UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TÍTULO DEL TRABAJO DE TITULACIÓN

"Desarrollo de algoritmo para detección temprana de anomalías en tráfico URL, en redes distribuidas para la Facultad de Sistema y Telecomunicaciones (FACSISTEL) de la Universidad Estatal Península de Santa Elena"

AUTOR

SALINAS TOMALÁ ARMILDO SHRRIBER

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 2023

UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

Ing. José Sánchez Aquino. Mgt.
DIRECTOR DE LA CARRERA

Lsi. Daniel Quirumbay Yagual, Msia
TUTOR

Ing. Iván Coronel Suárez. Mgt.
DOCENTE ESPECIALISTA

Ing. Marjorie Coronel Suárez. Mgt.
DOCENTE GUÍA UIC

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 Armildo Shrriber Salinas Tomalá, como requerimiento para la obtención del título de Ingeniero en Tecnologías de la Información.

La Libertad, a los 2 días del mes de Agosto del año 2023

TUTOR

Firmado electrónicamente por:
DANIEL IVAN QUIRUMBAY YAGUAL

Lsi. Daniel Quirumbay, Msia

UPSE

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

Yo, **Armildo Shrriber Salinas Tomalá**

DECLARO QUE:

El trabajo de Titulación, **"Desarrollo de algoritmo para detección temprana de anomalías en tráfico URL, en redes distribuidas para la Facultad de Sistema y Telecomunicaciones (FACSISTEL) de la Universidad Estatal Península de Santa Elena",** 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, al 1 día del mes de Agosto del año 2023

EL AUTOR

Armildo Shrriber Salinas Tomalá

UPSE

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 **"Desarrollo de algoritmo para detección temprana de anomalías en tráfico URL, en redes distribuidas para la Facultad de Sistema y Telecomunicaciones (FACSISTEL) de la Universidad Estatal Península de Santa Elena",** presentado por el estudiante, Armildo Shrriber Salinas Tomalá fue enviado al Sistema Antiplagio, presentando un porcentaje de similitud correspondiente al 6%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.


CERTIFICADO DE ANÁLISIS
magister

Armildo_Salinas_Tomalá_Titulacion2023

6% Similitudes

2% Texto entre comillas
< 1% similitudes entre comillas
2% Idioma no reconocido

Nombre del documento: Armildo_Salinas_Tomalá_Titulacion2023.docx
ID del documento: 74f8aB10c0de49a28eab3392cfaa6be4a6fdb574
Tamaño del documento original: 13,58 MB

Depositante: DANIEL IVAN QUIRUMBAY YAGUAL
Fecha de depósito: 2/8/2023
Tipo de carga: interface
fecha de fin de análisis: 2/8/2023

Número de palabras: 29.038
Número de caracteres: 204.026

TUTOR

Firmado electrónicamente por:
DANIEL IVAN QUIRUMBAY YAGUAL

Lsi. Daniel Quirumbay, Msia

UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **Armildo Shrriber Salinas Tomalá**

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, al 1 día del mes de Agosto del año 2023

EL AUTOR

Armildo Shrriber Salinas Tomalá

AGRADECIMIENTO

Mi principal agradecimiento es a Dios, quien me ha guiado y motivado a seguir mis estudios. Agradezco a mis padres por el apoyo incondicional durante todo este proceso, como no olvidarme de mi querida Universidad por su gran formación hacia mi persona, a mis queridos docentes por sus grandes aportes que hoy se ven reflejados en la culminación de este proyecto.

Deceso que este momento perdure en el tiempo, en la mente de todas las personas que estudian a mi alrededor.

Armildo Shrriber Salinas Tomalá

DEDICATORIA

Dedico este trabajo principalmente a Dios, por haberme dado la vida, en especial al Msc.Daniel Quirumbay mi asesor de Tesis, por su calidad de Docente para guiarme y hacer todo lo necesario en el proceso de desarrollo.

Por el tiempo y el esfuerzo que dedico a compartir sus conocimientos.

Armildo Shrriber Salinas Tomalá

Contenido

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

RESUMEN

El presente trabajo consiste en el desarrollo de un algoritmo para la detección temprana de anomalías en el tráfico URL de redes distribuidas en la Facultad de Sistemas y Telecomunicaciones (FACSISTEL) de la Universidad Estatal Península de Santa Elena. El objetivo del mismo es crear un algoritmo en Python que detecte y notifique peticiones http o https que han sido categorizadas como maliciosas, agregando una capa adicional de protección a la red.

Para lograrlo se analiza distintas herramientas con el fin identificar las adecuadas para el desarrollo del algoritmo y la creación de una interfaz web con visualización gráfica de datos, que permita las notificaciones automáticas al administrador al detectar páginas web anómalas. En conclusión, el trabajo busca mejorar la seguridad de la red en la facultad mediante el algoritmo desarrollado, protegiéndola contra posibles amenazas y garantizar un ambiente más seguro para los usuarios y sistemas en la institución.

Palabras claves: Algoritmo, Python, Tráfico malicioso, Analisis de peticiones http y https.

ABSTRACT

The present work consists of the development of an algorithm for the early detection of anomalies in the URL traffic of distributed networks in the Faculty of Systems and Telecommunications (FACSISTEL) of the Peninsula Santa Elena State University. The objective is to create an algorithm in Python that detects and notifies http or https requests that have been categorized as malicious, adding an additional layer of protection to the network.

To achieve this, different tools are analyzed in order to identify the appropriate ones for the development of the algorithm and the creation of a web interface with graphical data visualization, which allows automatic notifications to the administrator when detecting anomalous web pages. In conclusion, the work seeks to improve the security of the faculty network through the developed algorithm, protecting it against possible threats and ensuring a safer environment for users and systems in the institution.

Keywords: Algorithm, Python, Malicious traffic, Analysis of http and https requests.

INTRODUCCIÓN

El presente proyecto realizado se ha denominado “Desarrollo de algoritmo para detección temprana de anomalías en tráfico URL, en redes distribuidas para la Facultad de Sistema y Telecomunicaciones (FACSISTEL) de la Universidad Estatal Península de Santa Elena”, el cual uno de sus principales propósitos es crear un script que alerte sobre el ingreso a sitios web maliciosos dentro de la institución.

Esta capturará los paquetes y extrae la IP pública, la cual será enviada a un servidor de análisis que dará como respuesta el detalle del mismo, lo cual luego se clasificará como anómalo o limpio basándonos en el resultado obtenido, de esta manera se propone brindar una capa más de seguridad a la red de la institución.

En el capítulo 1 se explica la problemática la cual abarca el proyecto, del mismo modo se detalla las herramientas y las metodologías a utilizar en el desarrollo del algoritmo, dando una breve descripción del contenido de las faces llevadas a cabo dentro de esta propuesta.

En el capítulo 2 se detalla el contexto de la institución en donde se realizará las respectivas pruebas del funcionamiento del algoritmo, los conceptos y las teorías empleadas en el proyecto. Se presentan las metodologías y lo que se realizó en cada una de las faces dentro de ellas con su respectiva evidencia. Por último, se indican los resultados de la ejecución del algoritmo dentro de la institución.

CAPÍTULO I

1. FUNDAMENTACIÓN

1.1. Antecedentes

La pandemia del COVID-19 ha dejado una serie de consecuencias en la sociedad, incluyendo un aumento en la ciberdelincuencia. La Organización Internacional de Policía Criminal (INTERPOL) sostiene que estos tipos de delitos han aumentado a medida que las empresas migraron al teletrabajo [1]. Mencionando que en el primer cuatrimestre (desde enero a abril) del 2020, el organismo detecto un total de 737 incidentes de tipo malware y 48 000 relacionadas con URL maliciosas [1]. Del 2020 al 2022, estos tipos de ataques en Latinoamérica experimento un aumento del 36% según lo informado por la empresa de seguridad Kaspersky, llegando a detectar un total de, 2366 ataques tipo malware por minuto [2]. En términos de clasificación a nivel mundial, Ecuador se encuentra en el puesto 29 [2].

La Universidad Estatal Península de Santa Elena, cuyo campus matriz está ubicada en La Libertad, provincia de Santa Elena fue fundada el 22 de julio de 1998. Sus autoridades principales son el Rector Académico y Vicerrector Académico [3]. Actualmente, dispone de seis facultades entre ellas la Facultad de Sistema y Telecomunicaciones (FACSISTEL) fundada en el 2010, la misma que oferta las carreras de Tecnología de la Información, Telecomunicaciones, Electrónica y Automatización. Contando con diez zonas entre las cuales se encuentran la sala de docentes, las oficinas administrativas, laboratorio de CISCO, laboratorios generales y departamento de TICs [3].

La Universidad cuenta con el departamento de Dirección de Tecnologías de la información y Comunicación, el cual se responsabiliza de la supervisión del uso de los ordenadores en los laboratorios de la facultad. Actualmente, se dispone de cuatro laboratorios para el empleo de actividades académicas por parte de los estudiantes, en los cuales no se lleva un control en tiempo real de las páginas visitadas por los mismos al realizar sus actividades, lo que aumenta la posibilidad de que accedan a sitios web maliciosos, poniendo en riesgo la seguridad de los sistemas informáticos (Ver Anexo 1).

En el caso de los estudiantes, a menudo se ven en la necesidad de visitar diferentes tipos de páginas en línea para obtener información relacionadas con sus actividades académicas, llegando incluso a crear cuentas con su información personal para poder tener acceso a este contenido. Sin embargo, muchas de estas páginas pueden contener malware, phishing, botnes, spyware, pharming, entre otros, lo que puede poner en riesgo la seguridad de los ordenadores. Incluso aquellas páginas que parecen inofensivas, como de adopción de mascotas o sitios de artículos, pueden estar diseñadas para robar información del usuario, lo cual puede ser utilizado para llevar a cabo estafas o incluso robo de identidad.

Al no llevar un control de las páginas visitadas en la jornada académica, no se pueden detectar inmediatamente situaciones al acceso a páginas web con contenido malicioso, lo que causa un retraso en la movilización del personal pertinente para mitigar el incidente. Resultando en inconvenientes que interfieran con las actividades planificadas dentro de la institución.

En la Universidad Jaume I en España de la ciudad de Castellón de la Plana, en el año 2015, se propuso el tema "Redes neuronales. Un modelo de clasificación para la detección de dominios DNS malicioso" [4]. Este proyecto analiza el tráfico DNS de un sistema pasándolos por un validador de dominio y clasificándolo por medios de una red neuronal según corresponda. Sin embargo, este proyecto se centra en el análisis y clasificación de páginas, más no en un sistema de monitoreo y alerta en tiempo real.

El estudio realizado en la universidad Nacional de Colombia de la ciudad de Bogotá en el 2021, con el tema de "Detección de URLs maliciosas por medio de técnicas de aprendizaje autónomas" [5]. El proyecto presenta un sistema de detección y clasificación de URL mediante el uso de criterio léxico y ofuscación URL, empleando técnicas de aprendizaje autónomo. Sin embargo, este no presenta una forma de avisar al administrador cuando se ha detectado un enlace malicioso.

En Ecuador, en la Escuela Superior Politécnica del Litoral ubicada en la ciudad de Guayaquil en el año 2016, Se propuso el tema "Implementación de una plataforma de detección de accesos a sitios maliciosos" [6]. El proyecto implementa una plataforma en donde por medio de SPLUNK se detecta automáticamente el acceso

a sitios web maliciosos y se emite una alerta vía email al administrador, pero este proyecto utiliza una detección basada en un único listado previamente selecciona y no permite una detección más detallada.

Este algoritmo de control de peticiones HTTP y HTTPS se aplicará a la Facultad de Sistemas y Telecomunicaciones (FACSISTEL) de la Universidad Estatal Península de Santa Elena (UPSE), permitiendo el monitoreo constante de las páginas visitadas por los usuarios y detectar aquellas que presentan algún tipo de riesgo o amenaza para la seguridad de la red, por medio del método de análisis de reputación de página. La implementación del algoritmo contribuirá a la prevención de posibles incidentes y la protección de la información de los usuarios dentro de la red. Además, la propuesta dará la posibilidad de generar documentos estadísticos para el análisis y mejora del sistema de seguridad de la red institucional.

1.2. Descripción

La Facultad de Sistemas y Telecomunicaciones (FACSISTEL) cuenta con una gran cantidad de personas en el campus, tanto estudiantes como personal administrativo, que realizan actividades diarias, muchas de las cuales involucran la navegación en internet, visitando diferentes páginas web con el fin de encontrar información específica. Sin embargo, al buscar la información en la web, existe la posibilidad de ingresar en páginas que presenten contenido anómalo o malicioso, lo que puede ocasionar la infección del ordenador o el robo de información del usuario. Esta problemática puede generar inconvenientes en el funcionamiento del equipo y en la privacidad de información del usuario.

Por esta razón, se propone desarrollar un algoritmo que nos permita identificar solicitudes http y https que presenten contenido malicioso o anómalo, con el objetivo de alertar a los administradores de la red y mitigar los riesgos potenciales para la seguridad de la información y el funcionamiento de los equipos.

Para el desarrollo del algoritmo se seguirá los siguientes puntos de la metodología OMSTD [7]:

Organización y Estructura (ST)

1. Estructura básica de la organización de archivos

- Se crearán archivos y carpetas específicos para cara parte del proyecto, siguiendo la organización básica que nos presenta la metodología.

Entrada y Salida de información

1. Se establecerá cuáles son los datos entrantes en el algoritmo y su respectiva estructura
2. Se establecerá cuál es la información saliente del algoritmo y su respectiva estructura.

Retribuciones

1. Desarrollo del algoritmo.
    - Análisis las herramientas necesarias para el desarrollo del algoritmo.
    - Se genera el script de captura de paquetes.
    - Se genera el script de análisis IP con el servidor de APIVOID.
    - Se genera el script de registro de paquetes en la base de datos.
    - Se genera el script de consulta con la base de datos.
    - Se genera el script de envío de notificaciones al grupo de Telegram.

Despliegue

1. Realizar pruebas
    - Análisis tráfico mediante el algoritmo.

Se desarrolla un dashboard que nos permita interactuar con el algoritmo, siguiendo los puntos propuestos en el artículo "Claves para diseñar un dashboard de tu estrategia digital" [8]:

Planificación

1. Planificación de contenido
    - Determinar los usuarios de dashboard.
    - Analizar las herramientas necesarias para el desarrollo del dashboard.
    - Determinar la base de datos con a que estará conectada.

- Determinar el procedimiento de recolección de datos.

Creación de borrador.

1. Diseño del esquema web de dashboard.
2. Diseño del Wireframes del dashboard.
3. Diseño del formato de la alerta enviada por Telegram.
4. Análisis de los colores a implementar en el dashboard.
5. Diseño de diagrama del proceso de captura y clasificación de paquetes.

Diseño

1. Diseño y creación de base de datos.
2. Diseño y creación de dashboard.

Feedback y aplicación de cambios

1. Presentación del dashboard y verificación del mismo.

Para realizar el estudio dentro de la institución se usa la metodología ISO/IEC 27032 [7], constando con las siguientes fases:

Fase de Entendimiento de la organización

1. Realizar un estudio de observación
    - Estudiar la organización en donde se llevará a cabo el proyecto
    - Identificar el tipo de página más visitada por estudiantes al buscar información.

Fase de Análisis de Riesgo

1. Identificar Activos
    - Identificar los diferentes activos de la institución relacionados con el tema planteado
2. Identificar Amenazas
    - Identificar los diferentes riesgos a la que se exponen los usuarios al momento de visitar páginas web y métodos de acceso a las mismas.
3. Determinar Impacto y riesgo
    - Identificar el impacto y ocurrencia de los riesgos hallados.

Fase de Plan de Acción

1. Políticas
    - Proponer políticas que ayuden a la mitigación de los riesgos encontrados.
2. Identificar de roles
    - Identificar los encargados de implementar y gestionar las medidas de seguridad planteadas.
3. Métodos de implementación
    - Proponer diversos procesas a implementar al momento de suscitarse algunos de los riesgos hallados.
4. Procesos Afectados
    - Identificar los procesos de la organización que se verán afectados por las acciones tomadas ante los riesgos.
5. Controles tecnológicos
    - Desarrollar el algoritmo de análisis de peticiones http y https aplicando la metodología OMSTD.

Fase de Implementación

2. Existencia de Política de Seguridad
3. Planes de concienciación del personal
4. Monitorización TIC
5. Gestión de incidentes

1.2.1 Herramientas

En la elaboración de este proyecto se usará el lenguaje de programación Python junto con las siguientes herramientas que nos ayudaran en la elaboración del dashboard:

Visual Studio Code: Es un editor de código fuente ligero disponible para Windows, macOS y Linux. Viene con soporte integrado para JavaScript, TypeScript y Node.js y tiene un rico ecosistema de extensiones para otros lenguajes y tiempos de ejecución (como C++, C#, Java, Python, PHP, Go, .NET). Comience su viaje con VS Code con estos videos introductorios [9].

Flask: Micro Framework escrito en Python, facilita el desarrollo de Aplicaciones Web bajo el patrón MVC (forma de trabajar que permite diferenciar y separar lo que es el modelo de datos, la vista y el controlador) [10] [11].

Apivoid: Se utilizan para el análisis de amenazas web, la detección y la prevención de amenazas, lo que reduce y automatiza el trabajo manual de los analistas de seguridad, mediante esta API se escanea la URL y la compara en diferentes listas negras [12].

Telegram Bot API: Es una interfaz basada en HTTP creada para desarrollar bots para Telegram [13].

Xampp: Es una distribución de Apache completamente gratuita y fácil que contiene MariaDB, PHP y Perl. Diseñado para ser increíblemente fácil de instalar y usar [14].

Balsamiq Wireframes: Es una herramienta rápida de creación de tramas de interfaz de usuario de baja fidelidad que reproduce la experiencia de dibujar en un blogblo de notas o pizarra, pero usando una computadora [15].

phpMyAdmin: Es una herramienta gratuita escrita en PHP para la administración Web de MySQL. phpMyAdmin admite varias operaciones en MySQL y MariaDB. Las operaciones de uso frecuente (administración de bases de datos, tablas, columnas, relaciones, índices, usuarios, permisos, etc.) se pueden realizar a través de la interfaz de usuario, mientras aún tiene la capacidad de ejecutar directamente cualquier instrucción SQL [16].

MySQL: Es un sistema gestor de bases de datos relacionales, poderoso y versátil que puede manejar la mayoría de los proyectos en la web [17].

De la misma manera, para el desarrollo del algoritmo y su implementación con el dashboard se utilizarán las siguientes librerías de Python.

Pyshark: Envoltura de Python para Tshark, que permite el análisis de paquetes de Python mediante disectores Wireshark [18].

Scapy: Es una biblioteca de manipulación de paquetes, capas de capturar y decomisarlos [19].

Pandas: Es una herramienta de análisis y manipulación de datos, potente, flexible y fácil de usar [20].

Request: Es una librería para HTTP, que ofrece la mayoría de funcionalidades necesarias para este [21].

Matplotlib: Librería para la creación de estadísticas animadas e interactivas [22].

Chart.js: Es una librería de diferentes tipos de gráficos, complementos y opciones de personalización [23].

Email-validator: Librería de validación de capacidad de entrega y sintaxis de correos electrónicos [24].

ReportLab: Herramienta comercial insignia para crear archivos PDF rápidamente utilizando Report Markup Language y un preprocesador. Genere archivos PDF de la misma manera que crea páginas web dinámicas [25].

XlsxWriter: Liberia que nos permite escribir texto, fórmulas e hipervínculo en varias hojas en formato xlsx [26].

Flask-skectio: Brinda a las aplicaciones Flask acceso a comunicaciones bidireccionales de baja latencia entre los clientes y el servidor. La aplicación del lado del cliente puede utilizar cualquiera de las bibliotecas de cliente de SocketIO en Javascript, Python, C++, Java y Swift, o cualquier otro cliente compatible para establecer una conexión permanente con el servidor [27].

SQLAchemy: Es un mapeador/herramienta de mapeo relacional de objeto, u ORM. Una biblioteca que los desarrolladores utilizan para generar bases de datos y manipular sus datos sin la necesidad de saber/usar SQL [28].

Sqlclient: Implementa clases abstractas para clientes de servicios similares a SQL. Una subclase concreta utilizaría un paquete de cliente compatible con DB-API para el servicio y, en su mayoría, necesita averiguar cómo establecer una conexión con el servidor [29].

Pymysql: Este paquete contiene una biblioteca de cliente MySQL de Python puro, basada en PEP 249 [30].

Este proyecto contribuirá a la línea de investigación de Tecnología y Sistemas de la Información (TSI) con la sub – línea de redes y seguridad de la información, debido

a que el presente proyecto se relaciona con temas de seguridad de las Tecnologías de la información (TI), virtualización y seguridad de la infraestructura de la información que permita generar información indispensable para la toma de decisiones [31].

1.3. Objetivos

1.3.1. Objetivo General

Desarrollar un algoritmo que permita la detección de anomalías en tráfico URL basado en código Python para agregar una capa más de protección a la red en la Facultad de Sistemas y Telecomunicaciones.

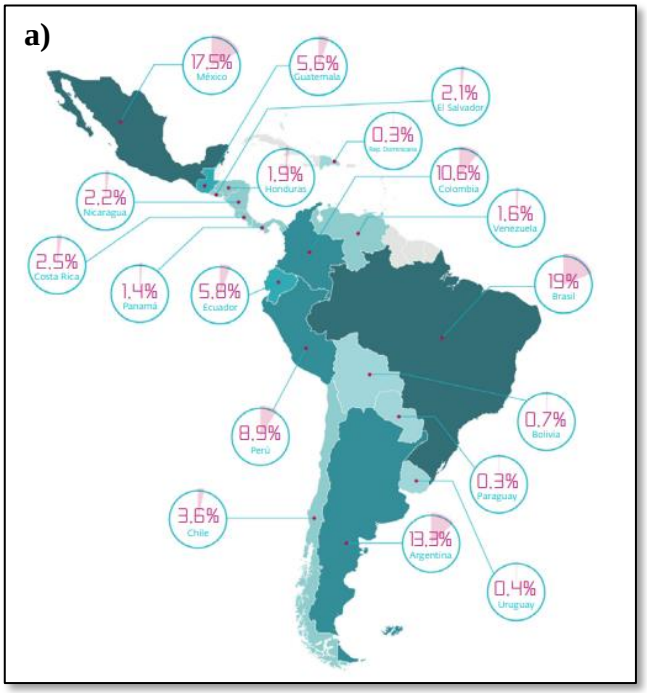
1.3.2. Objetivos Específicos

- Analizar el tráfico URL en peticiones http y https para detección de anomalías en los sitios web.
- Identificar las herramientas para el desarrollo del algoritmo utilizado en el análisis de la reputación de una página web.
- Desarrollar una interfaz web con capacidad de visualización gráfica de datos provenientes del análisis de páginas web y detección de páginas anómalas con notificaciones automáticas al administrador.

1.4. Justificación

El internet es una herramienta fundamental en la ejecución de actividades tanto personales como empresariales, tan solo en un día se llegan a conectar 5 mil millones de usuarios a este medio [32]. Al navegar en este entorno los usuarios se ven susceptible a ser víctima de ataques digitales, lo que conllevaría a robo de información o infección del equipo, tomando esto en cuenta resulta beneficioso tener un sistema que nos permita monitorear y detectar estos incidentes, brindando una capa más de seguridad a la red [33].

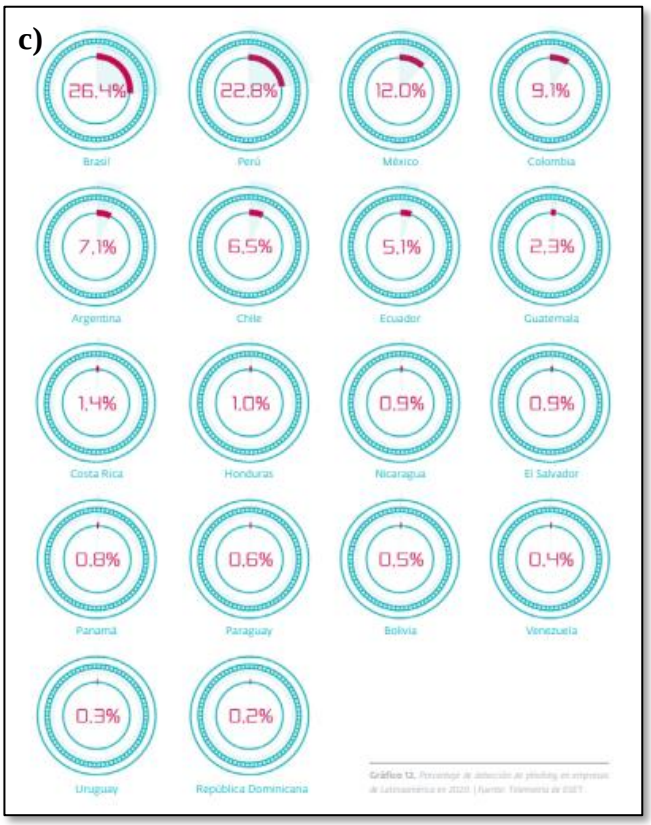
En el 2021 ESET realizo una encuesta en donde se determinó que a nivel Latinoamérica Ecuador ocupa el quinto puesto en infecciones de tipo malware con 5,8% y el séptimo puesto en ataques relacionados a ingeniería social con 5,1%, todo esto ligado a temas relevantes a la fecha como lo es la pandemia del COVID-19 [34].



b) Infección de Malware por país

1. 19% Brasil
2. 17.5% México
3. 13.3% Argentina
4. 10.6% Colombia
5. 8.9% Perú
6. 5.8% Ecuador
7. 5.6% Guatemala
8. 3.6% Chile
9. 2.5% Costar rica
10. 2.2% Nicaragua
11. 2.1% El Salvador
12. 1.9% Honduras
13. 1.6% Venezuela
14. 1.4% Panamá
15. 0.7% Bolivia
16. 0.4% Uruguay
17. 0.3% Rep. Dominicana
18. 0.3% Paraguay

Fig. 1. Infección de Malware por país (a) (b) *[34]*



d) Ingeniería Social por país

1. 26.4% Brasil
2. 22.8% Perú
3. 12.0% México
4. 9.1% Colombia
5. 7.1% Argentina
6. 6.5% Chile
7. 5.1% Ecuador
8. 2.3% Guatemala
9. 1.4% Costar rica
10. 1.0% Honduras
11. 0.9% Nicaragua
12. 0.9% El Salvador
13. 0.8% Panamá
14. 0.6% Paraguay
15. 0.5% Bolivia
16. 1.4% Venezuela
17. 0.3 Uruguay
18. 0.2% Rep. Dominicana

Fig. 2.Ataques de Ingeniería social por país (c) (d) *[34]*

En la actualidad, el control de la red en la Facultad de Sistemas y Telecomunicaciones (FACSISTEL) se efectúa mediante un firewall físico que permite filtrar las páginas que pueden ser visitadas dentro de la institución. Sin embargo, el método utilizado para este sistema se basa en permitir o denegar el acceso a una página y no ofrece un análisis más detallado de la misma o el motivo por el cual fue restringido su acceso. Por lo tanto, se requiere de una solución más sofisticada que permita monitorear y analizar la reputación de las páginas web visitadas en tiempo real.

En este proyecto se propone desarrollar un algoritmo que permita a los administradores de la red de FACSISTEL ejecutar un análisis de reputación de cada página web visitada dentro de la institución, con el fin de brindar una capa más de seguridad a la infraestructura de la Facultad. Se usa el servicio APIVOID para el análisis de peticiones https, el cual cuenta con una base de datos de reputación de páginas. De esta manera, se podrá determinar si una página es segura, si esta contiene malware o alguna clase de contenido malicioso, y posteriormente enviar notificaciones al administrador a través del servicio de mensajería de Telegram en caso de detectar alguna anomalía.

Es importante destacar que la implementación de este algoritmo permitirá mejorar la seguridad de la información en la Facultad de Sistemas y Telecomunicaciones (FACSISTEL), reduciendo los riesgos de infección de equipos y robo de información, y proporcionando una mayor tranquilidad a los usuarios que hacen uso de la red. Además, esta solución se adapta a las necesidades específicas de la institución y puede ser fácilmente implementada en otras instituciones que buscan mejorar la seguridad de su infraestructura de red.

El presente proyecto está direccionado al Plan de Creación de Oportunidades, el cual se describe a continuación:

Objetivo del Eje Social

Objetivo 5.- Proteger a las familias, garantizar sus derechos y servicios, erradicar la pobreza y promover la inclusión social [35].

Política 5.5.- Mejorara la conectividad digital y el acceso a nuevas tecnologías de la población [35].

Pol. 5.4

A5.- Fortalecer la conectividad y acceso a las TIC como vía para mejorar el acceso a otros servicios [35].

1.5. Alcance

El proyecto se basa en el desarrollo de un algoritmo de capturar de tráfico HTTP y HTTPS para la Faculta de sistemas y Telecomunicaciones (FACSISTEL) de la Universidad Estatal Península de Santa Elena (UPSE). Este permitirá detectar el acceso a páginas webs con contenido maliciosas dentro de la red monitoreada. El algoritmo implementará un sistema que verificará si la página web ingresada presenta contenido anómalo, utilizando el método de comprobación de listas negras como Blacklist Dominios, Blacklist Páginas, Blacklist TLD, más Abusados, Categorías, entre otros.

Cabe destacar que el proyecto está enfocado especialmente en la detección de páginas webs maliciosas mediante el análisis de tráfico http en los dispositivos dentro de la red. No abarcará otros aspectos de seguridad de la red como la implementación de medidas de mitigación de ataques cibernéticos. El objetivo principal es proporcionar una herramienta eficaz de detección y alerta de este tipo de riesgo a través del algoritmo desarrollado.

A continuación, se explicará el alcance de cada metodología aplicada al proyecto:

Metodología OMSTD

Organización y Estructura (ST)

En esta etapa se establecerá una estructura para ordenar y clasificar los diferentes archivos con código, asi como aquellas carpetas que contendrán imágenes o iconos.

Entrada y Salida de información (IO)

Se considera cuál es la información qué introduciremos en el algoritmo y cuál es aquella que queremos como resultado. Así mismo el tipo de documentación que obtendremos de cada análisis.

Redistribución

Se elabora los respectivos scripts que conforman arquitectura del algoritmo. Esto incluye el código necesario para la captura de paquetes, clasificación de paquetes, envió de peticiones de análisis a apivoid y alertas a Telegram.

Despliegue

Se pone a prueba el algoritmo en un entorno controlado para verificar su funcionamiento al capturar y analizar los paquetes web, asi mismo se comprobará el envío de notificaciones a Telegram. Revisando que los diferentes scripts puedan comunicarse entre sí y funcionen de manera correcta.

Desarrollo de Dashboard

Planificación

En esta etapa se asientan las bases para el desarrollo de dashboard, se identificará el tipo del usuario al cual va a estar dirigida la herramienta, los tipos de datos que se mostraran, así como la base de datos a utilizar para realizar el almacenamiento, por último, se establecerá los tipos de datos que se recolectaran y se diseñara el diagrama de proceso de la captura y clasificación de paquete.

Creación de borrador

Se desarrolla los diferentes borradores para el diseño del dashboard, como el respectivo esquema web de las diferentes páginas que conforma el entorno, se diseña el respectivo wireframe para las secciones más importantes, el formato de la notificación a enviar por Telegram y la respectiva paleta de colores que tendrá el dashboard.

Diseño

Se diseña la respectiva base de datos en donde se almacena la información proveniente de escaneo y análisis de paquetes, de la misma manera se elabora el

respectivo dashboard siguiendo los modelos y paleta de colores establecidos en la etapa anterior.

Freedback y aplicación de cambios

En esta etapa se pone a prueba el entorno desarrollado para verificar su funcionamiento, se iniciará la ejecución del algoritmo de manera gráfica, así como su finalización, por último, se comprobará como presenta la información recolectada en gráficas, así como el envío correcto de notificaciones a Telegram.

ISO/IEC 27032

Fase de Entendimiento de la Organización

En esta fase se estudiará la organización en la cual se llevará a cabo el proyecto. Se observa que tanto control tiene el área administrativa referente a las páginas visitadas por los usuarios, así como los horarios con más tráfico en la red dentro del periodo laboral. Todo esto por medio de un estudio de observación.

Fase de Análisis de Riesgo

La fase permitirá reconocer amenazas existentes dentro de la facultad, relacionadas con la navegación por internet, se identificará el tipo de amenaza y como se lleva a cabo los mismos. De la misma manera, reconocerá las vulnerabilidades que puede presentar un usuario al momento de visitar páginas con contenido malicioso que no fueron detectadas por las herramientas convencionales.

Fase de Plan de Acción

En esta fase se determinará cuál será el lenguaje base para desarrollar el algoritmo, las herramientas adicionales a implementar como framework, APIs y librerías para el desarrollo del mismo, se modelará la forma de dashboard como su funcionalidad, los colores que se usaran como las ventanas o secciones que este tendrá, así como su forma de desenvolverse con las actividades plateadas.

Fase de implementación

Se implantarán las herramientas antes mencionadas para el desarrollo de un algoritmo que permita el monitoreo de la red en la facultad, para posteriormente

analizar las peticiones HTTP y HTTPS, para detectar anomalías en las páginas web visitadas, con esto se va a tener alertas en tiempo real si se detecta la navegación en alguna página web con contenido malicioso.

El análisis de las peticiones HTTPS solo se realizará al protocolo IPv4, este estará orientado a la navegación que realiza los usuarios más no a la comunicación que puede haber entre los equipos. Las debidas notificaciones serán enviadas a través de la plataforma Telegram las cuales no se repetirán en el trascurso del día.

1.6. Metodología

1.6.1. Metodología de Investigación

Se utiliza la metodología de investigación de tipo exploratoria [36] para realizar la búsqueda de información y proyectos que tengan similitud o relación con él con el control y monitoreo de la red, con respecto a peticiones HTTPS para la identificación de anomalías dentro de páginas web, con el fin de comparar métodos y herramientas que permita realizar este tipo de análisis.

La investigación diagnostica [37] se actúa a través de un estudio de observación dentro de la Facultad de Sistemas y Telecomunicaciones, para identificar los factores que intervienen dentro de ella, la o las variables a medir, conociendo la situación en tiempo real del control y monitoreo del tráfico de red con respecto a peticiones web.

1.6.2. Beneficiarios del Proyecto

Los beneficiarios de este proyecto de investigación son el personal administrativo de la Facultad de Sistema y Telecomunicaciones (FACSISTEL) de la Universidad Estatal Península de Santa Elena. El desarrollo del algoritmo les brindará herramientas para analizar y monitorear el tráfico de red de la facultad, detectando sitios web maliciosos o anómalos. Permitiendo al personal administrativo tomar decisiones fundamentadas en la protección y fortalecimiento de la seguridad informática de la institución.

Los beneficiarios indirectos de la investigación son los estudiantes de FACSISTEL. La implementación de este algoritmo garantizará una mayor seguridad informática, protegiéndolos de posibles amenazas y ataques en entornos digitales. Como

resultado, los estudiantes podrán realizar sus actividades académicas sin interrupciones ni riesgo a la integridad de su información, lo que contribuirá a crear un ambiente propicio para su desarrollo educativo y éxito académico.

1.6.3. Variable

La presente investigación tiene como objetivo analizar el impacto de la implementación de un algoritmo en la detección de sitios web maliciosos. Específicamente, se busca evaluar la cantidad de paquetes web maliciosos detectados antes y después de la aplicación del algoritmo.

1.6.4. Técnicas de recolección de información

En el proceso de recolección de información para la investigación, se utilizaron diferentes técnicas e instrumentos con el objetivo de obtener los datos necesarios para alcanzar los objetivos establecidos. Entre las técnicas empleadas se encuentran la observación y la recopilación documental.

1.6.5. Análisis de recolección de información

En el caso específico de la Facultad de Sistemas y Telecomunicaciones (FACSISTEL) de la Universidad Estatal Península de Santa Elena, se empleó el método de observación para recopilar información sobre el uso de los ordenadores en la institución, tal como se detalla en el Anexo 1. Durante la observación, se pudo determinar que los laboratorios 1, 2 y 3 cuentan en total con 52 ordenadores destinados a ser utilizados por la comunidad estudiantil. Estos ordenadores son utilizados principalmente para realizar actividades de investigación y desarrollo.

En cuanto al acceso a páginas web, se observó que los estudiantes visitan con mayor frecuencia las páginas relacionadas con la institución, como la página web de la universidad, el ambiente virtual de aprendizaje y el sistema de gestión académica (SGA UPSE). Sin embargo, al realizar actividades como talleres o tareas, los estudiantes tienden a visitar blogs y páginas no oficiales. En términos de horarios, se pudo constatar que los períodos de mayor uso de los ordenadores son aproximadamente de 9 a 10 am y de 3 a 4 pm, dependiendo de las actividades académicas programadas.

En el Anexo 2 se presenta un estudio más enfocado en la infraestructura de los laboratorios de la facultad. Se identificó que los laboratorios 2 y 3 cuentan con un total de 44 ordenadores, es decir, 22 máquinas en cada uno, mientras que el laboratorio 1 dispone actualmente de 8 ordenadores, la misma cantidad que el laboratorio 6. Estos ordenadores están equipados con procesadores como el AMD Ryzen 7 2700 Eing-Core Processor 3.20 GHz y el Intel Core i5-4460 CPU 3.20 GHz.

En cuanto a la memoria RAM, se encontró que varía de 4GB a 8GB en las diferentes máquinas. Algunas de ellas cuentan con tarjetas gráficas integradas Intel HD Graphics 4600, mientras que otras tienen tarjetas NVIDIA GeForce GT 710. Todos los ordenadores cuentan con 17 puertos, incluyendo puertos USB 2.0 y 3.0, puertos DVI Video, VGA, PS/2, Minijack y puertos LAN con conectores RJ45.

Se observó que todos los ordenadores funcionan con sistemas operativos Windows 10 de 64 bits, y cuentan con programas académicos como "Paker Teacer" y "Visual Studio Code", entre otros. Los navegadores de preferencia son Google Chrome y Mozilla Firefox. Además, se realizaron pruebas de velocidad tanto por Wi-Fi como por conexión Ethernet, concluyendo que la conexión por cable Ethernet es más rápida, con un promedio de descarga de 92.35 Mbps y un promedio de carga de 94.25 Mbps, en comparación con la conexión Wi-Fi, que presenta un promedio de descarga de 14.2 Mbps y un promedio de carga de 14.4 Mbps.

Mencionando la infraestructura de la red, se logra observar que los ordenadores en el laboratorio 3 están conectados a un switch que está ubicado dentro del mismo, los ordenadores de los laboratorios 1 y 2 están conectados a switch que se encuentran en el área administrativa, de los cuales se conectan al departamento de tics en donde se relacionan con los servidores, servicio Fortinet para posterior tener salida a internet.

Por medio de la recopilación documental se revisó diversas investigaciones, tesis y artículos relacionadas con el tema planteado, tanto para recopilar datos que sirvan para el desarrollo del algoritmo como aquellos que aportan en un mejor entendimiento de la institución.

1.7. Metodología de desarrollo

1.7.1. Metodología OMSTD

Para el desarrollo del algoritmo se utilizará la metodología OMSTD (Open Methodology for Segrutity Tool Developers), el cual es una metodología de buenas prácticas en Python para el desarrollo de herramientas de seguridad [38], el cual nos menciona los siguientes subtemas para la elaboración de scripts:

Organización y Estructura (ST)

Se emplea una serie de normas para definir la estructura que va a tener el código, se establece secciones para cada tipo de funciones y parámetros. Se define una estructura de carpeta que contendrán parte o documentos específicos del algoritmo.

Entrada y Salida de información (IO)

Se determinará cuál será el funcionamiento del script, qué datos obtendrá y de qué manera lo hará. De la misma manera, la información que este le brindara al usuario por medio de reportes y gráficas mostrada en el dashboard.

Redistribución

Se realizará varios scripts para cada una de las partes, para posteriormente unificarlos en el dashboard, teniendo en cuenta su compatibilidad con el sistema operativo y la infraestructura de TI.

Despliegue

Se pondrá en funcionamiento la aplicación, dentro de un entorno controlado en la empresa, ejecutando las debidas pruebas y analizando los resultados.

Fig. 3. Metodología OMSTD para desarrollo de algoritmo *[7]*

1.7.2 Dashboard

Para permitir la interacción del algoritmo con el usuario, se plantea la elaboración de un dashboard, Según Sergio Gómez Rivera, en su artículo "Claves para diseñar un dashboard de tu estrategia digital", esta nos menciona cuatro puntos importantes a seguir para poder diseñar correctamente un dashboard [8], los cuales mencionaremos a continuación:

- **Planificación:** Para poder diseñar de manera correcta un dashboard, se empieza por asentar una base firme, para hacer esto se debe contestar una seria de preguntas [8]:
    - ¿Para quién está dirigido el dashboard?
    - ¿Cuáles son las herramientas que usaran para la creación?
    - ¿Qué tipo de dato quiere incluir y con qué fuente de datos se cuenta?
    - ¿Qué personas estarán involucradas?
    - ¿Cómo se recolectan los datos?
- **Creación de borrador:** Antes de iniciar con el desarrollo del mismo hay que pensar en el formato que tendrá el dashboard, para esto podemos considerar los siguientes puntos [8]:
    - El número de páginas requeridas y cómo va a subdividirse la información.
    - El tipo de componentes (gráficos, tablas, mapas…), que se van a emplear.
    - Los indicadores o iconos que se utilizara para guiar a los usuarios hacia la información en el dashboard.
    - La paleta de colores.
    - Posibles animaciones.
- **Diseño:** En esta fase intervienen las herramientas elegidas para el desarrollo y el borrador realizado con anterioridad, El proceso involucra la introducción de datos y su conversión en información gráfica [8].
- **Freedback y aplicación de cambios:** El objetivo de este punto es poner en fase de prueba al dashboard, para poder detectar fallos en sus procesos y poder corregirlos [8].

1.7.3. Metodología ISO/IEC 27032

Para el presente proyecto se implementará la metodología ISO/IEC 27032, la cual tiene como objetivo la protección de la infraestructura crítica de la información [39]. Enfocada en áreas como prevención, protección y detección, respuesta y comunicación, recuperación y aprendizaje [40]. Esta metodología se basa en los estándares de seguridad de la información de la norma ISO/IEC 27001

La metodología ISO/IEC 27032 siguiente cuatro fases:

Fase 1 Entendimiento de la Organización. – Se recopilará información dentro de la Facultad por medio de un estudio de observación, sobre los sistemas implementados, los ordenadores disponibles para el uso de estudiantes y los horarios que generan más tráfico en la red.

Fase 2 Análisis de Riesgo. – Se identificará las amenazas a las que se exponen los usuarios al visitar sitios web y como se ejecutan las mismas. Se analiza que tan susceptible es la Institución a que ocurra estos incidentes.

Fase 3 Plan de Acción. – Se estudiará e identificará las herramientas a utilizar para el desarrollo del algoritmo, los métodos para la detección y análisis de URL, el método de comunicación con el administrador, se diseñará el dashboard mediante la planificación, creación de borrador, Diseño, Freedback y aplicación de cambios, a su vez se aplicará la metodología OSMTD para el desarrollo del algoritmo.

Fase 4 Implementación. - Se procederá a ejecutar el algoritmo dentro del dashboard para realizar un monitoreo en la red, analizando las páginas URL visitadas por los usuarios conectados y notificando al personal administrativo sobre él ingresa a sitios que presenten anomalías.

Fig. 4. Metodología ISO/IEC 27032 *[40]*

CAPÍTULO II.

2. PROPUESTA

2.1. Marco Contextual

Universidad Estatal Península de Santa Elena

La Universidad Estatal Península de Santa Elena (UPSE), ubicada en la provincia de Santa Elena en el Ecuador, es una institución educativa con amplia trayectoria en la formación de profesionales en diversas áreas del conocimiento. La UPSE fue creada el 02 julio de 1998 mediante la Ley N° 110, y publicada en el suplemento del Registro Oficial N° 366 de 22 de julio de 1998. Su sede se encuentra en la avenida principal de La Libertad-Santa Elena, en el cantón La Libertad. La universidad cuenta con una infraestructura moderna y tecnológica que permite a sus estudiantes y docentes desarrollar sus actividades académicas de manera eficiente y efectiva [41].

Misión

Formas profesionales que aportan al desarrollo sostenible, contribuye a la solución de los problemas de la comunidad y promueve la cultura [42].

Visión

Ser reconocida por su calidad académica, impacto de sus investigaciones y su aporte al desarrollo de la sociedad [42].

Ubicación

Fig. 5 . Vista satelital ubicación de la Universidad Estatal Península de Santa Elena *[43]*

Fig. 6. Vista del mapa de evacuación de la Facultad de Sistemas y Telecomunicaciones

2.1.1 Base legal

2.1.1.1 Constitución de la república del Ecuador

Artículo 66.- Derecho a la protección de datos de carácter personal

Garantiza a todas las personas el derecho a la protección de sus datos personales. Este derecho implica que el individuo tiene el control y la decisión sobre la información y los datos que le conciernen, así como su correspondiente protección. Cualquier recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley [44].

2.1.1.2 Código Orgánico Integral Penal

Sección sexta

Artículo 178.- Violación a la intimidad

La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grave, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años [45].

Sección Novena

Artículo 190.- Apropiación fraudulenta por medios electrónicos

La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años [45].

La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes [45].

Sección tercera

Artículo 230.- Intersección ilegal de datos

Será sancionada con pena privativa de libertad de tres a cinco años:

1) La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible [45].

2) La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder [45].
3) La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares [45].
4) La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior [45].

Artículo 234.- Acceso no consentido a un sistema informático

La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años [45].

2.1.1.3 Ley Orgánica de datos personales

Artículo 37.- Seguridad de datos personales

El responsable o encargado del tratamiento de datos personales, según sea el caso, debería sujetarse al principio de seguridad de datos personales, para lo cual deberá tomar en cuenta las categorías y volumen de datos personales, el estado de la técnica, mejores prácticas de seguridad integral y los costos de aplicación de acuerdo a la naturaleza, alcance, contexto y los fines del tratamiento, así como identificar la probabilidad de riesgos [46].

El responsable o encargado del tratamiento de datos personales, deberá implementar un proceso de verificación, evaluación y valoración continua y permanente de la eficiencia y efectividad de las medidas de carácter técnico, organizativo y de cualquier otra índole, implementadas con el objeto de garantizar y mejorar la seguridad del tratamiento de datos personales [46].

Entre otras medidas, se podrán incluir las siguientes:

1) Medidas de anonimización, seudonimización o cifrado de datos personales.
2) Medidas dirigidas a mantener la confidencialidad, integridad y disponibilidad permanentes de los sistemas y servicios del tratamiento de datos personales y el acceso a los datos personales, de forma rápida en caso de incidentes.
3) Medidas dirigidas a mejorar la residencia técnica, física, administrativa y jurídica.
4) Los responsables y encargados del tratamiento de datos personales, podrán acogerse a estándares internacionales para una adecuada gestión de riesgos enfocada a la protección de derechos y libertades, así como para la implementación y manejo de sistemas de seguridad de la información o a códigos de conducta reconocidos y autorizados por la Autoridad de Protección de Datos Personales.

Artículo 40.- Análisis de riesgo, amenazas y vulnerabilidades

Para el análisis de riesgo, amenazas y vulnerabilidades, el responsable y el encargo del tratamiento de los datos personales deberán utilizar una metodología que considere, entre otros [46]:

1) Las particularidades del tratamiento.
2) Las particularidades de las partes involucradas
3) Las categorías y el volumen de datos personales objeto de tratamiento

Articulo 41.- Determinación de medidas de seguridad aplicables

Para determinar las medidas de seguridad, aceptadas por el estado de la técnica, a las que están obligadas el responsable y el encargado del tratamiento de los datos personales se deberán tomas en consideración, entre otros [46]:

1) Los resultados del análisis del riesgos, amenazas y vulnerabilidades.
2) La naturaleza de los datos personales.
3) Las características de las partes involucradas.
4) Los antecedentes de destrucción de datos personales, la perdida, alteración, divulgación o impedimento de acceso a los mismos por parte del titular, sean accidentales e intencionales, por acción u omisión, asi como los antecedentes de trasferencia, comunicación o de acceso no autorizado o acceso de autorización de tales datos.

2.2. Marco conceptual

2.2.1. Sistema de Información

Un sistema de Información (SI) es un conjunto de elementos organizados, relacionados y coordinados entre sí, con el fin de encargarse de facilitar el funcionamiento de una empresa o de cualquier otra actividad humana para conseguir sus objetivos [47].

Estos elementos son:

1) Recursos
2) Equipo Humano
3) Información
4) Actividades

2.2.2. Sistema de informático

Un sistema de Informático está constituido por un conjunto de elementos físicos (Hardware, dispositivos, periféricos y conexiones), lógicos (Sistemas operativos, aplicaciones, protocolos, entre otros.). Con frecuencia se incluyen también los elementos humanos (personal experto que manejan tanto el software como el hardware) [47].

2.2.3. Seguridad informática

Esta es una disciplina encargada del diseño de reglas, procedimiento, métodos y técnicas para crear sistemas de información seguros y confiables [47].

Para establecer este sistema de seguridad es necesario conocer lo siguiente:

1) Cuáles son los elementos
2) Cuáles son los peligros
3) Cuáles son las medidas

2.2.4. Ataques Informáticos

Un ataque informático consiste en aprovechar una debilidad o error (vulnerabilidad) en el software, hardware, e incluso personas que forman parte de un ambiente informático; con el fin de obtener un beneficio, por lo general de índole económico, causando un efecto negativo en la seguridad del sistema, que luego afecta directamente en los activos de la organización [48].

2.2.5. Redes Distribuidas

Son aquellas que se componen de varios nodos que están interconectados y trabajan de forma coordinada para proporcionar un servicio en conjunto. En el contexto de la detección de anomalías en tráfico URL, las redes distribuidas permiten que se monitoree el tráfico de múltiples puntos de la red, lo que permite detectar patrones de comportamiento anómalos con mayor eficacia [49].

2.2.6. Análisis de Tráfico de Red

Es la inspección de los paquetes de datos que se transmiten a través de una red para extraer información sobre su contenido, origen y destino. En el caso de la detección de anomalías en tráfico URL, el análisis de tráfico de red permite identificar patrones de comportamiento anómalo en las solicitudes de URL y detectar posibles amenazas [50].

Durante el análisis del tráfico de red, se pueden encontrar paquetes con contenido maliciosos o anómalos. Estos paquetes tendrán que ser analizados con más detalle para ver si se tratan de paquetes espontáneos o paquetes con un objetivo oculto [51].

2.2.7. Direcciones IP

El protocolo de Internet es un protocolo no orientado a conexión y que funciona a través de una red conmutada de paquetes. Es, por tanto, un protocolo de máximo esfuerzo de entrega de paquetes no confiable. Es uno de los protocolos de Internet más importantes, ya que permite el transporte de paquetes de datos a pesar de que se haga sin garantías [51].

2.2.8. Análisis de Paquete

El análisis de paquetes de red permite examinar el tráfico de la red en un nivel granular, evaluando los paquetes individualmente. Proporciona una visión detallada de la información contenida en cada paquete, lo que facilita la comprensión y el análisis específico del tráfico. Por otro lado, el análisis de flujo se enfoca en recopilar metadatos o información resumida sobre el tráfico de red. Esta información incluye detalles como direcciones IP, puertos y protocolos utilizados, permitiendo un análisis estadístico del tráfico en general. Ambos enfoques son complementarios y proporcionan perspectivas útiles para entender y gestionar el tráfico de red de manera efectiva [52].

2.2.9. Análisis por Flujo

El análisis de flujo tiene como objetivo recopilar metadatos o información sobre el tráfico de una red. Un flujo de IP se refiere a un conjunto de paquetes con atributos específicos de paquetes IP, donde cada paquete es direccionado y procesado por un conmutador o enrutador, y se incluye la siguiente información [53]:

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

2.2.9.1. NetFlow

NetFlow es un estándar ampliamente utilizado para recopilar estadísticas y datos sobre el flujo de tráfico en una red. Permite monitorear y registrar todo el tráfico que atraviesa una interfaz, analizando los datos de flujo recopilados para brindar visibilidad sobre el flujo y el volumen del tráfico. NetFlow proporciona información detallada sobre el origen y destino del tráfico, así como la cantidad de flujo generado en cualquier momento. Estos registros de información pueden ser

empleados para monitorear el uso de la red, detectar anomalías o llevar a cabo diversas tareas de gestión de redes. NetFlow ofrece valiosas herramientas para comprender y optimizar el tráfico de una red [53].

2.2.10. Análisis de Cabecera

La cabecera es el inicio de la red donde se procesa la información que se va a enviar a los abonados. Las cabeceras IP contienen las direcciones de las máquinas de origen y destino, direcciones IP, direcciones que serán usadas por los conmutadores de paquetes, switches y los enrutadores, routers para decidir el tramo de red por el que reenviarán los paquetes [54].

2.2.11. IP

Es la parte del direccionamiento de Internet y se encarga de intercambiar paquetes de datos de distintos dispositivos en la red, a todos los dispositivos conectados se les asigna una IP el cual es un número que los identifica en Internet [55].

2.2.11.1 IP v4

Este es uno de los principales protocolos de internet, utiliza 32 bits, teniendo un total de hasta 4300 millones de direcciones IP [55].

2.2.11.2 IP v6

Este protocolo de direcciones cuenta con una longitud de 128 bits, teniendo un total de 340 sextillones de direcciones, permitiendo de esta manera ampliar el direccionamiento y desarrollo de las tecnologías de la información asadas en internet [55].

2.2.12. Seguridad por capas

La seguridad en capas es una estrategia que combina varios elementos de seguridad, como software antivirus, firewalls y herramientas de evaluación de vulnerabilidades, para crear una barrera defensiva integral y más robusta que la suma de sus partes individuales [56]. Este enfoque aumenta significativamente el costo y la dificultad para que un atacante pueda penetrar en un sistema, lo que reduce la probabilidad de que se convierta en objetivo de ataques. Al implementar la seguridad en capas, se disuade a los atacantes de intentar asediar una institución debido al nivel adicional de protección y complejidad que deben superar [56].

2.2.13. Sitio Web

Es una estructura de información, como muchas otras, donde la peculiaridad de la hipertextualidad y su papel en diferentes escenarios, acceso múltiple y a gran escala, como el ciberespacio [57].

2.2.14. Página anómala

Una página anómala se refiere a aquellas que presentan comportamiento o resultado inusual o atípico en comparación con el patrón esperado, siendo su mayor característica, verse con total normalidad en términos de contenido, estructura o comportamiento. La detección de este tipo de páginas es esencial, debido a que permite identificar actividades maliciosas como ataques cibernéticos, phishing o distribución de malware [58].

2.2.15. Modelos de detección de anomalías

Actualmente, existen varios modelos de detección de páginas anómalas o fraudulentas, cada uno de ellos con sus propias características y aplicación. Entre las más usadas podemos encontrar detección basada en firmas, detección basada en heurística, basado en Machine Learning, y detección basada en listas [59] [60].

2.2.15.1. Detección basada en firmas.

La detección de amenazas se puede implementar de manera básica y sencilla utilizando firmas. Estas firmas consisten en una definición almacenada en una base de datos donde el software antivirus contiene información sobre los virus conocidos que está diseñado para detectar [59]. Este enfoque se basa en la identificación de patrones y firmas específicas de ataques o anomalías previamente identificadas.

Consiste en comparar los datos con una base de datos de firmas o patrones, buscando coincidencia con cadenas de código o palabras claves especificas asociadas comúnmente en actividades anómalas [61]. Sin embargo, una limitación importante de este enfoque radica en la detección de nuevas amenazas.

2.2.15.2. Detección basada en Heurística

La detección de amenazas en páginas web se puede realizar mediante enfoques basados en heurística. Estas técnicas de análisis de comportamiento activo permiten

determinar si una página web es maliciosa al observar su comportamiento y simular el análisis que realizaría un experto al examinar muestras de malware [59].

La detección basada en heurística ofrece varias ventajas significativas en el ámbito de la seguridad web. Permite a las empresas de protección anticiparse a nuevas variantes de malware y detectarlas, incluso si han sido modificadas para evadir las técnicas de detección convencionales. Sin embargo, también tiene algunos inconvenientes a tener en cuenta. Por ejemplo, el rendimiento puede verse afectado cuando es necesario realizar un análisis dinámico de la página web, lo cual puede repercutir en la velocidad de respuesta del sistema de detección de amenazas en tiempo real [59].

2.2.15.3. Detección basada en Machine Learning

Una de las técnicas más efectivas para la detección de páginas web fraudulentas es el uso de algoritmos de aprendizaje automático o machine learning. Esta técnica dinámica se basa en la implementación de algoritmos y métodos heurísticos que permiten extraer características distintivas de un conjunto de datos previamente recopilados, con el objetivo de diferenciar entre páginas de phishing y aquellas que no lo son [60].

Este modelo utiliza algoritmos de aprendizaje automático para poder analizar datos y detectar patrones de comportamiento normales en sitios web, y luego utilizar ese modelo para la detección de anomalías [62]. Estos sistemas son más efectivos que los basados en firma, debido a que permite adaptarse a nuevos patrones de comportamiento anómalos.

2.2.15.4. Detección basada en Listas

Existen dos enfoques principales usados en los sistemas de detección de páginas web fraudulentas: listas blancas y listas negras.

Los sistemas de detección basados en listas blancas recopilan un conjunto de páginas web consideradas de confianza. Cada página web que no esté incluida en la lista blanca se considera sospechosa. Estos sistemas confían en que las páginas web legítimas se encuentren en la lista blanca y, por lo tanto, se les permite el

acceso, mientras que las páginas no listadas se consideran potencialmente fraudulentas [60].

Por otro lado, los sistemas de detección basados en listas negras, también conocidas como blacklists, contienen URLs conocidas de páginas fraudulentas. Estas listas proporcionan un método de control de acceso para evitar que los usuarios visiten estas páginas. Si una URL coincide con la lista negra, se bloquea el acceso a la página web correspondiente [60].

Tanto las listas blancas como las listas negras son utilizadas en los sistemas de detección para clasificar y categorizar las páginas web con el objetivo de identificar posibles amenazas de phishing. Sin embargo, es importante tener en cuenta que estos enfoques tienen limitaciones, ya que las listas deben mantenerse actualizadas constantemente para adaptarse a las nuevas páginas fraudulentas o legítimas que surjan. Además, pueden generar falsos positivos o negativos, dependiendo de la precisión y exhaustividad de las listas utilizadas.

2.2.16. Algoritmo de detección

Los algoritmos de detección de fallas se dividen en dos categorías. Basados en el patrón de la anomalía y basados en el comportamiento normal de la red. Los modelos basados en el patrón anómalo requieren tener un conocimiento previo sobre las fallas para su posterior modelado, pero esto no siempre es posible debido a la complejidad del entorno de la red, por lo que pueden ocurrir nuevos tipos de fallas sin ser detectadas [63].

En el caso de un algoritmo basado en el comportamiento normal de la red, se crea un archivo de configuración que almacena los parámetros de funcionamiento normal en el equipamiento activo de la red, a partir de lo cual se definen los Acuerdos de Nivel de Operación y Servicio [63].

2.2.17. Base de datos

Una Base de datos (BD) es un conjunto de datos ordenado y estructurado que representa la realidad objetiva y que está organizado independientemente de las aplicaciones, por lo que puede ser utilizado y compartido por diferentes usuarios y aplicaciones [64].

2.2.18. Machine Learning

Es un subcampo, las ciencias de la computación y una rama de la inteligencia artificial que tiene como objetivo desarrollar técnicas en base al aprendizaje automático de patrones en basados en un conjunto de datos. Permitiendo que la computadora aprenda, convirtiéndola en un pilar fundamental para el trato de datos a gran escala [65].

2.2.19. API

Las Application Programming Interface (API) son interfaces o zonas de contacto de un conjunto de bibliotecas o paquetes de software, ser visto y ejecutados por otros software o programas. Es decir, las Api son herramientas que permiten que diferentes programas se comuniquen entre sí. La importancia del uso de API radica en su capacidad para permitir que diferentes programas, dispositivos y aplicaciones trabajen en conjunto y compartan información, creando de esta manera una conectividad denominada internet [66].

2.2.20. API Bot Telegram

Es una interfaz de programaciones de aplicaciones que permite a los desarrolladores crear y personalizar chatbots para interactuar con los usuarios a través de la plataforma de mensajería Telegram. La API proporciona métodos para enviar y recibir mensajes, gestionar grupos y canales, obtener información de usuarios, enviar archivos multimedia, entre otros. [13]

2.2.21. API Void

Esta API permite a los desarrolladores y analistas de seguridad obtener datos relevantes sobre una dirección IP específica, incluye su calificación de reputación, información geográfica, información del proveedor del servicio de internet y la lista de categorías asociadas a la IP, como spam, malware o actividades sospechosas [12]. Los servicios de esta API permiten a los usuarios acceder de forma rápida a datos actualizados y detallados sobre la reputación de una IP [12].

2.2.22. OMSTD

La Metodología abierta para desarrolladores de herramientas de seguridad u OMSTD por sus siglas en inglés, es una metodología que proporciona una guía de buenas prácticas fáciles, intuitiva y prácticas, para el desarrollo de herramientas en

el campo de la ciberseguridad [38]. Esta metodología está desarrollada tanto para proyectos pequeños como para los de mayor tamaño, centrado principalmente en el uso de Python, Aunque puede ser utilizados en otros lenguajes [7].

2.2.23. Norma ISO/IEC 27032

Esta normativa se centra en dos áreas: cubrir los espacios o huecos no cubiertos por normas anteriores de seguridad en este ámbito conceptual más amplio, en el que aparecen nuevos ataques y los riesgos asociados a estos, y el proceso de colaboración entre los agentes que operan en el entorno actual, en lo que se denomina comúnmente un Marco de Ciberseguridad o CSF, CyberSecurity Framework [40].

2.2.24. Malware

El Malware es un malicious software (software malicioso) diseñado para infiltrarse en su dispositivo sin su conocimiento, con el objetivo de causar daños e interrupciones en el sistema o robar datos [67]. Adware, spyware, virus, redes de robots (botnets), troyanos, gusanos, rootkits y ransomware, todos estos entran en la definición de malware [67].

2.2.25. Pharming

El pharming o suplantación de dominio es un delito cibernético muy similar al phishing que consiste en manipular el tráfico del sitio web para obtener información confidencial [68]. Este aprovecha el comportamiento de navegación de Internet, es decir, la manera de convertir una secuencia de letras para formar una dirección de Internet, como www.google.com, en una dirección IP por parte de un servidor DNS para establecer la conexión [68].

El exploit ataca de dos maneras. En primer lugar, es posible instalar un virus o un troyano dentro de una computadora de un usuario que cambia el archivo de hosts para redireccionar el tráfico fuera de su objetivo previsto, hacia un sitio web falso [68]. En segundo lugar, el hacker puede envenenar un servidor DNS para que los usuarios visiten el sitio falso sin darse cuenta [68].

2.2.26. Phishing

El phishing es un delito informático en donde por medio de la ingeniería social y medios técnicos para robar los datos de identificación personal de los consumidores y credenciales de cuentas financieras. Los esquemas de ingeniería social utilizan correos electrónicos engañosos que pretenden ser de empresas u organizaciones legítimas, diseñados para dirigir a los consumidores a sitios web falsos que engañan a los destinatarios para que revelen datos financieros, como nombres de usuario y contraseñas [69].

2.2.27. Spam

Se denominan Spam a todos los mensajes no solicitados o no deseados. Por lo general, los mensajes de spam no provienen de otro teléfono [70]. Principalmente, provienen de una computadora y se envían a tu teléfono mediante una dirección de correo electrónico o una cuenta de mensajería instantánea [70]. Debido a que se envían en línea, son baratos y los estafadores pueden enviarlos fácilmente [70].

2.2.28. Python

Python es un lenguaje de programación caracterizado por ser potente y fácil de aprender, teniendo una estructura de datos de alto nivel y un enfoque simple pero efectivo para la programación orientada a objetos [71]. Su sintaxis elegante y la tipificación dinámica de Python, en conjunto con su naturaleza interpretada, lo convierten en un lenguaje ideal para secuencias de comandos y desarrollo rápido de aplicaciones en muchas áreas en la mayoría de las plataformas. [71]

2.2.29. Wireshark

Wireshark es un analizador de protocolos open-source disponible para múltiples plataformas. Su función principal es el análisis de tráfico, que implementa extensos filtros que ayudan a definir criterios de búsqueda para más de 1100 protocolos soportados actualmente [72]. Wireshark permite entender la estructura de los protocolos, se puede visualizar las cabeceras y las capas que componen los paquetes, proporcionando un gran abanico de posibilidades [72].

2.2.30. Dashboard

Un Dashboard o “Tablero digital” es una interfaz gráfica de usuario en dónde se pueden administrar recursos informáticos y analizar información para la toma de

decisiones [73]. Tiene una interfaz gráfica que permite a los usuarios interactuar con los datos de una manera más intuitiva, aparte es altamente personalizable, lo que permite adaptarse a las necesidades y objetivos específicos de cada proyecto.

2.3. Marco Teórico

2.3.1. Modelo de defensa en profundidad para la protección contra ciberataques

El modelo de defensa profunda es una Teoría ampliamente aceptada en el campo de la seguridad informática, esta propone la implementación de múltiples capas de seguridad para proteger los sistemas y datos contra ciberataques. Este enfoque se basa bajo la premisa de que para una protección completa es necesario más de una medida de seguridad [74].

Según Cantor Ospina y Nohota Milena en su artículo "defensa en profundidad para la protección contra las amenazas persistentes avanzadas", indican que en los últimos años los atacantes informáticos utilizan con más frecuencia las nuevas tecnologías. Lo que da paso al concepto en seguridad de "Amenazas Persistentes Avanzadas (APT)" [74].

A continuación, se muestra un modelo de aprendizaje profundo empleado por autores o firmas como Microsoft, Esset, entre otros. Sobres un sistema tecnológico para la protección de las APT [74].

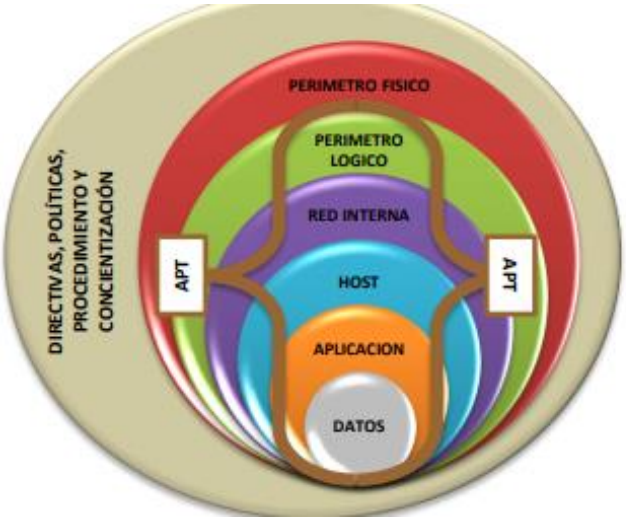


Fig. 7. Modelo de Defensa en Profundidad- Microsoft *[74]*.

2.3.2. Técnica de reputación de URL en la detección de anomalías en el tráfico de red

En seguridad informática, la detección de anomalías en el tráfico URL juega un papel fundamental para proteger los sistemas y datos amenazas potenciales. Para mejorar la precisión y eficiencia de dicha detección, se han desarrollado varias técnicas y enfoque, entre los que destaca el uso de técnicas de reputación URL [50].

Esta técnica se basa en la evaluación de la confiabilidad y reputación de los sitios web a través de recopilación y análisis de datos relevantes. Para evaluar las páginas se toman en cuenta diferentes aspectos, como el historial del dominio, la interacción previa con el sitio, la presencia de malware y las quejas de los usuarios [50].

Según Animesh Patcha y Parque Jung Min en su artículo "Una visión general de las técnicas de detección de anomalías: soluciones existentes y últimas tendencias tecnológicas", indica que el uso de esta técnica aporta una capa adicional de seguridad, al implementar estas en conjunto con otras técnicas de detección, se puede mejorar la identificación y clasificación de posibles amenazas [50].

En internet existen diversas plataformas que brindan el servicio de análisis de reputación a URL, IP o dominio. A continuación, se muestra diversas URLs en donde se pueden encontrar estos servicios y bases de datos de listas de reputación [75]:

- Virus total: https://www.virustotal.com/gui/home/upload
- Talos: https://talosintelligence.com/documents/ip-blacklist
- FireHoL IP Lists: https://iplists.firehol.org/
- Apility: https://apility.io/
- Foro Abuses: https://www.abuses.es/eswl/
- Broadcom: https://ipremoval.sms.symantec.com/
- MxToolBox: https://mxtoolbox.com/blacklists.aspx
- ApiVoid: https://www.apivoid.com/api/ip-reputation/
- AntiScan.Me: https://antiscan.me/

2.3.3. El uso de los Threads o Hilos de ejecución en aplicaciones informáticas

Los hilos de ejecución o también llamados threads se han convertido en un componente crucial en el diseño y desarrollo de aplicaciones informáticas modernas. Un hilo de ejecución representa secuencias de instrucciones que permiten que un programa pueda realizar múltiples tareas de manera simultánea. La correcta implementación de los hilos de ejecución puede tener un impacto significativo en la concurrencia y el rendimiento de la aplicación [76].

El uso de los hilos de ejecución permite el uso de diferentes partes del código en paralelo de tal manera que se pueda acelerar la capacidad de respuesta y aprovechar eficientemente los recursos del sistema [76]. Al utilizar este método en la elaboración del algoritmo, se plantea mejorar la eficiencia y la capacidad de procesamiento dentro del entorno en el que se está trabajando, considerando que su aplicación es sencilla debido al lenguaje de programación a utilizar, el cual es Python [76].

2.4. Requerimientos

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

R1. Para ejecutar el algoritmo se debe tomar en cuenta los siguientes requisitos del sistema.

Tabla 1. Requisitos Mínimos

Requisitos mínimos	
Procesador	Intel Core i3-5005U de 2GHz
Memoria RAM	4 GB
Espacio de almacenamiento	128 GB
Tarjeta de red	Realtek PCIe GbE
Trae geta de video	Tarjeta integrada Intel (R) UHD Graphics

Fuente: Elaboración propia

Tabla 2. Requisitos Recomendados

Requisitos Recomendados	
Procesador	Intel(R) Core (TM) i5-10110U CPU @ 2.10GHz 2.59 GHz o Superior
Memoria RAM	8 GB
Espacio de almacenamiento	500 GB
Requisitos Recomendados	
Tarjeta de red	Intel Wi-Fi 6 Ax201 160 MHz
Trae geta de video	Envidia GeForce GTX 1650

Fuente: Elaboración propia

R2. El usuario deberá crear una cuenta en el servicio de mensajería Telegram para poder crear el Bot y poder recibir las notificaciones.

R3. El usuario deberá generarse una cuenta en ApiVoid para poder tener una Key, la cual se usará para establecer el enlace entre el algoritmo y la API.

R4. El algoritmo podrá ser ejecutado en sistemas operativo Windows y Linux

R5. Para hacer uso de la aplicación se necesitará tener instalado Python3 versión 3.8.0 o superior.

R6. Para hacer uso del algoritmo es necesario tener instaladas las siguientes librerías: flask; flask_Login; flask_sqlalchemy; flask_socketio; flask_socketio; flask_wtf; flask-mail; requests ; scapy; matplotlib; pandas; reportlab; pymysql; pyshark; email_validator; itsdangerous; xlsxwriter.

R7. Para poder visualizar el dashboard es necesario tener instalado un navegador web, como Firefox, Google Crome, Microsoft Edge, entre otros.

R8. Las notificaciones que lleguen a Telegram se pueden visualizar desde un dispositivo móvil o desde un ordenador.

R9. El algoritmo debe tener la capacidad de realizar N análisis por segundo.

R10. Cada paquete analizado será clasificado según los resultados entre normales y anómalos y respaldados en la base de datos.

R11. Toda amenaza será notificada al ser detectada.

R12. Los administradores del programa tendrán la opción de crearse usuarios para asignar responsables de cada análisis.

R13. Los administradores podrán iniciar o detener un análisis una vez ingresando en el programa.

R14. El tiempo del aprendizaje del programa no debe exceder las 5 horas.

R15. En caso de presentar alguna inconsistencia dentro del programa, el personal administrativo deberá detener el actual análisis.

2.5. Componente de la Propuesta

2.5.1. Metodología OMSTD

Para el desarrollo del algoritmo se utilizará la metodología OMSTD [7], que incluye la Organización y Estructuración, Entrada y Salida de información, Redistribuciones y Despliegue.

Existen numerosos frameworks que facilitan la creación de dashboard de manera rápida y eficiente. En las siguientes tablas se comparará y analizará tres de los frameworks más populares: Flask, Django y FlaskAPI. Cada uno de ellos tiene sus propias características y fortalezas, por lo que es importante comprender sus diferencias antes de elegir el más adecuado para este proyecto.

Tabla 3- Comparativa de las principales características de Flask, Django y FastAPI *[77] [78] [79]*

Característica	Flask	Django	FastAPI
Arquitectura	Envoltorio para WSGI	Plantilla de vista de modelo (MVT)	Envoltorio para WSGI
Tipo de Framerwork	Micro-framework	Full-stack	Micro-framework
Comunidad	Más pequeña	Más grande	Creciendo rápidamente
Estilo de trabajo	Monolítico	Diversificado	Monolítico
Flexibilidad	Alto	Bajo	Alto
Uso	Se utiliza para desarrollar una aplicación web minimalista y REST APIs	Utilizado para desarrollar Full-stack, Aplicaciones Web y REST APIs	Utilizado para crear aplicaciones web rápidas y REST APIs
Facilidad de uso	Simple	Más compleja	Simple
Escalabilidad	Buena	Excelente	Excelente

Característica	Flask	Django	FastAPI
Rapidez	Mas rápido que Django.	No es tan rápido como las otras dos herramientas.	Ligeramente más rápida que Flask y mucho más rápida que Django
Soporte de base de datos	Se basa en SQLAlchemy u otras extensiones para ORM	ORM incorporado y Soporte para SQLite, PostgreSQL, MySQL, MariaDB y Oracle	Manual
Compatibilidad	Todas versiones de Python	Todas versiones de Python	Python 3.5 en adelante (No funciona con Python 3.5 o versiones anteriores)
Formularios	Requiere la extensión Flask-WTF	Incorporado	No definida
Despachador de URL	RESTful	Controlador RegEx	Controlador RegEx

Tabla 4- Comparativa entre Flask, Django y FastAPI *[77] [78]*

Característica	Flask	Django	FastAPI
Basada en Python	✓	✓	✓
Código Abierto	✓	✓	✓
Multiplataforma	✓	✓	✓
Desarrollo REST	✓	×	✓
Soporte de API	✓	×	✓
Modelos de datos integrados	×	✓	×
Soporte de aplicaciones de terceros	×	✓	✓
Ligero	✓	×	×
Soporta Ninja2	✓	×	✓
Manejo de rutas	✓	✓	✓
Seguro	✓	✓	×
Procesamiento de peticiones asíncronas	×	×	✓

Una vez analizado los tres fameworks, se ha llegado a la conclusión de que Flask es la opción ideal para el desarrollo del proyecto. Aunque Django es ampliamente reconocido por su enfoque integral y su potencial, Flask ofrece una mejor

flexibilidad y simplicidad, lo que se adapta perfectamente a los requisitos principales del proyecto. Además, con Flask se puede desarrollar de manera más rápida y sencilla aplicaciones web más pequeñas y personalizadas, sin comprometer la eficiencia del código.

2.5.1.1. Organización y Estructuración

Basándonos en el objetivo establecido, el cual es el desarrollo de un algoritmo y el diseño de un dashboard, junto con el framework de desarrollo web en Python seleccionado, se establece la siguiente estructura para el contenido del proyecto:

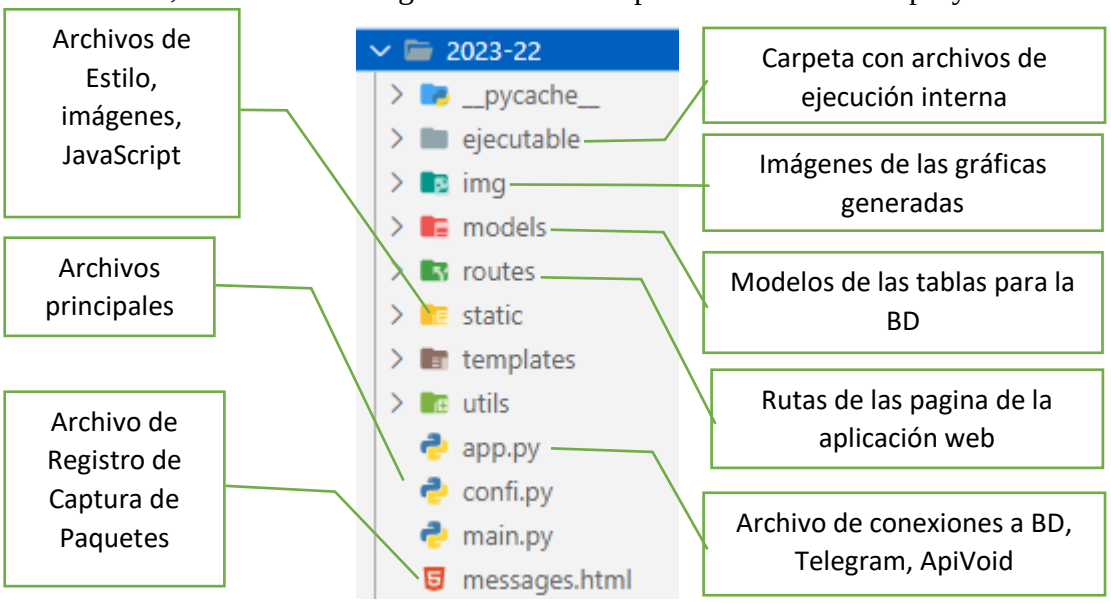


Fig. 8.Estructura del proyecto realizado en el Framework Flask

Fuente: Elaboración propia

2.5.1.2. Entrada y Salida de información

Teniendo en cuenta la finalidad del agente desarrollado, se toman a considerar las como datos ingresados a los siguientes.

- Ingreso del host por parte del usuario
- Ingreso de la interfaz de red por parte del usuario.
- Archivo JSON del resultado del análisis proporcionado por apivoid.
- Credenciales de usuarios al iniciar sesión.
- Información del usuario

Como salida se considera a los mensajes enviados a la consola del dashboard como la IP enviada al servidor de análisis.

- Mensajes enviados a la consola de la pagina
- IP enviada para el análisis
- Mensaje enviado al servidor de mensajería.
- Archivo generado del registro de captura de paquetes
- Mensajes emergentes dentro del dashboard

Consideramos también los datos a guardar en la base de datos, como las consultas o extracción de información dentro del mismo.

2.5.1.3. Redistribuciones

Se realizan los scripts bases del algoritmo, tanto para la captura de paquetes, análisis de paquetes y envió de notificaciones al usuario administrador

Script de captura de paquetes

Existen varias herramientas de procesamiento, captura y filtrado de tráfico en red, como PyShark, Scapy y TShark, utilizados para snirfear la red y capturara paquetes que transiten dentro de la misma. De esta manera, en las siguientes tablas se compara las características de cada una.

Tabla 5 - Comparativa de las principales características de PyShark, Scapy y TShark *[18] [80] [81]*

Característica	PyShark	Scapy	TShark
Lenguaje	Python	Python	C
Soporte de protocolos	Amplio	Amplio	Amplio
Rendimiento	Medio	Alto	Medio
Formato de captura	PyShark soporta varios formatos de captura de paquetes, incluyendo pcap, pcapng, y tshark	Scapy soporta varios formatos de captura de paquetes, incluyendo pcap, pcapng, y tshark	TShark soporta varios formatos de captura de paquetes, incluyendo pcap, pcapng, y tshark

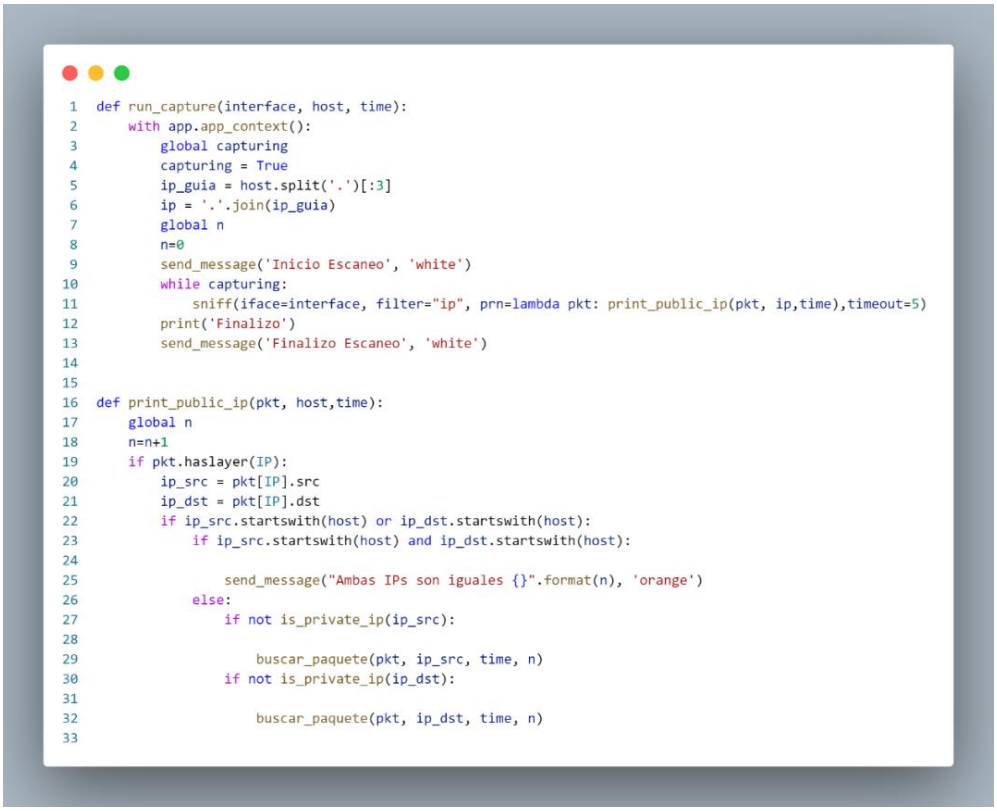
Característica	PyShark	Scapy	TShark
Extracción de informes	PyShark permite extraer información de las diferentes capas de protocolo, como TCP, IP, HTTP, DNS, etc.	Permite extraer información de los paquetes capturados mediante el uso de diferentes funciones y métodos incluidos en Scapy	TShark permite extraer información de las diferentes capas de protocolo, como TCP, IP, HTTP, DNS, etc.
Personalizable	PyShark es una herramienta de código abierto.	Scapy es una herramienta de código abierto y se puede modificar según las necesidades del usuario.	Es una herramienta de código abierto.
Capacidades	Análisis de paquetes, protocolos y des encapsulamiento	Creación y modificación de paquetes, protocolos y des encapsulamiento	Análisis de paquetes, protocolos y de encapsulamiento
Procesos	La ejecución del proceso no va a empezar hasta que sea realmente necesario, por lo que se ahorra un montón de recursos, que deriva a su vez en un mejor desempeño	Inicia su ejecución de procesos en el momento en que se carga en memoria. Una vez cargado, se pueden utilizar sus funciones y métodos para capturar, analizar y manipular paquetes de red.	TShark, al igual que Scapy, inicia su ejecución de procesos en el momento en que se ejecuta en la línea de comandos.

Tabla 6- Comparativa entre PyShark, Scapy y TShark *[18] [80] [81]*

Característica	PyShark	Scapy	TShark
Interfaz de línea de comandos	✗	✓	✓
Soporte de protocolos amplio	✓	✓	✓
Filtros avanzados	✓	✓	✓
Posibilidad de escribir scripts	✓	✓	✗
Integración con otras herramientas de análisis	✓	✓	✓
Filtros de captura	✓	✓	✓
Documentación buena	✓	✓	✓
Computación en memoria	✓	✓	✗

Característica	PyShark	Scapy	TShark
Visualización de archivos capturados	✓	✓	✓
Gráficos y visualización	✓	✓	✓

Tras evaluar estas tres herramientas de captura y filtrado de tráfico en la red, se ha decidido utilizar PyShark. Esta elección se basa en su facilidad de uso, la amplia información que proporciona sobre el tráfico de la red. Mediante el uso de esta librería se realiza el siguiente script de captura y filtrado de paquetes.



```python
def run_capture(interface, host, time):
    with app.app_context():
        global capturing
        capturing = True
        ip_guia = host.split('.')[:3]
        ip = '.'.join(ip_guia)
        global n
        n=0
        send_message('Inicio Escaneo', 'white')
        while capturing:
            sniff(iface=interface, filter="ip", prn=lambda pkt: print_public_ip(pkt, ip,time),timeout=5)
        print('Finalizo')
        send_message('Finalizo Escaneo', 'white')


def print_public_ip(pkt, host,time):
    global n
    n=n+1
    if pkt.haslayer(IP):
        ip_src = pkt[IP].src
        ip_dst = pkt[IP].dst
        if ip_src.startswith(host) or ip_dst.startswith(host):
            if ip_src.startswith(host) and ip_dst.startswith(host):

                send_message("Ambas IPs son iguales {}".format(n), 'orange')
            else:
                if not is_private_ip(ip_src):

                    buscar_paquete(pkt, ip_src, time, n)
                if not is_private_ip(ip_dst):

                    buscar_paquete(pkt, ip_dst, time, n)

```

Fig. 9. Script de captura de paquetes

Fuente: Elaboración propia

Script de análisis de IP con el servicio de ApiVoid

Existen varias herramientas que nos permiten evaluar la integridad de una página web o la IP de esta, para determinar su veracidad y descartar cualquier amenaza que esta pueda contener. En este sentido, se ha realizado las siguientes tablas comparativas:

Tabla 7 - Comparativa de las principales características de APIVoid, Virus Total y AntiScan.Me [12] [82] [83]

Característica	**APIVoid**	**VirusTotal**	AntiScan.Me
Tipo de herramienta	Solución de análisis de amenazas en línea	Solución de análisis de amenazas en línea	Solución de análisis de vulnerabilidades en línea
Enfoque	Análisis de amenazas, detección de malware	Análisis de amenazas, detección de malware	Análisis de vulnerabilidades de archivos
Comunidad	Activa en línea	En línea	Activa en línea
Detección de vulnerabilidades	Más avanzada	Menos avanzada	Avanzada
Detección de malware	Menos avanzada	Más avanzada	No especificado
Nivel de especialización	Especialización en análisis de amenazas en línea	Especialización en análisis de amenazas en línea	Especialización en análisis de vulnerabilidades en línea
Interfaz de usuario	Interfaz web sencilla	Interfaz web sencilla	Interfaz de usuario amigable
Integración con otros sistemas	Algunas opciones de integración	Algunas opciones de integración	Algunas opciones de integración
Precio	Gratis con límites en el uso de la API, Planes de precios desde $9.99/mes	Versión gratuita y planes de precios desde $10/mes	Planes de precios desde $9.99/mes
Cantidad de motores de análisis	+80	+70	No especificado

Tabla 8 - Comparativa entre APIVoid, Virus Total y AntiScan.Me *[12] [82] [83]*

Característica	**APIVoid**	**VirusTotal**	**AntiScan.Me**
Análisis de seguridad más amplio	✓	✓	✓
Comunidad activa	✓	✓	✓
Detección de vulnerabilidades	✓	✓	✓
Detección de malware	✓	✓	✓

Característica	APIVoid	VirusTotal	AntiScan.Me
Interfaz de usuario sencilla	✓	✓	✓
Funcionalidad de automatización	✓	✓	✓
Integración con otros sistemas	✓	✓	✓

Después de evaluar estas herramientas, se ha decidido escoger APIVoid debido a que ofrece una solución de análisis de amenazas en línea. De la misma manera se consideró la información que este remite después de un análisis, siendo de esta manera APIVoid superior a las demás. Considerando esto se crea a continuación el siguiente script de envió de petición de análisis a la IP.

```
def apivoid_iprep(ip):
    try:
        r = requests.get(url='https://endpoint.apivoid.com/iprep/v1/pay-as-you-go/?key='+apivoid_key+'&ip='+ip)
        #print(json.loads(r.content.decode()))
        return json.loads(r.content.decode())
    except Exception as e:
        return ""
```

Fig. 10. Script de envió de IP al servicio URLVOID para su análisis

Fuente: Elaboración propia

Script de registro de paquete en base de datos

Para poder clasificar y registrar los análisis de direcciones IP emitidos por el servicio de APIVoid, es necesario una base de datos. Existen diversas herramientas de gestión de bases de datos que se utilizan para administrar y mantener la Integridad de la información. En este sentido, se ha realizado las siguientes tablas comparativas de herramientas de gestión de base de datos.

Tabla 9 - Comparativa de las principales características de phpMyAdmin, MySQL Workbench Heidi SQL *[84] [85]*

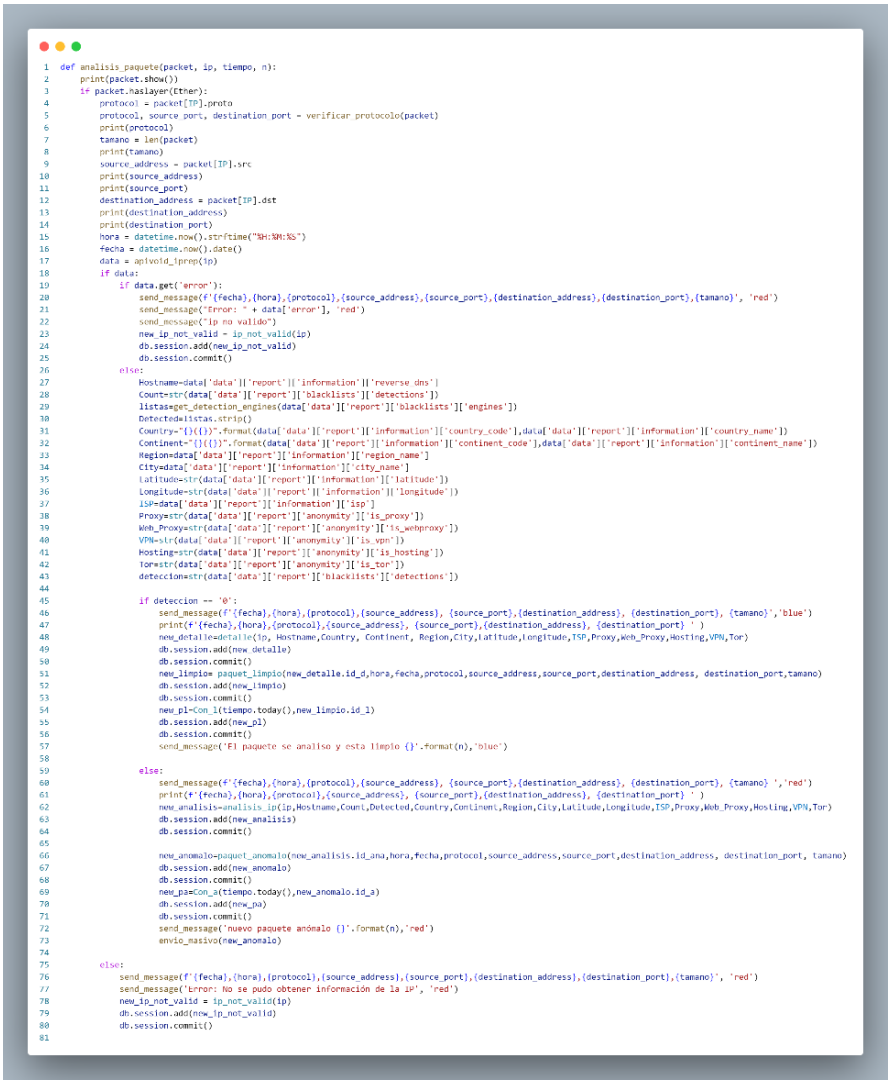
Herramienta	phpMyAdmin	MySQL Workbench	Heidi SQL
Lenguaje	PHP	C++	Delphi

Herramienta	phpMyAdmin	MySQL Workbench	Heidi SQL
Seguridad	Ofrece autenticación de dos factores y cifrado SSL	Ofrece autenticación de dos factores y cifrado SSL	Ofrece autenticación de dos factores y cifrado SSL
Interfaz de usuario	Interfaz web intuitiva	Interfaz gráfica de usuario	Interfaz gráfica de usuario
Compatibilidad	Compatible con MySQL y MariaDB	Compatible con MySQL	Compatible con MySQL, Microsoft SQL Server y PostgreSQL
Facilidad de uso	Fácil de usar para usuarios principiantes	Requiere conocimientos previos de SQL	Fácil de usar para usuarios principiantes
Sistema operativo	Se puede descargar de forma gratuita e instalar en cualquier computadora, servidor o sistema operativo que ejecute PHP (que incluye Linux) además de Windows	Cualquier sistema operativo, sea Linux, Windows o Mac	Puede ser instalado en cualquier versión de Windows posterior a Windows 98, Linux que utilice MacOS X

Tabla 10 - Comparativa entre phpMyAdmin, MySQL Workbench y Heidi *[84] [85]*

Herramienta	phpMyAdmin	MySQL Workbench	Heidi SQL
Interfaz web	✓	✗	✗
Soporte de varios idiomas	✓	✓	✓
Compatibilidad con varios tipos de bases de datos	✗	✗	✓
Facilidad de uso	✓	✓	✓
Personalización	✓	✓	✓
Creación de gráficos	✗	✓	✗
Creación de relaciones	✓	✓	✓
Acceso remoto mediante ssh o ssl	✓	✓	✓
Gratuita	✓	✓	✓

Después de evaluar las diferentes herramientas, se ha decidido utilizar phpMyAdmin debido a su interfaz web intuitiva y su compatibilidad con MySQL. A continuación, se realiza el script para clasificar el resultado del análisis y registrar en la base de datos.



```
def analisis_paquete(packet, ip, tiempo, n):
    print(packet.show())
    if packet.haslayer(Ether):
        protocol = packet[IP].proto
        protocol, source_port, destination_port = verificar_protocolo(packet)
        print(protocol)
        tamano = len(packet)
        print(tamano)
        source_address = packet[IP].src
        print(source_address)
        print(source_port)
        destination_address = packet[IP].dst
        print(destination_address)
        print(destination_port)
        hora = datetime.now().strftime("%H:%M:%S")
        fecha = datetime.now().date()
        data = apivoid_1prep(ip)
        if data:
            if data.get('error'):
                send_message(f'{fecha},{hora},{protocol},{source_address},{source_port},{destination_address},{destination_port},{tamano}', 'red')
                send_message('Error: ' + data['error'], 'red')
                send_message("ip no valido")
                new_ip_not_valid = ip_not_valid(ip)
                db.session.add(new_ip_not_valid)
                db.session.commit()
            else:
                Hostname=data['data']['report']['information']['reverse_dns']
                Count=str(data['data']['report']['blacklists']['detections'])
                listas=get_detection_engines(data['data']['report']['blacklists']['engines'])
                Detected=listas.strip()
                Country="{}({})".format(data['data']['report']['information']['country_code'],data['data']['report']['information']['country_name'])
                Continent="{}({})".format(data['data']['report']['information']['continent_code'],data['data']['report']['information']['continent_name'])
                Region=data['data']['report']['information']['region_name']
                City=data['data']['report']['information']['city_name']
                Latitude=str(data['data']['report']['information']['latitude'])
                Longitude=str(data['data']['report']['information']['longitude'])
                ISP=data['data']['report']['information']['isp']
                Proxy=str(data['data']['report']['anonymity']['is_proxy'])
                Web_Proxy=str(data['data']['report']['anonymity']['is_webproxy'])
                VPN=str(data['data']['report']['anonymity']['is_vpn'])
                Hosting=str(data['data']['report']['anonymity']['is_hosting'])
                Tor=str(data['data']['report']['anonymity']['is_tor'])
                deteccion=str(data['data']['report']['blacklists']['detections'])

                if deteccion == '0':
                    send_message(f'{fecha},{hora},{protocol},{source_address}, {source_port},{destination_address}, {destination_port}, {tamano}','blue')
                    print(f'{fecha},{hora},{protocol},{source_address}, {source_port},{destination_address}, {destination_port} ' )
                    new_detalle=detalle(ip, Hostname,Country, Continent, Region,City,Latitude,Longitude,ISP,Proxy,Web_Proxy,Hosting,VPN,Tor)
                    db.session.add(new_detalle)
                    db.session.commit()
                    new_limpio= paquet_limpio(new_detalle.id_d,hora,fecha,protocol,source_address,source_port,destination_address, destination_port,tamano)
                    db.session.add(new_limpio)
                    db.session.commit()
                    new_pl=Con_l(tiempo.today(),new_limpio.id_l)
                    db.session.add(new_pl)
                    db.session.commit()
                    send_message('El paquete se analiso y esta limpio {}'.format(n),'blue')

                else:
                    send_message(f'{fecha},{hora},{protocol},{source_address}, {source_port},{destination_address}, {destination_port}, {tamano} ','red')
                    print(f'{fecha},{hora},{protocol},{source_address}, {source_port},{destination_address}, {destination_port} ' )
                    new_analisis=analisis_ip(ip,Hostname,Count,Detected,Country,Continent,Region,City,Latitude,Longitude,ISP,Proxy,Web_Proxy,Hosting,VPN,Tor)
                    db.session.add(new_analisis)
                    db.session.commit()

                    new_anomalo=paquet_anomalo(new_analisis.id_ana,hora,fecha,protocol,source_address,source_port,destination_address, destination_port, tamano)
                    db.session.add(new_anomalo)
                    db.session.commit()
                    new_pa=Con_a(tiempo.today(),new_anomalo.id_a)
                    db.session.add(new_pa)
                    db.session.commit()
                    send_message('nuevo paquete anómalo {}'.format(n),'red')
                    envio_masivo(new_anomalo)

        else:
            send_message(f'{fecha},{hora},{protocol},{source_address},{source_port},{destination_address},{destination_port},{tamano}', 'red')
            send_message('Error: No se pudo obtener información de la IP', 'red')
            new_ip_not_valid = ip_not_valid(ip)
            db.session.add(new_ip_not_valid)
            db.session.commit()
```

Fig. 11. Script de análisis de resultados de paquetes y clasificación del mismo como limpio o anómalo

Fuente: Elaboración propia

Script de consulta de paquete en base de datos

En el desarrollo de aplicaciones web y gestión de base de datos, el uso de un mapeo Objeto-relación (ORM) se ha vuelto más relevante. En las siguientes tablas exploraremos tres diferentes ORM disponible para Python.

Tabla 11 - Comparativa de las principales características SQLAlchemy, Peewee y Django ORM *[79] [86]*

Herramienta	**SQLAlchemy**	**Peewee**	Django ORM
Complejidad de la API	Alta	Baja	Media
Flexibilidad ORM	Alta	Media	Media
Sintaxis	Mas compleja	Mas simple	Similar a SQLAlchemy
Performance	Alta	Media	Alta
Integración con el marco	No está ligado a ninguno	No está ligado a ninguno	Integrado con Django
Modo de trabajo: ORM o SQL puro	Ambos	Ambos	ORM
Tipos de consulta	Soporta SQL avanzado	Soporta SQL avanzado	Limitado a ORM
Facilidad de uso	Requiere experiencia con ORM	Fácil de usar	Fácil de usar, pero limitado en comparación con SQLAlchemy

Tabla 12 - Comparativa entre SQLAlchemy, Peewee y Django ORM *[79] [86]*

Herramienta	**SQLAlchemy**	**Peewee**	**Django ORM**
Multiplataforma	✓	✓	✓
Compatible con varios motores de base de datos	✓	✓	×
Independencia de base de datos	✓	✓	×
Librería independiente	✓	✓	×
Soporte para ORM	✓	✓	✓
documentación extensa	✓	✓	✓
Comunidad	✓	✓	✓
Estabilidad	✓	✓	✓

Al evaluar estas herramientas ORM, se ha decidido utilizar SQLAlchemy para la respectiva conexión y consultas con la base de datos, debido a su compatibilidad con la base de datos utilizada en este proyecto y su facilidad de uso. El siguiente script muestra una búsqueda de información en la base de datos por medio del uso del ORM.

```python
def buscar_paquete(packet, ip,tiempo, n):
    print(ip)
    ip_not_valid_record = ip_not_valid.query.filter_by(ip=ip).first()
    print(ip_not_valid_record)
    paquet_anomalo_record = paquet_anomalo.query.filter((paquet_anomalo.d_destino == ip) | (paquet_anomalo.d_origen == ip)).first()
    paquet_limpio_record = paquet_limpio.query.filter((paquet_limpio.d_destino == ip) | (paquet_limpio.d_origen == ip)).first()
    if ip_not_valid_record:

        send_message('Ip no valida {}'.format(n),'white')
    elif paquet_anomalo_record:

        send_message('Paquete anómalo o pagina anómala {}'.format(n),'red')
        new_pa=Con_a(tiempo,paquet_anomalo_record.id_a)
        db.session.add(new_pa)
        db.session.commit()
        envio_masivo(paquet_anomalo_record)

    elif paquet_limpio_record:
        send_message('El paquete esta limpio {}'.format(n),'green')
        new_pl=Con_l(tiempo,paquet_limpio_record.id_l)
        db.session.add(new_pl)
        db.session.commit()

    else:
        analisis_paquete(packet,ip,tiempo,n)
```

Fig. 12. Script de Búsqueda de paquetes en base de datos.

Fuente: Elaboración propia

Script de configuración y envío de mensajes a Telegram

Para él envió de notificaciones o mensajes al personal administrativo, es necesario contar con un servicio de mensajería, En las siguientes tablas compararemos tres de los servicios más usados.

Tabla 13 - Comparativa de las principales características de Telegram API, WhatsApp API y Discord API *[13] [87] [88]*

Herramienta	Telegram API	WhatsApp API	Discord API
Plataforma	Multiplataforma	Multiplataforma	PC, móvil y web
Base de usuarios	200 millones de usuarios activos mensuales	2 mil millones de usuarios activos mensuales	Más de 140 millones de usuarios activos mensuales
Lenguajes compatibles	Compatible con varios lenguajes de programación como Python, Java, C#, PHP, Ruby, Swift, etc. Además.	Ccon diferentes lenguajes de programación como Java, Python, C#, entre otro	Compatible con varios lenguajes de programación populares como JavaScript, Python, C#, Java, Ruby, Go, entre otros.

Herramienta	Telegram API	WhatsApp API	Discord API
Sistemas operativos compatibles	Compatible con diferentes sistemas operativos como Windows, MacOS, Linux, iOS y Android	Compatible con diferentes plataformas como Android, iOS, web y ordenadores de escritorio.	Compatible con diferentes sistemas operativos como Windows, MacOS, Linux, y tiene una amplia variedad de herramientas y bibliotecas de desarrollo disponibles.
Seguridad	Telegram utiliza el protocolo MTProto para garantizar la seguridad de las comunicaciones y la privacidad de los usuarios.	La API de WhatsApp utiliza encriptación de extremo a extremo para garantizar la privacidad y la seguridad de los mensajes.	Utiliza autenticación basada en token para garantizar que solo las aplicaciones autorizadas pueden acceder a la API. También cuenta con medidas de seguridad adicionales, como la verificación de la dirección IP del servidor
Costo	La API de Telegram es totalmente gratuita.	Las primeras 1000 conversaciones son gratis, el costo es de $0.06 cada conversación por empresa y $0.02 por usuario.	La API de Telegram es totalmente gratuita.

Tabla 14 - Comparativa entre Telegram API, WhatsApp API y Discord API *[13] [87] [88]*

Herramienta	Telegram API	WhatsApp API	Discord API
Facilidad de uso	✓	✓	✓
Flexibilidad	✓	✗	✓
Documentación	✓	✓	✓
Requiere verificación	✗	✓	✗

Herramienta	Telegram API	WhatsApp API	Discord API
Acceso a mensajes privados	✓	✗	✓
Uso de Bots	✓	✓	✓
Multiplataforma	✓	✓	✓
Mensajería ilimitada	✓	✗	✗
Soporte de medios y archivos	✓	✓	✓
Cifrado	✓	✓	✓
Soporte de grupos de chat	✓	✓	✓
Envío masivo	✓	✓	✗
Gratuita	✓	✗	✓

Una vez evaluada cada una de estas herramientas de mensajería, se ha decidido el uso de Telegram API debido a que ofrece una amplia gama de funcionalidades, siendo una plataforma segura, privada y gratuita. En la siguiente imagen se muestra el uso del API para el envío de mensajes a un grupo de Telegram.

```python
class TelegramBot():
    def __init__(self):
        self._token= "5676698504:AAEbOC1YEW1j7_flySsn3XmZlu8yk_NsFow"
        self._group= "-1001821517613"
        self._channel= "-1001821517613"

    def get_me(self):
        url= f"https://api.telegram.org/bot{self._token}/getme"
        response=requests.get(url)
        if response.status_code==200:
            salida =json.loads(response.text)
            return salida
        return None

    def get_update(self):
        url= f"https://api.telegram.org/bot{self._token}/getUpdates"
        print(url)
        response=requests.get(url)
        if response.status_code==200:
            salida =json.loads(response.text)
            return salida
        return None

    def mensagge_to_group(self, message):
        url= f"https://api.telegram.org/bot{self._token}/sendMessage"
        data={"chat_id":self._group, "text": message}
        max_attempts = 3
        attempt = 0
        while attempt < max_attempts:
            attempt += 1
            try:
                response=requests.post(url, data=data)
                if response.status_code==200:
                    salida= json.loads(response.text)
                    return salida
                return None
            except requests.exceptions.RequestException as e:
                send_message(f"Error en la conexión a Telegram (intento {attempt}/{max_attempts}): ", "red")
                print(f"Error en la conexión a Telegram (intento {attempt}/{max_attempts}): ", e)
        return None
```

Fig. 13. Script de configuración de mensajería con el servicio de TELEGRAM

Fuente: Elaboración propia

```
def envio_masivo(data):
    tiempo=datetime.datetime.now()
    hora=tiempo.time().strftime("%H:%M:%S")
    if men_envio.query.filter((men_envio.id_paquete==data.id_a) & (men_envio.fecha==datetime.date.today())).first() :
        send_message('El mensaje ya ha sido enviado con anterioridad','blue')
        #print("el mensaje ya ha sido enviado con anterioridad")
    else:
        listado=buscar_lista(data.id_a)
        men ="Se detecto la siguiente ip anómalo: {}\nId del paquete: {}\nHostname: {}\nFue detectada por: {} \nEl cual corresponde a:\n{}".format(data.analisis.ip_analisis,data.id_a,data.analisis.hostname,data.analisis.de_por,listado)
        telegram_bot.mensagge_to_group(men)
        send_message("mensaje enviado","blue")
        #print("mensaje enviado")
        new_mensaje=men_envio(data.id_a,hora,datetime.date.today())
        db.session.add(new_mensaje)
        db.session.commit()
```

Fig. 14.Script de envío de mensajes a Telegram

Fuente: Elaboración propia

2.5.1.4 Despliegue

Se procede a poner en práctica el algoritmo en un entorno controlado, de tal manera que pueda clasificar efectivamente los paquetes.

```
El paquete esta limpio
El paquete esta limpio
El paquete esta limpio
El paquete esta limpio
Ambas ips son de la red local
El paquete esta limpio
El paquete esta limpio
El paquete esta limpio
El paquete esta limpio
El paquete esta limpio
El paquete esta limpio
El paquete esta limpio
El paquete esta limpio
El paquete esta limpio
El paquete esta limpio
El paquete esta limpio
El paquete esta limpio
El paquete esta limpio
El paquete esta limpio
El paquete esta limpio
El paquete esta limpio
El paquete esta limpio
El paquete esta limpio
```

Fig. 15. Salida por consola del análisis de paquetes

Fuente: Elaboración propia

2.5.2 Elaboración del Dashboard

2.5.2.1. Planificación

Este proyecto propone desarrollar un dashboard interactivo para visualizar los paquetes anómalos recolectados en el escaneo de la red. El propósito del dashboard es proporcionar una representación gráfica y fácil de interpretar de los datos recopilados por el sniffer, lo que permite a los usuarios interactuar y explorara de manera eficiente la información recolectada, proporcionándole una mejor experiencia.

El dashboard está diseñado para satisfacer las necesidades de diferentes tipos de usuarios, como los siguientes:

- Analistas de seguridad Informática
- Administrador de red
- Desarrolladores de software
- Investigadores de ciberseguridad
- Departamentos de seguridad de la información en diversas organizaciones.
- Empresas de seguridad cibernética y protección de datos.
- Usuarios comunes.
- Administradores de áreas específicas.

La elaboración de un dashboard eficaz requiere de una etapa inicial de maquetación, donde se plasman ideas y conceptos visuales. Para lograr esto, es importante contar con herramientas adecuadas que faciliten el proceso de creación de maquetas. En las siguientes tablas, se presentará una comparación entre diversas herramientas utilizadas con este propósito.

Tabla 15 -Comparativa de las principales características de Balsamiq, Figma y Sketch *[89] [90]*

Característica	**Balsamiq**	**Figma**	**Sketch**
Funcionalidades	Enfoque en la creación de bocetos y prototipos rápidos, interfaz de usuario simple y fácil de usar.	Enfoque en la colaboración en tiempo real, interfaz de usuario intuitiva y amplia gama de funcionalidades	Amplia gama de funcionalidades, como la creación de diseños vectoriales, la colaboración en tiempo real y la integración con otras aplicaciones y servicios
Facilidad de uso	Muy fácil de usar, incluso para principiantes	Fácil de usar, pero tiene una curva de aprendizaje más pronunciada que Balsamiq	Fácil de usar, pero tiene una curva de aprendizaje más pronunciada que Balsamiq

Característica	Balsamiq	Figma	Sketch
Personalización	Opciones de personalización limitadas	Muy personalizable	Muy personalizable
Creación de prototipos	Sin funciones de creación de prototipos integradas	Funciones básicas de creación de prototipos	Funciones avanzadas de creación de prototipos
Exportación	Puede exportar wireframes y prototipos en varios formatos, como PNG, JPG, PDF y HTML	Puede exportar wireframes y prototipos en varios formatos, como PNG, JPG, PDF y HTML	Puede exportar wireframes y prototipos en varios formatos, como PNG, JPG, PDF y HTML
Costo	Gratuito para uso personal, 99 $/año para uso profesional	Gratuito para uso personal, 12 $/mes para Figma Cloud, 19 $/mes para Figma Enterprise	99 $/año

Tabla 16 -Comparativa de características de Balsamiq, Figma y Sketch *[89] [90]*

Característica	Balsamiq	Figma	Sketch
Plan Gratuito	✓	✓	✗
Plan de Pago	✓	✓	✓
Fácil de usar	✓	✓	✓
Colaboración	✗	✓	✓
Exportación	✓	✓	✓

Evaluada estas herramientas de diseño de prototipo, se ha decidido utilizar Balsamiq debido a que es una herramienta fácil de usar y cuenta con una interfaz intuitiva que permite a los usuarios crear prototipo de manera rápida y eficiente.

En este proyecto, que utiliza el lenguaje Python, es necesario contar con una Liberia que nos permita manipular y analizar datos de manera eficiente. En las siguientes tablas, se presentará tres herramientas ampliamente utilizadas y sus características principales.

Tabla 17 -Comparativa de las principales características entre Pandas, NumPy y SciPy *[91] [92]*

Característica	Pandas	NumPy	SciPy
Facilidad de uso	Fácil de usar	Fácil de usar	Fácil de usar
Documentación	Completa	Completa	Completa
Estructuras de datos	Tablas	Arrays	Matrices

Tabla 18 -Comparativa entre Pandas, NumPy y SciPy *[91] [92]*

Característica	Pandas	NumPy	SciPy
Análisis de datos	✓	✗	✓
Manipulación de datos	✓	✓	✓
Limpieza de datos	✓	✗	✗
Integración con otras herramientas	✓	✓	✓
Código abierto	✓	✓	✓

Una vez analizadas las herramientas, se optó por el uso de Pandas para la manipulación de datos, debido a su manipulación de alto nivel, permitiendo el análisis de datos y contando con la estructura necesaria para limpiar los datos en bruto para que estos sean aptos para el análisis.

El punto clave del dashboard es permitir la visualización de los datos de manera clara y eficaz al usuario. En este sentido, existen varias bibliotecas de Python para visualizar datos, entre las que encontramos Matplotlib, Chart.js y Plotly, A continuación, se muestra una comparativa de estas herramientas.

Tabla 19 -Comparativa de las principales características entre Matplotlib,Chart.js y Plotly *[93] [94] [95]*

Característica	Matplotlib	Chart.js	Plotly
Interfaz de usuario	No amigable para el usuario	Interactivo y amigable con el usuario.	Interactivo y amigable para el usuario
Estética predeterminada	Básica	Mejorada y más atractiva	Mejorada y más atractiva

Característica	Matplotlib	Chart.js	Plotly
Personalización	Muy personalizable	Muy personalizable	Algo limitado en comparación con Matplotlib
Gráficos dinámicos	Sí, a través de animaciones	Si, con varias animaciones	Sí, con una amplia variedad de opciones
Integración con otros lenguajes	Sí, con herramientas como PyQt o Tkinter	Sí, con herramientas como Flask o Django	Sí, con herramientas como Flask o Django
Interacción con el usuario	Limitada	Limitada	Alta
Documentación y soporte	Amplia documentación y comunidad activa	Amplia documentación y comunidad activa	Amplia documentación y comunidad activa

Tabla 20 - Comparativa entre Matplotlib,Chart.js y Plotly *[93] [23] [95]*

Característica	Matplotlib	Chart.js	Plotly
Interfaz de usuario amigable	✗	✓	✓
Estética predeterminada atractiva	✗	✓	✓
Personalización avanzada	✓	✓	✗
Gráficos dinámicos	✓	✓	✓
Integración con otros lenguajes	✓	✓	✓
Documentación y soporte amplios	✓	✓	✓
Gráficos en 3D	✓	✗	✓
Integración con dashboards	✓	✓	✓
Uso de datos en tiempo real	✓	✗	✓

Una vez analizada cada una de estas herramientas, se ha decidido el uso de Maptplotlib para la generación de gráficas estadísticas en la documentación pdfy chart.js para las gráficas dinámicas mostradas en el dashboard, debido a que ambas son bibliotecas visuales con una amplia variedad de gráficas, y su compatibilidad con el entorno al proyecto a desarrollar.

Tabla 21 - Comparativa de las principales características entre ReportLab PyPDF2 y FPDF *[25] [96] [97]*

Característica	ReportLab	PyPDF2	FPDF
Soporté de lenguajes	Python	Python	Python
Soporté de formatos	PDF	PDF	PDF
Documentación	Completa	Completa	Completa

Tabla 22 -Comparativa entre ReportLab PyPDF2 y FPDF *[25] [96] [97]*

Característica	ReportLab	PyPDF2	FPDF
Soporte de imágenes	✓	✓	✓
Soporte de fuentes	✓	✓	✓
Soporte de tablas	✓	✓	✓
Soporte de gráficos	✓	✗	✗
Soporte de hipervínculos	✓	✓	✓
Soporte de Unicode	✓	✓	✓

Tras analizar estas herramientas, se optó por usar ReportLab debido a su facilidad de uso y los elementos que este proporciona para la elaboración de documentos PDF. De igual manera se analizará diferentes herramientas que sirvan para la generación de archivos xlsx.

Tabla 23.-Comparativa de las principales características entre XlsxWrite, Openpyxl y Pandas *[26] [98] [20]*

Característica	XlsxWrite	Openpyxl	Pandas
Soporte de lenguajes	Python	Python	Python
Formato	.xlsx	xlsx	xlsx
Rendimiento	Alto	Moderado	Variado (depende del tamaño del DataFrame)
Documentación	Completa	Completa	Completa
Integración con otras bibliotecas	Varias	Varias	Sí (integración con NumPy, Matplotlib, etc.)

Tabla 24.- Comparativa de características entre XlsxWrite, Openpyxl y Pandas *[26] [98] [20]*

Característica	XlsxWrite	Openpyxl	Pandas
Soporte de graficas	✓	✗	✗
Soporte de imágenes	✓	✗	✗
Formatos de celda personalizados	✓	✓	✗
Autofiltros	✓	✓	✗
Soporte de hipervínculos	✓	✓	✓

Analizadas etas herramienta se optó por el uso de XlsxWrite para la generación de archivos de extencion .xlsx. De la misma manera se utilizará las siguientes librerías diseñadas para integrarse específicamente a Flask:

- Flask_Login.

- Flask_socketio
- Flask_wtf
- Flask-Mail
- Email-validator

Mediante el escaneo de la red se recolectarán los paquetes pertenecientes al mismo host establecido con anterioridad, entre los datos que se tomaran en cuenta en la captura son:

- Tiempo de la captura (hora y fecha)
- Tipo de protocolo
- Dirección de origen
- Puerto de origen
- Dirección de destino
- Puerto de destino.

La dirección IP del paquete será analizado por ApiVoid, la cual nos retornará lo siguiente:

- Cantidad de detecciones
- Motores de análisis que han detectado
- País
- Continente
- Región
- Ciudad
- Latitud
- Longitud
- Isp
- Es proxi
- Es web proxy
- Es VPN
- Es hosting
- Es Tor

La información se recolecta y clasifica según los parámetros establecidos en el proyecto, posterior a esto serán almacenados en la base de datos.

2.5.2.1.1. Estructura del proceso de análisis de paquetes de red

Definimos el proceso que se lleva a cabo en el escaneo de red, desde el momento que se captura el paquete, se lo analiza y se lo clasifica según los resultados del análisis, lo cual está descrito de mejor manera en el siguiente diagrama:

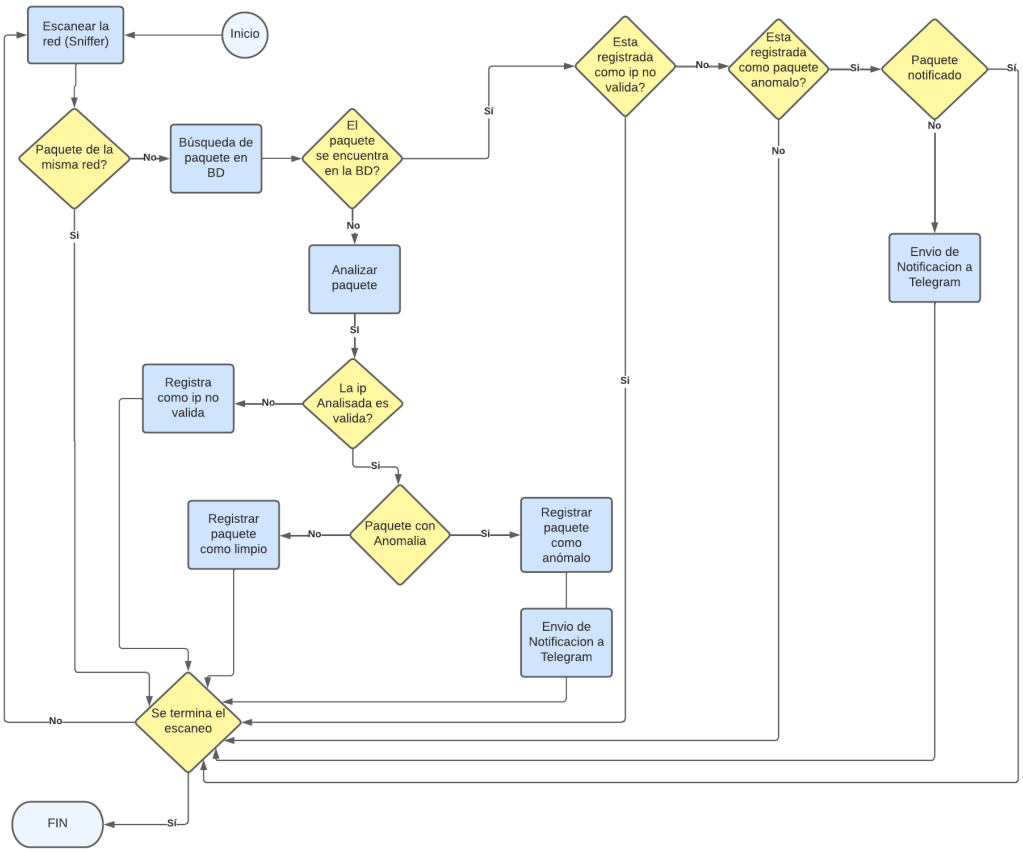


Fig. 16. Diagrama de proceso de captura y clasificación de paquete

Fuente: Elaboración propia

2.5.2.1.2 Arquitectura del Sistema

En la siguiente imagen se muestra la arquitectura de cómo se implementa el sistema dentro de una organización, este estará dentro de la red a monitorear para poder capturar paquetes, de la misma manera se mencionan las partes principales del algoritmo desarrollado.

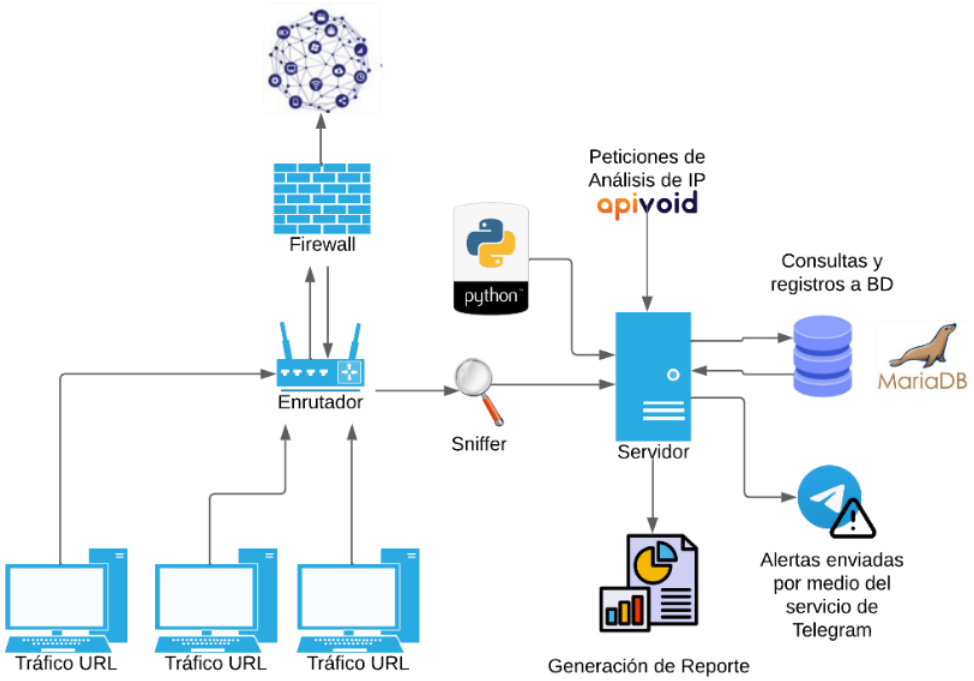


Fig. 17. Arquitectura del sistema

2.5.2.2. Creación de borrador

El dashboard se desarrolla en un sistema web local, el cual contará con tres páginas principales, el Home, Escáner y Reporte, a su vez la página Home constará con tres sub páginas, página de paquete limpio, paquete anómalo y página de mensajes enviados a Telegram. Tanto la subpágina de paquete limpio como el anómalos tendrán una sub página cada uno correspondiente a detalle de paquete limpio y detalle de paquete anómalo

Las sub páginas mensajes enviados a Telegram tendrá la misma sub página qué paquetes anómalos, debido a que esta mostrará la misma información. Con respecto a la página principal Reporte constara con una subpágina denominada generar reporte, en resumen, el dashboard constara con dos páginas principales y seis subpáginas respectivamente, las cuales se detalla de mejor manera en la siguiente gráfica:

Esquema Web de ZEUSniffer

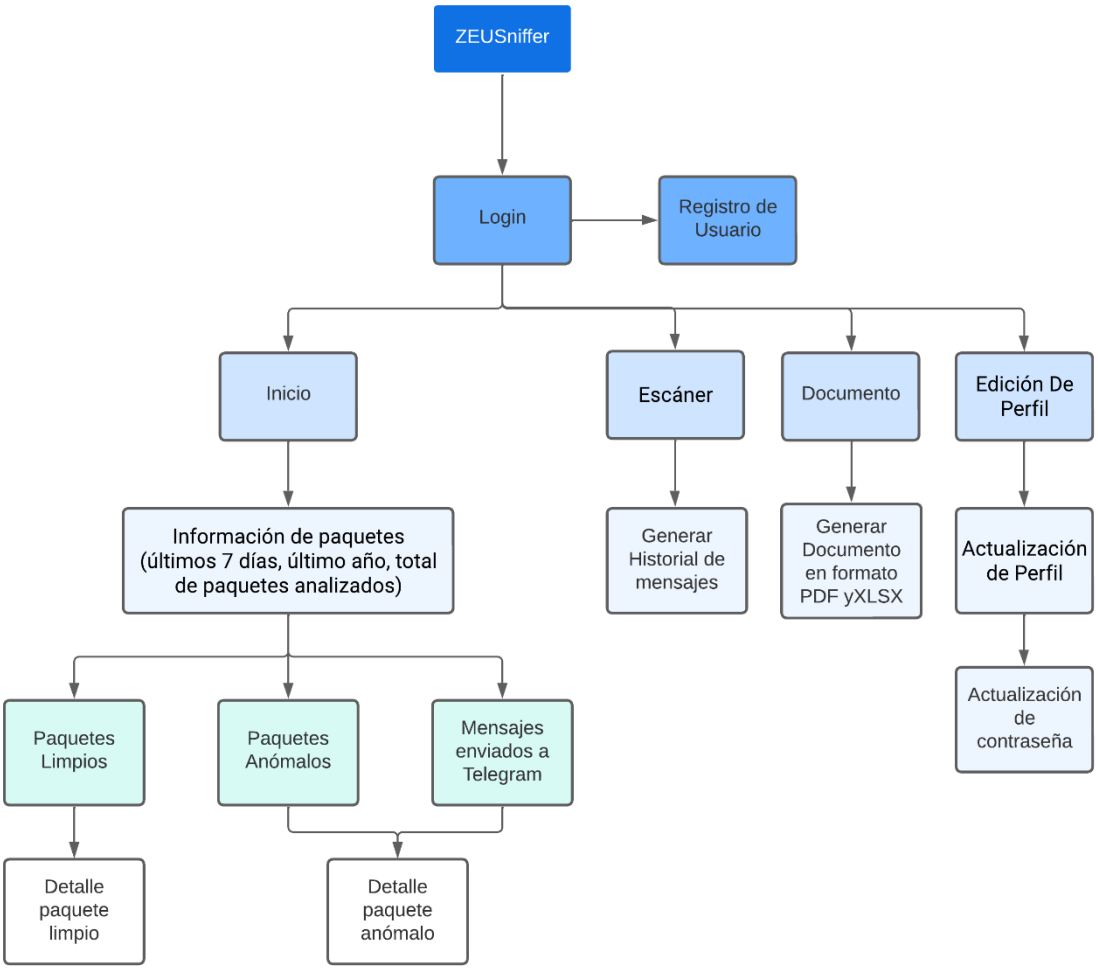


Fig. 18. Esquema web

Fuente: Elaboración propia

Se realiza un Wireframes (Esquema de página) del dashboard para determinar las secciones, elementos, información, ingreso de datos, imágenes, etc. Las cuales contendrán cada una de las páginas establecidas con anterioridad, para esto utilizaremos la herramienta Balsamiq Wireframes, con la cual elaboraremos este esquema.

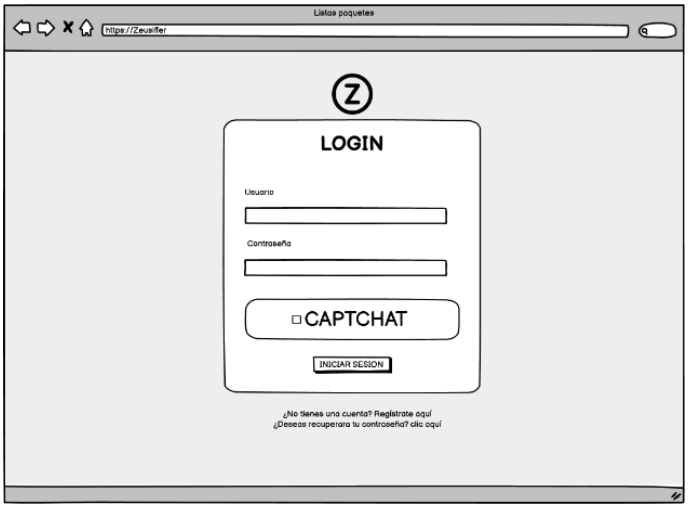


Fig. 19 . Vista del modelo de Login

Fuente: Elaboración propia

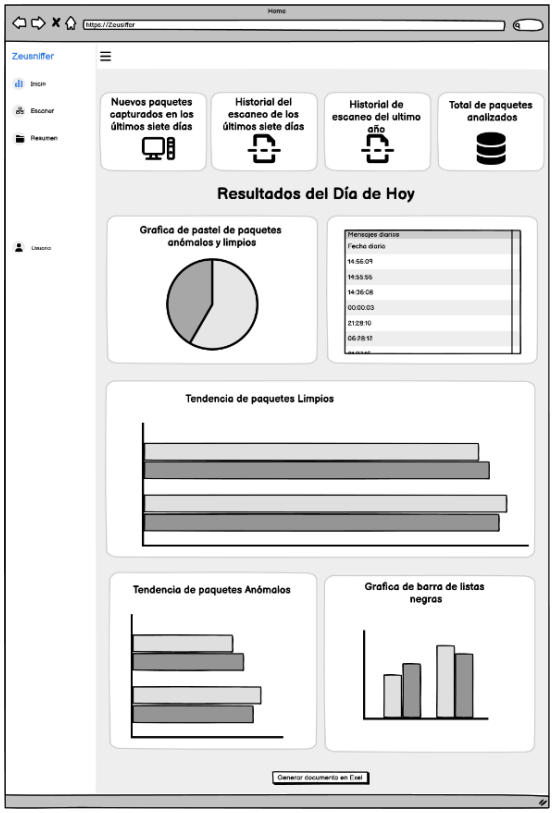


Fig. 20 . Vista de modelo de página Home

Fuente: Elaboración propia

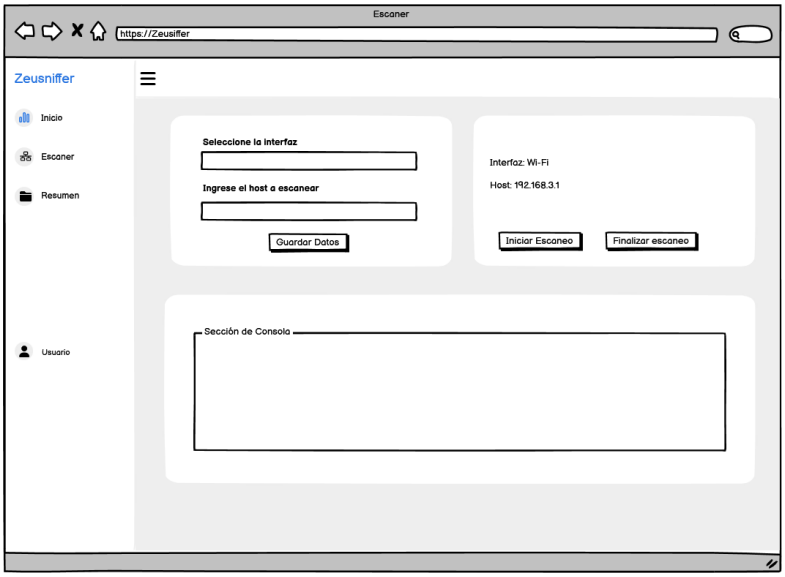


Fig. 21 . Vista de modelo de página Escáner

Fuente: Elaboración propia

Fig. 22 .Vista de modelo de página De Documentación visual

Fuente: Elaboración propia

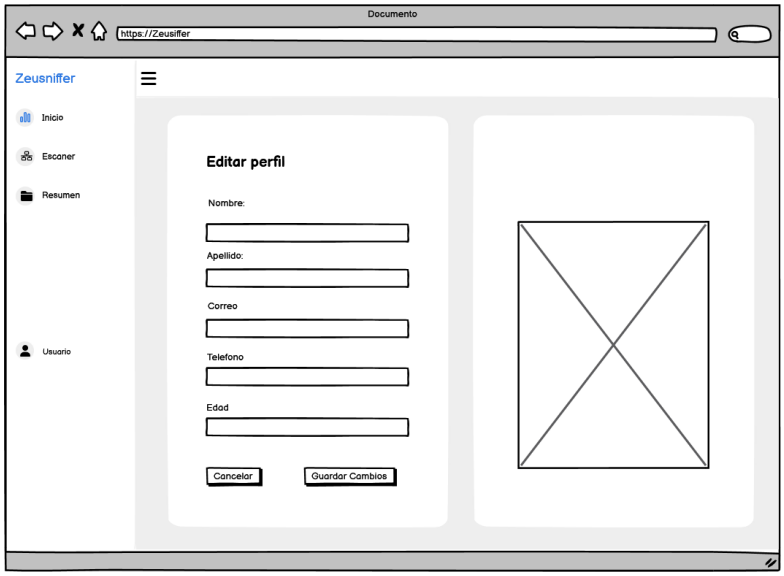


Fig. 23. Vista de modelo de página De Edición de Perfil.

Fuente: Elaboración propia

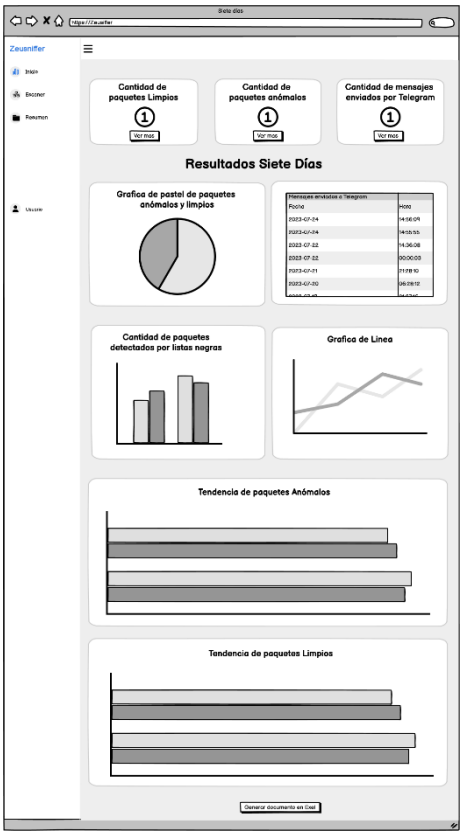


Fig. 24. Vista de modelo de página de datos y estadística (últimos siete días).

Fuente: Elaboración propia

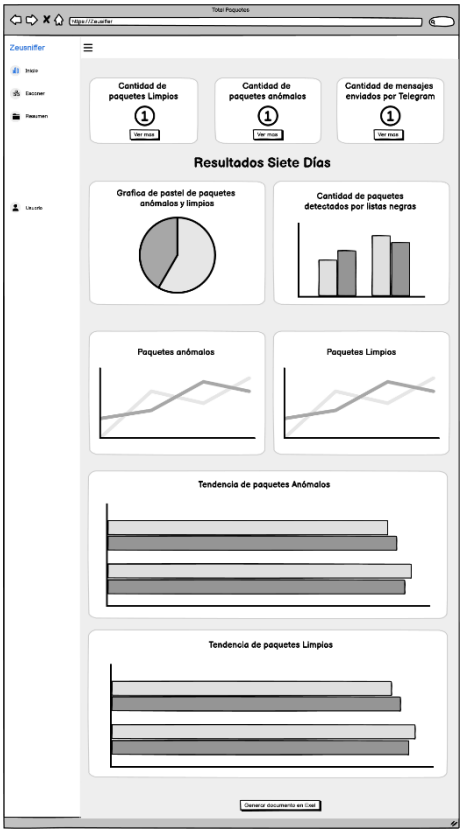


Fig. 25. Vista de modelo de página de datos y estadística.

Fuente: Elaboración propia

Fig. 26. Vista de modelo de página de historial de paquetes anómalos y limpios

Fuente: Elaboración propia

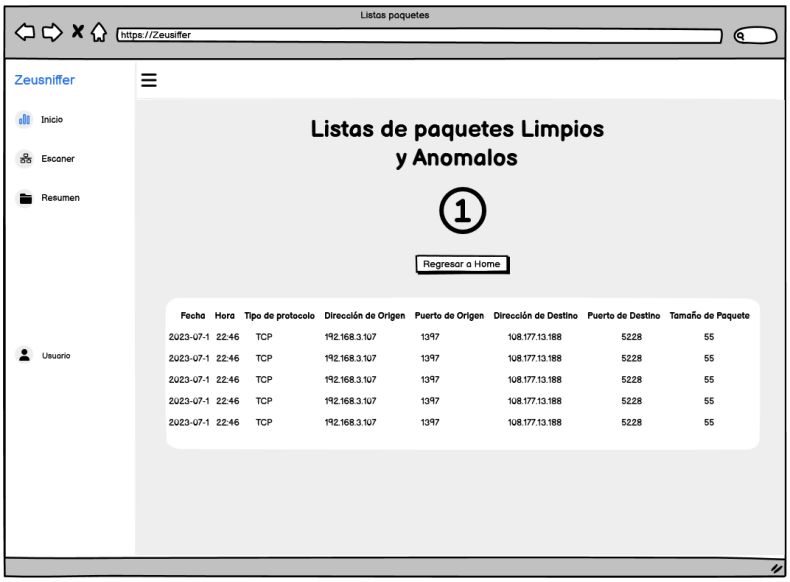


Fig. 27. Vista de modelo de página de paquetes anómalos y limpios

Fuente: Elaboración propia

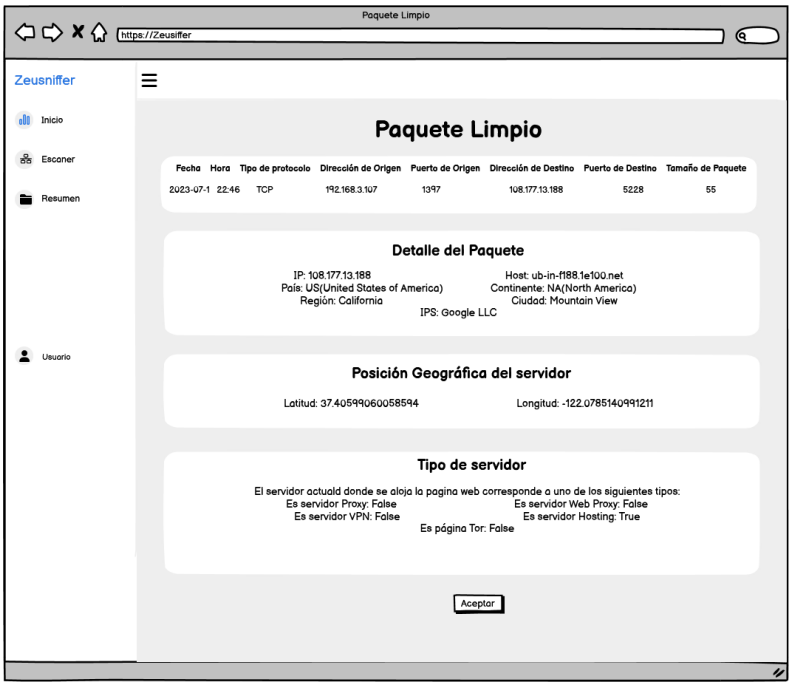


Fig. 28. Vista de modelo de página de detalle de paquete limpios

Fuente: Elaboración propia

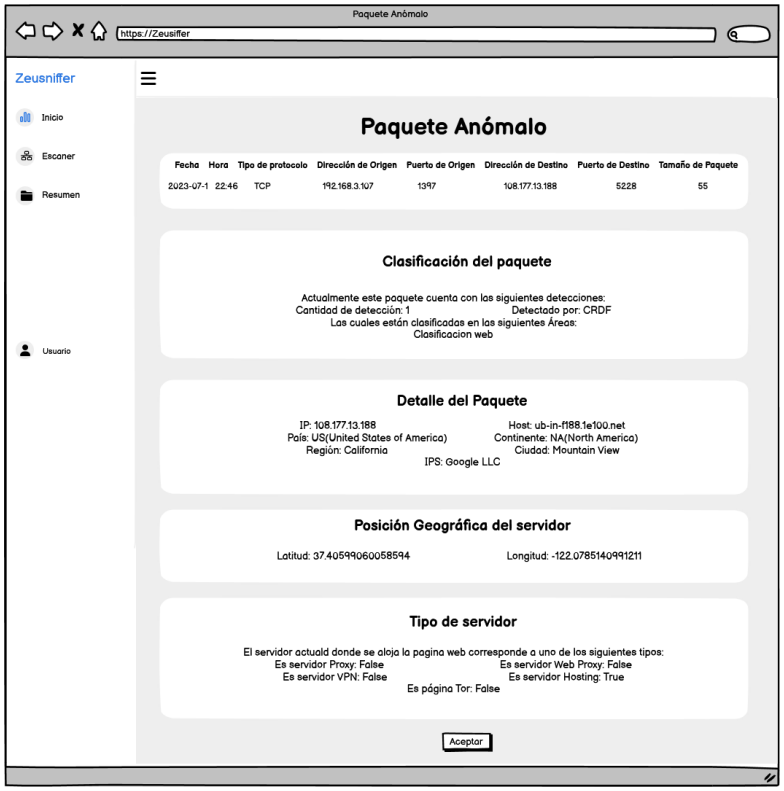


Fig. 29. Vista de modelo de página de detalle de paquete anómalo

Fuente: Elaboración propia

De la misma manera diseñamos la estructura que contendrá el mensaje que será enviado al grupo en donde se encuentran los administradores notificándole la detección de un paquete anómalo.

Se detecto la siguiente ip anómalo: 157.240.6.53

Id del paquete: 21

Hostname: whatsapp-cdn-shv-01-bog1.fbcdn.net

Fue detectada por: PlonkatronixBL

El cual corresponde a:

['Escaneo de puertos-Ataque de fuerza bruta-DOS, Escaneo de vulnerabilidades, Phishing-Abuso-Estafa, Spam, Tor']

Otro punto a tomar en cuenta en este borrador es la paleta de colores, el cual es crucial para brindar un ambiente de tranquilidad y seguridad [99]. Se ha seleccionado para este proyecto colores suaves y acogedores, como verde agua, el azul cielo, el gris suave y blanco, para crear un ambiente visualmente atractivo he equilibrado.

Estos colores reflejen la tranquilidad y la estabilidad, trasmitiendo una sensación de confianza y serenidad al usuario. En el siguiente cuadro describiremos los colores a utilizar con su respectiva característica.

Tabla 25 -Paquete de colores *[99]*

Nombre	Código	Descripción	Color
Azul profundo	#1783DB 23,131,219	Confianza y Seguridad	
Gris Suave	#F5F5F5 245,245,245	Neutral y Equilibrado	
Blanco	#FFFFFF 255,255,255	Pureza y claridad	
Verde Esmeralda	#00CC66 0,204,102	Serenidad y Estabilidad	
Rojo	#DC2626 220,38,38	Alertas importantes	
Naranja Brillante	#FFC00 255,204,0	Alertas menores	

Nombre	Código	Descripción	Color
Amarillo Brillante	#FFFB00 255,251,0	Alertas moderadas	

El uso de paletas de colores también tiene un impacto positivo en la usabilidad y la accesoriedad del dashboard. En resumen, la elección cuidadosa de la papeleta de colores es un aspecto clave en el diseño de un dashboard efectivo, y es fundamental para lograr un ambiente de tranquilidad y seguridad en el dashboard sensación.

2.5.2.3. Diseño

Diseño y Creación de base de datos

Para almacenar la información recolectada durante el escaneo se procede a crear la siguiente base de datos, la cual contendrá tablas para la información de paquetes limpios como anómalos, tomando una estructura de base de datos no relacional, debido a que no todas las tablas de la base de datos están relacionadas.

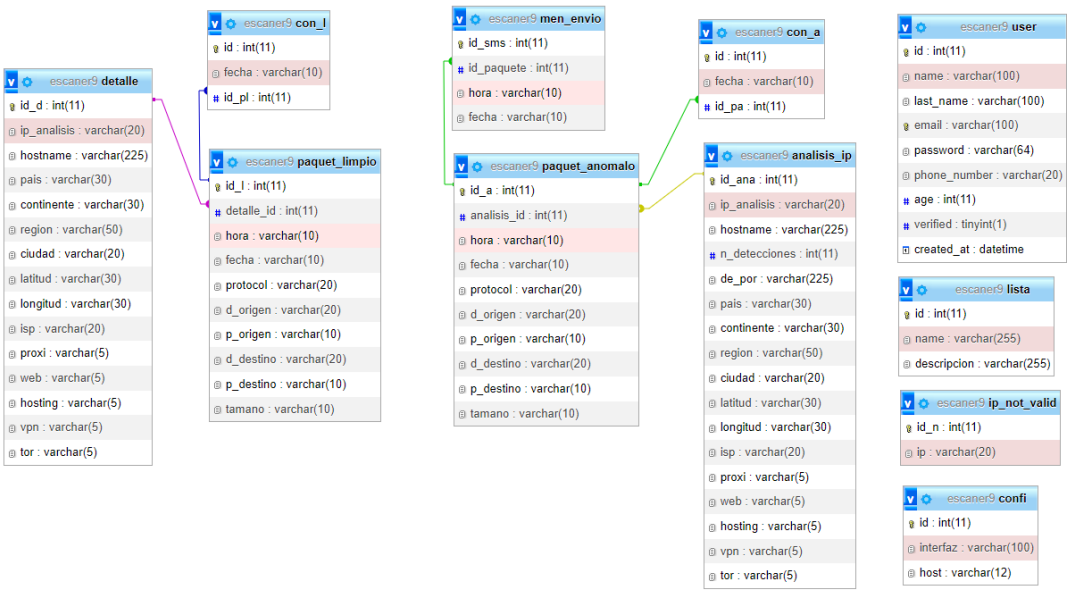


Fig. 30. Base de datos de Zeusniffer

Fuente: Elaboración propia

Creación de dashboard

Procederemos a desarrollar el dashboard, haciendo uso del borrador y los procedimientos especificados en el punto anterior. A continuación, se mostrará el resultado final de cada una de las páginas del dashboard.

Página Login

Esta página corresponde al inicio de sesión seguro. Para acceder a ella, es necesario proporcionar las credenciales asociadas a tu cuenta. Además, como medida adicional de seguridad, se requiere completar un captcha para garantizar que eres un usuario legítimo y no un bot automatizado.

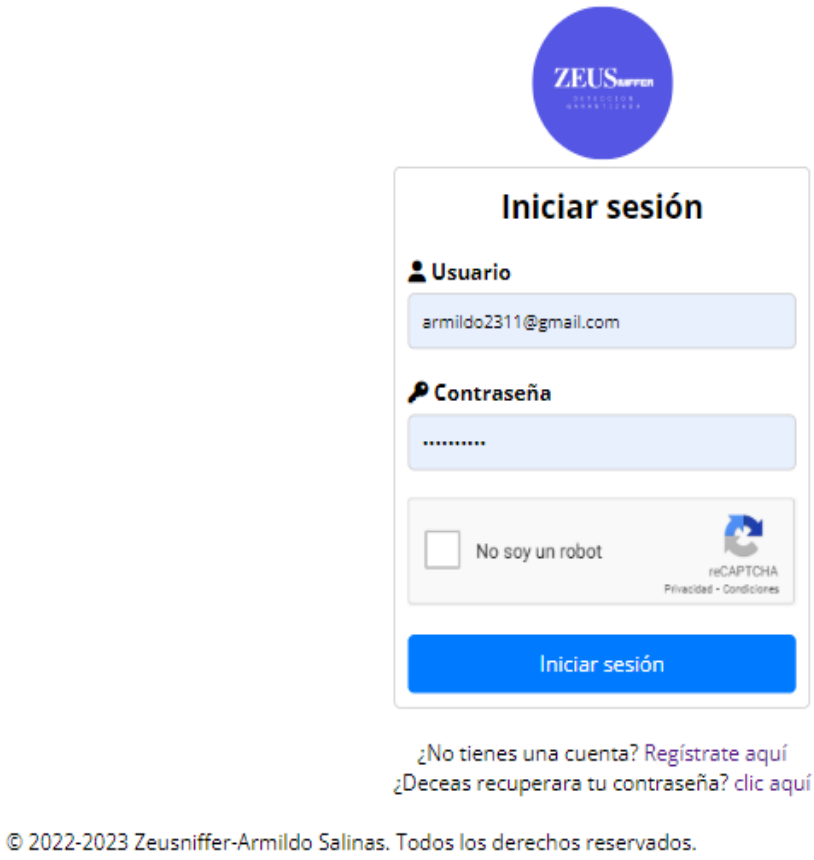


Fig. 31. Pagina Login de Zeusniffer

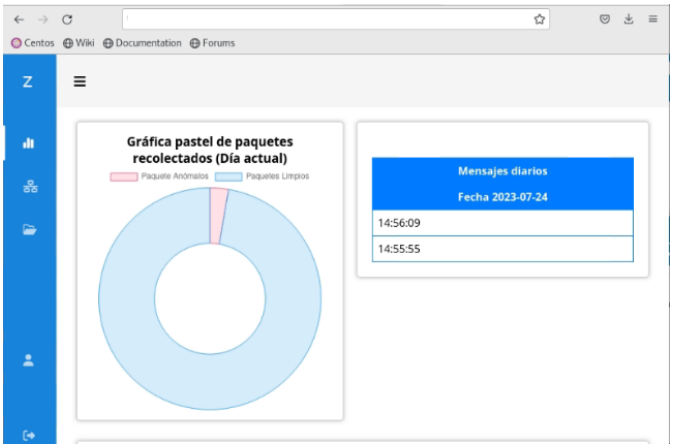
Fuente: Elaboración propia

Página Home

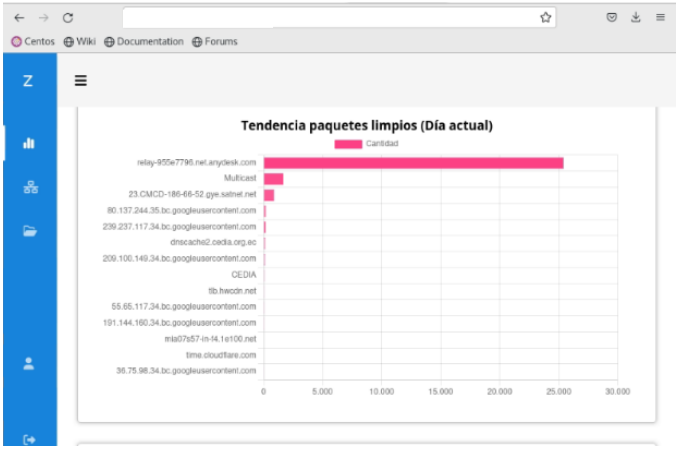
En esta página se presenta la información correspondiente al escaneo del día.

a)

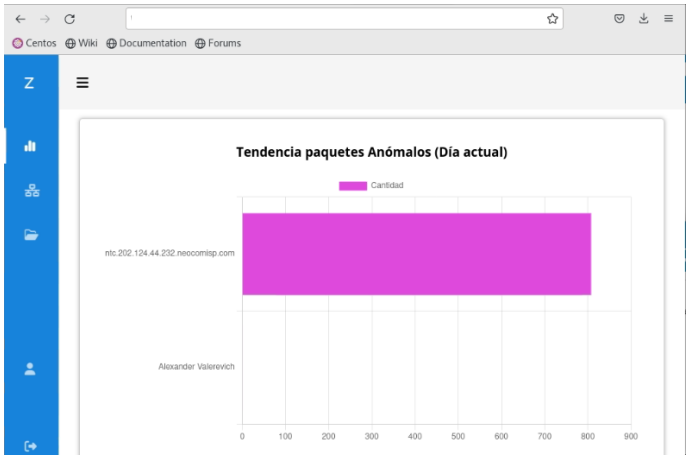
b)



c)



d)



e)

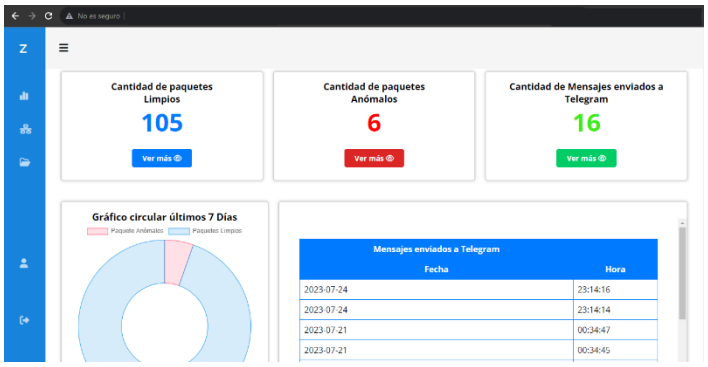
Fig. 32. Página home de Zeusniffer (a) (b) (c) (d) (e)

Fuente Elaboración propia

Página últimos siete días

En esta página se presenta la información de los nuevos paquetes capturados en los últimos 7 días.

a)



b)

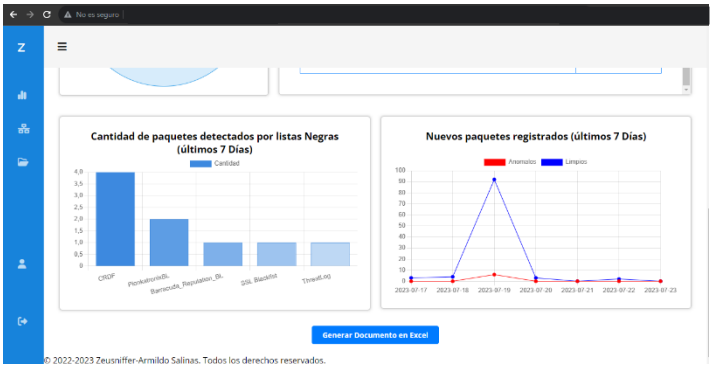


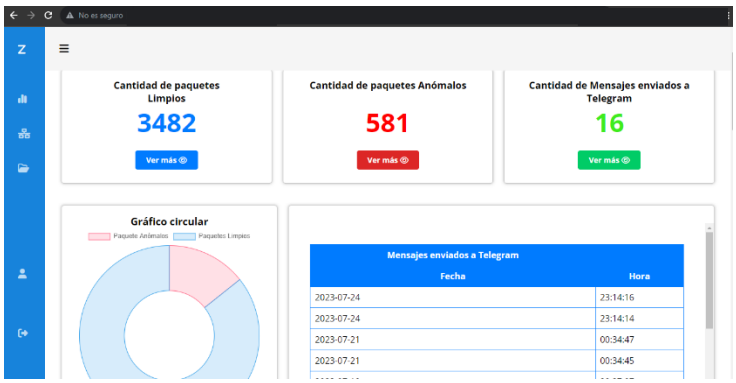
Fig. 33. Pagina últimos siete días (a) (b)

Fuente: Elaboración propia

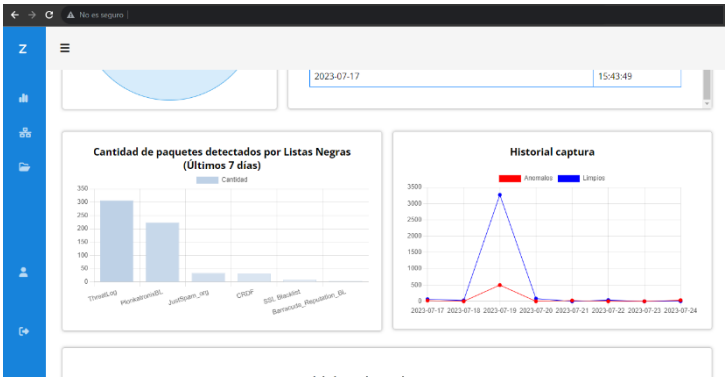
Página historial últimos siete días

En esta página se presenta la información del historial de escaneo de los últimos 7 días.

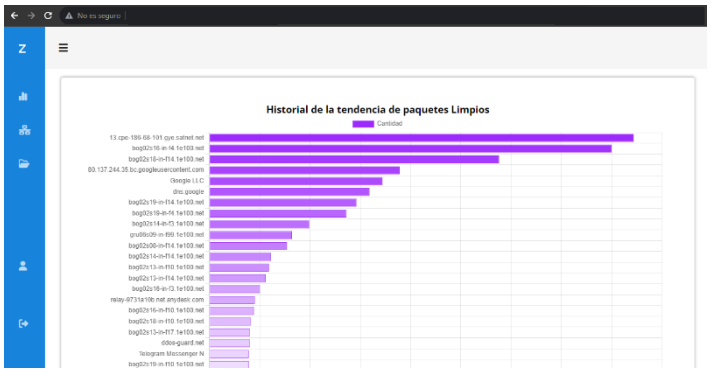
a)



b)



c)



d)

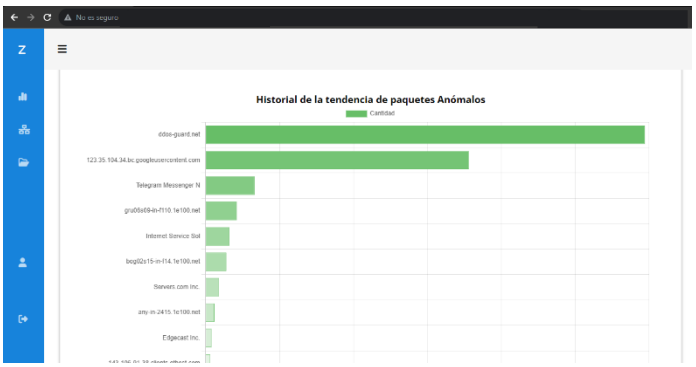


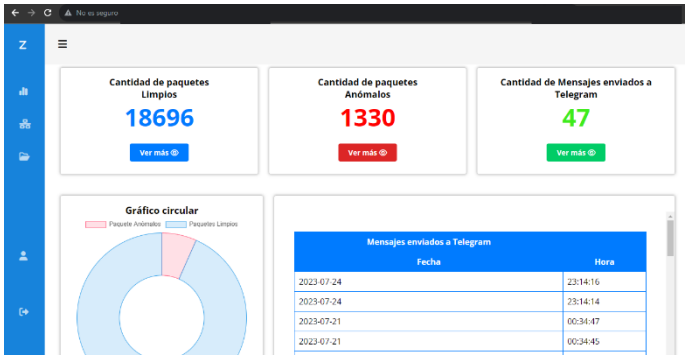
Fig. 34. Pagina historial de últimos siete días (a) (b) (c) (d)

Fuente: Elaboración Propia

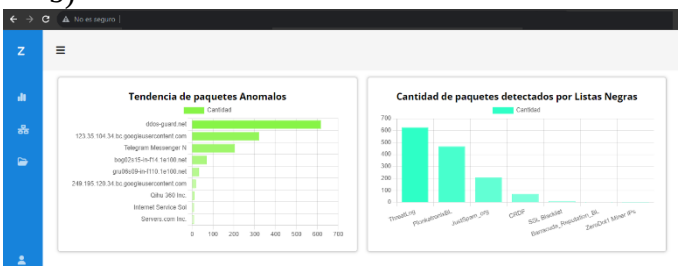
Página historial de paquetes

En esta página se presenta el historial de escaneo.

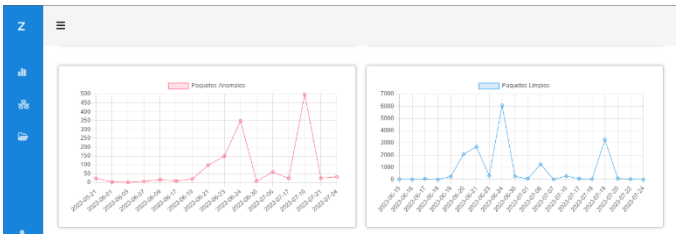
a)



b)



c)



d)

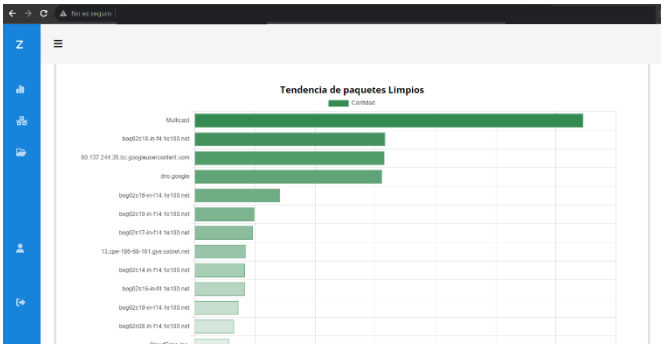


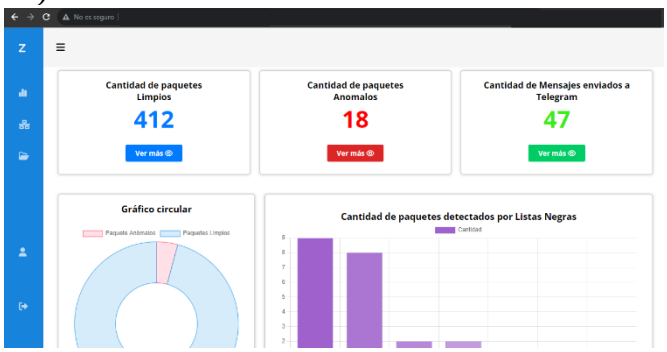
Fig. 35. Página de historial de Paquetes (a) (b) (c) (d).

Fuente: Elaboración propia

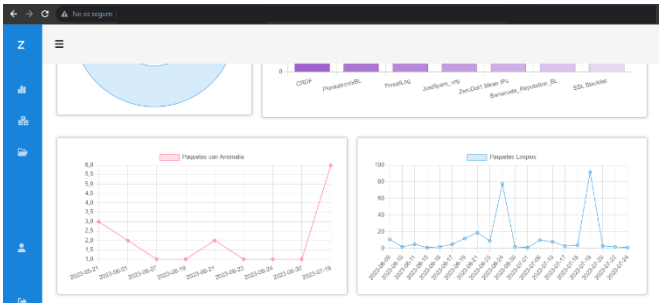
Página nuevos paquetes

Esta página se presenta la información referente a los nuevos paquetes.

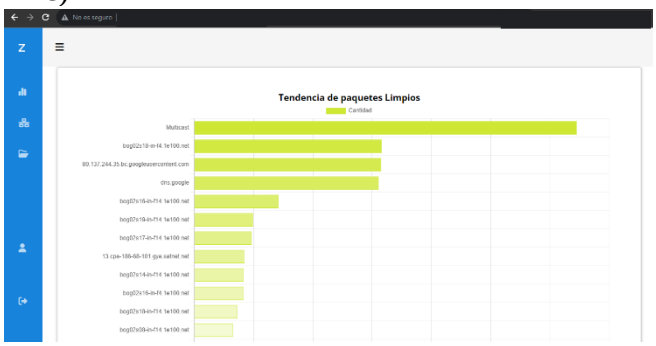
a)



b)



c)



d)

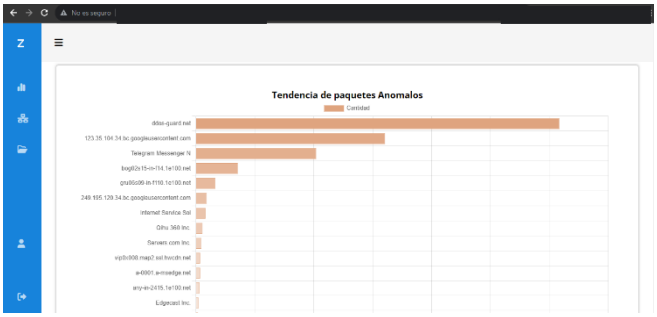


Fig. 36. Página de nuevos paquetes (a) (b) (c) (d).

Fuente: Elaboración propia

Página paquete limpio

En esta página se presenta el listado de los paquetes limpios capturados.

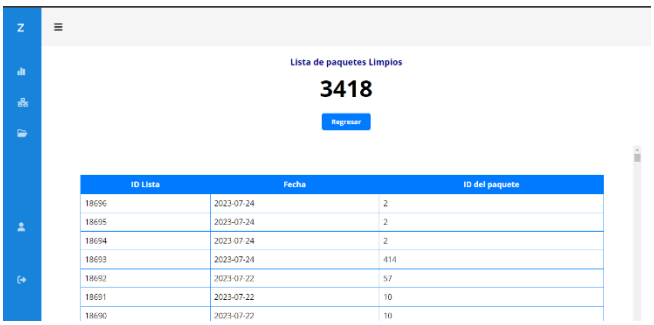


Fig. 37. Página de listado de paquetes limpios.

Fuente: Elaboración Propia

Página de listado de paquetes anómalos

Esta página muestra la lista de los paquetes capturados clasificados como anómalos.

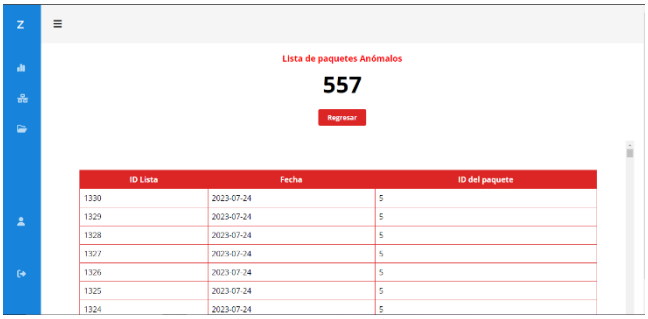


Fig. 38. Página de lista de paquetes clasificados como anómalos.

Fuente: Elaboración propia

Página de detalle de paquete limpio

En esta página se muestra el detalle del análisis de paquetes limpios.

a)

b)

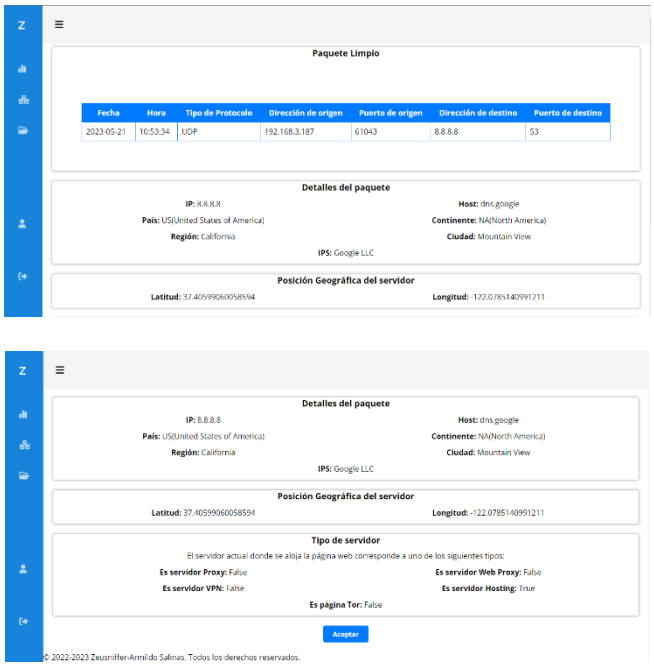


Fig. 39. Página de detalle de paquete limpio (a) (b)

Fuente: Elaboración propia

Página de detalle de paquete anómalo

En esta página se muestra el detalle del paquete categorizado como anómalo.

a)

b)

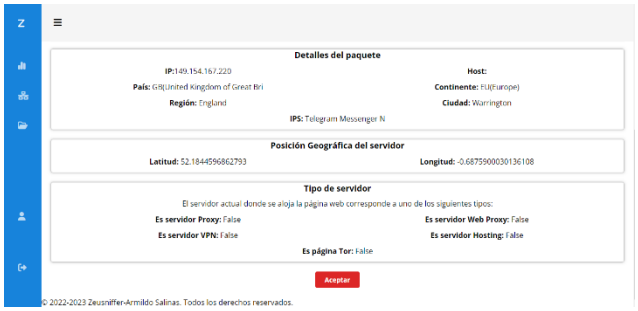


Fig. 40. Página de detalle de paquete anómalo (a) (b).

Fuente: Elaboración propia

Página de escaneo

En esta página se presenta la sección en donde podemos ingresar la interfaz de red junto al host de escaneo, además, nos permite poder iniciar y finalizar el escaneo.

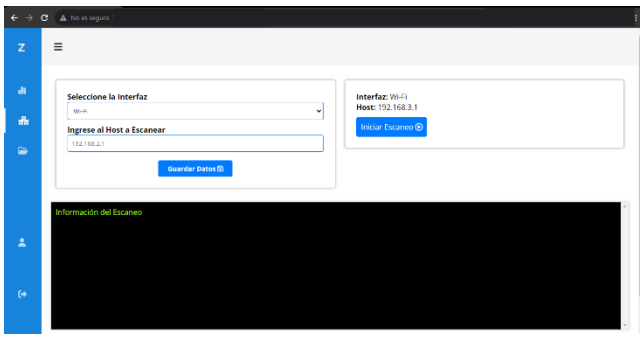


Fig. 41. Página de escaneo

Fuente: Elaboración propia

Página de Documentación

En esta página se puede generar la documentación de la información proveniente de los escaneos, tanto en PDF como Excel.

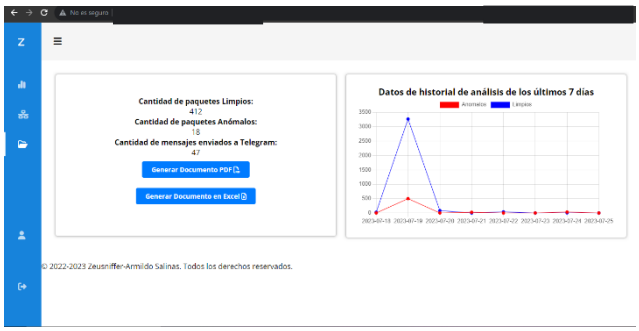


Fig. 42. Página de descarga de documentación.

Fuente: Elaboración propia

2.5.2.4. Freedback y aplicación de cambios

En este punto procederemos a ejecutar el dashboard y verificar si existen errores, a continuación, se presentará captura de su ejecución y visualización de eventos:

Inicio del escaneo

Se ejecuta el programa para iniciar el escaneo, se puede divisar en pantalla la información correspondiente a los paquetes analizados

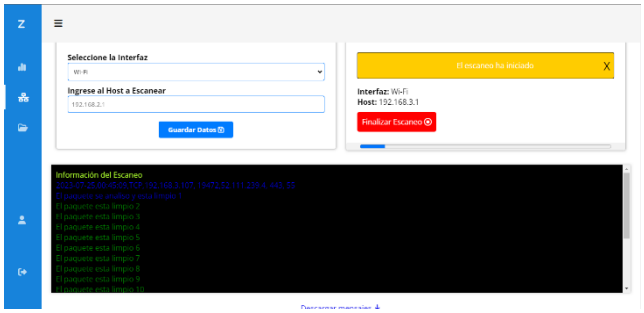


Fig. 43 . Inicio de escaneo.

Fuente: Elaboración propia

Finalización del escaneo

Se finaliza el escaneo, se puede divisar en pantalla como este ha finalizado y se muestra los últimos paquetes capturados junto a la frase “Finalizo Escaneo”.

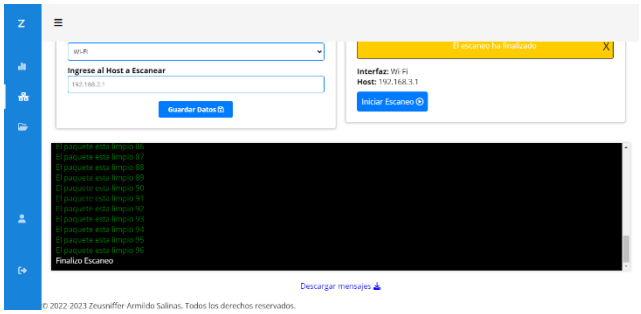


Fig. 44. Finalización de escaneo.

Fuente: Elaboración propia

Mensajes de escaneo

Dentro de la misma página se encuentra la opción de descargar la información mostrada en consola durante el escaneo, este se descargará en un archivo formato HTML, el cual se muestra a continuación.

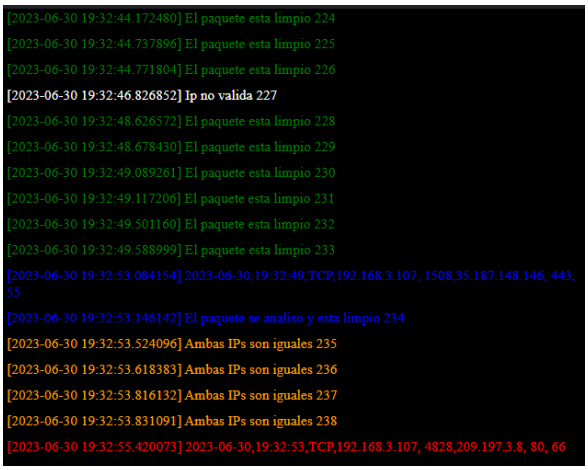


Fig. 45. Historial de mensajes de escaneo

Fuente: Elaboración propia

Alerta de detección de paquete anómalo

Dentro de Telegram se crea un nuevo grupo al cual denominamos alerta_infe, por medio de Telegram bot creamos un enlace que reciba los mensajes emitidos desde el aplicativo, para ser mostrado en el grupo.

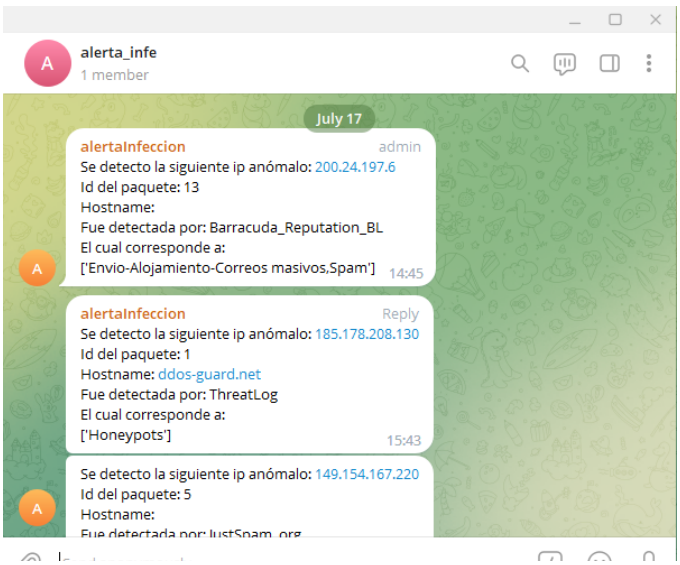


Fig. 46. Notificación recibida en Telegram

Fuente: Elaboración propia

Ejecución del algoritmo en sistema operativo Windows y Linux

Para la ejecución del algoritmo en conjunto con el dashboard desarrollado, se tienen que tener instaladas las librerías necesarias, posterior a esto identificar la interfaz de red que se usara para realizar el escaneo.

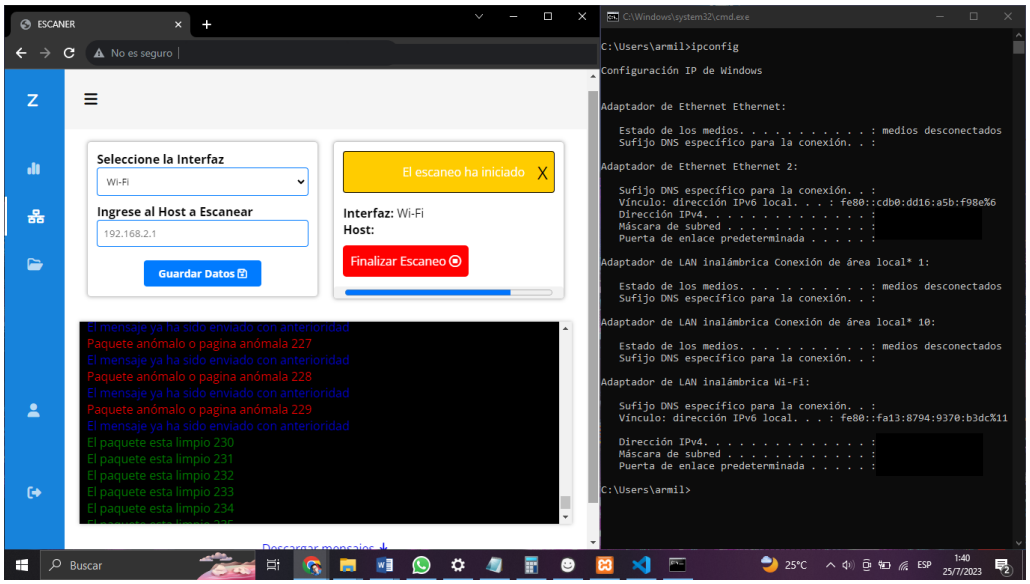


Fig. 48. Prueba del proyecto en sistema operativo Windows 10

Fuente: Elaboración Propia

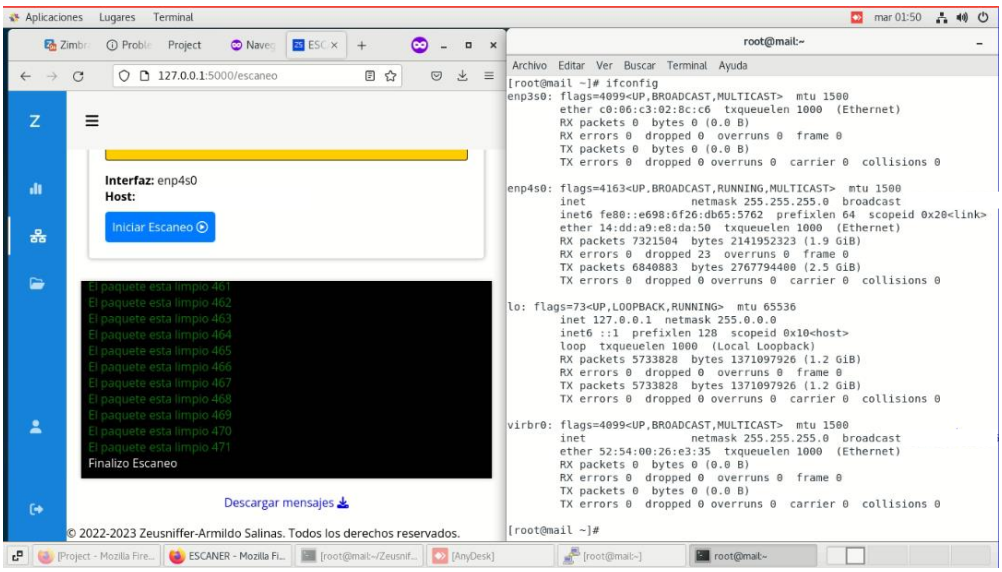


Fig. 47. Prueba del proyecto en sistema operativo Linux (CentOS 7)

Fuente: Elaboración propia

2.5.3. ISO/IEC 27032

Para llevar a cabo el proyecto de escaneo de red en la Universidad, se utilizará la metodología ISO/IEC 27032, que se enfoca en la ciberseguridad y proporciona un enfoque sistemático para la gestión de la seguridad de la información [40]. Esta metodología es altamente reconocida y utilizada en todo el mundo y se basa en los estándares de seguridad de la información de la norma ISO/IEC 27001. La metodología ISO/IEC 27032 consta de cuatro fases.

- Entendimiento de la Organización
- Análisis de Riesgo
- Plan de acción
- Implementación

2.5.3.1. Fase I: Entendimiento de la Organización

En esta fase de la metodología ISO 27032 [40], se busca obtener un conocimiento profundo de la organización, en este caso, la Facultad de Sistemas y Telecomunicaciones (FACSISTEL) de la Universidad Estatal Península de Santa Elena. Es necesario realizar un análisis exhaustivo de la infraestructura de red, los sistemas y las aplicaciones utilizadas en la facultad. Además, se debe comprender la estructura organizativa, los roles y responsabilidades del personal involucrado en la gestión y seguridad de la red. Este entendimiento permitirá identificar los activos de información críticos, los posibles puntos de vulnerabilidad y los riesgos asociados al tráfico URL en redes distribuidas de la facultad.

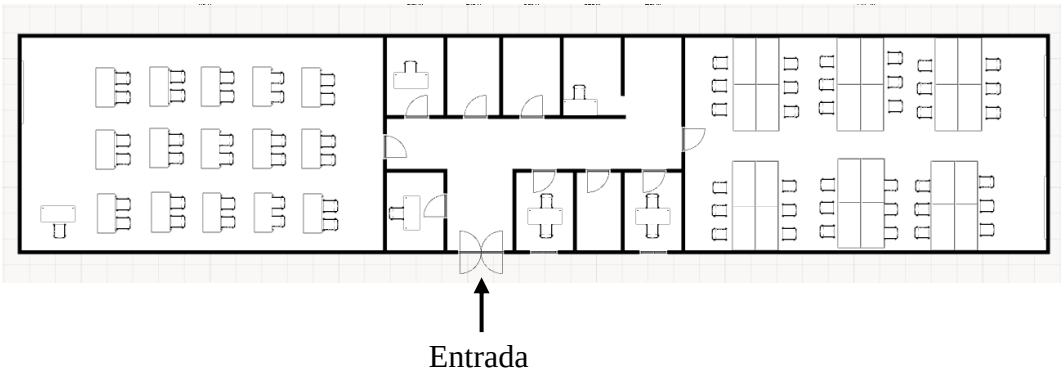


Fig. 49. Esquema Laboratorio de Redes y Telecomunicaciones

Fuente: Elaboración propia

Fig. 50. Esquema de Laboratorio 1,2 y 3

Fuente: Elaboración propia

Diagrama lógico y de red de los laboratorios 1, 2, 3, redes y telecomunicaciones

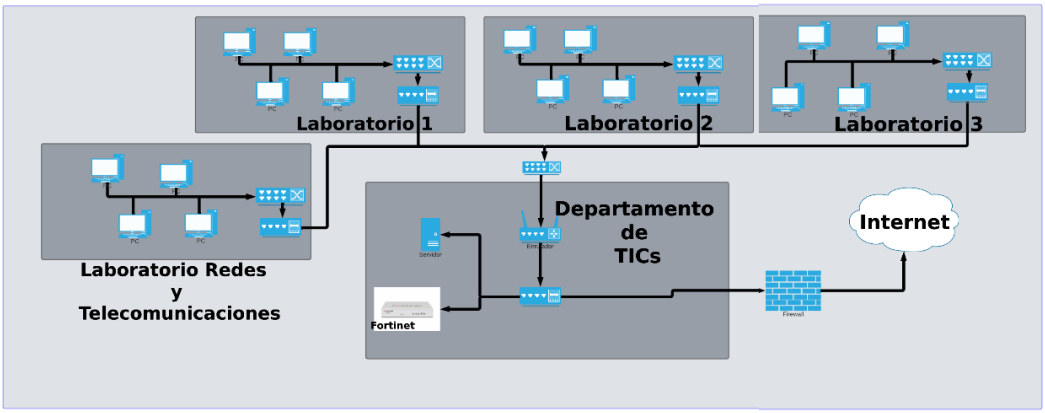


Fig. 51. Diagrama lógico de laboratorios 1, 2, 3, redes y telecomunicaciones

Fuente: Elaboración propia

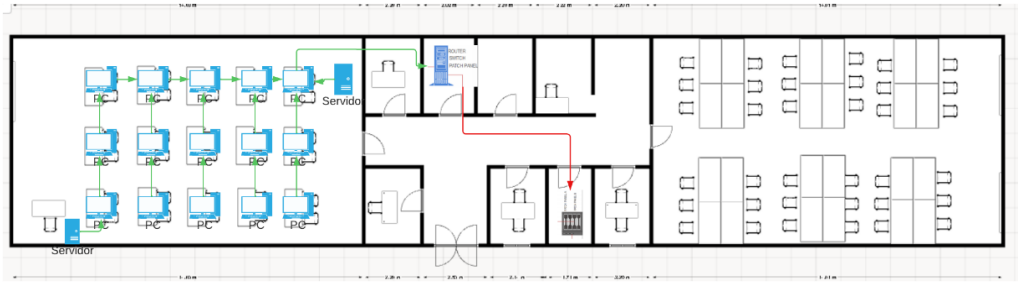


Fig. 52. Diagrama de red laboratorio de Redes y Telecomunicaciones

Fuente: Elaboración propia

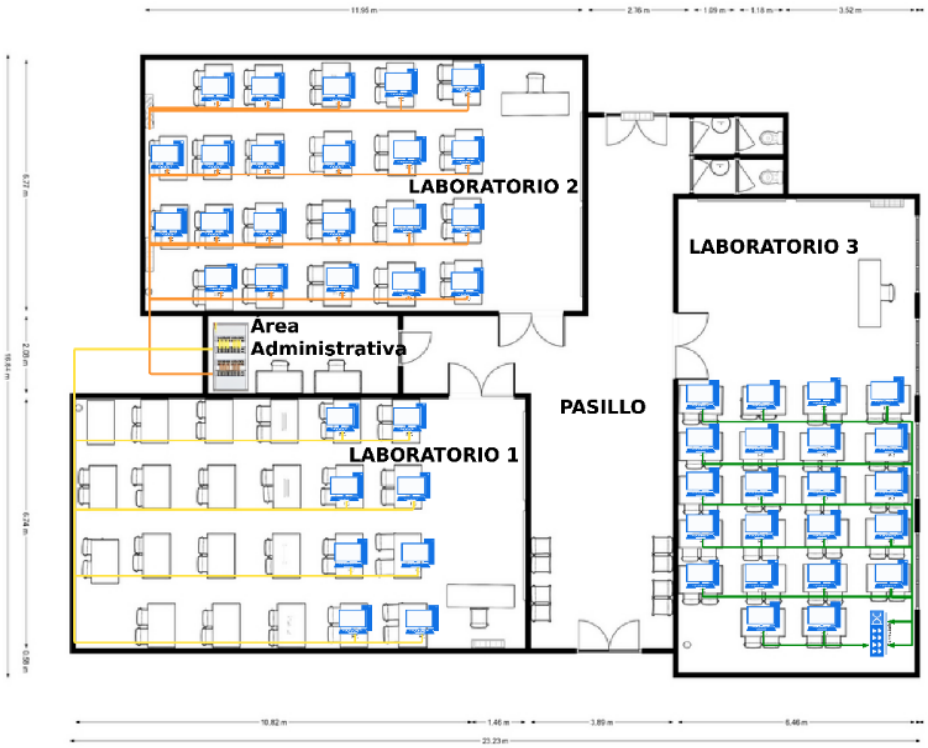


Fig. 53. Diagrama de red de los laboratorios 1,2 y 3

Fuente: Elaboración propia

Modelado 3D de laboratorio 1,2 y 3

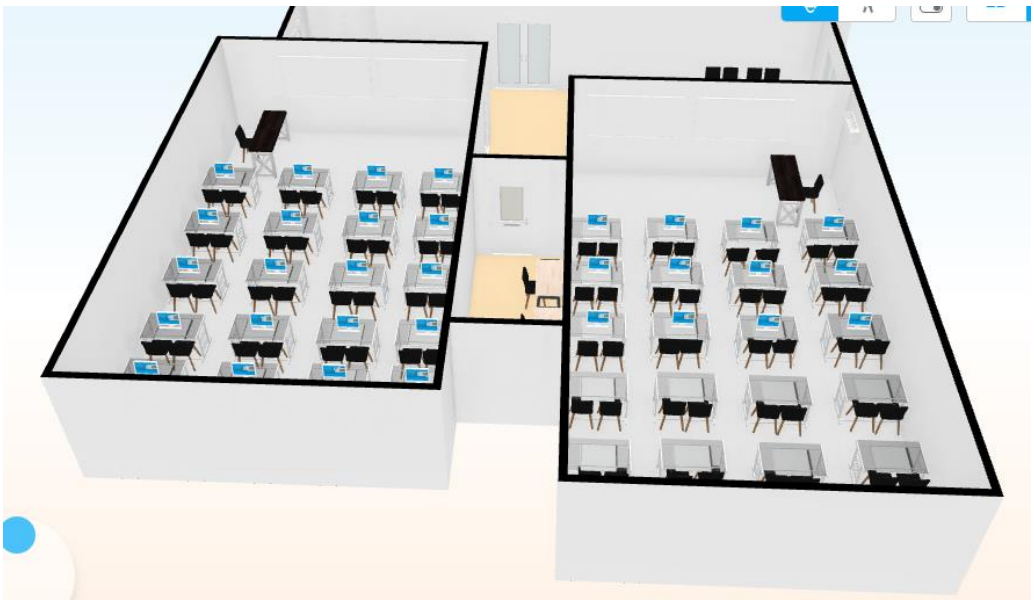


Fig. 54. Modelado 3D de Laboratorio 1 y 2

Fuente: Elaboración propia

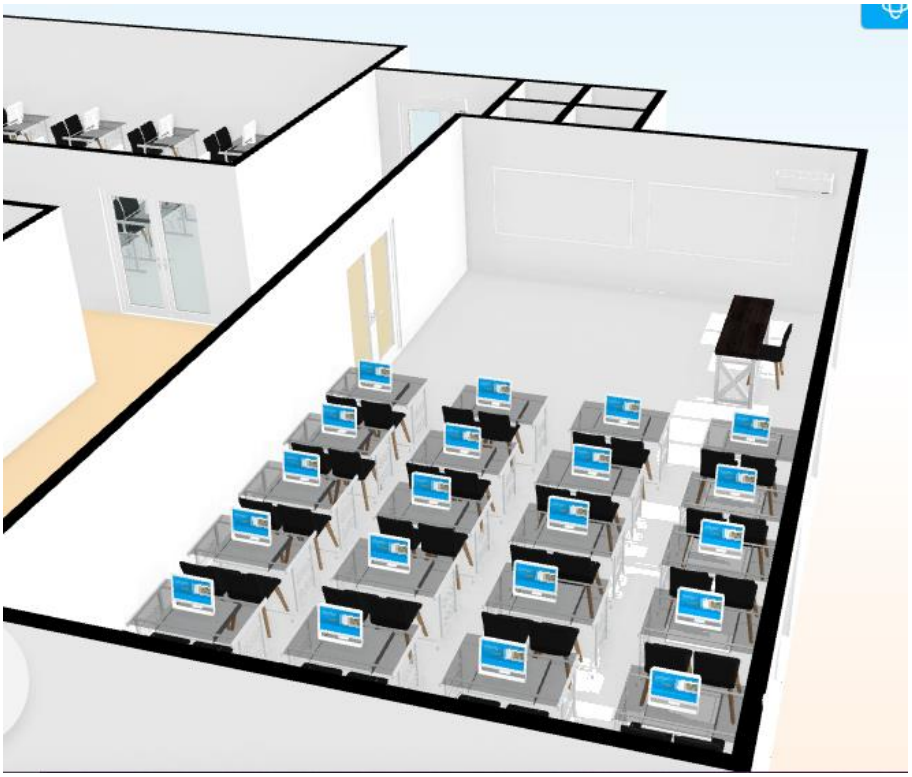


Fig. 55. Modelado 3D de Laboratorio 3

Fuente: Elaboración propia

Modelo 3D de laboratorio de Redes y Telecomunicaciones

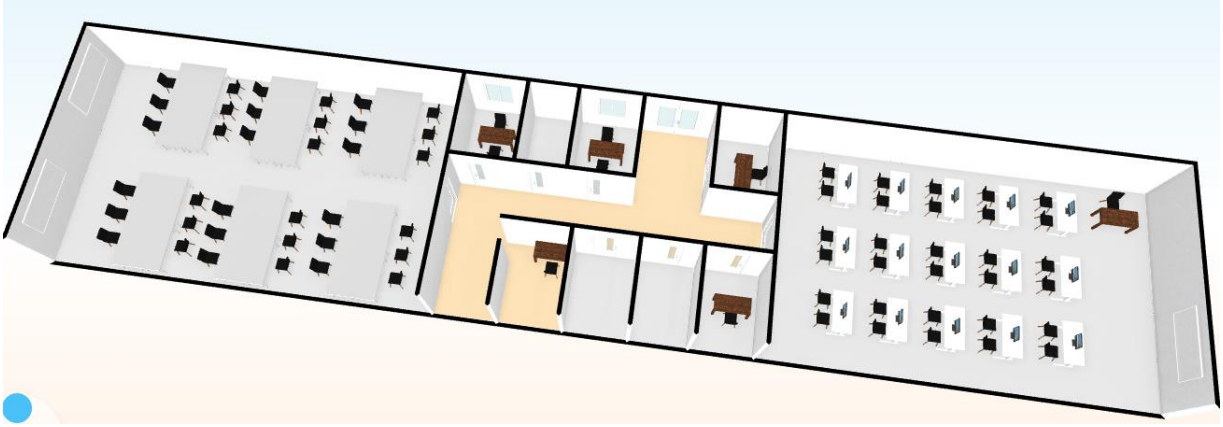


Fig. 56. Modelo 3D de laboratorio de redes y Telecomunicaciones

Fuente: Elaboración propia

Recursos tecnológicos de la Institución

Tabla 26. Característica de los ordenadores en el laboratorio 1 de la Facultado de Sistema y Telecomunicaciones

Número del laboratorio	LAB 1
Número de Ordenadores	8
Procesador	AMD Ryzen 7 2700 Eing-Core Processor 3.20 GHz Intel Core i5-4460 CPU 3.20 GHz
Memoria RAM	4 GB – 8GB
Sistema Operativo	Windows 10 Pro
Tipo de sistema	x64
Tarjeta Grafica	NVIDIA GeForce GT 710 - Intel HD Graphics 4600
Tarjeta de Red	Realtek PCIe GbE
Espacio de Almacenamiento	HDD 1 TB

Puerto USB 2.0	5
Puerto USB 3.0	2
Puerto DVI Video	2
Puerto VGA	2
Puerto HDMI	2
Puerto PS/2	1
Puertos Minijack	2
Puerto LAN (RJ45)	1

Fuente: Elaboración propia

Tabla 27. Característica de los ordenadores en el laboratorio 2 y 3 de la Facultado de Sistema y Telecomunicaciones

Numero de Laboratorio	LAB 2- LAB 3
Número de Ordenadores	22
Procesador	AMD Ryzen 7 2700 Eing-Core Processor 3.20 GHz – Intel Core i5-4460 CPU 3.20 GHz
Memoria RAM	4 GB – 8GB
Sistema Operativo	Windows 10 Pro
Tipo de sistema	x64
Tarjeta Grafica	NVIDIA GeForce GT 710 – Intel HD Graphics 4600
Tarjeta de Red	Realtek PCIe GbE
Espacio de almacenamiento	HDD 1 TB
Puerto USB 2.0	5
Puerto USB 3.0	2
Puerto DVI Video	2
Puerto VGA	2

Puerto HDMI	2
Puerto PS/2	1
Puertos Minijack	2
Puerto LAN (RJ45)	1

Fuente: Elaboración propia

Tabla 28. Característica de los ordenadores en el laboratorio 6 de la Facultado de Sistema y Telecomunicaciones

Número de Laboratorio	LAB 6
Número de Ordenadores	8
Procesador	Intel Core i7-4790 CPU 3.60 GHz
Memoria RAM	4 GB – 8GB
Sistema Operativo	Windows 10 Pro
Tipo de sistema	x64
Tarjeta Gráfica	Intel HD Graphics 4600
Tarjeta de Red	Realtek PCIe GbE
Espacio de almacenamiento	HDD 1 TB
Puerto USB 2.0	4
Puerto DVI Video	2
Puerto VGA	1
Puerto HDMI	1
Puerto PS/2	2
Puertos Minijack	4
Puerto LAN (RJ45)	1

Fuente: Elaboración propia

Tabla 29. Características de Switch Laboratorios

Equipo	Switch
Número de equipos	2
Modelo	Cisco Modelo CATALYST 2960 - WS-C296048TT-L.
Número de puertos	48 puertos

Fuente: Elaboración propia

Test de velocidad de internet

Se procedió a realizar un análisis de la velocidad de internet en el área de los laboratorios 1,2 y 3, tanto por WiFi como por entrada Ethernet. Para esto se utiliza el servicio de Speedtest por Ookla.

Fig. 57. Test de velocidad de internet mediante Wi-Fi desde ordenador portátil por medio del servicio Speedtest

Fuente: Elaboración propia

Fig. 58. Test de velocidad de internet mediante Wi-Fi desde dispositivo móvil por medio del servicio Speedtest

Fuente: Elaboración propia

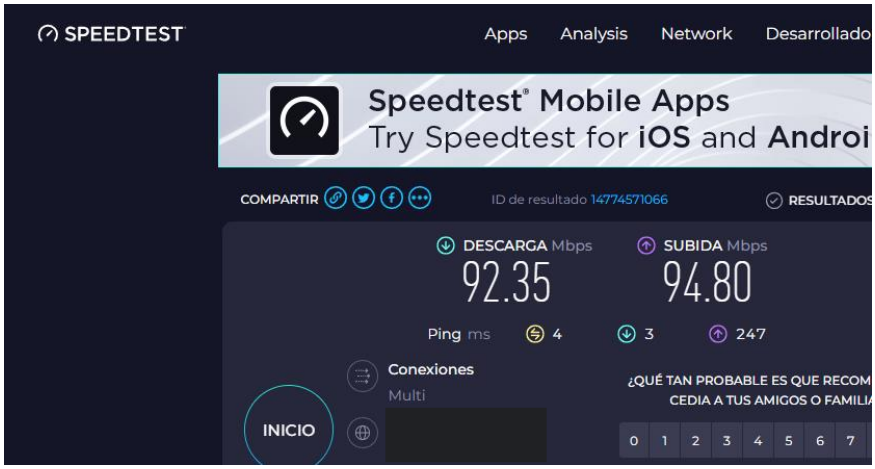


Fig. 59. Test de velocidad de internet mediante Conexión Ethernet desde PC por medio del servicio Speedtest

Fuente: Elaboración propia

2.5.3.2. Fase II: Análisis de Riesgos

En esta fase, se efectúa una evaluación de las amenazas que pueden afectar la seguridad informática dentro de la organización, enfocada al tema planteado en este proyecto. Este análisis identifica y comprende los posibles escenarios de riesgo, determinando su probabilidad de ocurrencia y su impacto potencial.

Activos de la Empresa

En el contexto del análisis de riesgo según la metodología ISO 27032 [40], es de vital importancia llevar a cabo la identificación y clasificación de los activos de información. Estos activos pueden incluir elementos de software, hardware, redes y la infraestructura presente en la institución. A continuación, se presentan los tipos de activos junto con su descripción:

Tabla 30 - Tipo de Activo

Tipos de activos Descripción	Tipos de activos Descripción
Servicio	Son los que se necesitan para la gestión de los datos.
Software	Herramientas que permiten manejar los datos.
Hardware	Equipos informáticos que permiten alojar datos, servicios y aplicaciones.

Tipos de activos Descripción	Tipos de activos Descripción
Comunicaciones	Redes y dispositivos que permiten transmitir e intercambiar datos.
Soportes de Información	Son los encargados del almacenamiento de la Información.
Equipamiento Auxiliar	Son complementos necesarios para los elementos informáticos.
Instalaciones	Infraestructura donde se instalan los sistemas de información y comunicaciones.
Personal	Personas encargadas del manejo, administración y control de los sistemas de información y comunidad estudiantil

Fuente: Elaboración propia

Mediante el método de recolección de información se identificaron los siguientes activos de la Facultad de Sistemas y Telecomunicaciones de la Universidad Estatal Península de Santa Elena.

Tabla 31 - Matriz de identificación de activos

Tipo de Activo	ID	Activo	Descripción	Responsable
Servicio	ACT01	Aula virtual	Página web dedicada a las actividades académicas y administrativas	Departamento de TICs
	ACT02	Página web Institucional	Página web dedicada a presentación de información y actividades relacionadas con la Institución	Departamento de TICs

	ACT03	SGA UPSE	Página web dedicada a actividades más administrativas por parte del personal y estudiantes	Departamento de TICs
Hardware	ACT04	CPU CORE i5-4460 Cuarta Generación	CPU utilizada por la comunidad estudiantil para sus actividades académicas	Departamento de soporte Técnico
	ACT05	CPU AMD Ryzen 7	CPU utilizada por la comunidad estudiantil para sus actividades académicas	Departamento de soporte Técnico
Comunicaciones	ACT06	SWITCH CORE HP 550AF48G-POE	Switch Core a Switch principal	Jefe de Redes e Infraestructura
	ACT07	Cisco Modelo CATALYST 2960 - WS-C296048TT-L.	Swict ubicados en los laboratorios	Jefe de Redes e Infraestructura
	ACT08	Router Cisco	Router primario de internet CEDIA	Jefe de Redes e Infraestructura
Soportes de Información	ACT09	Discos duros externos	Discos duros de almacenamiento sin espacio que almacenan formación de equipos de cómputo y servidores	Departamento de soporte Técnico

Tipo de Activo	ID	Activo	Descripción	Responsable
Soportes de Información	ACT10	Unidades USB	Memorias USB que almacenan información del talento humano del departamento de TICS	Departamento de soporte Técnico
Equipamiento Auxiliar	ACT11	Aire Acondicionado	Aires acondicionados utilizados en los Laboratorios	Departamento de soporte Técnico
	ACT12	Sistema de vigilancia	Cámaras de seguridad monitoreando los laboratorios	Departamento de soporte Técnico
Instalaciones	ACT13	Laboratorios	Laboratorios ubicados dentro de la Facultad	Coordinador de áreas
Personal	ACT14	Personal administrativo	Conformado por personal de TIC, Administradores y Docentes	Comunidad administrativa
	ACT15	Comunidad Estudiantil	Conformado por estudiantes de la UPSE	Comunidad estudiantil

Fuente: Elaboración propia

Identificación de Amenazas

Una vez definido los activos, se procederá a identificar las amenazas que genere riesgos y puedan afectar a los activos. En el ámbito de la ciberseguridad, podemos clasificar las amenazas de la siguiente manera [100]:

- Externas
- Internas

Identificación de riesgos

Teniendo identificado los activos correspondientes, se categorizará los posibles riesgos existentes que puedan afectar a la institución. Los riesgos fueron obtenidos mediante un estudio de observación (Ver anexo 3) y recolección de información mediante un análisis de paquetes realizado con la herramienta desarrollada durante un periodo de tiempo determinado (Ver anexo 4) [101].

Tabla 32.- Riesgo Identificados

Categoría	ID	Riesgo	Descripción
Externas	R01	Phishing	Ingreso a páginas web que usen esta técnica de Ingeniería social para robo de credenciales.
	R02	Código malicioso/Virus (Malware)/ WebSpan	Ingreso a páginas web con contenido malicioso, virus, malware o páginas consideradas como redireccionamiento de Spam.
	R03	DDOS	Ingreso a sitios web categorizados como cedes de ataque de denegación de servicio.
	R04	Fraude informático	Engaño o estafa en páginas web
	R05	Ransomware	Ingreso a página web que tenga adherido Ransomwere.

Categoría	ID	Riesgo	Descripción
Interna	R06	Ingreso a páginas restringidas por medio de servidor proxy	Permite acceder a páginas restringidas por el firewall empleando servidores proxy de terceros.
	R07	Ingreso a páginas restringidas por medio del uso de VPN	Permite acceder a páginas restringidas por el firewall utilizando una VPN instalada o como extensión.
	R8	Ingreso a páginas restringidas por medio de Google Translate	Permite acceder a páginas restringidas utilizando la herramienta de traducción de Google Translate.
	R9	Ingreso a páginas restringidas por medio de páginas precargadas.	Permite acceder a páginas web precargadas que normalmente estarían bloqueadas por el firewall.
	R10	Páginas maliciosas sin detección por firewall institucional	Posibilita el acceso a páginas maliciosas que no han sido detectadas por el firewall.

Fuente: Elaboración propia.

Criterio de valoración de riesgo

Los riesgos serán evaluados y valorados según los siguientes puntos:

- Probabilidad de Ocurrencia
- Nivel de Impacto

En el análisis de riesgo, se considera una escala que comprende la probabilidad de materialización de una amenaza y la magnitud o gravedad del daño asociado. Estos valores se determinan teniendo en cuenta la frecuencia y el daño esperado. A continuación, se mostrará la escala con la que se evaluará el nivel de riesgo.

Tabla 33 - Nivel de riesgo a considerar

Nivel de Riesgo	Valor	Concepto
Muy Bajo	1	Indica un riesgo demasiado bajo, casi insignificante. Se vigilará el riesgo hasta cuando las medidas sean necesarias.
Bajo	2	Indica un riesgo con impacto y probabilidad de ocurrencia bajos. Las medidas de mitigación pueden ser menos urgentes.
Medio	3-8	Indica un riesgo con impacto o probabilidad de ocurrencia moderados. Se requieren medidas de mitigación adecuadas.
Alto	9-12	Indica un riesgo con impacto y probabilidad de ocurrencia altos. Se deben tomar medidas de mitigación urgentes.
Muy Alto	15-25	Indica un riesgo con impacto y probabilidad de ocurrencia muy altos. Es necesario abordarlo de manera inmediata.

Probabilidad de Ocurrencia

La probabilidad de ocurrencia nos proporciona una evaluación de las posibilidades de que se produzcan los distintos riesgos identificados. A través de esta evaluación, podemos determinar qué amenazas tienen una probabilidad baja, media o alta de ocurrir. Consideraremos los valores según los resultados obtenidos tras la captura y análisis de paquetes efectuados (Ver anexo 4).

Tabla 34 - Tabla de Clasificación de Nivel de Ocurrencia

Nivel de Ocurrencia	Valor	Rango
Muy Bajo	1	0-1 ves por día.
Bajo	2	2-5 veces al día.
Medio	3	6-10 veces al día.
Alto	4	11-20 veces al día.
Muy Alto	5	Más de 20 veces al día.

Nivel de Impacto

El impacto es una herramienta que nos permite evaluar y clasificar los posibles efectos o consecuencias de la materialización de cada riesgo identificado. Mediante la asignación de niveles de impacto, podemos comprender y visualizar de manera clara el alcance de los daños potenciales que podrían ocurrir en caso de que se produzca cada riesgo. Esta información es fundamental para priorizar y enfocar nuestros esfuerzos en la implementación de medidas de mitigación adecuadas.

Tabla 35 - Tabla de clasificación de nivel de Impacto

Nivel de Impacto	Valor	Concepto
Muy Alto	5	El impacto muy alto implica consecuencias extremadamente significativas en términos de la confidencialidad, integridad y disponibilidad de la información o los sistemas. Puede resultar en una pérdida grave o completa de datos, interrupciones prolongadas de servicios críticos o daños catastróficos a la reputación de la organización.
Alto	4	El impacto alto implica consecuencias significativas en términos de la confidencialidad, integridad y disponibilidad de la información o los sistemas. Puede resultar en una pérdida importante de datos, interrupciones significativas de servicios o daños significativos a la reputación de la organización.
Medio	3	El impacto medio indica que las consecuencias tienen un nivel moderado en términos de la confidencialidad, integridad y disponibilidad de la información o los sistemas. Puede resultar en una pérdida limitada o parcial de datos, interrupciones temporales de servicios o un impacto moderado en la reputación de la organización.

Nivel de Impacto	Valor	Concepto
Bajo	2	El impacto bajo significa que las consecuencias tienen un impacto limitado en la confidencialidad, integridad y disponibilidad de la información o los sistemas. Puede resultar en una pérdida mínima de datos, interrupciones leves de servicios o un impacto insignificante en la reputación de la organización.
Muy Bajo	1	El impacto muy bajo indica que las consecuencias son extremadamente limitadas en términos de la confidencialidad, integridad y disponibilidad de la información o los sistemas. Puede resultar en una pérdida insignificante o nula de datos, interrupciones mínimas de servicios o un impacto despreciable en la reputación de la organización.

Matriz de Riesgo

La matriz de probabilidad e impacto utilizada en el proyecto es una herramienta valiosa para realizar un análisis cualitativo de riesgos. Su objetivo principal es categorizar los riesgos en diferentes niveles de importancia, teniendo en cuenta la evaluación de la probabilidad de que ocurra el riesgo y el impacto que tendría en los activos afectados en caso de que se materialice una amenaza.

Tabla 36 - Matriz de evaluación de probabilidad e Impacto

Matriz de Riesgos Cualitativa		Nivel de Impacto				
		Muy Bajo	Bajo	Medio	Alto	Muy Alto
		1	2	3	4	5
Probabilidad de Ocurrencia	Muy Alto	5	10	15	20	25
	Alto	4	8	12	16	20
	Medio	3	6	9	12	15
	Bajo	2	4	6	8	10
	Muy Bajo	1	2	3	4	5

El cálculo del resultado del riesgo se obtiene mediante la multiplicación de la probabilidad de ocurrencia de una amenaza por la gravedad o magnitud del daño. Esta fórmula se expresa de la siguiente manera:

- **Np** = Nivel Ocurrencia
- **Ni** = Nivel Impacto.
- **Nr** = Nivel del riesgo resultante.

El nivel de la probabilidad se refiere a la evaluación de la posibilidad de que ocurra la amenaza, mientras que el nivel de la magnitud del daño se relaciona con la gravedad o impacto que tendría en los activos afectados.

Fórmula de cálculo de riesgo:

Nivel de Riesgo = NP* NI

El análisis de los colores en cada celda permite obtener conclusiones sobre el nivel de riesgo que ocurre en cada activo de la institución. Esto facilita la identificación de incidentes significativos y la determinación de las posibles medidas de protección necesarias para abordar el problema de manera adecuada.

Riesgos existentes

En la siguiente tabla de análisis de riesgo, se realizará una evaluación y clasificación de cada amenaza de acuerdo a su nivel de riesgo:

Tabla 37 - Tabla de cálculo del nivel de riesgo

Riesgo	ID	Impacto	Probabilidad	Nivel de Riesgo	
Phishing	R01	3	1	3	Medio
Código malicioso/Virus (Malware)	R02	4	3	12	Alto
DDOS	R03	4	2	8	Medio
Fraude informático	R04	4	2	12	Alto

Riesgo	ID	Impacto	Probabilidad	Nivel de Riesgo	
Ransomware	R05	5	1	5	Medio
Ingreso a paginas restringidas por medio de servidor proxy	R06	3	1	3	Medio
Ingreso a paginas restringidas por medio del uso de VPN	R07	3	4	12	Alto
Ingreso a paginas restringidas por medio de Google Translate	R08	3	1	3	Medio
Ingreso a paginas restringidas por medio de páginas precargadas.	R09	3	1	3	Medio
Paginas maliciosas sin bloquear por firewall	R10	3	3	9	Medio
Promedio				7	Medio

Fuente: Elaboración propia

Esta tabla nos ayudará a identificar y priorizar las amenazas según su nivel de riesgo, considerando tanto la probabilidad de ocurrencia como el impacto que pueden tener en la confidencialidad, integridad y disponibilidad de la información o los sistemas. A través de este análisis, podremos tomar decisiones informadas sobre las medidas de protección y mitigación necesarias para cada amenaza identificada.

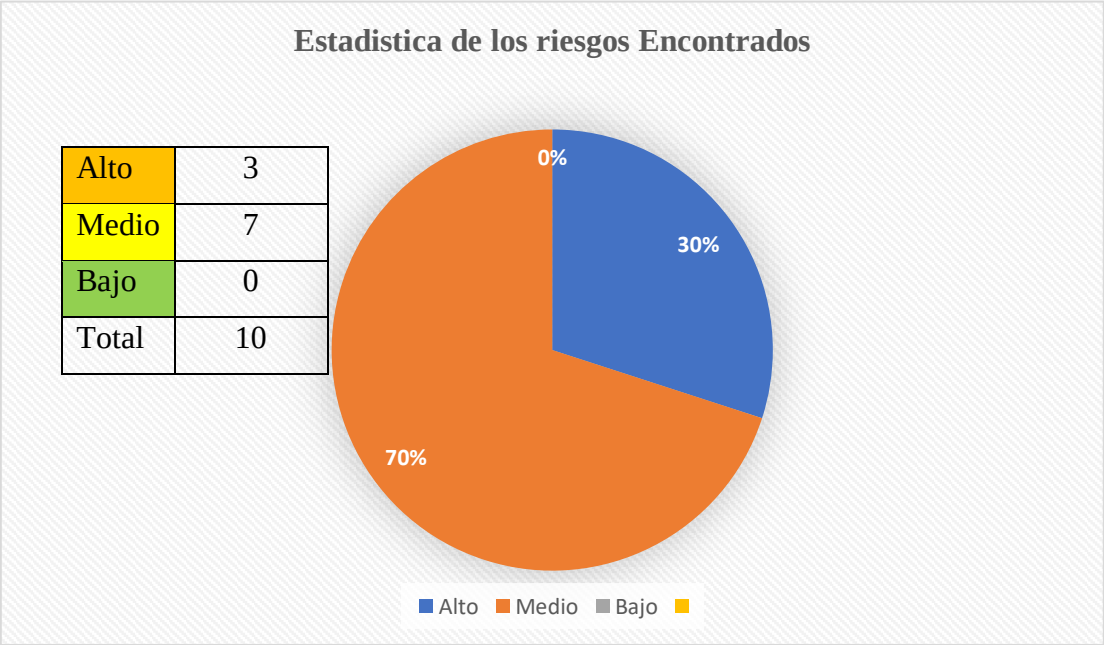


Fig. 60 . Resultados del nivel de riesgo

Fuente: Elaboración propia.

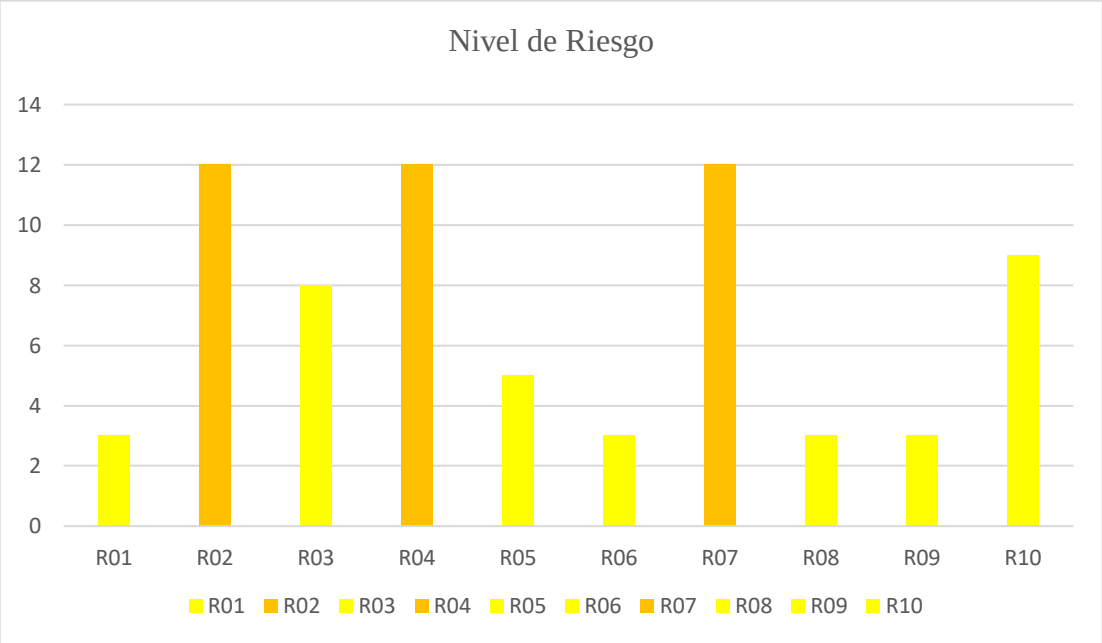


Fig. 61 . Gráfico estadístico de niveles de riesgo según su clasificación

Fuente: Elaboración propia

Los resultados obtenidos muestran la importancia de considerar estas debilidades en el ámbito de la seguridad de la información. Al evaluar su impacto y probabilidad, se puede determinar el nivel de riesgo asociado a cada una de ellas. Esto proporciona una visión integral de las amenazas potenciales y permite la implementación de medidas de mitigación adecuadas para reducir la exposición a incidentes de seguridad.

Es fundamental tener en cuenta que estas debilidades pueden representar una puerta de entrada a posibles ataques y comprometer la confidencialidad, integridad y disponibilidad de la información dentro de la institución. Por lo tanto, es necesario adoptar estrategias proactivas para fortalecer las defensas y garantizar un entorno seguro en el acceso a las páginas web.

2.5.3.3. Fase III: Plan de Acción

En esta fase, se elabora un plan detallado que incluye las acciones y medidas específicas a implementar para fortalecer la detección temprana de anomalías en el tráfico URL.

Creación de Políticas

Se plantean una serie de políticas para mitigar las amenazas y fortalecer la seguridad de la red ante posibles incidentes de seguridad. Estas políticas han sido desarrolladas en base a las plantillas proporcionadas por SANS Institute [102]. A continuación, se detallan las políticas elaboradas:

Política de uso aceptable

Propósito

El propósito de esta política es describir el uso aceptable de equipos informáticos y otros dispositivos electrónicos dentro de la FACSISTEL. Estas reglas existen para proteger a la comunidad universitaria de la UPSE. El uso inapropiado expone a la institución a riesgos cibernéticos, incluidos ataques de virus, ransomware, compromiso de los sistemas y servicios de red, violación de datos y problemas legales [103].

Alcance

Esta política se aplica al uso de información, dispositivos electrónicos e informáticos y recursos de red para realizar actividades académicas dentro de la institución. Todo el personal administrativo y comunidad estudiantil es responsable de ejercer buen juicio con respecto al uso adecuado de la información, los dispositivos electrónicos y los recursos de la red de acuerdo con las políticas, normas de UPSE, las leyes y reglamentaciones locales [103].

Política:

1. Uso general y propiedad
    a. Por motivos de seguridad y mantenimiento de la red, las personas autorizadas dentro de FACSISTEL pueden monitorear los equipos, los sistemas y el tráfico de la red en cualquier momento, según las normas de TICs. Política de auditoría [103].
    b. UPSE se reserva el derecho de auditar redes y sistemas periódicamente para garantizar el cumplimiento de esta política [103].
2. Seguridad e información de propiedad
    a. Todos los dispositivos que se conecten a la red interna deberán cumplir con las políticas de acceso mínimo [103].
    b. Las contraseñas de nivel de sistema y de usuario deben cumplir con las políticas de contraseñas [103].
    c. Todos los dispositivos informáticos deben estar protegidos con una pantalla de bloqueo protegida por contraseña con la función de activación automática establecida en 10 minutos o menos. Debe bloquear la pantalla o cerrar la sesión cuando el dispositivo esté desatendido [103].
3. Uso inaceptable
    a. Introducción de programas maliciosos en la red o servidor (por ejemplo, virus, gusanos, troyanos, ransomware, etc.).

b. El escaneo de puertos o el escaneo de seguridad está expresamente prohibido a menos que se realice una notificación previa al equipo de administrativo [103].
c. Eludir la autenticación de usuario o la seguridad de cualquier host, red o cuenta [103].
d. Introducir honeypots, honeynets o tecnología similar en la red de FACSISTEL [103].

Política de seguridad de los laboratorios

Propósito

Esta política establece los requisitos de seguridad de la información para ayudar a administrar y salvaguardar los recursos del laboratorio y las redes de FACSISTEL al minimizar la exposición de la infraestructura crítica y los activos de información a las amenazas que pueden resultar de hosts desprotegidos y acceso no autorizado [104].

Alcance

Esta política se aplica a toda la comunidad universitaria de la UPSE. Esta política se aplica a los laboratorios de FACSISTEL [104].

Política:

1. Requisitos generales
    a. Las computadoras de laboratorio basadas en PC deben tener el software antivirus compatible estándar de UPSE instalado y programado para ejecutarse a intervalos regulares. Además, el software antivirus y los archivos de patrones de virus deben mantenerse actualizados [104].
    b. Las computadoras infectadas con virus deben eliminarse de la red hasta que se verifique que están libres de virus. Los administradores/gerentes de laboratorio son responsables de crear procedimientos que aseguren que el software antivirus se ejecute a intervalos regulares y que las computadoras se revisen como libres de virus [104].

2. Requisitos de seguridad del laboratorio interno
    a. La Organización de soporte de red debe mantener un dispositivo de firewall entre la red de universitaria y todo el equipo de laboratorio [104].
    b. Todo el tráfico entre el área administrativa y la red del laboratorio debe pasar por un firewall mantenido por la Organización de soporte de red [104].

Política de control y filtrado del uso de Internet por parte de la comunidad estudiantil

Propósito

El propósito de esta política es definir estándares para los sistemas que monitorean y limitan el uso de la web desde cualquier host dentro de la red de FACSISTEL. Estos estándares están diseñados para garantizar que los estudiantes usen Internet de manera segura y responsable, y garantizar que el uso de la web por parte de los estudiantes pueda ser monitoreado o investigado durante un incidente [105].

Alcance

Esta política se aplica al personal administrativo y comunidad estudiantil con acceso a una computadora o estación de trabajo propiedad de UPSE o de propiedad personal conectada a la red de FACSISTEL [105].

Esta política se aplica a todas las comunicaciones iniciadas por el usuario final entre la red de FACSISTEL e Internet, incluida la navegación web, la mensajería instantánea, la transferencia de archivos, el uso compartido de archivos y otros protocolos estándar y propietarios [105].

Política:

1. Supervisión del sitio web
    a. El Departamento de Tecnologías de la Información deberá monitorear el uso de Internet de todas las computadoras y dispositivos conectados a la red corporativa. Para todo el tráfico, el sistema de monitoreo debe registrar la dirección IP de origen, la

fecha, la hora, el protocolo y el sitio o servidor de destino. Siempre que sea posible, el sistema debe registrar el ID de usuario de la persona o cuenta que inicie el tráfico. Los registros de uso de Internet deben conservarse durante 180 días [105].

b. Analizar la detección de anomalías en el tráfico URL para determinar la causa raíz.
c. Realizar un seguimiento forense exhaustivo para identificar el origen y la naturaleza de las anomalías.
d. Notificar de manera oportuna y adecuada a los departamentos y personas involucradas sobre las anomalías detectadas.

2. Acceso a Informes de Monitoreo del Sitio Web
    a. Los informes generales de tendencias y actividades estarán disponibles para cualquier empleado según sea necesario previa solicitud al Departamento de Tecnología de la Información [105].
3. Sistema de Filtrado de Uso de Internet
    a. El Departamento de Tecnologías de la Información bloqueará el acceso a los sitios y protocolos de Internet que se consideren inadecuados para el entorno corporativo de UPSE. Se deben bloquear los siguientes protocolos y categorías de sitios web [105]:
        i. Material para adultos/sexualmente explícito
        ii. Anuncios y ventanas emergentes
        iii. Chat y mensajería instantánea
        iv. Juego
        v. Hackear
        vi. Drogas ilegales
        vii. Ropa íntima y trajes de baño
        viii. Intercambio de archivos punto a punto
        ix. Contactos y citas
        x. Servicios de redes sociales
        xi. SPAM, Phishing y Fraude
        xii. Software espía
        xiii. Contenido insípido y ofensivo

xiv. Violencia, intolerancia y odio
xv. Correo electrónico basado en la web

4. Cambios en las reglas de filtrado de uso de Internet
    a. El Departamento de Tecnologías de la Información revisará periódicamente y recomendará cambios a las reglas de filtrado web y de protocolos. Los cambios en las reglas de filtrado web y de protocolos se registrarán en la Política de control y filtrado del uso de Internet [105].

Política de uso de Internet

Propósito

El propósito de esta política es definir los usos apropiados de Internet por parte del personal administrativo y la comunidad estudiantil [106].

Alcance

La Política de uso de Internet se aplica a todos los usuarios de Internet que acceden a Internet a través de los recursos informáticos o de red [106].

Servicios de Internet permitidos

El acceso a Internet debe utilizarse únicamente con fines educativos. Se proporcionarán capacidades para los siguientes servicios estándar de Internet a los usuarios según sea necesario:

- Navegación: servicios WWW según sea necesario para fines comerciales, utilizando una herramienta de navegador de protocolo de transferencia de hipertexto (HTTP). Acceso completo a Internet; acceso limitado desde Internet solo a servidores web públicos dedicados de la empresa [106].

Política:

1. Uso de recursos
    a. El acceso a Internet se aprobará y proporcionará solo para actividades académicas. Los servicios de Internet se otorgarán en

función de las responsabilidades laborales actuales de los usuarios [106].

2. Uso permitido
    a. El uso de Internet se otorga con el único propósito de apoyar las actividades académicas. Todos los usuarios deben seguir los principios corporativos con respecto al uso de recursos y ejercer buen juicio al usar Internet [106].
    b. El uso aceptable de Internet para realizar funciones diarias puede incluir:
        i. Soporte técnico de TI descargando actualizaciones y parches de software;
        ii. Revisión de posibles sitios web de proveedores para obtener información sobre productos;
        iii. Información reglamentaria o técnica de referencia.
        iv. Actividades académicas
3. Uso personal
    a. El uso de los recursos informáticos de la empresa para acceder a Internet con fines personales, sin la aprobación del gerente del usuario y del departamento de TI, puede considerarse causa de acción disciplinaria que puede incluir el despido [106].
    b. Los usuarios que eligen almacenar o trasmitir información personal, como claves privadas, números de tarjetas de crédito o certificados, o hacer uso de “billeteras” de internet, lo hacen bajo su propio riesgo, la empresa no es responsable de ninguna perdida de información consecuente de propiedad personal [106].
4. Uso prohibido
    a. Se prohíbe específicamente la adquisición, el almacenamiento y difusión de datos que sean ilegales, pornográficos o que representen negativamente la raza, el sexo o el credo [106].
    b. Acceder a información de la empresa que no está dentro del ámbito de su trabajo. Esto incluye la lectura no autorizada de la información de la cuenta del cliente, el acceso no autorizado a la información del

archivo del personal y el acceso a información que no es necesaria para la ejecución adecuada de las funciones laborales [106].

c. Usar indebidamente, divulgar sin la debida autorización o alterar la información del cliente o del personal. Esto incluye realizar cambios no autorizados en un archivo de personal o compartir datos electrónicos del cliente o del personal con personal no autorizado [106].

5. Monitoreo
    a. Los usuarios deben considerar sus actividades en Internet como monitoreadas periódicamente y limitar sus actividades en consecuencia [106].
    b. La gerencia se reserva el derecho de examinar el correo electrónico, los directorios de archivos personales, el acceso web y otra información almacenada en las computadoras de la empresa, en cualquier momento y sin previo aviso [106].
    c. Este examen asegura el cumplimiento de las políticas internas y ayuda en la gestión de los sistemas de información de la empresa [106].

Métodos de implementación

La siguiente tabla presenta un resumen de las estrategias y medidas de mitigación propuestas para abordar las debilidades identificadas. A través de la implementación de las estrategias y medidas adecuadas, se busca fortalecer la protección y confidencialidad de los sistemas, garantizando un entorno seguro y confiable para el intercambio de información en la facultad.

Tabla 38- Estrategias y medidas de mitigación a amenazas web

Amenaza	Estrategias y Medidas de Mitigación
Phishing	▪ Uso de soluciones de filtrado y detección de phishing ▪ Capacitación continua sobre identificación y evitación de ataques de phishing

Amenaza	Estrategias y Medidas de Mitigación
Código malicioso/Virus	▪ Implementación de software antivirus y antimalware actualizado. ▪ Escaneo periódico de archivos y descargas
DDOS	▪ Implementar soluciones de protección contra ataques DDoS, como sistemas de mitigación y servicios de red distribuida (CDN).
Robo de identidad	▪ Uso de sistemas de autenticación robustos y seguros ▪ Políticas de privacidad y protección de datos personales
Fraude Informático	▪ Implementar soluciones de detección de fraudes y análisis de comportamiento anómalo
Ransomware	▪ Uso de soluciones de seguridad avanzadas para la detección y prevención del ransomware ▪ Realización de copias de seguridad regulares y almacenamiento seguro de los datos
Ingreso por servidor proxy	▪ Establecer políticas y procedimientos para la autorización y supervisión del uso de servidores proxy. ▪ Implementar soluciones de monitoreo de la red. ▪ Bloquear el acceso a página que proporcionen proxy web.
Ingreso por uso de VPN	▪ Establecer políticas claras y restrictivas para el uso de VPN. ▪ Implementar soluciones de seguridad que permitan monitorear y auditar el tráfico VPN.
Ingreso por medio de Google Translate	▪ Configurar el firewall para bloquear el acceso a la herramienta de traducción de Google Translate. ▪ Implementar soluciones de filtrado y detección de uso no autorizado de Google Translate

Amenaza	Estrategias y Medidas de Mitigación
Páginas maliciosas sin bloquear por firewall	▪ Mejorar la configuración del firewall para bloquear el acceso a páginas maliciosas conocidas. ▪ Implementar sistemas de detección y prevención de malware.
Ingreso por medio de páginas precargadas	▪ Realizar pruebas de seguridad periódicas sobre la navegación en páginas precargadas.

Estas estrategias y medidas de mitigación están diseñadas para reducir los riesgos asociados a cada debilidad identificada, fortaleciendo la seguridad y protección de las redes distribuidas de la Facultad de Sistemas y Telecomunicaciones.

Procesos afectados

Al implementar las estrategias y medidas a tomar en caso de presentarse uno de los riesgos mencionados, se espera fortalecer la protección y confidencialidad de la red. A continuación, se describen los procesos que pueden verse involucrado en estas medidas:

1. Capacitación y Concientización: La capacitación continua sobre cómo reconocer y evitar los ataques de phishing, así como la concientización sobre otras amenazas cibernéticas, será parte del programa de capacitación de la agencia, que incluirá sesiones de capacitación e información. Se asignarán recursos para educar a los usuarios sobre las mejores prácticas de seguridad y cómo reconocer y evitar diferentes tipos de ataques.
2. Configuración y mantenimiento: La implementación de soluciones de seguridad avanzadas requerirá procesos de configuración y mantenimiento de los sistemas de la agencia. Se garantizarán actualizaciones regulares del software de seguridad, escaneos regulares y una configuración adecuada de los sistemas de protección.

3. Monitoreo y Vigilancia: Implementar el monitoreo de la red, la detección de malware significará establecer procesos de monitoreo y vigilancia para los sistemas de la agencia. Se asignarán recursos para monitorear continuamente los incidentes de seguridad, identificar comportamientos inusuales y responder a posibles incidentes de seguridad de manera oportuna.

Controles Tecnológicos

Para poder agregar una capa más de seguridad a la red, en términos de detección del ingreso a páginas web con contenido maliciosos, se plantea el uso del algoritmo desarrollado.

2.5.3.4. Fase IV: Implementación

En esta última fase, se ejecuta el plan de acción definido previamente. Esto implica la implementación de las medidas de seguridad y control establecidas, la configuración y puesta en marcha del algoritmo desarrollado para la detección temprana de anomalías en el tráfico URL, así como la realización de pruebas exhaustivas para garantizar su eficacia y rendimiento.

Planes de concienciación del personal

La conciencia del personal en la seguridad de la información es cada vez más importante. Proteger los activos y datos de la Facultad de Sistemas y Telecomunicaciones de la Universidad Estatal Península de Santa Elena (FACSISTEL) fue una prioridad. Un programa de concientización de los empleados se convierte en una herramienta importante para garantizar que cada miembro del equipo comprenda la importancia de la seguridad de la información y esté capacitado para reconocer amenazas potenciales en el tráfico de URL. Este plan constituye una guía práctica para desarrollar e implementar acciones específicas de concientización y capacitación, permitiendo fortalecer la postura de seguridad de la Facultad y mejorar la eficacia del algoritmo desarrollado.

Tabla 39.-Plan de Concientización del Personal

Plan de Concientización del Personal	
Objetivo:	Informar al personal de la Facultad de Sistemas y Telecomunicaciones (FACSISTEL) sobre la importancia de la seguridad de la información y la detección temprana de anomalías en tráfico URL en redes distribuidas, reduciendo de brecha digital a relación de navegabilidad de páginas web.
Actividades	1. Evaluación de Conocimiento y Concientización del Personal - Realizar una evaluación inicial mediante encuestas y entrevistas para medir el nivel de conocimiento y conciencia del personal en seguridad de la información y detección de anomalías en tráfico URL. - Identificar áreas de mejora y necesidades de capacitación específicas. 2. Desarrollo de Materiales Educativos - Crear materiales educativos y recursos informativos, como presentaciones, guías y folletos, que expliquen de manera clara y concisa los conceptos y prácticas de seguridad de la información y la detección de anomalías en tráfico URL. - Adaptar los materiales al lenguaje y nivel de comprensión del personal de la FACSISTEL. 3. Sesiones de Capacitación y Concientización - Realizar sesiones de capacitación y concientización presenciales o virtuales para todo el personal de la FACSISTEL. - Cubrir temas como la importancia de la seguridad de la información, las mejores

	prácticas en el manejo de URL, el reconocimiento de posibles anomalías y la reportación de incidentes. 4. Promoción de la Cultura de Seguridad - Fomentar una cultura de seguridad de la información mediante la comunicación regular y la promoción de prácticas seguras. - Enfatizar la responsabilidad individual y colectiva de proteger la información y fomentar la colaboración en la detección y reporte de anomalías en tráfico URL. 5. Evaluación y Seguimiento - Realizar evaluaciones periódicas para medir el impacto del plan de concientización en el conocimiento y comportamiento del personal. - Recopilar retroalimentación del personal y utilizarla para mejorar y ajustar el plan de concientización de manera continua. 6. Integración Continua - Mantener la concientización en seguridad de la información como un proceso continuo e integrado en las actividades diarias de la FACSISTEL. - Actualizar el plan de concientización en función de las nuevas amenazas y desafíos que puedan surgir en el entorno de seguridad de la información.
Alcance	1. El plan de concientización se aplicará a todo el personal de la Facultad de Sistemas y Telecomunicaciones

	(FACSISTEL) de la Universidad Estatal Península de Santa Elena 2. El enfoque principal estará en la seguridad de la información y la detección temprana de anomalías en el tráfico URL en redes distribuidas.
Resultados esperados	3. Mayor conocimiento y conciencia del personal en relación con la seguridad de la información y la detección temprana de anomalías en tráfico URL. 4. Mejora en las prácticas de seguridad del personal al utilizar URL y al reconocer y reportar posibles amenazas o anomalías. 5. Una cultura de seguridad fortalecida en la Facultad, donde cada miembro del personal comprenda su rol y responsabilidad en la protección de la información y la detección de posibles riesgos. 6. Reducción de incidentes de seguridad relacionados con el tráfico URL y una respuesta más rápida y eficiente ante posibles anomalías. 7. Mejora en la protección de los activos y datos de la Facultad, lo que garantiza la integridad, confidencialidad y disponibilidad de la información.

Fuente: Elaboración propia

Monitorización de TIC

Se procede a monitorear el tráfico de la red de la institución con el algoritmo previamente diseñado durante un lapso de tiempo de ocho días, durante un tiempo de 30 min en horarios volátiles.

Resultados del análisis.

La siguiente tabla presenta un análisis realizado desde el 17 de julio del 2023 hasta el 26 de julio del 2023, en dos horarios diferentes, los cuales fueron seleccionados de forma dinámica, durante un lapso de 30 min cada uno (Ver anexo 4).

Tabla 40. Tabla de análisis de paquete

Dia	Tiempo	Análisis 1	Cantidad	Tiempo	Análisis 2	Cantidad
17-7-2023	30 min	12:07-12:37pm	27647	30 min	2:43: 3:13pm	7403
18-7-2023	30 min	9:50-10:20am	2907	30 min	2.00-2.30pm	3712
19-7-2023	30 min	10:00-10-30am	3797	30 min	2:00-2:30pm	9062
20-7-2023	30 min	10:00-10:30am	5329	30 min	4:40-5:25pm	1668
21-7-2023	30 min	9:55-10:25am	2778	30 min	4:12-4:42pm	5256
24-7-2023	30min	2:55-3:25pm	3647	30min	4:00-4:30pm	25612
25-7-2023	30min	10:50-11:20am	44577	30 min	1:40-2:10pm	2626
26-7-2023	30min	1:00-1:30 pm	1512	30min	4:50-5:20 pm	1732

Fuente: Elaboración propia.

En la siguiente tabla se muestra un fragmento de los paquetes capturados durante el tiempo de análisis, correspondiente a los paquetes limpios.

Tabla 41 - Fragmento de captura de paquetes limpios en el trascurso de análisis.

Hora	Fecha	Protocolo	IP de Origen	Puerto origen	IP de destino	Puerto de destino	Tamaño del paquete
14:46:44	2023-07-17	TCP	192.168.23.21	38450	54.161.181.184	443	112
13:40:41	2023-07-18	TCP	192.168.23.21	54090	54.185.202.81	443	74

Hora	Fecha	Protocolo	IP de Origen	Puerto origen	IP de destino	Puerto de destino	Tamaño del paquete
10:04:16	2023-07-19	TCP	192.168.23.21	33984	212.102.60.232	443	66
10:04:45	2023-07-19	TCP	192.168.23.21	36296	104.16.89.20	443	105
10:04:54	2023-07-19	TCP	192.168.23.21	51848	65.8.248.61	443	112
10:04:58	2023-07-19	TCP	192.168.23.21	39436	142.250.217.163	443	105

Fuente: Elaboración propia.

En la siguiente imagen se muestra una captura del dashboard en donde se presenta las capturas de nuevos paquetes anómalos durante el tiempo de análisis.

Fig. 62. Lista de nuevos paquetes anómalos capturados.

Fuente: Elaboración propia

Paquete anómalo detectado el 17 de julio del 2023 con la siguiente ip: 200.24.197.6, este fue detectado por el motor de análisis Barracuda_Reputation_BL, el cual mantiene historiales de direcciones IP de spammers conocidos y remitentes con buenas prácticas de correo. Esto contribuye al Sistema de Reputación de Barracuda, que permite al Firewall contra Spam y Virus de Barracuda bloquear o permitir un mensaje según la IP del remitente y la reputación de las URLs en el mensaje. Al

combinar ambos datos, Barracuda puede identificar rápidamente si un mensaje es spam o legítimo [107].

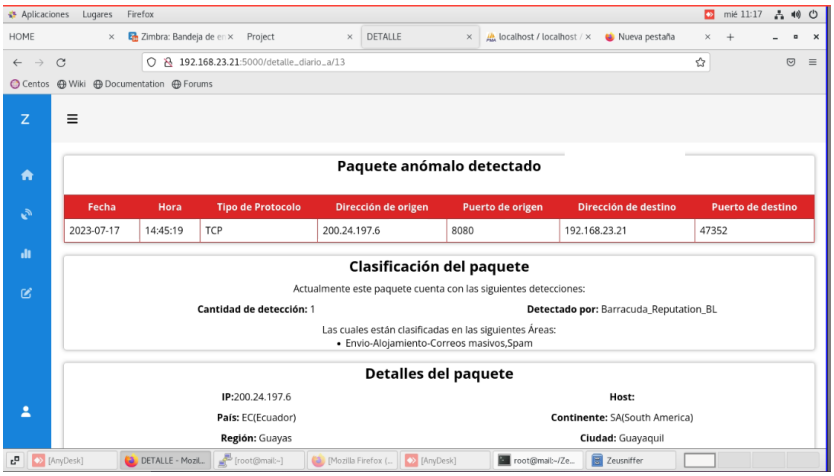


Fig. 63 . Parte 1 del detalle del análisis de la IP 200.24.197.6

Fuente: Elaboración propia

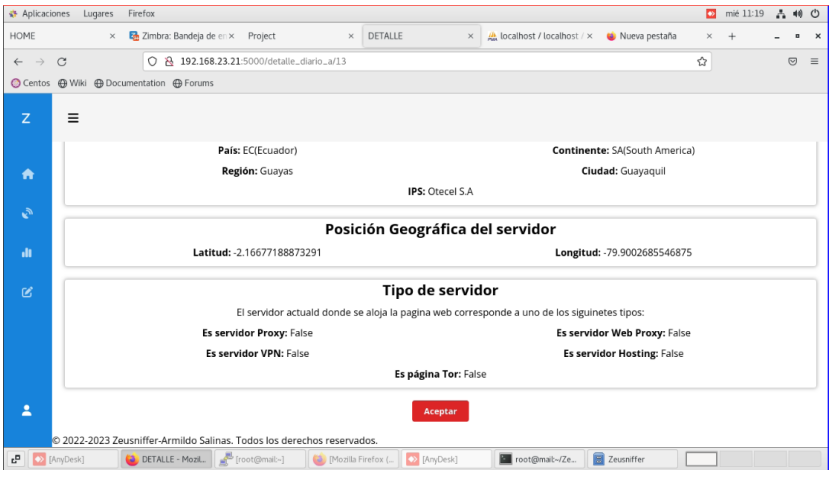


Fig. 64. Parte 2 del detalle del análisis de la IP 200.24.197.6

Fuente: Elaboración propia

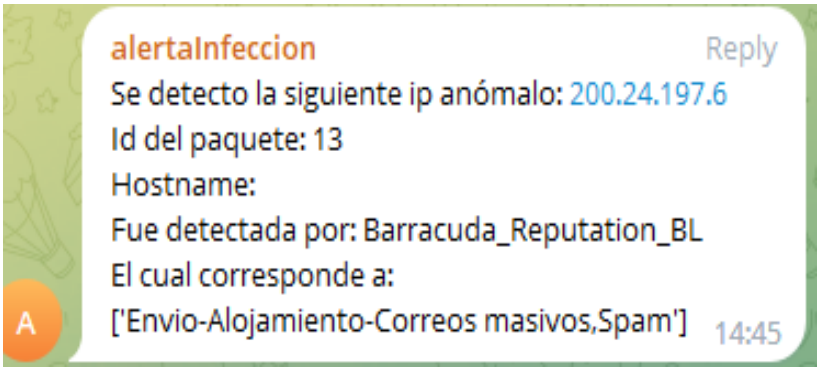


Fig. 65 . Mensaje enviado al grupo de Telegram sobre la IP 200.24.197.6

Fuente: Elaboración propia

Paquete anómalo detectado el 26 de julio del 2023 con la siguiente ip: 109.205.213.22, lo cual fue detectado por 6 motores diferentes de análisis: lacklists_co, BlockedServersRBL, CI Army List, CRDF, IPsum, PlonkatronixBL, las cuales corresponden a IP involucradas con escaneo de puertos o ataques de fuerza bruta [108], IP web que han disparado varias alertas maliciosas [109], estado anómalo de una página web [110], entre otros.

Fig. 66. Parte 1 del detalle del análisis de la IP 109.205.213.22

Fuente: Elaboración propia

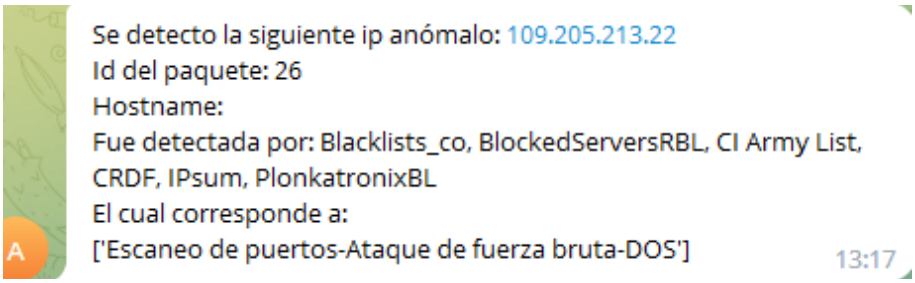


Fig. 67. Mensaje enviado al grupo de Telegram sobre la IP 109.205.213.22

Fuente: Elaboración propia

Paquete anómalo detectado el 24 de Julio 2023 con la siguiente IP: 202.124.44.232 lo cual fue detectado por 5 motores diferentes de análisis: CRDF, IPSpamList, IPsum, JustSpam_org, S5hbl, las cuales corresponden a Sitio web malicioso estándar [108].

Fig. 68. Parte 2 del detalle del análisis de la IP 109.205.213.22

Fuente: Elaboración propia

Fig. 69. Parte 1 del detalle del análisis de la IP 202.124.44.232

Fuente: Elaboración propia

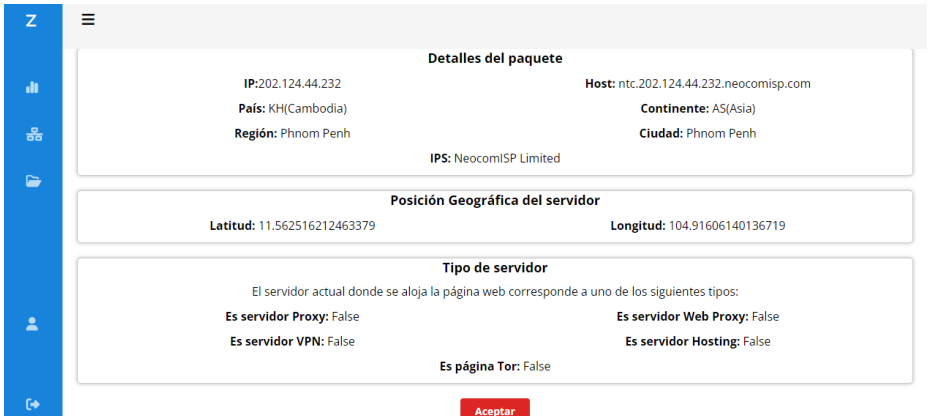


Fig. 70. Parte 2 del detalle del análisis de la IP 202.124.44.232

Fuente: Elaboración propia

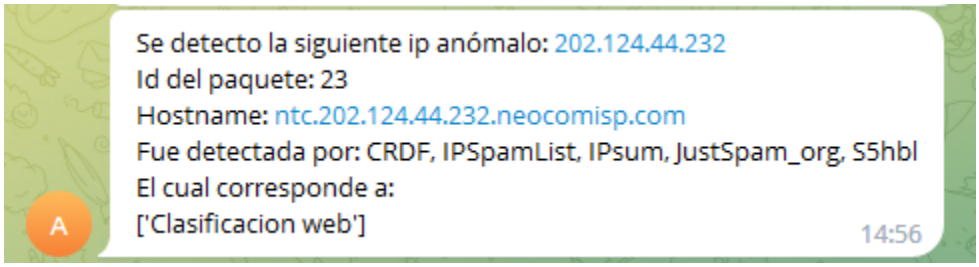


Fig. 71. Mensaje enviado al grupo de Telegram sobre la IP 202.124.44.232

Fuente: Elaboración propia

Paquete anómalo detectado el 30 de Junio 2023 con la siguiente IP: 209.197.3.8 lo cual fue detectado por 2 motores diferentes de análisis: CRDF, PlonkatronixBL, las cuales corresponden a página web anómala [110] e IP sospechosa y/o maliciosa [111].

Fig. 72. Parte 1 del detalle del análisis de la IP 209.197.3.8

Fuente: Elaboración propia

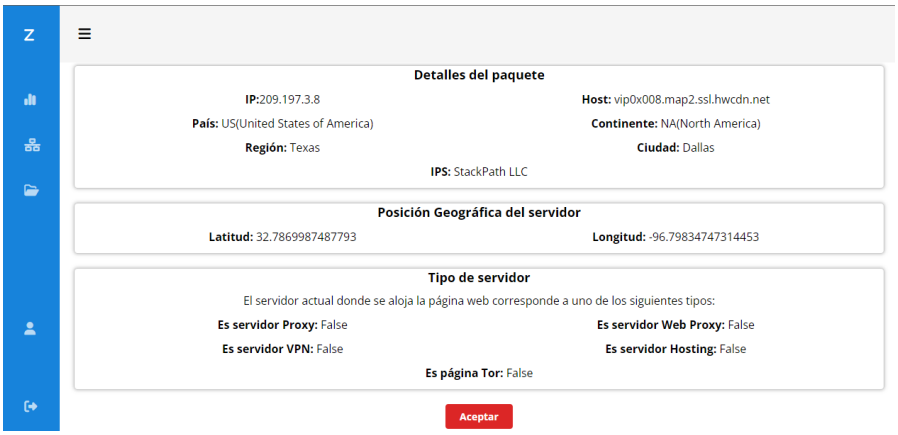


Fig. 73. Parte 2 del detalle del análisis de la IP 209.197.3.8

Fuente: Elaboración propia

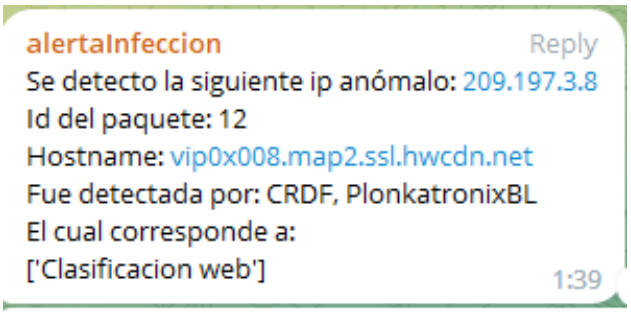


Fig. 74. Mensaje enviado al grupo de Telegram sobre la IP 202.124.44.232

Fuente: Elaboración propia

Paquete anómalo detectado el 22 de Julio 2023 con la siguiente IP: 192.33.4.12 lo cual fue detectado el motor de análisis: Etnetera BL, las cuales corresponden detección de anomalías en la red [112].

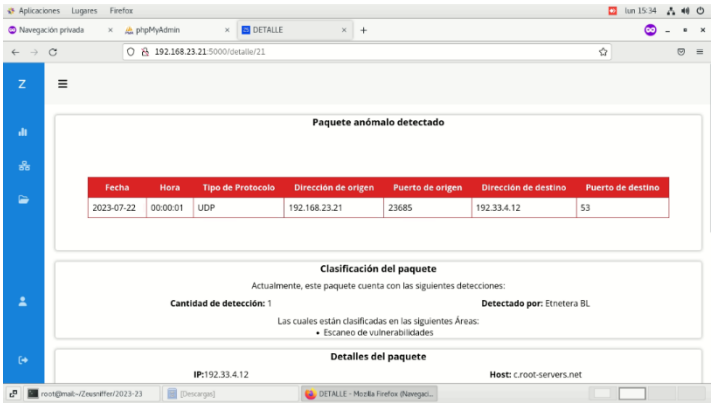


Fig. 75. Parte 1 del detalle del análisis de la IP 192.33.4.12

Fuente: Elaboración propia

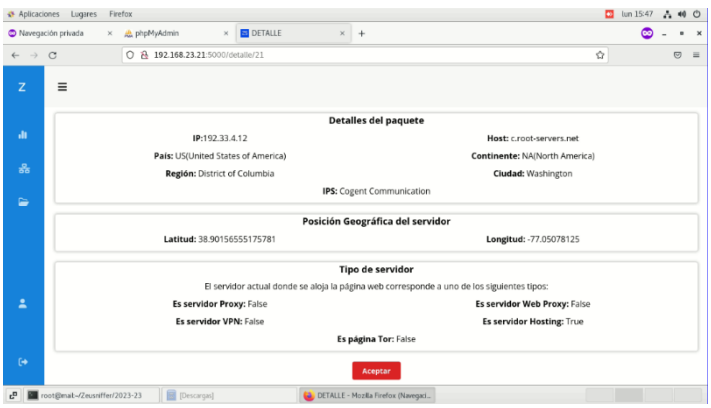


Fig. 76. Parte 2 del detalle del análisis de la IP 192.33.4.12

Fuente: Elaboración propia

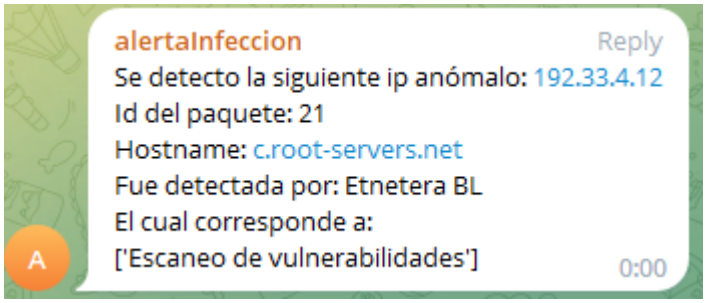


Fig. 77. Mensaje enviado al grupo de Telegram sobre la IP 192.33.4.12

Fuente: Elaboración propia

2.6. Resultados

2.6.1. Resultados finales

El trabajo propuesto del desarrollo de algoritmo para detección temprana de anomalías en tráfico URL, en redes distribuidas para la facultad de sistema y telecomunicaciones (FACSISTEL) de la Universidad estatal península de Santa Elena tiene como resultado lo siguiente:

- El algoritmo está diseñado para ser compatible con diversos sistemas operativos, tanto para Windows como Linux, siempre y cuando tenga las librerías necesarias instaladas.
- El algoritmo captura todos los paquetes que estén dentro de una trama específica de la red.
- El algoritmo tiene la capacidad de capturar y analizar N cantidad de paquetes, el rendimiento del mismo está ligado a la cantidad de máquinas dentro del segmento de red y la capacidad de infraestructura con la que cuenta el equipo en donde se encuentra instalado.
- Las herramientas que se seleccionaron para el desarrollo del algoritmo fueron la más idónea para el proceso planteado, permitiendo una correcta captura y análisis de paquetes.
- El algoritmo puede funcionar en conjunto con otros sistemas de seguridad como, antivirus o firewall, para de esta manera proporcionar una capa más de seguridad a la red de la institución.
- El administrador podrá ser notificado del ingreso a páginas anómalas vía Telegram.

- La Información del análisis de los paquetes podrá ser visualizada en el dashboard, de igual manera las estadísticas provenientes de los análisis referentes a paquetes anómalos y limpio.
- El dashboard permite la descarga de información de los análisis tanto en PDF como en formato Xlsx.
- El algoritmo tiene la capacidad de trabajar en conjunto con otras herramientas de seguridad como antivirus y firewall, de esta manera se agrega una capa más de seguridad a la red.
- En la siguiente imagen se muestra la estadística de captura de los análisis realizados en los últimos ocho días, este se realizó por un lapso de 30 minutos en dos horarios al día, los cuales fueron seleccionados de manera dinámica, en este se puede visualizar que dentro del tráfico capturado se detectó cierta cantidad de paquetes anómalos.

Fecha	Cantidad Limpios	Catidad Anomalos
2023-07-19	53393	67
2023-07-20	6997	1
2023-07-21	17334	1
2023-07-22	9258	60
2023-07-23	0	0
2023-07-24	29259	809
2023-07-25	47203	23
2023-07-26	979	536
Tiempo de cada analisis		
30 min		
Responsable: Armildo Salinas Tomalá		

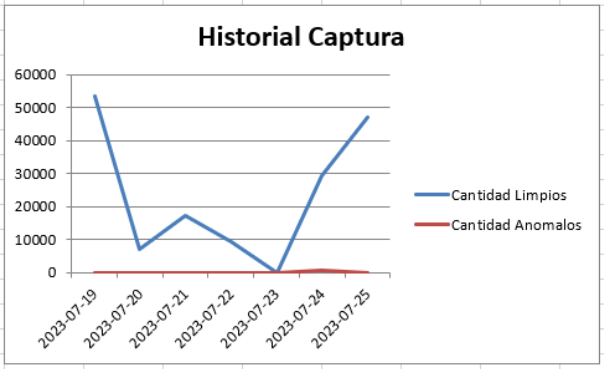


Fig. 78. Resultado de la captura y análisis de paquetes

Fuente: Elaboración propia

2.6.2. Resultados de las variables

A continuación, se presenta los resultados obtenidos referentes a la variable propuesta en el proyecto.

Variable: Cantidad de paquetes anómalos capturados dentro del segmento de red.

Durante una prueba realizada en un segmento de red se logra capturar 2800 paquetes, los cuales no fueron clasificados como anómalos o limpios, al

implementar el algoritmo dentro del mismo segmento y mismo lapso de tiempo, se recolectaron un total de 2694 paquetes de los cuales se clasificaron 2489 como limpios y 205 como anómalos (Ver anexo 6).

Tabla 42 - Paquetes capturados y clasificados antes y después de la implementación del algoritmo

	Limpios	Anómalos	Paquetes recolectados
Antes del Algoritmo	0	0	2088
Después del Algoritmo	2489	205	2694

Con base a los resultados descritos, se puede observar una mejora en la capacidad de detección de paquetes anómalos, demostrando la efectividad del algoritmo al momento de detección y notificación de estos tipos de incidentes.

Conclusiones

- Las herramientas utilizadas para la elaboración del algoritmo y el dashboard, fueron seleccionadas tras comprarlas con otras que realicen el mismo funcionamiento o similar.
- La información de los escaneos podrá ser visualizada en el dashboard, la misma solo estará disponible para los usuarios registrados.
- Las notificaciones enviadas a Telegram son de la captura y análisis del día, si una página anómala ya fue notificada durante el día, esta no se notificará nuevamente.
- La notificación será enviada a un grupo de Telegram, cada notificación envida contendrá la información más relevante del análisis, como IP analizada, el ID del paquete, el host analizado, los motores de análisis por el que fue detectado y la categoría a la que corresponde el paquete anómalo detectado.
- El resultado de los análisis podrá ser descargados en documento formato PDF y formato Xlsx, para posteriormente poder ser utilizado en toma de decisiones dentro de la organización.

Recomendaciones

- Se recomienda que antes de ejecutar el algoritmo se instalen las librerías necesarias dentro del Sistema Operativo adecuado.
- Se sugiere que el algoritmo se ejecute en un servidor para mejorar el proceso de captura y análisis.
- Se propone que el personal administrativo revise periódicamente los resultados de los análisis.
- Se recomienda la revisión del sistema cada cierto tiempo para comprobar su correcto funcionamiento.
- Se recomienda que para futuros trabajos relacionados con la captura y análisis de paquetes web, se utilice la captura enfoca por flujo.

Bibliografía

[1] INTERPOL, «INTERPOL,» 4 Agosto 2020. [En línea]. Available: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19. [Último acceso: 12 Noviembre 2022].

[2] K. Team, «Kaspersky daily,» 17 Noviembre 2022. [En línea]. Available: https://latam.kaspersky.com/blog/panorama-amenazas-latam-2022/25509/. [Último acceso: 22 Julio 2023].

[3] UNIVERSIDAD ESTATAL PENINSULA DE SANTA ELENA, «upse,» 2021. [En línea]. Available: https://upse.edu.ec/images/2021/Mayo/ESTATUTO_REFORMADO_2021.pdf. [Último acceso: 7 Mayo 2022].

[4] Y. J. Payá, «Redes neuronales. Un modelo de clasificación para la detección de dominios DNS maliciosos.,» España- Castellon de la Plana, 2015.

[5] M. M. C. Maestre, «Detección de URLs maliciosas por medio de técnicas de aprendizaje automático,» Bogotá, Colombia, 2021.

[6] I. K. C. MANOSALVAS, «IMPLEMENTACIÓN DE UNA PLATAFORMA DE DETECCIÓN DE ACCESOS A SITIOS MALICIOSOS,» GUAYAQUIL - ECUADOR, 2016.

[7] OMSTD Project, « OMSTD Project,» OMSTD Project, 4 Diciembre 2014. [En línea]. Available: https://books.google.com.ec/books?id=wo6fDwAAQBAJ&printsec=frontcover&hl=es

&source=gbs_ge_summary_r&cad=0#v=onepage&q=OSMTD&f=false. [Último acceso: 28 Mayo 2023].

[8] S. G. Rivera, «BEEDIGITAL,» 6 Abril 2022. [En línea]. Available: https://www.beedigital.es/marketing/claves-para-disenar-un-dashboard-de-tu-estrategia-digital/. [Último acceso: 30 Enero 2023].

[9] Visual Studio Code, «Visual Studio Code,» Visual Studio Code, [En línea]. Available: https://code.visualstudio.com/docs. [Último acceso: 20 Diciembre 2022].

[10] J. D. Muñoz, «OpenWebinars,» OpenWebinars, 17 Noviembre 2017. [En línea]. Available: https://openwebinars.net/blog/que-es-flask/. [Último acceso: 23 Noviembre 2022].

[11] FLASK, «FLASK web development, one drop at a time,» [En línea]. Available: https://flask.palletsprojects.com/en/2.2.x/. [Último acceso: 31 Enero 2023].

[12] APIVoid, «APIVoid,» APIVoid, [En línea]. Available: https://www.apivoid.com/api/ip-reputation/. [Último acceso: 18 Mayo 2023].

[13] Telegram, «Telegram,» [En línea]. Available: https://core.telegram.org/bots/api. [Último acceso: 23 Noviembre 2022].

[14] Apachefriends, «Apachefriends,» Apachefriends, [En línea]. Available: https://www.apachefriends.org/es/index.html. [Último acceso: 19 Abril 2023].

[15] Balsamiq, «balsamiq,» balsamiq, [En línea]. Available: https://balsamiq.com/wireframes/. [Último acceso: 19 Abril 2023].

[16] phpmyadmin, «phpmyadmin,» phpmyadmin, [En línea]. Available: https://www.phpmyadmin.net/. [Último acceso: 19 Abril 2023].

[17] desarrolloweb.com, «desarrolloweb.com,» [En línea]. Available: https://desarrolloweb.com/home/mysql. [Último acceso: 23 Noviembre 2022].

[18] KimiNew, «GitHub,» [En línea]. Available: http://kiminewt.github.io/pyshark/. [Último acceso: 23 Noviembre 2022].

[19] Sxapy, «Scapy,» [En línea]. Available: https://scapy.net/. [Último acceso: 22 Julio 2023].

[20] Pandas, «Pandas,» Pandas, [En línea]. Available: https://pandas.pydata.org/. [Último acceso: 19 Abril 2023].

[21] Request, «Request,» 2013. [En línea]. Available: https://requests.readthedocs.io/projects/es/es/latest/. [Último acceso: 22 Julio 2023].

[22] matplotlib, «matplotlib,» matplotlib, [En línea]. Available: https://matplotlib.org/. [Último acceso: 19 Abril 2023].

[23] Chart.js, «chart.js,» 28 Abril 2023. [En línea]. Available: https://www.chartjs.org/docs/latest/. [Último acceso: 23 Julio 2023].

[24] Joshua.Tauberer, «pypi,» 19 abril 2023. [En línea]. Available: https://pypi.org/project/email-validator/. [Último acceso: 22 Julio 2023].

[25] ReportLab, «ReportLab,» ReportLab, [En línea]. Available: https://docs.reportlab.com/. [Último acceso: 19 Abril 2023].

[26] J. McNamara., «XlsxWriter,» [En línea]. Available: https://xlsxwriter.readthedocs.io/index.html. [Último acceso: 23 Julio 2023].

[27] M. Grinberg, «Flask-SocketIO,» Flask-SocketIO, 2018. [En línea]. Available: https://flask-socketio.readthedocs.io/en/latest/. [Último acceso: 19 Abril 2023].

[28] 4Geeks, «4Geeks,» [En línea]. Available: https://4geeks.com/lesson/everything-you-need-to-start-using-sqlalchemy. [Último acceso: 23 Noviembre 2022].

[29] Pypi, «Pypi,» Pypi, 25 Abril 2021. [En línea]. Available: https://pypi.org/project/sqlclient/. [Último acceso: 19 Abril 2023].

[30] Pypi, «Pypi,» Pypi, 27 Marzo 2023. [En línea]. Available: https://pypi.org/project/pymysql/. [Último acceso: 19 Abril 2023].

[31] UNIVERSIDAD ESTATAL “PENÍNSULA DE SANTA ELENA”, «Resolución RCF-FST-SO-09 No. 03-2021,» Santa Elena- LA libertad, 2021.

[32] Worldometers, «Worldometers,» [En línea]. Available: https://www.worldometers.info/. [Último acceso: 12 Diciembre 2022].

[33] IBM, «IBM,» [En línea]. Available: https://www.ibm.com/es-es/topics/network-security. [Último acceso: 12 Diciembre 2022].

[34] ESET, «ESET,» Junio 2021. [En línea]. Available: https://www.welivesecurity.com/wp-content/uploads/2021/06/ESET-security-report-LATAM2021.pdf. [Último acceso: 12 Diciembre 2022].

[35] S. N. d. Planificación, «Plan de Creación de Oportunidades,» de *Plan de Creación de Oportunidades*, Quito, 2021, p. 64.

[36] M. Orlando Zafra Galvis, «Tipos de Investigación,» *Revista Científica General José María Córdova,* vol. IV, nº 4, pp. 13-14, 2006.

[37] D. J. M. Capa, «INVESTIGACIÓN DIAGNOSTICA OBTENCIÓN Y RECOLECCIÓN DE DATOS PRIMARIOS,» 10 Julio 2020. [En línea]. Available:

https://es.slideshare.net/DenisseJMaza/investigacion-diagnostica-236627991. [Último acceso: 18 Diciembre 2022].

[38] J. M. O. Candel, Hacking ético con herramientas Python, Colombia, Bogotá: Editorial Ra-ma(España), 2018.

[39] Blue Hat corporation, «Blue Hat corporation,» 13 Diciembre 2022. [En línea]. Available: https://www.bluehatcorp.com/iso-27032-ciberseguridad-inicio/. [Último acceso: 20 Diciembre 2022].

[40] isec auditors, «isec auditors,» [En línea]. Available: https://www.isecauditors.com/consultoria-csf-iso-27032. [Último acceso: 20 Diciembre 2022].

[41] U. E. P. d. S. Elena, «UPSE,» 22 Julio 1998. [En línea]. Available: https://www.upse.edu.ec/secretariageneral/images/archivospdfsecretaria/5.%20INSTRUCTIVOS/09%20EXPEDIR%20EL%20INSTRUCTIVO%20DE%20POLITICAS%20DE%20GESTIONINSTITUCIONAL%20DE.pdf. [Último acceso: 9 Mayo 2022].

[42] UPSE, «Universidad Estatal Peninsula de Santa Elena (UPSE),» 14 Diciembre 2021. [En línea]. Available: https://www.upse.edu.ec/index.php?option=com_content&view=article&id=12&Itemid=167. [Último acceso: 9 Mayo 2023].

[43] Google, «Google Maps,» Google Maps, [En línea]. Available: https://goo.gl/maps/MEeDzjKuKaXKSJPM6. [Último acceso: 28 Mayo 2023].

[44] R. D. ECUADOR, CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR, LexisFinder, 2008.

[45] R. D. E. A. NACIONAL, CÓDIGO ORGÁNICO INTEGRAL PENAL, COIP, LexisFinder, 2021.

[46] ASAMBLEA NACIONAL, «LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES,» Quito, 2021.

[47] A. López, Seguridad Informatica, EDITEX, 2010.

[48] J. Mieres, Ataques informáticos Debilidades de seguridad comúnmente explotadas, Evil fingers, 2009.

[49] M. Á. P. García, «inkedin,» 30 Marzo 2019. [En línea]. Available: https://es.linkedin.com/pulse/redes-centralizadas-vs-distribuidas-miguel-%C3%A1ngel-p%C3%A9rez-garc%C3%ADa. [Último acceso: 9 Mayo 2023].

[50] A. Patcha y J.-M. Park, «An overview of anomaly detection techniques: Existing solutions and latest technological trends,» *ScienceDirect,* vol. 51, nº 12, pp. 3448-3470, 22 Agosto 2007.

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

[52] W. B. ANJELINO, «HARASDADICO,» HARASDADICO, 27 noviembre 2022. [En línea]. Available: https://www.harasdadinco.cl/que-es-analisis-de-paquetes/#:~:text=El%20an%C3%A1lisis%20de%20paquetes%20otorga,ella%20facilitar%20un%20an%C3%A1lisis%20estad%C3%ADstico.. [Último acceso: 5 junio 2023].

[53] Corporation Pvt.Ltd.All, «ManageEngine,» NetFlow Analyzer, [En línea]. Available: https://www.manageengine.com/latam/netflow/que-es-netflow.html. [Último acceso: 5 junio 2023].

[54] C. A. G. Barría, «Análisis de la Tecnología IP sobre WDM,» 2006. [En línea]. Available: http://cybertesis.uach.cl/tesis/uach/2006/bmfcig216a/sources/bmfcig216a.pdf. [Último acceso: 6 junio 2023].

[55] A. F. R. Calderon, W. C. L. Valero y J. M. L. Mateus, «ESTRATEGIA PARA LA ACTUALIZACIÓN DE PROTOCOLO DE DIRECCIONAMIENTO IP EN UNA EMPRESA, TRANSFIRIENDO DESDE LA TECNOLOGIA IPv4 HACIA IPv6,» 2022. [En línea]. Available: https://repository.ucc.edu.co/server/api/core/bitstreams/209a095f-1e8a-4f0c-8fa2-23d293dde248/content. [Último acceso: 25 Julio 2023].

[56] E. M. G. BÁRCENES, «SEGURIDAD INFORMATICA POR CAPAS PARA LA PROTECCION DE LA INFORMACION EN LA INTRANET DE LA COOPERATIVA DE AHORRO Y CREDITO JUAN PIO DE MORA.,» diciembre 2015. [En línea]. Available: http://dspace.uniandes.edu.ec/handle/123456789/1814. [Último acceso: 5 junio 2023].

[57] A. G. d. León y A. G. Díaz, «LOS SITIOS WEB COMO ESTRUCTURAS DE INFORMACIÓN: Un primer abordaje en los criterios de calidad,» *Biblios,* vol. 3, nº 12, 2002.

[58] V. Chandola, A. Banerjee y V. Kumar, «Anomaly Detection: A Survey,» *To Appear in ACM Computing Surveys,* pp. 4-192, 15 Agosto 2007.

[59] J. R. Ruiz, «Detección de Malware, Métodos Estadísticos y Machine Learning.,» 2019. [En línea]. Available: https://openaccess.uoc.edu/bitstream/10609/89547/6/jaruizrTFM0119memoria.pdf. [Último acceso: 19 Junio 2023].

[60] H. H. C. Huamán, A. Han y L. S. García, «Detección Automática de Sitios Web Fraudulentos,» Junio 2020. [En línea]. Available: https://eprints.ucm.es/id/eprint/68262/1/CORONADO_HUAMAN_Deteccion_Automatica_de_Sitios_Web_Fraudulentos_4398577_603315633.pdf. [Último acceso: 19 Junio 2023].

[61] J. L. R. Pérez, «modelo basado en firmas, el modelo basado en aprendizaje automático, el modelo basado en aprendizaje profundo y el modelo híbrido,» *Revista Cubana de Ciencias Informáticas,* vol. 8, nº 4, pp. 52-73, 2014.

[62] S. Tejal, «GEEKFLARE,» GEEKFLARE, 9 Enero 2023. [En línea]. Available: https://geekflare.com/es/anomaly-detection/. [Último acceso: 27 Mayo 2023].

[63] Q. Zhang y T. Chu, «Structure regularized traffic monitoring model for traffic matrix estimation and anomaly detection,» *IEEE,* nº 34, pp. 4980-4985, 2015.

[64] D. Á. P. Gómez, J. J. R. Jalca, J. G. García, O. Q. Sánchez, K. M. Parrales y J. M. Merino, FUNDAMENTOS SOBRE LA GESTIÓN DE BASE DE DATOS, ALCOY: Área de Innovación y Desarrollo,S.L., 2017.

[65] D. H. RAMÍREZ, «EL MACHINE LEARNING A TRAVÉS DE LOS TIEMPOS, Y LOS APORTES A LA,» 2018. [En línea]. Available: https://repository.unilibre.edu.co/bitstream/handle/10901/17289/EL%20MACHINE%20LEARNING.pdf?sequence=1&isAllowed=y. [Último acceso: 9 Mayo 2023].

[66] Cámara de Comercio de Bogotá, «Cámara de Comercio de Bogotá,» 9 Enero 2019. [En línea]. Available: http://hdl.handle.net/11520/22728. [Último acceso: 15 Mayo 2023].

[67] I. Belcic, «Avast,» 19 Abril 2023. [En línea]. Available: https://www.avast.com/es-es/c-malware#:~:text=Malware%20es%20un%20t%C3%A9rmino%20general,el%20sistema%20o%20robar%20datos. [Último acceso: 15 Mayo 2023].

[68] Karpersky, «Karpersky,» 2023. [En línea]. Available: https://latam.kaspersky.com/resource-center/definitions/pharming. [Último acceso: 15 Mayo 2023].

[69] M. S. M. Leguizamón, «EL PHISHING,» Universitat Jaume I, 2015.

[70] Kaspersky, «Kaspersky,» [En línea]. Available: https://latam.kaspersky.com/resource-center/preemptive-safety/how-to-stop-spam-texts. [Último acceso: 18 Mayo 2023].

[71] Python, «python,» python, [En línea]. Available: https://docs.python.org/3/tutorial/index.html. [Último acceso: 19 Mayo 2023].

[72] R. C. Z. Martínez, «ANÁLISIS Y CAPTURA DE PAQUETES DE DATOS EN UNA RED MEDIANTE LA HERRAMIENTA WIRESHARK,» Universidad Tecnológica Israel, Quito-Ecuador, 2011.

[73] I. M.-P. P. N. R.-F. M. y. P.-T. R. REYES-DE LOS SANTOS, «Dashboard para el Tutor,» *Revista_de_Investigación_y_Desarrollo,* vol. 2, nº 4, p. 5, 2016.

[74] C. Ospina y N. Milena, DEFENSA EN PROFUNDIDAD PARA LA PROTECCION CONTRA LAS AMENAZAS PERSISTENTES AVANZADAS, Bogota: UNIVERSIDAD PILOTO DE COLOMBIA – ESPECIALIZACION SEGURIDAD INFORMATICA, 2019.

[75] C. Mezquida Salva, «Universidad Oberta de Catalunya,» 2019 Diciembre 29. [En línea]. Available: http://hdl.handle.net/10609/107627. [Último acceso: 15 Mayo 2023].

[76] D. O. d. Penha, J. B. T. Corrêa y C. A. P. S. Martins, «Análise Comparativa do Uso de Multi-Thread e OpenMP Aplicados a Operações de Convolução de Imagem,» *SBC,* vol. III, pp. 118-125, 202.

[77] FastAPI, «FastAPI,» [En línea]. Available: https://fastapi.tiangolo.com/. [Último acceso: 31 Enero 2023].

[78] V. S. Khatri y R. Johns, «Flask vs Django: Which Python Web Framework to Use in 2023?,» 28 marzo 2023. [En línea]. Available: https://hackr.io/blog/flask-vs-django. [Último acceso: 11 junio 2023].

[79] D. Ghimi, «Comparative study on Python web frameworks: Flask and,» 5 Mayo 2020. [En línea]. Available: https://www.theseus.fi/bitstream/handle/10024/339796/Ghimire_Devndra.pdf?sequence=2&isAllowed=y. [Último acceso: 12 Junio 2023].

[80] E. Amoany, «RdHat,» 10 noviembre 2020. [En línea]. Available: https://www.redhat.com/sysadmin/using-wireshark-tshark1. [Último acceso: 11 junio 2023].

[81] Digital Services, «Digital Services,» 1 septiembre 2020. [En línea]. Available: https://santandergto.com/guia-uso-de-scapy-con-python/. [Último acceso: 11 junio 2023].

[82] InnovaciónDigital360, «InnovaciónDigital360,» 12 enero 2023. [En línea]. Available: https://www.innovaciondigital360.com/cyber-security/que-es-virustotal/. [Último acceso: 11 junio 2023].

[83] P. O. MONTEJO, «Ofuscament de malware per al bypass dels antivirus comercials,» Febrero 2021. [En línea]. Available: https://upcommons.upc.edu/bitstream/handle/2117/339432/memoria_TFG-340GREIN18.pdf?sequence=2&isAllowed=y. [Último acceso: 11 Junio 2023].

[84] D. DELÉGLISE, MySQL 5 (versiones 5.1 a 5.6): Guía de referencia del desarrollador, Ediciones ENI, 2013.

[85] M. Juszczyk y E. Milosz, «SELECCIÓN DE HERRAMIENTAS DE DISEÑO DE BASES DE DATOS DE CÓDIGO ABIERTO PARA USO EN LA ENSEÑANZA DE CIENCIAS DE LA COMPUTACIÓN,» *Conferencia Internacional Anual de Educación, Investigación e Innovación,* pp. 921-926, 14 Noviembre 2018.

[86] G. M. Esteban, «Control avanzado de recursos protegidos,» 2017. [En línea]. Available: https://oa.upm.es/51569/1/TFG_GUILLERMO_MARTINEZ_ESTEBAN.pdf. [Último acceso: 12 Junio 2023].

[87] Discord, «Discord,» DEVELOPER PORTAL, [En línea]. Available: https://discord.com/developers/docs/getting-started. [Último acceso: 12 Junio 2023].

[88] J. A. Ávila, «Implementación de WhatsApp Business como solución basada en las tecnologías de la información para mejorar la comunicación en organizaciones educativas sin fines de lucro,» Universidad Autónoma de Querétaro, Querétaro, 2021.

[89] J. Smith, «Instituto Americano de Gráficos,» 13 Diciembre 2022. [En línea]. Available: https://www.agitraining.com/ux/classes/figma-vs-sketch-vs-xd-prototyping-apps. [Último acceso: 12 Junio 2023].

[90] CAPTERRA, «CAPTERRA,» CAPTERRA, [En línea]. Available: https://www.capterra.com/prototyping-software/compare/145723-175027/Balsamiq-Mockups-vs-Figma. [Último acceso: 12 Junio 2023].

[91] J. Nunes-Iglesias, S. v. d. Walt y H. Dashnow, Elegant SciPy, Estados Unidos de America: O´Reilly Media, Inc, 2017.

[92] DataScientest, «DataScientest,» [En línea]. Available: https://datascientest.com/es/pandas-python. [Último acceso: 13 Junio 2023].

[93] Aprendeconalf, «Aprendeconalf,» [En línea]. Available: https://aprendeconalf.es/docencia/python/manual/matplotlib/. [Último acceso: 7 Febrero 2023].

[94] D. Rodríguez, «ANALYTICS LANE,» 20 Julio 2018. [En línea]. Available: https://www.analyticslane.com/2018/07/20/visualizacion-de-datos-con-seaborn/#:~:text=Seaborn%20es%20una%20librer%C3%ADa%20para,defecto%20en%20la%20distribuci%C3%B3n%20Anaconda.. [Último acceso: 7 Febrero 2023].

[95] B. D. e. I. Artificial, «ITELLIGENT,» 6 Septiembre 2018. [En línea]. Available: https://itelligent.es/es/tag/plotly/#:~:text=y%20datos%20personalizados.-,Caracter%C3%ADsticas%3A,a%20los%20datos%20de%20Twitter.. [Último acceso: 7 Febrero 2023].

[96] PyFPDF, «PyFPDF,» [En línea]. Available: https://pyfpdf.readthedocs.io/en/latest/FAQ/index.html#how-does-this-library-compare-to. [Último acceso: 13 Junio 2023].

[97] Recursos Python, «Recursos Python,» Recursos Python, 3 Julio 2018. [En línea]. Available: https://recursospython.com/guias-y-manuales/crear-documentos-pdf-en-python-con-reportlab/. [Último acceso: 13 Junio 2023].

[98] E. Gazoni y C. Clark, «openpyxl,» 11 Marzo 2023. [En línea]. Available: https://openpyxl.readthedocs.io/en/stable/. [Último acceso: 24 Julio 2023].

[99] DISSENY, «PSICOLOGIA DEL COLOR,» [En línea]. Available: https://perio.unlp.edu.ar/catedras/iddi/wp-content/uploads/sites/125/2020/04/Psicologia-del-color.pdf. [Último acceso: 31 Enero 2023].

[100] CarolinaDibarratDaniel, «CIBERSEGURIDADCOMO HERRAMIENTA FUNDAMENTAL,ANTE LA INMINENTE AMENAZA GLOBAL,» *Revista Ensayos Militares,* vol. 8, nº 1, pp. 33-51, 2023.

[101] Universidad Nacional de Plata, «Universidad Nacional de Plata,» 2017. [En línea]. Available: https://www.econo.unlp.edu.ar/detise/amenazasinformaticas-3918. [Último acceso: 26 Junio 2023].

[102] SANS, «SANS,» SANS, 2022. [En línea]. Available: https://www.sans.org/information-security-policy/. [Último acceso: 26 Julio 2023].

[103] SANS, «SANS,» 2022. [En línea]. Available: https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt207beda4b7c14d22/636f1a30e3836b0c88e8f0a8/Acceptable_Use_Policy.pdf. [Último acceso: 26 Julio 2023].

[104] SANS, «SANS,» 2022. [En línea]. Available: https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/bltc7c9696ebeb0c083/636f12e0a7c5e176a54fda5f/Lab_Security_Policy.pdf. [Último acceso: 26 Julio 2023].

[105] SANS, «SANS,» 2022. [En línea]. Available: https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt0002043f11ac7d81/5e9e08ced275f070a0330ba0/employee_internet_use_monitoring_and_filtering_policy.pdf. [Último acceso: 26 Julio 2023].

[106] SANS, «SANS,» 2022. [En línea]. Available: https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/bltec1d5c2b1e7d13b3/5e9e04a233f6b8718946a34d/internet_usage_policy.pdf. [Último acceso: 26 Julio 2023].

[107] Barracuda, «Barracuda Reputation,» Barracuda Reputation, [En línea]. Available: https://www.barracudacentral.org/lookups. [Último acceso: 19 julio 2023].

[108] BLACKLISTS.CO, «BLACKLISTS.CO,» 2018. [En línea]. Available: http://blacklists.co/. [Último acceso: 27 Julio 2023].

[109] CINS.com, «Puntuacion CINS.com,» [En línea]. Available: http://cinsscore.com/#list. [Último acceso: 27 Julio 2023].

[110] CRDF LABS, «CRDF LABS,» 2000-2023. [En línea]. Available: https://threatcenter.crdf.fr/check.html. [Último acceso: 27 Julio 2023].

[111] @stamparm, «GitHub,» [En línea]. Available: https://github.com/stamparm/ipsum. [Último acceso: 27 Julio 2023].

[112] Etnetera BL, «Etnetera BL,» Etnetera BL, [En línea]. Available: https://www.etnetera.cz/bezpecnostni-monitoring-site. [Último acceso: 31 Julio 2023].

ANEXOS

Anexo 1:Recopilacion de información de los laboratorios

UNIVERSIDAD ESTATAL PENINSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

Desarrollo de algoritmo para detección temprana de anomalías en tráfico URL, en redes distribuidas para la Facultad de Sistema y Telecomunicaciones (FACSISTEL) de la Universidad Estatal Península de Santa Elena

Fase: Entendimiento de la Organización

Objetivos de la Fase:

- Recopilar información de actividades en él laboratorio.
- Observar el uso dado de los laboratorios dentro de las actividades estudiantiles.

Técnica:

Se utilizó un estudio de observación para la recopilación de información.

Tipo de Observación:

Natural

Tiempo de ejecución	48 horas
Fecha del estudio	16 de noviembre del 2022 – 17 noviembre del 2022

Procedimiento:

Mediante el estudio de observación se recopila información de los laboratorios.

Resultados:

Como resultado se obtuvieron la siguiente información:

- ✓ En total, se identificaron 52 ordenadores distribuidos en los laboratorios 1,2 y 3
- ✓ Los ordenadores se utilizan tanto en la jornada matutina como en la vespertina.

- ✓ Los estudiantes utilizan los ordenadores principalmente para actividades de investigación y desarrollo.
- ✓ Se observo que muchos estudiantes acceden a las primeras páginas recomendadas por el navegador al buscar información en internet.
- ✓ La institución cuenta con tres páginas web activas, siendo la de ambiente virtual de aprendizaje la más usada por la comunidad estudiantil para actividades académicas, seguida del SGA UPSE y la página principal de la Universidad Estatal Península de santa Elena.
- ✓ Los estudiantes suelen visitar blogs y sitios no considerados oficiales al buscar información.
- ✓ Algunas páginas requieren que los estudiantes creen cuentas e ingresen sus datos personales para acceder a la información.
- ✓ En caso de que un ordenador sea infectado con virus debe ser notificado al técnico docente para que este comunique al personal de tics correspondiente.
- ✓ No se realiza un monitoreo en tiempo real del acceso a páginas con contenido anómalo por parte del administrador.
- ✓ Los horarios con mayor cantidad de usuarios conectados a la red son de 9 a 10 am y 3 a 4 pm
- ✓ Durante los horarios con actividades educativas, se observa un mayor número de usuarios navegando por internet en los laboratorios de la Facultad

Responsable:	Armildo Shrriber Salinas Tomalá

Anexo 2. Recopilación de Información de la Infraestructura de los Laboratorios

UNIVERSIDAD ESTATAL PENINSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

Desarrollo de algoritmo para detección temprana de anomalías en tráfico URL, en redes distribuidas para la Facultad de Sistema y Telecomunicaciones (FACSISTEL) de la Universidad Estatal Península de Santa Elena

Fase: Entendimiento de la Organización

Objetivos de la Fase:

- Recopilar información de infraestructura de la institución.
- Revisar el uso dado a los ordenadores de la institución en actividades académicas.

Técnica:

Se utilizó un estudio de observación para la recopilación de información.

Tipo de Observación:

Natural

Tiempo de ejecución	3 horas
Fecha del estudio	22 de mayo del 2023

Procedimiento:

Mediante el estudio de observación se recopila información de los laboratorios.

Resultados:

Como resultado se obtuvieron la siguiente información:

- ✓ El laboratorio 2 y 3 cuentan con un total de 22 ordenadores cada uno.
- ✓ El laboratorio 1 cuenta actualmente con 8 ordenadores.
- ✓ Entre los procesadores utilizados en los ordenadores de los laboratorios se encuentran los modelos AMD Ryzen 7 2700 Eing-Core Processor 3.20 GHz e Intel Core i5-4460 CPU 3.20 GHz
- ✓ La memoria RAM de las máquinas varía de 4GB a 8 GB
- ✓ Se Identifica dos tipos diferentes de tarjeta gráfica: NVIDIA GeForce GT 710 e Intel HD Graphics 4600
- ✓ Todos los ordenadores cuentan con 17 puertos, incluyendo puertos USB 2.0 y 3.0, puertos DVI Video, VGA, PS/2, Minijack y puertos LAN con conectores RJ45.
- ✓ En el laboratorio 3 se encuentra un switch.
- ✓ Los ordenadores del laboratorio 3 están conectados al switch presente en el mismo que a su vez se conectan al enrutador principal ubicado en el área administrativa.
- ✓ En el área administrativa se encuentra switch y enrutadores para proporcionar servicio de internet a los laboratorios.
- ✓ Los ordenadores de los laboratorios 2 y 3 están conectados a switch ubicados en el área administrativa que a su vez se conectan al enrutador.

✓ Se observó una mejor conexión utilizando la entrada LAN de los ordenadores en comparación a la señal Wi-Fi. ✓ Los ordenadores de los laboratorios se utilizan principalmente en actividades académicas, tanto de desarrollo como investigación. ✓ Los navegadores comúnmente utilizados son Google Crome y Mozilla Firefox, los cuales se encuentran instalados en los ordenadores.

Responsable:	Armildo Shrriber Salinas Tomalá

Anexo 3. Análisis de navegación por internet

UNIVERSIDAD ESTATAL PENINSULA DE SANTA ELENA **FACULTAD DE SISTEMAS Y TELECOMUNICACIONES** **CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN**
Desarrollo de algoritmo para detección temprana de anomalías en tráfico URL, en redes distribuidas para la Facultad de Sistema y Telecomunicaciones (FACSISTEL) de la Universidad Estatal Península de Santa Elena
Fase: Análisis de Riesgo
Objetivos de la Fase: • Identificar la existencia de páginas sin bloqueadas por el firewall, pero con contenido anómalo. • Identifica posibles debilidades o vulnerabilidades en el firewall que puedan permitir eludir su protección • Recopilar información sobre los métodos más usados para navegar sin restricciones por parte de los estudiantes.
Técnica: Se utilizó un estudio de observación para la recopilación de información. Tipo de Observación: Natural

Tiempo de ejecución	3 días
Fecha del estudio	22 de junio del 2023 – 26 junio del 2023
Procedimiento:	

Mediante el estudio se utilizaron varios métodos para navegar por internet sin el bloqueo del firewall.

Búsqueda en la web en páginas sin detectar por el firewall, que tienen cometido sospechoso.

Se utilizo un estudio de observación para la recopilación de información.

Tipo de Observación:

Natural

Resultados:

Como resultado se obtuvieron la siguiente información:

- ✓ Se puede eludir el firewall por medio del uso de servidores proxi, entre los usados para la prueba tenemos los siguientes:
  - Kproxy
  - Hidester
  - Hideme
- ✓ Se puede eludir el firewall por medio del uso de VPN, entre los usados para esto tenemos:

  VPN para Pc
  - Psiphon

  VPN para móvil
  - 1.1.1.1 vpn
  - Fast VPN Free
- ✓ Se puede eludir el firewall por medio del uso de traducción de página de Google translate.
- ✓ Existen páginas que no están siendo bloqueados por el firewall, pero al ingresar en ella los antivirus del computador como 360 Total Security o extensiones de seguridad en el navegador como Adaware adBlock o Malwarebytes Browser Guard, entre las páginas en las cuales hemos encontrado esta novedad tenemos los siguientes:
  - www.Vertvenvivo.net
  - w4.cuevana3.ia
  - ww3.animeonline.ninja
  - www.serieslan.com

▪ www.apkmirror.com ✓ Es posible eludir el firewall de una institución llevando ya precargada la página a la red de la institución. Esto se debe a que el firewall controla el tráfico que entra y sale de la red, pero no tiene control sobre el tráfico que ya está dentro de la red. ✓ Se pudo observar que la mayoría de estudiantes hacen uso de VPN, por otro lado las opciones de usar servidores proxi o páginas pre cargadas son poco conocidos y usados, la opción del uso de Google Translate, es totalmente desconocida.

Responsable:	Armildo Shrriber Salinas Tomalá

Anexo 4. Resultado de análisis de paquetes

UNIVERSIDAD ESTATAL PENINSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

Desarrollo de algoritmo para detección temprana de anomalías en tráfico URL, en redes distribuidas para la Facultad de Sistema y Telecomunicaciones (FACSISTEL) de la Universidad Estatal Península de Santa Elena	
Fase: Análisis de Riesgo	
Objetivos de la Fase: • Realizar un escaneo con el algoritmo desarrollado durante un lapso de tiempo determinado.	
Técnica: Análisis mediante el algoritmo desarrollado.	
Tiempo de ejecución	8 días
Fecha del estudio	19 de julio del 2023 – 26 julio del 2023
Procedimiento: Se procedió a ejecutar el algoritmo desarrollado dentro de las instalaciones de la Facultad, en un segmento de red de rango 23 (192.168.23.1), este funciono por 30 min en la mañana y en la tarde en horarios dinámicos.	
Resultados:	

Como resultado se obtuvieron la siguiente información:

- ✓ Se obtuvo un promedio de 20552 paquetes limpios y 187 paquetes anómalos durante los ocho días de análisis.
- ✓ Los días con más detecciones de anomalías fueron los siguientes:
    - 24 de Julio con un total de 809 paquetes anómalos.
    - 26 de julio con un total de 536 paquetes anómalos.
    - 19 de julio con un total de 67 paquetes anómalos.
    - 22 de julio con un total de 60 paquetes anómalos.
    - 25 de julio con un total de 23 paquetes anómalos.
    - Los demás días tuvieron 1 o 0 paquetes anómalos.
- ✓ Las notificaciones enviadas al grupo de Telegram fueron de 1 a 6 por día.
- ✓ Una de la facilidad del algoritmo es que, si un paquete ya fue notificado, este no se volverá a notificar hasta el día siguiente, sin embargo, dentro del dashboard y en la sección de historial del escaneo diario, se muestra los paquetes reincidentes detectados.
- ✓ La cantidad de paquetes reincidente se debe a las reiteradas peticiones enviadas a la página web, estas debido a las estandarizas por los protocolos web, la navegación en la página o subpáginas de la misma.
- ✓ En el lapso de periodo de escaneo se detectó lo siguiente referente a los motores de análisis.
    - Se obtuvo un promedio de una notificación por día de página detectada por CRDF, correspondiente a sitio web malicioso.
    - Detección con el motor de análisis JustSpam_org, solo se notificaron tres veces en todo el tiempo de escaneo, este corresponde a sitios web que se detectaron que enviaban de manera masiva correos de Spam con link que los redirigía a ellos.
    - Solo una notificación sobre una detección realizada por el motor ThreatLog, correspondiente a un sitio web que trabaja como un Heneypots.

- Se notificó una sola vez un paquete detectado por el motor Backscatterer, correspondiente a una página con redireccionamiento de clic a otra página con contenido anómalo. - Solo una notificación de detención por el motor S5hbl, dos por el motor IPSpamList y una de Barracuda_Reputation_BL correspondiente a páginas web que envían correos Spam con link de redireccionamiento a la página. - Una notificación de motor BlackLists_co, correspondiente a sitio web con malware.	
Responsable:	Armildo Shrriber Salinas Tomalá

Anexo 5. Análisis de la red elaborado de forma normal con Wireshark y análisis realizado con la herramienta desarrollada Zeusniffer

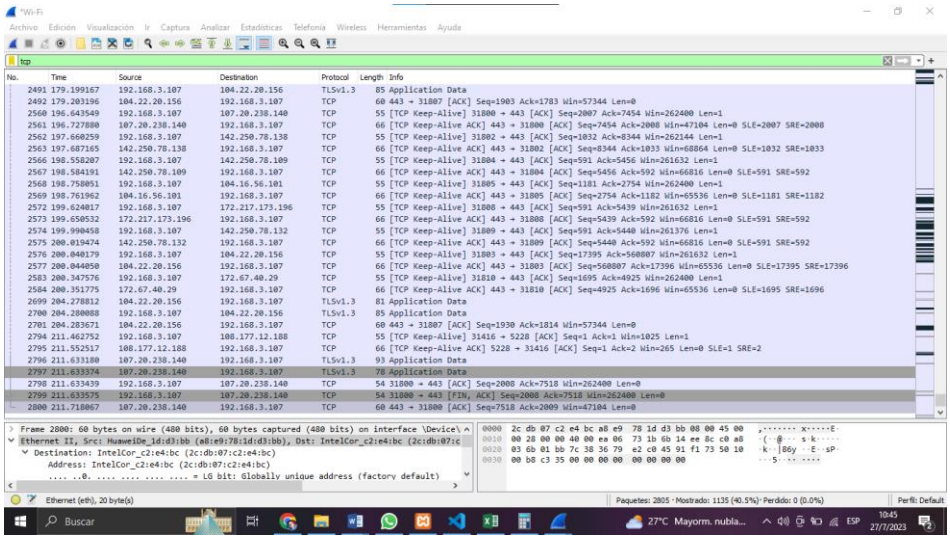


Fig. 79. Análisis empleado con Wireshark

Fuente: Elaboración propia

Fig. 80. Análisis empleando Zeusniffer

Fuente: Elaboración propia

Anexo 6. Clasificación de Listas Negras

Numero	Motores de análisis	Black list Apivoid	Botnet	Clasificacion web	Cryptojacking	Envió-Alojamiento-Correos masivos	Escaneo de puertos-Ataque de fuerza bruta-DOS	Escaneo de vulnerabilidades	Exe,Doc xls, Elf con malware	Honeypots	Hosting	IDS	IP telefónico malicioso	IRC	Lista Roja	Mail Login	Malware	Motores de Análisis secundario	Otros	Phishing-Abuso-Estafa	Rastreo-Espionaje	Redireccionamiento de clic	Script Kiddies	Spam	SSL maliciosas	Tor	Web server
1	Anti-Attacks BL																			X				X			
2	AntiSpam_by_CleanTalk																							X			
3	APEWS-L2					X																		X			
4	AZORult Tracker																X										
5	Backscatterer																					X					
6	Barracuda_Reputation_BL					X																		X			
7	Blacklists_co						X																				
8	BlockedServersRBL																	X									
9	Blocking_rocks																		X								

Numero	Motores de análisis	Black list Apivoid	Botnet	Clasificacion web	Cryptojacking	Envió-Alojamiento-Correos	Escaneo de puertos-Ataque de fuerza bruta-DOS	Escaneo de vulnerabilidades	Exe,Doc xls, Elf con malware	Honeypots	Hosting	IDS	IP telefónico malicioso	IRC	Lista Roja	Mail Login	Malware	Motores de Análisis secundario	Otros	Phishing-Abuso-Estafa	Rastreo-Espionaje	Redireccionamiento de clic	Script Kiddies	Spam	SSL maliciosas	Tor	Web server
10	Blocklist.net.ua																X										
11	BlockList_de						X									X				X							X
12	BloggingFusion BL																		X								
13	Botscout (Last Caught)		X																								
14	Botvrij.eu											X								X							
15	Brute Force Blocker						X																				
16	C-APT-ure					X											X										
17	CERT-PA					X													X								
18	Charles Haley						X																				
19	CI Army List											X															
20	CRDF			X																							
21	CruzIT Blocklist						X	X																			

Numero	Motores de análisis	Black list Apivoid	Botnet	Clasificacion web	Cryptojacking	Envió-Alojamiento-Correos masivos	Escaneo de puertos-Ataque de fuerza bruta-DOS	Escaneo de vulnerabilidades	Exe,Doc xls, Elf con malware	Honeypots	Hosting	IDS	IP telefónico malicioso	IRC	Lista Roja	Mail Login	Malware	Motores de Análisis secundario	Otros	Phishing-Abuso-Estafa	Rastreo-Espionaje	Redireccionamiento de clic	Script Kiddies	Spam	SSL maliciosas	Tor	Web server
22	CSpace Hostings IP BL										X																
23	Cybercrime-tracker.net		X																								
24	Darklist.de						X																	X			
25	EFnet_RBL						X							X												X	
26	Etnetera BL							X																			
27	Feodo Tracker																										
28	FSpamList																							X			
29	GPF DNS Block List						X										X										
30	GreenSnow Blocklist						X																				
31	HoneyDB			X																							

Numero	Motores de análisis	Black list Apivoid	Botnet	Clasificacion web	Cryptojacking	Envió-Alojamiento-Correos	Escaneo de puertos-Ataque de fuerza bruta-DOS	Escaneo de vulnerabilidades	Exe,Doc xls, Elf con malware	Honeypots	Hosting	IDS	IP telefónico malicioso	IRC	Lista Roja	Mail Login	Malware	Motores de Análisis secundario	Otros	Phishing-Abuso-Estafa	Rastreo-Espionaje	Redireccionamiento de clic	Script Kiddies	Spam	SSL maliciosas	Tor	Web server
32	IBM_Cobion			X																							
33	InterServer IP List																		X								
34	IPSpamList					X																		X			
35	IPsum							X																			
36	ISX.fr DNSBL					X																					
37	JamesBrine IP List						X																				
38	JustSpam_org																							X			
39	Known Scanning Service							X																			
40	LAPPS Grid Blacklist																		X								
41	Liquid Binary					X																					
42	M4lwhere Intel																X										

Numero	Motores de análisis	Black list Apivoid	Botnet	Clasificacion web	Cryptojacking	Envió-Alojamiento-Correos masivos	Escaneo de puertos-Ataque de fuerza bruta-DOS	Escaneo de vulnerabilidades	Exe,Doc xls, Elf con malware	Honeypots	Hosting	IDS	IP telefónico malicioso	IRC	Lista Roja	Mail Login	Malware	Motores de Análisis secundario	Otros	Phishing-Abuso-Estafa	Rastreo-Espionaje	Redireccionamiento de clic	Script Kiddies	Spam	SSL maliciosas	Tor	Web server
43	Mark Smith Blocked IPs																		X								
44	Megumin																		X								
45	Mirai Tracker						X																				
46	MKXT_NET SSH BL						X																				
47	Myip.ms Blacklist		X														X							X			
48	NEU SSH Black list																										
49	Nginx Bad Bot Blocker						X															X		X			
50	NOC_RUB_DE																		X								
51	NordSpam																							X			

Numero	Motores de análisis	Black list Apivoid	Botnet	Clasificacion web	Cryptojacking	Envió-Alojamiento-Correos masivos	Escaneo de puertos-Ataque de fuerza bruta-DOS	Escaneo de vulnerabilidades	Exe,Doc xls, Elf con malware	Honeypots	Hosting	IDS	IP telefónico malicioso	IRC	Lista Roja	Mail Login	Malware	Motores de Análisis secundario	Otros	Phishing-Abuso-Estafa	Rastreo-Espionaje	Redireccionamiento de clic	Script Kiddies	Spam	SSL maliciosas	Tor	Web server
52	NoVirusThanks			X																							
53	NUBI Bad IPs						X										X		X								
54	OpenPhish																			X							
55	Peter-s NUUG IP BL																			X							
56	PhishTank																			X							
57	PlonkatronixBL						X	X												X				X		X	
58	PSBL																							X			
59	RealtimeBLACKLIST					X																					
60	Redactia																		X								
61	Redstout Threat IP list														X												

Numero	Motores de análisis	Black list Apivoid	Botnet	Clasificacion web	Cryptojacking	Envió-Alojamiento-Correos masivos	Escaneo de puertos-Ataque de fuerza bruta-DOS	Escaneo de vulnerabilidades	Exe,Doc xls, Elf con malware	Honeypots	Hosting	IDS	IP telefónico malicioso	IRC	Lista Roja	Mail Login	Malware	Motores de Análisis secundario	Otros	Phishing-Abuso-Estafa	Rastreo-Espionaje	Redireccionamiento de clic	Script Kiddies	Spam	SSL maliciosas	Tor	Web server
62	Ring-u NOC												X														
63	RJM Blocklist						X										X						X				
64	Roquesor BL																		X								
65	Rutgers Drop List			X																							
66	S.S.S.H.I.A																				X						
67	S5hbl					X																					
68	Sblam		X																					X			
69	SORBS					X																					
70	SpamCop																							X			
71	SSL Blacklist																								X		
72	Talos IP Blacklist																	X									
73	Threat Crowd																		X								

Numero	Motores de análisis	Black list Apivoid	Botnet	Clasificacion web	Cryptojacking	Envió-Alojamiento-Correos	Escaneo de puertos-Ataque de fuerza bruta-DOS	Escaneo de vulnerabilidades	Exe,Doc xls, Elf con malware	Honeypots	Hosting	IDS	IP telefónico malicioso	IRC	Lista Roja	Mail Login	Malware	Motores de Análisis secundario	Otros	Phishing-Abuso-Estafa	Rastreo-Espionaje	Redireccionamiento de clic	Script Kiddies	Spam	SSL maliciosas	Tor	Web server
75	ThreatLog									X																	
76	TweetFeed																	X									
77	UCEPROTECT Level 1					X																		X			
78	URLhaus																X										
79	URLVir								X																		
80	USTC IP BL						X																				
81	ViriBack C2 Tracker																X										
82	VoIP Blacklist	X																									
83	VXVault																X										
84	ZeroDot1 Bad IPs				X																						
85	ZeroDot1 Miner IPs				X																						