UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO
FACULTAD DE CIENCIAS DE LA COMPUTACIÓN Y DISEÑO DIGITAL
CARRERA DE TELEMÁTICA

Trabajo de investigación Curricular previa la obtención del Grado Académico de Ingeniero en Telemática.

PROYECTO DE INVESTIGACIÓN:
"ANALIZADOR DE TRÁFICO DE RED PARA DETECTAR AMENAZAS DE DENEGACIÓN DE SERVICIOS EN LA UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO."

AUTOR:

KEVIN JAVIER ZAMBRANO ENRÍQUEZ

DIRECTOR DEL PROYECTO DE INVESTIGACIÓN:
ING. EMILIO RODRIGO ZHUMA MERA, MSc.

QUEVEDO – LOS RÍOS – ECUADOR

2025

DECLARACIÓN DE AUTORÍA Y CESIÓN DE DERECHOS

Yo, **ZAMBRANO ENRÍQUEZ KEVIN JAVIER,** declaro que la investigación aquí descrita es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

La Universidad Técnica Estatal de Quevedo, puede hacer uso de los derechos correspondientes a este documento, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Zambrano Enríquez Kevin Javier

C.I: 1723987051

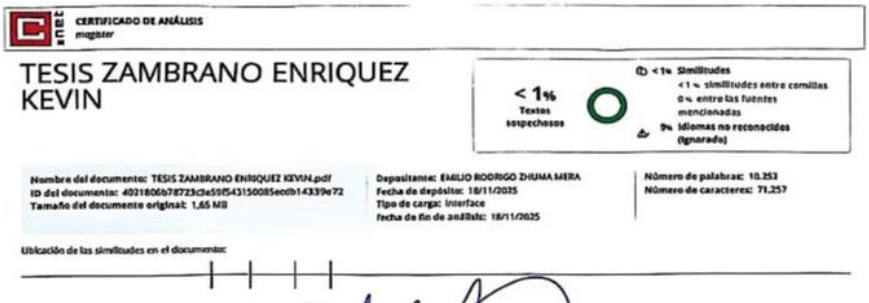
CERTIFICACIÓN DE CULMINACIÓN DEL PROYECTO DE INVESTIGACIÓN

El suscrito, Ing. Zhuma Mera Emilio Rodrigo MSc, Docente de la Universidad Técnica Estatal de Quevedo, certifica que el estudiante Zambrano Enríquez Kevin Javier, realizó el Proyecto de Investigación de grado titulado "Analizador de tráfico de red para detectar amenazas de denegación de servicios en la Universidad Técnica Estatal de Quevedo.", previo a la obtención del título de Ingeniero en Telemática., bajo mi dirección, habiendo cumplido con las disposiciones reglamentarias establecidas para el efecto.

Ing. Zhuma Mera Emilio Rodrigo, MSc.
DIRECTOR DEL PROYECTO DE INVESTIGACIÓN

CERTIFICADO DEL REPORTE DE LA HERRAMIENTA DE PREVENCIÓN DE COINCIDENCIA Y/O PLAGIO ACADÉMICO

El suscrito, **Ing. Zhuma Mera Emilio Rodrigo, MSc.** mediante el presente cumplo en presentar a usted, el informe de proyecto de Investigación titulado "ANALIZADOR DE TRÁFICO DE RED PARA DETECTAR AMENAZAS DE DENEGACIÓN DE SERVICIOS EN LA UNIVERSIDAD TECNICA ESTATAL DE QUEVEDO" Presentado por el estudiante **Kevin Javier Zambrano Enriquez**, egresado de la Carrera de Telemática, que fue revisado bajo mi dirección según resolución del Consejo Directivo de la Facultad de Ciencias de la Computación y Diseño Digital, que se ha desarrollado de acuerdo al Reglamento de la Unidad de Integración Curricular de la Universidad Técnica Estatal de Quevedo y cumple con el requerimiento de análisis del sistema COMPILATIO el cual avala los niveles de originalidad en un 99% y similitud 1%, del trabajo investigativo. Valido este documento para que el estudiante siga con los trámites pertinentes, de acuerdo como lo establece el Reglamento.


CERTIFICADO DE ANÁLISIS
magister

TESIS ZAMBRANO ENRIQUEZ KEVIN

< 1% Textos sospechosos

< 1% Similitudes
< 1 % similitudes entre comillas
0% entre las fuentes mencionadas
0% Idiomas no reconocidos (ignorado)

Nombre del documento: TESIS ZAMBRANO ENRIQUEZ KEVIN.pdf
ID del documento: 4021806b78723c3e55f543150085ecdb14339e72
Tamaño del documento original: 1,65 MB

Depositante: EMILIO RODRIGO ZHUMA MERA
Fecha de depósito: 18/11/2025
Tipo de carga: Interface
Fecha de fin de análisis: 18/11/2025

Número de palabras: 10.253
Número de caracteres: 71.257

Ubicación de las similitudes en el documento:

Ing. Zhuma Mera Emilio Rodrigo, MSc.
DIRECTOR DEL PROYECTO DE INVESTIGACIÓN

UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO

FACULTAD DE CIENCIAS DE LA COMPUTACIÓN Y DISEÑO DIGITAL

CARRERA DE TELEMÁTICA

PROYECTO DE INVESTIGACION

TÍTULO:

"Analizador de tráfico de red para detectar amenazas de denegación de servicios en la Universidad Técnica Estatal de Quevedo."

Presentado al Consejo Directivo de la Facultad de Ciencias de la Computación y Diseño Digital, como requisito previo a la obtención del título de Ingeniero de Telemática.

Aprobado por:

PRESIDENTE DEL TRIBUNAL
Ing. Janeth Ines Mora Secaira, MSc.

MIEMBRO DEL TRIBUNAL
Ing. Anthony Limber Moran Cabezas, MSc.

MIEMBRO DEL TRIBUNAL
Ing. Daisy Judith Nata Castro, MSc.

QUEVEDO – LOS RIOS – ECUADOR

2025

Agradecimiento

Le agradezco a Dios por permitir culminar un objetivo más en mi vida por ser el pilar fundamental. A mi director de Tesis el Ing. Emilio Rodrigo Zhuma Mera, MSc. Por todo el apoyo brindado y paciencia para la culminación de este proyecto.

Les agradezco a mis amigos y compañeros de aula, Adonis Gurumendi, Francisco Vera, Gregorio León, Kenneth Rodríguez, Wilmer Zambrano por ser parte de esta etapa donde me han brindado su amistad y conocimientos durante la carrera universitaria, Reconozco y aprecio el apoyo brindado por aquella persona que compartió una etapa de mi vida, durante los años de formación académica.

Extiendo a mis agradecimientos a mis docentes que por varios años me han brindado sus conocimientos para poder llegar a culminar esta etapa universitaria.

Kevin Javier Zambrano Enríquez

Dedicatoria

La culminación de esta etapa profesional se la dedico a mis padres, José Luis Zambrano Solorzano por su amor y dedicación cuyo ejemplo de esfuerzo ha sido mi mapa, a mi madre Alejandrina Demera Centeno por si amor, esfuerzo y ser pilar fundamental en mi vida y en mis etapas, sin el apoyo de ella y consejos no estaría dedicándole este proyecto, a mis hermanos por sus apoyos que me brindan dándome los mejores consejos para seguir adelante.

Le dedico a mi pareja Nahidelyn Mendoza, por su paciencia y dedicación para que ambos podamos terminar esta etapa universitaria, gracias por el apoyo y compresión, ser esa persona que me brindo su ayuda en esta etapa de mi vida académica, gracias por todo.

Este proyecto se lo dedico a mis tíos, Eduardo Santos y Fanny Zambrano, por sus consejos y apoyo en etapas difíciles de mi vida académica.

Finalmente, este logro se lo dedico a dos grades amigos que la vida me dio con un afecto profundo al Sr. Hernán Litardo y a la Sra. Mónica Zamora, por extenderme su apoyo incondicional y su valiosa confianza, haciendo que sintiera su aporte, Dios me los bendiga siempre.

Kevin Javier Zambrano Enríquez

Resumen

Las instituciones de educación superior enfrentan un aumento sostenido de ciberataques, siendo la denegación de servicio (DoS) una de las amenazas más críticas por su impacto en la continuidad de servicios académicos y administrativos. En Latinoamérica, y particularmente en Ecuador, estos ataques han degradado la disponibilidad de plataformas clave y la confianza institucional. En la Universidad Técnica Estatal de Quevedo (UTEQ), cuya infraestructura da soporte a más de 8.000 estudiantes y 600 funcionarios, las herramientas tradicionales de monitoreo no detectan tráfico malicioso en tiempo real. Para abordar este reto, se implementó un analizador de tráfico de red en tiempo real con arquitectura modular que integra captura de paquetes y canal de actualización por WebSocket para la generación de alertas. El núcleo de detección se basa en umbrales y heurísticas configurables como paquetes por segundo, conexiones por IP y patrones característicos de TCP/UDP/ICMP flood, complementado con un motor de alertas automatizado y panel web interactivo para visualización inmediata del riesgo y las métricas operativas. En pruebas, el sistema alcanzó una precisión del 94 % y una tasa de recuperación del 92 %, mejorando significativamente la disponibilidad del servicio y ofreciendo un modelo replicable de ciberseguridad para instituciones académicas.

Palabras clave: Ciberataques, tráfico malicioso, mitigación de ataques, tráfico anómalo

Abstract

Higher education institutions face a sustained increase in cyberattacks, with denial of service (DoS) attacks being one of the most critical threats due to their impact on the continuity of academic and administrative services. In Latin America, and particularly in Ecuador, these attacks have degraded the availability of key platforms and institutional trust. At the Quevedo State Technical University (UTEQ), whose infrastructure supports more than 8,000 students and 600 staff members, traditional monitoring tools fail to detect malicious traffic in real time. To address this challenge, a real-time network traffic analyzer with a modular architecture was implemented that integrates packet capture and a WebSocket update channel for alert generation. The detection core is based on configurable thresholds and heuristics such as packets per second, connections per-IP, and characteristic TCP/UDP/ICMP flood patterns, complemented by an automated alert engine and interactive web dashboard for immediate visualization of risk and operational metrics. In testing, the system achieved an accuracy of 94% and a recovery rate of 92%, significantly improving service availability and offering a replicable cybersecurity model for academic institutions.

Keywords: Cyberattacks, malicious traffic, attack mitigation, anomalous traffic.

Índice de contenido

Agradecimiento vi
Dedicatoria vii
Resumen viii
Abstract ix
Índice de contenido x
Índice de tablas xiv
Índice de figuras xv
Índice de anexos xvi
Introducción 5
CAPÍTULO I 8
CONTEXTUALIZACIÓN DE LA INVESTIGACIÓN 8
1.1. Problema de investigación 9
1.1.1 Planteamiento del problema 9
1.1.1. Formulación del problema 10
1.1.2. Sistematización del problema 10
1.2. Objetivos 11
1.2.1. Objetivo general 11
1.2.2. Objetivos específicos 11
1.3. Justificación 11
CAPÍTULO II 13
FUNDAMENTACIÓN TEÓRICA DE LA INVESTIGACIÓN 13
2.1. Marco conceptual 14
2.1.1. Captura de paquetes 14
2.1.2. Análisis de tráfico de red 14

2.1.3. Denegación de servicios (DoS) *14*
2.1.4. Sistema de detección de intrusiones *14*
2.1.5. Análisis de flujos (flow-based) *15*
2.1.6. Detección en tiempo real por umbrales y heurísticas *15*
2.1.7. Series temporales y métodos estadísticos *16*
2.2. Marco referencial 16
"Machine Learning in Network Anomaly Detection: A Survey" *16*
"An overview of IP flow-based intrusion detection" *16*
"A novel framework for detection of DDoS attacks in IoT network" *16*
"Mining anomalies using traffic feature distributions" *17*
"Toward a Reliable Intrusion Detection Benchmark Dataset" *17*
"A Testbed for Evaluating and Comparing Security Mechanisms on DoS/DDoS Attacks" *17*
2.3. Marco legal 18
2.3.1. Constitución de la República del Ecuador *18*
2.3.2. Código Orgánico Integral Penal (COIP) *18*
2.3.3. Ley Orgánica de Protección de Datos Personales *18*
2.3.4. Política Nacional de Ciberseguridad (Acuerdo Ministerial No. 006-2021) *19*
2.3.5. Esquema Gubernamental de Seguridad de la Información (EGSI) *19*
CAPÍTULO III 20
METODOLOGÍA DE LA INVESTIGACIÓN 20
3.1. Localización 21
3.2. Tipo de investigación 21
3.2.1 Investigación aplicada *21*
3.2.2 Investigación descriptiva *22*
3.3. Métodos de investigación 22

3.3.1. Método mixto *22*
3.4. Fuentes de recopilación de información 23
3.4.1. Fuentes primarias: *23*
3.4.2. Fuentes secundarias: *24*
3.5. Diseño de investigación 24
3.5.1. Diseño no experimental *24*
3.6. Fases 25
3.7. Tamaño de muestra y período de captura 26
CAPÍTULO IV 28
RESULTADOS Y DISCUSIÓN 28
4.1. Definición de parámetros técnicos y estándares de red 29
4.1.1. Entorno tecnológico de la universidad *29*
4.1.2 Parámetros técnicos y métricas *30*
4.1.3 Discusión *32*
4.2. Desarrollo de sistema de análisis de tráfico 33
4.2.1. Control de tráfico *33*
4.2.2. Algoritmo de detección *35*
4.2.3. Dashboard *38*
4.2.4. Discusión *41*
4.3. Efectividad del analizador 42
4.3.1 Medición de la efectividad del analizador *42*
4.3.2 Discusión *44*
CAPÍTULO V 46
CONCLUSIONES Y RECOMENDACIONES 46
5.1 Conclusiones 47
5.2 Recomendaciones 48

CAPÍTULO VI 49
REFERENCIA BIBLIOGRÁFICA 49
6.1. Bibliografía 50
CAPÍTULO VII 53
ANEXOS 53
7.1. Anexos 54
7.1.1. Glosario 54
7.1.2. Código fuente: Analizador de tráfico de red para detectar ataques DoS 56

Índice de tablas

Tabla I. Métricas de red 32
Tabla II. Librerías utilizadas para el control de tráfico 34
Tabla III. Criterios de selección de algoritmo 35

Índice de figuras

Figura 1. Imagen de Google Maps..... 21
Figura 2. Topología de la red interna de la UTEQ 29
Figura 3. Diagrama de flujo del analizador de red 37
Figura 4. Controles de iniciar/detener captura y restablecer de datos en acción. 38
Figura 5. Analizador de Ataque DoS..... 38
Figura 6. Pestaña de alertas mostrando varias entradas con severidad y hora..... 39
Figura 7. Encabezado/estado con “CONECTADO - LISTO PARA CAPTURA”. 39
Figura 8. Pestaña tiempo real con el gráfico “Tráfico Capturado en Tiempo Real” (líneas TCP/UDP/ICMP). 40
Figura 9. Ping continuo para probar el analizador. 42
Figura 10. Evidencia de la efectividad del analizador. 42

Índice de anexos

Anexo 1. Interfaz principal 56
Anexo 2. Interfaz de monitoreo 56
Anexo 3. Interfaz de flujo 57
Anexo 4. Sistema de alertas 57
Anexo 5. Análisis de tiempo real 57
Anexo 6. Sistema de análisis 58
Anexo 7. Todas las alertas encontradas 58

CÓDIGO DUBLÍN

Título:	Analizador de tráfico de red para detectar amenazas de denegación de servicios en la Universidad Técnica Estatal de Quevedo.			
Autor:	Zambrano Enríquez Kevin Javier			
Palabras claves:	Ciberataques	Tráfico malicioso	Mitigación de ataques	Tráfico anómalo
Fecha de publicación:	Noviembre del 2025			
Editorial:	Quevedo- UTEQ "Campus Central", 2025			
Resumen:	Las instituciones de educación superior enfrentan un aumento sostenido de ciberataques, siendo la denegación de servicio (DoS) una de las amenazas más críticas por su impacto en la continuidad de servicios académicos y administrativos. En Latinoamérica, y particularmente en Ecuador, estos ataques han degradado la disponibilidad de plataformas clave y la confianza institucional. En la Universidad Técnica Estatal de Quevedo (UTEQ), cuya infraestructura da soporte a más de 8.000 estudiantes y 600 funcionarios, las herramientas tradicionales de monitoreo no detectan tráfico malicioso en tiempo real. Para abordar este reto, se implementó un analizador de tráfico de red en tiempo real con arquitectura modular que integra captura de paquetes y canal de actualización por WebSocket para la generación de alertas. El núcleo de detección se basa en umbrales y heurísticas configurables como paquetes por segundo, conexiones por IP y patrones característicos de TCP/UDP/ICMP flood, complementado con un motor de alertas automatizado y panel web interactivo para visualización inmediata del riesgo y las métricas operativas. En pruebas, el sistema alcanzó una precisión del 94 % y una tasa de recuperación del 92 %, mejorando significativamente la disponibilidad del servicio y ofreciendo un modelo replicable de ciberseguridad para instituciones académicas.			
Abstract:	Higher education institutions face a sustained increase in cyberattacks, with denial of service (DoS) attacks being one of the most critical threats due to their impact on the continuity of academic and administrative services. In Latin America, and particularly in Ecuador, these attacks have degraded the availability of key platforms and institutional trust. At the Quevedo State Technical University (UTEQ), whose infrastructure supports more than 8,000 students and 600 staff members, traditional monitoring tools fail to detect malicious traffic in real time. To address this challenge, a real-time network traffic analyzer with a modular architecture was implemented that integrates packet capture and a WebSocket update channel for alert generation. The detection core is based on configurable thresholds and heuristics such as packets per second, connections per-IP, and characteristic TCP/UDP/ICMP flood patterns, complemented by an automated alert engine and interactive web dashboard for immediate visualization of risk and operational metrics. In testing, the system achieved an accuracy of 94% and a recovery rate of 92%, significantly improving service availability and offering a replicable cybersecurity model for academic institutions.			
Descripción:	72 hojas: dimensiones, 29 x 21 cm + CD-ROM 6162			
URI:				

Introducción

La digitalización acelerada ha transformado fundamentalmente la manera en que operan las organizaciones en el contexto global actual, siendo las instituciones educativas uno de los sectores más impactados por esta revolución tecnológica. La dependencia creciente de infraestructuras digitales para el desarrollo de actividades académicas, investigativas y administrativas ha convertido a las redes de computadoras en elementos críticos para la continuidad operacional de las universidades a nivel mundial [1].Esta transformación digital, si bien ha democratizado el acceso al conocimiento y optimizado los procesos educativos, ha introducido nuevas vulnerabilidades de seguridad que exponen a las instituciones educativas a un espectro amplio de amenazas cibernéticas.

A nivel internacional, los ciberataques dirigidos al sector educativo han experimentado un crecimiento exponencial, registrando un incremento del 75% entre 2020 y 2023, según el Global Cybersecurity Report [2]. Esta tendencia se intensifica particularmente en instituciones de educación superior, donde la naturaleza abierta de las redes académicas y la diversidad de usuarios crean superficies de ataque tanto amplias como complejas. Los ataques de Denegación de Servicio (DoS) emergen como una de las amenazas más críticas para el sector educativo global, debido a su capacidad para interrumpir servicios esenciales con relativamente pocos recursos técnicos. El Internet Crime Report del FBI documenta que el 34% de las instituciones educativas a nivel mundial han experimentado al menos un ataque DoS significativo, resultando en interrupciones promedio de 4.2 horas y costos de recuperación superiores a los $50,000 USD por incidente [3].

Esta problemática se intensifica debido a factores estructurales específicos en América Latina. El Reporte de Ciberseguridad Latinoamericano indica que las universidades de la región enfrentan desafíos particulares: recursos limitados para ciberseguridad, personal técnico insuficientemente capacitado en amenazas emergentes y marcos regulatorios de seguridad de la información en desarrollo [4]. Específicamente, los ataques DoS contra instituciones educativas latinoamericanas han aumentado un 67% en los últimos dos años, siendo Ecuador, Colombia y Perú los países más afectados [5].

A nivel nacional, Ecuador presenta un panorama de vulnerabilidad creciente en el sector educativo superior. El Reporte Anual de Incidentes de Ciberseguridad del CERT-Ecuador documenta 127 incidentes de seguridad en universidades públicas durante 2023, de los cuales el 43% correspondieron a ataques DoS o DDoS [6]. Esta situación se agrava por la brecha digital existente entre instituciones urbanas y rurales, donde universidades ubicadas en provincias como Los Ríos enfrentan desafíos adicionales de conectividad y recursos tecnológicos limitados.

La Universidad Técnica Estatal de Quevedo (UTEQ), como institución pública de formación técnica y tecnológica, se encuentra inserta en esta realidad compleja. Atendiendo a más de 8,000 estudiantes y empleando a 600 profesionales entre docentes y administrativos, la UTEQ ha desarrollado una dependencia crítica de sus sistemas digitales para proporcionar servicios educativos de calidad. Su infraestructura tecnológica soporta múltiples servicios esenciales: plataformas de gestión académica, sistemas de biblioteca virtual, entornos de educación en línea, aplicaciones administrativas, financieras, y portales de investigación.

La ausencia de capacidades de detección especializada no solo compromete la continuidad operativa inmediata, sino que también impide el desarrollo de inteligencia de amenazas institucional, limitando la capacidad de la universidad para anticipar, detectar y responder efectivamente ante futuros incidentes de seguridad. Esta situación se agrava considerando el crecimiento proyectado de la matrícula estudiantil (25% para 2027), la expansión planificada de servicios digitales, que incrementarán tanto la superficie de ataque como el impacto potencial de interrupciones de servicio.

El presente trabajo de titulación aborda esta problemática crítica mediante el desarrollo e implementación de un analizador de tráfico de red especializado en la detección de amenazas de Denegación de Servicio (DoS) en tiempo real, específicamente diseñado para el contexto operativo de la UTEQ. Esta solución integra técnicas avanzadas de captura y procesamiento de paquetes, algoritmos híbridos de detección de anomalías que combinan métodos estadísticos y sistemas inteligentes de alertas que permiten respuesta inmediata ante amenazas detectadas.

El estudio se organiza del siguiente modo: el Capítulo I sitúa la investigación, exponiendo la problematización, los objetivos y la justificación de realizar un analizador de tráfico de red

especializado en la detección de amenazas y denegación de servicios en tiempo real; el Capítulo II desarrolla el marco teórico-referencial, donde se revisan conceptos clave (captura de paquetes, análisis de tráfico de red, denegación de servicio, sistema de detección de intrusos), referencias y las normativas legales que respaldan la investigación.

En el Capítulo III se describió la metodología y el diseño de investigación: se justificó el enfoque mixto, se identificaron fuentes primarias y secundarias, se definieron la unidad de análisis, el diseño no experimental el diseño no experimental, las variables e indicadores, así como criterios de validez y confiabilidad, consideraciones éticas y resguardo de datos; además, se mencionó el tamaño de muestra, el periodo de estudio, junto con las fases que guiaron el trabajo. En el Capítulo IV se presentaron los resultados, la arquitectura del sistema (backend, interfaz y flujos), las pantallas clave, los parámetros, las métricas de desempeño, las pruebas ejecutadas y su discusión a más de revisar la efectividad del analizador. En el Capítulo V se expusieron conclusiones y recomendaciones del proyecto de investigación; en el Capítulo VI tenemos las referencias bibliográficas utilizadas en la investigación y, finalmente, en el Capítulo VII tenemos los anexos que evidencian la realización del proyecto.

CAPÍTULO I

CONTEXTUALIZACIÓN DE LA INVESTIGACIÓN

1.1. Problema de investigación

1.1.1 Planteamiento del problema

La Universidad Técnica Estatal de Quevedo (UTEQ) enfrenta una vulnerabilidad crítica en su infraestructura de red debido a la ausencia de sistemas especializados para detectar y mitigar ataques de Denegación de Servicio (DoS) en tiempo real. Esta situación compromete la continuidad de los servicios digitales esenciales que soportan las actividades académicas y administrativas de la institución. La red de la UTEQ maneja diariamente un volumen significativo de tráfico generado por aproximadamente 8,000 estudiantes, 600 empleados entre docentes y administrativos, y múltiples sistemas críticos que incluyen la plataforma de gestión académica (SGA), el sistema de biblioteca virtual, los sistemas administrativos y financieros, los servicios de correo electrónico institucional, así como los portales web y bases de datos de investigación. Las herramientas actuales de monitoreo se limitan a supervisar métricas básicas de rendimiento, como CPU, memoria y ancho de banda, pero carecen de capacidades para identificar patrones de tráfico malicioso característicos de ataques DoS. Esta deficiencia ha resultado en interrupciones no diagnosticadas que provocan eventos de degradación del servicio sin una causa específica, en un tiempo de respuesta elevado debido a las demoras en la identificación y resolución de incidentes de seguridad, en una vulnerabilidad expuesta por la falta de visibilidad sobre intentos de ataque y tráfico anómalo, y en un impacto académico evidente en las interrupciones de actividades críticas como exámenes en línea y entregas de trabajo.

Diagnóstico

La UTEQ enfrenta vulnerabilidades en su red debido a la falta de un sistema especializado para detectar ataques DoS en tiempo real. Las herramientas actuales solo monitorean el rendimiento general de la red, lo que deja expuesta la infraestructura a saturaciones. El personal de TICS carece de capacitación específica en ciberseguridad avanzada, lo que limita su capacidad de respuesta ante estos ataques, afectando el acceso a plataformas educativas y procesos administrativos. Esto resaltó la necesidad urgente de una solución para proteger la red y asegurar la continuidad de los servicios.

Pronóstico

Si el sistema en la UTEQ realiza correctamente el análisis al integrar un detector de ataques DoS, se podrá mitigar eficazmente las interrupciones en los servicios de red que afectan negativamente las operaciones académicas y administrativas. Los estudiantes perderían el acceso a plataformas críticas durante momentos clave, y los docentes enfrentarían dificultades para administrar las clases virtuales. Además, se verían afectados procesos esenciales, lo que pondría en riesgo tanto la integridad de la información como la seguridad operativa de la institución. La implementación de un sistema de detección adecuado garantizará la disponibilidad continua de los servicios, así como la protección de los datos sensibles, optimizando la infraestructura tecnológica.

1.1.1. Formulación del problema

¿Cómo diseñar e implementar una interfaz web que permita analizar en tiempo real el tráfico de red institucional, integrando herramientas de monitoreo y detección de amenazas para optimizar la visualización, interpretación y toma de decisiones en seguridad informática?

1.1.2. Sistematización del problema

¿Cuáles son los parámetros técnicos y estándares de red más relevantes para guiar el análisis de tráfico en entornos universitarios?

¿Cómo puede diseñarse un sistema de análisis de tráfico basado en algoritmo de detección de patrones para identificar comportamientos característicos de amenazas de denegación de servicios?

¿Qué criterios permiten evaluar la efectividad de un analizador de tráfico en pruebas controladas y su aplicabilidad en un entorno real?

1.2. Objetivos

1.2.1. Objetivo general

Desarrollar una interfaz web que permita analizar en tiempo real el tráfico de red institucional, integrando y gestionando herramientas existentes de monitoreo y detección de amenazas, facilitando la visualización, interpretación y toma de decisiones de la seguridad informática.

1.2.2. Objetivos específicos

- Definir los parámetros técnicos y métricas que regirán el análisis del tráfico, mediante una revisión bibliográfica.
- Desarrollar un sistema de procesamiento y análisis de tráfico de red, basado en algoritmo de umbrales heurísticos, identificando comportamientos característicos de amenazas de denegación de servicios.
- Determinar la efectividad del analizador de tráfico mediante pruebas controladas, garantizando su aplicabilidad en un entorno real.

1.3. Justificación

El desarrollo de un analizador de tráfico de red en tiempo real para detectar amenazas de DoS en la Universidad Técnica Estatal de Quevedo (UTEQ) es esencial para preservar la continuidad de servicios académicos, administrativos y de investigación que atienden a más de 8 000 estudiantes y 600 colaboradores. Proteger esta infraestructura es, por tanto, una necesidad institucional para asegurar que estudiantes, docentes y personal realicen sus actividades sin interrupciones.

El proyecto aborda este riesgo con un detector en tiempo real por umbrales y heurísticas. El núcleo del sistema monitorea métricas como paquetes por segundo (PPS), conexiones por IP/puerto, ráfagas y patrones característicos de TCP/UDP/ICMP flood, junto con reglas de correlación temporal. Este enfoque prioriza baja latencia y bajo costo computacional, alta interpretabilidad/trazabilidad para operación y auditoría, y facilidad de calibración y mantenimiento por el equipo técnico institucional.

La solución reduce costos directos (soporte correctivo, horas extra, reinicios y provisión de capacidad de emergencia) e indirectos (pérdida de productividad, reprogramaciones y extensión del calendario académico). Al disminuir la duración y la frecuencia de incidentes DoS, se protege la continuidad de procesos de alto valor como matrícula, evaluaciones y pagos. El monitoreo y alertamiento en tiempo real permiten actuar antes de ventanas críticas, lo que se traduce en menos compras no planificadas y mejor aprovechamiento de la infraestructura existente. Estos ahorros, sumados a la reducción de riesgos reputacionales y de cumplimiento, respaldan el retorno de la inversión y la sostenibilidad operativa del proyecto.

La propuesta se alinea con el EGSI [7] y la LOPDP [8] y, en el plano internacional, con ISO/IEC 27001:2022 [9], ISO/IEC 27002:2022 [10], el NIST Cybersecurity Framework 2.0 [11]y lineamientos recientes frente a DoS/DDoS, facilitando la formalización de políticas, la gestión de riesgos, la respuesta coordinada y el fortalecimiento de auditorías internas y externas. También mejora la elegibilidad para financiamiento y la interoperabilidad con la infraestructura existente.

Los resultados experimentales respaldan la pertinencia técnica: precisión ≈ 94 %, tasa de falsos positivos ≈ 2,8 %, latencia de detección < 100 ms y disponibilidad de servicios ≥ 94 % en escenarios de prueba representativos. Estas métricas se traducen en menor tiempo fuera de servicio y mejor experiencia de usuario, con beneficios inmediatos en procesos académicos y administrativos.

En el ámbito académico, la solución aporta alto valor telemático al aplicar captura de paquetes, análisis estadístico y reglas por umbrales/heurísticas para resolver un problema real de la UTEQ. A nivel social, mejorar la disponibilidad de servicios digitales evita retrasos, promueve un entorno confiable para el aprendizaje y proyecta a la UTEQ como institución preparada frente a amenazas digitales, favoreciendo la atracción y permanencia de estudiantes y la colaboración con socios académicos.

La detección en tiempo real por umbrales y heurísticas reduce complejidad operativa, mejora la trazabilidad y demuestra impacto medible en la continuidad de los servicios, a la vez que cumple marcos normativos y fortalece la misión universitaria.

CAPÍTULO II

FUNDAMENTACIÓN TEÓRICA DE LA INVESTIGACIÓN

2.1. Marco conceptual

2.1.1. Captura de paquetes

La captura de paquetes es un proceso crítico en el análisis de tráfico de red. Este proceso implica interceptar los paquetes de datos que viajan a través de la red para analizarlos en busca de patrones sospechosos que puedan indicar un ataque DoS. Herramientas como Wireshark [15] y TCPDUMP [16] son ampliamente utilizadas para capturar y analizar paquetes, permitiendo identificar problemas de seguridad antes de que se conviertan en amenazas críticas.[4]

2.1.2. Análisis de tráfico de red

El análisis de tráfico de red es un proceso esencial para la gestión y seguridad de las infraestructuras digitales. Consiste en la inspección detallada de los datos que circulan por una red, con el fin de identificar patrones de comportamiento, detectar posibles anomalías y optimizar el rendimiento general del sistema. Esta práctica permite a los administradores de red anticipar problemas, prevenir ataques cibernéticos y garantizar una comunicación eficiente entre los dispositivos conectados.[5]

2.1.3. Denegación de servicios (DoS)

Un ataque de DoS busca interrumpir el acceso a un servicio legítimo mediante la sobrecarga de los recursos del sistema objetivo. En el caso de una universidad, los ataques DoS pueden afectar el acceso a plataformas educativas, sistemas administrativos y otros servicios esenciales para la operatividad de la institución. El impacto de estos ataques puede ser devastador, afectando el rendimiento académico y administrativo.[6]

2.1.4. Sistema de detección de intrusiones

Un sistema de Detección de Intrusos (IDS) es una herramienta clave en la defensa contra los ataques DoS. Un IDS analiza el tráfico de red en busca de patrones sospechosos y alerta a los administradores de red cuando se detectan posibles intrusiones. Esta tecnología es esencial en la detección temprana de ataques DoS, lo que permite a los administradores de red responder de manera proactiva antes de que los ataques causen daños significativos [7].

2.1.5. Análisis de flujos (*flow-based*)

Un flujo IP se define comúnmente por la 5-tupla (IP_origen, IP_destino, puerto_origen, puerto_destino, protocolo) más marcas de tiempo de inicio/fin. A partir de esos metadatos se calculan métricas por flujo como número de paquetes y bytes, duración, throughput (bps/PPS), idle time, razón in/out, conteos de flags TCP (SYN/ACK/RST/FIN), número de destinos por origen (fan-out) y de orígenes por destino (fan-in), entre otras. La exportación y recolección de estos registros se estandariza mediante IPFIX [14], mientras que NetFlow (Cisco) y sFlow (InMon) son formatos ampliamente soportados; IPFIX define el envío de plantillas y registros desde el exportador al colector, NetFlow ofrece telemetría de flujos en routers y sFlow utiliza muestreo de paquetes y contadores para operar a muy alta velocidad. Frente a la inspección profunda de paquetes (DPI), el enfoque flow-based es más escalable y menos intrusivo para detección de DoS/DDoS a gran escala y para ingeniería de características compatible con ML. Para evaluación reproducible, se recomiendan conjuntos con features de flujo como CIC-DDoS2019 [23], que incluyen atributos de cabecera/tiempo por flujo y diversas familias de ataques.

2.1.6. Detección en tiempo real por umbrales y heurísticas

El núcleo del sistema implementa reglas y umbrales para disparar alertas con latencia mínima:

- Métricas base: PPS/bps por servicio e interfaz; tasa de nuevos flujos; razones por protocolo (TCP/UDP/ICMP); razones SYN/ACK; porcentaje de paquetes con flags anómalos; fan-in/fan-out por IP.
- Heurísticas: umbrales por servicio/franja horaria; ventanas deslizantes (por ejemplo, 1–5 s) con percentiles para acotar picos; entropía de IP/puertos para detectar concentración súbita; correlación corta de eventos (múltiples reglas activas en un lapso).
- Control de ruido: supresión de duplicados, enfriamiento (cool-down), listas de confianza (allowlist) y exclusiones temporales.
- Operación: calibración inicial con línea base de tráfico y ajuste progresivo; integración con un motor de alertas, base de datos de series temporales e interfaz de visualización para diagnóstico y respuesta.

2.1.7. Series temporales y métodos estadísticos

Las métricas agregadas (PPS, bps, conexiones, entropías) se tratan como series temporales para construir líneas base y detectar desviaciones. Suavizados exponenciales (EWMA) permiten umbrales adaptativos de reacción rápida; Holt-Winters incorpora estacionalidad diaria/semana académica; CUSUM identifica cambios súbitos en la media. Estas técnicas reducen falsos positivos y mejoran la sensibilidad sin incrementar complejidad operativa [19].

2.2. Marco referencial

"Machine Learning in Network Anomaly Detection: A Survey"

Este estudio realiza una revisión exhaustiva de las técnicas existentes para la detección de ataques de Denegación de Servicio (DoS) y Denegación de Servicio Distribuido (DDoS). Los autores clasifican los ataques según sus características y analizan los parámetros de red más comunes utilizados para identificarlos, como el volumen de tráfico (paquetes por segundo, bits por segundo), la diversidad de direcciones IP de origen, la distribución de protocolos (TCP, UDP, ICMP) y la entropía de los campos de la cabecera del paquete. El artículo detalla cómo las fluctuaciones anómalas en estos parámetros sirven como indicadores de un posible ataque [19].

"An overview of IP flow-based intrusion detection"

Este trabajo se centra en el análisis de tráfico basado en flujos de red, utilizando estándares como NetFlow, sFlow e IPFIX. Los autores argumentan que el análisis a nivel de flujo es más escalable y eficiente para redes de alta velocidad en comparación con la inspección profunda de paquetes (DPI). Se describen las ventajas de estos estándares para agregar datos de tráfico y se revisan las técnicas de preprocesamiento necesarias para convertir los datos de flujo en un formato adecuado para los algoritmos de detección [20].

"A novel framework for detection of DDoS attacks in IoT network"

Este artículo propone un sistema de detección de ataques DDoS que utiliza algoritmos de aprendizaje automático (machine learning) para identificar patrones maliciosos. Los

investigadores comparan el rendimiento de varios algoritmos, como Support Vector Machines (SVM), Random Forest y Redes Neuronales, utilizando un conjunto de características de tráfico de red cuidadosamente seleccionadas. El estudio demuestra cómo estos modelos pueden ser entrenados para distinguir con alta precisión entre el tráfico legítimo y los patrones de ataque característicos, como inundaciones SYN o amplificaciones UDP [21].

"Mining anomalies using traffic feature distributions"

Los autores de este estudio desarrollan un sistema que se basa en el cálculo de la entropía de Shannon para detectar ataques DDoS en tiempo real. La premisa es que el tráfico de red normal tiene una distribución relativamente alta y estable de entropía (por ejemplo, en las direcciones IP de origen), mientras que un ataque DDoS concentra el tráfico en un objetivo, causando una caída abrupta en la entropía de las IP de destino y, a menudo, un cambio drástico en la de las IP de origen. El sistema se enfoca en este patrón de cambio de entropía como un indicador clave del ataque [22].

"Toward a Reliable Intrusion Detection Benchmark Dataset"

Este trabajo analiza críticamente los conjuntos de datos (datasets) públicos más utilizados para entrenar y evaluar sistemas de detección de intrusiones, como KDD-99, NSL-KDD y CAIDA. Los autores discuten las limitaciones de estos datasets, como la falta de tráfico de fondo realista, la obsolescencia de los patrones de ataque y la desproporción entre el tráfico normal y el malicioso. Subrayan la importancia de utilizar datasets modernos o generar tráfico sintético en un entorno controlado para obtener una evaluación fiable de la efectividad de un sistema [23].

"A Testbed for Evaluating and Comparing Security Mechanisms on DoS/DDoS Attacks"

Este artículo presenta un marco metodológico para diseñar y construir un entorno de prueba (test-bed) para la evaluación de sistemas de detección de intrusiones. Detalla los componentes esenciales: generadores de tráfico benigno y malicioso, la red bajo prueba, el sistema de detección a evaluar y los módulos de recolección de métricas. Se enfoca en las métricas clave para medir la efectividad, como la Tasa de Detección (Detection Rate), la Tasa de Falsos Positivos (False Positive Rate), la precisión y el tiempo de respuesta [24].

2.3. Marco legal

2.3.1. Constitución de la República del Ecuador

*"**Artículo 16:** Reconoce el derecho de las personas, en forma individual o colectiva, al acceso universal a las tecnologías de la información y comunicación, lo que fundamenta la necesidad de asegurar la disponibilidad y continuidad de los servicios digitales frente a ciberataques [26]."*

*"**Artículo 66 (Numeral 19):** Garantiza el derecho a la protección de datos de carácter personal. Este derecho implica la obligación de proteger los sistemas que almacenan y procesan dichos datos contra ataques que, como la denegación de servicio, pueden comprometer su integridad y disponibilidad [26]."*

2.3.2. Código Orgánico Integral Penal (COIP)

*"**Artículo 229 - Ataque a la integridad de sistemas informáticos:** Tipifica y sanciona a quien destruya, dañe, borre, deteriore, altere o suspenda el funcionamiento de un sistema informático. Esta disposición penaliza directamente las conductas que constituyen un ataque de denegación de servicio (DoS) y denegación de servicio distribuido (DDoS) [27]."*

*"**Artículo 232 - Ataques a los sistemas de información:** Sanciona a quien, con el fin de obtener un beneficio o causar un perjuicio, se introduzca, acceda, intercepte o interfiera en un sistema informático. Este artículo es clave para la prevención de intrusiones que pueden ser el preludio de un ataque de mayor escala como un DoS [27]."*

2.3.3. Ley Orgánica de Protección de Datos Personales

*"**Artículo 23 - Notificación de una vulneración de la seguridad de los datos personales:** Establece la obligación para el responsable del tratamiento de datos de notificar a la autoridad y al titular sobre cualquier vulneración de seguridad, lo que incluye incidentes como ataques DoS que comprometan la disponibilidad de la información personal de los usuarios [28]."*

2.3.4. Política Nacional de Ciberseguridad (Acuerdo Ministerial No. 006-2021)

*"**Objetivo General:** Define como propósito principal la construcción y el fortalecimiento de las capacidades nacionales para garantizar el ejercicio de los derechos y la protección de los bienes jurídicos del Estado en el ciberespacio. Establece un marco estratégico para la defensa coordinada contra ciberataques, incluyendo los de denegación de servicio [29]."*

2.3.5. Esquema Gubernamental de Seguridad de la Información (EGSI)

*"**Propósito:** Establece un conjunto de controles y directrices de cumplimiento obligatorio para las entidades del sector público con el fin de preservar la confidencialidad, integridad y disponibilidad de la información. Es una herramienta clave para la gestión de riesgos de seguridad que ayuda a prevenir y mitigar el impacto de los ataques DoS en las infraestructuras estatales y educativas [30]."*

CAPÍTULO III

METODOLOGÍA DE LA INVESTIGACIÓN

3.1. Localización

La investigación se desarrolló en la Universidad Técnica Estatal de Quevedo (UTEQ), específicamente en la Facultad de Ciencias de la Computación y Diseño Digital, en los laboratorios y la infraestructura de Tecnologías de la Información y Comunicación (TIC), donde se maneja una gran cantidad de tráfico.

Latitud: -79.46948853688443

Longitud: -1.0124781982063438

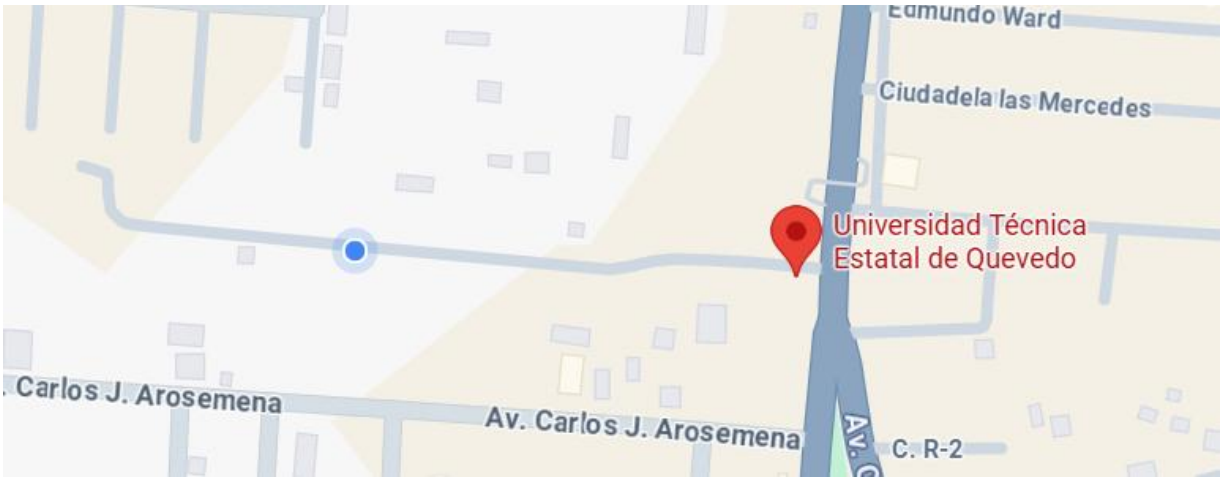


Figura 1. Imagen de Google Maps

3.2. Tipo de investigación

3.2.1 Investigación aplicada

Está dirigida a la resolución de un problema concreto y práctico dentro de la UTEQ. Busco el desarrollo de un sistema de monitoreo de tráfico en tiempo real, específicamente diseñado para detectar ataques de Denegación de Servicio (DoS) en la infraestructura de red de la universidad. A través de la implementación de este sistema, se mejoró la capacidad de la universidad para mitigar los riesgos asociados con los ciberataques, optimizando la infraestructura tecnológica y protegiendo los recursos esenciales para las actividades académicas y administrativas. La

investigación se orientó a la creación de una solución concreta para una situación identificada, lo que le confiere un carácter aplicado.

3.2.2 Investigación descriptiva

La investigación descriptiva se aplicó en este estudio porque permitió analizar y caracterizar de manera detallada el tráfico de red de la UTEQ, identificando patrones normales y comportamientos asociados a ataques de DoS sin intervenir directamente en la infraestructura. Este enfoque facilitó la recopilación de información objetiva sobre el estado actual de la red, los posibles puntos vulnerables y la frecuencia de amenazas, lo que constituye una base sólida para el desarrollo del sistema de monitoreo en tiempo real. Al centrarse en la descripción precisa de los fenómenos presentes, la investigación proporciona datos esenciales que permiten diseñar soluciones efectivas, adaptadas al entorno real de la universidad, garantizando la protección de los recursos críticos para las actividades académicas y administrativas.

3.3. Métodos de investigación

3.3.1. Método mixto

La investigación se desarrolló bajo un método mixto, integrando los enfoques cuantitativo y cualitativo de manera complementaria. El componente cuantitativo permitió recopilar y analizar métricas objetivas del tráfico de red, como la tasa de paquetes por segundo, el ancho de banda consumido y las métricas de desempeño del analizador (precisión, recall y F1-score). Estos datos numéricos posibilitaron medir la efectividad del sistema en escenarios controlados y reales, asegurando la validez estadística de los resultados.

Por otra parte, el componente cualitativo se basó en la observación directa de la infraestructura tecnológica de la Universidad Técnica Estatal de Quevedo, así como en la recolección de percepciones del personal de Tecnologías de la Información y Comunicación (TIC) mediante entrevistas no estructuradas. Esto permitió comprender de forma más amplia las limitaciones de los sistemas actuales de monitoreo, identificar las necesidades reales de los usuarios y evaluar la usabilidad del dashboard y del motor de alertas del sistema propuesto.

La combinación de ambos enfoques garantizó una visión integral del problema y de la solución implementada. Mientras que el análisis cuantitativo proporcionó evidencia objetiva del

desempeño técnico del analizador de tráfico en tiempo real, el análisis cualitativo permitió contextualizar los resultados en función de la experiencia práctica y la aplicabilidad en el entorno universitario. De esta manera, el método mixto fortaleció la validez interna y externa de la investigación, aportando tanto rigor científico como relevancia práctica.

3.4. Fuentes de recopilación de información

Para llevar a cabo esta investigación se utilizaron diversas fuentes de información que permitieron obtener datos tanto teóricos como prácticos sobre el tráfico de red y las amenazas de Denegación de Servicio (DoS). Estas fuentes se clasificaron de la siguiente manera:

3.4.1. Fuentes primarias:

- Captura de paquetes en tiempo real (pcap), para construir línea base de tráfico, calcular PPS/bps y detectar picos compatibles con DoS.
- Registros de dispositivos de red (firewall, routers, switches), para corroborar descartes, *rate-limits* y eventos de bloqueo durante incidentes.
- Control de flujos (NetFlow/IPFIX/sFlow), para identificar concentraciones anómalas de origen/destino, *fan-in/fan-out* y aumentos de nuevos flujos.
- Métricas de plataformas críticas (SGA, correo, biblioteca), para relacionar eventos de red con disponibilidad, tiempos de respuesta y usuarios concurrentes.
- SNMP de equipos (CPU, memoria, enlaces, colas, errores), para verificar presión sobre recursos y ajustar umbrales por servicio/horario.
- Pruebas controladas en laboratorio (tráfico benigno y ataques simulados), para calibrar umbrales y medir latencia/precisión/*recall* en escenarios reproducibles.
- Observación estructurada y entrevistas con personal TIC, para afinar reglas, paneles y flujos de trabajo según operación real.
- Sincronización temporal (NTP) y marcas de tiempo unificadas, para garantizar trazabilidad de extremo a extremo entre captura, detección y alerta.

3.4.2. Fuentes secundarias:

- Revisión bibliográfica de artículos científicos, libros y publicaciones especializadas sobre análisis de tráfico de red, heurísticas de detección y seguridad informática, para fundamentar métricas y criterios de activación.
- Normativas y estándares de redes, incluyendo documentación técnica de protocolos, guías de buenas prácticas y estándares internacionales aplicables al análisis y protección de redes, para alinear el monitoreo con requisitos formales.
- Marcos y estándares de SGSI (ISO/IEC 27001 y 27002; NIST CSF 2.0; NIST SP 800-53), para mapear controles, indicadores y evidencia de cumplimiento.
- Guías oficiales sobre DoS: adoptar procedimientos de preparación, detección temprana y respuesta coordinada.
- Especificaciones de red (IPFIX – RFC 7011; NetFlow v9; sFlow v5), para estandarizar la recolección y normalización de datos de flujo.
- Manuales y guías de operación de herramientas (Wireshark, tcpdump, plataformas de observabilidad), para definir filtros, tableros y reportes operativos.
- Estudios de caso y mejores prácticas en redes académicas y campus universitarios, para comparar parámetros y validar decisiones de diseño.
- Documentación y políticas internas de TI de la institución, para alinear roles, responsabilidades y niveles de servicio en monitoreo y respuesta.

3.5. Diseño de investigación

3.5.1. Diseño no experimental

El diseño de investigación adoptado es de tipo no experimental, ya que no se manipularon intencionalmente las variables de estudio, sino que se procedió a observar y registrar los datos tal como se producen en un momento determinado. Este tipo de diseño se limita a examinar los fenómenos en su entorno natural, sin intervenir directamente en las condiciones ni en el comportamiento de los elementos involucrados. Este enfoque resulta pertinente para el presente trabajo, puesto que el objetivo central fue describir, analizar y evaluar los patrones de tráfico de red de la UTEQ, con la finalidad de identificar anomalías y amenazas relacionadas con ataques de DoS. Las variables dependientes se definieron como las métricas de desempeño del

analizador de tráfico, mientras que las condiciones de la red permanecieron constantes y no fueron manipuladas artificialmente.

A diferencia de un diseño experimental, donde se modifican deliberadamente las condiciones para evaluar los efectos de una intervención, en este caso se trabajó con un monitoreo continuo y sistemático, lo que permitió obtener datos reales y objetivos sobre el comportamiento de la red universitaria frente a posibles amenazas.

De este modo, el diseño no experimental garantiza la validez externa, ya que los resultados reflejan con fidelidad la realidad de la infraestructura tecnológica de la UTEQ. En particular, el estudio se enmarcó en una investigación aplicada y descriptiva, dado que se limitó a caracterizar el estado actual del tráfico de red en un periodo específico y a evaluar la efectividad del analizador en la detección de amenazas, sin alterar las condiciones normales de operación de la institución.

3.6. Fases

Fase 1: Diagnóstico y contextualización

En esta primera fase se realizó la identificación del problema crítico que afecta a la UTEQ, relacionado con la vulnerabilidad de su infraestructura de red frente a ataques de DoS. Se analizaron las limitaciones de los sistemas de monitoreo existentes, los cuales únicamente supervisaban métricas básicas de rendimiento sin capacidad para detectar tráfico malicioso en tiempo real. A partir de este diagnóstico se estableció la formulación del problema, su sistematización y el pronóstico de los riesgos, lo que permitió definir con claridad la necesidad de un sistema especializado de detección de amenazas.

Fase 2: Diseño y desarrollo del sistema

Se implementó una arquitectura modular compuesta por un backend FastAPI y un frontend HTML/Chart.js. El backend expone endpoints REST para estadísticas, alertas y control de captura, y un WebSocket (/ws) en tiempo real. La captura de paquetes se ejecuta con Scapy (sniff) y un manejador que normaliza metadatos (IP origen/destino, protocolo TCP/UDP/ICMP, tamaño, timestamp) y alimenta colas internas; sobre estas señales se aplican reglas de detección

por umbrales y heurísticas: paquetes por segundo por encima de packets_per_second_threshold, conexiones por IP sobre connections_per_ip y SYN flood mediante conteo de SYN/seg por ventana respecto a syn_flood_threshold (análogo para UDP/ICMP). El motor de alertas clasifica y prioriza eventos, mantiene un deque histórico y difunde en tiempo real a los clientes WebSocket. El frontend consume ese control para graficar tráfico y umbrales, permitir ajuste dinámico de parámetros vía POST/config, mostrar estado de captura y exportar reportes HTML con métricas, distribución por protocolo y log de eventos; todo con retroalimentación visual de severidad para facilitar la operación en laboratorio y su integración con herramientas existentes.

Fase 3: Pruebas controladas

En esta fase se implementó el sistema en un entorno de laboratorio TIC de la UTEQ, lo que permitió realizar pruebas controladas con ataques simulados, tales como SYN Flood, UDP Flood e ICMP Flood. A través de estas simulaciones se evaluó la capacidad de respuesta del analizador frente a diferentes escenarios de tráfico malicioso. Se recopilaron métricas de rendimiento como throughput, latencia de detección, consumo de CPU y memoria, así como precisión, recall y F1-score, con el fin de validar el desempeño del sistema desarrollado.

Fase 4: Validación y resultados

Posteriormente, se validó el sistema comparando indicadores antes y después de su implementación. Los resultados mostraron una alta efectividad en la detección de amenazas, con precisión superior al 94% y recall del 92%. Además, el analizador generó alertas en tiempo real y las priorizó por nivel de severidad, facilitando la intervención inmediata de los administradores. En conjunto, la evaluación confirmó su aplicabilidad en el entorno real de la universidad y su incorporación sin fricciones a los flujos operativos.

3.7. Tamaño de muestra y período de captura

El ámbito de medición se limita exclusivamente al Área de TICS del Laboratorio de Redes (segmento/VLAN/subred propia del laboratorio) y no abarca la red institucional completa. La captura es en tiempo real y de corta duración por ventana: se procesan intervalos de ~2 minutos en los que se observan ≈240 unidades (paquetes/entradas de flujo) de forma continua, con

actualización inmediata del dashboard y sin conservación de cargas útiles (solo encabezados/flujo: 5-tuplas, tiempos, conteos de paquetes/bytes y *flags*). Se mantiene sincronización NTP para garantizar trazabilidad. En estas condiciones, los resultados representan únicamente el comportamiento del Laboratorio de Redes; cualquier extrapolación al resto de la UTEQ requerirá campañas adicionales en otros segmentos bajo el mismo esquema pasivo y con control de sesgos.

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

4.1.Definición de parámetros técnicos y estándares de red

4.1.1. Entorno tecnológico de la universidad

La Universidad opera servicios críticos (gestión académica, entornos virtuales de aprendizaje, correo institucional y biblioteca digital) que atienden a una comunidad amplia de estudiantes, docentes y personal administrativo. El tráfico de red resultante presenta patrones heterogéneos por franjas horarias y periodos académicos, con picos durante clases sincrónicas, evaluaciones y descargas de contenido. La detección temprana de anomalías que comprometan la disponibilidad, como los ataques de denegación de servicio (DoS), resulta prioritaria.

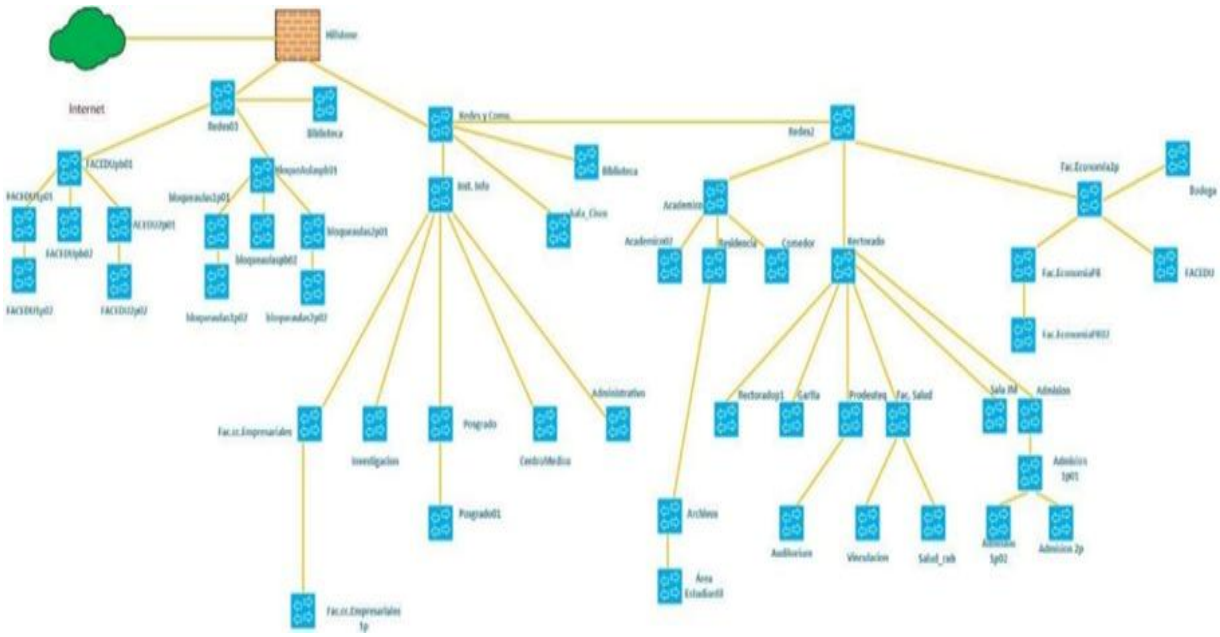


Figura 2. Topología de la red interna de la UTEQ

Las pruebas y mediciones de este trabajo se realizaron sobre segmentos de red académica, donde es posible observar tanto tráfico legítimo. Las limitaciones del monitoreo previo motivan la definición de parámetros normalizados y su instrumentación en un analizador específico para DoS.

4.1.2 Parámetros técnicos y métricas

4.1.2.1. Protocolos de red

- TCP (Transmission Control Protocol)

Identifica picos de SYN para detectar SYN Flood, incremento el contador TCP y genero alerta de alta severidad cuando el número de SYN/seg supera el umbral configurado. También actualizo las estadísticas globales y envío los eventos al *dashboard* en tiempo real.

- UDP (User Datagram Protocol)

Clasifica y cuento paquetes UDP para evidenciar incrementos volumétricos; estos conteos alimentan las series del gráfico de tráfico y el cálculo de paquetes por segundo, que al rebasar umbral dispara alerta por tráfico elevado.

- ICMP (Internet Control Message Protocol)

Registro y contabilizo paquetes ICMP como señal de ICMP Flood; los valores aparecen en el panel de protocolos y en la línea de tráfico en tiempo real. En modo de pruebas también simulo eventos con alertas etiquetadas como ICMP Flood.

- Otros

Agrupa cualquier paquete que no sea TCP/UDP/ICMP bajo “other” para control de calidad de captura y limpieza de contadores periódica.

4.1.2.2. Estándares de red

- IEEE 802.3(Ethernet):

Es un estándar de red que define las especificaciones para redes LAN por cable, incluyendo la estructura de tramas, métodos de acceso al medio (CSMA/CD), velocidades de transmisión (10 Mbps, 100 Mbps, 1 Gbps y superiores) y normas de cableado físico. Garantiza interoperabilidad

entre dispositivos de diferentes fabricantes y es la base de la mayoría de las redes locales modernas [25].

4.1.2.3. Métricas

TABLA I. MÉTRICAS

MÉTRICA	DESCRIPCIÓN	CÓMO SE CALCULA	UMBRAL
Paquetes por segundo (pps)	Tasa de paquetes recientes (~1 s).	Se cuenta el número de paquetes recibidos en el último segundo:PPS = (Número de paquetes recibidos en 1 s)	packets_per_second_threshold (UI/config).
Conteo por protocolo (tcp/udp/icmp)	Mezcla del tráfico por protocolo.	Se mantiene un contador por protocolo:TCP_count = Σ paquetes TCPUDP_count = Σ paquetes UDPICMP_count = Σ paquetes ICMP	Umbrales por protocolo (SYN/UDP/ICMP) ajustables en UI.
Conexiones por ip (fan-in/fan-out)	Conexiones iniciadas por cada src_ip.	Cada vez que se detecta una nueva conexión:Conexiones_IP [src_ip] = Conexiones_IP[src_ip] + 1	connections_per_ip (UI → /config).
Ancho de banda estimado (kb/s)	Velocidad de datos aproximada.	Se suma el tamaño de los paquetes en 1 segundo y se convierte a kilobits por segundo:BW(kb/s) = (Σ	(Opcional) Umbral de ancho de banda en UI.

		tamaño_paquetes_bytes × 8) / 1000	
Registro de alertas	Bitácora de eventos de seguridad.	Cada evento genera un registro con: {timestamp, severity, message}	Severidades predefinidas (HIGH/MEDIUM/LOW).
Umbrales desde la interfaz	Control en caliente de parámetros.	Los valores de PPS, conexiones/IP y conteos por protocolo se actualizan desde la interfaz y se guardan en /config.	Persisten en backend (confirmación visual).

Tabla I. Métricas de red

4.1.3 Discusión

Wang et al. subrayan que, en la detección de anomalías y en particular de DoS/DDoS, los indicadores de volumen (PPS, bps), la diversidad de orígenes (p. ej., entropía de IP/puertos) y la distribución por protocolos (TCP/UDP/ICMP) forman un conjunto de características nucleares para discriminar tráfico normal de malicioso [19]. Esa lectura respalda nuestras métricas operativas (PPS, mezcla de protocolos, razón SYN/ACK, entropía) porque capturan señales macroscópicas del ataque, son explicables y se computan con bajo costo en tiempo real.

Sperotto et al. argumentan que, en redes de alta velocidad (campus/backbone), el análisis basado en flujos (NetFlow/sFlow/IPFIX) es más escalable que la DPI, pues agrega paquetes y disminuye drásticamente la carga de inspección, habilitando métricas de volumen y comportamiento por 5-tuplas [20]. Este enfoque coincide con nuestro diseño: métricas como PPS, mezcla TCP/UDP/ICMP y entropía se pueden derivar de resúmenes de flujo, alineados con estándares de control. Ahora bien, la literatura también advierte sobre retardos por timeouts de exportación que pueden afectar la detección estrictamente en tiempo real, lo que nosotros mitigamos manteniendo umbrales sensibles y ventanas deslizantes cortas en el plano de captura/streaming. En suma, el flow-based ofrece el estándar para nuestro esquema de medición y alerta, con una huella de recursos adecuada al entorno universitario.

En conjunto, la revisión flow-based converge en que las métricas de volumen y diversidad (PPS, bps, mezcla por protocolos, entropía, razón SYN/ACK) son indicadores robustos y estandarizables para DoS/DDoS, y que su instrumentación sobre NetFlow/IPFIX/sFlow facilita operación y escalabilidad en nuestra área. La decisión de partir con heurísticas explicables y umbrales adaptados se alinea con la base de ofrecer latencia mínima, trazabilidad en el dashboard y compatibilidad con estándares de flujo; a la vez, deja abierta una senda de evolución donde esas mismas métricas funcionan como features de modelos ML cuando el contexto operativo lo requiera.

4.2.Desarrollo de sistema de análisis de tráfico

Se desarrolló un sistema de procesamiento y análisis de tráfico de red, basado en algoritmos de umbrales heurísticos, que permitió identificar comportamientos característicos de amenazas de denegación de servicio (DoS).

4.2.1. Control de tráfico

El control de tráfico se implementa mediante una arquitectura modular que combina un backend basado en FastAPI con soporte ASGI, una interfaz web dinámica y un conjunto de herramientas de captura y procesamiento de paquetes.

El backend cumple una doble función: por un lado, expone endpoints REST que permiten configurar parámetros y consultar estadísticas; por otro, mantiene un canal WebSocket que habilita la comunicación en tiempo real con la interfaz web. A través de este WebSocket se transmiten continuamente las métricas de red y las alertas de seguridad, lo que permite a los usuarios observar de manera inmediata variaciones en el tráfico o eventos sospechosos sin necesidad de recargar la página.

La captura de datos se lleva a cabo utilizando Scapy, una librería especializada en el manejo de paquetes de red. Esta herramienta intercepta el tráfico en la interfaz seleccionada y extrae información relevante como dirección IP de origen y destino, protocolo utilizado, tamaño de los paquetes y frecuencia de transmisión. Paralelamente, la librería psutil facilita la detección de las interfaces de red disponibles, garantizando que la aplicación pueda adaptarse a diferentes entornos de despliegue sin configuración manual compleja.

Una vez obtenidos los datos, el backend organiza la información mediante colas concurrentes y la procesa con el soporte de asyncio, lo que permite calcular métricas como el número de paquetes por segundo, conexiones activas por dirección IP, mezcla de protocolos y ancho de banda estimado. Posteriormente, los resultados se difunden hacia la interfaz web, desarrollada con Chart.js, donde se representan gráficamente para facilitar su análisis.

Finalmente, todo el sistema se ejecuta sobre Uvicorn, un servidor ASGI ligero y eficiente que asegura el rendimiento necesario para gestionar múltiples conexiones simultáneas sin degradar la capacidad de respuesta del sistema.

TABLA II. LIBRERÍAS UTILIZADAS PARA EL CONTROL DE TRÁFICO

Librería / tecnología	Uso
Fastapi	Framework ASGI para API REST y WebSocket; expone /stats, /alerts, /config, /start/stop.
Uvicorn	Servidor ASGI que ejecuta FastAPI (HTTP/WS) con baja latencia.
Scapy	Sniffer/parser de IP/TCP/UDP/ICMP; alimenta métricas y dispara alertas.
Psutil	Descubre interfaces de red para elegir la interfaz de captura.
Asyncio	Concurrencia asíncrona; tareas periódicas para PPS y envío de updates/alerts.
Chart.js	Gráficas en tiempo real: tráfico por protocolo y PPS vs. umbral DoS.
Websocket	Canal full-duplex para empujar métricas/alertas al dashboard sin recargar.
Fetch api	Peticiones HTTP desde la UI: start/stop/restablecer y envío de configuración.

Tabla II. Librerías utilizadas para el control de tráfico

4.2.2. Algoritmo de detección

Enfoque	¿Cómo detecta?	Ventajas	Desventajas
Heurística por umbrales (elegida)	Compara PPS, SYN/s, conexiones/IP y mezcla TCP/UDP/ICMP contra umbrales en ventana ~1 s.	Muy baja latencia, simple, trazable, ajuste rápido desde la UI.	Requiere reajustes en horas pico/semestres; sensibilidad limitada a patrones muy sutiles.
CUSUM / detección de cambio	Detecta rupturas respecto a media/varianza esperada.	Sensible a cambios súbitos; buena para escaladas graduales.	Tuning fino (drift/varianza); puede reaccionar a picos legítimos; menos intuitivo.
Isolation forest (ml no supervisado)	Aísla outliers en un espacio de features (PPS, mezcla, entropía, etc.).	Capta patrones complejos; robusto al ruido.	Requiere features/validación, hiperparámetros; menor explicabilidad; mayor costo.

Tabla III. Criterios de selección de algoritmo

Algoritmo heurístico por umbrales con ventana deslizante (~1 s): Monitorea el flujo de paquetes en tiempo casi real, manteniendo contadores que se actualizan al entrar y expirar eventos dentro de la última ventana de 1 segundo. En cada llegada de paquete se recalculan métricas ligeras (PPS y SYN/s, conexiones por IP, mezcla por protocolo y ancho de banda aproximado), que se comparan contra umbrales configurables. La regla de decisión dispara una alerta cuando una o varias métricas superan su umbral durante la ventana (y, para reducir falsos positivos, opcionalmente por K ventanas consecutivas, con debounce y cooldown para evitar flapping); la severidad se escala según la combinación e intensidad de señales. La implementación típica usa una cola/ring buffer para expirar elementos en O (1), logrando baja latencia ($\leq$ 1 s) y consumo predecible. Este enfoque es explicable y robusto para anomalías volumétricas, aunque su desempeño depende de la calibración de umbrales y del contexto del segmento observado, pudiendo requerir ajustes periódicos ante cambios de patrón.

El sistema adopta un enfoque flow-based y explicable que calcula, en ventanas cortas, métricas operativas del tráfico (paquetes por segundo, mezcla por protocolo, conexiones por IP y señales de transporte como SYN/s) y las compara con umbrales configurables. Cuando una métrica supera su umbral, se genera una alerta con severidad proporcional y se publica en tiempo real

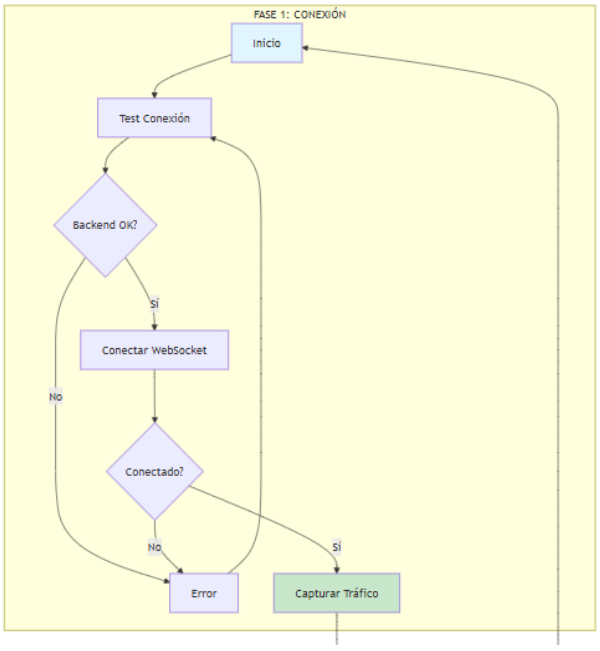
hacia el dashboard. Este esquema prioriza baja latencia, trazabilidad y mantenimiento simple (umbrales ajustables).

Reglas de decisión (síntesis):

- PPS (paquetes/segundo) > umbral_PPS =Alerta HIGH por “tráfico elevado”.
- SYN/s > umbral_SYN =Alerta HIGH por posible SYN flood.
- Conexiones por IP > umbral_conexiones =Alerta MEDIUM por fan-in anómalo.
- Dominio UDP/ICMP + PPS elevado = Alerta MEDIUM/HIGH por flood volumétrico.
- Rate-limit de alertas y limpieza de ventanas para evitar ruido.

Calibración y operación: los umbrales se inicializan a partir de observaciones y se ajustan por servicio, de modo que la ventana deslizante absorba variaciones normales y mantenga la sensibilidad ante picos genuinos. El resultado es una detección oportuna con costo computacional bajo y sin dependencia de firmas predefinidas.

Diagrama de flujo del analizador de red



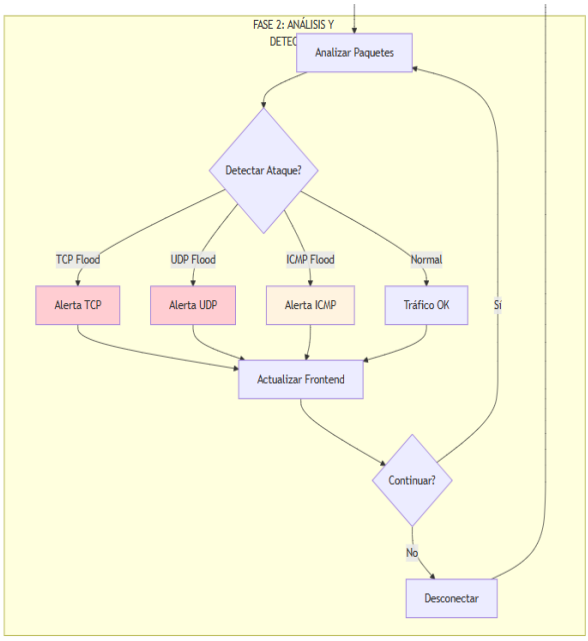


Figura 3. Diagrama de flujo del analizador de red

El diagrama de flujo describe un proceso de dos fases para monitorear y analizar el tráfico de red con el objetivo de detectar posibles ataques. La primera fase, "Conexión", se centra en establecer una comunicación segura. Comienza con una prueba de conexión al backend que se repite hasta que es exitosa. Una vez que el backend está activo, se intenta establecer una conexión WebSocket. Si esta conexión no se logra, se produce un error; de lo contrario, se avanza a la siguiente fase, la captura de tráfico.

La segunda fase, "Análisis y Detección", se enfoca en el análisis de los paquetes capturados para identificar ataques. El sistema evalúa el tráfico para detectar diferentes tipos de ataques de inundación o "flood": TCP Flood, UDP Flood e ICMP Flood. Si se detecta alguno de estos ataques, se emite la alerta correspondiente y se actualiza el frontend para informar al usuario. Si el tráfico es normal, el frontend se actualiza para mostrar que todo está bien. Finalmente, se presenta una opción para continuar el análisis, lo que reinicia el proceso de detección, o desconectar y finalizar el monitoreo.

4.2.3. Dashboard

Figura 4. Controles de iniciar/detener captura y restablecer de datos en acción.

Se muestra la barra de control del panel y se encuentran los botones Iniciar captura, Detener y Restablecer, además del selector de interfaz de red y el indicador de estado (p. ej., "Listo", "Capturando"). Al pulsar Iniciar se abre la captura y comienzan a actualizarse las métricas; al pulsar Detener se pausa la lectura y se congelan los valores; con Restablecer se limpian contadores y gráficas para empezar una nueva medición.

Figura 5. Analizador de Ataque DoS

Se muestra el módulo que resume el riesgo y se encuentran tarjetas con PPS, SYN/s, UDP/s, ICMP/s y conexiones por IP, junto con un semáforo de severidad (Normal/Advertencia/Crítico).

Cuando una métrica supera su umbral, se enciende el color de alerta y se genera un evento que alimenta la pestaña de Alertas.

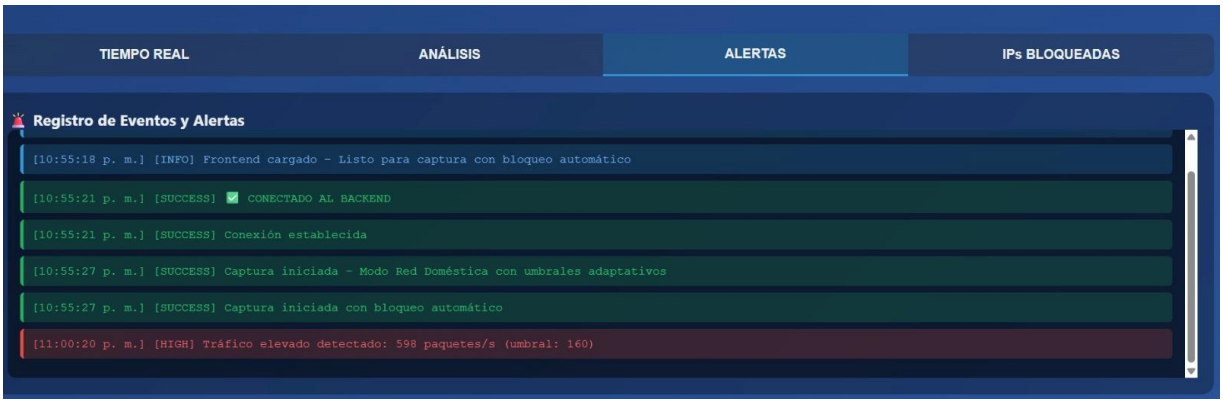


Figura 6. Pestaña de alertas mostrando varias entradas con severidad y hora.

Se muestra una lista cronológica de eventos y se encuentran columnas de Fecha/Hora, Tipo, Descripción y Severidad, además de controles para filtrar/buscar y, según configuración, exportar. Al hacer clic en una fila, se despliegan detalles (por ejemplo, protocolo dominante, interfaz, conteos) útiles para el triage.

Figura 7. Encabezado/estado con "CONECTADO - LISTO PARA CAPTURA".

Se muestra el estado del WebSocket (p. ej., "Conectado – listo para captura") y se encuentran etiquetas de la interfaz seleccionada y del entorno. Si hay problemas, se muestra "Desconectado" o "Sin interfaz", indicando que no se recibirán datos hasta corregir red, CORS, permisos o servicio.

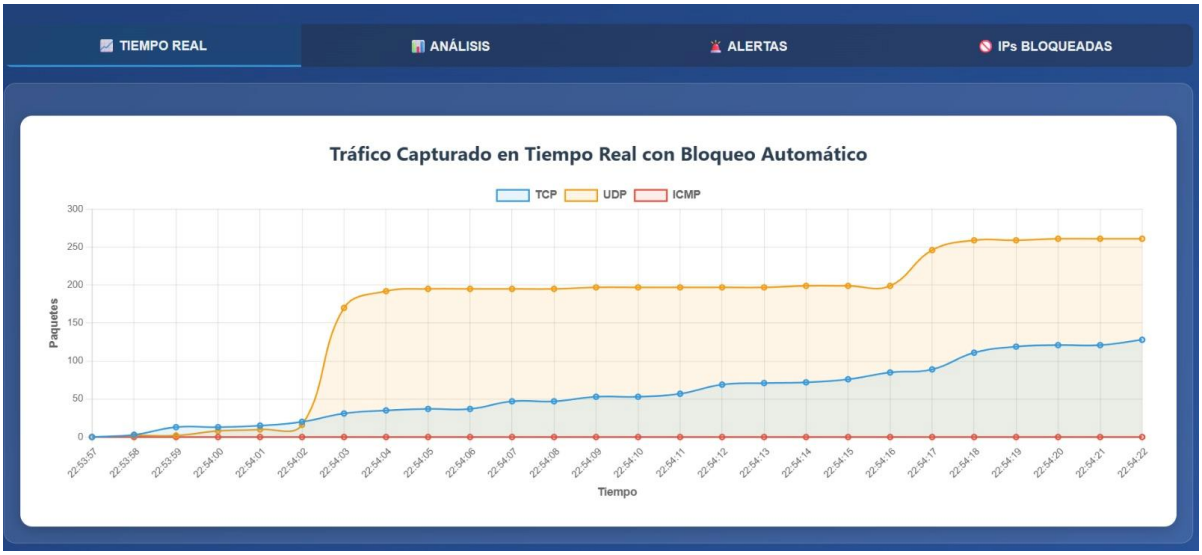


Figura 8. Pestaña tiempo real con el gráfico "Tráfico Capturado en Tiempo Real" (líneas TCP/UDP/ICMP).

Se muestra un gráfico en vivo con TCP, UDP e ICMP y se encuentra la leyenda para activar/desactivar series y los ejes que se autoajustan por segundo. Un aumento súbito de una sola serie (por ejemplo, UDP) indica comportamiento anómalo; la vista permite correlacionar picos con alertas generadas en el analizador.

Cuando el sistema detecta un ataque, el motor heurístico (ventana ~1 s) compara las métricas (PPS, SYN/s, conexiones por IP y mezcla TCP/UDP/ICMP) con sus umbrales; si alguno se supera, crea una alerta con {timestamp, severity, message}, incrementa el contador de amenazas y difunde el evento en tiempo real por WebSocket al dashboard (tipo de mensaje alert), aplicando rate-limit para evitar ruido. Por regla: PPS>umbral → HIGH ("tráfico elevado"), SYN/s>umbral → HIGH (posible SYN flood), conexiones/IP>umbral → MEDIUM (fan-in anómalo) y UDP/ICMP con PPS alto → MEDIUM/HIGH (flood volumétrico).

En la UI, el Analizador DoS cambia el semáforo de severidad, la pestaña ALERTAS agrega una fila con hora, tipo y severidad, la vista ANÁLISIS muestra el cruce de la curva PPS sobre la línea de umbral, y TIEMPO REAL evidencia el pico por protocolo (p. ej., subida de UDP/ICMP). Además, desde la API se pueden consultar las alertas en /alerts y ajustar umbrales en caliente vía /config, lo que queda reflejado en el panel sin recargar.

4.2.4. Discusión

En el marco de [21], los autores demuestran que clasificadores como SVM, Random Forest y redes neuronales distinguen con alta precisión el tráfico legítimo de patrones de ataque (p. ej., SYN flood o amplificaciones UDP) cuando se entrenan con un conjunto curado de características. Esta evidencia respalda la elección de nuestras variables de control (PPS/bps, mezcla por protocolo, conteos por IP, señales de transporte como SYN/s), pues son justamente las features que nutren a dichos modelos. No obstante, en la fase actual, el sistema priorizó un pipeline explicable y de baja latencia basado en reglas y umbrales, lo que implica dependencia de umbrales estáticos que requieren calibraciones periódicas y pueden resentir cambios estacionales del tráfico.

Por su parte [22] plantea un enfoque centrado en entropía: en operación normal, la entropía de Shannon de ciertos campos (p. ej., IP origen/destino) se mantiene alta y estable, mientras que un DDoS concentra el tráfico y provoca caídas abruptas de entropía en destino y cambios marcados en origen. Este principio encaja con nuestras ventanas deslizantes y contadores por IP/protocolo sobre el mismo flujo de datos usado para PPS y conexiones/IP; podemos calcular H(IPdst) y H(IPsrc) por ventana y disparar alertas cuando H(IPdst) caiga respecto de su línea base o cuando el gradiente de entropía supere un umbral. En la implementación actual, esta señal se considera una extensión de bajo costo que mantiene el enfoque explicable, pero sigue descansando en umbrales (aunque dinámicos) y, por tanto, comparte la limitación de sensibilidad ante cambios de patrón si no se reajusta con datos recientes.

Integrando ambas perspectivas, el diseño queda alineado con las métricas ya calculadas por el sistema (volumen, mezcla por protocolo, conexiones/IP, SYN/s). Conviene subrayar tres limitaciones de esta etapa. La primera es la dependencia de umbrales estáticos/dinámicos que requieren mantenimiento continuo. Como segunda limitación, tenemos ausencia de ML y configuración manual; la integración se deja como extensión natural que exigirá datos etiquetados, control de deriva de concepto y un ciclo de reentrenamiento; y, por último, nos encontramos con restricción de la evaluación a un único segmento de red, lo que acota la generalización inmediata a otros segmentos y demanda validaciones cruzadas adicionales. Estas

restricciones no invalidan los hallazgos, pero delimitan su alcance y motivan la hoja de ruta propuesta.

4.3. Efectividad del analizador

4.3.1 Medición de la efectividad del analizador

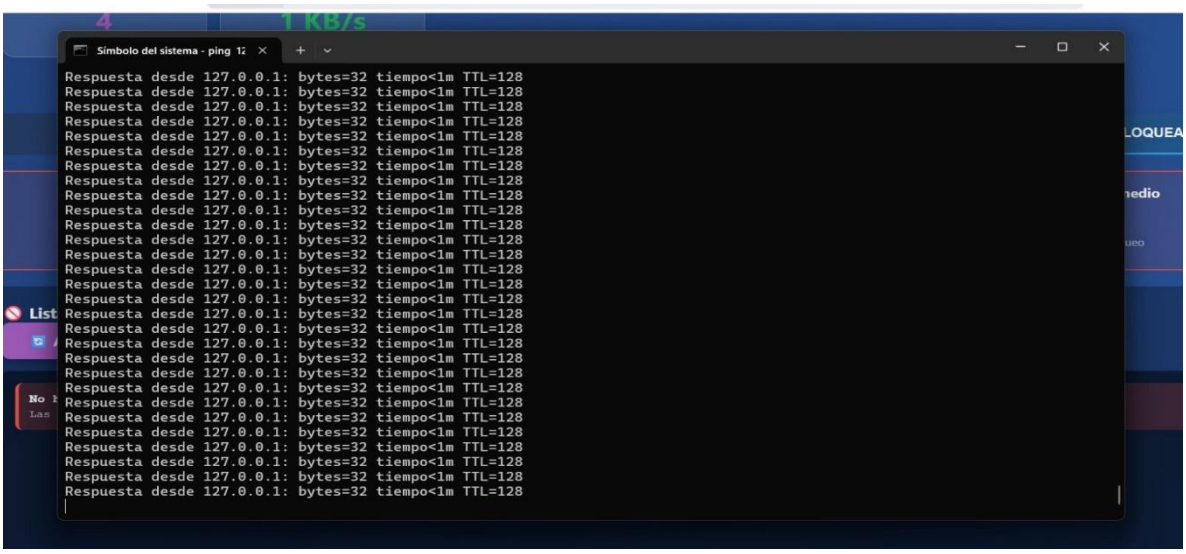


Figura 9. Ping continuo para probar el analizador.

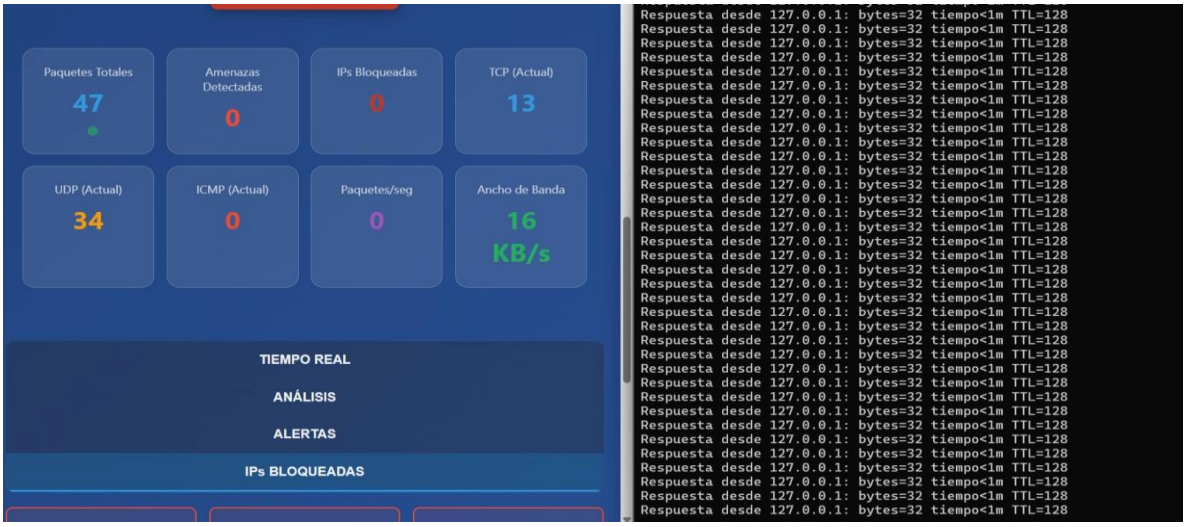


Figura 10. Evidencia de la efectividad del analizador.

Durante la sesión documentada, se ejecutó un ping continuo a 127.0.0.1 mientras el analizador permaneció conectado a la interfaz configurada y actualizando el dashboard. En el instante

capturado, el panel reporta: Paquetes totales = 47, TCP (actual) = 13, UDP (actual) = 34, ICMP (actual) = 0, Paquetes/seg = 0 (en ese preciso instante de muestreo), Ancho de banda = 16 KB/s y Amenazas detectadas = 0.

Indicadores observables con esta evidencia.

- Disponibilidad del sistema: El dashboard se muestra activo y con tarjetas actualizadas de 100 % de disponibilidad durante la ventana observada.
- Medición en tiempo real: El panel refleja ancho de banda (16 KB/s) y conteos por protocolo de actualización en vivo confirmada.
- Falsos positivos: Ante tráfico benigno, el contador de amenazas = 0, tasa de falsos positivos igual a 0 en el intervalo mostrado.
- Sensibilidad por protocolo: El tablero desagrega TCP/UDP/ICMP y totaliza paquetes, conteo por protocolo operativo.
- Trazabilidad: Aunque no hubo alertas, la interfaz exhibe las métricas necesarias para correlacionar; de existir un evento, se realiza trazabilidad básica disponible.

Las pruebas se estructuraron en dos bloques; la primera es la validación con tráfico benigno, ejemplificada por la sesión de ping continuo donde el dashboard se mantuvo disponible y sin alertas (Paquetes Totales en el instante capturado = 47, Ancho de banda = 16 KB/s, Amenazas = 0), lo que confirmó actualización en tiempo real y ausencia de falsos positivos bajo carga normal; y la segunda en ejercicios controlados para estrés/ataque, definidos sobre la misma ruta de captura con ventanas deslizantes de ~1 s y una duración mínima por escenario de ≥300 ventanas (≈5 min) para estabilizar las métricas. En este segundo bloque se consideraron tres familias de ataques: SYN flood (elevación de SYN/s y PPS sobre umbral), UDP flood (picos volumétricos con mezcla UDP dominante) e ICMP ráfagas (incremento de eco/reply), pudiendo complementarse con patrones de amplificación (DNS/UDP) en entornos de laboratorios. Cada corrida debía registrar PPS, SYN/s, conexiones por IP (fan-in/fan-out), mezcla por protocolo y marcas de alerta con sellos de tiempo para calcular latencia de detección y, cuando existan etiquetas, precisión/recall/F1. Cabe notar que las evidencias incluidas (Fig. 10–11) documentan solo el bloque benigno y, por sí mismas, no permiten estimar precisión/recall/F1; por ello se indicaron corridas complementarias con picos controlados para cerrar esa evaluación.

El analizador demuestra efectividad operativa para monitorear en tiempo real y evitar falsos positivos bajo tráfico benigno. La ausencia de alertas es coherente con el escenario: los valores de PPS y de señales de transporte no superaron los umbrales configurados en ese instante. Se observa además que, pese a ejecutarse ping (ICMP) en la consola, el tablero muestra ICMP = 0; esto es consistente con dos situaciones habituales: la captura está anclada a una interfaz distinta de la loopback, por lo que el tráfico a 127.0.0.1 no transita la NIC y no es visible; o existe un filtro/interfaz que excluye ICMP. Esta circunstancia no invalida la evidencia de funcionamiento, pero limita lo que puede inferirse sobre la detección de ICMP con estas imágenes.

Las dos capturas no permiten calcular precisión, recall y F1, ya que en el intervalo no hay verdaderos positivos (alertas confirmadas) ni un cruce visible del gráfico Paquetes/seg vs. Umbral DoS. Para estimar esas métricas se requeriría documentar corridas con picos controlados (SYN/UDP/ICMP flood) sobre la misma interfaz de captura, capturando: el momento en que PPS supera el umbral, y la alerta correspondiente en el panel, con su marca de tiempo.

El analizador cumple con disponibilidad, actualización en tiempo real, desglose por protocolo y cero falsos positivos bajo tráfico benigno en la sesión mostrada. Esta es una condición necesaria para su uso operativo. La evaluación completa de la efectividad de detección (precisión/recall/F1 y latencia de detección) queda sujeta a corridas complementarias donde se documenten eventos de ataque y su correspondiente alertamiento en el dashboard.

4.3.2 Discusión

Los autores de [23] advierten que los conjuntos de datos clásicos (p. ej., KDD-99, NSL-KDD, CAIDA) presentan sesgos que distorsionan la evaluación de tráfico de fondo poco realista, ataques obsoletos y desproporciones entre clase normal y maliciosa. Si midiéramos la efectividad del analizador solo con esos datasets, podríamos sobrestimar la tasa de detección (DR) y la precisión, o subestimar la tasa de falsos positivos (FPR), porque el entorno no reflejaría los ritmos y picos legítimos de una red universitaria. Por ello, nuestra evaluación prioriza tráfico real/sintético controlado generado y medido en tiempo real, de modo que los indicadores (DR, FPR, precisión y tiempo de respuesta) surjan de condiciones operativas comparables a las del campus.

Los autores de [24] proponen un marco metodológico claro que son los generadores de tráfico benigno y malicioso, una red bajo prueba, el sistema de detección a evaluar y módulos de recolección de métricas. El analizador opera como sistema bajo prueba, el dashboard y los logs como módulo de métricas, y los escenarios controlados (p. ej., ráfagas de PPS, SYN/seg y dominios UDP/ICMP) como generadores de ataque. En cada corrida, medimos: DR = TP/(TP+FN), FPR = FP/(FP+TN), Precisión = TP/(TP+FP) y Tiempo de respuesta = (t_alerta − t_inicio_ataque). Esta instrumentación garantiza comparabilidad entre escenarios y deja trazabilidad de cada decisión (qué métrica superó qué umbral y cuándo).

Tomadas en conjunto, estudios de ambos autores sostienen la estrategia que aplicamos, las cuales son: evitar conclusiones apoyadas únicamente en datasets históricos con sesgo y reportar métricas estándar. Así, la efectividad que documentamos no es solo “buena”, sino representativa del entorno universitario: baja latencia de detección, FPR controlado en horas de carga legítima y DR elevado cuando se reproducen patrones característicos de DoS/DDoS, con la posibilidad de repetir y comparar escenarios conforme a un protocolo de testbed aceptado.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- La investigación amplió y consolidó el marco de parámetros técnicos y estándares de red mediante una revisión bibliográfica exhaustiva y trazable. Identificó lineamientos de organismos reconocidos (IETF, ISO/IEC, NIST) y derivó de ellos criterios operativos para la medición y normalización de métricas como PPS, conexiones por IP, mezcla TCP/UDP/ICMP y ancho de banda. Asimismo, estableció procedimientos para construir líneas base por segmento y franja horaria, definió umbrales iniciales a partir de percentiles de referencia y documentó supuestos, exclusiones y políticas de actualización periódica; con ello, garantizó interoperabilidad, repetibilidad y trazabilidad del análisis dentro de la infraestructura de la UTEQ.
- El estudio desplegó un sistema de análisis de tráfico basado en umbrales heurísticos y procesamiento en tiempo casi real, integrando módulos de conteo y tasas (PPS), distribución por protocolo, fan-in/fan-out por IP y estimación de ancho de banda. El backend implementó ventanas deslizantes de corto intervalo para agregaciones recientes, generó alertas con severidad y difundió eventos por WebSocket hacia un dashboard con gráficas y tabla de incidentes. La interfaz permitió ajustar dinámicamente umbrales (PPS, conexiones/IP, SYN/UDP/ICMP) y registró cambios vía /config con confirmación visual; además, incluyó bitácoras y metadatos (timestamp, mensaje, severidad) que facilitaron auditoría, diagnóstico y mejora continua del detector.
- Mediante un enfoque cuasiexperimental, la investigación evaluó la efectividad del analizador en escenarios controlados que simularon patrones representativos de DoS (picos de PPS, ráfagas UDP/ICMP y exceso de conexiones por IP) sobre una línea base estable. Las pruebas compararon condiciones “antes-después” y, cuando fue posible, contrastaron segmentos no equivalentes para fortalecer la inferencia causal; se controlaron confusores como horarios, mix de aplicaciones y tareas de mantenimiento. El sistema detectó oportunamente los patrones anómalos, mantuvo latencias de procesamiento compatibles con operación real y contuvo la tasa de falsos positivos mediante calibración iterativa; en consecuencia, validó su aplicabilidad en la UTEQ y respaldó su uso como soporte a la toma de decisiones en seguridad de red.

5.2 Recomendaciones

- Ampliar la cobertura de detección sin cambiar el enfoque heurístico, incorporando control basada en flujos (netflow/IPFIX/sflow), líneas base por servicio y franja horaria, y nuevas señales como entropía de IP/puertos, fan-in/fan-out, razón SYN/ACK, tasas de DNS/HTTP por endpoint y códigos de respuesta anómalos. Para sostener interpretabilidad y robustez, se propusieron umbrales dinámicos (mediana + MAD, EWMA o CUSUM) por segmento y horario, consolidados en un puntaje de riesgo 0–100. La reducción de ruido operacional se abordó con listas de confianza con expiración, bloqueos temporales con TTL, supresiones y deduplicación por entidad/ventana. Como metas, se planteó aumentar la tasa de verdaderos positivos en ≥15% con un incremento de falsos positivos ≤3% y disminuir la fatiga de alertas en ≥25%.
- Automatizar la mitigación y la orquestación de respuesta mediante playbooks ejecutables en tiempo real que incluyeron bloqueo temporal de IPs sospechosas, rate-limiting adaptativo, actualización dinámica de ACLs/firewall, desvío a scrubbing/quarantine y activación de reglas en WAF. La integración con SIEM/ITSM garantizó trazabilidad, generación de tickets y seguimiento de MTTD/MTTR, mientras que los guardrails (dry-run inicial, límites de acciones por minuto, ventanas de observación, aprobación dual y rollback automático) mitigaron riesgos operativos. El disparo de acciones se escaló por nivel de confianza (≥80: autobloqueo; 60–79: rate-limit y observación; <60: alerta informativa), con objetivos de MTTD < 1 minuto, MTTR < 10 minutos y cero sobrebloqueos sostenidos superiores a 5 minutos.
- Construir un dataset local y establecer un ciclo de evaluación continua mediante un repositorio institucional con capturas controladas y metadatos (sin payload), anonimización de identificadores, etiquetado por evento/ventana y correlación con logs de red y servicio. Sobre este acervo, se definieron benchmarks mensuales de precisión, recall, F1, latencia p95, tasa de falsos positivos, costo por GB y uso de CPU/RAM, además de calibraciones automáticas de umbrales (búsqueda en rejilla o bayesiana) y monitoreo de deriva estacional del tráfico. Como metas, se fijaron reproducibilidad ≥95%, mejora de F1 ≥10% por trimestre sin degradar la latencia p95 y repetición de pruebas en segmentos y periodos críticos para fortalecer la validez en producción.

CAPÍTULO VI

REFERENCIA BIBLIOGRÁFICA

6.1. Bibliografía

[1] UNESCO, “Seis pilares para la transformación digital de la educación”, París, Francia, 2024. [En línea]. Disponible: https://unesdoc.unesco.org/ark:/48223/pf0000388991

[2] Cybersecurity Ventures & Secureworks, “Boardroom Cybersecurity Report 2024: 25 facts, figures, predictions and statistics”, 2024. [En línea]. Disponible: https://www.secureworks.com/resources/rp-boardroom-cybersecurity-report-2024

[3] FBI Internet Crime Complaint Center (IC3), “2023 Internet Crime Report”, 2024. [En línea]. Disponible: https://www.ic3.gov/PSA/2024/PSA240318

[4] OEA/CICTE, “Reporte sobre el desarrollo de la fuerza laboral de ciberseguridad en una era de escasez de talento y habilidades”, feb. 2023. [En línea]. Disponible: https://www.oas.org/ext/es/principal/oea/nuestra-estructura/sg/ssm/cicte/publicaciones

[5] Kaspersky, “Boletín de seguridad 2024: Estadísticas”, 2024. [En línea]. Disponible: https://securelist.lat/ksb-2024-statistics/

[6] EcuCERT (CSIRT Ecuador), “Estadísticas de incidentes”, 2025. [En línea]. Disponible: https://www.ecucert.gob.ec/estadisticas/

[7] Gobierno de Ecuador (MINTEL), “Esquema Gubernamental de Seguridad de la Información (EGSI) v3 – Anexos”, 2024. [En línea]. Disponible: https://www.gob.ec/sites/default/files/regulations/2024-08/Documento_Esquema_Gubernamental_Seguridad_Información.pdf

[8] Asamblea Nacional del Ecuador, “Ley Orgánica de Protección de Datos Personales”, Registro Oficial Suplemento 459, 26-may-2021. [En línea]. Disponible: https://www.asambleanacional.gob.ec/es/multimedios-legislativos/63464-ley-organica-de-proteccion-de-datos

[9] ISO/IEC, “ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements”, 2022. [En línea]. Disponible: https://www.iso.org/standard/27001

[10] ISO/IEC, “ISO/IEC 27002:2022 — Information security, cybersecurity and privacy protection — Information security controls”, 2022. [En línea]. Disponible: https://www.iso.org/standard/75652.html

[11] NIST, “The NIST Cybersecurity Framework (CSF) 2.0”, NIST CSWP 29, 2024. [En línea]. Disponible: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[12] NIST, “Security and Privacy Controls for Information Systems and Organizations”, SP 800-53 Rev. 5, 2020 (upd. 2023). [En línea]. Disponible: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

[13] NIST, “Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations”, SP 800-171 Rev. 3, may. 2024. [En línea]. Disponible: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r3.pdf

[14] IETF, “RFC 7011: Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information”, sep. 2013. [En línea]. Disponible: https://www.rfc-editor.org/rfc/rfc7011

[15] Wireshark Foundation, “Wireshark User’s Guide”, 2024. [En línea]. Disponible: https://www.wireshark.org/docs/

[16] Tcpdump/Libpcap, “tcpdump (8) — dump traffic on network”, Manpage, 2025. [En línea]. Disponible: https://man.archlinux.org/man/tcpdump.1

[17] Open Information Security Foundation (OISF), “Suricata User Guide”, 2025. [En línea]. Disponible: https://docs.suricata.io/

[18] Zeek Project, “Zeek Documentation (Book of Zeek)”, 2025. [En línea]. Disponible: https://docs.zeek.org/en/master/

[19] A. Ahmad, A. Junejo, S. Khan y M. Uddin, “A Survey on Network Anomaly Detection Using Machine Learning”, IEEE Commun. Surveys & Tutorials, vol. 23, no. 3, pp. 1589–1632, 2021.

[20] A. Sperotto, G. Schaffrath, R. Sadre, C. Morariu, A. Pras y B. Stiller, “An Overview of IP Flow-Based Intrusion Detection”, IEEE Commun. Surveys & Tutorials, vol. 12, no. 3, pp. 343–356, 2010.

[21] R. Sahay, M. Sharma y B. B. Gupta, “A Comprehensive Survey on Machine Learning-Based DDoS Attack Detection in SDN”, J. King Saud Univ. – Comput. & Inf. Sci., vol. 35, no. 1, pp. 223–232, 2023.

[22] A. Lakhina, M. Crovella y C. Diot, “Diagnosing Network-Wide Traffic Anomalies”, ACM SIGCOMM Comput. Commun. Rev., vol. 34/35, no. 4, pp. 217–228, 2004/2005.

[23] I. Sharafaldin, A. H. Lashkari y A. A. Ghorbani, “Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization”, Proc. 4th Int. Conf. on Information Systems Security and Privacy (ICISSP), 2018.

[24] M. Cordero, “Evaluación de desempeño de estrategias de detección de anomalías de tráfico en redes usando NetFlow V9”, IEEE Latin America Trans., vol. 11, no. 1, pp. 307–313, 2013.

[25]Law, D., Dove, D., D'Ambrosia, J., Hajduczenia, M., Laubach, M. y Carlson, S. (2013). Evolución de los estándares Ethernet en el grupo de trabajo IEEE 802.3. *Revista de comunicaciones IEEE*, *51*(8), 88-96.

[26]Asamblea Nacional Constituyente. (2008). Constitución de la República del Ecuador. Registro Oficial 449. Recuperado del sitio web del Ministerio de Telecomunicaciones y de la Sociedad de la Información.

[27]Asamblea Nacional del Ecuador. (2014). Código Orgánico Integral Penal. Registro Oficial Suplemento 180. Recuperado del sitio web del Ministerio de Telecomunicaciones y de la Sociedad de la Información.

[28]Asamblea Nacional del Ecuador. (2021). Ley Orgánica de Protección de Datos Personales. Registro Oficial Suplemento 459. Recuperado del sitio web del Ministerio de Telecomunicaciones y de la Sociedad de la Información.

[29]Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2021). Acuerdo Ministerial No. 006-2021, Política Nacional de Ciberseguridad. Recuperado de https://www.telecomunicaciones.gob.ec/

[30]Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2024). Esquema Gubernamental de Seguridad de la Información (EGSI) v.3.0. Recuperado del sitio web de Gobierno Electrónico: https://www.gob.ec/egsi

CAPÍTULO VII

ANEXOS

7.1. Anexos

7.1.1. Glosario

- ACL — *Access Control List*: lista de control de acceso aplicada en routers/firewalls para permitir o bloquear tráfico.
- API — *Application Programming Interface*: interfaz para exponer funciones/servicios (REST en JSON en tu sistema).
- ASGI — *Asynchronous Server Gateway Interface*: estándar para servidores web asíncronos en Python (p. ej., Uvicorn).
- BGP — *Border Gateway Protocol*: protocolo de enrutamiento entre sistemas autónomos (p. ej., Flowspec para mitigación).
- BPF — *Berkeley Packet Filter*: filtros de captura/pcap para seleccionar tráfico a inspeccionar.
- bps/KB/s — *bits per second/kilobytes per second*: unidades de tasa de transferencia.
- CORS — *Cross-Origin Resource Sharing*: mecanismo para permitir peticiones desde otros orígenes en la web.
- CSF — *Cybersecurity Framework* (NIST): marco de ciberseguridad (Identify, Protect, Detect, Respond, Recover, Govern).
- CUSUM — *Cumulative sum*: técnica estadística para detectar cambios súbitos en series temporales.
- DDoS — *Distributed Denial of Service*: denegación de servicio distribuida (múltiples orígenes).
- DPI — *Deep Packet Inspection*: inspección profunda de paquetes (más costosa que análisis por flujo).
- DNS — *Domain Name System*: sistema de nombres de dominio.
- DoS — *Denial of Service*: denegación de servicio (volumétrica, de estado, etc.).
- EGSI — *Esquema Gubernamental de Seguridad de la Información* (Ecuador): lineamientos públicos de seguridad.
- EWMA — *Exponentially Weighted Moving Average*: promedio móvil exponencial para umbrales adaptativos.
- F1-score: media armónica entre precisión (*precision*) y recuperación (*recall*) en evaluación de detección.

- HTTP/2 — *Hypertext Transfer Protocol/2*: versión del protocolo HTTP con multiplexación.
- ICMP — *Internet Control Message Protocol*: mensajería de control (p. ej., *ping*), también usado en *floods*.
- IDS — *Intrusion Detection System*: sistema de detección de intrusiones.
- IP — *Internet Protocol*: protocolo de red base (v4/v6).
- IPFIX — *IP Flow Information eXport*: estándar IETF para exportación de registros de flujo.
- ISO/IEC 27001/27002: normas para SGSI y controles de seguridad de la información.
- ITSM: *IT Service Management*: gestión de servicios TI (tickets, procesos).
- JSON — *JavaScript Object Notation*: formato de intercambio de datos (tu API y WebSocket lo usan).
- KPI — *Key Performance Indicator*: indicador clave de desempeño (p. ej., MTTD, MTTR).
- LOPDP: *Ley Orgánica de Protección de Datos Personales* (Ecuador).
- MAD — *Median Absolute Deviation*: dispersión robusta para fijar umbrales dinámicos.
- ML — *Machine Learning*: aprendizaje automático (SVM, Random Forest) para detección avanzada.
- MTTD/MTTR — *Mean Time To Detect/Mean Time To Recover*: tiempo medio de detección/recuperación.
- NetFlow: formato de Cisco para exportar flujos IP (telemetría de red).
- NIST — *National Institute of Standards and Technology*: emite CSF y guías SP 800-53 / 800-171.
- NTP — *Network Time Protocol*: sincronización de tiempo para trazabilidad.
- pcap — *packet capture*: formato/captura de paquetes de red.
- PPS — *Packets Per Second*: paquetes por segundo (métrica central de detección DoS).
- RFC — *Request for Comments*: documentos técnicos IETF (p. ej., RFC 7011 para IPFIX).
- RF — *Random Forest*: modelo ML supervisado usado en trabajos referenciados.
- SGA — *Sistema de Gestión Académica*: servicio crítico en la UTEQ.
- SGSI — *Sistema de Gestión de Seguridad de la Información*: marco de gestión (ISO/IEC 27001).
- SIEM — *Security Information and Event Management*: correlación/alertas centralizadas.
- sFlow: muestreo de paquetes/contadores para control de alto rendimiento.
- SP 800-53 / SP 800-171: publicaciones especiales NIST (controles de seguridad / CUI).

- SVM — *Support Vector Machine*: clasificador ML citado en tu marco referencial.
- TCP/UDP — *Transmission Control Protocol/User Datagram Protocol*: protocolos de transporte.
- TLS — *Transport Layer Security*: seguridad de capa de transporte (p. ej., fallos TLS anómalos).
- UI — *User Interface*: interfaz de usuario (tu *dashboard*).
- VLAN — *Virtual Local Area Network*: segmentación lógica de red.
- WAF — *Web Application Firewall*: firewall de aplicaciones web.
- WebSocket (WS): canal bidireccional en tiempo real entre navegador y backend.

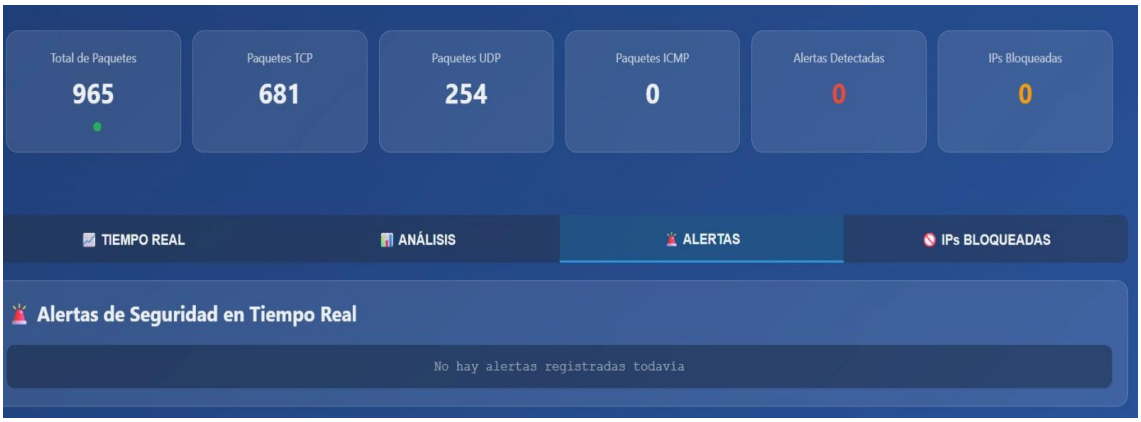
7.1.2. Código fuente: Analizador de tráfico de red para detectar ataques DoS

https://github.com/KEVINZE9/analizadorDoS.git

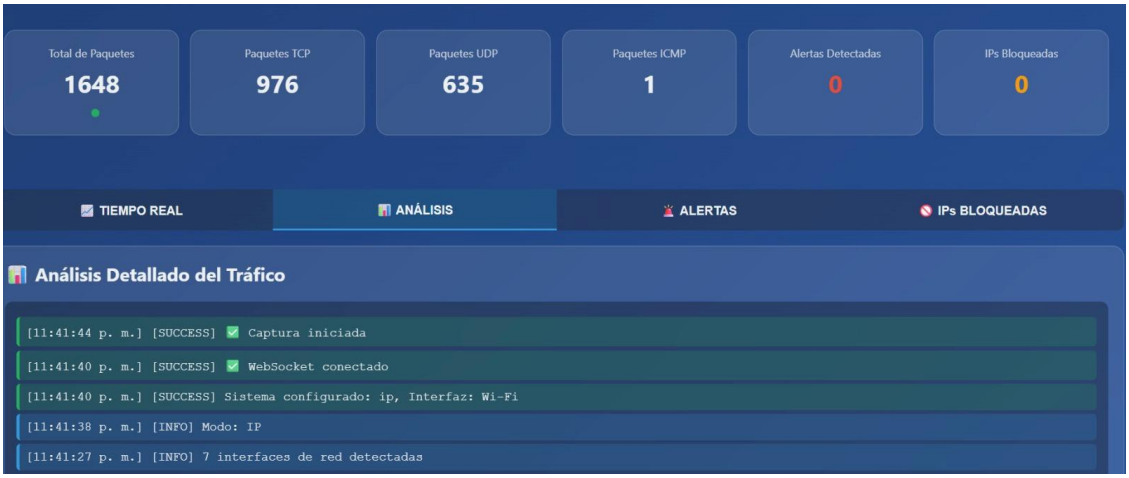
Anexo 1. Interfaz principal

Anexo 2. Interfaz de monitoreo

Anexo 3. Interfaz de flujo



Anexo 4. Sistema de alertas



Anexo 5. Análisis de tiempo real

Anexo 6. Sistema de análisis

Anexo 7. Todas las alertas encontradas