UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TITULO DEL TRABAJO DE TITULACIÓN

MONITOREO DE RED INTELIGENTE USANDO IDS Y DISPOSITIVOS DE EDGE COMPUTING

AUTOR

TIGRERO TIGRERO, DIANA GRACE

TRABAJO DE INTEGRACIÓN CURRICULAR

Previo a la obtención del grado académico en
INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

TUTOR

Lsi. Daniel Quirumbay Yagual, MSIA

Santa Elena, Ecuador

Año 2024

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por Tigrero Tigrero Diana Grace, como requerimiento para la obtención del título de Ingeniero en Tecnologías de la Información.

La Libertad, a los 13 días del mes de diciembre del año 2024

TUTOR

DANIEL IVAN QUIRUMBAY YAGUAL

Lsi. Daniel Quirumbay Yagual, MSIA

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **DIANA GRACE TIGRERO TIGRERO**

DECLARO QUE:

El trabajo de Titulación, "**Monitoreo de red inteligente usando ids y dispositivos de edge computing"**, previo a la obtención del título en Ingeniero en Tecnologías de la Información, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

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

La Libertad, a los 13 días del mes de diciembre del año 2024

EL AUTOR

Diana Grace Tigrero Tigrero

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado "**Monitoreo de red inteligente usando ids y dispositivos de edge computing"**, presentado por el estudiante, **Diana Grace Tigrero Tigrero** fue enviado al Sistema Antiplagio, presentando un porcentaje de similitud correspondiente al 9%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.

TUTOR

DANIEL IVAN QUIRUMBAY YAGUAL

Lsi. Daniel Quirumbay Yagual, MSIA

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

AUTORIZACIÓN

Yo, Diana Grace Tigrero Tigrero

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

Cedo los derechos en línea patrimoniales de artículo profesional de alto nivel con fines de difusión pública, además apruebo la reproducción de este artículo académico dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor

Santa Elena, a los 13 días del mes de diciembre del año 2024

EL AUTOR

Diana Grace Tigrero Tigrero

AGRADECIMIENTO

Mi agradecimiento a Jehová por darme salud, sabiduría, paciencia de seguir y no abandonar este camino hacia mi titulación.

Agradezco a mi hermosa madre Bélgica A. Tigrero B. porque ha sido el pilar fundamental durante toda mi carrera, gracias por tu apoyo incondicional y por cuidar de mí y después a mi hija.

A mi padre Antonio Tigrero y a hermanas Licenciadas Yulissa, Jadira y Dennisse Tigrero por impulsarme a seguir a culminar mis estudios de tercer nivel, gracias por creer en mí.

A mi compañero de vida Joel Escalante por ser parte de este proceso ayudándome en todos los aspectos posibles, A mi hija Grace Isabel Escalante Tigrero que aún no entiende cómo funciona la vida, sin embargo, sé que Jehová la envió a ser la motivación más bonita de mi vida.

Por último, pero no menos importante, a mi tutor de tesis el Lsi. Daniel Quirumbay, quien me ayudo a realizar este trabajo de titulación, agradezco también a la Universidad Estatal Península de Santa Elena por abrirme las puertas de sus instalaciones. Aquí experimenté fracasos, mis logros académicos que me permitieron crecer como persona.

.Diana Grace, Tigrero Tigrero

DEDICATORIA

Este trabajo este dedicado a:

La memoria de mi abuela Dima Balón por ser el ángel que me guía y me protege, aunque ya no estas a mi lado te siento tan presente en todo.

A mi madre Bélgica Tigrero quien, con su amor incondicional, paciencia y consejos me ayudo a cumplir este logro, sin ella nada hubiera sido posible.

A mi padre y mis hermanas Antonio, Yulissa, Jadira, Dennise Tigrero por su apoyo.

A mi esposo Joel Escalante y a mi hija Grace Isabel Escalante Tigrero los amores de mi vida, por la paciencia de siempre esperar mi regreso de la universidad para atenderlos como se merecen, los amo.

Diana Grace, Tigrero Tigrero

INDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El proyecto presenta el desarrollo de un sistema de detección de intrusos (IDS) eficiente y de bajo costo, enfocado en la ciberseguridad en entornos domésticos y pymes. El sistema utiliza herramientas de detección de intrusos como Snort, combinadas con dispositivos edge computing como Raspberry Pi, para monitorear el tráfico de red en tiempo real y reducir la latencia. Además, se integran algoritmos de aprendizaje automático para identificar patrones maliciosos y automatizar la creación de reglas de seguridad. El proyecto sigue una metodología iterativa y se divide en fases que incluyen planificación, análisis, diseño, implementación, pruebas y evaluación. Se realizan pruebas en entornos simulados para validar la precisión del sistema en la detección de amenazas. Una característica destacada es su panel interactivo, que permite la visualización en tiempo real del tráfico y las alertas de seguridad, busca mejorar la ciberseguridad en entornos de recursos limitados mediante soluciones escalables y rentables, aprovechando la computación de borde y el aprendizaje automático para optimizar la detección y prevención de amenazas.

Palabras claves: Ciberseguridad, Detección de intrusos (IDS), Raspberry Pi.

ABSTRACT

The project presents the development of an efficient and low-cost intrusion detection system (IDS) focused on cybersecurity in home and SMB environments. The system uses intrusion detection tools such as Snort, combined with edge computing devices such as Raspberry Pi, to monitor network traffic in real time and reduce latency. In addition, machine learning algorithms are integrated to identify malicious patterns and automate the creation of security rules. The project follows an iterative methodology and is divided into phases that include planning, analysis, design, implementation, testing and evaluation. Tests are conducted in simulated environments to validate the system's accuracy in detecting threats. An outstanding feature is its interactive dashboard, which allows real-time visualization of traffic and security alerts, seeks to improve cybersecurity in resource-constrained environments through scalable and cost-effective solutions, leveraging edge computing and machine learning to optimize threat detection and prevention.

Keywords: Cybersecurity, Intrusion Detection System (IDS), Raspberry Pi.

INTRODUCCIÓN

En el presente proyecto de titulación denominado “Monitoreo de red inteligente usando ids y dispositivos de edge computing”, se propone el diseño e implementación de un sistema de monitoreo de red avanzado que permita mejorar la seguridad tanto en el ámbito doméstico como en pequeñas y medianas empresas (PYMES). Dado el crecimiento exponencial de dispositivos conectados y el incremento de ciberataques dirigidos a redes privadas y empresariales, se hace cada vez más necesario contar con sistemas de seguridad eficientes y en tiempo real que no solo identifiquen, sino que también reaccionen ante amenazas cibernéticas.

El proyecto integra sistemas de detección de intrusiones (IDS) y tecnologías de edge computing, que permiten descentralizar el procesamiento de datos y mejorar la capacidad de respuesta. Esto es especialmente relevante en entornos como el hogar y las PYMES, donde los recursos tecnológicos suelen ser limitados en comparación con grandes organizaciones, pero las vulnerabilidades son igualmente significativas.

Este capítulo 1, se establece las bases para el proyecto de monitoreo de red inteligente utilizando IDS y dispositivos de edge computing, con un enfoque en la implementación de soluciones accesibles y eficientes para la seguridad informática en el hogar y en las instituciones educativas.

En el capítulo 2, se aborda el contexto tanto del entorno doméstico como de la (PyME), detallando la infraestructura tecnológica utilizada y los experimentos realizados para validar el sistema de monitoreo de red inteligente con IDS y dispositivos de edge computing. Se presentan los resultados obtenidos tras la ejecución del IDS en un entorno, subrayando su capacidad para identificar con alta precisión anomalías en el tráfico que contiene el CVS normalizado, particularmente en conexiones HTTPS, gracias a la implementación de reglas especializadas.

Este proyecto contribuye significativamente al fortalecimiento de la ciberseguridad tanto en el entorno doméstico como en la PyME, demostrando cómo la integración de sistemas IDS basados en dispositivos de edge computing y reglas personalizadas puede transformar el análisis y monitoreo del tráfico de red. A través de la detección inteligente de amenazas, como anomalías en el tráfico cifrado y patrones de ataque sofisticados, se

proporciona una capa adicional de seguridad, crucial para proteger datos sensibles en ambos contextos.

Además, este trabajo produce saberes útiles en un gran número de contextos donde la seguridad digital es crucial, fomentando la implementación de tecnologías de vanguardia en la batalla contra las amenazas cibernéticas. Al poner en marcha soluciones eficaces que fusionan vigilancia en tiempo real y análisis a nivel de borde de la red, se fomenta la utilización de herramientas de ciberseguridad contemporáneas que no solo potencian la identificación de ataques, sino que también maximizan la utilización de recursos tecnológicos, volviéndolas asequibles y eficientes tanto para viviendas como para pequeñas empresas.

CAPÍTULO 1. FUNDAMENTACIÓN

1.1. ANTECEDENTES

El crecimiento exponencial de la infraestructura tecnológica en las instituciones educativas y en los hogares ha traído consigo múltiples beneficios, como el acceso rápido a la información, la automatización de procesos administrativos, académicos y domésticos, así como la mejora en la conectividad entre dispositivos. Sin embargo, este avance también ha incrementado significativamente la vulnerabilidad de estas entidades frente a amenazas cibernéticas [1]. Tanto las organizaciones educativas, que manejan grandes volúmenes de datos sensibles, como los hogares, donde dispositivos inteligentes y sistemas conectados son cada vez más comunes, se han convertido en objetivos atractivos para ciberdelincuentes que buscan explotar debilidades en sus sistemas de seguridad. A pesar de la implementación de medidas de protección como firewalls, antivirus y redes privadas virtuales, los ataques cibernéticos son cada vez más sofisticados, lo que pone en peligro tanto la integridad de la información como la continuidad de los servicios tecnológicos en ambos ámbitos.

La Universidad Estatal Península de Santa Elena fue fundada en 1998 y su sede principal se encuentra en La Libertad, Santa Elena. La institución está dirigida por un Rector y Vicerrector Académico, y cuenta con siete facultades. La Facultad de Sistema y Telecomunicaciones (FACSISTEL) fue fundada en el año 2010. Los programas de tecnología de la información, software, telecomunicaciones, electrónica y automatización están disponibles en Facsistel. El campus tiene varias áreas, incluidas oficinas administrativas, salas para docentes y laboratorios especializados en CISCO. Los equipos informáticos en los laboratorios de la facultad están bajo la supervisión de la Dirección de Tecnologías de la Información y Comunicación. La falta de capacitación en ciberseguridad en las instituciones educativas es otro factor importante en este contexto. Muchas veces, los equipos de tecnología de la información (TI) no reciben la capacitación adecuada para implementar y administrar sistemas de detección de intrusos sofisticados. Esto hace que las redes sean más vulnerables y dificulta la adopción de tecnologías más avanzadas. Es esencial crear soluciones que no solo sean efectivas, sino también sencillas de implementar y gestionar, lo que permitirá a las instituciones educativas asegurar sus redes sin depender de especialistas externos [2].

En la actualidad, existen cuatro laboratorios enfocados en las tareas académicas de los alumnos. No obstante, no se lleva a cabo un monitoreo en tiempo real de las páginas web que los alumnos visitan durante sus clases. Esta ausencia de control incrementa la posibilidad de ingresar a páginas web que podrían ser peligrosas, lo que podría poner en riesgo la seguridad de los sistemas de computación de la universidad [2].

En este contexto, los sistemas de detección de intrusiones (IDS) han surgido como una herramienta clave para identificar y prevenir posibles amenazas en las redes. Los IDS permiten analizar el tráfico de red en tiempo real y alertar sobre actividades sospechosas que podrían comprometer la seguridad de la infraestructura. No obstante, la implementación de estos sistemas suele estar limitada por los altos costos asociados a soluciones comerciales, lo que dificulta su adopción en instituciones educativas, especialmente en aquellas que operan con presupuestos reducidos. Por lo tanto, surge la necesidad de buscar alternativas más económicas que mantengan un alto nivel de eficacia en la detección de amenazas [3].

Los dispositivos de edge computing, como las Raspberry Pi, han demostrado ser una solución prometedora en este campo, al ofrecer un enfoque descentralizado para el procesamiento de datos. Estos dispositivos permiten realizar tareas de detección de intrusiones a nivel local, lo que reduce la carga sobre los servidores centrales y mejora la eficiencia del sistema en términos de tiempo de respuesta. Además, su bajo costo los hace accesibles para instituciones educativas con limitaciones presupuestarias. [4] El uso de estos dispositivos en conjunto con sistemas IDS de código abierto, como Snort, Suricata, etc. ofrece una solución robusta y escalable para monitorear redes de manera continua. La creciente sofisticación de los ataques cibernéticos representa otro reto importante. Las técnicas avanzadas como el malware, el ransomware y los ataques de denegación de servicio (DoS) requieren sistemas IDS capaces de adaptarse y evolucionar para detectar nuevas amenazas. Los algoritmos de machine learning, cuando se implementan en sistemas de detección de intrusiones, pueden mejorar significativamente la precisión en la identificación de comportamientos anómalos en la red [4].

1.2. Descripción del Proyecto

El proyecto de tesis titulado "Monitoreo de red inteligente usando IDS y dispositivos de edge computing" tiene como objetivo desarrollar un sistema inteligente de detección de intrusiones (IDS) basado en Python y hardware de bajo costo (como Raspberry Pi), capaz de monitorear, identificar y alertar en tiempo real sobre amenazas de seguridad en redes. Este sistema será una solución robusta para entornos donde los recursos computacionales son limitados, aprovechando la computación en el borde (edge computing) para realizar el procesamiento y análisis de datos cercanos a la fuente de origen, lo que reduce la latencia y mejora la capacidad de respuesta.

La metodología seleccionada para este proyecto es la heurística iterativa, la cual permite un desarrollo flexible y enfocado en la mejora continua del sistema a lo largo de las diferentes fases del proyecto. Esta metodología fomenta la creación de prototipos rápidos y su evaluación mediante pruebas y ajustes sucesivos, permitiendo incorporar mejoras basadas en la experiencia obtenida y en la efectividad del sistema en la detección de intrusiones. De esta manera, el proceso iterativo permitirá optimizar progresivamente los algoritmos y la precisión del IDS, garantizando un enfoque adaptativo y personalizado que se ajuste a las necesidades y características específicas de la red monitoreada.

El proyecto se llevará a cabo en diversas etapas fundamentales: Basándose en la metodología heurística iterativa:

1. **Fase de Planificación y Requisitos**: Definición de los objetivos del proyecto, selección de IDS (Snort), dispositivos de edge computing, y expectativas de los usuarios, junto con la investigación preliminar para la selección del IDS más adecuado.
2. **Fase de Análisis y Diseño**: Diseño de la arquitectura del sistema, definiendo cómo Snort analizará el tráfico, integrará el CSV normalizado para detección de IPs maliciosas, y cómo se gestionarán las reglas de seguridad.
3. **Fase de Implementación**: Desarrollo del sistema de monitoreo con Snort, integración del script de Python para detección de IPs maliciosas, y configuración de reglas en Snort basadas en los datos obtenidos.
4. **Fase de Pruebas**: Validación del sistema en entornos de prueba, utilizando tráfico simulado para medir la efectividad en la detección de IPs maliciosas y la generación automática de reglas en Snort.

5. **Fase de Evaluación y Revisión**: Análisis de los resultados mediante gráficos de rendimiento y detección, ajustes basados en la precisión del sistema, y optimización del monitoreo en tiempo real en el entorno doméstico y la pyme.

1.3. Objetivos del Proyecto

1.3.1. Objetivo General

Diseñar un sistema inteligente de detección de intrusiones (IDS), basado en Python y ordenadores monoplaca (SBC), capaz de monitorear, identificar y alertar sobre amenazas de seguridad en tiempo real.

1.3.2. Objetivos Específicos

⊳ Implementar un entorno de prueba seguro para simular diferentes tipos de ataques e intrusiones, permitiendo evaluar y ajustar la efectividad del IDS en la identificación y notificación de actividades sospechosas.

⊳ Implementar un sistema de captura de tráfico de red utilizando herramientas para capturar paquetes de red en tiempo real.

⊳ Recolectar datos para el análisis de ciberataques mediante algoritmos de machine learning y hardware de bajo costo, con el fin de identificar patrones y comportamientos maliciosos en el tráfico web, facilitando la detección automática y la prevención de amenazas cibernéticas.

⊳ Desarrollar un dashboard o interfaz gráfica para visualizar en tiempo real los resultados y reportes generados por el IDS.

1.4. Justificación del Proyecto

La seguridad es indispensable para proteger la integridad, autenticidad y la confidencialidad de la información, ya que, si no se implementan correctamente las políticas de seguridad, estaríamos expuestos a diversas amenazas que ponen en riesgo la información de la institución [5]. Actualmente es importante dar seguridad a la información y a los datos que se transmiten en las redes, a la vez tener políticas de seguridad para proteger los datos de posibles intrusiones que afecten a dicho intercambio de datos. Existen herramientas diseñadas para atacar a las redes internas de una empresa con el único fin de robar o dañar la información que se maneja, el administrador de red debe de conocer estos tipos de ataques para poder prevenir y/o proteger la red.

En la actualidad, la seguridad informática se ha convertido en una prioridad fundamental para organizaciones de todos los tamaños, debido al incremento en la frecuencia y sofisticación de los ciberataques. Dentro de este contexto, los Sistemas Inteligentes de Detección de Intrusos (IDS) juegan un papel crucial al permitir la identificación y mitigación de actividades maliciosas dentro de una red [6]. Sin embargo, muchos IDS existentes son costosos y requieren hardware especializado, lo que puede ser un obstáculo para su implementación en pequeñas y medianas empresas, así como en entornos con recursos limitados.

El presente trabajo de tesis titulado "Monitoreo de red inteligente usando ids y dispositivos de edge computing tiene como objetivo desarrollar un sistema accesible y

eficiente que facilite la detección de tráfico web malicioso mediante técnicas de sistemas inteligentes y minería de datos. Este proyecto se enmarca dentro de una línea de investigación "Detección automática de tráfico HTTP malicioso mediante el desarrollo de sistemas inteligentes y minería de datos". La elección de hardware de bajo costo se justifica en la necesidad de generalizar el acceso a tecnologías avanzadas de seguridad informática, permitiendo que organizaciones con presupuestos limitados puedan protegerse adecuadamente contra amenazas cibernéticas. Utilizando dispositivos económicos, como el raspberrypi3 que es considerado de bajo costo, se pretende demostrar que es posible implementar soluciones de alta efectividad sin incurrir en gastos significativos.

El proyecto favorecerá directamente a FACSISTEL al ofrecer un ids que pueda supervisar la red en tiempo real, lo que facilitará a los profesionales administrativo y técnico tomar decisiones más fundamentadas para salvaguardar y robustecer la seguridad informática de la institución. Es crucial implementar soluciones tecnológicas en consonancia con las mejores prácticas de ciberseguridad para preservar la integridad operativa y el prestigio.

Por otro lado, la integración de técnicas de sistemas inteligentes y minería de datos permitirá mejorar la precisión y velocidad de detección de amenazas. Estos enfoques proporcionan capacidades avanzadas de análisis y aprendizaje, permitiendo al IDS adaptarse a nuevas formas de ciberataques y minimizar los falsos positivos. La aplicación de algoritmos de aprendizaje automático y análisis de patrones en grandes volúmenes de

datos de tráfico HTTP contribuirá a identificar comportamientos anómalos y potencialmente peligrosos de manera autónoma y eficiente.

1.5. Alcance del Proyecto

El proyecto "Monitoreo de red inteligente usando IDS y dispositivos de Edge Computing" tiene como objetivo diseñar e implementar un sistema de detección de intrusiones (IDS) descentralizado, enfocado en mejorar la seguridad de redes en entornos domésticos y pequeñas empresas. Este sistema permitirá identificar ataques informáticos de manera oportuna, protegiendo la integridad, disponibilidad y confidencialidad de la información en redes locales.

El sistema se utilizará para monitorear el tráfico de red en tiempo real y detectar posibles amenazas a la seguridad. El proyecto incluye la creación de un entorno controlado donde se simularán diversos tipos de ataques cibernéticos, lo que permitirá probar la eficacia del sistema bajo diferentes escenarios de riesgo que podrían darse en redes empresariales o domésticas.

Para capturar y analizar el tráfico de red, se utilizarán herramientas como Snort, combinadas con dispositivos de bajo costo como Raspberry Pi 3, lo que hará que la solución sea rentable y escalable. Además, el sistema será capaz de detectar IPs maliciosas utilizando un archivo CSV ya normalizado, automatizando la creación de reglas en Snort para bloquear o monitorear esas IPs.

También se desarrollará una interfaz gráfica que permitirá a los usuarios visualizar en tiempo real los resultados del análisis de la red, facilitando el monitoreo continuo y la toma rápida de decisiones. El sistema será probado en diversas condiciones y con diferentes volúmenes de tráfico para asegurar su efectividad y capacidad de adaptación a distintos tipos de redes.

Este proyecto beneficiará tanto a la Facultad de Sistemas y Telecomunicaciones de la Universidad Estatal Península de Santa Elena, donde se aplicará en la protección de la red interna, como a redes domésticas.

1.6. Metodología del proyecto

1.6.1. Metodología de la investigación

Para el desarrollo del proyecto "Monitoreo de red inteligente usando IDS y dispositivos de edge computing", se ha elegido la metodología heurística iterativa. Esta metodología se centra en la experimentación y ajuste constante a lo largo de varias fases, permitiendo

una mejora progresiva del sistema. Al ser un proyecto donde la detección de intrusiones en tiempo real es fundamental, la flexibilidad y capacidad de ajuste que ofrece esta metodología resulta particularmente adecuada. El enfoque iterativo permite que cada fase sea un ciclo de prueba, evaluación y modificación, en el cual se analizan los resultados de los experimentos y se ajustan tanto los parámetros de configuración como los algoritmos utilizados. Esta naturaleza cíclica garantiza que, a medida que se avanza, el sistema se vuelve más preciso y efectivo al adaptarse a las necesidades específicas de un entorno de red y al comportamiento de las amenazas emergentes.

Además, al trabajar con dispositivos de edge computing y hardware de bajo costo, la metodología facilita la optimización del rendimiento de cada componente del IDS, asegurando que se aprovechen al máximo los recursos limitados. Cada iteración no solo contribuye a mejorar la eficacia del sistema, sino que también permite identificar configuraciones y técnicas que maximicen su eficiencia sin sacrificar capacidad de respuesta ni precisión en la detección. De este modo, la metodología heurística iterativa no solo responde a la necesidad de obtener un sistema de detección ágil y robusto, sino que también fomenta un proceso de desarrollo adaptable, asegurando que el IDS cumpla con los objetivos de monitoreo en tiempo real y aporte valor al entorno de red en el que se implementará.

1.6.2. Beneficiarios del proyecto

1.6.2.1. Beneficiario Directo

La Facultad de Sistemas y Telecomunicaciones, junto con el entorno doméstico, se beneficiará del proyecto "Monitoreo de red inteligente usando IDS y dispositivos de edge computing." En la facultad, este sistema garantizará una respuesta rápida y efectiva ante posibles amenazas cibernéticas, mejorando la seguridad informática en sus entornos. Además, servirá como una valiosa herramienta académica para enseñar e investigar sobre ciberseguridad, análisis de tráfico de red e implementación de tecnologías avanzadas de edge computing.

En el ámbito doméstico, el sistema ofrecerá un nivel de protección similar, permitiendo a los usuarios gestionar y monitorear la seguridad de sus redes personales de manera eficiente, brindando tranquilidad frente a posibles vulnerabilidades y amenazas en un contexto donde la conectividad en el hogar es cada vez más crucial. De esta manera, el

proyecto no solo tiene un impacto institucional, sino que también extiende sus beneficios al uso cotidiano y personal, fomentando una cultura de seguridad digital integral.

1.6.2.2 Beneficiarios Indirectos

Los estudiantes de (FACSISTEL) se beneficiarán indirectamente de esta investigación mediante la implementación de un sistema de detección de intrusos que contribuye significativamente al enriquecimiento del conocimiento en el área de seguridad de redes y sistemas de detección de intrusiones.

Además, este sistema no solo está diseñado para beneficiar a la comunidad académica, sino que también brindará una mayor seguridad a los usuarios en entornos domésticos, ofreciendo una solución eficiente para proteger sus redes frente a posibles amenazas cibernéticas.

1.6.3. Variable

La investigación tiene como objetivo medir la efectividad del sistema de detección de intrusos (IDS) en identificar actividades sospechosas o amenazas dentro de la red. Se puede expresar como el porcentaje de intrusiones detectadas en relación con el total de intentos de intrusión conocidos.

1.6.4. Técnicas de Recolección

Se emplearán técnicas de recolección como la captura de paquetes de red y el análisis de registros de sistema para identificar patrones de tráfico y detectar anomalías en tiempo real. Además, se realizarán pruebas de intrusión controladas y simulaciones de ataques para evaluar la eficacia del sistema IDS en condiciones reales, permitiendo así ajustar sus algoritmos de detección y mejorar su rendimiento en la protección de la red.

1.6.5. Análisis de Recolección de Datos

Para el desarrollo de esta investigación, se plantea un análisis exhaustivo de la recolección de datos en el contexto de un sistema de monitoreo de red inteligente utilizando IDS (Sistemas de Detección de Intrusos) y dispositivos de edge computing.

En el análisis de recolección de datos, se utilizó un archivo CSV previamente normalizado, que contiene información clave del tráfico de red monitoreado, como direcciones IP, puertos y protocolos, entre otros atributos. Este archivo se sube a un sistema que ha sido desarrollado en Python para automatizar la detección de IPs maliciosas, basándose en reglas establecidas previamente en Snort.

El código en Python analiza los datos del CSV, identificando patrones o comportamientos que corresponden a posibles amenazas o anomalías. Cuando se detecta una IP maliciosa, se crea una nueva regla para Snort, permitiendo que el IDS (sistema de detección de intrusos) reaccione en tiempo real ante futuras detecciones de esa IP o patrones similares. Esta integración asegura que el sistema sea proactivo en la protección de la red, actualizando continuamente sus reglas basadas en los datos obtenidos.

1.7. Metodología de Desarrollo

Para el proyecto "Monitoreo de red inteligente usando IDS y dispositivos de edge computing" se fundamenta en la metodología heurística iterativa. Este enfoque se justifica por la necesidad de abordar tanto la eficacia técnica del sistema como la percepción de los usuarios respecto a su usabilidad y efectividad.

1. **Fase de Planificación y Requisitos**: En esta fase inicial, el objetivo es definir el alcance del proyecto, los objetivos generales y específicos, los requisitos técnicos y además, en esta etapa se lleva a cabo una investigación exhaustiva de diversas soluciones IDS disponibles, con el propósito de seleccionar la más adecuada para nuestro proyecto, considerando aspectos como eficiencia, capacidad de integración con dispositivos de edge computing, y precisión en la detección de anomalías.
2. **Fase de Análisis y Diseño**: En esta fase, se analiza en detalle cómo se implementará el sistema de monitoreo de red inteligente. Se estudian las características del IDS seleccionado y se definen las reglas y configuraciones necesarias para su correcta operación junto a los dispositivos de edge computing. El análisis incluye la identificación de posibles amenazas cibernéticas, tipos de ataques y patrones de tráfico malicioso que el sistema deberá detectar. Además, se diseñan los procesos para la recolección de datos, donde se establece el uso de Snort como herramienta para capturar el tráfico de red y generar alertas. También se planea la estructura del archivo CSV normalizado que será utilizado para almacenar y procesar las IPs detectadas, permitiendo su análisis automatizado mediante scripts de Python, que a su vez generarán reglas específicas para Snort. Durante esta fase, se detallan los flujos de datos, la arquitectura del sistema y las interfaces necesarias para una operación eficiente y eficaz.
3. **Fase de Implementación**: En esta fase, se lleva a cabo la instalación y

configuración del sistema de detección de intrusiones (IDS) y los dispositivos de edge computing en el entorno definido (hogar y pyme). Se implementa Snort como IDS, ajustando sus reglas de detección para adaptarse a los tipos de tráfico y amenazas identificadas en la fase anterior. Además, se desarrolla el código en Python para procesar el archivo CSV normalizado, el cual contiene datos de tráfico de red con posibles IPs maliciosas. Este código automatiza la detección de estas IPs y actualiza las reglas de Snort de forma dinámica, lo que permite que el sistema esté en constante evolución frente a nuevas amenazas.

4. **Fase de Pruebas**: En esta fase, se verifica el funcionamiento del sistema de monitoreo en condiciones controladas. Se realizan pruebas exhaustivas tanto en el entorno doméstico como en la pyme para asegurarse de que el sistema de detección de intrusiones (IDS) y los dispositivos de edge computing operen de manera efectiva. Se utilizan escenarios simulados y tráfico de red real para comprobar la capacidad del sistema de detectar amenazas, como direcciones IP maliciosas y tráfico anómalo, de manera precisa y en tiempo real.

   Además, se valida el proceso de integración entre el código en Python que analiza el archivo CSV normalizado y el IDS Snort, asegurando que las IPs maliciosas detectadas se traduzcan correctamente en reglas actualizadas para Snort. Se prueban también las notificaciones automáticas, verificando que los alertas se envíen de manera oportuna y confiable a los responsables de la seguridad cuando se identifiquen actividades sospechosas.

5. **Fase de Evaluación y Revisión:** En esta fase, se realiza un análisis exhaustivo del desempeño del sistema de monitoreo de red inteligente desarrollado. El objetivo principal es verificar que el sistema cumpla con los requisitos definidos en fases anteriores y que funcione correctamente en diferentes escenarios de uso.

2 CAPITULO 2. PROPUESTA

2.1. Marco Contextual

La Universidad Estatal Península de Santa Elena (UPSE), situada en Santa Elena, es un centro educativo con extensa experiencia en la capacitación de profesionales en variados campos del saber. El 2 de julio de 1998, la UPSE fue establecida a través de la Ley N° 110, y se publicó en el suplemento del Registro Oficial N° 366 del 22 de julio de 1998. Su emplazamiento está ubicado en la avenida principal de La Libertad-Santa Elena, ubicada en el cantón La Libertad. La universidad dispone de una infraestructura avanzada y tecnológica que facilita a sus alumnos y profesores la realización eficaz y eficiente de sus tareas académicas. [7].

MISIÓN

Formar profesionales que aportan al desarrollo sostenible, contribuye a la solución de los problemas de la comunidad y promueve la cultura [7].

VISIÓN

Ser reconocida por su calidad académica, impacto de sus investigaciones y su aporte al desarrollo de la sociedad [7].

UBICACIÓN

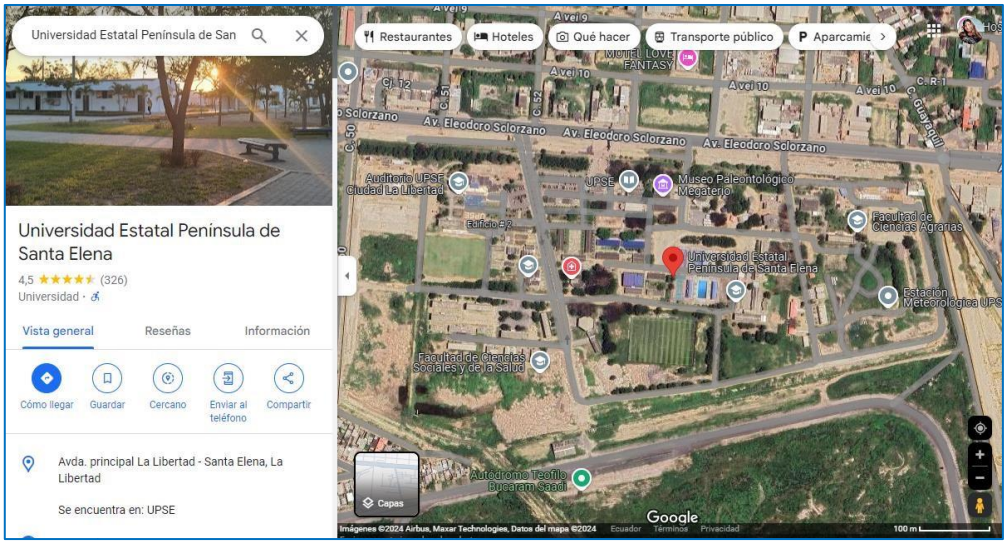


Fig. 1 UPSE, VIA SATELITAL

2.1.1. Educación Superior

Las instituciones de educación superior son cruciales para la formación de profesionales y el desarrollo de nuevas tecnologías que ayudan al avance del país en varios sectores, como las TIC. Las universidades y facultades son centros importantes de investigación y desarrollo en áreas emergentes como la ciberseguridad, las redes inteligentes.

2.1.2. PYME - Segmento de Red

Las PYMEs son empresas de tamaño reducido o mediano que, aunque tienen menos recursos que las grandes corporaciones, siguen siendo vulnerables a ciberataques debido a la falta de sistemas de seguridad robustos y personal especializado en ciberseguridad. En una PYME local, el sistema de red generalmente está compuesto por equipos de trabajo interconectados a través de una red local (LAN), que permite la comunicación interna entre los diferentes dispositivos y sistemas, y generalmente se conecta a Internet para realizar actividades comerciales o administrativas.

El Sistema de Detección de Intrusiones (IDS) en esta red puede monitorear todo el tráfico entre los dispositivos conectados a la red interna de la PYME, analizando el comportamiento de la red para identificar posibles intrusiones o comportamientos anómalos que puedan indicar un intento de ataque, como un ataque DDoS, phishing, malware o infección por ransomware. A través de un sistema IDS basado en Edge computing, es posible realizar análisis en tiempo real de los datos generados por los dispositivos de la red sin sobrecargar la infraestructura central.

2.1.3. Seguridad en el Hogar

En los últimos años, los hogares se han convertido en espacios altamente conectados gracias al uso de dispositivos inteligentes como cámaras de vigilancia, asistentes de voz, termostatos, luces y otros dispositivos IoT. Sin embargo, esta creciente conectividad trae consigo una mayor exposición a riesgos de ciberseguridad. Cada dispositivo conectado a la red doméstica representa una potencial puerta de entrada para ciberataques, lo que hace esencial contar con soluciones de seguridad adecuadas. A medida que los ciberataques evolucionan, se hace evidente que la seguridad básica que ofrecen los enrutadores convencionales ya no es suficiente.

2.1.2 Base Legal

2.1.3.1. Ley Orgánica de datos personales

Artículo 37.- Seguridad de datos personales

Según el caso, el encargado o responsable del tratamiento de datos personales debería adherirse al principio de seguridad de datos personales. Para ello, debe considerar las categorías y el volumen de datos personales, el estado de la técnica, las mejores prácticas de seguridad integral y los costos de aplicación en función de la naturaleza, el alcance, el contexto y los objetivos del tratamiento, además de reconocer la probabilidad de riesgos. El encargado o responsable del manejo de datos personales tiene la obligación de establecer un proceso de comprobación, evaluación y valoración constante y constante de la eficacia y eficiencia de las acciones técnicas, organizacionales y de cualquier otro tipo, puestas en marcha con el fin de asegurar y potenciar la seguridad en el tratamiento de datos personales [8].

Entre otras acciones, podrían considerarse las siguientes:

1) Procedimientos para la anonimización, seudonimización o encriptación de información personal.

2) Medidas orientadas a preservar la privacidad, la integridad y la disponibilidad constante de los sistemas y servicios encargados de la gestión de datos personales y el acceso a los mismos, de manera rápida ante incidentes.

3) Medidas orientadas a optimizar la residencia en aspectos técnicos, físicos, administrativos y legales.

4) Los encargados y responsables de la gestión de datos personales, podrán adherirse a normas internacionales para una correcta administración de riesgos orientada a la salvaguarda de derechos y libertades, además de la implementación y administración de sistemas de seguridad de la información o a códigos de comportamiento reconocidos y autorizados por la Autoridad de Protección de Datos Personales.

Art. 40.- Análisis de riesgo, amenazas y vulnerabilidades. - Para el estudio de riesgos, amenazas y vulnerabilidades, el encargado y el responsable de la gestión de la información personal deberán emplear una metodología que tome en cuenta, entre otras cosas, [8]:

1) Los detalles específicos del tratamiento;

2) Las especificidades de los participantes implicados; y,
3) Las categorías y el volumen de información personal que se está tratando.

Art. 41.-Determinación de medidas de seguridad aplicables. -Para establecer las medidas de seguridad autorizadas por el estado de la técnica, a las que está obligado el responsable y el responsable del manejo de la información personal, se deben considerar, entre otros aspectos, los siguientes factores: [8].

2.1.3.2. Constitución de la república del Ecuador

Art. 66.- Derecho a la protección de datos de carácter personal. - Asegura a todos los individuos el derecho a la salvaguarda de sus datos personales. Este derecho significa que la persona posee el dominio y la elección sobre la información y los datos que le pertenecen, además de su correspondiente salvaguarda. Cualquier recopilación, almacenamiento, tratamiento, reparto o divulgación de estos datos o información necesitarán la aprobación del titular o la disposición de la ley. [9].

2.1.3.3. Código Orgánico Integral Penal

Sección sexta

Artículo 178.- Violación a la intimidad

El individuo que, sin el permiso o la autorización legal, acceda, intercepte, examine, conserve, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, datos contenidos en dispositivos informáticos, comunicaciones privadas o reservadas de otro individuo por cualquier medio, será penalizado con una pena de reclusión de uno a tres años. [10].

Artículo 234.- Acceso no consentido a un sistema informático

El individuo que, sin permiso, ingrese total o parcialmente a un sistema de computación o telemático o de telecomunicaciones o permanezca en él en contra de la voluntad de quien posee el derecho legítimo, con el fin de aprovechar ilegalmente el acceso obtenido, modificar un portal web, desviar o redirigir tráfico de datos o voz u ofrecer servicios que estos sistemas brindan a terceros, sin abonarlos a los proveedores de servicios legítimos, se considera [10].

2.2. Marco Conceptual

2.2.1. Monitoreo de Red

El monitoreo de red implica el uso de programas de seguimiento de red para supervisar de manera constante el estado y la fiabilidad de una red informática. Los sistemas de Gestión de Rendimiento de Redes (NPM) suelen elaborar mapas de topología y perspectivas prácticas basándose en los datos de rendimiento recolectados y estudiados. Este mapa de red proporciona a los equipos de TI una total visibilidad de los elementos de la red, el monitoreo del desempeño de las aplicaciones y la infraestructura de TI vinculada. Esto les facilita seguir el estado global de la red, identificar señales rojas y mejorar el tráfico de datos. [11].

Ya sea que los recursos de red se encuentren en un lugar local, en un centro de datos, hospederos de un proveedor de servicios en la nube o integrantes de un ecosistema híbrido, un sistema de vigilancia de red identifica dispositivos de red que no operan correctamente y recursos saturados. Por ejemplo, podría detectar CPU saturadas en los servidores, elevadas frecuencias de fallos en switches y routers, o incrementos bruscos en el tráfico de red. Un atributo fundamental del software de NPM es informar a los administradores de red cuando se identifica un problema de desempeño.

2.2.2. Importancia de Ciberseguridad

En un mundo que se digitaliza progresivamente, la ciberseguridad resulta esencial para salvaguardar la información personal y corporativa de riesgos cibernéticos. La conexión entre sistemas y dispositivos incrementa la susceptibilidad a ataques como el hurto de información, el hackeo y el ransomware. La ciberseguridad no solo protege información sensible y recursos digitales, sino que también garantiza la continuidad de las operaciones de infraestructuras esenciales y el acatamiento de las regulaciones, ajustándose de manera constante a la progresión de amenazas. Por lo tanto, se resguarda tanto a personas como a entidades, reforzando la confianza y la capacidad de resistencia en el ambiente digital [12].

2.2.3. ¿Qué es un IDS?

Un Sistema de Detección de Intrusos o IDS (Sistema de Detección de Intrusos) es un instrumento de seguridad responsable de supervisar los sucesos que suceden en un sistema de computación para detectar intentos de infiltración.

Explicamos el intento de intrusión como cualquier esfuerzo por poner en riesgo la privacidad, integridad o disponibilidad de un sistema de computación, o por eludir los sistemas de seguridad correspondientes.

2.2.3.1. Las intrusiones se pueden producir de varias formas:

Atacantes que ingresan a los sistemas a través de la red.

- Usuarios autorizados del sistema que buscan obtener privilegios extra para los que no cuentan con permiso.
- Usuarios privilegiados que utilizan de manera indebida los privilegios o recursos que se les han otorgado.

Para distinguir claramente lo que es intrusión de lo que no, una entidad debería definir una política de seguridad, en la que se especifique claramente qué se permite y qué no. Para obtener más detalles sobre este asunto, consultar este sitio web[13].

2.2.3.2. Las intrusiones se pueden producir de varias formas:

Detectar intrusiones facilita a las organizaciones la protección de sus sistemas frente a las amenazas que surgen al aumentar la interconexión entre las redes. Los ataques de denegación de servicio (DoS) en febrero de 2000 contra Amazon.com y E-Bay, entre otros, evidenciaron la necesidad de instrumentos eficaces para identificar intrusos, particularmente en empresas de comercio electrónico y públicas en línea. [13].

2.2.3.3. Clasificación de los IDSs

Hay diversas categorizaciones posibles de los IDSs, dependiendo del rasgo en el que nos concentremos. A continuación, las analizaremos:

2.2.3.4. Fuentes de información

Hay diversas fuentes desde las que un IDS puede capturar sucesos. Algunos sistemas de detección de intrusiones examinan paquetes de red, capturados del núcleo de la red o de segmentos LAN, mientras que otros sistemas de detección de intrusiones examinan sucesos producidos por sistemas operativos o programas de aplicación en busca de señales de intrusión [13].

2.2.3.5. IDSs basados en red (NIDS)

La mayoría de los sistemas para detectar intrusos se fundamentan en red. Estos sistemas de detección de intrusiones identifican ataques capturando y examinando paquetes de red.

En un segmento de red, un NIDS tiene la capacidad de supervisar el tráfico de red que impacta a varios hosts vinculados a ese segmento de red, salvaguardando de esta manera a estos hosts.

Los sistemas de detección de intrusiones basados en red suelen estar compuestos por un grupo de sensores situados en distintos lugares de la red. Estos sensores supervisan el tráfico en la red, llevando a cabo análisis en el lugar e informando sobre ataques a la consola de administración. Dado que los sensores están restringidos a realizar el IDS, pueden ser protegidos con mayor facilidad frente a ataques. Numerosos de estos sensores están diseñados para funcionar en modo de carrera. [13].

Ventajas:

Un sistema de detección de intrusiones bien ubicado puede supervisar una gran red.

Los NIDSs ejercen una influencia mínima en la red, siendo usualmente aparatos pasivos que no obstaculizan las operaciones cotidianas de esta.

Es posible configurarlos para que sean extremadamente seguros frente a ataques, volviéndolos invisibles en la red [13].

Desventajas:

Pueden enfrentarse a problemas al procesar todos los paquetes en una red amplia o con gran cantidad de tráfico y pueden no identificar ataques ejecutados durante periodos de gran tráfico. Algunos comerciantes están tratando de solucionar este problema poniendo IDSs totalmente en hardware, lo que los convierte en mucho más veloces.

Los sistemas de detección de intrusiones basados en red no examinan la información cifrada. Este inconveniente se intensifica cuando la entidad emplea cifrado en el nivel de red (IPSec) entre los hosts, pero puede solucionarse con una política de seguridad más flexible (como IPSec en modo túnel).

La mayoría de los sistemas de detección de intrusiones basados en red desconocen si el ataque fue exitoso o no, lo único que pueden confirmar es que el ataque se realizó. Esto implica que, una vez detectado un ataque por un NIDS, los administradores deben examinar manualmente cada host atacado para establecer si el intento de infiltración fue exitoso o no [13].

Algunos sistemas NIDS experimentan dificultades al abordar ataques basados en red que se desplazan en paquetes fragmentados. Estos paquetes provocan que el sistema de detección de intrusiones no identifique tal ataque o que sea inestable y pueda derrumbarse.

2.2.3.6. IDSs basados en host (HIDS)

Los HIDS constituyeron el primer tipo de sistemas de detección de intrusiones desarrollados e implementados. Trabajan con los datos obtenidos desde el interior de un ordenador, como pueden ser los archivos de auditoría del sistema operativo. Esto posibilita que el sistema de detección de intrusiones examine las actividades ocurridas con gran exactitud, identificando precisamente qué procesos y usuarios participan en un ataque específico dentro del sistema operativo. En contraposición a los NIDSs, los HIDSs tienen la capacidad de observar el desenlace de un intento de ataque, así como tener la capacidad de acceder directamente y supervisar los archivos de datos y procesos del sistema atacado.

Ventajas:

- Los sistemas de detección de intrusiones basados en host, al poseer la habilidad de supervisar sucesos locales en un host, pueden identificar ataques que un sistema de detección de intrusiones basado en red no puede percibir.
- Suelen funcionar en un ambiente donde el tráfico de red se desplaza cifrado, dado que la fuente de información se produce antes de que los datos sean cifrados y/o después de que el dato sea desencriptado en el destino host

Desventajas:

- Los sistemas de detección de intrusiones basados en host son más caros de gestionar, dado que deben ser administrados y configurados en cada host supervisado.
- Si la estación de análisis se encuentra en el host supervisado, el sistema de detección de intrusiones puede ser desactivado si un ataque consigue tener éxito en la máquina.
- No son apropiados para identificar ataques a toda una red (como escaneos de puertos), ya que el sistema de detección de intrusiones solo percibe aquellos paquetes de red que se han enviado a él.
- Algunos ataques de DoS pueden desactivarlos.
- Emplean recursos del anfitrión que están supervisando, afectando el desempeño del sistema que están supervisando [13].

2.2.4. Edge Computing

Es una de las tecnologías que definirá y revolucionará la manera en la que humanos y dispositivos se conectan a internet. Afectará a industrias y sectores como la del coche conectado, los videojuegos, la Industria 4.0, la inteligencia artificial o el machine learning. Conseguirá que otras tecnologías como la nube o el internet de las cosas sean aún mejores de lo que son ahora. Como es probable que oigas el término a menudo en los próximos años, vamos a detallar qué es el Edge Computing, explicado en términos sencillos [14].

2.2.5. Algoritmos de Machine Learning

Los algoritmos de machine learning son técnicas que permiten a las computadoras aprender de los datos y hacer predicciones o decisiones sin ser programadas explícitamente. En el contexto de la ciberseguridad, se utilizan para identificar patrones en el tráfico de red, clasificar actividades normales y anormales, y mejorar la precisión de la detección de intrusiones [15].

2.2.6. Metodología heurística iterativa

Se trata de un método centrado en la búsqueda y modificación constante de soluciones, a través de iteraciones consecutivas, hasta alcanzar una solución ideal o satisfactoria. En el marco de tu proyecto de vigilancia inteligente de red mediante IDS y dispositivos de computación a distancia, esta metodología se ajusta de manera óptima, pues facilita la adaptación y mejora gradual del sistema a medida que se examinan diversas configuraciones, modelos y técnicas [16].

2.2.7. Análisis de Datos

El análisis de datos consiste en la revisión, purificación y modelación de datos con la finalidad de hallar información valiosa, respaldar la toma de decisiones y emitir conclusiones. Dentro del marco de la identificación de intrusiones, el estudio de datos conlleva la valoración de patrones de tráfico y comportamientos con el fin de detectar potenciales amenazas y potenciar la seguridad de la red [17].

2.2.8. Patrones de Comportamiento Malicioso

Estos son patrones detectables en el tráfico de red que señalan acciones que podrían ser perjudiciales o no permitidas. El estudio de estos patrones posibilita que los sistemas de detección de intrusiones identifiquen y reaccionen de manera rápida a los peligros [18].

2.2.9. ¿Qué es Raspberry Pi?

La Raspberry Pi es una computadora asequible y de tamaño reducido, apta para una tarjeta de crédito, que puede conectarse a un monitor de ordenador o una televisión, y funcionar con un ratón y teclado estándar. Es un diminuto ordenador que funciona con un sistema operativo Linux, que permite a individuos de cualquier edad explorar la computación y aprender a programar en lenguajes como Scratch y Python. Es capaz de desempeñar la mayoría de las funciones habituales de un ordenador de escritorio, desde explorar la web, visualizar vídeos de alta resolución, manejar documentos de oficina, hasta jugar a juegos.

Adicionalmente, la Raspberry Pi posee la capacidad de interactuar con el entorno exterior, y puede emplearse en una gran diversidad de proyectos digitales, que van desde reproductores de música y video, identificadores de padres, estaciones de clima hasta cajas de aves equipadas con cámaras infrarrojas. Deseamos que comprendas que la Raspberry Pi puede ser utilizada por niños y adultos a nivel global, para aprender a programar y comprender el funcionamiento de los ordenadores [19].

2.2.10. ¿Qué es Python?

Python es un lenguaje de programación muy empleado en aplicaciones web, la creación de software, la ciencia de datos y el aprendizaje automático (ML). Los programadores emplean Python debido a su eficacia y sencillez de aprendizaje, además de su capacidad para funcionar en diversas plataformas. El programa Python se puede descargar sin costo, se incorpora eficazmente a cualquier tipo de sistema y potencia la rapidez del desarrollo [20].

2.2.10.1. ¿Qué beneficios ofrece Python?

Los beneficios de Python incluyen los siguientes:

- Los desarrolladores pueden leer y comprender fácilmente los programas de Python debido a su sintaxis básica similar a la del inglés.

- Python permite que los desarrolladores sean más productivos, ya que pueden escribir un programa de Python con menos líneas de código en comparación con muchos otros lenguajes.
- Python cuenta con una gran biblioteca estándar que contiene códigos reutilizables para casi cualquier tarea. De esta manera, los desarrolladores no tienen que escribir el código desde cero.
- Los desarrolladores pueden utilizar Python fácilmente con otros lenguajes de programación conocidos, como Java, C y C++.
- La comunidad activa de Python incluye millones de desarrolladores alrededor del mundo que prestan su apoyo. Si se presenta un problema, puede obtener soporte rápido de la comunidad.
- Hay muchos recursos útiles disponibles en Internet si desea aprender Python. Por ejemplo, puede encontrar con facilidad videos, tutoriales, documentación y guías para desarrolladores.
- Python se puede trasladar a través de diferentes sistemas operativos de computadora, como Windows, macOS, Linux y Unix [20].

2.2.11. Ataques Informáticos

Un ataque informático implica explotar una vulnerabilidad o fallo (vulnerabilidad) en el software, hardware e incluso individuos que componen un entorno informático, con el objetivo de conseguir un beneficio, generalmente económico, provocando un impacto negativo en la seguridad del sistema, que posteriormente repercute directamente en los activos de la organización [21].

2.212 IDS SNORT

Es un programa de código abierto sin costo que pueden utilizar individuos y entidades. La terminología de la regla SNORT establece qué tráfico de red debe ser recolectado y qué sucesos deben ocurrir cuando identifica paquetes malintencionados. Este concepto de Snort puede emplearse igual que los detectores y sistemas de detección de intrusos en la red para identificar paquetes malintencionados, o como una solución IPS de red completa que supervisa la actividad de la red y identifica y bloquea posibles vectores de ataque [22].

2.2.12.1 ¿Cuáles son las características de software SNORT?

Existen varias funciones que hacen que SNORT sea útil para que los administradores de red monitoreen sus sistemas y detecten actividades maliciosas.

- **Monitor de tráfico en tiempo real. -** se puede utilizar para monitorear el tráfico que entra y sale de una red. Monitoreará el tráfico en tiempo real y emitirá alertas a los usuarios cuando descubra paquetes potencialmente maliciosos o amenazas en redes de Protocolo de Internet (IP).
- **Registro de paquetes. -** habilita el registro de paquetes a través de su modo registrador de paquetes, lo que significa que registra paquetes en el disco. En este modo, recopila cada paquete y lo registra en un directorio jerárquico basado en la dirección IP de la red host.
- **Análisis de protocolo. –** permite realizar análisis de protocolo, que es un proceso de detección de red que captura datos en capas de protocolo para análisis adicionales. Esto permite al administrador de red examinar más a fondo los paquetes de datos potencialmente maliciosos, lo cual es crucial, por ejemplo, en la especificación del protocolo de pila del protocolo de control de transmisión/IP (TCP/IP) [22].
- **Emparejamiento de contenido. -** recopila reglas por protocolo, como IP y TCP, luego por puertos, y luego por aquellos con contenido y aquellos sin él. Las reglas que tienen contenido utilizan un emparejador de varios patrones que aumenta el rendimiento, especialmente cuando se trata de protocolos como el Protocolo de transferencia de hipertexto (HTTP). Las reglas que no tienen contenido siempre se evalúan, lo que afecta negativamente el desempeño [22].
- **Las reglas son fáciles de implementar.** - Las reglas SNORT son fáciles de implementar y ponen en funcionamiento la supervisión y protección de la red. Su lenguaje de reglas también es muy flexible, y crear nuevas reglas es bastante simple, lo que permite a los administradores de red diferenciar la actividad regular de Internet de la actividad anómala o maliciosa [22].

2.2.13. Análisis de Tráfico de Red

Es la revisión de los paquetes de datos que se envían por una red con el fin de obtener datos acerca de su contenido, procedencia y destino. Para identificar irregularidades en el tráfico URL, el análisis de tráfico de red facilita la identificación de patrones de comportamiento irregular en las peticiones de URL e identificar potenciales amenazas [23].

2.2.14. Direcciones IP

El protocolo de Internet es un protocolo que no busca la conexión y opera mediante una red de paquetes configurada. Por lo tanto, es un protocolo de gran intensidad para la

entrega de paquetes no fiables. Es uno de los protocolos de Internet de mayor relevancia, puesto que posibilita el traslado de paquetes de datos, aunque se realice sin garantías. [24].

2.2.15. Análisis de Paquete

El estudio de paquetes de red facilita la evaluación del tráfico de la red en un nivel granular, valorando cada uno de los paquetes de manera individual. Ofrece una perspectiva minuciosa de los datos presentes en cada paquete, lo que simplifica el entendimiento y el estudio específico del tráfico. En contraposición, el análisis de flujo se centra en recolectar metadatos o datos condensados acerca del tráfico en la red. Esta información abarca datos como las direcciones IP, los puertos y los protocolos empleados, lo que facilita un estudio estadístico del tráfico global. Los dos enfoques son complementarios y ofrecen visiones valiosas para comprender y administrar el tráfico de red de forma eficaz [25].

2.2.16. Análisis por Flujo

El propósito del análisis de flujo es recolectar metadatos o datos acerca del tráfico en una red. Un flujo de IP alude a un grupo de paquetes que poseen características particulares de paquetes IP, en los que cada paquete es direccionado y procesado por un conmutador o enrutador, e incluye la siguiente información [26]:

- IP de origen
- IP de destino
- Puerto de origen
- Puerto de destino
- Clase de servicio
- Tipo de protocolo
- Interfaz

2.2.17. Seguridad por capas

La estrategia de seguridad en capas es una táctica que fusiona diversos componentes de seguridad, tales como programas antivirus, cortafuegos y herramientas de evaluación de vulnerabilidades, con el objetivo de construir una barrera defensiva completa y más sólida

que la combinación de sus componentes individuales. Este método incrementa notablemente el precio y la complejidad para que un atacante pueda infiltrarse en un sistema, lo que disminuye la posibilidad de que se transforme en blanco de ataques. Al establecer la seguridad en niveles, se desanima a los atacantes a tratar de asaltar una institución debido al grado extra de resguardo y complejidad que deben sobrepasar.

2.2.18. Malware

El Malware es un software malicioso (malware) creado para entrar en su dispositivo sin su consentimiento, con la finalidad de provocar daños e interrupciones en el sistema o sustraer información. Adware, spyware, virus, agrupaciones de robots (botnets), troyanos, gusanos, rootkits y ransomware, son todos elementos que conforman la definición de malware [27].

2.2.19. Seguridad Informática

La Información Se define la información como un conjunto de datos que persiguen un determinado objetivo independientemente de los que cada dato significa.

- **Hay dos clases de datos:** la información pública (a la que todos pueden acceder), y la información privada (a la que únicamente ciertos usuarios pueden acceder). Este último debe mantenerse inalterable, dado que es información vital que asegura la continuidad de las operaciones de la organización, valiosa dado que es un recurso corporativo y delicada dado que debe ser reconocida por aquellos que requieran la información. Para que cualquier organización asegure la información que gestiona, necesita satisfacer tres elementos esenciales:

  - **Accesibilidad. -** La información debe estar disponible siempre que el usuario lo requiera.
  - **Privacidad. -** Solo el individuo autorizado debe tener acceso a la información.
  - **Constancia. -** Los datos deben ser precisos y completos.

2.2.20. ¿Qué es la Seguridad Informática?

La seguridad informática abarca todas las normativas, acciones, técnicas, procedimientos y métodos utilizados para proteger la información que se halla y se difunde a través de aparatos informáticos.

2.2.21. Amenazas en la seguridad informática.

Una amenaza se refiere a cualquier suceso, individuo o acción, con el potencial de perjudicar los componentes de un sistema mediante el hurto, aniquilación, divulgación, alteración de datos o renuncia a servicios.

Los clasificaremos en dos categorías:

2.2.22. Amenazas maliciosas

Son las amenazas que si finalidad es causar daño a la institución y estas pueden ser externas o internas.

Externas. - son amenazas que son provocadas por personas ajenas a la institución, y que no están autorizados para acceder. Muchas de estas amenazas provienen de Internet y desde ahí se logran filtrar hackers, crackers, virus, gusanos, etc.

Internas. - Son amenazas que provienen del interior de la institución, y pueden ocasionar mucho daño ya que cuentan con determinados privilegios que le permiten acceder a ciertos servicios.

2.2.23. Amenazas no maliciosas

Son amenazas causadas por usuarios que no están debidamente capacitados y que de manera involuntaria o por simple curiosidad ocasionan algún daño a la red interna.

2.2.24. Ataques Informáticos

Se denomina ataque informático a toda acción que trate de vulnerar la seguridad de nuestra red con el propósito de afectar la confidencialidad, integridad y disponibilidad de la información.

- **Intercepción. -** Sucede cuando la información llega a un punto distinto al que debería de llegar y así poder revisar la información capturada.
- **Modificación. -** Se da cuando alguien no autorizado tiene acceso a la información de un sistema a su base de datos logrando cambiarla, modificarla y/o eliminarla.
- **Suplantación. -** Más conocido como “Phishing” y se trata de replicar sitios WEB para engañar a los usuarios y de esta manera poder obtener datos confidenciales.
- **Autentificación. -** Tiene como objetico engañar al sistema de la víctima y hacerse pasar por ellos mediante la obtención previa de un usuario y password o sesiones ya establecidas.

- **Explotación de errores. -** Suceden cuando se hallan vulnerabilidades en el sistema operativo, protocolos de red o aplicaciones.
- **Ataques de Denegación de Servicios (DoS). -** Se basa en saturar un determinado servidor con una cantidad abrumante de peticiones, dejándolo así sin poder brindar sus servicios.

2.3.Marco Teórico

Se revisó varios trabajos de investigación desarrollados en las áreas de seguridad informática, implementaciones de IDS/IPS y utilidades del Raspberry.

2.3.1. "Diseño de un sistema de gestión de seguridad de datos mediante Firewall, AAA, IPS, y SIEM"

Autores. - Jorge Luis Chalén Pincay, Erick Paul Chávez López - 2015

Resumen. - Este estudio examina la infraestructura de red actual, especificando sus dificultades y sus potenciales causas y consecuencias, y sugiriendo 4 mecanismos de seguridad de red que contribuirán al control y administración de la gestión de la información. Por lo tanto, contamos con la implementación del Firewall (Cortafuegos), IPS (Sistemas de Prevención de Intrusos), Protocolo AAA (Autenticación, Autorización y Contabilización) y el SIEM (Sistemas de Detección de Intrusos). (Sistema de Gestión de Información y Eventos). En contraste con este trabajo, se emplea un firewall Fortigate 300c con un costo aproximado de $ 8000 (Ocho mil dólares americanos) [28].

2.3.2. "Seguridad Informática para la red de datos en la Cooperativa de Ahorro y Crédito Unión Popular LTDA."

Universidad Técnica de Ambato, Facultad de Ingeniería en sistemas electrónica e industrial, Ambato - Ecuador

Autor. - Silvana Judith Garcés Ulloa – 2015

Resumen. - Este esfuerzo, que se fundamenta en la aplicación de políticas de seguridad basadas en el Sistema de gestión de seguridad de la información ISO 27001, implementa políticas de accesos, cortafuegos, servidor PROXY y servidor IDS en la Cooperativa de Ahorro y Crédito Unión Popular LTDA. Con el objetivo de salvaguardar la información que se envía e interactúa en la red de información. Implementando recursos de red que garanticen la eliminación de obstáculos de acceso que puedan causar pérdidas a la cooperativa, y que los servicios ofrecidos por la red se empleen de la forma más eficiente y estén al alcance de todos los usuarios.

El sistema de detección de intrusiones no cuenta con una interfaz gráfica que nos facilite el manejo y la gestión de sucesos sucedidos en relación a intentos de infiltración. En este proyecto se propondrá y desarrollará una interfaz visual y un administrador de eventos [29].

2.3.3. "Sistema de consulta y notificación de alertas de seguridad mediante VoIP en Raspberry Pi" Universidad de Sevilla, Escuela Técnica Superior de Ingeniería Departamento de Ingeniería Telemática – Sevilla, España

Autor. - Ismael Narváez Berenjeno – 2015

Resumen. - Este documento abarca el procedimiento de creación y evaluación de un sistema de detección de intrusiones, que emplea un sistema de alertas y Consulta de alertas, fundamentado en llamadas VoIP. Todo esto está montado en un sistema económico y de bajo consumo, tal como la Raspberry Pi B+. El sistema cumple dos funciones: la función de alerta que examina el tráfico que recibe y, si identifica una amenaza, alerta al administrador a través de una llamada telefónica; y la función de consulta donde el administrador puede verificar la presencia de alertas de una determinada importancia, efectuando una llamada al sistema. Sugiere a SNORT como sistema de detección de intrusiones y a Asterisk como gestor de llamadas telefónicas. Sin embargo, solo produce alertas. En nuestra puesta en marcha, optimizaremos la aplicación del IDS y lo complementaremos con la configuración de un IPS. Además, emplearemos SNORBY como sistema de información para eventos y riesgos. Y la versión más actualizada del equipo Raspberry Pi 3 [30].

2.3.4. "Esquema de seguridad perimetral y control de incidencias de la red de datos para la Universidad Técnica de Cotopaxi"

Universidad Regional Autónoma de los Andes, Maestría de en Informática Empresarial, Facultad de Sistemas Mercantiles – Ambato, Ecuador

Autor. - Ing. Edison Fernando Aimacaña Chancusic - 2015

Resumen. - Este trabajo se fundamenta en la propuesta de seleccionar el software más adecuado para la Gestión Unificada de Amenazas (UTM), lo cual se ha establecido mediante la puesta en marcha del Esquema de Seguridad Perimetral y Control de Incidencias por el Software Check Point, gracias al análisis detallado del cuadrante

mágico de Gardner. La implementación de esta propuesta conllevará un alto costo y la renovación de las licencias cada tres años. [31].

2.3.5. Auditor WiFi desde Raspberry Pi controlado por dispositivo Android" Universitat Politècnica de València, Escola Tècnica Superior d´Enginyeria Informàtica – Valencia, España.

Autor. - Pablo Adrián Moreno Sierra – 2014/2015

Resumen. - Este proyecto tiene como objetivo modificar una Raspberry Pi 2 con el sistema operativo Kali Linux, de manera que se puedan usar las aplicaciones de auditoría WiFi en movilidad. El usuario es un aparato Android, que administra el servidor incorporado en la Raspberry Pi 2 a través de botones y listas para la elección de alternativas, transmitiendo de esta manera comandos Bash para la ejecución del servidor. La interacción entre el servidor y el cliente se lleva a cabo a través de Bluetooth, y tanto el servidor como el cliente se fundamentan principalmente en el lenguaje de programación Java. Utilizaremos el sistema operativo Raspbian en nuestro proyecto para incrementar la estabilidad y el rendimiento de nuestro dispositivo Raspberry Pi 3 [32].

2.3.6. "Virtualización de una red LAN con servidores de código abierto para evaluar los niveles de seguridad" Universidad Católica de Santiago de Guayaquil, Sistema de Posgrado – Guayaquil, Ecuador

Autor. - Cesar Libardo Rosado Muñoz – 2014

Resumen. - Con la herramienta VMWare se virtualiza una red interna para poner en marcha un cortafuegos con Iptables, que implementa una cadena de desplazamiento de direcciones y filtrado de paquetes. Y emplea CentOS como sistema operativo para poner en práctica el cortafuegos. Para poder llevar a cabo ataques sin comprometer la red física [33].

2.4. Requerimientos

Para la implementación del proyecto, se necesita de los siguientes requerimientos:

2.4.1. Requerimientos Funcionales

Código	Descripción
RF1	El sistema debe capturar tráfico de red en tiempo real utilizando el Raspberry Pi 3.
RF2	El sistema debe analizar los paquetes de red capturados e identificar posibles amenazas o intrusiones utilizando Snort.
RF3	El sistema debe generar alertas basadas en la detección de IPs maliciosas contenidas en el archivo CSV normalizado.
RF4	El sistema debe permitir el análisis de patrones de tráfico malicioso mediante algoritmos de machine learning integrados en Python.
RF5	El sistema debe almacenar los logs y resultados del análisis en el disco duro externo de 500GB.
RF6	El sistema debe ofrecer una interfaz gráfica (dashboard) para visualizar en tiempo real las IPs maliciosas detectadas.
RF7	El sistema debe permitir la conexión remota desde la laptop HP utilizando Real VNC o Putty.

Tabla 1 Requerimiento Funcionales

2.4.2. Requerimientos de Hardware

Dispositivo	Especificaciones	Descripción
Raspberry Pi 3	Procesador ARM Cortex-A53, 1GB RAM	Ejecución de scripts IDS, captura de paquetes, análisis en tiempo real.
Tarjeta de Memoria	MicroSD de 16 GB	Almacenamiento del sistema operativo y scripts.
Disco Duro	Externo de 500 GB.	Almacenamiento de logs, resultados de análisis y archivos CSV.
Router	Router estándar con capacidad de red LAN.	Para la conexión del Raspberry Pi a la red local.
Cable de Red (Ethernet)	Cable Ethernet para la conexión del Raspberry Pi al router.	Captura de tráfico de red en tiempo real.
Mouse, Teclado, Monitor	Mouse, teclado estándar, monitor VGA	Interacción local con el Raspberry Pi.
Laptop HP (Core i3)	Laptop con procesador Intel Core i3	Conexión remota al Raspberry Pi para administración.

Tabla 2 Requerimiento de HARWARE

2.4.3. Requerimiento de Software

Software		Descripción

Python	Lenguaje de programación principal	Desarrollo de scripts para la detección de intrusiones y análisis de tráfico.
Sistema Operativo	Debian o Raspberry Pi OS	Sistema operativo para Raspberry Pi.
Snort	Sistema de Detección de Intrusiones (IDS)	Monitoreo de red y detección de actividades sospechosas.
Real VNC	Herramienta de conexión remota	Acceso remoto al Raspberry Pi desde la laptop HP.
CSV Normalizado	Archivo CSV preprocesado con estructura específica	Análisis de IPs maliciosas y generación de reglas.

Tabla 3 Requerimientos de Software

Código	Descripción
RNF1	El sistema debe ser capaz de operar continuamente 24/7 con el Raspberry Pi 3, sin interrupciones.
RNF2	El procesamiento de los datos debe realizarse en tiempo real, con una latencia mínima en la captura y análisis de paquetes.
RNF3	La interfaz gráfica debe ser intuitiva y fácil de usar, mostrando visualizaciones claras de los resultados de la detección de intrusiones.
RNF4	El sistema debe ser fácilmente mantenible, permitiendo actualizaciones de software y ajustes de reglas de detección sin interrumpir el servicio.

RNF5	El sistema debe poder integrar fácilmente nuevos algoritmos o tecnologías sin requerir una reestructuración completa del código.

Tabla 4 Requerimiento no Funcionales

2.5. Componente de la propuesta tecnológica

En esta sección se procederá a demostrar la parte práctica de la propuesta tecnológica, donde se desarrolló un sistema de detección de amenazas en tráfico de red mediante el uso de Snort y análisis de datos con Python. El sistema está diseñado para identificar y notificar sobre posibles direcciones IP maliciosas utilizando técnicas avanzadas de análisis de registros CSV y la visualización de resultados a través de un dashboard interactivo.

El desarrollo sigue un enfoque heurístico iterativo [16], adaptada a un entorno de red basado en edge computing. Este enfoque garantiza que cada fase del proyecto sea probada y mejorada continuamente hasta alcanzar un sistema robusto y funcional. Las fases se dividen de la siguiente manera:

Fase 1: Planificación y Requisitos

Fase 2: Análisis y Diseño

Fase 3: Implementación

Fase 4: Pruebas

Fase 5: Evaluación y Revisión

2.5.1. Fase 1: Planificación y Requisitos

2.5.1.1. configuración del Sistema de Monitoreo en Edge Computing

En esta fase inicial, se configura el hardware y el software necesario para el monitoreo de la red. Esto incluye:

Instalación del Raspberry Pi 3 como dispositivo de edge computing central en la red local (LAN). El Raspberry Pi está conectado al router que gestiona el tráfico de Internet y LAN, Conexión de un disco externo al Raspberry Pi para almacenar registros históricos de tráfico y análisis de datos.

Fig. 2 Hardware necesario para el monitoreo de red

Para este proyecto se realizó un cuadro comparativo para escoger el mejor ids que encaje con nuestro proyecto "monitoreo de red inteligente usando ids y dispositivos de edge computing"

2.5.1.2. Cuadro Comparativo de los ids existentes en el mercado

Nombre Del Ids	Tipo	Costo	Años En El Mercado	Características Claves	Eficacia En Protección De Infraestructura
Snort	Tradicional	Gratuito (Open Source)	20+	Basado En Reglas, Alta Personalizacion	Alta para amenazas conocidas, limitada para amenazas nuevas
Suricata	Tradicional	Gratuito (Open Source)	10+	Multihilo, Alta Velocidad	Muy Buena para redes de alto rendimiento
Cisco Firepower	Tradicional	De Pago	15+	Integracion Con Otros Productos Cisco	Excelente para ecosistemas cisco

Darktrace	IA	De Pago	8+	Aprendizaje Automatico No Supervisado	Muy alta, especialmente para amenazas desconocidas
Vectra Cognito	IA	De Pago	7+	Detección Basada En Comportamiento	Excelente para detección de amenazas internas

Tabla 5 Cuadro comparativo IDS/IDSIA

2.5.2. Fase 2: Análisis y Diseño

2.5.2.1. Monitoreo y Captura de Datos de Tráfico de Red

En esta fase se define la arquitectura del sistema de monitoreo de red inteligente utilizando IDS y dispositivos de edge computing. Se analiza el tráfico de red que será monitoreado y los posibles ataques que se buscan detectar, como intrusiones en protocolos comunes (HTTP, HTTPS, DNS, etc.). A partir de este análisis, se diseñan los componentes clave: módulos de captura y análisis de tráfico, almacenamiento de datos, generación de alertas, y la interfaz gráfica para visualización en tiempo real.

El diseño también incluye la elección de Snort como IDS, integrándolo con un sistema que procese logs y detecte IPs maliciosas mediante el uso de Python. Se asegura que el sistema sea escalable y funcione de manera eficiente en dispositivos de bajo costo como el Raspberry Pi 3. Además, se plantea un enfoque modular que permita futuras mejoras, como la incorporación de algoritmos de aprendizaje automático para mejorar la detección de amenazas más avanzadas.

2.5.2.2. Evaluación de las tecnologías existentes.

En este apartado se realizará una investigación sobre las herramientas de detección de intrusos de código abierto más relevantes que se pueden encontrar en el mercado. Las herramientas de código abierto han sido elegidas para la comparación son:

SNORT y SURICATA son herramientas complementarias que brindan robustez y adaptabilidad a el proyecto de vigilancia de red inteligente. SNORT, caracterizado por su potente habilidad de identificación basada en firmas y su ligereza, es perfecto para su implementación en dispositivos de computación a distancia. SURICATA, gracias a su habilidad de procesamiento paralelo y análisis detallado de tráfico, ofrece una perspectiva

más exhaustiva y integral del tráfico en la red. Al fusionarlos, conseguirás un sistema más eficiente para identificar y atenuar riesgos en tiempo real, mejorando la utilización de recursos y disminuyendo la latencia.

2.5.2.3. Snort

Snort se trata de un Sistema de Prevención de Intrusiones (IPS) de código abierto, siendo uno de los más utilizados en el mundo. El Snort IPS utiliza un conjunto de reglas que permiten definir lo que se considera como actividad de red maliciosa y utiliza esas reglas para encontrar paquetes que coincidan con ellas. De esta forma, en caso de que se encuentren paquetes que coincidan con las reglas se generarán alertes para los usuarios del sistema. Como se ha comentado, Snort puede ser desplegado en línea, de forma que permita parar aquellos paquetes que puedan ser maliciosos. De la misma forma, esta herramienta puede ser utilizada como un Sistema de Detección de Intrusos.

Fig. 3 Logo IDS SNORT

Snort fue desarrollado en 1998 y desde entonces ha tenido muchas actualizaciones y tiene una comunidad muy activa. Por otra parte, Snort carece de interfaz gráfica, por lo que necesitaría de herramientas que cubran esa carencia.

2.5.2.4. Suricata

Suricata consiste en un software de alto rendimiento utilizado para el análisis de redes y la detección de amenazas. Este IDS es utilizado por un gran número de organizaciones privada y públicas para la protección de sus recursos en red.

Fig. 4 IDS SURICATA

Finalmente escogí Snort para mi proyecto en lugar de Suricata debido a su madurez, popularidad y menor consumo de recursos, lo que lo hace ideal para dispositivos de edge computing como el Raspberry Pi 3. Snort ofrece una configuración más sencilla, es altamente eficiente en entornos con recursos limitados, y cuenta con una amplia compatibilidad de reglas y herramientas de análisis. Además, su enfoque en la detección basada en firmas es adecuado para el monitoreo de redes pequeñas, brindando un equilibrio óptimo entre simplicidad y funcionalidad avanzada en este tipo de implementación.

2.5.3. Fase 3: Implementación

2.5.3.1. Análisis Automatizado con Python

En la Fase 3 de este proyecto, se procede a la implementación del sistema de monitoreo de red inteligente basado en la arquitectura diseñada en fases anteriores. Esta etapa incluye la instalación, configuración y desarrollo del software necesario para la captura de tráfico, análisis de datos, generación de reglas de detección y notificación de amenazas en tiempo real. Se ha utilizado un Raspberry Pi 3 como plataforma principal para la ejecución de los procesos, junto con herramientas de código abierto como Snort, Suricata y un sistema automatizado desarrollado en Python.

El análisis automatizado es una parte fundamental del sistema de monitoreo. En esta sección se describe cómo se utiliza Python para realizar la captura, procesamiento y análisis de tráfico de red. Mediante scripts personalizados, el sistema es capaz de identificar patrones sospechosos, generar alertas en tiempo real y actualizar las reglas del IDS. Este proceso garantiza una respuesta rápida ante posibles amenazas, reduciendo el tiempo de exposición de la red ante posibles ataques.

2.5.3.2. Instalación del ids snort

Instalación y configuración de Snort como sistema IDS para monitorizar el tráfico de red, incluyendo el tráfico HTTPS, con la capacidad de detectar amenazas, direcciones IP maliciosas y patrones sospechosos.

- Se utiliza los comandos para realizar la respectiva actualización e instalación del ids snort

- **apt-get update && apt-get upgrade**
- **apt-get install snort**

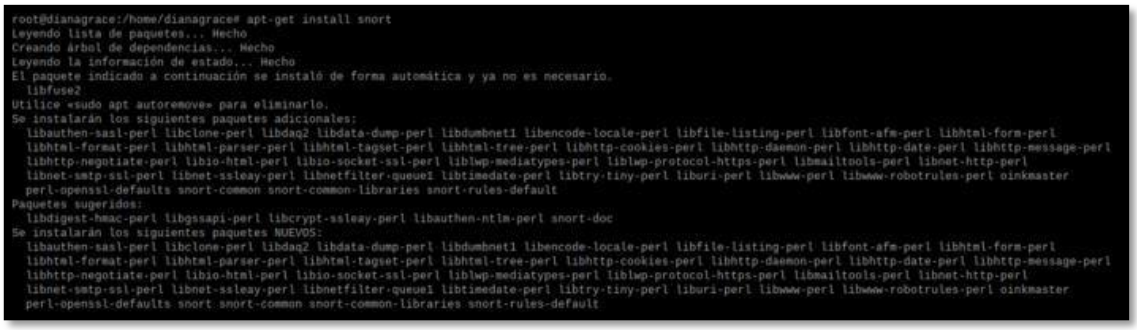


Fig. 5Instalación ids snort en Raspberrypi3

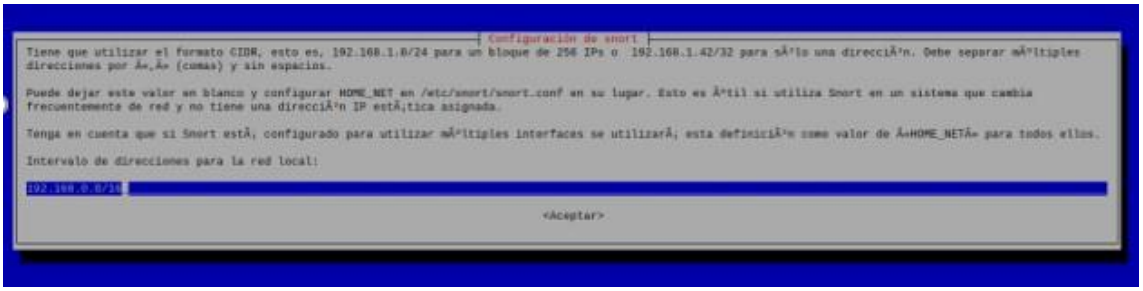


Fig. 6 configuración de ip

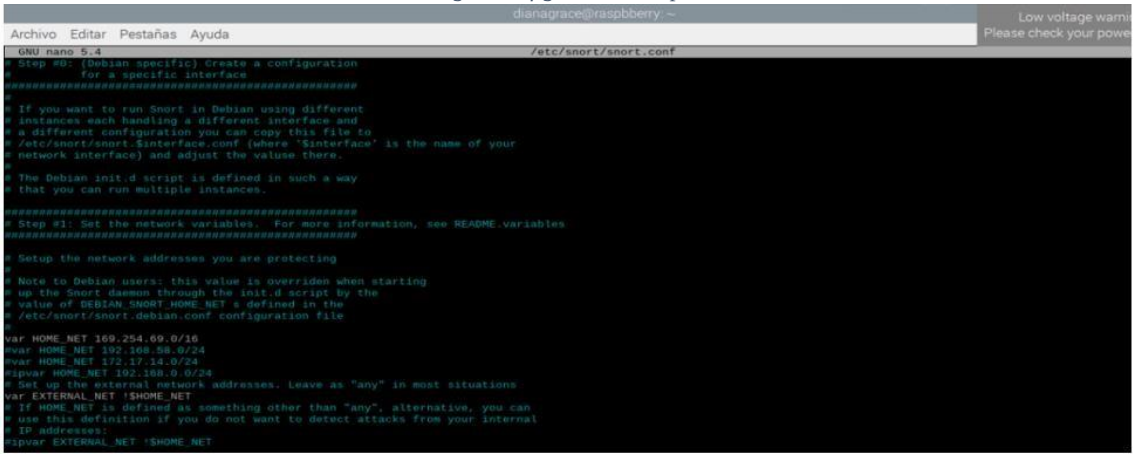


Fig. 7Configuración de las ip necesarias en snort.conf

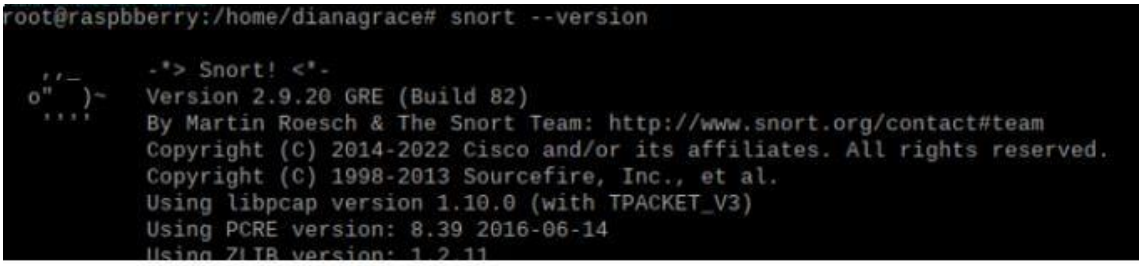


Fig. 8 Versión instalada de Ids Snort

En esta parte del proyecto realizamos el código de python para poder analizar el csv normalizado:

- Ingresamos a nuestro entorno llamaddo (env)

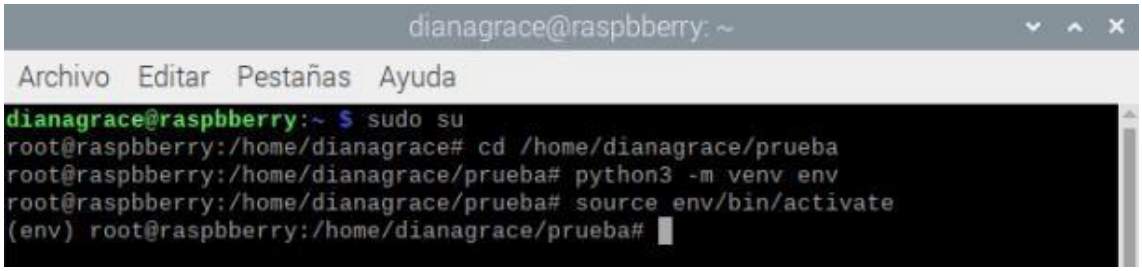


Fig. 9 entorno

El código desarrollado tiene como objetivo cargar archivos en formato CSV, JSON o Parquet que contengan datos de tráfico de red para identificar y extraer direcciones IP maliciosas. Estas IPs maliciosas se utilizan para generar reglas de Snort, las cuales permiten monitorear y alertar sobre posibles amenazas en la red.

El sistema funciona de la siguiente manera:

```python
# Configuración del directorio para guardar los archivos cargados
UPLOAD_FOLDER = 'uploads'
ALLOWED_EXTENSIONS = {'csv', 'json', 'parquet'}
app.config['UPLOAD_FOLDER'] = UPLOAD_FOLDER

# Asegurarse de que el directorio de uploads exista
if not os.path.exists(UPLOAD_FOLDER):
    os.makedirs(UPLOAD_FOLDER)

def allowed_file(filename):
    """Verifica que el archivo tenga una extensión permitida"""
    return '.' in filename and filename.rsplit('.', 1)[1].lower() in ALLOWED_EXTENSIONS

def load_file(file_path):
    """Carga un archivo dependiendo de su extensión y extrae las IPs maliciosas"""
    file_extension = os.path.splitext(file_path)[1].lower()
    if file_extension == ".csv":
        return load_csv(file_path)
    elif file_extension == ".json":
        return load_json(file_path)
    elif file_extension == ".parquet":
        return load_parquet(file_path)
    else:
        raise ValueError("Formato de archivo no soportado")
```

Fig. 10 código para cargar archivo parte 1

```python
def load_csv(file_path):
    """Cargar un archivo CSV y extraer IPs maliciosas con su frecuencia"""
    ip_counts = {}
    try:
        with open(file_path, mode='r') as file:
            reader = csv.DictReader(file)
            for row in reader:
                if "Srcip" in row and "Resultado" in row:
                    try:
                        resultado = int(row["Resultado"])
                        if resultado == 1:  # IP maliciosa
                            ip = row["Srcip"]
                            ip_counts[ip] = ip_counts.get(ip, 0) + 1
                    except ValueError:
                        print(f"Error: 'Resultado' no es un número válido en la fila {row}")
    except Exception as e:
        print(f"Error al procesar el archivo CSV: {e}")
    return ip_counts
```

Fig. 11 código de carga archivo parte 2

```
def generate_rules(malicious_ips):
    """Genera reglas de Snort basadas en las IPs maliciosas"""
    rules = []
    for ip in malicious_ips:
        sid = random.randint(1000000, 9999999)
        rule = f"alert ip {ip} any -> $HOME_NET any (msg:\"IP Maliciosa detectada\"; sid:{sid};)"
        rules.append(rule)
    return rules

def save_rules(rules):
    """Guarda las reglas generadas en el archivo de reglas de Snort"""
    rules_file = "/etc/snort/rules/custom.rules"
    try:
        with open(rules_file, 'r') as file:
            existing_rules = set(file.readlines())
        new_rules = [rule + "\n" for rule in rules if rule + "\n" not in existing_rules]
        if new_rules:
            with open(rules file, 'a') as file:
```

Fig. 12 código parte 3

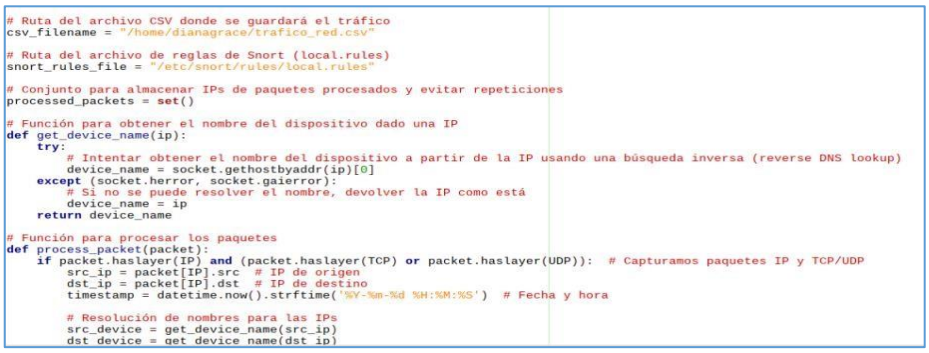
Este código index.html realiza una página web que permite al usuario cargar un archivo de dataset en formato CSV. La página presenta un formulario simple con un campo para seleccionar el archivo y un botón para subirlo al servidor, utilizando el método `POST` con el tipo de codificación `multipart/form-data`. El diseño es limpio y profesional, con un esquema de colores en tonos grises y azules, donde el contenido principal está centrado dentro de un contenedor estilizado, ofreciendo una interfaz fácil de usar.

```
        label {
            font-size: 1.1em;
            color: #34495e; /* Gris oscuro */
        }
        input[type="file"] {
            font-size: 1em;
            padding: 10px;
            border: 2px solid #bdc3c7; /* Gris claro */
            border-radius: 5px;
            background-color: #ecf0f1; /* Fondo suave gris */
        }
        input[type="file"]:hover {
            border-color: #2980b9; /* Color azul en hover */
        }
        button {
            background-color: #2980b9; /* Azul serio */
            color: white;
            border: none;
            padding: 12px;
            font-size: 1.1em;
            cursor: pointer;
            border-radius: 5px;
            transition: background-color 0.3s ease;
        }
        button:hover {
            background-color: #3498db; /* Azul más brillante en hover */
        }
        table {
            width: 100%;
            margin-top: 20px;
            border-collapse: collapse;
        }
        table, th, td {
            border: 1px solid #bdc3c7; /* Borde gris claro */
        }
```

Fig. 13 índex

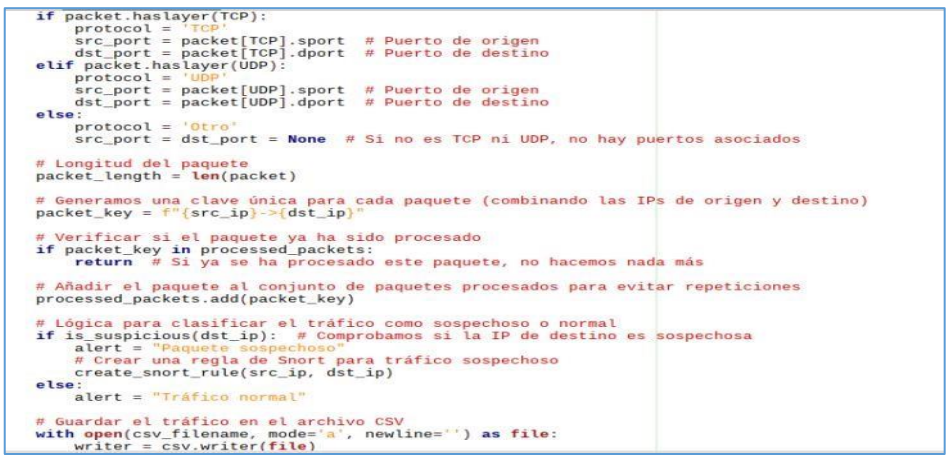
Realizamos el código de Python para la captura de tráfico en tiempo real y generación de dasboard de acuerdo con el tráfico que se va capturando:

Este código implementa un sistema automatizado de captura y análisis de tráfico de red utilizando Python y la biblioteca Scapy. Su objetivo es capturar paquetes IP que utilizan los protocolos TCP y UDP, analizar su información relevante (como IP de origen y destino, puertos, y tipo de tráfico) y almacenar estos datos en un archivo CSV. Además, el código identifica si el tráfico es sospechoso y, en tal caso, genera reglas para Snort en su archivo de reglas local.



```
# Ruta del archivo CSV donde se guardará el tráfico
csv_filename = "/home/dianagrace/trafico_red.csv"

# Ruta del archivo de reglas de Snort (local.rules)
snort_rules_file = "/etc/snort/rules/local.rules"

# Conjunto para almacenar IPs de paquetes procesados y evitar repeticiones
processed_packets = set()

# Función para obtener el nombre del dispositivo dado una IP
def get_device_name(ip):
    try:
        # Intentar obtener el nombre del dispositivo a partir de la IP usando una búsqueda inversa (reverse DNS lookup)
        device_name = socket.gethostbyaddr(ip)[0]
    except (socket.herror, socket.gaierror):
        # Si no se puede resolver el nombre, devolver la IP como está
        device_name = ip
    return device_name

# Función para procesar los paquetes
def process_packet(packet):
    if packet.haslayer(IP) and (packet.haslayer(TCP) or packet.haslayer(UDP)):  # Capturamos paquetes IP y TCP/UDP
        src_ip = packet[IP].src  # IP de origen
        dst_ip = packet[IP].dst  # IP de destino
        timestamp = datetime.now().strftime('%Y-%m-%d %H:%M:%S')  # Fecha y hora

        # Resolución de nombres para las IPs
        src_device = get_device_name(src_ip)
        dst_device = get_device_name(dst_ip)
```

Fig. 14 Código Sistema Automatizado de captura y análisis de trafico



```
    if packet.haslayer(TCP):
        protocol = 'TCP'
        src_port = packet[TCP].sport  # Puerto de origen
        dst_port = packet[TCP].dport  # Puerto de destino
    elif packet.haslayer(UDP):
        protocol = 'UDP'
        src_port = packet[UDP].sport  # Puerto de origen
        dst_port = packet[UDP].dport  # Puerto de destino
    else:
        protocol = 'Otro'
        src_port = dst_port = None  # Si no es TCP ni UDP, no hay puertos asociados

    # Longitud del paquete
    packet_length = len(packet)

    # Generamos una clave única para cada paquete (combinando las IPs de origen y destino)
    packet_key = f"{src_ip}->{dst_ip}"

    # Verificar si el paquete ya ha sido procesado
    if packet_key in processed_packets:
        return  # Si ya se ha procesado este paquete, no hacemos nada más

    # Añadir el paquete al conjunto de paquetes procesados para evitar repeticiones
    processed_packets.add(packet_key)

    # Lógica para clasificar el tráfico como sospechoso o normal
    if is_suspicious(dst_ip):  # Comprobamos si la IP de destino es sospechosa
        alert = "Paquete sospechoso"
        # Crear una regla de Snort para tráfico sospechoso
        create_snort_rule(src_ip, dst_ip)
    else:
        alert = "Tráfico normal"

    # Guardar el tráfico en el archivo CSV
    with open(csv_filename, mode='a', newline='') as file:
        writer = csv.writer(file)
```

Fig. 15 Código Sistema Automatizado de captura y análisis de trafico

A continuación, tenemos el código implementa un sistema interactivo de visualización de datos de tráfico de red utilizando el framework Dash y Plotly. Su objetivo principal es leer, procesar y mostrar información sobre el tráfico de red a partir de un archivo CSV. Los datos incluyen información sobre el tipo de tráfico, como "Tráfico Normal" y "Paquete Sospechoso" (o tráfico malicioso), y son utilizados para generar gráficos de barras y tablas en tiempo real. El gráfico de barras presenta el número de alertas agrupadas por tipo de tráfico a lo largo del tiempo, permitiendo a los usuarios identificar visualmente patrones de tráfico y posibles amenazas. Las barras se colorean dinámicamente, utilizando verde para el tráfico normal y rojo para el tráfico sospechoso, facilitando la distinción entre ambos.

2.5.4. Fase 4: Pruebas

2.5.4.1. Pruebas y Validación del Sistema

En esta fase, se lleva a cabo la validación y pruebas del sistema implementado para asegurar que el sistema de monitoreo de red inteligente es funcional, eficiente y capaz de detectar intrusiones de manera precisa.

Se realiza la ejecución de captura.py la misma que muestra lo siguiente:

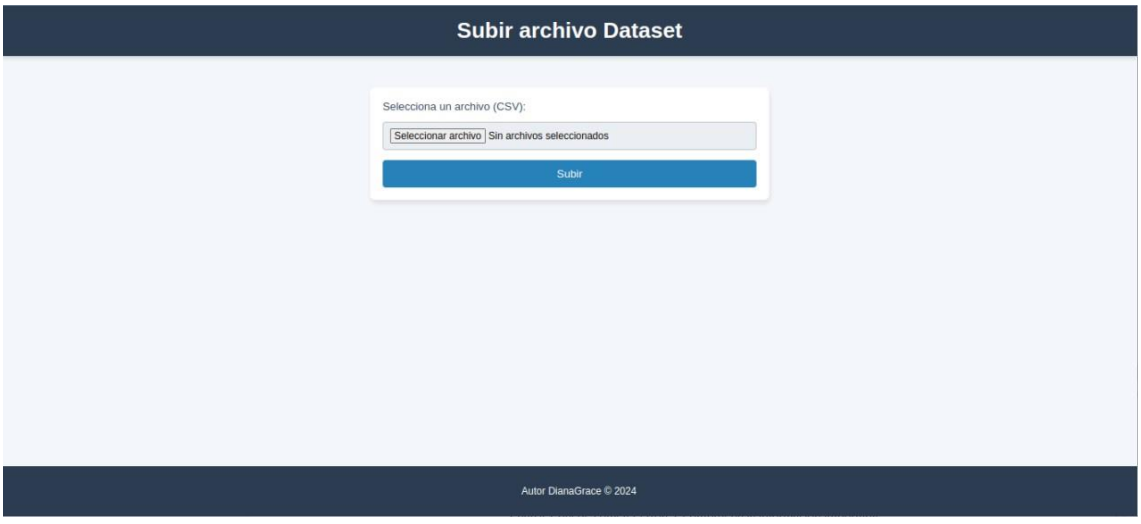


Fig. 16 Interfaz de Dataset

Procedemos a subir el csv proporcionado que ya está normalizado para seguir con el proceso:

Fig. 17 proceso para subir archivos

Al subirse el csv, nos muestra los botones para visualizar, reglas, ip maliciosas y el grafico de barras, dispersión según lo analizado:

Fig. 18 Resultados del dataset

En esta imagen mostramos las reglas creadas de manera automática mediante nuestro código de Python, estas están mostrándose en la interfaz gráfica:

Reglas creadas en ids Snort:

Reglas Generadas con Éxito

Número total de reglas generadas: **509**

#	Regla
1	alert ip 172.26.0.4 any -> $HOME_NET any (msg:"IP Maliciosa detectada"; sid:3194163;)
2	alert ip 172.26.0.6 any -> $HOME_NET any (msg:"IP Maliciosa detectada"; sid:6739385;)
3	alert ip 192.168.14.220 any -> $HOME_NET any (msg:"IP Maliciosa detectada"; sid:6434551;)
4	alert ip 172.23.0.23 any -> $HOME_NET any (msg:"IP Maliciosa detectada"; sid:9770557;)
5	alert ip 172.31.1.73 any -> $HOME_NET any (msg:"IP Maliciosa detectada"; sid:7474056;)
6	alert ip 172.31.0.216 any -> $HOME_NET any (msg:"IP Maliciosa detectada"; sid:2883600;)
7	alert ip 172.31.6.13 any -> $HOME_NET any (msg:"IP Maliciosa detectada"; sid:5712085;)
8	alert ip 172.15.0.42 any -> $HOME_NET any (msg:"IP Maliciosa detectada"; sid:2350921;)
9	alert ip 172.27.0.3 any -> $HOME_NET any (msg:"IP Maliciosa detectada"; sid:1768371;)
10	alert ip 172.19.3.203 any -> $HOME_NET any (msg:"IP Maliciosa detectada"; sid:8042949;)
11	alert ip 172.31.3.220 any -> $HOME_NET any (msg:"IP Maliciosa detectada"; sid:5849321;)

Fig. 19 Reglas en ids snort

En este apartado mostramos las veces que la ip se ha detectado como maliciosa:

Y finalmente mostramos el grafico de dispersión, el mismo que fue generado mediante el código de Python al subir el dataset normalizado:

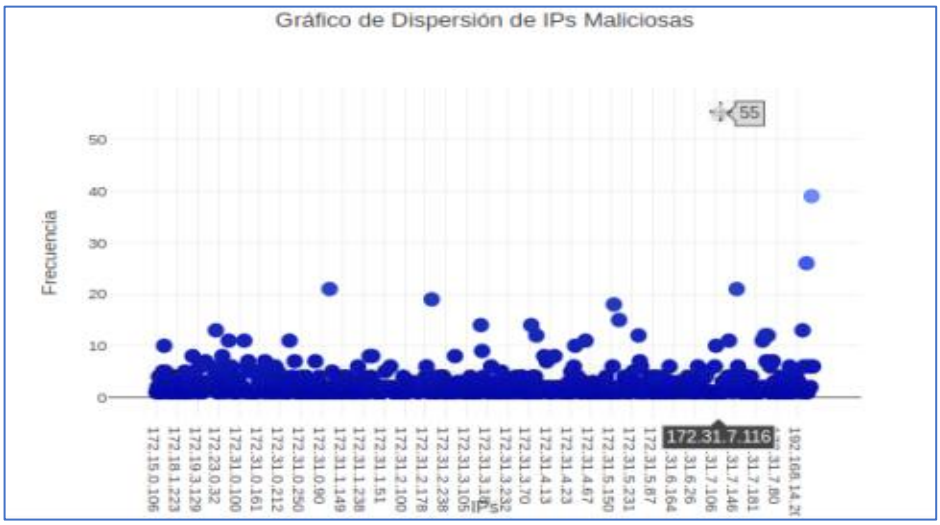


Figura 20: Resultado csv

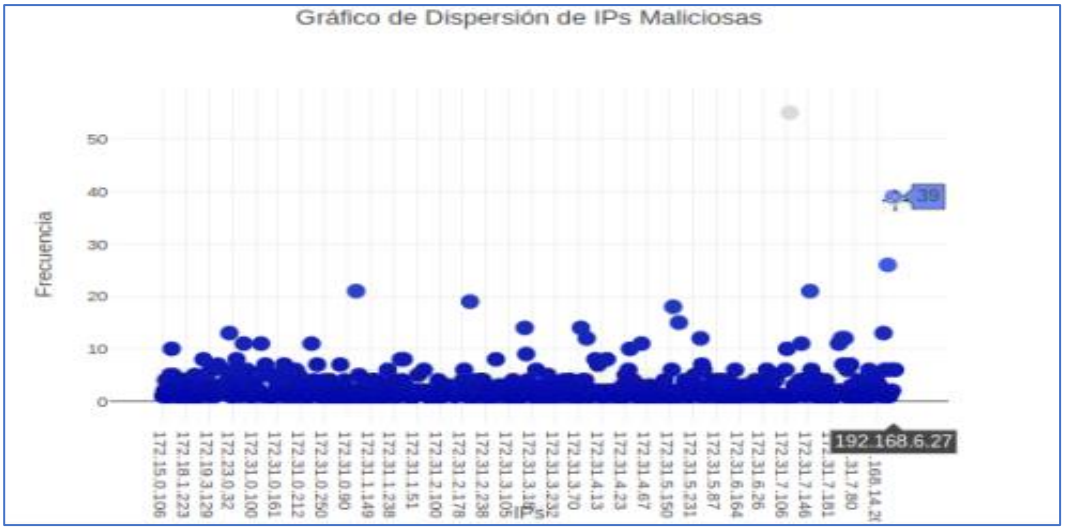


Figura 20: Resultado csv

Ahora ingresamos de nuevo al entorno para ejecutar nuestro archivos.py los cuales hacen la captura de datos en tiempo real y en el dashboard se muestra el resultado según el tráfico que se va capturando:

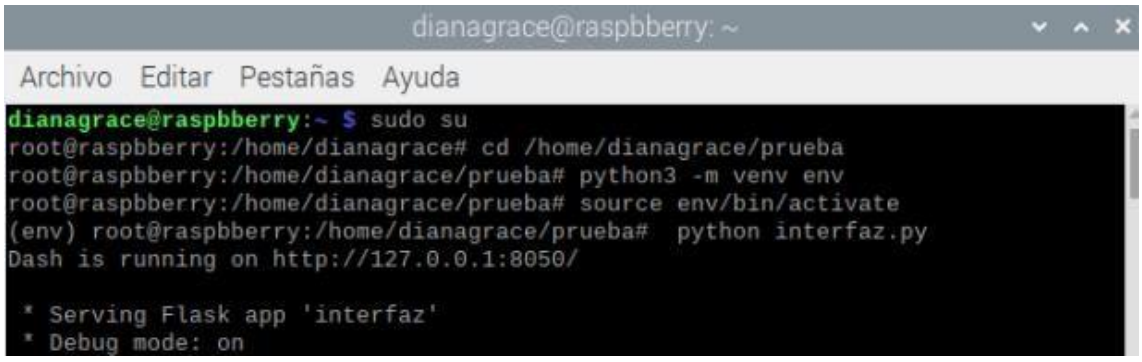


Fig. 21 proceso para captura en tiempo real

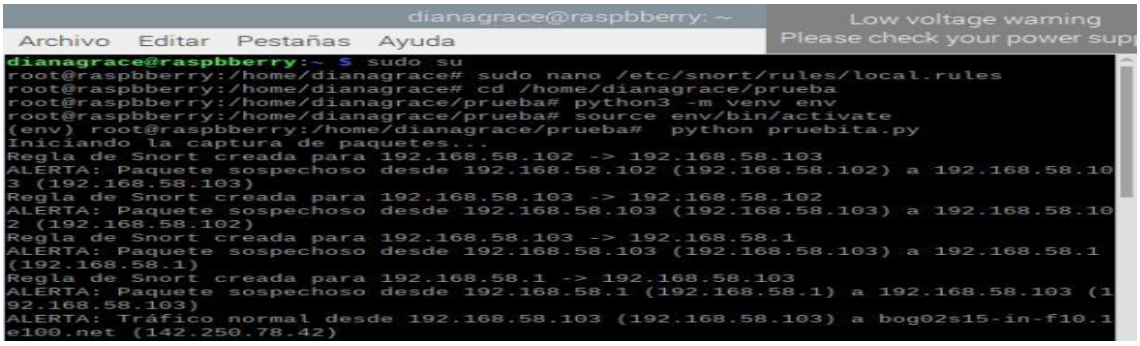
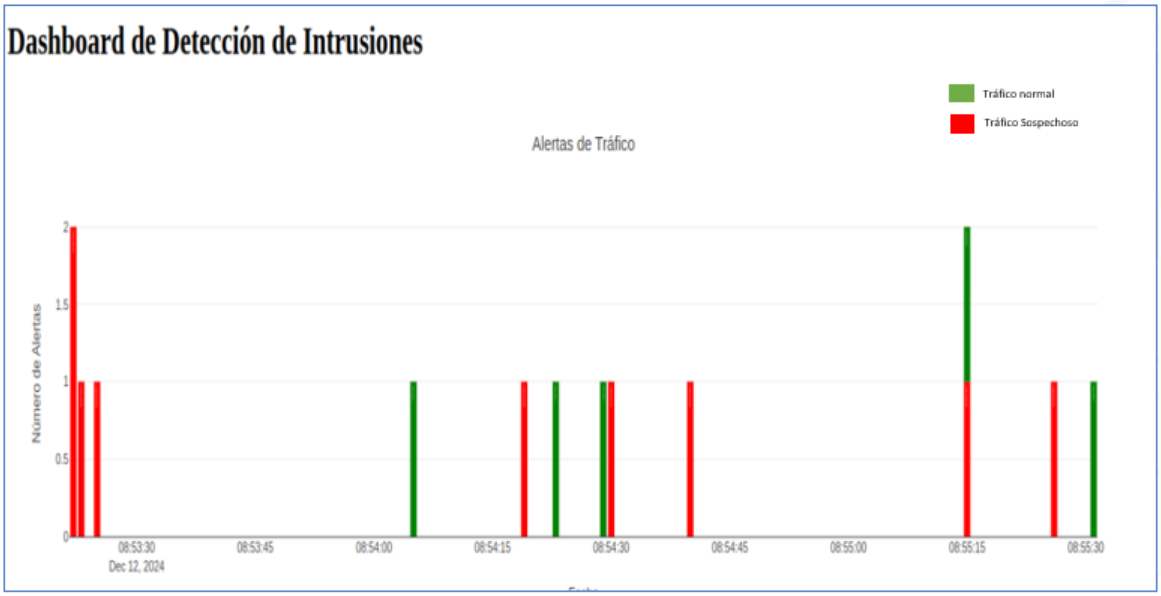


Fig. 22 inicio de capturación de trafico

Mientras se ejecutan estos los archivos al mismo tiempo en la página se muestra la gráfica que proporciona el tráfico normal y el tráfico sospechoso, la tabla donde se clasifica el tipo de tráfico que se está generando en el momento:



Fecha	IP de origen	Dispositivo de origen	Puerto de origen	IP de destino	Dispositivo de destino	Puerto de destino	Tipo de tráfico
2024-12-09T13:27:10	192.168.58.103	192.168.58.103	5900	192.168.58.102	192.168.58.102	49778	Paquete Sospechoso
2024-12-09T13:27:10	192.168.58.102	192.168.58.102	49778	192.168.58.103	192.168.58.103	5900	Paquete Sospechoso
2024-12-09T13:27:10	192.168.58.103	192.168.58.103	48277	192.168.58.1	192.168.58.1	53	Paquete Sospechoso
2024-12-09T13:27:11	192.168.58.1	192.168.58.1	53	192.168.58.103	192.168.58.103	48277	Paquete Sospechoso
2024-12-09T13:27:48	192.168.58.103	192.168.58.103	41606	35.196.193.138	138.193.196.35.bc.googleusercontent.com	443	Tráfico Normal
2024-12-09T13:27:49	35.196.193.138	138.193.196.35.bc.googleusercontent.com	443	192.168.58.103	192.168.58.103	41606	Paquete Sospechoso
2024-12-09T13:27:56	192.168.58.103	192.168.58.103	37157	142.250.78.74	bog02s16-in-f10.1e100.net	443	Tráfico Normal
2024-12-09T13:27:57	142.250.78.74	bog02s16-in-f10.1e100.net	443	192.168.58.103	192.168.58.103	37157	Paquete Sospechoso
2024-12-09T13:28:00	192.168.58.104	192.168.58.104	60357	239.255.255.250	239.255.255.250	1900	Tráfico Normal
2024-12-09T13:28:21	142.250.78.42	bog02s15-in-f10.1e100.net	443	192.168.58.103	192.168.58.103	58855	Paquete Sospechoso
2024-12-09T13:28:41	192.168.58.103	192.168.58.103	58407	239.255.255.250	239.255.255.250	1900	Tráfico Normal
2024-12-09T13:34:35	192.168.58.103	192.168.58.103	5900	192.168.58.102	192.168.58.102	49778	Paquete Sospechoso
2024-12-09T13:34:36	192.168.58.102	192.168.58.102	49778	192.168.58.103	192.168.58.103	5900	Paquete Sospechoso
2024-12-09T13:34:36	192.168.58.103	192.168.58.103	38461	192.168.58.1	192.168.58.1	53	Paquete Sospechoso
2024-12-09T13:34:36	192.168.58.1	192.168.58.1	53	192.168.58.103	192.168.58.103	38461	Paquete Sospechoso
2024-12-09T13:36:35	192.168.58.103	192.168.58.103	53385	239.255.255.250	239.255.255.250	1900	Tráfico Normal
2024-12-09T13:36:41	172.217.172.10	bog02s09-in-f10.1e100.net	443	192.168.58.103	192.168.58.103	38694	Paquete Sospechoso
2024-12-09T13:39:31	192.168.58.102	192.168.58.102	49778	192.168.58.103	192.168.58.103	5900	Paquete Sospechoso
2024-12-09T13:39:31	192.168.58.103	192.168.58.103	5900	192.168.58.102	192.168.58.102	49778	Paquete Sospechoso
2024-12-09T13:39:31	192.168.58.103	192.168.58.103	43230	192.168.58.1	192.168.58.1	53	Paquete Sospechoso
2024-12-09T13:39:31	192.168.58.1	192.168.58.1	53	192.168.58.103	192.168.58.103	43230	Paquete Sospechoso
2024-12-09T13:40:12	192.168.58.103	192.168.58.103	53500	142.250.78.74	bog02s16-in-f10.1e100.net	443	Tráfico Normal
2024-12-09T13:40:58	142.250.78.74	bog02s16-in-f10.1e100.net	443	192.168.58.103	192.168.58.103	53500	Paquete Sospechoso
2024-12-09T14:19:09	192.168.58.103	192.168.58.103	5900	192.168.58.102	192.168.58.102	49778	Paquete Sospechoso
2024-12-09T14:19:09	192.168.58.102	192.168.58.102	49778	192.168.58.103	192.168.58.103	5900	Paquete Sospechoso
2024-12-09T14:19:09	192.168.58.103	192.168.58.103	47232	192.168.58.1	192.168.58.1	53	Paquete Sospechoso

Fig. 24 Resultado de la captura de trafico

2.5.5. Fase de Evaluación y Revisión:

2.5.5.1. Fase 5: Visualización de Resultados y Dashboard

En esta fase, se desarrolló e implementó el dashboard interactivo, cuyo objetivo es mostrar los resultados del monitoreo de la red de manera clara y en tiempo real. El dashboard presenta gráficos, tablas y alertas que facilitan la visualización de los eventos de seguridad más relevantes detectados por el sistema IDS. La visualización de los resultados es esencial para que los administradores de red puedan interpretar rápidamente las amenazas y tomar acciones correctivas en caso de intrusiones.

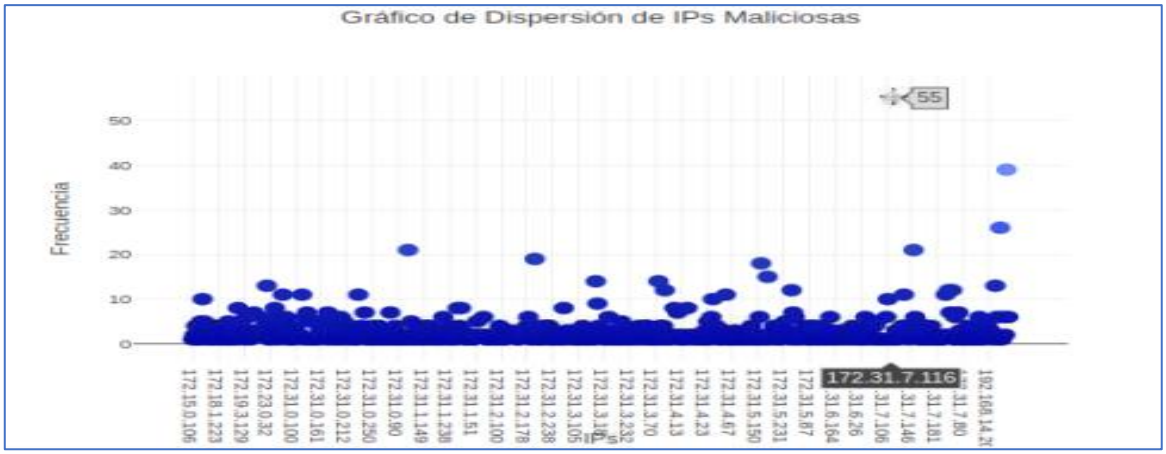


Figura 25: Resultado del csv

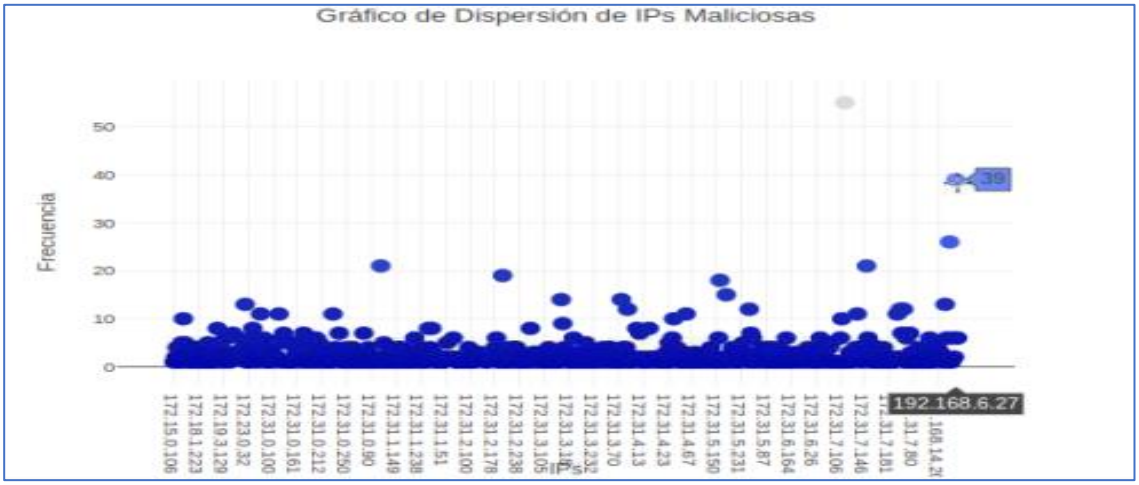


Figura 25: Resultado del csv

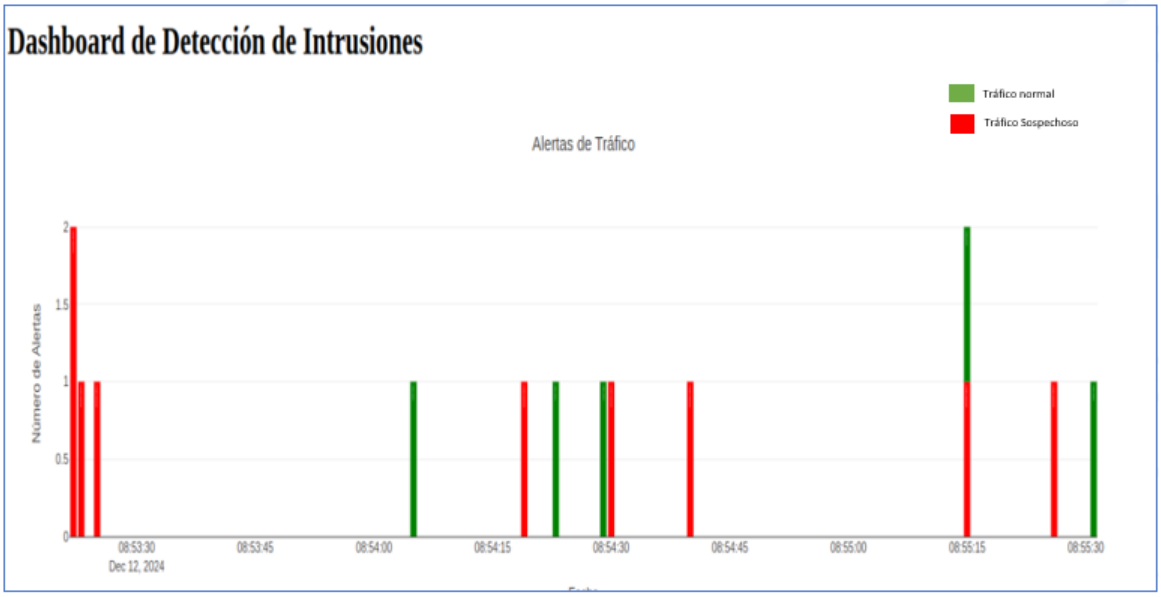


Figure 29: Alertas de tráfico en tiempo real

2.6. Arquitectura de detección de tráfico web

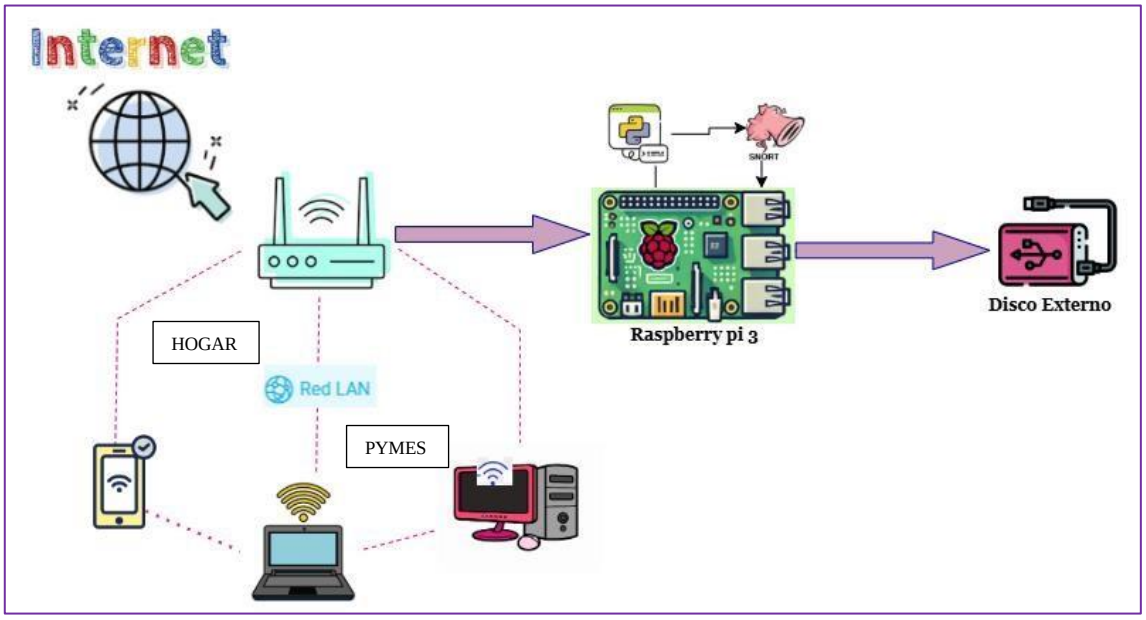


Fig. 27 arquitectura de trafico

El sistema está diseñado para monitorear y analizar el tráfico de red dentro de una Red LAN mediante la integración de dispositivos de bajo costo y software especializado. El componente central es un raspberry Pi 3, que actúa como el nodo de procesamiento y análisis del tráfico.

1. Conexión a Internet y Red LAN: El sistema está conectado tanto a la red local (LAN) como a Internet. Los distintos dispositivos en la LAN (computadoras, teléfonos móviles y otros dispositivos conectados) envían y reciben datos a través de un router. Esta red de dispositivos es monitoreada por el Raspberry Pi, que captura el tráfico para su análisis.
2. Raspberry Pi 3 como Nodo de Monitoreo: El Raspberry Pi 3 se encarga de ejecutar un sistema de detección de intrusiones (IDS) utilizando herramientas como Snort para inspeccionar el tráfico en tiempo real. El software instalado en el Raspberry Pi, desarrollado en Python, analiza el tráfico, detecta comportamientos anómalos, y registra cualquier amenaza o actividad sospechosa. La elección de un raspberry Pi 3 asegura un sistema asequible y eficiente, capaz de funcionar de manera continua y con bajo consumo de energía.

3. Almacenamiento Externo: El sistema incluye un disco externo conectado al Raspberry Pi, que almacena los logs y registros del tráfico de red capturado, así como cualquier alerta o resultado generado por el IDS. Este componente asegura que los datos se mantengan seguros y disponibles para análisis posteriores, a la vez que libera espacio en el Raspberry Pi.

4. Interacción con Dispositivos de la Red: Los dispositivos conectados a la red LAN, como laptops, computadoras de escritorio y teléfonos móviles, son monitorizados pasivamente. Toda la información de tráfico que pasa por el router se canaliza al Raspberry Pi para ser inspeccionada. La interacción entre los dispositivos y el sistema de monitoreo se realiza de manera transparente, sin interrumpir el flujo normal de la red.

Esta arquitectura optimiza el monitoreo de seguridad en tiempo real para redes pequeñas o medianas (como hogares o pymes), utilizando una infraestructura sencilla pero efectiva. El Raspberry Pi centraliza el procesamiento y el análisis, mientras que el disco externo asegura el almacenamiento de los datos capturados, formando una solución robusta y escalable para la detección de intrusiones y la protección de la red.

2.6.1. Arquitectura de sistema de monitoreo de red inteligente

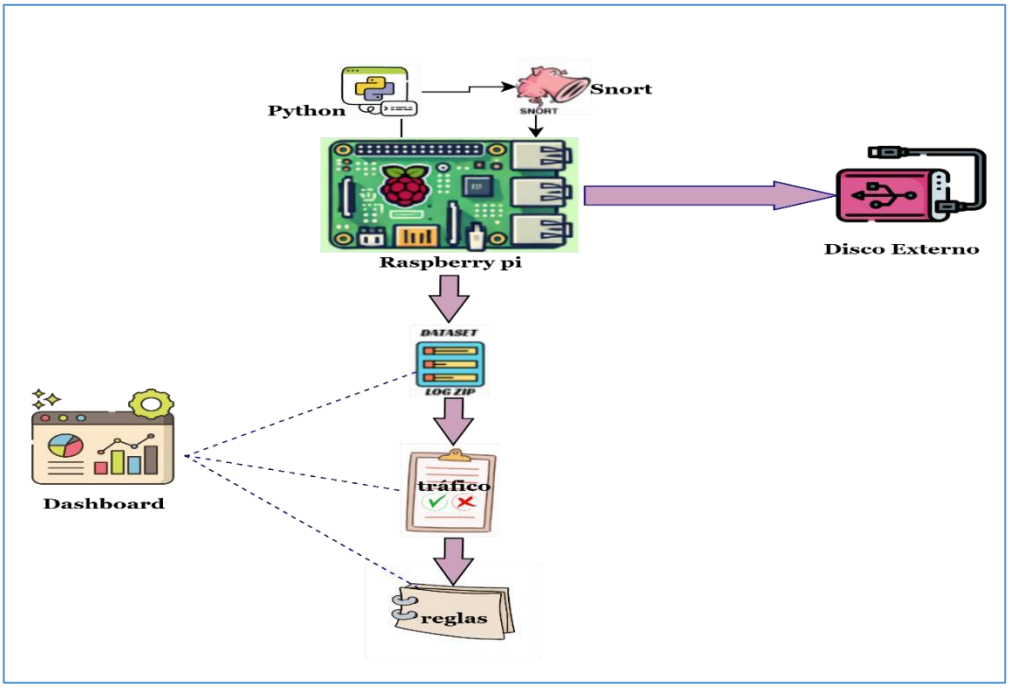


Fig. 28 arquitectura de sistema de monitoreo de red inteligente

El diagrama presentado describe el flujo de datos y la arquitectura de un sistema de monitoreo de red inteligente, diseñado para la detección de intrusiones y la gestión del tráfico de red utilizando herramientas de software y hardware especializado. En el centro del sistema se encuentra un Raspberry Pi, un ordenador de bajo costo que actúa como el nodo principal, gestionando tanto la captura de datos de red como su procesamiento. Conectado a un dispositivo de almacenamiento externo a través de un puerto USB, el Raspberry Pi recopila los datos de tráfico y los registros de eventos de red para su posterior análisis.

En la parte superior del diagrama, se destacan dos componentes clave: Snort y Python. Snort es un sistema de detección de intrusiones (IDS) que se utiliza para monitorear el tráfico de red en busca de actividad sospechosa o patrones que indiquen posibles ciberataques. Python, por su parte, parece estar desempeñando un rol esencial en el procesamiento y análisis automatizado de estos datos, permitiendo la integración de scripts personalizados que potencian las capacidades del sistema.

Los datos de tráfico y los registros recolectados por el Raspberry Pi son almacenados en un formato comprimido ("Dataset / Log ZIP"), optimizando su gestión y facilitando su análisis. A partir de estos datos, el sistema realiza un análisis profundo del tráfico de red, clasificándolo en categorías de "bueno" o "malicioso", lo cual es visualizado en informes detallados. La detección de tráfico malicioso está representada por un informe que discrimina claramente entre tráfico legítimo y sospechoso, posibilitando la rápida identificación de amenazas.

Finalmente, a partir de los resultados del análisis de tráfico, se generan reglas que probablemente son utilizadas para configurar el propio Snort o algún sistema de firewall, mejorando la seguridad de la red de manera proactiva. Este sistema se complementa con una interfaz gráfica de usuario o dashboard, que permite visualizar en tiempo real los resultados del análisis de tráfico, proporcionando al administrador de la red una visión clara y comprensible del estado de la seguridad y de las amenazas detectadas.

2.7. Resultados

El sistema de detección de intrusiones (IDS) desarrollado en este proyecto demostró una alta eficiencia en la identificación de amenazas de seguridad en tiempo real. Al utilizar la

herramienta SNORT, el sistema fue capaz de capturar y analizar el tráfico de red, generando alertas ante la detección de comportamientos sospechosos o IPs maliciosas.

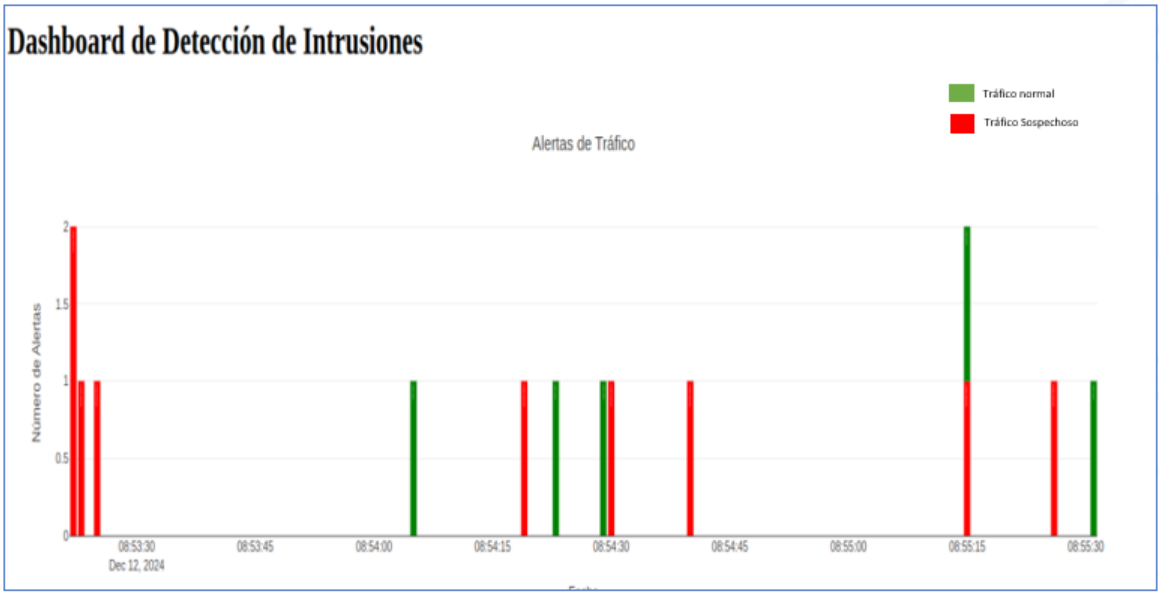


Figure 29: resultado de tráfico en tiempo real

El sistema incluye una interfaz gráfica interactiva diseñada con Dash, que permite visualizar en tiempo real los datos recolectados. La interfaz muestra gráficos interactivos, como gráficos de dispersión y tablas que detallan el tráfico de red. Los resultados resaltan la capacidad de la interfaz para detectar patrones en los datos, facilitando la identificación de IPs maliciosas y proporcionando una vista clara del tráfico sospechoso y normal. Esta herramienta permite al usuario monitorear la red de manera eficiente y tomar decisiones rápidas basadas en los reportes generados.

Fecha	IP de origen	Dispositivo de origen	Puerto de origen	IP de destino	Dispositivo de destino	Puerto de destino	Tipo de tráfico
2024-12-12T08:53:22	192.168.58.106	192.168.58.106	51695	192.168.58.108	192.168.58.108	5900	Paquete Sospechoso
2024-12-12T08:53:22	192.168.58.108	192.168.58.108	5900	192.168.58.106	192.168.58.106	51695	Paquete Sospechoso
2024-12-12T08:53:23	192.168.58.108	192.168.58.108	56429	192.168.58.1	192.168.58.1	53	Paquete Sospechoso
2024-12-12T08:53:25	192.168.58.1	192.168.58.1	53	192.168.58.108	192.168.58.108	56429	Paquete Sospechoso
2024-12-12T08:54:05	192.168.58.108	192.168.58.108	53422	239.255.255.250	239.255.255.250	1900	Tráfico Normal
2024-12-12T08:54:19	35.196.193.138	138.193.196.35.bc.googleusercontent.com	443	192.168.58.108	192.168.58.108	56730	Paquete Sospechoso
2024-12-12T08:54:23	192.168.58.108	192.168.58.108	56730	35.196.193.138	138.193.196.35.bc.googleusercontent.com	443	Tráfico Normal
2024-12-12T08:54:29	192.168.58.108	192.168.58.108	34836	142.250.217.170	mia07s60-in-f10.1e100.net	443	Tráfico Normal
2024-12-12T08:54:30	142.250.217.170	mia07s60-in-f10.1e100.net	443	192.168.58.108	192.168.58.108	34836	Paquete Sospechoso
2024-12-12T08:54:40	192.168.58.106	192.168.58.106	137	192.168.58.255	192.168.58.255	137	Paquete Sospechoso
2024-12-12T08:55:15	192.168.58.108	192.168.58.108	35047	142.250.64.234	mia07s57-in-f10.1e100.net	443	Tráfico Normal
2024-12-12T08:55:15	142.250.64.234	mia07s57-in-f10.1e100.net	443	192.168.58.108	192.168.58.108	35047	Paquete Sospechoso
2024-12-12T08:55:26	52.149.246.39	52.149.246.39	443	192.168.58.108	192.168.58.108	33206	Paquete [illegible]
2024-12-12T08:55:31	192.168.58.108	192.168.58.108	33206	52.149.246.39	52.149.246.39	443	Tráfico Normal
2024-12-12T08:56:22	192.168.58.108	192.168.58.108	35875	192.178.50.42	lcmiaa-aa-in-f10.1e100.net	443	Tráfico Normal

Fig. 30 resultado de captura de trafico

CONCLUSIONES

El presente proyecto logró implementar un sistema inteligente de detección de intrusiones (IDS) eficiente, utilizando hardware de bajo costo como el Raspberry Pi 3 y software basado en Python. Este sistema permitió el monitoreo y análisis en tiempo real del tráfico de red, detectando con precisión amenazas de seguridad mediante herramientas como SNORT, complementadas con algoritmos de machine learning La visualización de los datos recolectados se implementó mediante una interfaz gráfica interactiva diseñada en Dash, la cual facilita el análisis de tráfico de red y ofrece una representación clara y accesible de las actividades sospechosas y normales.

La implementación de este sistema en hardware asequible demostró ser una solución viable y efectiva para proteger redes en entornos de pequeñas empresas y hogares, cumpliendo con los objetivos establecidos. Asimismo, el análisis automatizado y la generación de reglas de seguridad en formato Snort optimizaron la operación del sistema, permitiendo una respuesta más rápida y precisa ante nuevas amenazas. Los resultados reflejan que es posible diseñar e implementar soluciones de ciberseguridad inteligentes y

de bajo costo, que integren machine learning y tecnologías de captura de tráfico, contribuyendo a la detección de patrones anómalos y a la mejora de la seguridad en redes informáticas.

RECOMENDACIONES

Se recomienda mejorar el rendimiento del sistema de detección de intrusiones mediante la implementación de hardware más potente, como un Raspberry Pi 4 o un servidor dedicado, especialmente en redes con alto volumen de tráfico. Aunque el sistema actual basado en Raspberry Pi 3 es funcional para entornos pequeños, un hardware más avanzado permitirá un procesamiento más rápido y eficiente, mejorando la velocidad de detección y respuesta ante las amenazas. Esta optimización es crucial si se busca expandir el sistema a redes más grandes o complejas.

También se sugiere explorar técnicas avanzadas de machine learning para incrementar la precisión de la detección de intrusiones. El uso de algoritmos más sofisticados, como redes neuronales profundas o algoritmos de detección de anomalías, podría mejorar la capacidad del sistema para detectar ataques complejos y reducir la tasa de falsos positivos. Para maximizar el rendimiento de estos modelos, se recomienda entrenarlos con datasets más amplios y representativos, lo que contribuirá a una mayor capacidad de generalización del sistema frente a nuevas amenazas. La incorporación de técnicas de inteligencia artificial más robustas incrementará el nivel de seguridad ofrecido.

Además, sería beneficioso integrar mecanismos de respuesta automatizada, como el bloqueo automático de IPs maliciosas o la modificación dinámica de las reglas del firewall en tiempo real. Esto permitiría que el sistema no solo notifique al administrador de posibles amenazas, sino que también actúe de manera inmediata para neutralizarlas, aumentando la protección de la red. Finalmente, se recomienda realizar pruebas en entornos reales y asegurar actualizaciones periódicas del sistema y las reglas de seguridad, ya que las amenazas evolucionan constantemente, y el sistema debe mantenerse actualizado para ser efectivo.

BIBLIOGRAFÍA

[1] N. C. S. Chamba, «"Estrategias para mejorar el proceso de enseñanza-aprendizaje en estudiantes de educación inicial,",» Loja, 2021.

[2] UPSE, «UPSE,» [En línea]. Available: https://www.upse.edu.ec/index.php?option=com_content&view=article&id=10&Itemid=166.

[3] IBM. [En línea]. Available: https://www.ibm.com/es-es/topics/intrusiondetection-system..

[4] Seidor, «Seidor,» [En línea]. Available: https://www.seidor.com/es-es/blog/elimpacto-del-edge-computing-y-la-inteligencia-artificial-en-el-ecosistema-deaplicaciones..

[5] P. García, «“Confidencialidad, integridad y disponibilidad”,» Feb 2018.

[6] K. Networks, «“Importancia de ciberseguridad y ciberdefensa para los países”».

[7] UPSE, «UNIVERSIDAD ESTATAL PENINSULA DE SANTA ELENA,» [En línea]. Available: https://www.upse.edu.ec/index.php?option=com_content&view=article&id=10&Itemid=166.

[8] A. NACIONAL, «"LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES",» 2021.

[9] R. D. ECUADOR, «CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR,» *LexisFindeRr,* 2008.

[10] R. D. E. A. NACIONAL, «L, CÓDIGO ORGÁNICO INTEGRAL PENAL, COIP,» *LexisFinder,* 2021.

[11] IBM, «IBM,» [En línea]. Available: https://www.ibm.com/mxes/topics/network-monitoring.

[12] UNIR. [En línea]. Available: https://colombia.unir.net/actualidad-unir/que-esciberseguridad/#:~:text=La%20importancia%20de%20la%20ciberseguridad&t e xt=La%20ciberseguridad%20no%20solo%20salvaguarda,la%20evoluci%C3%B3n%20de%20las%20amenazas..

[13] E. J. M. Alfaro, 13 Enero 2002. [En línea]. Available: http://mural.uv.es/emial/informatica/html/IDS.html#key-16.

[14] T. Tech, «"Edge Computing: ¿Qué es?,",» 2023.

[15] A. W. Services, «"¿Qué es el Machine Learning?,",» 21 sep 2023.

[16] A. González, «Uso de técnicas de minería de datos en la detección de intrusiones,» *Redalyc,* vol. 5, nº 1, pp. 1-12, 2015.

[17] Verza, «Análisis de datos,» nº 1, 2023.

[18] I. IT, «Análisis de Comportamiento de Red: ¿Qué es?,» nº 1, 2023.

[19] R. P. Chile, «"¿Qué es Raspberry Pi?",» 2023.

[20] A. W. Services, «¿Qué es Python?,» 2023.

[21] Á. BST, «"Tipos de vulnerabilidades y amenazas informáticas,,» 13 Julio 2023. [En línea]. Available: https://www.ambit-bst.com/blog/tipos-devulnerabilidades-y-amenazas-inform%C3%A1ticas.. [Último acceso: 15 Sep 2024].

[22] Fortinet, «Fortinet,» [En línea]. Available: https://www.fortinet.com/lat/resources/cyberglossary/snort. [Último acceso: 25 sep 2024].

[23] ManageEngine, «ANÁLISIS DE TRÁFICO DE LA RED,» [En línea]. Available: https://www.manageengine.com/latam/netflow/analisis-de-traficode-red.html. [Último acceso: 20 Octubre 2024].

[24] S. M. I. y. M. M. Cruz, ««ANÁLISIS Y CONFORMACIÓN DE TRÁFICO EN INTERNET,»,» p. 106, 2011.

[25] W. B. ANJELINO, ««HARASDADICO,»,» *HARASDADICO*, 2022.

[26] C. Pvt.Ltd.All, ««ManageEngine,»,» [En línea]. Available: https://www.manageengine.com/latam/netflow/que-es-netflow.html.

[27] W. C. L. V. y. J. M. L. M. A. F. R. Calderon, ««SEGURIDAD INFORMATICA POR CAPAS PARA LA PROTECCION DE LA INFORMACION EN LA INTRANET DE LA COOPERATIVA DE AHORRO Y CREDITO JUAN PIO DE MORA,» 2015.

[28] J. &. C. P. Chalén, «Diseño de un sistema de gestión de seguridad de datos mediante Firewall, AAA, IPS, SIEM(tesis de grado),» Guayaquil, 2015.

[29] S. Garcés, «Seguridad Informática para la red de datos en la Cooperativa de Ahorro y Crédito Unión Popular LTDA.(tesis de grado),» Ambato, 2015.

[30] I. Narváez, «Sistema de consulta y notificación de alertas de seguridad mediante VoIP en Raspberry Pi. (Proyecto de fin de carrera).,» Sevilla, 2015.

[31] E. Aimacaña, «Esquema de seguridad perimetral y control de incidencias de la red de datos para la Universidad Técnica de Cotopaxi (Tesis de grado previo a la obtencion del titulo magister),» Ambato-Ecuador, 2015.

[32] P. Moreno, «Auditor WiFi desde Raspberry Pi controlado por dispositivo Android (Tesis de fin de grado),» Valencia-España, 2014/2015.

[33] C. Rosado, «Virtualización de una red LAN con servidores de código abierto para evaluar los niveles de seguridad (Tesis para la obtención de título de magister).,» Guayaquil-Ecuador, 2014.

[34] O. M. d. Turismo, «Guía para el desarrollo del turismo gastronómico.,» *OMT,* p. 54, 2020.

[35] Ministerio de Turismo Ministerio de Turismo (MINTUR), «Programas y Servicios: Direccion de Inversión Turística,» 2019. [En línea]. Available: https://ecuadorec.com/ministerio-de-turismo-www-turismo-gob-ec/.

[36] INEC, «Instituto Nacional de Estadistica y Censos,» 2010. [En línea]. Available: https://www.ecuadorencifras.gob.ec/wp-content/descargas/Manulateral/Resultados-provinciales/santa_elena.pdf.

[37] Ortiz; Peralta, «El Turismo de sol y playa: Impacto turístico en los ecosistemas de la comuna Ayangue, para mejorar la gestión de la actividad turística en la provincia de Santa Elena.,» *Revista Científica y Tecnológica UPSE,,* vol. 6, nº 2, pp. 82-90, 2019.

[38] Banco Central del Ecuador, «Rendición de cuentas 2018,» 2018. [En línea]. Available: https://www.turismo.gob.ec/wp-content/uploads/2019/02/InformeRendici%C3%B3n-de-Cuentas-2018-MINTUR.pdf.

[39] R. D. Ramírez, «Gastronomía,» 07 03 2019. [En línea]. Available: https://ecuador.gastronomia.com/noticia/8754/santa-elena-destinogastronomico. [Último acceso: 10 11 2020].

[40] F. Torres Oñate, J. Romero Fierro y F. Viteri M., «DIVERSIDAD GASTRONÓMICA Y SU APORTE A LA IDENTIDAD CULTURAL,» *Revista de Comunicación de la SEECI.*, nº 44, pp. 1-13, 2017.

[41] M. O. Mejía, W. C. Franco, M. C. Franco y F. Z. Flores, «Perfil y Preferencias de los Visitantes en Destinos Con Potencial Gastronómico: Caso 'Las Huecas' de Guayaquil [Ecuador],» *Rosa dos Ventos,* vol. 9, nº 2, 2017.

[42] S. J. L. Quintero, «Sostenibilidad sociocultural del turismo: propuestas para el cantón Playas. Provincia del Ecuador,» *Revista Espiga,* vol. 15, nº 31, pp. 31-43, 2016.

[43] J. Prada Trigo y S. Pesántez Loyola, «SATISFACCIÓN Y MOTIVACIÓN EN DESTINOS CULTURALES: TIPOLOGÍA DE LOS TURISTAS ATRAÍDOS POR EL PATRIMONIO INMATERIAL EN CUENCA (ECUADOR),» *Diálogo Andino - Revista de Historia, Geografía y Cultura Andina,* nº 52, pp. 77-91, 2017.

[44] Huilcapi, Castro y Jácome, «Motivación: las teorías y su relación en el ámbito empresarial,» *Dominio de las Ciencias,* vol. 3, nº 2, pp. 311-333, 2017.

[45] A. H. Maslow, «A theory of human motivation”.,» *Psychological Review,* vol. 50, pp. 370-396., 1943.

[46] A. Bormann, «Doctrina del turismo: un plano de planta. Sociedad de ayudas para la enseñanza de las ciencias del transporte en d. Reichsbahn alemán.,» *Deutschen Reichsbahn.,* 1930.

[47] Hunziker y Krapf, «Plano de la educación turística general.,» *Universidad de Berna,* 1942.

[48] A. M. Hjalager y G. Richard, «Demand for the gastronomy tourism product. Motivacional factors. In: Tourism and Gastronomy.,» *Routledge,,* pp. 36-50, 2002.

[49] F. A. Llano, «Gastronomía, turismo y potencialidades territoriales: el plato minero y la salazón, bases para el turismo alimentario en Nemocón,» *Cuadernos de Geografía - Revista Colombiana de Geografía,* vol. 26, nº 2, pp. 295-306, 2017.

[50] Hernández, Tamayo, Castro y Muñoz, «Tendencias gastronómicas predominantes en la producción de revistas científicas de Iberoamérica,» *Ciencia Ergo Sum,* vol. 23, nº 1, pp. 76-84, 2016.

[51] Moratt, Zapata y Messager, «Conceptualización de ciclo vital familiar: una mirada a la producción durante el período comprendido entre los años 2002 a 2015,» *CES Psicología,,* vol. 8, nº 2, pp. 103-121, 2015.

[52] S. L. León, «Tendencias actuales de la economía y su influencia sobre la teoría del consumidor,» *100-cS*, pp. 1-33, 2019.

[53] D. C. Iturralde, «Los paradigmas del desarrollo y su evolución: Del enfoque económico al multidisciplinario.,» *Ciencias de la Administración y Economía,* vol. 9, nº 17, pp. 7-23, 2019.

[54] G. Araújo Pereira y M. de Sevilha Gosling, «LOS VIAJEROS Y SUS MOTIVACIONES Un estudio exploratorio sobre quienes aman viajar,» *Estudios y Perspectivas en Turismo,* vol. 26, nº 1, pp. 62-85, 2017.

[55] Armijos, Bustamante y C. Iñiguez, «Percepción del turista sobre el servicio de alimentos y bebidas. Sitio, Playa Bajoalto, Cantón El Guabo, El Oro, Ecuador,» *Revista Interamericana de Ambiente y Turismo,* vol. 15, nº 1, pp. 93-101, 2019.

[56] T. J. Loaiza, «Del ciclo de vida del producto al ciclo de vida del cliente: Una aproximación hacia una construcción teórica del ciclo de vida del cliente,,» *Investigación & Negocios,* vol. 11, nº 18, pp. 100-110, 2018.

[57] Kowszyk y Rajiv, «Estudios de caso sobre modelos de Economía Circular e integración de los Objetivos de Desarrollo Sostenible en estrategias empresariales en la UE y ALC,» *Perspectivas Económicas Birregionales*, pp. 162-175, 2018.

[58] J. C. (. I. J. o. G. a. F. S. D. e. h. c.-b. Arboleya, «Arboleya, J. C.,» *Board,* 2014.

[59] Reyes, Guerra y Quintero, «Educación en gastronomía: su vínculo con la identidad cultural y el turismo. El periplo sustentable,,» *Scielo.*, vol. 9, nº 32, 2017.

[60] Hernández; Tamayo; Castro; Iberoamérica, Muñoz, «Tendencias gastronómicas predominantes en la producción de revistas científicas de Iberoamérica,» *Científicas de Iberoamérica,* vol. 23, nº 1, pp. 76-84, 2016.

[61] P. L. G. Asencio, «El Turismo Gastronómico como generador de empleos en la

Comuna Libertador Bolívar, Cantón Santa Elena, provincia de Santa Elena, año 2016.,» 2017. [En línea]. Available: repositorio.upse.edu.ec/bitstream/46000/4121/1/UPSE-THT-2017-0002.pdf. [Último acceso: 20 11 2020].

[62] MINTUR, «Ministerio de Turismo del Ecuador. El Plan Nacional de turismo 2030,» 2019. [En línea]. Available: https://www.turismo.gob.ec/wpcontent/uploads/2020/03/PLAN-NACIONAL-DE-TURISMO-2030-v.-finalRegistro-Oficial-sumillado-comprimido_compressed.pdf.

[63] Reglamento Turístico de Alimentos y Bebidas, «Acuerdo Ministerial 53 Registro Oficial Edición Especial 575 de octubre 5 del 2018 Estado: Vigente,» 2018. [En línea]. Available: https://www.turismo.gob.ec/wpcontent/uploads/2018/11/Reglamento-de-alimentos-y-bebidas_OCTUBRE.pdf. [Último acceso: 26 11 2020].

[64] Sánchez y Ruano, «Diseño de Productos y servicios turísticos locales HOTI0108,» IC , 2018, pp. 46-48.

[65] Lemoine, Castellanos, Hernández, Zambrano y Carvajal, «Análisis de los atractivos y recursos turísticos del cantón San Vicente, Ecuador,,» *Retos de la dirección*, vol. 12, nº 2, pp. 133-148, 2018.

[66] R. Arnandis, «¿Qué es el desarrollo Turístico? Un análisis Delphi a la Academia Hispana,» *Cuadernos de Turismo*, nº 43, pp. 39-68, 2019.

[67] Fernández, Rodríguez, Pozo y Espinosa, «Estrategias para el fortalecimiento del Turismo Gastronómico en el Cantón Pastaza, Ecuador.,» *Amazónica Ciencia y Tecnología*, vol. 5, nº 2, pp. 118-136, 2016.

[68] L. Fernández Sánchez, Z. Rodríguez Cotilla, J. M. Pozo Rodríguez y J. M. Espinosa Manfugás, «Estrategias para el Fortalecimiento del Turismo

Gastronómico en el Cantón Pastaza, Ecuador,» *Revista Amazónica Ciencia y Tecnología,* vol. 5, nº 2, pp. 118-136, 2016.

[69] M. Carvache Franco, W. Carvache Franco y M. Torres Naranjo, «ANÁLISIS DE SATISFACCIÓN. La gastronomía de Samborondón - Ecuador,» *Estudios y Perspectivas en Turismo,* vol. 26, nº 3, pp. 731-745, 2017.

[70] M. A. Monroy Ceseña y F. J. Urcádiz Cázares, «Calidad en el servicio y su incidencia en la satisfacción del comensal en restaurantes de La Paz, México,» *Investigación administrativa,* vol. 48, nº 123, 2019.

[71] Hernández y Dancausa, «Turismo Gastronómico La gastronomía tradicional de Córdoba (España) Estudios y Perspectivas en Turismo,,» *Estudios y Perspectivas en Turismo,* vol. 27, nº 2, 2018.

[72] G. Mordecki y L. Ramírez, «¿Qué es lo primero: el crecimiento del PIB o la inversión? El caso de una economía pequeña y abierta,» *EL TRIMESTRE ECONÓMICO,* vol. LXXXV (1), nº 137, pp. 115-136, enero-marzo 2018.

[73] C. Iturralde Durán, «Los paradigmas del desarrollo y su evolución: Del enfoque económico al multidisciplinario,» *Revista de Ciencias de la Administración y Economía,* vol. 9, nº 17, pp. 7-23, 2019.

[74] J. Mejía, «CRECIMIENTO ECONÓMICO DE LARGO PLAZO EN ANTIOQUIA, COLOMBIA: ESTIMACIÓN DEL PIB, 1800-1913,» *Cuadernos de Economía,* vol. XXXIV, nº 66, pp. 507-544, 2015.

[75] L. L. Mora Pisco, N. P. M. Díaz Rodríguez y D. A. Vergara Cevallos, «El turismo en la matriz productiva de Ecuador: resultados y retos actuales.,» *Universidad y Sociedad,* vol. 10, nº 5, pp. 255-262, octubre-diciembre 2018.

[76] I. E. Orlandini González, P. L. Paco Janco y P. F. Torricos Ponce, «CRECIMIENTO ECONÓMICO Y LA INDUSTRIA HOTELERA UN ANÁLISIS EN DOS CIUDADES PATRIMONIALES DEL SUR DE BOLIVIA,» *Revista Investigación y Negocios,* vol. 12, nº 19, pp. 36-45, 2019.

[77] A. M. Castillo Canalejo y S. M. Sánchez Cañizares, «DESARROLLO

Actitudes de los residentes,» *Estudios y Perspectivas en Turismo,* vol. 26, nº 3, pp. 644-661, 2017.

[78] N. I. Santiago Chávez, A. J. Romero Fernández y G. A. Álvarez Gómez, «Actualidad y proyecciones de desarrollo del turismo internacional en Ecuador,» *UNIANDES EPISTEME: Revista de Ciencia, Tecnología e Innovación,* vol. 4, nº 3, julio-septiembre 2017.

[79] Naranjo, N. A y Leones, «La Gastronomía. Atractivo Turístico en Crecimiento en la ciudad de Colombia,» *Original,* vol. 24, nº 65, pp. 105-115, 2018.

[80] C. J. F. Romero, «La gastronomía como atractivo turístico primario en el centro histórico de Quito,» vol. 3, nº 11, pp. 194-203, 2018.

[81] T. E. Huertas López, E. A. Pilco Segovia, E. Suárez García, M. Salgado Cruz y B. Jiménez Valero, «Acercamiento conceptual acerca de las modalidades del turismo y sus nuevos enfoques.,» *Universidad y Sociedad,* vol. 12, nº 2, pp. 7081, 2020.

[82] O. Reyes Pérez, J. G. Rivera González y X. Castañeda Camacho, «Destinos turísticos potenciales en el litoral del Pacífico Sur Occidental Mexicano: un diseño construido desde abajo,» *El periplo sustentable,* nº 32, 2017.

[83] M. Á. Beltrán Bueno y M. C. Parra Meroño, «Perfiles turísticos en función de las motivaciones para viajar,» *Cuadernos de Turismo,* nº 39, pp. 41-65, enero-junio 2017.

[84] R. S. Acle Mena, J. Y. Santos Díaz y B. Herrera López, «La gastronomía tradicional como atractivo turístico de la ciudad de puebla, México,» *Rev.investig.desarro.innov.,* vol. 10, nº 2, pp. 237-248, 2020.

[85] G. A. Muñoz Fernández, C. P. Uribe Lotero, J. C. Pérez Gálvez y I. C. Ríos Rivera, «Festivales Gastronómicos y Turismo en Latinoamérica. El Festival Raíces de Guayaquil, Ecuador,» *Revista Rosa dos Ventos – Turismo e Hospitalidade,* vol. 9, nº 3, pp. 356-376, jul-sep 2017.

[86] L. I. Sosa Argaez y M. A. Silvestre Campos, «Evaluación de la calidad de los servicios turísticos gastronómicos en los establecimientos de alimentos y bebidas de comida tradicional regional Colimota en Manzanillo, Colima,» *El Periplo Sustentable,* nº 35, pp. 151 - 179, Julio / Diciembre 2018.

[87] F. Fusté Forné, F. X. Medina y L. Mundet i Cerdan, «La Proximidad de los Productos Alimentarios: Turismo Gastronómico y Mercados de Abastos en la Costa Daurada (Cataluña, España),» *Revista de Geografía Norte Grande*, vol. 76, pp. 213-231, 2020.

[88] M. d. C. Navarrete Torres y C. G. Muñoz Aparicio, «TURISMO GASTRONÓMICO: SABOR Y TRADICIÓN,» *Journal of Tourism and Heritage Research* , vol. 1, nº 3, pp. 23-40, 2018.

[89] F. Franco Jubete, «PATRIMONIO GASTRONÓMICO Y TURISMO,» *PITTM,* nº 89, pp. 303-309, 2018.

[90] J. Gabriel Ortega, «Cómo se genera una investigación científica que luego sea motivo de publicaciónº,» *J. Selva Andina Res. Soc.* , vol. 8, nº 2, 2017.

[91] E. L. Guelmes Valdés. y L. E. Nieto Almeida, «Algunas reflexiones sobre el enfoque mixto de la investigación pedagógica en el contexto cubano.,» *Revista Universidad y Sociedad* , vol. 7, nº 2, pp. 23-29, 2015.

[92] N. D. Piza Burgos, F. A. Amaiquema Marquez y G. Beltrán Baquerizo, «Métodos y técnicas en la investigación cualitativa. Algunas precisiones necesarias,» *Revista Conrado,* vol. 15, nº 70, pp. 455-459, 2019.

[93] C. Troncoso Pantoja y A. Amaya Placencia, «Entrevista: guía práctica para la recolección de datos cualitativos en investigación de salud,» *Rev. Fac. Med.* , vol. 65 , nº 2, pp. 329-332, 2017.

[94] C. Castro Rodríguez, I. González Roca, M. I. Marsinyach Ros, M. Sánchez Luna y M. I. Pescador Chamorro, «Encuesta de satisfacción sobre atención hospitalaria tras el nacimiento y seguimiento al alta del recién nacido sano,» *An Pediatr,* 2020.

[95] J. Arias Gómez, M. Á. Villasís Keever y M. G. Miranda Novales, «El protocolo de investigación III: la población de estudio,» *Revista Alergia México,* vol. 63, nº 2, pp. 201-206, abril-junio 2016.

[96] J. L. VENTURA LEÓN y M. BARBOZA PALOMINO, «El tamaño de la muestra: ¿Cuántos participantes son necesarios en estudios cualitativos?,» *Revista Cubana de Información en Ciencias de la Salud,* vol. 28, nº 3, 2017.

[97] C. de la Cuesta Benjumea, «LA CALIDAD DE LA INVESTIGACIÓN CUALITATIVA: DE EVALUARLA A LOGRARLA,» *Florianópolis,* vol. 24, nº 3, pp. 883-890, Jul-Sep 2015.

[98] P. Cadena Iñiguez, R. Rendón Medel, J. Aguilar Ávila, E. Salinas Cruz, F. d. R. de la Cruz Morales y D. M. Sangerman Jarquín, «Métodos cuantitativos, métodos cualitativos o su combinación en la investigación: un acercamiento en las ciencias sociales,» *Revista Mexicana de Ciencias Agrícolas,* vol. 8, nº 7, pp. 1603-1617, septiembre-noviembre 2017.

[99] J. Corona Lisboa, «Apuntes sobre métodos de investigación,» *Medisur,* vol. 14, nº 1, febrero 2016.

[100] P. Bedregal, C. Besoain, A. Reinoso y T. Zubarew, «La investigación cualitativa: un aporte para mejorar los servicios de salud,» *Rev Med Chile,* nº 145, pp. 373379, 2017.

[101] M. Hernán García, C. Lineros González y A. Ruiz Azarola, «Cómo adaptar una investigación cualitativa a contextos de confinamiento,» *Gac Sanit,* 2020.

[102] M. Madrazo Miranda, «Algunas consideraciones en torno al significado de la tradición.,» *Coatepec,* nº 9, pp. 115-132, 2005.

[103] C. Gutiérrez, «La cocina tradicional kumiai de ensenada, México: un análisis teórico sobre globalización y cultura alimentaria.,» *Multidisciplina,* nº 23, pp. 100-119, 2016.

[104] S. Oliveira, «La gastronomía como atractivo turístico primario de un destino. El Turismo Gastronómico en Mealhada-Portugal,,» *Estudios y Perspectivas en Turismo,,* vol. 20, nº 3, pp. 738-752, 2012.

[105] D. Navarro, «Recursos turísticos y atractivos turísticos: conceptualización, clasificación y valoración,» *Cuadernos de Turismo,,* nº 35, pp. 335-357, 2015.

[106] R. Boullón, «Planificación del espacio Turístico. 3ra.ed.,» México, Trillas, 2006.

[107] Espinoza, Martínez, Ortiz y Vizcarra, «Motives for food choice of consumers in Central México Br Food J,,» vol. 1, nº 18, pp. 2744-2760, 2016.

[108] P. C. Troncoso, «Nutrición,» *Educación,* vol. 2, nº 8, pp. 124-136, 2011.

[109] Lopez, Carabias y Díaz, «Ofertas gastronómicas,» Madrid, España, Paraninfo S.A., 2017, p. 124.

[110] Panosso y Lohman, «Epistemología del turismo. Teoría del Turismo: Conceptos, modelos y sistemas,» México , Trillas. , 2012 , pp. 27-28.

[111] S. Molina, «El marco del turismo: hacia una definición de turismo, turismo e industria turística,» *Annals of Tourism Research,,* pp. 390-407, 1994.

[112] Larousse, «Cocina criolla,» 2021. [En línea]. Available: https://laroussecocina.mx/palabra/cocina-criolla/.

[113] T. Castro y Marcano, «Ecoturismo y Geoturismo: alternativas estratégicas para la promoción del turismo ambiental sustentable venezolano,» *de Investigación,* vol. 40, nº 88, pp. 202-228, 2016.

[114] S. C. García, «Cocina casera,» 2006. [En línea]. Available: https://cocinacasera.com/cocina-criolla-que-es-y-platos/.

[115] MINTUR., «Mapa gastronómico del Ecuador,» 2018. [En línea]. Available: https://files.goraymi.com/2020/04/01/60d71579ff1651d857a1a6c8f25af41c.pdf.

[116] Ortiz y Peralta, «El Turismo de sol y playa: Impacto turístico en los ecosistemas de la comuna Ayangue, para mejorar la gestión de la actividad turística en la provincia de Santa Elena,» *Científica y Tecnológica*, vol. 6, nº 2, pp. 82-90, 2019.

[117] MINTUR, «Turismo ecuatoriano crecio un 11 por ciento en 2018,» 2018. [En línea]. Available: www.turismo.gob.ec:https://www.turismo.gob.ec/el-turismoecuatoriano-crecio-un-11-en-2018.

[118] Hernández, Di-Clemente y López, «El turismo gastronómico como experiencia cultural. El caso práctico de la ciudad de Cáceres (España),» *Boletín de la Asociación de Geógrafos Españoles,* nº 68, pp. 407-427, 2015.

[119] M. B. Gómez, «Retos del turismo español ante el cambio climático,» *Investigaciones Geográfica,* pp. 31-47, 2017.

[120] J. &. C.-B. R. Moya-Morillo, «Sistemas de detección de intrusos (IDS) basados en aprendizaje automático: Una revisión».

[121] D. A. a. E. L. C. Cecchini, "Desigualdad digital en América Latina y el Caribe: medición y políticas públicas,", Santiago, Chile, 2022.

[122] J. R. C. y. L. S. M. J. Robalino López, « "Blockchain: Ventajas, desventajas y aplicaciones en la cadena de suministro",» *Innovación y Desarrollo Tecnológico,* vol. 1, nº 2, pp. 73-85.

[123] «Innova Solutions,» 16 feb 2023. [En línea]. Available: https://inovasolutions.com.ec/datos-sensibles-educativos/.

[124] C. C. Ceballos, «"La educación en América Latina y el Caribe: un análisis desde la perspectiva de la desigualdad,",» CEPAL, Santiago, Chile, 2021.

[125] Sydle, «Sydle,» 28 Oct 2021. [En línea]. Available: https://www.sydle.com/es/blog/edge-computing-6255a8bb3bbdd676573d5af3.

[126] TELECOMUNICACIONES, «LEY DE COMERCIO ELECTRONICO, FIRMAS Y MENSAJES DE DATOS».