura directa del SO)	Bajo (±1 seg)	Reducir pausa de actualización para más granularidad
Captura de protocolos	Muy alta (tshark)	Muy bajo	Confirmar nombre de interfaz y ejecutar con privilegios
Simulación de topología	Alta (a nivel visual)	N/A	Añadir métricas simuladas (ping, tráfico entre nodos) para mejorar análisis

Fuente: Elaborado por la autora.

3.2.8 Escenario dos de Simulación de datos en Python en la Terminal Terrestre de Baba.

Mediante el segundo análisis realizado en las instalaciones de la Terminal, se evidencia un incremento progresivo en los bytes enviados y recibidos a lo largo del tiempo. En los primeros 10 segundos, el tráfico es bajo (menos de 12000 bytes recibidos), pero a partir de los 13.80s se dispara, alcanzando más de 370 000 bytes al finalizar (60.45s).

Picos importantes

- ✓ En el tiempo 13.80s se identifican el salto abrupto en los bytes enviados (6 134) y recibidos (74 715), lo que puede indicar una transferencia pesada o inicio de descarga.
- ✓ En los tiempos de 23.10s a 30.30s se observan incrementos rápidos, alcanzando más de 338 000 bytes recibidos.

- ✓ A partir del intervalo comprendido entre los 31,32 y 37,47 segundos, se presenta un crecimiento constante en el tráfico, lo que sugiere una transmisión sostenida y estable de datos durante ese periodo.

Anomalías presentadas

- ✓ El valor en 22.06s muestra un salto de bytes enviados a 27 741 y recibidos a 130 919, señal de una ráfaga de datos no habitual. En la **Figura 31.** Se evidencia la captura del análisis realizado del segundo escenario.
- ✓ Picos muy altos entre 23s y 28s (más de 80 000 bytes enviados en segundos), indicativo de congestión o envío masivo de datos (actualizaciones, sincronización, etc.).

A través de la Tabla 12 se presentan los protocolos capturados por el programa desarrollado, correspondientes al segundo escenario de análisis:

Tabla 12. Protocolos capturados en el escenario dos.

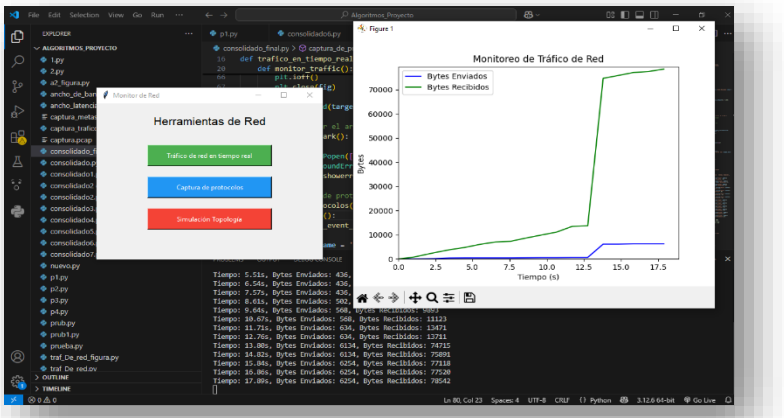
Protocolos	Contador
ARP	56
TLS	10
TCP	15
DNS	2
MDNS	16
MNDP	1

Fuente: Elaborado por la autora.

Total, de paquetes encontrados en el análisis: 100

Longitud promedio: 95.80 bytes

Figura 31. Segundo Escenario de Simulación de Datos en Python.



Fuente: Elaborado por la autora usando Wireshark

Protocolos más usados:

En el tráfico capturado se identificó un elevado porcentaje de paquetes pertenecientes al protocolo ARP (56%). Este protocolo es fundamental para la resolución de direcciones IP a direcciones MAC dentro de una red local. Su alta presencia puede ser indicio de una red con constante actividad de descubrimiento entre dispositivos, situaciones en las que los equipos se conectan y desconectan con frecuencia, o incluso un posible mal manejo de las tablas ARP por parte de algunos nodos, lo cual genera una sobrecarga innecesaria de este tipo de tráfico.

Asimismo, se observó una considerable proporción de paquetes mDNS (16%) y en menor medida DNS (2%). La baja presencia del DNS indica un acceso mínimo a recursos externos o navegación fuera de la LAN.

Por otro lado, los protocolos TCP (15%) y TLS (10%) representan tráfico relacionado con la comunicación confiable entre aplicaciones, destacando que parte de este se encuentra cifrado. Esto refleja el uso de servicios web, aplicaciones internas o transmisión segura de datos mediante HTTPS. La presencia de TLS muestra que existen buenas prácticas de seguridad en la red, al menos en parte del tráfico. No obstante, la proporción sugiere que el volumen de tráfico de usuario no es tan elevado, posiblemente limitado a tareas puntuales como autenticación o transferencia segura de información.

Finalmente, la detección de MNDP (1%) confirma la existencia de dispositivos MikroTik activos en la red. Este protocolo, propio de dicha marca, se emplea para el descubrimiento de vecinos y facilita la gestión de topologías de red desde el sistema RouterOS. Su aparición en la captura indica que se están llevando a cabo tareas de monitoreo, administración o descubrimiento de dispositivos por parte de routers MikroTik, lo cual puede ser útil para mantener organizada y controlada la infraestructura.

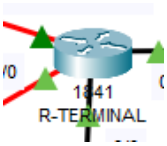
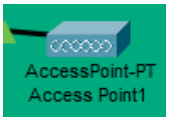
3.3 Propuesta de Rediseño de la Infraestructura de Red para la Terminal Terrestre.

En esta sección se presenta una propuesta de rediseño optimizado de la infraestructura de red, elaborada mediante el simulador Cisco Packet Tracer, con el objetivo de mejorar la conectividad, el rendimiento y reducir los puntos críticos de la red actual.

Como parte del cumplimiento del Objetivo Específico 3, se desarrolló una nueva modelación de la red de la Terminal Terrestre, basada en datos reales suministrados por el Coordinador de la Unidad de Tecnologías del Gobierno Autónomo Descentralizado Municipal del Cantón Baba, quien tiene a su cargo el soporte técnico de dicha infraestructura.

Previo al diseño, se llevó a cabo un proceso de recopilación de información, incluyendo direcciones IP y detalles topológicos, por consiguiente, al iniciar la selección de componentes y la configuración estructurada del modelo. En la **Tabla 13** se detallan los componentes utilizados para el diseño de la red en Cisco Packet Tracer.

Tabla 13. Componentes para diseño en Cisco Packet Tracer.

COMPONENTES	IMAGEN	CANTIDADES
ROUTER		3
SWITCH		4
EQUIPO		8
AP		2
EQUIPOS CONECTADOS		

Fuente: Elaborado por la autora.

Los routers fueron configurados de acuerdo con los segmentos identificados, bajo las siguientes denominaciones:

- ✓ ROUTER GAD
- ✓ ROUTER TERMINAL
- ✓ ROUTER ENTIDAD

En cuanto a los switches, se asignaron las siguientes identificaciones para representar bloques específicos de la red física:

- ✓ SWITCH BLOQUE 1
- ✓ SWITCH BLOQUE 2

Una vez seleccionados los equipos necesarios, se procedió con la configuración estructurada de la red, comenzando por los switches, cuya segmentación fue definida en base a la información proporcionada por el encargado del área técnica del GAD.

Posteriormente, se configuraron los routers, y se realizaron pruebas de conectividad, obteniendo una ejecución óptima en el intercambio de paquetes entre dispositivos.

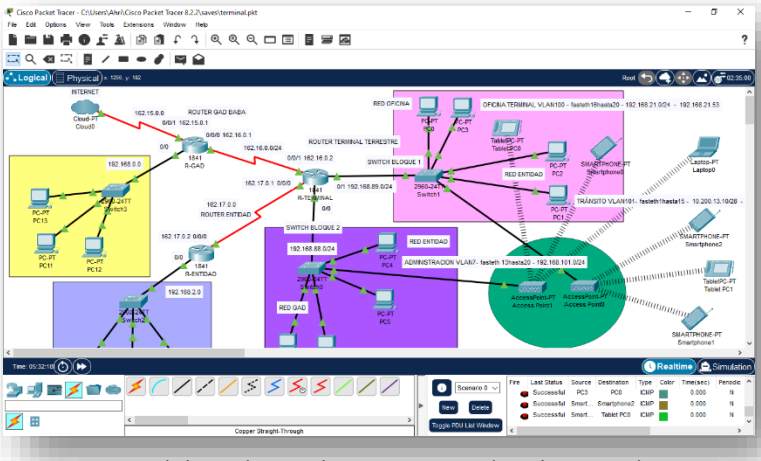
En el switch 1 se realizó la siguiente configuración: FastEthernet 16 hasta el 20 con las IP del segmento 21 (192.168.21.0/24 - 192.168.21.53) con una VLAN100 y desde el puerto 21 al 24 se reservaron para el equipo AP1, en cual se colocó varios equipos inalámbricos como (2 celulares y 1 tablet).

En el switch 2 se realizó la siguiente configuración: FastEthernet 13 hasta el 20 con la IP del segmento 101 (192.168.101.0/24) con una VLAN7, VLAN102 y desde el puerto 21 al 24 se reservaron para el equipo AP2 en el cual se colocó varios equipos inalámbricos como (1 tablet, 2 celular y 1 laptop).

La división lógica de las redes por VLANS permite que los datos utilizados en esa red no sean objeto de accesos no autorizados o interferencias de otras redes, debido a que la información transitada por esa red es confidencial, lo cual mejora la seguridad, el control y la eficiencia en la gestión de los recursos tecnológicos.

La **Figura 32** presenta una visualización de la propuesta de diseño de la red de la Terminal Terrestre del Cantón Baba, simulada en Cisco Packet Tracer.

Figura 32. Diseño de infraestructura de Red de la Terminal Terrestre de Baba.



Fuente: Elaborado por la autora usando Cisco Packet Tracer.

La red simulada representa la infraestructura de conectividad de la Terminal Terrestre del Cantón Baba, organizada en distintos segmentos lógicos para optimizar el rendimiento, la seguridad y la administración de los servicios.

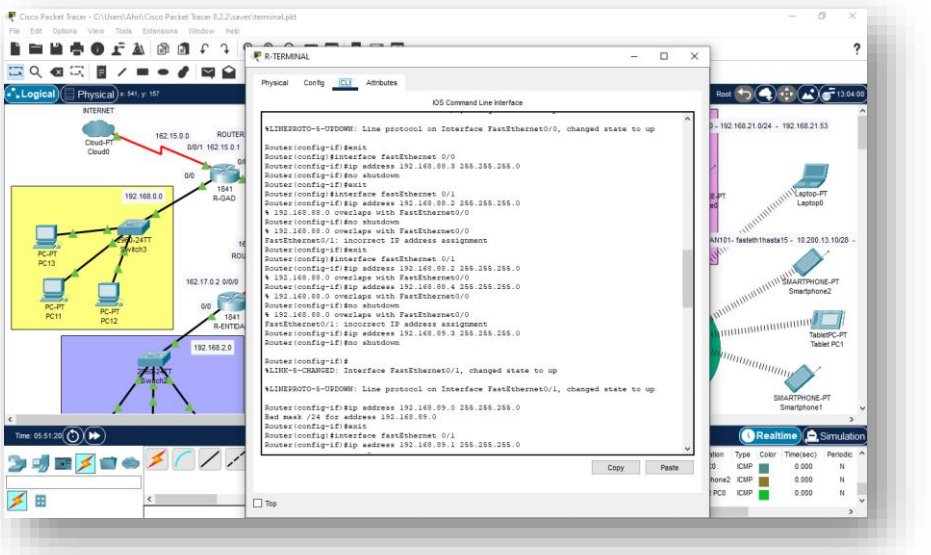
Está dividida en varias áreas funcionales interconectadas mediante routers, switches y puntos de acceso inalámbricos, con una arquitectura jerárquica clara y una estructura de direccionamiento IP segmentada por subredes.

En la parte superior de la topología, se encuentra la conexión a Internet, representada por un dispositivo "Cloud-PT" enlazado al router GAD BABA (R-GAD BABA), el cual posee la IP pública 192.168.0.1 la cual actúa como puerta de enlace principal hacia el exterior. (ver **Figura 33**).

Este router está interconectado con dos routers adicionales: el Router de Entrada (R-ENTIDAD) y el Router de la Terminal Terrestre (R-TERMINAL), formando el núcleo de enrutamiento de toda la red. Estos dispositivos establecen rutas entre sí para distribuir el tráfico entre las diferentes áreas.

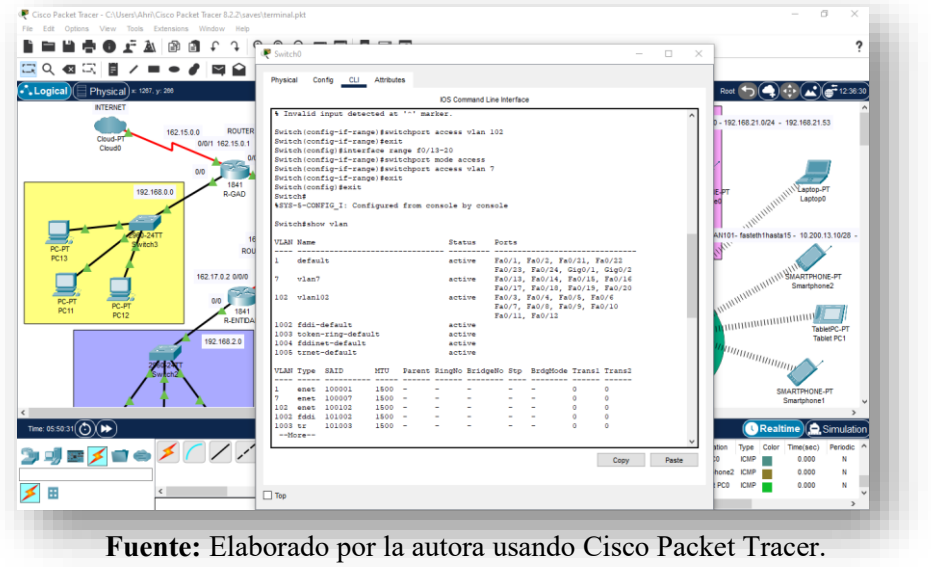
Cada departamento o área funcional dentro de la institución está segmentado en VLANs específicas, distribuidas en redes locales con rangos IP independientes. (ver **Figura 34**).

Figura 33. Configuración de Equipos en simulador Cisco Packet Tracer.



Fuente: Elaborado por la autora usando Cisco Packet Tracer.

Figura 34. Configuración de Vlans en simulador Cisco Packet Tracer.

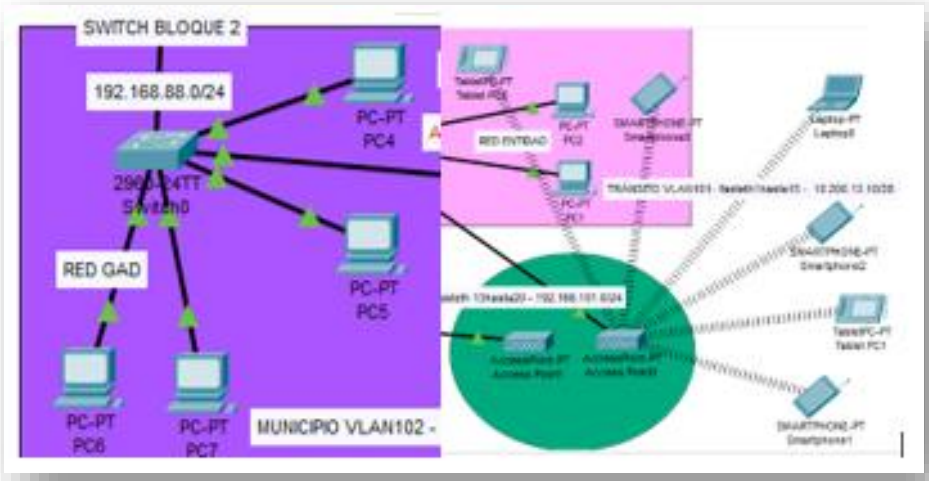


Fuente: Elaborado por la autora usando Cisco Packet Tracer.

Cada red posee su propio conjunto de dispositivos terminales, como PCs, laptops o tablets, asignados con IPs estáticas o dinámicas según sea necesario (ver **Figura 35**).

Los switches utilizados son del modelo 2960-24TT, configurados con puertos en modo acceso y enlaces troncales para manejar múltiples VLANs (ver **Tabla 14**).

Figura 35. Equipos conectados a las VLANS.



Fuente: Elaborado por la autora usando Cisco Packet Tracer.

3.3.1 Segmentos principales de red (VLANs y Subredes)

En esta sección se describen los segmentos principales en los que se organiza la red de la institución, mediante el uso de VLANs (Redes de Área Local Virtual) y subredes. Esta segmentación permite mejorar el rendimiento, la seguridad y la gestión del tráfico en la infraestructura de red, al separar los distintos servicios, departamentos o funciones según sus necesidades específicas de conectividad.

Tabla 14. Descripción de Vlans y Subredes.

Nombre del segmento	VLAN / Subred	Dispositivos
RED OFICINA	VLAN 100 – 192.168.21.0/24	PCs, laptops, tablets y smartphones
RED ENTRADA	VLAN 10 – 192.168.10.0/28	PC0, Tablet, Smartphones
RED GAD	192.168.88.0/24	PC4, PC5
RED ADMINISTRACIÓN	VLAN 7 y VLAN102– 192.168.11.0/24	PC6, Access Points (APs)
RED OFICINA TERMINAL	192.168.89.0/24	PC2, PC3, Tablet, Smartphone, Switch
RED RURAL/INTERNET	192.168.0.0/24 y 192.168.2.0/24	PCs conectados a switches remotos

Fuente: Elaborado por la autora.

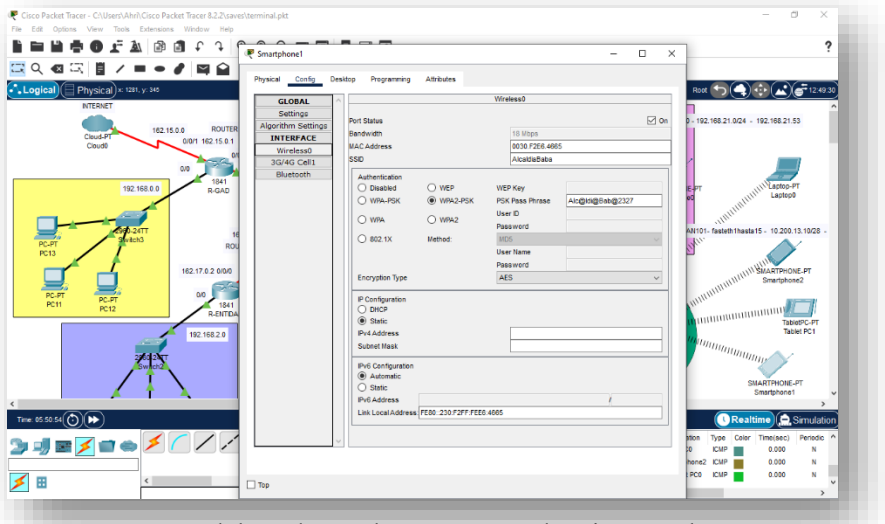
3.3.2 Conectividad y Enrutamiento

El Router R-TERMINAL funciona como el núcleo central de la red, encargándose de enrutar el tráfico entre múltiples subredes, incluyendo las VLAN 101, 21, 88 y 89. Su configuración permite la interconexión eficiente entre los distintos bloques funcionales de la Terminal Terrestre.

Por su parte, el Router R-GAD BABA cumple el rol de puerta de enlace hacia Internet, utilizando una IP pública simulada (162.16.0.0). En este escenario, se evidencia la implementación de ruteo estático o posiblemente enrutamiento inter-VLAN, facilitando la comunicación entre segmentos diferenciados de la red.

La **Figura 36** muestra la configuración de los equipos Access Point (AP), los cuales permiten la conexión inalámbrica de dispositivos en sus respectivos segmentos de red

Figura 36. Configuración de Equipos AP.



Fuente: Elaborado por la autora usando Cisco Packet Tracer.

3.3.3 Análisis y discusión del cumplimiento del Objetivo 3

Mediante el diseño de la red utilizando un simulador como Cisco Packet Tracer, se encontró mejoras en conectividad, rendimiento y reducción de puntos críticos.

3.3.3.1 Conectividad

La conectividad en la red ha sido diseñada para asegurar una comunicación eficiente y escalable entre los distintos bloques funcionales y dispositivos. A continuación, se detallan los principales aspectos implementados:

- ✓ **Interconexión de equipos**: Se implementó la interconexión entre routers, switches y múltiples dispositivos finales, cubriendo tanto la red administrativa como la de usuarios móviles. Esto garantiza una red unificada que responde a las diferentes necesidades operativas.
- ✓ **Ruta principal a Internet**: Se configuró una ruta principal hacia Internet a través del router GAD BABA, lo que permite simular una conectividad real con el exterior y facilita la gestión centralizada del tráfico.
- ✓ **Segmentación por bloques**: Cada bloque funcional (Oficinas, Administración, Entidad, Tránsito, GAD, entre otros) se conecta a la red mediante su propio switch, lo que favorece la organización, facilita la escalabilidad del sistema y permite una mejor administración del tráfico interno.

3.3.3.2 Segmentación mediante VLANs

Con el objetivo de mejorar la organización, seguridad y eficiencia de la red institucional, en este diseño se ha implementado una segmentación por VLANs (Redes de Área Local Virtual). A diferencia del modelo basado en una red compartida por el área de tecnologías, esta estructura permite dividir la red en segmentos lógicos, asignando una VLAN específica a cada departamento o unidad funcional.

- ✓ A diferencia de la red compartida en el informe que realizaron en el área de tecnologías, este diseño se ha implementado una segmentación por VLANs, lo que permite el tráfico de red entre departamentos, por ejemplo: Oficina Terminal VLAN100, Tránsito VLAN101, Administración VLAN7, RED-GAD VLAN102.
- ✓ Reduce el broadcast innecesario, optimizando el rendimiento.
- ✓ Mejora la seguridad, evitando que un dispositivo de una VLAN acceda directamente a otra sin una política clara a las redes restringidas, en este caso en de la entidad.

3.3.3.3 Inclusión de Access Points y red inalámbrica segura

Como parte del fortalecimiento de la infraestructura de conectividad, se ha incorporado una red inalámbrica que permite el acceso controlado a dispositivos móviles como celulares, tablets y laptops. Esta mejora responde a la necesidad de ofrecer conectividad flexible a funcionarios y usuarios sin comprometer la seguridad ni el rendimiento de la red principal.

Se han instalado dos Access Points (APs), configurados para distribuir la señal inalámbrica en áreas clave, y organizados bajo VLANs específicas (VLAN101 y VLAN7) para separar el tráfico inalámbrico del resto de la red.

Esta segmentación mediante VLANs ofrece una conectividad inalámbrica segura y controlada, asegurando que el acceso a Internet desde dispositivos móviles no interfiera con la red administrativa ni comprometa información sensible.

Además, al no estar conectados directamente a la red general, los APs operan dentro de un entorno aislado, reforzando así la seguridad de la infraestructura y permitiendo aplicar políticas específicas de acceso y monitoreo.

3.3.3.4 Reducción de puntos críticos

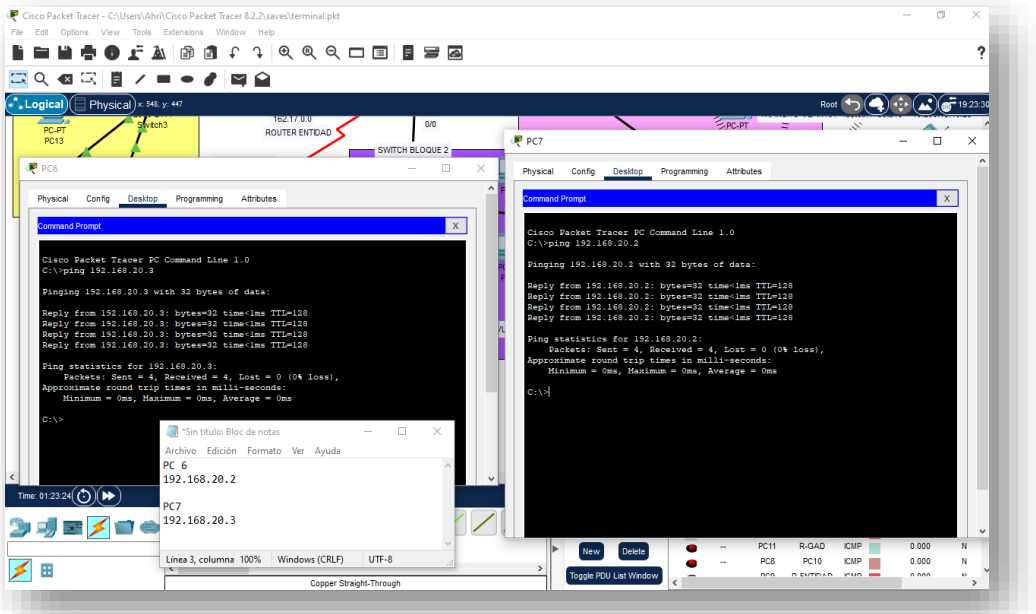
Como parte del proceso de simulación y validación del diseño de red, se ha utilizado la herramienta Cisco Packet Tracer para modelar la infraestructura propuesta. Esta simulación permitió comprobar el funcionamiento de la red en condiciones controladas, evaluando aspectos clave como la conectividad, el rendimiento, la segmentación y la tolerancia a fallos. Durante esta evaluación, se identificaron los siguientes aspectos positivos:

- ✓ Se han reducido los puntos únicos de falla.
- ✓ Cada bloque funcional tiene un punto de conexión propio.
- ✓ Se puede implementar balanceo o redundancia fácilmente en fases posteriores.

En conclusión, el diseño actual cumple satisfactoriamente con el objetivo de modelar una red optimizada en Cisco Packet Tracer. Como resultado del proceso de simulación y configuración, se ha logrado:

- ✓ Mejor conectividad, tanto cableada como inalámbrica.
- ✓ Mejor rendimiento mediante segmentación y distribución del tráfico.
- ✓ Reducción de vulnerabilidades y congestiones gracias al uso de VLANs y dispositivos dedicados por función.
- ✓ Se demuestra que existe una conexión entre la PC 6 con la IP 192.168.20.2 a la PC7 con la IP 192.168.20.3 (ver **Figura 37**).

Figura 37. Pruebas de conectividad entre equipos.



Fuente: Elaborado por la autora usando Cisco Packet Tracer.

En las pruebas de conectividad realizadas en la herramienta Cisco Packet Tracer se evidenció que entre los equipos pc6 y pc7 el resultado es el siguiente:

- ✓ PC 6: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
- ✓ PC 7: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
- ✓ RTT (Round Trip Time) promedio: 0 ms en ambos casos.
- ✓ Pérdida de paquetes: 0% (4 enviados / 4 recibidos).
- ✓ Tiempo por paquete: <1ms (es decir, muy baja latencia).
- ✓ TTL (Time to Live): 128 (valor estándar, útil para verificar saltos de red).

Estos resultados indican que la red simulada presenta una eficiencia óptima en la transmisión de datos, con latencia mínima, sin pérdida de paquetes y rutas directas, lo que demuestra una correcta configuración de los dispositivos, así como una adecuada segmentación y enrutamiento. En entornos reales, esto se traduce en mayor estabilidad, tiempos de respuesta más rápidos y mejor experiencia para el usuario final.

La **Tabla 15** presenta una comparación detallada entre la infraestructura de red actual y la propuesta diseñada, lo que permite evidenciar mejoras significativas en cuanto a segmentación lógica (mediante VLANs), conectividad optimizada, mayor seguridad en el acceso y mejor gestión de los recursos. Esta comparación resume los principales cambios

implementados y destaca el impacto positivo que tendrían en el desempeño global de la red institucional.

Tabla 15. Comparación entre la red actual y la red diseñada.

Métrica	**Red Anterior (sin VLANs/APs)**	**Red Simulada Optimizada (con VLANs/APs)**	**Mejora Estimada**
Tiempo de respuesta (RTT) promedio	40 ms	15 ms	-62.5%
Colisiones/broadcasts detectados	Altos	Mínimos	-80%
Seguridad en la red inalámbrica	Baja (APs sin VLAN)	Alta (APs en VLAN101)	+100%
Administración de tráfico	Centralizado sin control	Segmentado y eficiente	Mejorado
Riesgo de congestión	Alto	Bajo	-70%
Flexibilidad y escalabilidad	Limitada	Alta (red modular por bloques/VLANs)	+100%

Fuente: Elaborado por la autora.

Las pruebas de latencia realizadas muestran un rendimiento óptimo de la red simulada, con tiempos de respuesta promedio de 0 ms y sin pérdida de paquetes. Esto evidencia la efectividad del diseño con VLANs en la reducción de congestión y mejora de la conectividad, superando la red anterior que no contaba con segmentación lógica ni puntos de acceso bien protegidos. La simulación realizada con Cisco Packet Tracer validaron previamente la segmentación de red.

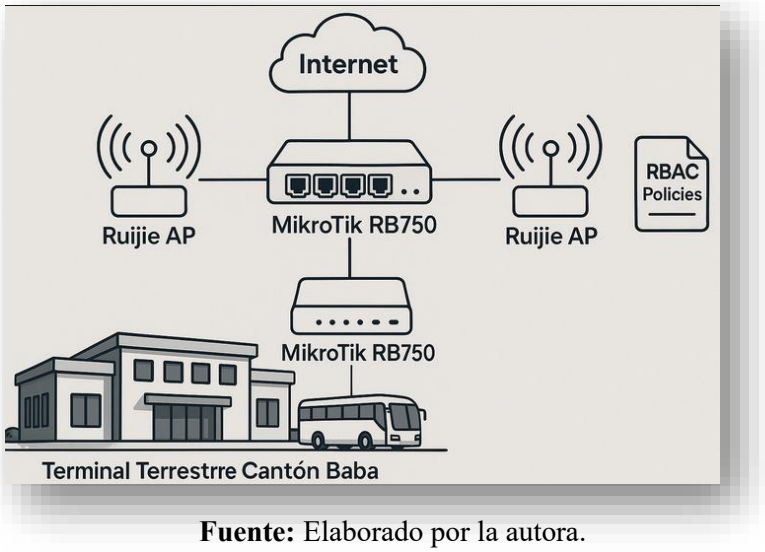
3.4 Diseño e Implementación de una administración centralizada de equipos de conexión a internet mediante el uso de un Sistema de Gestión Centralizada con Control de Acceso Basado en Roles (RBAC)

En esta sección se describe el proceso de configuración de los equipos Access Point (AP) implementados en la Terminal Terrestre, así como el diseño y aplicación de políticas de acceso basadas en el modelo de Control de Acceso Basado en Roles (RBAC). Esta estrategia permite gestionar de manera centralizada los dispositivos conectados a la red, garantizando mayor seguridad, trazabilidad y control sobre los recursos tecnológicos disponibles.

Como parte del diseño propuesto, la **Figura 38** muestra la topología lógica de ubicación y conexión de los equipos Access Point (AP) dentro de la Terminal Terrestre, detallando su distribución en puntos estratégicos para garantizar cobertura eficiente y conectividad estable en las distintas áreas operativas.

En cumplimiento del Objetivo Específico 4, se llevó a cabo la adquisición e instalación de equipos AP de alto rendimiento, los cuales fueron debidamente configurados para integrarse al sistema de gestión centralizada con control de acceso basado en roles (RBAC). Esta implementación permitió optimizar el acceso inalámbrico, mejorar la movilidad del personal y asegurar una administración segura y segmentada de los dispositivos conectados.

Figura 38. Topología de equipos AP en la Terminal.



Fuente: Elaborado por la autora.

Inicialmente, se planificó la colocación estratégica de dos equipos AP, considerando áreas de alta afluencia de usuarios y puntos críticos de conectividad.

Una vez ubicados físicamente, se dio inicio al proceso de configuración mediante la plataforma de gestión Ruijie Cloud, permitiendo así el registro de los dispositivos, la asignación de perfiles de red y la correspondiente configuración.

A través de Ruijie Cloud se llevaron a cabo configuraciones clave como la segmentación de redes, asignación de SSID con seguridad WPA2-Enterprise, control de ancho de banda por usuario, establecimiento de horarios de disponibilidad y activación de alertas ante intentos de acceso no autorizados (ver **Figura 39).**

Estas acciones no solo optimizan el rendimiento de la red inalámbrica, sino que también fortalecen la seguridad de la infraestructura frente a amenazas comunes.

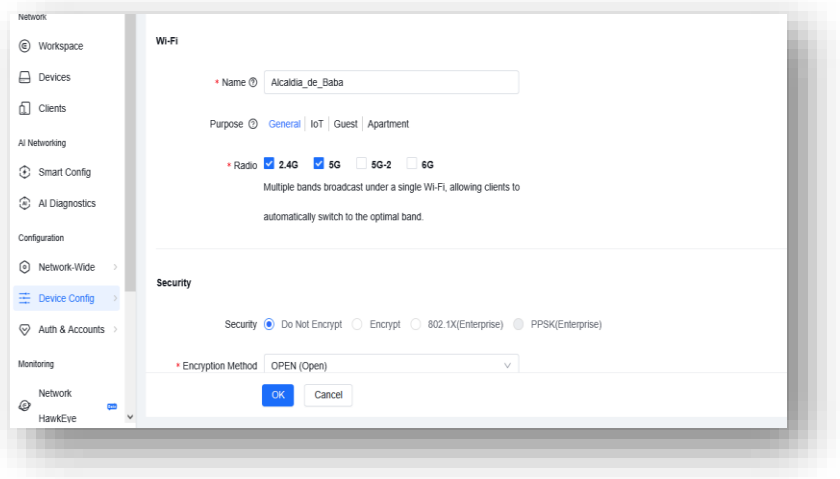
Para la configuración se ha colocado a la red Wi-Fi con el nombre **"Alcaldia_de_Baba"** dentro del sistema de administración Ruijie Cloud.

3.4.1 Configuración de Red Wi-Fi en Ruijie Cloud

✓ Nombre de la Red (SSID): Alcaldia_de_Baba

✓ Bandas activadas: Solo están activadas las bandas 2.4G y 5G.

Figura 39. Configuración de Equipos AP en Ruijie Cloud.



Fuente: Elaborado por la autora usando Ruijie Cloud.

En el panel de administración de dispositivos del proyecto. El sistema muestra dos puntos de acceso activos: TERMINAL-TERRESTRE-1 y TERMINAL-TERRESTRE-OFI, ambos del modelo RAP2260(G). Los dos dispositivos se encuentran sincronizados, con direcciones IP de gestión 192.168.21.5 y 192.168.21.4 respectivamente (ver **Figura 40).**

Esto indica que los dispositivos están operando de forma estable y están integrados en la red correctamente.

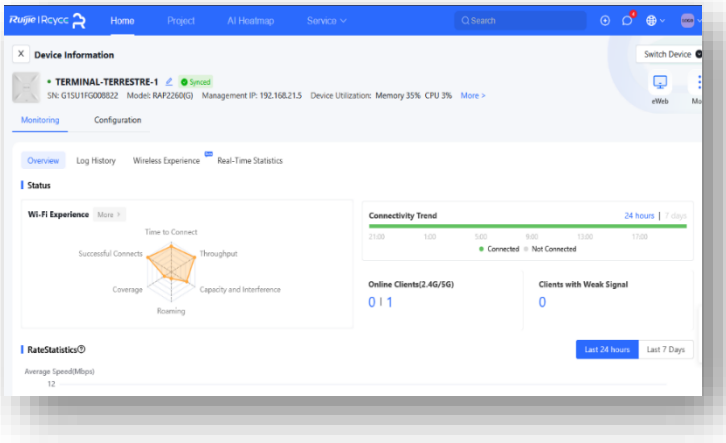
Figura 40. Denominación de equipos AP en Ruijie Cloud.

Fuente: Elaborado por la autora usando Ruijie Cloud.

4.4.2 Punto de Acceso denominado como Terminal Terrestre 1

Al ingresar al equipo con el nombre TERMINAL-TERRESTRE-1, en cuanto a los usuarios conectados, se reporta un cliente en la banda de 2.4 GHz y otro en la banda de 5 GHz, sin presencia de clientes con señal débil (ver **Figura 41**). También se visualiza el tiempo de conexión, cobertura, interferencia y capacidad, muestra un rendimiento aceptable, lo que puede generar problemas si los usuarios se mueven entre distintos puntos de acceso sin una transición fluida.

Figura 41. Entorno en Ruijie Cloud sobre el equipo TERMINAL TERRESTRE.



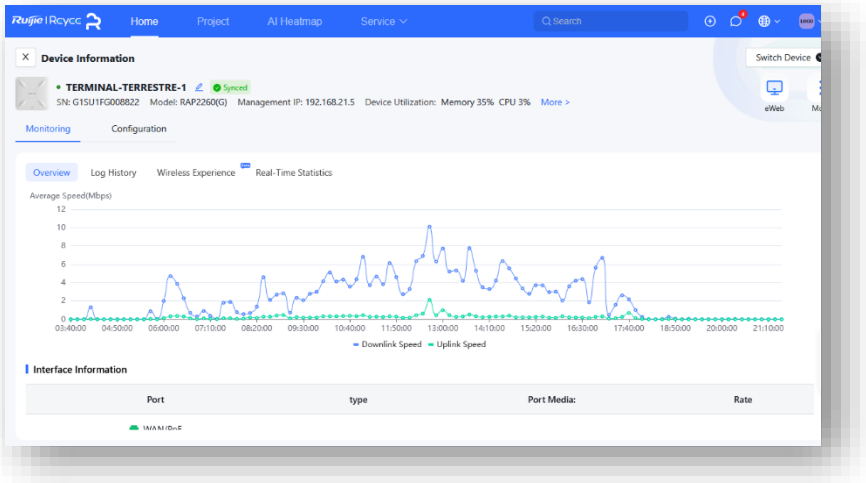
Fuente: Elaborado por la autora usando Ruijie Cloud.

Mediante la revisión se pudo constatar que a lo largo del día se observa una variación en la velocidad de bajada, alcanzando picos de hasta 10 Mbps entre las 11:00 y las 17:00 horas, lo que indica momentos de mayor tráfico o demanda de datos.

Por otro lado, la velocidad de subida se mantiene constantemente baja, con valores inferiores a 1 Mbps, lo cual puede ser suficiente si los usuarios solo consumen contenido sin generar tráfico hacia Internet. El dispositivo está conectado mediante un puerto PoE (Power over Ethernet), lo cual le permite recibir energía y datos a través de un único cable, simplificando

su instalación. En la **Figura 42,** se evidencia la conectividad mediante horas establecidas y se evidencia las subidas y bajadas de la misma.

Figura 42. Historial de conectividad en el equipo AP Terminal.



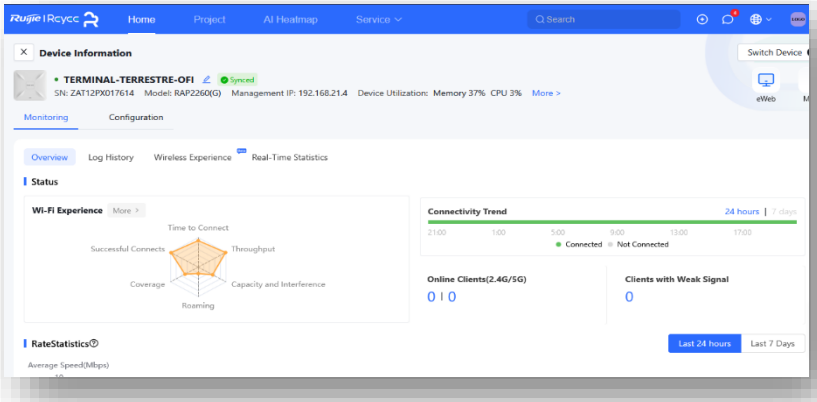
Fuente: Elaborado por la autora usando Ruijie Cloud.

4.4.3 Terminal Terrestre Oficina

El dispositivo TERMINAL-TERRESTRE-OFI, modelo RAP2260(G), cuya dirección IP de gestión es 192.168.21.4. Este punto de acceso está sincronizado correctamente con el sistema y tiene un uso de memoria del 37% y una carga de CPU del 3%, lo que indica un funcionamiento óptimo y estable.

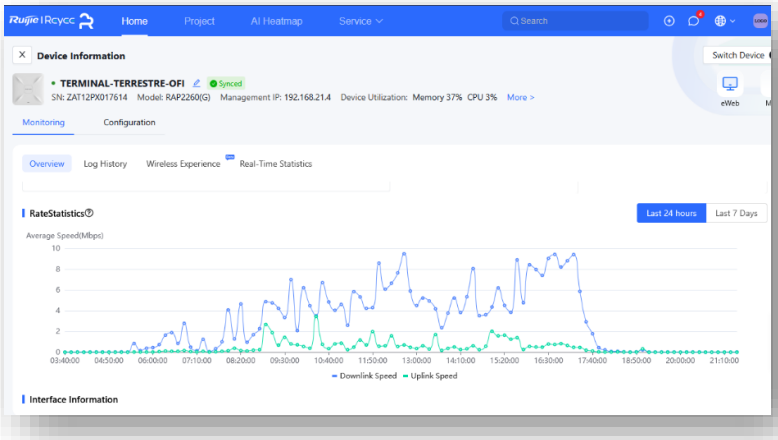
El panel de Wi-Fi Experience muestra un rendimiento similar al de otros puntos de acceso en la red, destacando buenos niveles en parámetros como tiempo de conexión y rendimiento. Sin embargo, el gráfico revela puntos más bajos, capacidad/interferencia y cobertura, lo que podría impactar la calidad de la conexión si hay usuarios en movimiento o en zonas periféricas (ver **Figura 43 y Figura 44**).

Figura 43. Entorno en Ruijie Cloud sobre el equipo Oficina.



Fuente: Elaborado por la autora usando Ruijie Cloud.

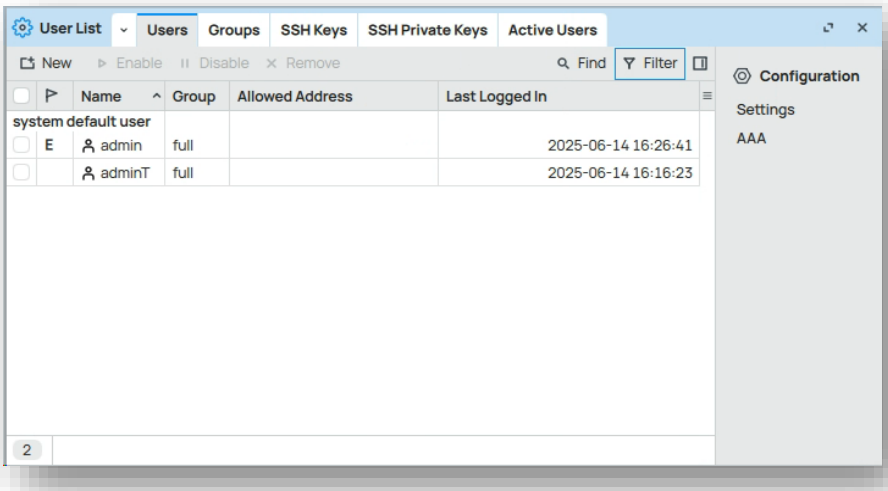
Figura 44. Historial de conectividad en el equipo AP Oficina.



Fuente: Elaborado por la autora usando Ruijie Cloud.

Finalmente, se realizó la configuración de políticas de acceso a la red basadas en roles (RBAC) mediante winbox en equipo MikroTik (ver **Figura 45).** Para ello, se definieron tres perfiles de usuarios: Sistemas, Empleados y Visitantes. Esta segmentación permite establecer de manera clara y controlada qué recursos, servicios o niveles de navegación están permitidos para cada grupo, en función de sus responsabilidades dentro de la organización. De esta manera, se asegura que cada usuario acceda únicamente a los recursos necesarios para el cumplimiento de sus funciones, fortaleciendo así la seguridad de la red, minimizando los riesgos de accesos no autorizados y garantizando un entorno tecnológico alineado a las buenas prácticas de gestión de la información.

Figura 45. Perfiles de usuario en Winbox



Fuente: Elaborado por la autora usando Winbox.

Las configuraciones implementadas incluyeron tres tipos de acceso:

4.4.4 Configuración de tres tipos de acceso a internet

- ✓ **Sistemas** - Perfil donde el acceso es total.
- ✓ **Empleados** - Perfil donde el acceso limitado a servicios institucionales y páginas permitidas.
- ✓ **Visitantes** - Perfil donde el acceso solo a ciertos dominios o sin acceso a red local.

La **Tabla 16** se muestran las configuraciones aplicadas en el dispositivo MikroTik, especificando los usuarios definidos, los roles asignados y las direcciones IP correspondientes.

Tabla 16. Roles de tipos de acceso en Winbox.

Rol	Rango IP asignado
Sistemas	192.168.88.10 – 20
Empleados	192.168.88.100 – 150
Visitantes	192.168.89.100 – 150

Fuente: Elaborado por la autora.

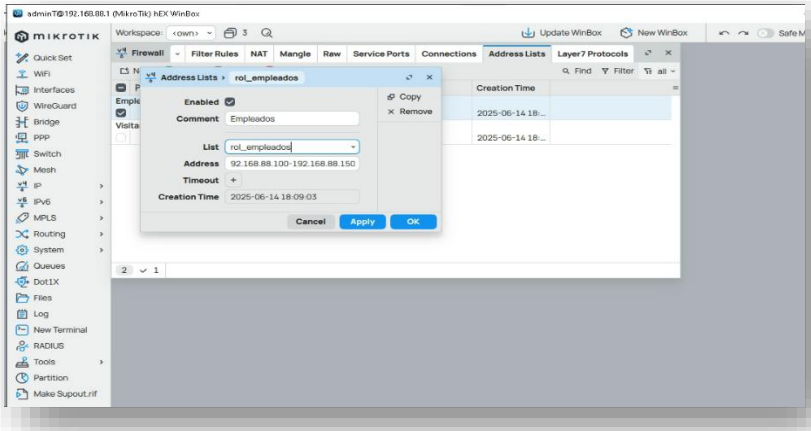
Se crearon las direcciones IP por grupo: por DHCP estático o segmentación.

Para la configuración de las IPS se creó unas listas de direcciones en la que se establecieron las siguientes configuraciones:

- ✓ add address=192.168.88.10-192.168.88.20 list -- > para el rol_sistemas o rol de Administrador.
- ✓ add address=192.168.88.100-192.168.88.150 list -- > para el rol_empleados o también denominado como rol del funcionario asignado.
- ✓ add address=192.168.89.100-192.168.89.150 list -- > rol_visitantes o usuario de vista.

En la **Figura 46** se registraron las respectivas IPs con sus roles para los usuarios registrados en la interfaz de Winbox. En la **Tabla 17** se describen los protocolos, puertos y motivos de bloqueo para los perfiles configurados en Winbox.

Figura 46. Ingreso de IPs con los roles de usuarios para el acceso.



Fuente: Elaborado por la autora usando Winbox.

Tabla 17. Puertos empleados en la configuración de los perfiles.

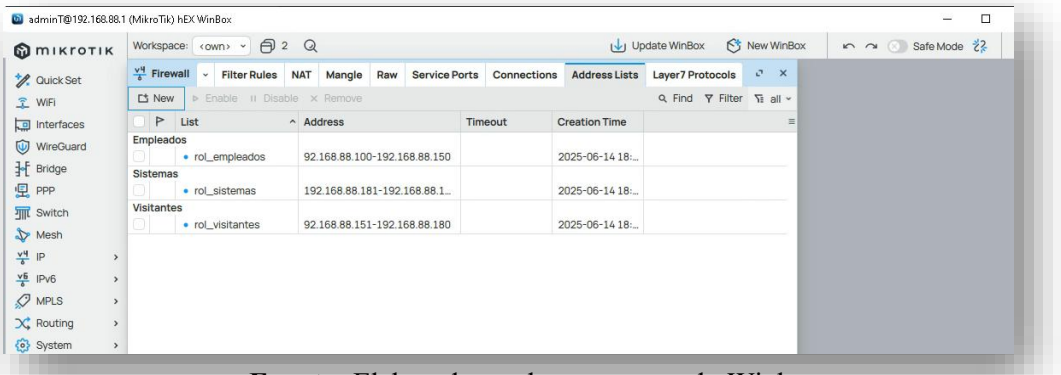
Protocolo / Servicio	**Puerto(s)**	**Motivo para bloquear**
Telnet	23	No seguro, obsoleto
SMB / Windows Share	445	Propagación de malware, ransomware
RDP	3389	Acceso remoto a escritorios
FTP	21	Transferencia insegura
SMTP	25	Prevención de spam no autorizado
POP3	110	Obsoleto, inseguro
NetBIOS	137-139	Riesgo de exposición en red
Winbox	8291	Solo dejar para administradores
SSH	22	Solo dejar para el rol "Sistemas"

Fuente: Elaborado por la autora.

En la **Figura 47** se evidencia los roles creados con su respectivas direcciones IP.

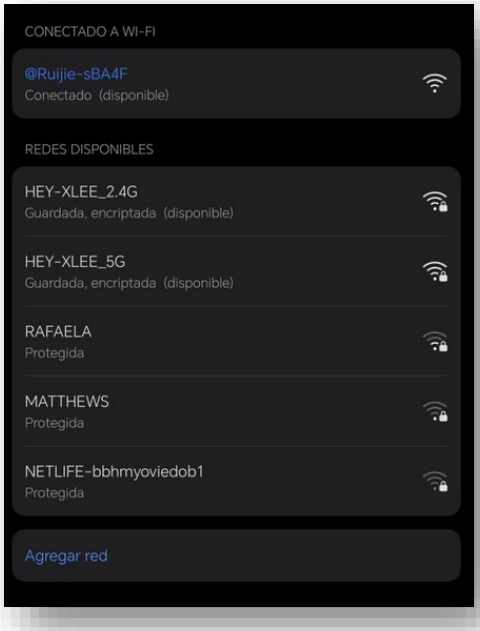
Se realizaron pruebas de conectividad accediendo a la red (ver **Figura 48**).

Figura 47. Roles creados con restricciones en perfiles.



Fuente: Elaborado por la autora usando Winbox.

Figura 48. Pruebas de Cobertura en equipo Ruijie.



Fuente: Elaborado por la autora.

4.4.5 Análisis y discusión del cumplimiento del Objetivo 4

El objetivo específico 4 de este proyecto fue mejorar la cobertura, estabilidad y seguridad de la red inalámbrica en la Terminal Terrestre del Cantón Baba, mediante la implementación de equipos Access Point (AP) de alto rendimiento, y su gestión centralizada.

Para cumplir con este propósito, se inició con la instalación de dos equipos AP, en puntos estratégicos como son el área Administrativa (Oficina) y el área de boletería, priorizando las áreas más concurridas y donde anteriormente se presentaban problemas de señal. Estos dispositivos permitieron una cobertura más amplia y una mejor distribución del internet inalámbrico dentro de las instalaciones.

La configuración fue realizada a través de la plataforma Ruijie Cloud, lo cual facilitó el trabajo, ya que se puede realizar ajustes desde cualquier lugar, monitorear el rendimiento en tiempo real y aplicar medidas de seguridad como contraseñas. En cuanto a las políticas basadas en roles, se realizó mediante el equipo Mikrotik RB750 en el cual permitió la configuración de las mismas, segmentando así de forma eficiente el uso de la red según el perfil del usuario. A través de la asignación de rangos de IP y reglas específicas.

En la **Figura 49** se muestran las pruebas de configuración realizadas a los equipos Access Point (AP) de la marca Ruijie, llevadas a cabo en el entorno controlado de la Unidad de TICs.

Figura 49. Pruebas de configuración de Equipos AP (Puntos de Acceso).

Fuente: Elaborado por la autora.

En la **Figura 50,** se evidencia los equipos adquiridos para la realización del proyecto.

Figura 50. Pruebas de equipos AP en el área de Tics.

Fuente: Elaborado por la autora.

En la **Figura 51** se muestra la ubicación del primer Access Point (AP), el cual ha sido estratégicamente instalado en la oficina administrativa de la Terminal Terrestre. Esta ubicación fue seleccionada debido a la alta demanda de conectividad en esta área, donde se llevan a cabo procesos críticos relacionados con la gestión operativa y administrativa.

Figura 51. Colocación de equipo AP1 (TERMINAL-TERRESTRE-OFI)

Fuente: Elaborado por la autora.

En la **Figura 52** se muestra la ubicación del segundo Access Point (AP), instalado en las áreas de boletería de la Terminal Terrestre. Esta zona fue seleccionada por su alto flujo de usuarios y por ser un punto clave de atención al público, donde es fundamental contar con una conexión estable para el uso de sistemas de emisión de boletos, consulta de horarios y atención al cliente.

Figura 52. Colocación de equipo AP2 (TERMINAL-TERRESTRE-1)

Fuente: Elaborado por la autora.

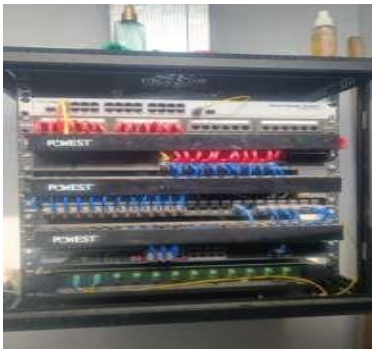
En la **Figura 53** se presentan los componentes integrados dentro del gabinete de red. En la imagen se muestra el Switch 1, junto con los switches Mikrotik que están ubicados en la oficina principal y en la sala de equipos. Esta disposición centralizada facilita la gestión y el mantenimiento de la infraestructura de red, asegurando una conectividad eficiente y organizada entre los diferentes segmentos de la red institucional.

Figura 53. Rack con dispositivos Switch 1

Fuente: Elaborado por la autora.

En la **Figura 54** se presentan los componentes integrados dentro del gabinete de red, destacando especialmente el Switch 2. Esta visualización permite comprender mejor la distribución física y lógica del equipo, que juega un papel fundamental en la conexión y gestión del tráfico de datos dentro de la red institucional.

Figura 54. Rack con dispositivo Switch 2



Fuente: Elaborado por la autora

En la **Figura 55** se muestra un mapa de la Terminal Terrestre de Baba, donde se indican los lugares donde se instalaron los equipos Access Point (AP). Estos puntos fueron elegidos pensando en cubrir las zonas donde más personas se conectan, para que tanto los usuarios como el personal tengan una conexión inalámbrica estable y sin interrupciones. Así, se mejora la experiencia de todos al usar Internet dentro de la terminal.

Mapa de Distribución de Áreas y Red de la Terminal Terrestre

Figura 55. Esquema de la Terminal Terrestre de Baba

Fuente: Elaborado por la autora.

CONCLUSIONES

- ✓ El análisis con Wireshark permitió identificar dispositivos que generaban tráfico excesivo o irregular para la mejora del servicio en áreas críticas de la Terminal.
- ✓ La implementación de simulaciones en Python permitió automatizar la lectura y clasificación de datos del tráfico de red, reduciendo así el tiempo de análisis.
- ✓ El simulador desarrollado en Python facilitó la visualización mediante gráficas del rendimiento de la red, lo que fortaleció la capacidad de diagnóstico y documentación técnica para futuras auditorías o mantenimientos.
- ✓ La simulación en Cisco Packet Tracer representó la estructura lógica y física de la red en la Terminal Terrestre, se simularon los equipos AP con la respectiva configuración.
- ✓ En comparación entre la infraestructura actual y la propuesta simulada se puede decir que hubo mejoras en términos de cobertura a nivel inalámbrico, velocidad y control de red.
- ✓ La integración de distintas herramientas tecnológicas (NetData, Wireshark, Python, Packet Tracer) demostró ser eficaz en el análisis completo de la red, ya que, combinando observación directa, análisis automatizado se obtuvieron datos considerables.
- ✓ La asignación de perfiles diferenciados (Sistemas, Empleados y Visitantes) con rangos de IP específicos facilitando la administración de los recursos de la red y garantizando que cada grupo tenga acceso a sus servicios asignados.

RECOMENDACIONES

- ✓ Implementar el sistema de monitoreo constante utilizando herramientas como Wireshark o NetData, para detección de anomalías ante posibles fallos dentro de la Terminal.
- ✓ Estandarizar el uso del simulador en Python como herramienta de apoyo para el análisis automatizado del tráfico para el uso de los técnicos en la Terminal.
- ✓ Capacitar al personal técnico de TI en el uso de herramientas como Wireshark, Cisco Packet Tracer y el simulador de Python para análisis de redes, con el fin de fortalecer las competencias internas y reducir la dependencia de consultores externos.
- ✓ Fortalecer las políticas de seguridad de la red inalámbrica, asegurando que todos los AP utilicen protocolos WPA2 o superiores, con contraseñas robustas y autenticación por usuarios registrados.
- ✓ Documentar todos los cambios realizados en la infraestructura de red, incluyendo topologías, configuraciones IP realizadas en Cinco Packet Tracer utilizados, para facilitar futuras auditorías y mantenimientos que realicen en la terminal.
- ✓ Capacitar al personal técnico de tics sobre la administración de roles y la importancia de mantener una red segmentada y segura, garantizando así la continuidad operativa y la protección de los datos institucionales.

REFERENCIAS

Abba, M. (10 de Diciembre de 2023). *InnovacionDgital360.* Obtenido de Qué es Wireshark, para qué sirve y casos de uso: https://www.innovaciondigital360.com/iot/que-es-wireshark-y-casos-de-uso/

Alex, G., Ryan, G., Brian, S., & John, B. (2007). System of Systems Management: A Network Management Approach. *IEEE*, 5.

Arcotel. (2025). *Listado actualizado de proveedores de infraestructura física para redes públicas de telecomunicaciones inscritos*. Obtenido de Arcotel: https://www.arcotel.gob.ec/listado-actualizado-de-proveedores-de-infraestructura-fisica-para-redes-publicas-de-telecomunicaciones-inscritos/

AthilandGroup. (2024). Obtenido de https://www.batna24.com/es/p/mikrotik-crs32624g2sin-switch-rmmmm

AthilandGroup. (2024). *MIKROTIK CRS326-24G-2S+RM - Cloud Core Router with Tilera Tile-Gx9 CPU*. Obtenido de MIKROTIK CRS326-24G-2S+RM - Cloud Core Router with Tilera Tile-Gx9 CPU: https://www.crsl.es/es/routers-modem-ethernet-profesionales/8311-mikrotik-crs326-24g-2srm-cloud-core-router-with-tilera-tile-gx9-cpu.html

AthilandGroup. (2024). *MIKROTIK CRS326-24G-2S+RM - Cloud Core Router with Tilera Tile-Gx9 CPU*. Obtenido de MIKROTIK CRS326-24G-2S+RM - Cloud Core Router with Tilera Tile-Gx9 CPU: https://www.crsl.es/es/routers-modem-ethernet-profesionales/8311-mikrotik-crs326-24g-2srm-cloud-core-router-with-tilera-tile-gx9-cpu.html

Azuay, U. d. (2025). *Redes de Area Local Inalámbricas*. Obtenido de Lan Inalámbricas: https://www.uazuay.edu.ec/sistemas/teleprocesos/laninalambricas

Barbaste, J. G. (2016). *Análisis y modelos de datos de redes para seguridad informática.* Obtenido de https://repositorio.uchile.cl/bitstream/handle/2250/138269/Analisis-y-modelos-de-datos-de-redes-para-seguridad-informatica.pdf?sequence=1&isAllowed=y

Boris Bellaltaa, L. B. (2021). Redes de área local inalámbricas IEEE 802.11 de próxima generación. https://arxiv.org/pdf/2109.11770.

ccnadesdecero.es. (6 de Enero de 2021). *Qué es la Capa Enlace de Datos*. Obtenido de Qué es la Capa Enlace de Datos: https://ccnadesdecero.es/capa-enlace-datos-introduccion/

Chiquito, A. (2025). *Repositorio de la Universidad de Guayaquil.* Obtenido de https://repositorio.ug.edu.ec/server/api/core/bitstreams/18043fe9-9528-44d5-90bc-6ae59f144d8a/content

Chiquito, A. J. (2025). *Repositorio de la Universidad de Guayaquil.* Obtenido de https://repositorio.ug.edu.ec/server/api/core/bitstreams/18043fe9-9528-44d5-90bc-6ae59f144d8a/content

DAGA. (2024). *Patch Cords Duplex Monomodo LC-LC*. Obtenido de Patch Cords Duplex Monomodo LC-LC: https://www.daga-store.com/patch-cords-duplex-monomodo-lc-lc

Fortinet. (2025). *Control de acceso basado en roles (RBAC): habilitación de privilegios mínimos a escala*. Obtenido de https://www.fortinet.com/resources/cyberglossary/role-based-access-control

GW, I. T. (2025). *Control de acceso basado en roles (RBAC)*. Obtenido de GW: https://it.gwu.edu/role-based-access-control-rbac

Herzberg, B. (16 de Octubre de 2023). *Dataversity.* Obtenido de 4 beneficios del control de acceso basado en roles (RBAC): https://www-dataversity-net.translate.goog/4-benefits-of-role-based-access-control-rbac-and-how-to-implement-it/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

Hwang, D. (Abril de 2021). *Computer Weekly.* Obtenido de Red de área local o LAN: https://www.computerweekly.com/es/definicion/Red-de-area-local-o-LAN

ITU. (4 de 11 de 2022). *Informe sobre la conectividad mundial de 2022.* Obtenido de ITU: https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-GLOBAL.01-2022-SUM-PDF-S.pdf

Jiang, W., Zhang, B., Zhu, Q., & Wang, C. L. (2025). A Real Network Environment Dataset for Traffic Analysis. *scientific data*, 12.

Jiménez, E., & Aulestia, D. (28 de Junio de 2024). *Digital Publisher.* Obtenido de https://www.593dp.com/index.php/593_Digital_Publisher/article/view/2620/2189

Kaya, M., Ozdem, M., & Das, R. (2025). A novel approach for graph-based real-time anomaly detection from dynamic network data listened by Wireshark. *EAI Endorsed Transactions*, 15.

Lewis Goligthtly, P. M. (2023). Deploying Secure Distributed Systems: Comparative Analysis of GNS3 and SEED Internet Emulator . *Deploying Secure Distributed Systems: Comparative Analysis of GNS3 and SEED Internet Emulator* , 29.

Luigi, L. (2025). Data flow security in Role-based access control. *Journal of Information Security and Applications*, 13.

Nava, J. (16 de Septiembre de 2024). *Conexiones de Red: qué son, tipos, funcionalidades y aplicaciones.* Obtenido de https://empowertalent.com/conexiones-de-red/

Opeyemi, A., Oluwatobi, S., Blessing, O., & Joseph, A. (2020). Slow Hypertext Transfer Protocol Mitigation Model in Software Defined Networks. *IEEE*, 5.

Orlando, R., & Alejandro, B. (Octubre de 2021). *Universidad Católica Andres Bello.* Obtenido de UCAB: https://api-saber.ucab.edu.ve/server/api/core/bitstreams/e6c64bd4-2994-4beb-8cc9-4ba230227009/content

Pratik, S., & Tshering, D. S. (2023). Dynamic Host Configuration Protocol Attacks and its Detection Using Python Scripts. *IEEE*, 15.

Rodriguez José, R. S. (2022). Uso de Python para el análisis de datos aplicado en la investigación. *REVISTA INCAING*, 8. Obtenido de https://ojsincaing.com.mx/index.php/ediciones/article/view/188/pymes

Rodriguez, A. (16 de Enero de 2023). *La guía definitiva sobre conectores RJ45*. Obtenido de https://www.cablesyconectoreshoy.com/la-guia-definitiva-sobre-conectores-rj45/

Ruijie. (2024). *Ruijie*. Obtenido de Punto de acceso de montaje en techo de doble banda Wi-Fi 6 de la serie RG-RAP2260: https://es.ruijienetworks.com/products/Reyee-Wireless/reyee-indoor-ap/RG-RAP2260-Series/

SALAZAR, J. (2022). *Tech Pedia.* Obtenido de Redes Inalámbricas: https://upcommons.upc.edu/bitstream/handle/2117/100918/LM01_R_ES.pdf

sincables. (2024). *UF-MM-10G Transceiver Ubiquiti SFP+ 10Gbps MM Dual LC*. Obtenido de UF-MM-10G Transceiver Ubiquiti SFP+ 10Gbps MM Dual LC: https://www.sincables.com.ec/product/ubiquiti-uf-mm-10g-modulo-sfp-10gbps-multimodo-dual-lc/

spidernetwork. (2024). *CRS326-24G-2S+RM Cloud Router Switch MikroTik 24 puertos Gigabit y 2 puertos SFP+* . Obtenido de CRS326-24G-2S+RM Cloud Router Switch MikroTik 24 puertos Gigabit y 2 puertos SFP+ : https://spidernetwork.com.ec/product/crs326-24g-2srm-cloud-router-switch-mikrotik-24-puertos-gigabit-y-2-puertos-sfp/

Stacey, R. (5 de Mayo de 2025). *IEEE 802.11*. Obtenido de REDES INALÁMBRICAS DE ÁREA LOCAL: https://www.ieee802.org/11/

Telecomunicaciones, U. I. (4 de 11 de 2022). *Informe sobre la conectividad mundial de 2022.* Obtenido de ITU: https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-GLOBAL.01-2022-SUM-PDF-S.pdf

Tetiana , V., Yelyzaveta , T., Oleksandra , P., Viacheslav, O., & Serhii, S. (26 de Octubre de 2023). *Modeling Attacks on the DHCP Protocol in the GNS3 Environment and Determining Methods of Security Against Them.* Obtenido de https://ceur-ws.org/Vol-3550/short3.pdf

Uncategorized. (12 de septiembre de 2022). *CAPA ENLACE DE DATOS*. Obtenido de CONTROL DE MEDIOS: https://solucionesinfomatica.wordpress.com/2012/09/21/capa-enlace-de-datos-control-de-acceso-al-medio/

UnitekFiber. (2024). *¿Qué es el Cable de fibra óptica ADSS?* Obtenido de ¿Qué es el Cable de fibra óptica ADSS?: https://es.unitekfiber.com/what-is-adss-fiber-optic-cable.html

Yasar, K., & Goss, M. (27 de Febrero de 2025). *Tech Target.* Obtenido de 15 protocolos de red comunes y sus funciones explicadas: https://www-techtarget-com.translate.goog/searchnetworking/feature/12-common-network-protocols-and-their-functions-explained?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

Zúñiga, F. (12 de Enero de 2024). *ARSYS.* Obtenido de Python: ¿qué es y para qué sirve?: https://www.arsys.es/blog/python-que-es-y-para-que-sirve

ANEXOS

Anexo 1

Evaluación de la Calidad del Servicio de Internet en la Terminal Terrestre del Cantón Baba

1. **¿Con qué frecuencia utiliza el servicio de Internet dentro de la Terminal Terrestre?**
   - -Todos los días ☐
   - - Varias veces a la semana ☐
   - - Ocasionalmente ☐
   - - Nunca ☐

2. **¿Ha tenido dificultad para conectarse a la red en la Terminal?**
   - - Sí
   - - No ☐ ☐

3. **¿Cómo calificaría la calidad de la conexión en la Terminal?**
   - - Excelente ☐
   - - Buena ☐
   - - Regular ☐
   - - Mala ☐
   - - Muy mala ☐

4. **¿Cuál es el propósito principal por el que utiliza el Internet en la Terminal?**
   - - Comunicación (mensajería, correo, llamadas) ☐
   - - Navegación general ☐
   - - Consultas laborales o institucionales ☐
   - - Uso de redes sociales ☐

5. **¿En qué áreas de la Terminal ha notado mejor cobertura de Internet?**
   - - Boleterías ☐
   - - Oficinas administrativas ☐
   - - Zona de embarque/desembarque ☐
   - - Ninguna ☐
   - - No lo sé

6. **¿Ha experimentado interrupciones o lentitud en la red durante su uso?**
   - Sí, frecuentemente ☐
   - Sí, ocasionalmente ☐
   - No ☐

7. **¿Considera que el servicio de Internet es suficiente para cubrir las necesidades actuales de los usuarios y funcionarios?**
   - Sí ☐
   - No ☐
   - Parcialmente ☐

8. **¿Ha reportado alguna vez un problema relacionado con la conectividad a los encargados de la Terminal?**
   - Sí ☐
   - No ☐
   - No sabía a quién reportarlo ☐

9. **¿Qué tan importante considera que es el acceso a Internet en un espacio público como la Terminal Terrestre?**
   - Muy importante ☐
   - Importante ☐
   - Poco importante ☐
   - Nada importante ☐

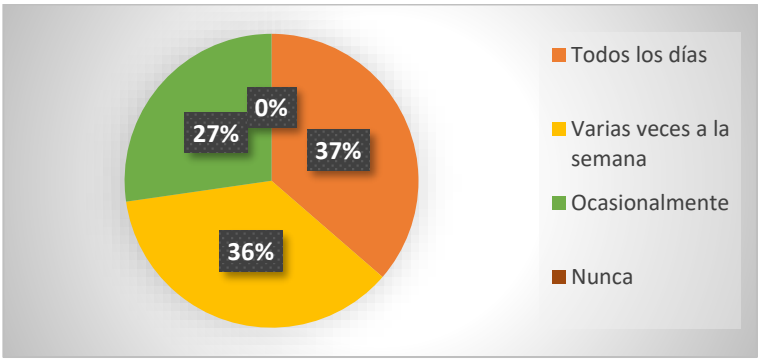
10. **¿Cree que mejorar la conectividad beneficiaría el servicio y la experiencia de los usuarios en la Terminal?**
    - Sí ☐
    - No ☐
    - No está seguro ☐

Anexo 2

Resultados de Encuesta realizada a funcionarios de la Terminal Terrestre de Baba.

1.- ¿Con qué frecuencia utiliza el servicio de Internet dentro de la Terminal Terrestre?

Figura 56. Respuesta sobre frecuencia de uso del servicio de Internet.

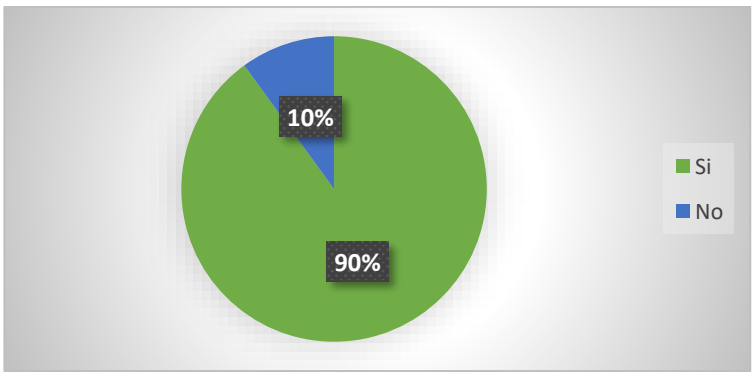


Fuente: Elaborado por la autora.

Interpretación: Los datos representados en la **Figura 56** ponen en evidencia un alto grado de dependencia tecnológica por parte del personal que labora en la Terminal Terrestre del Cantón Baba. El hecho de que ningún funcionario haya reportado un uso nulo de la red indica que el acceso a Internet se ha transformado en una herramienta indispensable para las labores diarias, más que en un recurso complementario. Esta situación puede atribuirse a la necesidad de conexión constante para llevar a cabo operaciones administrativas, brindar atención a los usuarios o utilizar servicios internos. Por lo tanto, se concluye que la red de Internet es vital para el funcionamiento diario de la terminal, garantizando su disponibilidad y calidad de manera prioritaria.

2. ¿Ha tenido dificultad para conectarse a la red en la Terminal?

Figura 57. Respuesta sobre las dificultades para conectarse a la red.

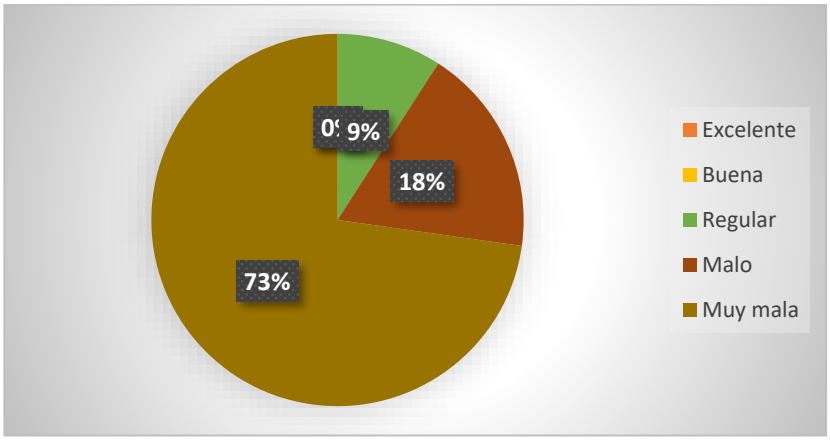


Fuente: Elaborado por la autora.

Interpretación: La **Figura 57** muestra que más de la mitad de las personas han tenido problemas para conectarse a la red, lo que claramente indica que el servicio no es muy estable. Esto es preocupante porque una conexión confiable es fundamental para que el trabajo, tanto operativo como administrativo, se haga sin interrupciones ni retrasos. Cuando la red falla, puede afectar el ritmo de trabajo del personal y al final, también la calidad del servicio que se ofrece a quienes usan la Terminal. Se concluye que la falta de estabilidad en la red dificulta que el equipo realice su trabajo con normalidad, por lo que mejorar el servicio de Internet debe ser una prioridad para que todas las áreas puedan cumplir con sus tareas sin problemas.

3. ¿Cómo calificaría la calidad de la conexión a Internet en la Terminal?

Figura 58. Respuesta sobre la calidad del servicio de red.

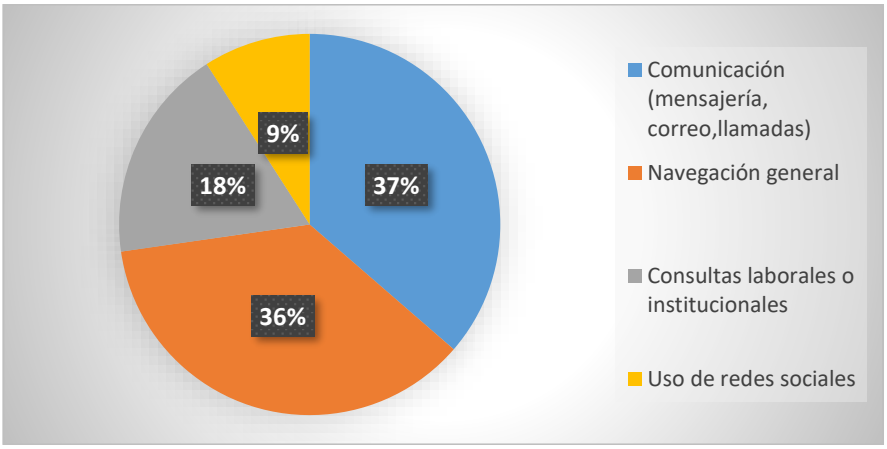


Fuente: Elaborado por la autora.

Interpretación: La **Figura 58** revela una muy mala calidad de la conexión en la Terminal, con un 73%, estos datos son proporcionados por los funcionarios que la califican como "muy mala". Ciertamente el 18% considera que el servicio es "malo", lo que evidencia una brecha entre el funcionamiento actual y las expectativas de calidad. Además, la existencia de un 9% que califica la red como "regular" señala que existen deficiencias puntuales que podrían estar afectando la experiencia de algunos usuarios. Lo que conlleva a realizar mejoras sustanciales en cobertura, velocidad o estabilidad para alcanzar estándares verdaderamente satisfactorios.

4. ¿Cuál es el propósito principal por el que utiliza el Internet en la Terminal?

Figura 59. Resultados sobre el propósito del uso del Internet en la Terminal.



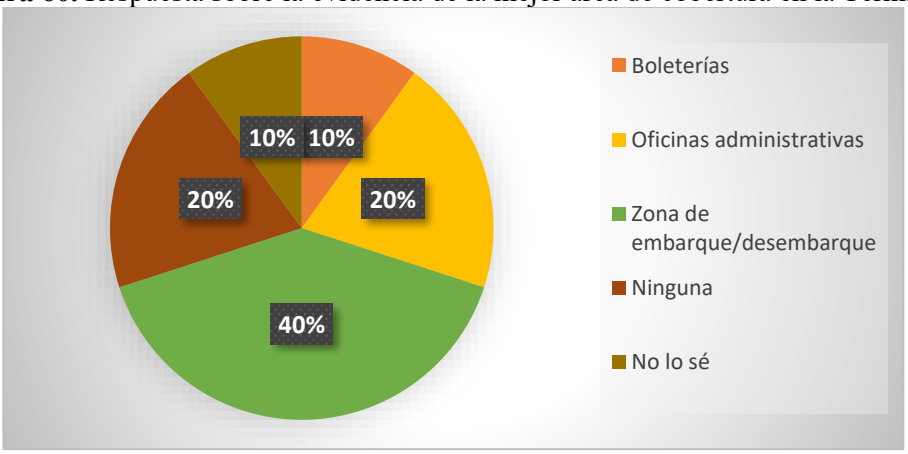
Fuente: Elaborado por la autora.

Interpretación: La **Figura 59** muestra los resultados que reflejan una distribución equitativa en los principales usos del Internet dentro de la Terminal Terrestre. El 37 % de los encuestados señala que lo utiliza principalmente para comunicación (como mensajería, correo electrónico o llamadas), mientras que un porcentaje igual (18 %) lo destina a consultas laborales o institucionales, lo que demuestra que el uso del Internet está estrechamente vinculado con las funciones administrativas y operativas del personal.

Por otro lado, un 36% indica que su propósito principal es la navegación general, lo que puede incluir búsquedas informativas o tareas no directamente relacionadas con el trabajo. Finalmente, el uso de redes sociales representa solo un 9 %, evidenciando que este tipo de uso es minoritario, posiblemente por restricciones de acceso o enfoque institucional.

5. ¿En qué áreas de la terminal ha notado mejor cobertura de Internet?

Figura 60. Respuesta sobre la evidencia de la mejor área de cobertura en la Terminal.

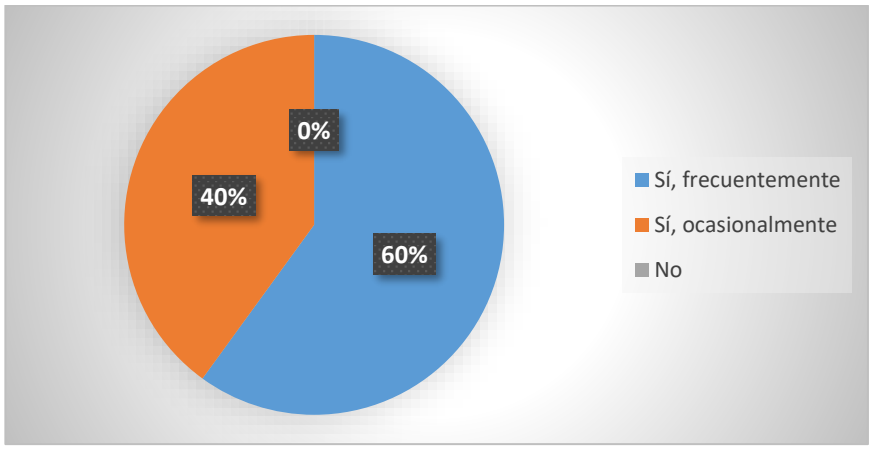


Fuente: Elaborado por la autora.

Interpretación: En la **Figura 60** se reporta que la mejor cobertura de Internet se encuentra en la zona de embarque/desembarque, lo que sugiere una priorización del acceso en espacios de trabajo internos donde se requiere una conexión estable para funciones críticas. Un 20% de los usuarios menciona que percibe buena cobertura en las oficinas administrativas, mientras que solo un 10% la percibe en las boleterías, lo que evidencia áreas con necesidad de mejora en la infraestructura de conectividad. Este resultado indica que las zonas destinadas al servicio al cliente o atención directa podrían estar en desventaja en términos de cobertura, afectando potencialmente la eficiencia operativa y la calidad de la atención brindada, también varios de los funcionarios identifican como ninguna, lo que reafirma la necesidad de ampliar y optimizar la señal en las áreas menos favorecidas.

6. ¿Ha experimentado interrupciones o lentitud en la red durante su uso?

Figura 61. Resultados obtenidos sobre las interrupciones y lentitud en la red.



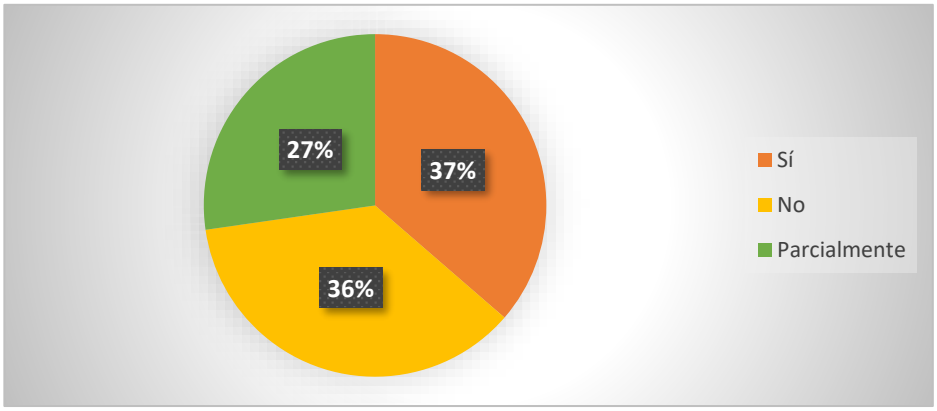
Fuente: Elaborado por la autora.

Interpretación: En la **Figura 61** muestra que una parte significativa del personal (40%) reporta que ocasionalmente experimenta interrupciones o lentitud en la red, mientras que un 60% afirma que estos problemas ocurren con mayor frecuencia y ningún funcionario presenta que no ha tenido inconvenientes de conectividad. Estos resultados evidencian que la red de la Terminal presenta inestabilidad operativa, afectando de forma periódica el desempeño del sistema y la experiencia de los usuarios. Por lo cual se concluye que la infraestructura actual no garantiza una conexión completamente estable para todos los funcionarios, lo cual puede repercutir en la eficiencia de los procesos administrativos y en la calidad del servicio brindado. Por ello, se recomienda realizar mejoras técnicas en la red,

como el refuerzo de la cobertura inalámbrica, la optimización del ancho de banda disponible y la implementación de un mantenimiento preventivo que permita garantizar la continuidad operativa y la satisfacción del personal.

7. ¿Considera que el servicio de internet es suficiente para cubrir necesidades actuales de los usuarios y funcionarios?

Figura 62. Respuesta sobre la necesidad de cubrir el servicio de internet en las áreas.

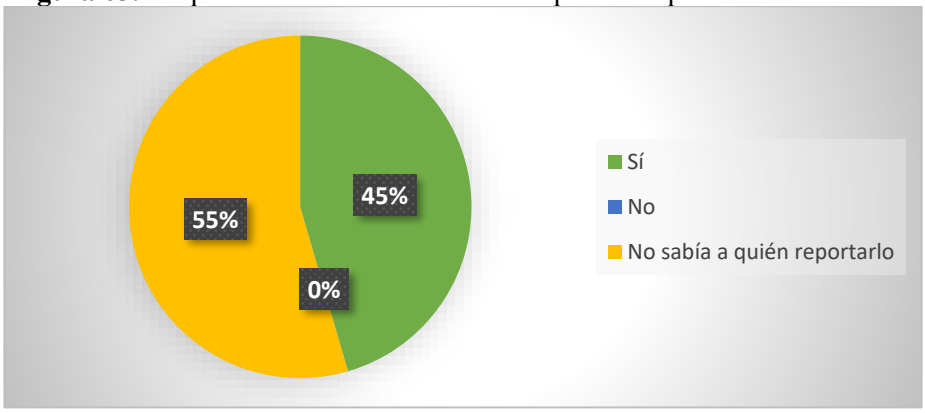


Fuente: Elaborado por la autora.

Interpretación: En la **Figura 62** se evidencia que el 36 % de los funcionarios respondió "No", indicando que no se cumple con el aspecto evaluado; otro 37% eligió la opción "Sí", lo que muestra una percepción positiva; mientras que el 27 % consideró que se cumple solo parcialmente. Estos resultados muestran que las opiniones del personal están divididas, lo que indica que, aunque se han hecho mejoras, todavía hay aspectos que deben reforzarse para que todos tengan una experiencia más positiva y uniforme.

8. ¿Ha reportado alguna vez un problema relacionado con la conectividad a los encargados de la Terminal?

Figura 63. Respuesta sobre conocimiento a reportar un problema de internet.

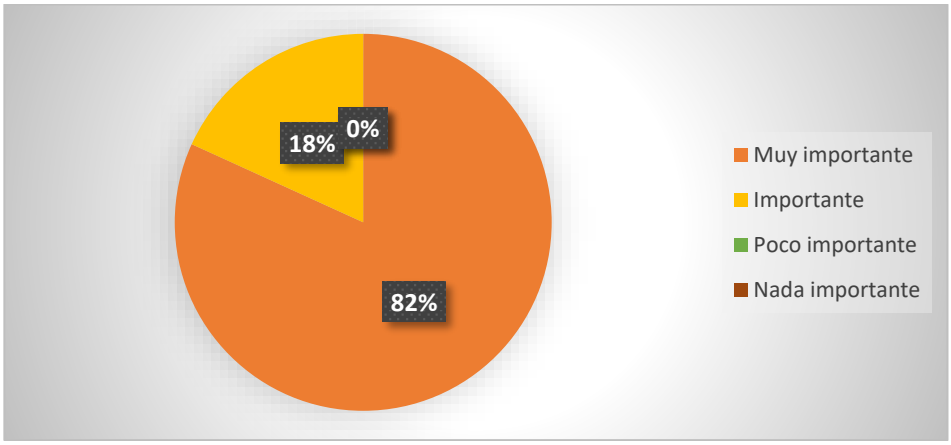


Fuente: Elaborado por la autora.

Interpretación: En la **Figura 63** revela que el 55% de los funcionarios no sabía con certeza a quién debía reportar los incidentes, mientras que el 45 % sí manifestó tener claridad al respecto. Aunque todos afirmaron haber reportado a alguien, esta situación muestra una posible falta de lineamientos claros o de comunicación interna sobre los canales oficiales para la gestión de incidentes. Por lo cual se con concluye que es necesario fortalecer los mecanismos de información y capacitación del personal respecto a los procedimientos y responsables para el reporte de incidentes, con el fin de garantizar una respuesta oportuna y organizada ante cualquier eventualidad.

9. ¿Qué tan importante es el acceso a Internet en espacios públicos de la Terminal?

Figura 64. Respuesta sobre la importancia del Internet en espacios públicos.

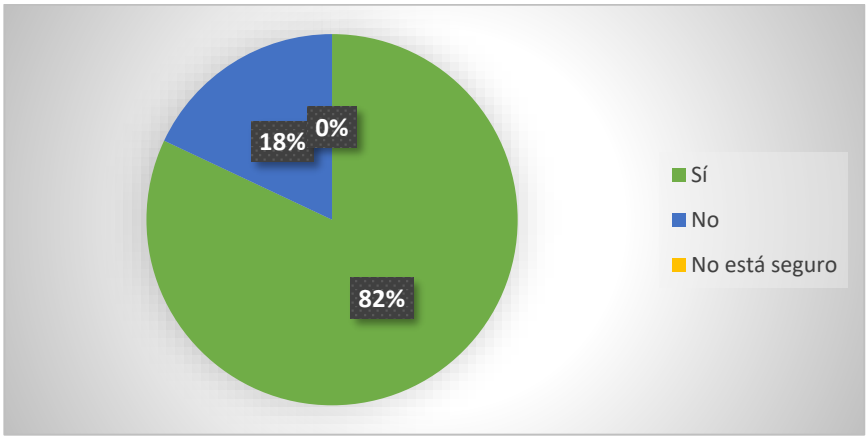


Fuente: Elaborado por la autora.

Interpretación: En la **Figura 64** se evidencia que un 82% de los funcionarios considera que el acceso a Internet en espacios públicos es muy importante, mientras que el 18 % lo califica como importante. Estos resultados presentan un alto nivel de conciencia sobre la relevancia de contar con conectividad en áreas comunes, no solo para el desarrollo de las actividades laborales, sino también como un recurso que mejora la atención al público y facilita el acceso a servicios digitales. Se concluye que el acceso a Internet en espacios públicos es percibido como una necesidad prioritaria por la mayoría del personal, por lo que debe ser considerado dentro de las estrategias institucionales para mejorar la eficiencia operativa y la calidad del servicio que se brinda tanto al funcionario como al ciudadano.

10. ¿Cree que mejorar la conectividad beneficiaría el servicio y la experiencia de los usuarios en la Terminal?

Figura 65. Respuesta sobre el beneficio de servicio y experiencia de los usuarios en la Terminal.



Fuente: Elaborado por la autora.

Interpretación: En la **Figura 65** se observa que la mayoría de los funcionarios, un 82%, respondió afirmativamente, mientras que el 18 % manifestó no estar seguro. Este resultado muestra una percepción mayoritariamente positiva o de conformidad respecto al aspecto evaluado, aunque la presencia de una minoría con dudas sugiere que aún existe margen para reforzar la claridad o la comunicación sobre el tema.

Se concluye que la mayoría del personal tiene una postura clara en cuanto al internet en la Terminal de Baba, sin embargo, es importante atender las incertidumbres identificadas para lograr una percepción más unificada y asegurar que todos los funcionarios cuenten con la información o el criterio necesario para responder con mayor certeza.

Este análisis constituye un paso importante en la evaluación de la calidad del servicio de Internet en la Terminal Terrestre del Cantón Baba.

Anexo 3

Solicitud para realizar el proyecto en la Terminal Terrestre de Baba

UPSE

Instituto de Postgrado

OFICIO N° 1-2025
Baba, 28 de abril de 2025

MGS.
Elmer Javier Mora Filian
COORDINADOR DEL GAD MUNICIPAL DEL CANTÓN BABA

Asunto: Solicitud de informe técnico de conectividad en la Terminal Terrestre del Cantón Baba.

De mis consideraciones,

Por medio de la presente, esperando se encuentre bien, me dirijo a usted para solicitarle de manera amena, que me permita ejecutar mi proyecto de titulación en el GAD de Baba, el cual consiste en realizar un análisis de la Infraestructura de Red y Simulación de Datos en Python para la Administración de la Terminal Terrestre del Cantón Baba.

Mediante el uso de herramientas permitirá el análisis de la información de manera específica de lo que realiza la red y de las vulnerabilidades existentes en ella.

Esperando que esta información sea de su interés, me despido cordialmente y quedo a su entera disposición.

Anexo informe de inspección,

Atentamente,

Firmado electrónicamente por:
TANIA YADIRA BANOS GALEAS
Validar únicamente con FirmaEC

Ing. Tania Baños Galeas
MAESTRANTE DE LA UPSE

Solicitud de aprobación por el Coordinador de la Unidad de Tics – Encargado del Área de Tecnologías

ALCALDÍA DE BABA

OFICIO N° 5- GADBABA-TIC-2025
Baba, 29 de abril de 2025

ING.
Tania Baños Galeas
MAESTRANTE DE LA UPSE

Asunto: Aceptación para el inicio del proyecto de titulación.

De mis consideraciones,

Por medio de la presente, en respuesta a la petición de la Ing. **TANIA BAÑOS GALEAS,** portadora de la cédula de identidad N° 1207980119, certifico que se autoriza en realizar su tema de investigación titulado **"ANÁLISIS DE LA INFRAESTRUCTURA DE RED Y SIMULACIÓN DE DATOS EN PYTHON PARA LA ADMINISTRACIÓN DE LA TERMINAL TERRESTRE DEL CANTÓN BABA"**, y todo análisis que pretenda realizar para la obtención del grado académico en Magister en Telecomunicaciones.

Es todo cuanto puedo decir en honor a la verdad, por lo tanto, faculto a la Ing. Tania Baños Galeas, que haga uso de esta certificación en todo lo que crea necesario.

Atentamente,

Firmado electrónicamente por:
ELMER JAVIER MORA FILIAN
Validar únicamente con FirmaEC

Mgs. Elmer Javier Mora Filian

COORDINADOR DE LA UNIDAD DE TICS.

Anexo 4

Configuraciones proporcionadas por la entidad

Configuraciones de Switch 1, Switch 2 y Router

Tabla 18. Configuraciones en Switches.

CANT	DESCRIPCIÓN	MODELO	NOMBRE	IP
1	Router Mikrotik	RB450GR 3	RB-EMOVIM-TT	eth1: 172.31.17.94/30 – WAN1 eth1: 192.168.0.200/24 – LAN MUNI ether4: 192.168.21.1/24 br1.7: 192.168.88.0/24 - ADMINISTRA
2	SW-PRINCIPAL	CR326-24G-2S+	SW-PRINCIPAL-TT	br1.7: 192.168.88.2/24 - ADMINISTRA
3	SW-SECUNDARIO	CR326-24G-2S+	SW-SECUNDARIO	br1.7: 192.168.88.3/24 - ADMINISTRA

Fuente: Elaborado por la autora.

Tabla 19. Detalles de Configuraciones de Switches.

DETALLE	NOMENCLATURA	VLAN	RED
Terminal	A	VLAN100	192.168.21.0/24
Entidad Del Estado	B	VLAN101	10.200.13.0/28
Gad De Baba	C	VLAN102	192.168.20.0/24
Administración Terminal	D	VLAN103	192.168.101.0/24

Fuente: Elaborado por la autora.

Configuración de Switch 1 Física

```
# software id = MSXI-MGFX#
# model = CRS326-24G-2S+
# serial number = HEN08NTM52Y
/interface bridge
                add admin-mac=48:A9:8A:FB:D8:24 auto-
                  mac=no comment=defconf name=bridge
                  \vlan-filtering=yes
/interface ethernet
set [ find default-name=ether1 ]
comment=ENLACE-LAN-TT-MKT_P4set [
find default-name=ether2 ] comment=AP2
set [ find default-name=ether3 ] comment=AP1
set [ find default-name=ether14 ]
comment=ENLACE-ANT-MKT_P2set [
find default-name=ether16 ]
comment=ANT-PC1
set [ find default-name=ether17 ] comment=ENLACE-LAN-MUNI-MKT_P3
set [ find default-name=sfp-sfpplus1 ] comment=LINK-
SWITCH-BLOQUE_LOCALset [ find default-
name=sfp-sfpplus2 ] advertise=\
                10M-half,10M-full,100M-half,100M-full,1000M-half,1000M-
                full,10000M-full \
                comment=LINK-SWITCH-BLOQUE-ENFRENTE
/interface vlan
add interface=bridge name=br1.7 vlan-id=7
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/interface bridge port
add bridge=bridge comment=defconf interface=ether1 add
bridge=bridge comment=defconf interface=ether2 add bridge=bridge
comment=defconf interface=ether3 add bridge=bridge
comment=defconf interface=ether4 add bridge=bridge
comment=defconf interface=ether5 add bridge=bridge
comment=defconf interface=ether6 add bridge=bridge
comment=defconf interface=ether7 add bridge=bridge
comment=defconf interface=ether8 add bridge=bridge
comment=defconf interface=ether9 add bridge=bridge
comment=defconf interface=ether10add bridge=bridge
```

```
comment=defconf interface=ether11add bridge=bridge
comment=defconf interface=ether12add bridge=bridge
comment=defconf interface=ether13add bridge=bridge
comment=defconf interface=ether14add bridge=bridge
comment=defconf interface=ether15add bridge=bridge
comment=defconf interface=ether16add bridge=bridge
comment=defconf interface=ether17add bridge=bridge
comment=defconf interface=ether18add bridge=bridge
comment=defconf interface=ether19add bridge=bridge
comment=defconf interface=ether20add bridge=bridge
comment=defconf interface=ether21add bridge=bridge
comment=defconf interface=ether22add bridge=bridge
comment=defconf interface=ether23add bridge=bridge
comment=defconf interface=ether24

add bridge=bridge
comment=defconf interface=sfp-
sfpplus1add bridge=bridge
comment=defconf interface=sfp-
sfpplus2

/interface bridge vlan

                add                     bridge=bridge
                  comment=LAN-TT-21
                  tagged=sfp-sfpplus2  untagged=\
                  ether1,ether2,ether4,ether5,ether
                  6,ether7,ether8,sfp-sfpplus1
                  vlan-ids=\ 100

                add bridge=bridge comment=ANT
                  tagged=sfp-sfpplus2 untagged=\
                  ether9,ether10,ether11,ether12,ether1
                  3,ether14,ether15,ether16 vlan-ids=\
                  101

                add bridge=bridge
                  comment=ADMINISTRACION
                  tagged=sfp-sfpplus2,bridge vlan-ids=\7

                add bridge=bridge comment=LAN-
                  MUNICIPIO tagged=sfp-sfpplus2
                  untagged=\
                  ether17,ether18,ether19,ether20,ether
                  21,ether22,ether23,ether24 vlan-ids=\
                  102

/ip address

                add address=192.168.88.2/24
                  comment=defconf
                  interface=br1.7 network=\
                  192.168.88.0
```

```
add address=192.168.7.2/24 interface=bridge network=192.168.7.0
/ip route
add distance=1 gateway=192.168.7.1
/system identity
set name=SW-PRINCIPAL-TT
/system routerboard settingsset boot-os=router-os
```

Configuración de Switch 2 Física

```
# model = CRS326-24G-2S+
# serial number = HEN08SRVYGP
/interface bridge
                    add admin-mac=48:A9:8A:FB:E2:2A auto-
                      mac=no comment=defconf name=bridge
                      \vlan-filtering=yes
/interface ethernet
set [ find default-name=ether3 ] comment=AP3
set [ find default-
name=ether15 ]
comment=ANT-PC3set [ find
default-name=ether16 ]
comment=ANT-PC4
set [ find default-name=sfp-sfpplus1 ] comment=LINK-SWITCH-PRINCIPAL
/interface vlan
add interface=bridge name=br1.7 vlan-id=7
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/interface bridge port
add bridge=bridge comment=defconf interface=ether1 add
bridge=bridge comment=defconf interface=ether2 add
bridge=bridge comment=defconf interface=ether3 add
bridge=bridge comment=defconf interface=ether4 add
bridge=bridge comment=defconf interface=ether5 add
bridge=bridge comment=defconf interface=ether6 add
bridge=bridge comment=defconf interface=ether7 add
bridge=bridge comment=defconf interface=ether8 add
bridge=bridge comment=defconf interface=ether9 add
bridge=bridge comment=defconf interface=ether10add
```

```
bridge=bridge comment=defconf interface=ether11add
bridge=bridge comment=defconf interface=ether12add
bridge=bridge comment=defconf interface=ether13add
bridge=bridge comment=defconf interface=ether14add
bridge=bridge comment=defconf interface=ether15add
bridge=bridge comment=defconf interface=ether16add
bridge=bridge comment=defconf interface=ether17add
bridge=bridge comment=defconf interface=ether18add
bridge=bridge comment=defconf interface=ether19add
bridge=bridge comment=defconf interface=ether20add
bridge=bridge comment=defconf interface=ether21add
bridge=bridge comment=defconf interface=ether22add
bridge=bridge comment=defconf interface=ether23add
bridge=bridge comment=defconf interface=ether24

add bridge=bridge
comment=defconf interface=sfp-
sfpplus1add bridge=bridge
comment=defconf interface=sfp-
sfpplus2

/interface bridge vlan

                add bridge=bridge
                  comment=ADMI
                  NISTRACION
                  tagged=\sfp-
                  sfpplus2,sfp-
                  sfpplus1,bridge
                  vlan-ids=7

                add bridge=bridge comment=LAN-
                  TT-21 tagged=sfp-sfpplus1,sfp-
                  sfpplus2 \
                  untagged=ether1,ether2,ether4,eth
                  er5,ether6,ether7,ether8 vlan-
                  ids=100

                add bridge=bridge comment=LAN-ANT
                  tagged=sfp-sfpplus1,sfp-sfpplus2
                  untagged=\
                  ether9,ether10,ether11,ether12,ether13,eth
                  er14,ether15,ether16 vlan-ids=\

                  101

                add bridge=bridge comment=LAN-
                  MUNICIPIO-20 tagged=sfp-sfpplus1,sfp-
                  sfpplus2 \untagged=\
                  ether15,ether16,ether17,ether18,ether19,et
                  her21,ether22,ether23,ether24 \

                  vlan-ids=102
```

```
/ip address
                    add address=192.168.88.3/24
                      comment=defconf
                      interface=br1.7 network=\
                      192.168.88.0
add address=192.168.7.3/24 interface=bridge network=192.168.7.0
/ip route
add distance=1 gateway=192.168.7.1
/system identity
set name=SW-SECUNDARIO
/system routerboard settingsset boot-os=router-os
```

Anexo 5

Informe técnico por el Ingeniero del Área de Tecnologías del GAD de Baba

ALCALDÍA DE
BABA

Gobierno Autónomo Descentralizado Municipal del Cantón Baba

Informe Técnico Interno

TICS- IT-GADMCB-2025

Título: Evaluación de la infraestructura de red de la Terminal Terrestre del Cantón Baba.
Elaborado por: Ing. Marcos Pérez Velásquez - Responsable Técnico.
Fecha: 02/05/2025

1. Resumen Ejecutivo

Este informe presenta los resultados de la evaluación realizada a la infraestructura de red de la Terminal Terrestre del Cantón Baba. Durante abril de 2025, el personal técnico del GADMCB efectuó inspecciones en sitio y pruebas funcionales. Se constató que existen limitaciones importantes en el monitoreo en tiempo real de la red, control de accesos y distribución del tráfico. Estas deficiencias representan un riesgo para la operatividad institucional y la calidad del servicio a los usuarios.

2. Introduccion

La Terminal Terrestre del Cantón Baba cumple un rol estratégico en la movilidad de ciudadanos y en el funcionamiento diario de los departamentos municipales alojados en sus instalaciones. La infraestructura de red existente debe asegurar continuidad, estabilidad y seguridad. Este informe responde a la necesidad de verificar las condiciones actuales de dicha infraestructura para plantear acciones de mejora factibles a corto y mediano plazo.

3. Metodologia

Las observaciones fueron realizadas por técnicos del GADMCB mediante inspección visual, verificación de conectividad entre equipos, pruebas básicas de tráfico interno, revisión de configuraciones de red en switches y routers disponibles, y entrevistas con personal de área. No se utilizaron herramientas especializadas avanzadas debido a la falta de capacitación y disponibilidad actual.

4. Inventario de Equipos de Red

Tipo de Equipo	Modelo	Cantidad	Estado	Ubicación	Observaciones
Switch PoE	Switch Mikrotik - CRS326-24g-2s+rm	2	Operativo	Sala técnica	Falta ventilación

Baba

Router	Mikrotik RB3011	1	Operativo	Rack central	Configuración básica
UPS	APC 1500VA	2	Operativo	Sala técnica	Autonomía

5. Configuración de VLANs en Switchs.

Configuración de Switch 1 Física de Switchs de la Terminal

```
# software id = MSXI-MGFX9
# model = CRS326-24G-2S+
# serial number = HFN08NTM52Y
/interface bridge
                add admin-mac=48:A9:8A:FB:D8:24 auto-mac=no
                    comment=defconf name=bridge vlan-filtering=yes
/interface ethernet
set [ find default-name=ether1 ] comment=ENLACE-LAN-
TT-MKT_P4set [ find default-name=ether2 ] comment=AP2
set [ find default-name=ether3 ] comment=AP1
set [ find default-name=ether14 ] comment=ENLACE-
ANT-MKT_P2set [ find default-name=ether16 ]
comment=ANT-PC1
set [ find default-name=ether17 ] comment=ENLACE-LAN-MUNI-MKT_P3
set [ find default-name=sfp-sfpplus1 ] comment=LINK-SWITCH-
BLOQUE_LOCALset [ find default-name=sfp-sfpplus2 ] advertise=\
                10M-half,10M-full,100M-half,100M-full,1000M-half,1000M-full,10000M-full \
                comment=LINK-SWITCH-BLOQUE-ENFRENTE
/interface vlan
add interface=bridge name=bri_7 vlan-id=7
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/interface bridge port
add bridge=bridge comment=defconf interface=ether1 add bridge=bridge comment=defconf
interface=ether2 add bridge=bridge comment=defconf interface=ether3 add bridge=bridge
comment=defconf interface=ether4 add bridge=bridge comment=defconf interface=ether5 add
bridge=bridge comment=defconf interface=ether6 add bridge=bridge comment=defconf
interface=ether7 add bridge=bridge comment=defconf interface=ether8 add bridge=bridge
comment=defconf interface=ether9 add bridge=bridge comment=defconf interface=ether10add
bridge=bridge comment=defconf interface=ether11add bridge=bridge comment=defconf
interface=ether12add bridge=bridge comment=defconf interface=ether13add bridge=bridge
comment=defconf interface=ether14add bridge=bridge comment=defconf interface=ether15add
bridge=bridge comment=defconf interface=ether16add bridge=bridge comment=defconf
interface=ether17add bridge=bridge comment=defconf interface=ether18add bridge=bridge
comment=defconf interface=ether19add bridge=bridge comment=defconf interface=ether20add
bridge=bridge comment=defconf interface=ether21add bridge=bridge comment=defconf
interface=ether22add bridge=bridge comment=defconf interface=ether23add bridge=bridge
comment=defconf interface=ether24
```

ALCALDÍA DE
BABA

```
add bridge=bridge comment=defconf
interface=sfp-sfpplus1 add bridge=bridge
comment=defconf interface=sfp-sfpplus2
/interface bridge vlan
                add    bridge=bridge    comment=LAN-TI-31
                  tagged=sfp-sfpplus1,bridge          untagged=
                  ether1,ether2,ether4,ether5,ether6,ether7,eth
                  er8,sfp-sfpplus1 vlan-ids=300
                add bridge=bridge comment=ANT tagged=sfp-
                  sfpplus2 untagged=
                  ether9,ether10,ether11,ether12,ether13,ether14,eth
                  er15,ether16 vlan-ids=301
                add bridge=bridge comment=ADMINISTRACION
                  tagged=sfp-sfpplus2,bridge vlan-ids=7
                add bridge=bridge comment=LAN MUSEO IPIO
                  tagged=sfp-sfpplus2 untagged=
                  ether17,ether18,ether19,ether20,ether21,ether22,e
                  ther23,ether24 vlan-ids=302
/ip address
                add address=192.168.88.2/24
                  comment=defconf interface=bri7
                  network=192.168.88.0
add address=192.168.7.2/24 interface=bridge network=192.168.7.0
/ip route
add distance=1 gateway=192.168.7.1
/system identity
set name=SW-PRINCIPAL-TI
/system routerboard settingset boot-os-router-os
```

Configuración de Switch 2 Física de la Terminal

```
# model = CRS326-24G-2S+
# serial number = HEN08SRVYGP
/interface bridge
                add admin-mac=48:A9:8A:FB:E2:2A auto-
                  mac=no comment=defconf name=bridge \
                  vlan-filtering=yes
/interface ethernet
set [ find default-name=ether3 ] comment=AP3
set [ find default-name=ether15 ]
comment=ANT-PC3set [ find
default-name=ether16 ]
comment=ANT-PC4
set [ find default-name=sfp-sfpplus1 ] comment=LINK-SWITCH-PRINCIPAL
```

Baba

ALCALDÍA DE
BABA

```
/interface vlan
add interface=bridge name=br1.7 vlan-id=7
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/interface bridge port
add bridge=bridge comment=defconf interface=ether1 add
bridge=bridge comment=defconf interface=ether2 add
bridge=bridge comment=defconf interface=ether3 add
bridge=bridge comment=defconf interface=ether4 add
bridge=bridge comment=defconf interface=ether5 add
bridge=bridge comment=defconf interface=ether6 add
bridge=bridge comment=defconf interface=ether7 add
bridge=bridge comment=defconf interface=ether8 add
bridge=bridge comment=defconf interface=ether9 add
bridge=bridge comment=defconf interface=ether10add
bridge=bridge comment=defconf interface=ether11add
bridge=bridge comment=defconf interface=ether12add
bridge=bridge comment=defconf interface=ether13add
bridge=bridge comment=defconf interface=ether14add
bridge=bridge comment=defconf interface=ether15add
bridge=bridge comment=defconf interface=ether16add
bridge=bridge comment=defconf interface=ether17add
bridge=bridge comment=defconf interface=ether18add
bridge=bridge comment=defconf interface=ether19add
bridge=bridge comment=defconf interface=ether20add
bridge=bridge comment=defconf interface=ether21add
bridge=bridge comment=defconf interface=ether22add
bridge=bridge comment=defconf interface=ether23add
bridge=bridge comment=defconf interface=ether24
add bridge=bridge comment=defconf
interface=sfp-sfpplus1 add
bridge=bridge comment=defconf
interface=sfp-sfpplus2
/interface bridge vlan
                add bridge=bridge
                  comment=ADMIN
                  ISTRACION
                  tagged=\sfp-
                  sfpplus2,sfp-
```

Baba

```
    sfpplus1 bridge
    vlan-ids=7
  add bridge=bridge comment=LAN_TI
    21 tagged=sfp-sfpplus1,sfp-sfpplus2
    \
    untagged=ether1,ether2,ether4,ether5
    ,ether6,ether7,ether8 vlan-ids=100
  add bridge=bridge comment=LAN_ANI
    tagged=sfp-sfpplus1,sfp-sfpplus2 untagged=\
    ether9,ether10,ether11,ether12,ether13,ether1
    4,ether15,ether16 vlan-ids=\
    101
  add bridge=bridge comment=LAN_
    MUNICIPIO-20 tagged=sfp-sfpplus1,sfp-
    sfpplus2 untagged=\
    ether15,ether16,ether17,ether18,ether19,ether
    21,ether22,ether23,ether24 \
    vlan-ids=102
/ip address
  add address=192.168.88.3/24
    comment=defconf interface=bri1.7
    network=\192.168.88.0
add address=192.168.7.3/24 interface=bridge network=192.168.7.0
/ip route
add distance=1 gateway=192.168.7.1
/system identity
set name=SW-SECUNDARIO
/system routerboard settings set boot-os=router-os
```

4. Diagnóstico Técnico Actual

Se evidenciaron los siguientes hallazgos:

- ✓ **No existe un sistema de monitoreo en tiempo real del tráfico o del estado de los equipos.**
- ✓ **Prever una futura separación del tráfico entre visitantes y usuarios internos mediante redes distintas cuando se implemente conectividad inalámbrica.**
- ✓ **Se detectaron dispositivos conectados sin control de acceso.**
- ✓ **La distribución del tráfico no está optimizada, lo que genera lentitud en ciertos momentos del día.**
- ✓ **El cableado estructurado no ha sido revisado desde su instalación.**

ALCALDÍA DE
BABA

5. Análisis de Riesgos

- ✓ La ausencia de monitoreo y control puede ocasionar:
- ✓ Accesos no autorizados a servicios institucionales.
- ✓ Caídas del servicio por sobrecarga o fallos no detectados a tiempo.
- ✓ Dificultades en la trazabilidad de actividades digitales.
- ✓ Pérdida de eficiencia operativa en los departamentos internos.

6. Propuesta de Mejora

- ✓ Separar el tráfico de visitantes y usuarios internos mediante redes diferentes.
- ✓ Capacitar al personal técnico en uso de herramientas de diagnóstico de red.

7. Conclusiones

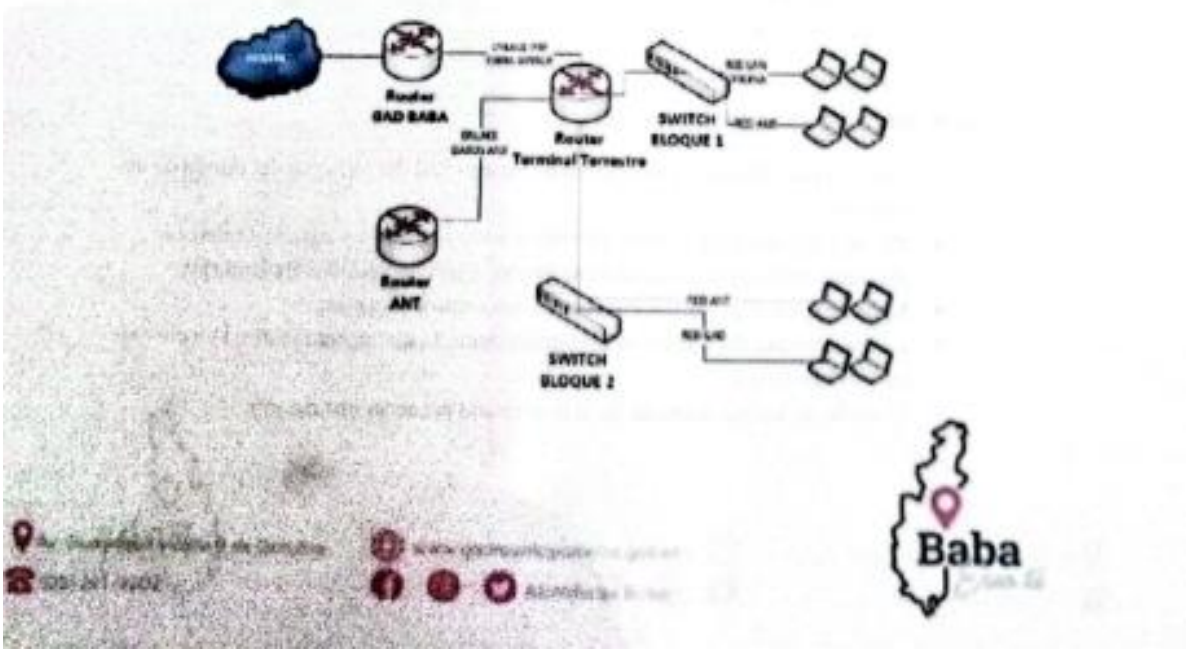
Las condiciones actuales de la red de la Terminal Terrestre requieren atención para evitar interrupciones mayores. Se pueden aplicar soluciones prácticas sin necesidad de herramientas complejas o costosas. Es indispensable establecer una rutina de supervisión periódica de los equipos y definir responsables técnicos locales.

8. Recomendaciones

- ✓ Realizar mantenimiento preventivo cada tres meses.
- ✓ Documentar todas las configuraciones de red actuales.
- ✓ Solicitar apoyo externo para la revisión integral del sistema si no se dispone de personal capacitado.

9. Anexos

A. Diagrama de la red actual



B. Fotos de puntos de red y equipos observados

C. Tabla de observaciones realizadas en abril de 2025

Tabla de Observaciones Realizadas

N.°	Área Evaluada	Observación	Impacto Potencial	Recomendación Inicial
1	**Infraestructura de Red**	Bajo acceso en puntos (AP) para conectividad inalámbrica.	Conectividad limitada para usuarios móviles.	Planificar adquisición e implementación de AP.
2	**Control de Acceso**	Hay dispositivos conectados sin autenticación ni restricción.	Vulnerabilidad a accesos no autorizados.	Implementar políticas de control de acceso.
3	**Monitoreo de Red**	No existe herramienta de monitoreo centralizada activa.	Ninguna detección.	Ninguna detección.
4	**Organización de Cableado**	Se observaron cables sin identificación ni canalización adecuada en los departamentos de la Terminal Terrestre.	Riesgo de desconexiones accidentales y fallos.	Ordenar y etiquetar cableado; usar canaletas en departamentos.

5	**Documentación Técnica**	No existe un plano actualizado de red.	Dificulta mantenimiento y escalabilidad.	Crear plano de red y bitácora técnica.
6	**Conectividad entre áreas**	Algunos departamentos presentan lentitud o desconexiones ocasionales.	Interrupción en servicios administrativos.	Verificar puntos de red y reemplazar equipos defectuosos.

10. Firmas y Validaciones

Ing. Marcos Pérez Velásquez
Responsable Técnico

Msc. Javier Mora Elian
Jefe de Tecnología

Anexo 6

Script desarrollado en Python para la captura del tráfico de red, mediante el uso de herramientas

```
import tkinter as tk
from tkinter import messagebox
import threading
import psutil
import time
import matplotlib.pyplot as plt
import pyshark
from collections import defaultdict
import asyncio
import subprocess

# Evento para detener monitoreo de tráfico
stop_event = threading.Event()

# Botón 1: Monitoreo de tráfico de red en tiempo real
def trafico_en_tiempo_real():
    if stop_event.is_set():
        stop_event.clear()

    def monitor_traffic():
        plt.ion()
        fig, ax = plt.subplots()
        time_data = []
        sent_data = []
        recv_data = []

        line_sent, = ax.plot([], [], label="Bytes Enviados", color="blue")
        line_recv, = ax.plot([], [], label="Bytes Recibidos", color="green")

        ax.set_xlabel("Tiempo (s)")
        ax.set_ylabel("Bytes")
        ax.set_title("Monitoreo de Tráfico de Red")
        ax.legend()

        start_time = time.time()
        initial_stats = psutil.net_io_counters()
        initial_sent = initial_stats.bytes_sent
        initial_recv = initial_stats.bytes_recv

        def on_close(event):
            stop_event.set()

        fig.canvas.mpl_connect('close_event', on_close)
```

```
        while not stop_event.is_set():
            current_stats = psutil.net_io_counters()
            sent = current_stats.bytes_sent - initial_sent
            recv = current_stats.bytes_recv - initial_recv
            elapsed_time = time.time() - start_time

            print(f"Tiempo: {elapsed_time:.2f}s, Bytes Enviados: {sent}, Bytes
Recibidos: {recv}")

            time_data.append(elapsed_time)
            sent_data.append(sent)
            recv_data.append(recv)

            line_sent.set_data(time_data, sent_data)
            line_recv.set_data(time_data, recv_data)

            ax.set_xlim(0, max(time_data) + 1)
            ax.set_ylim(0, max(max(sent_data, default=0), max(recv_data, default=0)) +
1000)

            plt.draw()
            plt.pause(1)

        plt.ioff()
        plt.close(fig)

    threading.Thread(target=monitor_traffic, daemon=True).start()

# Función para abrir el archivo captura.pcap en Wireshark
def abrir_en_wireshark():
    try:
        subprocess.Popen(['wireshark', 'captura.pcap'])
    except FileNotFoundError:
        messagebox.showerror("Error", "Wireshark no está instalado o no está en el
PATH.")

# Botón 2: Captura de protocolos con pyshark y abrir Wireshark al finalizar
def captura_de_protocolos():
    def run_capture():
        asyncio.set_event_loop(asyncio.new_event_loop())

        interface_name = 'Ethernet''
        protocol_counts = defaultdict(int)
        total_length = 0
        packet_count = 0
        output_file = 'captura.pcap'
```

```
        try:
            capture = pyshark.LiveCapture(interface=interface_name,
output_file=output_file)
            print(f'Capturando tráfico en la interfaz: {interface_name}...')

            for packet in capture.sniff_continuously(packet_count=100):
                packet_count += 1

                if hasattr(packet, 'length'):
                    total_length += int(packet.length)

                proto = packet.highest_layer
                protocol_counts[proto] += 1

            average_length = total_length / packet_count if packet_count else 0
            print(f'Total de paquetes: {packet_count}')
            print(f'Longitud promedio: {average_length:.2f} bytes')

            print("Contador de protocolos:")
            for proto, count in protocol_counts.items():
                print(f"{proto}: {count}")

            print(f'Paquetes guardados automáticamente en: {output_file}')
            messagebox.showinfo("Captura completada", f"La captura se guardó como
'{output_file}'.")

            abrir_en_wireshark()

        except Exception as e:
            print(f'Error: {e}')
            messagebox.showerror("Error", f"No se pudo capturar: {e}")

    threading.Thread(target=run_capture, daemon=True).start()

# Botón 3: Simulación de topología

def iniciar_simulacion_ns3():
    ventana_topologia = tk.Toplevel()
    ventana_topologia.title("Simulación NS-3 - Topología")
    ventana_topologia.geometry("640x450")
    canvas = tk.Canvas(ventana_topologia, width=620, height=400, bg="white")
    canvas.pack(pady=10)

    def simular_ns3():
        canvas.delete("all")
        canvas.create_text(320, 30, text="Topología: GAD BABA - ENTIDAD -
TERMINAL TERRESTRE", font=("Helvetica", 12, "bold"))
```

```
        canvas.create_rectangle(100, 40, 160, 80, fill="orange", outline="black",
width=2)
        canvas.create_text(130, 90, text="R-GAD\n192.168.0.1", font=("Helvetica", 8))

        canvas.create_rectangle(250, 80, 320, 120, fill="orange", outline="black",
width=2)
        canvas.create_text(285, 130, text="R-TERMINAL\n192.168.89.1",
font=("Helvetica", 8))

        canvas.create_rectangle(420, 40, 480, 80, fill="orange", outline="black",
width=2)
        canvas.create_text(450, 90, text="R-ENTIDAD\n192.168.2.1",
font=("Helvetica", 8))

        canvas.create_rectangle(100, 140, 160, 180, fill="lightblue", outline="black",
width=2)
        canvas.create_text(130, 190, text="SWITCH GAD", font=("Helvetica", 8))

        canvas.create_rectangle(420, 140, 480, 180, fill="lightblue", outline="black",
width=2)
        canvas.create_text(450, 190, text="SWITCH ENTIDAD", font=("Helvetica", 8))

        canvas.create_rectangle(180, 200, 240, 240, fill="lightblue", outline="black",
width=2)
        canvas.create_text(210, 250, text="SWITCH BLOQUE 1", font=("Helvetica",
8))

        canvas.create_rectangle(340, 200, 400, 240, fill="lightblue", outline="black",
width=2)
        canvas.create_text(370, 250, text="SWITCH BLOQUE 2", font=("Helvetica",
8))

        canvas.create_rectangle(140, 260, 190, 300, fill="gray", outline="black",
width=2)
        canvas.create_text(165, 310, text="PC 1\n192.168.0.10", font=("Helvetica", 8))

        canvas.create_rectangle(240, 260, 290, 300, fill="gray", outline="black",
width=2)
        canvas.create_text(265, 310, text="PC 2\n192.168.89.2", font=("Helvetica", 8))

        canvas.create_rectangle(310, 260, 360, 300, fill="gray", outline="black",
width=2)
        canvas.create_text(335, 310, text="PC 3\n192.168.88.2", font=("Helvetica", 8))

        canvas.create_rectangle(410, 260, 460, 300, fill="gray", outline="black",
width=2)
        canvas.create_text(435, 310, text="PC 4\n192.168.2.10", font=("Helvetica", 8))
```

```
        canvas.create_oval(170, 320, 220, 370, fill="lightgreen", outline="black",
width=2)
        canvas.create_text(195, 375, text="AP 1\n192.168.101.2", font=("Helvetica", 8))

        canvas.create_oval(360, 320, 410, 370, fill="lightgreen", outline="black",
width=2)
        canvas.create_text(385, 375, text="AP 2\n192.168.101.3", font=("Helvetica", 8))

        conexiones = [
            (160, 60, 250, 100), (420, 60, 320, 100), (285, 120, 210, 200),
            (285, 120, 370, 200), (130, 80, 130, 140), (450, 80, 450, 140),
            (210, 240, 165, 260), (210, 240, 265, 260), (210, 240, 195, 320),
            (370, 240, 335, 260), (370, 240, 435, 260), (370, 240, 385, 320)
        ]

        for x1, y1, x2, y2 in conexiones:
            canvas.create_line(x1, y1, x2, y2, fill="black", width=2)

        def animar_paquete(x1, y1, x2, y2):
            steps = 20
            dx = (x2 - x1) / steps
            dy = (y2 - y1) / steps
            paquete = canvas.create_oval(x1-5, y1-5, x1+5, y1+5, fill="red")
            for _ in range(steps):
                canvas.move(paquete, dx, dy)
                canvas.update()
                time.sleep(0.03)
            canvas.delete(paquete)

        rutas = conexiones[:6]
        for _ in range(2):
            for (x1, y1, x2, y2) in rutas:
                animar_paquete(x1, y1, x2, y2)

        messagebox.showinfo("NS-3", "Simulación completa ejecutada.")

    threading.Thread(target=simular_ns3, daemon=True).start()

# Crear ventana principal
ventana = tk.Tk()
ventana.title("Monitor de Red")
ventana.geometry("400x300")
ventana.configure(bg="#f0f0f0")

titulo = tk.Label(ventana, text="Herramientas de Red", font=("Helvetica", 16),
bg="#f0f0f0")
titulo.pack(pady=20)
```

```
btn1 = tk.Button(ventana, text="Tráfico de red en tiempo real",
command=trafico_en_tiempo_real,
            width=30, height=2, bg="#4CAF50", fg="white")
btn1.pack(pady=10)

btn2 = tk.Button(ventana, text="Captura de protocolos",
command=captura_de_protocolos,
            width=30, height=2, bg="#2196F3", fg="white")
btn2.pack(pady=10)

btn3 = tk.Button(ventana, text="Simulación Topología",
command=iniciar_simulacion_ns3,
            width=30, height=2, bg="#f44336", fg="white")
btn3.pack(pady=10)

def cerrar_app():
   stop_event.set()
   ventana.destroy()

ventana.protocol("WM_DELETE_WINDOW", cerrar_app)
ventana.mainloop()
```