UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO

FACULTAD DE POSGRADO

MAESTRÍA EN CIENCIA DE DATOS

Proyecto de Investigación previo la obtención del Grado Académico de Magíster en Ciencia de Datos

TEMA

MODELO PREDICTIVO DE CIBERATAQUES EN ENTORNOS DE INTERNET DE LAS COSAS

AUTOR:

ING. ARIAS CHEVEZ GERMAN NELSON

DIRECTOR:

ING. ZHUMA MERA EMILIO RODRIGO, MSC.

QUEVEDO – LOS RÍOS – ECUADOR

2024

CERTIFICACIÓN

El suscrito certifica que el proyecto de investigación para la obtención del grado académico de Magister en Ciencia de Datos, **MODELO PREDICTIVO DE CIBERATAQUES EN ENTORNOS DE INTERNET DE LAS COSAS**. De autoría del Ing. Nelson German Arias Chevez ha sido revisado en todos sus componentes, por lo por lo que autoriza su presentación formal ante el tribunal respectivo.

Quevedo, 5 de Junio del 2024

EMILIO RODRIGO ZHUMA MERA

Firmado digitalmente por EMILIO RODRIGO ZHUMA MERA

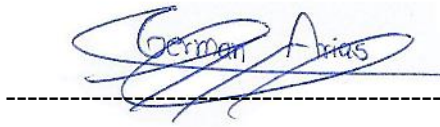
Ing. Zhuma Mera Emilio Rodrigo, MSc.

DIRECTOR

AUTORÍA

Yo, Nelson German Arias Chevez, declaro que el proyecto de investigación aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

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



Ing. Arias Chevez Nelson German

AUTOR

DEDICATORIA

Este proyecto de investigación es una dedicación a Dios, quien ha sido la fuente de mi fuerza y determinación para alcanzar este hito en mi carrera profesional. La fortaleza y la inspiración que he recibido de Él han sido fundamentales para mantener mi motivación y perseverancia en la consecución de mis metas diarias. Este logro es un testimonio de su gracia y un reflejo de mi compromiso constante con el crecimiento y la mejora continua.

A mis padres y a toda mi familia, quienes han sido mi pilar de apoyo constante en cada etapa de mi vida. Su amor y apoyo inquebrantable me han dado la fuerza para superar los desafíos y seguir adelante. Para ellos, ofrezco todo mi amor, y quiero que sepan que cada esfuerzo y sacrificio que he hecho ha sido por y para ellos. Mi constante dedicación y trabajo duro son un reflejo de mi amor y gratitud hacia ellos. Gracias por estar siempre a mi lado.

Ing. Arias Chevez Nelson German

AGRADECIMIENTO

Primero que nada, quiero expresar mi más profundo agradecimiento a Dios por darme fortaleza, salud, esperanza y capacidad para poder cumplir una meta más en la vida. A mis padres por toda la guía y apoyo incondicional que me ha brindado toda mi familia, ya que con la fé y el amor familiar todo se puede cumplir en esta vida.

Expreso mi gratitud a la Universidad Técnica Estatal de Quevedo, que me brindó la oportunidad de superarme y alcanzar un nuevo objetivo en mi carrera profesional. Asimismo, quiero agradecer a mi director, el Ing. Zhuma Mera Emilio Rodrigo, MSc. Su paciencia, sabiduría y entusiasmo fueron fundamentales en la realización de esta investigación.

A mis amigos de maestrías por permitirme conocer la calidad humana que los caracteriza y profesionalismo, cualidades que sin duda los llevarán a grandes alturas. Su amistad es un tesoro preciado que siempre llevaré conmigo.

A todos los que han compartido este viaje conmigo, a aquellos que han estado a mi lado en cada paso del camino, no puedo sino expresar mi más sincero agradecimiento. Su apoyo y compañía han sido invaluables en este viaje. Gracias por ser parte de esta importante etapa de mi vida.

Ing. Arias Chevez Nelson German

PRÓLOGO

Los entornos del Internet de las Cosas están en constante crecimiento, a su vez, la seguridad cibernética se ha convertido en un asunto de vital importancia. Con el creciente número de dispositivos conectados a través de internet, surge la necesidad de proteger estos sistemas ante posibles ciberataques, una necesidad que se intensifica cada vez más. En este escenario, la Ciencia de Datos se presenta como un recurso esencial para identificar y prevenir amenazas en ambientes de IoT.

En este proyecto de investigación del autor Ing. Nelson Arias Chevez, nos sumerge en el fascinante universo de la Ciencia de Datos y la ciberseguridad en dispositivos de Internet de las Cosas. A través del análisis de datos recopilados en el conjunto CICIOT2023, el autor explora cómo las técnicas de aprendizaje automático pueden ayudar a predecir y prevenir posibles amenazas en estos entornos digitales a través del desarrollo de modelos predictivos.

Los resultados de esta investigación demuestran que la aplicación de algoritmos de aprendizaje automático supervisado para generar modelos predictivos permite predecir la probabilidad de posibles ataques maliciosos a dispositivos del Internet de las Cosas. Este documento representa un valioso recurso para aquellos interesados en la ciberseguridad, la Ciencia de Datos y el Internet de las Cosas. Además, abre las puertas a futuras investigaciones y desarrollos en un área crucial para el avance tecnológico.

Ing. Ángel Torres Quijije, MSc

RESUMEN

La Ciencia de Datos permite, en entornos de Internet de las Cosas, detectar y prevenir ciberataques utilizando el poder de las técnicas de aprendizaje automático para encontrar de forma autónoma las mejores soluciones para resolver los problemas que afrontan los dispositivos frente a los ciberataques y vulnerabilidades que poseen. El conjunto de datos CICIOT2023 contiene registros de los distintos tipos de ciberataques dirigidos a dispositivos de Internet de las Cosas.

El objetivo de la presente investigación es generar un modelo predictivo aplicando técnicas de aprendizaje automático para detectar ciberataques en entornos de Internet de las Cosas utilizando el conjunto de datos de CICIOT2023, en este trabajo se destaca la importancia que tienen los modelos de predicción para proteger los entornos de Internet de las Cosas y reducir vulnerabilidades mediante el uso de técnicas de aprendizaje automático y minería de datos.

Se aplican algoritmos de clasificación, regresión de aprendizaje automático y técnicas de minería de datos con conjuntos de datos de entrenamiento y pruebas, para llevar a cabo el modelado predictivo de una variedad de ciberataques. Estos ataques se categorizan en siete familias: Distributed Denial of Service (DDoS), Denial-of-Service (DoS), Reconocimiento, ataques basados en la web, Fuerza Bruta, Spoofing y Mirai. Además, se pretenda utilizar algoritmos de visualización de datos para identificar patrones que influyan en la seguridad de los protocolos frente a los ciberataques.

Los resultados de la investigación muestran la importancia de un modelo predictivo para mantener la seguridad de los dispositivos de IoT frente a las actividades de los ciberdelincuentes, y de esta manera proteger y reducir vulnerabilidades en entornos de

Internet de las Cosas. El proyecto de investigación desarrollado puede resultar de gran utilidad para aquellas empresas especializadas en ciberseguridad.

Palabras claves: Internet de las Cosas, Ciberataques, Ciberdelincuentes, Aprendizaje automático, Modelo predictivo.

ABSTRACT

Data Science allows, in Internet of Things environments, to detect and prevent cyber-attacks using the power of machine learning techniques to autonomously find the best solutions to solve the problems faced by devices in the face of cyber-attacks and vulnerabilities they possess. The CICIOT2023 dataset contains records of the different types of cyber-attacks targeting Internet of Things devices.

The objective of the present research is to generate a predictive model by applying machine learning techniques to detect cyber-attacks in Internet of Things environments using the CICIOT2023 dataset, this work highlights the importance of predictive models to protect Internet of Things environments and reduce vulnerabilities by using machine learning and data mining techniques.

Classification algorithms, machine learning regression and data mining techniques are applied with training and test data sets to perform predictive modeling of a variety of cyber-attacks. These attacks are categorized into seven families: Distributed Denial of Service (DDoS), Denial-of-Service (DoS), Reconnaissance, Web-based attacks, Brute Force, Spoofing and Mirai. In addition, data visualization algorithms are intended to be used to identify patterns that influence the security of protocols against cyber-attacks.

The research results show the importance of a predictive model to maintain the security of IoT devices against the activities of cybercriminals, and thus protect and reduce vulnerabilities in Internet of Things environments. The research work developed can be very useful for those companies specialized in cybersecurity.

Keywords: Internet of Things, Cyberattacks, Cybercriminals, Machine Learning, Predictive Model.

ÍNDICE DE CONTENIDO

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

INTRODUCCIÓN

El Internet de las Cosas (IoT) actualmente se ha vuelto en una de las tecnologías más populares y utilizadas en todo el mundo. Esta tecnología permite la conexión de dispositivos y objetos cotidianos a Internet, lo que ha generado una gran cantidad de datos que pueden ser utilizados para mejorar la calidad de vida de las personas y optimizar procesos en diferentes sectores. Sin embargo, el uso masivo de dispositivos de IoT también ha generado una serie de riesgos y vulnerabilidades en seguridad digital. Los ciberataques a estos dispositivos son cada vez más frecuentes y sofisticados, lo que ha llevado a la necesidad de desarrollar nuevas técnicas y herramientas para prevenir y detectar estos ataques.

En este contexto, la Ciencia de Datos se ha convertido en una disciplina clave para la detección de ciberataques en entornos IoT. La aplicación de técnicas de aprendizaje automático y minería de datos, permiten analizar grandes cantidades de información y generar modelos predictivos para identificar patrones y comportamientos anómalos en los dispositivos de Internet de las Cosas.

En este estudio, se presenta una investigación sobre la detección de ciberataques en entornos de IoT utilizando técnicas de aprendizaje automático. El objetivo principal de este estudio es desarrollar un modelo predictivo de ciberataques en entornos de IoT utilizando el conjunto de datos CICIOT2023, el cual pertenece al (Institute for Cybersecurity, 2023).

Para lograr este objetivo, se realizó una revisión bibliográfica de trabajos previos relacionados con la detección de ciberataques en entornos de IoT. Esta revisión permitió identificar las brechas en la literatura existente y definir el marco contextual de la

investigación. Este trabajo puede resultar en un recurso valioso para cualquier persona interesada en la seguridad digital y en la aplicación de técnicas de Ciencia de Datos en entornos de IoT. Posteriormente, se procedió a la recolección y preprocesamiento del conjunto de datos CICIOT2023. Este conjunto de datos contiene registros de los distintos tipos de ciberataques dirigidos a dispositivos de IoT.

Una vez preprocesado el conjunto de datos, se procedió con la selección de variables y la aplicación de algoritmos de clasificación para generar modelos predictivos de ciberataques en entornos de IoT. Se utilizaron diferentes algoritmos de predicción basados en aprendizaje supervisado.

CAPÍTULO I

MARCO CONTEXTUAL DE LA INVESTIGACIÓN

1.1. UBICACIÓN Y CONTEXTUALIZACIÓN DE LA PROBLEMÁTICA

El gasto mundial en el Internet de las Cosas (IoT) ha experimentado un crecimiento significativo en los últimos años y según las predicciones realizadas por *International Data Corporation* (IDC), se prevé que para 2025 haya aproximadamente 16.500 millones de dispositivos conectados mediante el IoT (Fernández, statista, 2023).

El creciente ecosistema de dispositivos de IoT, donde la proliferación de estos dispositivos conectados a la red ha dado lugar a una creciente preocupación por la seguridad cibernética. La interconexión de dispositivos de IoT se encuentra en una amplia variedad de aplicaciones, desde hogares inteligentes y sistemas de atención médica hasta la industria manufacturera y la infraestructura urbana, ha creado una superficie de ataque expandida que atrae la atención de ciberdelincuentes. Por lo tanto, muchos de los ciberataques se encuentran recopilados en el conjunto de datos CICIOT2023 representa un recurso invaluable para abordar esta problemática, ya que proporciona información detallada sobre incidentes de seguridad y tráfico de red en entornos a los dispositivos de IoT.

Por lo tanto, en el conjunto de datos CICIOT2023 recopilados por (University of New Brunswick, 2023), existe una gran cantidad de ciberataques registrados que representan un recurso invaluable para abordar esta problemática, ya que proporciona información detallada sobre incidentes de seguridad y tráfico de red en entornos a los dispositivos de IoT.

En Latinoamérica, el número de ciberataques ha aumentado en los últimos años. Según datos de Kaspersky (Diazgranados, 2021), en América Latina los ciberataques han

aumentado un 24 % durante los primeros ocho meses de 2021. Este mismo informe de Kaspersky, revela que los 20 programas maliciosos más populares representan más de 728 millones de intentos de infección en la región, lo que equivale a un promedio de 35 ataques por segundo. En cuanto a Ecuador, es el país que lidera la lista con un aumento del 75 % en ciberataques, seguido de Venezuela con el 29 %, Guatemala el 43 %, Panamá el 60 % y por último Perú con un 71 %. En este contexto, Ecuador registra 89 intentos de infección por minuto (Diazgranados, 2021).

1.2. SITUACIÓN ACTUAL DE LA PROBLEMÁTICA

Según datos de estadísticos de Statista (Fernández, Statista, 2023), el porcentaje de personas con acceso a internet a nivel mundial sigue en aumento debido al continuo desarrollo de infraestructuras de redes de telecomunicaciones. Si bien se nota que existe un creciente aumento de usuarios con acceso a la red, la seguridad en entornos de IoT se convierte en un tema muy importante para tener en cuenta, ya que muchos de estos usuarios se pueden encontrar vulnerables frente a posibles ciberataques. En el año 2023, se ha observado un incremento significativo en la incidencia de ciberataques a nivel global. Según un estudio realizado por *Check Point Research* (CPR), hubo un aumento del 38 % en los ciberataques durante el año 2022. En el primer trimestre de 2023, se registró un incremento adicional del 7 % en la frecuencia de estos ataques (Horowitz, 2023).

Por otro lado, en un reciente incidente en Ecuador (Consejo Nacional Electoral, 2023), el sistema de votación en el extranjero del Consejo Nacional Electoral (CNE) fue objeto de ciberataques. Estos ataques, según informes preliminares, se originaron en varios países, incluyendo India, Bangladesh, Pakistán, Rusia, Ucrania, Indonesia y China. La

presidenta del CNE, Diana Atamaint, atribuyó a estos ciberataques las dificultades que enfrentaron los ciudadanos ecuatorianos en el extranjero para ejercer su derecho al voto en las elecciones presidenciales y legislativas. A pesar de la gravedad de estos ataques (Consejo Nacional Electoral, 2023), Atamaint aseguró que los votos emitidos en el extranjero no han sido comprometidos. Este incidente subraya la creciente amenaza de los ciberataques a los sistemas electorales y la necesidad de reforzar las medidas de seguridad cibernética para proteger la integridad del proceso electoral.

1.3. PROBLEMA DE INVESTIGACIÓN

1.3.1. Problema General

¿Cómo detectar los ciberataques considerando la creciente complejidad de amenazas y la necesidad de proteger los entornos de internet de las cosas?

1.3.2. Problemas derivados

- ¿Cuáles son los ataques más frecuentes en entornos de Internet de las Cosas?
- ¿Cómo se pueden Identificar los protocolos de seguridad más vulnerables en entornos de Internet de las Cosas?
- ¿Cómo se podría predecir los ciberataques en entornos de Internet de las Cosas?

1.4. DELIMITACIÓN DEL PROBLEMA

El estudio se enfocó exclusivamente en la predicción de ataques futuros y la evaluación de la efectividad de protocolos de seguridad en dispositivos de Internet de las Cosas utilizando el conjunto de datos CICIOT2023:

- **Campo:** Tecnología de la información, Seguridad informática, Internet de las Cosas y Ciencias de Datos.
- **Área:** Seguridad informática y Redes
- **Línea:** Ciencia de Datos, Big Data y Aprendizaje Automático
- **Lugar:** Ecuador, Los Ríos, Quevedo
- **Tiempo:** Septiembre 2023 - Enero de 2024

1.5. OBJETIVOS

1.5.1. Objetivo General

Generar un modelo predictivo aplicando técnicas de aprendizaje automático para detectar ciberataques en entornos de Internet de las Cosas utilizando el conjunto de datos de CICIOT2023.

1.5.2. Objetivos Específicos

- Identificar patrones de ataques en entornos de Internet de las Cosas utilizando técnicas de análisis descriptivo.
- Analizar protocolos de seguridad más vulnerados en dispositivos de Internet de las Cosas.
- Evaluar algoritmos para predecir los ciberataques en entornos de Internet de las Cosas.

1.6. JUSTIFICACIÓN

El Internet de las Cosas representa una revolución en la forma en que interactuamos con el mundo digital y físico. La sociedad actual se encuentra cada vez más inmersa en el entorno del internet de las cosas, esto resulta que el incremento de estos dispositivos siga en constante aumento, conectando una variedad de dispositivos y sistemas a través de internet. Esta creciente interconexión de la que podemos hacer uso hoy en día nos ofrece innumerables beneficios en términos de eficiencia, comodidad y automatización, desde casas y ciudades inteligentes hasta aplicaciones en la industria y la atención médica. Sin embargo, junto con las muchas ventajas que nos ofrece, el aumento de dispositivos también ha generado una serie de desafíos significativos en el ámbito de la ciberseguridad, lo que hace que la investigación en modelos predictivos de ciberataques en entornos de IoT sea fundamental y altamente relevante.

La aplicación de algoritmos de aprendizaje automático brinda soluciones para afrontar la problemática de los ciberataques, convirtiéndose en una opción viable mediante la cual podemos predecir y prevenir ataques. Además, al contar con un conjunto de datos donde se encuentran una gran cantidad de ataques registrados a dispositivos de Internet de las Cosas, podemos identificar distintos patrones que ayuden para predecir estos ciberataques.

En este proyecto de investigación se pretende generar un modelo predictivo con buena precisión para la detección de ciberataques, y a su vez fortalecer la seguridad de los equipos de redes. Por otro lado, este trabajo puede ser utilizado por las empresas u organizaciones para predecir posibles ataques, ya que la detección temprana no solo minimiza el impacto de los ataques, sino que también reduce los costos asociados con la recuperación y la reparación de daños. Por lo tanto, este trabajo puede ser un recurso

valioso para que las empresas pueden tomar medidas preventivas para proteger sus dispositivos y sistemas de IoT.

.

CAPÍTULO II

MARCO CONTEXTUAL DE LA INVESTIGACIÓN

2.1. FUNDAMENTACIÓN CONCEPTUAL

2.1.1. Instituto Canadiense de Ciberseguridad (CIC)

El Instituto Canadiense de Ciberseguridad (CIC) perteneciente a la (University of New Brunswick, 2023) es una unidad multidisciplinaria integral de capacitación, investigación y desarrollo y emprendimiento que aprovecha la experiencia de investigadores en ciencias sociales, negocios, informática, ingeniería, derecho y ciencias. La institución CIC es la primera de su tipo que reúne a investigadores y profesionales de todo el espectro académico para compartir ideas innovadoras, crear tecnología disruptiva y llevar a cabo investigaciones innovadoras sobre los desafíos de ciberseguridad más apremiantes de nuestro tiempo.

2.1.2. Internet de las Cosas

Según (International Business Machines, 2023), el Internet de las cosas (IoT) hace referencia a una variedad de dispositivos físicos, desde vehículos hasta electrodomésticos, que están equipados con sensores, software y conectividad a la red, lo que les permite recolectar y compartir información. Según el autor, estos dispositivos, también denominados objetos inteligentes, pueden abarcar desde sencillos dispositivos de hogares inteligentes como termostatos, hasta dispositivos portátiles como relojes inteligentes y ropa con tecnología RFID, e incluso maquinaria industrial sofisticada y sistemas de transporte. Los expertos en tecnología están incluso visualizando ciudades enteras basadas en la tecnología del Internet de las Cosas, conocidas como “ciudades inteligentes”.

2.1.3. Ciberataques

Los ciberataques son un problema importante para las personas y organizaciones que se encuentran interconectadas en la red. Según (Cisco, 2023), un ciberataque se refiere a un esfuerzo intencional y dañino realizado por una persona o entidad para violar el sistema de información de otra persona o entidad. Según el autor, el agresor generalmente persigue algún tipo de ganancia al interrumpir la red del objetivo.

2.1.4. Ciberseguridad

La ciberseguridad es un factor importante para todos aquellos que desean navegar en la red de forma segura. Según (Avast, 2022), la ciberseguridad es la práctica de proteger datos críticos en dispositivos, redes y programas contra ataques y accesos no autorizados. También, se menciona que la ciberseguridad protege los sistemas contra piratas informáticos y otras personas que intentan explotar vulnerabilidades e infiltrarse en redes informáticas. El autor menciona que el objetivo de la ciberseguridad es combatir los delitos cibernéticos, como el uso de software malicioso, el robo de información sensible, la extorsión y la interrupción del negocio. Las prácticas de ciberseguridad previenen los ciberataques que tienen como objetivo información importante de personas o empresas.

2.1.5. Base de Datos

una base de datos es cualquier colección de información interrelacionada. Cuando escribes una lista de compras en una hoja de papel, estás creando una pequeña base de datos analógica. Pero ¿qué es una base de datos en informática? En ese contexto, se define "base de datos" como una colección de información que se almacena como datos

en un sistema informático, como el inventario de la tienda de comestibles local (Microsoft, 2023).

2.1.6. Big Data

En la era digital actual, la cantidad de información generada y almacenada en todo el mundo está creciendo a una velocidad vertiginosa. Este torrente incesante de datos proviene de una variedad de fuentes, como redes sociales, dispositivos móviles, sensores, transacciones en línea y mucho más. Este fenómeno, conocido como "Big Data", según (Statistical Analysis System, 2023) el término "Big Data" hace alusión a los datos que son tan voluminosos, veloces o complejos que resulta complicado o imposible procesarlos con técnicas convencionales. La práctica de acceder y almacenar grandes volúmenes de información para el análisis ha sido una constante desde hace mucho tiempo.

2.1.7. Minería de Datos

En la encrucijada de la tecnología y la información, donde vastas cantidades de datos se generan y almacenan diariamente, la capacidad para extraer conocimiento valioso de este océano de información se ha vuelto esencial. La minería de datos, también conocida como "Minería de Datos," es la disciplina que se ha convertido en el faro guía para explorar y descubrir patrones, tendencias y conocimientos ocultos en conjuntos de datos masivos. Según (Oracle Cloud Infrastructure, 2023) lo define como el proceso de descubrir conocimientos cuando se trata de grandes volúmenes de datos. Estos datos pueden provenir de muchas fuentes o de una sola base de datos, y la información se puede generar mediante el descubrimiento manual o la automatización. Existen muchos caminos diferentes para producir conocimientos, a menudo dependiendo de variables,

como recursos, capacidades de aprendizaje automático/inteligencia artificial, complejidad de los datos, volumen de datos y la capacitación y experiencia del personal. Este proceso implica un análisis profundo de datos para descubrir patrones y factores subyacentes, todo para crear conclusiones y producir decisiones informadas.

2.1.8. Aprendizaje Automático

En la intersección de la informática y la inteligencia artificial, el concepto de "Aprendizaje Automático" ha emergido como una disciplina revolucionaria que está transformando la forma en que las máquinas comprenden y responden a datos y patrones complejos, (Google, 2023) describe al aprendizaje automático como una rama de la inteligencia artificial que posibilita que una máquina o sistema aprenda de forma autónoma y mejore con la experiencia. En lugar de depender de una programación directa, emplea algoritmos para analizar grandes conjuntos de datos, extraer conocimientos valiosos y tomar decisiones fundamentadas. A medida que los algoritmos de aprendizaje automático se entrenan y se exponen a más información, su rendimiento mejora. Los modelos de aprendizaje automático son el producto o lo que el sistema aprende al aplicar un algoritmo a un conjunto de datos de entrenamiento. Cuantos más datos se utilicen, mejor será el modelo resultante.

2.1.9. Aprendizaje supervisado

En el mundo de la ciencia de datos el aprendizaje supervisado emerge como uno de los pilares fundamentales de este entorno, según (Deepai, 2023), el aprendizaje supervisado es el proceso de enseñar un modelo alimentándolo con datos de entrada y datos de salida correctos. Este par de entrada/salida generalmente se conoce como "datos etiquetados". Piense en un maestro que, sabiendo la respuesta correcta, recompensará o

quitará calificaciones a un estudiante en función de la corrección de su respuesta a una pregunta. El aprendizaje supervisado se utiliza a menudo para crear modelos de aprendizaje automático para dos tipos de problemas. Uno de ellos es la regresión, que consiste en que el modelo busca salidas que son variables reales (números que pueden tener decimales). El otro tipo es la clasificación, que consiste en que el modelo encuentra clases en las que colocar sus entradas.

2.1.10. Modelo de Predicción

En un mundo impulsado por datos y toma de decisiones informadas, la capacidad de anticipar eventos futuros es un recurso invaluable. Los "modelos predictivos" se han convertido en una herramienta esencial en este esfuerzo, permitiendo a empresas, organizaciones y científicos analizar información histórica y patrones de datos para pronosticar resultados futuros con un alto grado de precisión. La empresa (Express Analytics, 2023) refiere a los modelos predictivos como al uso de algoritmos para analizar datos recopilados sobre eventos anteriores con el fin de predecir el resultado de eventos futuros.

2.1.11. Correlación

La correlación se refiere a la relación estadística entre las dos entidades. Mide el grado en que dos variables están relacionadas linealmente. Por ejemplo, la altura y el peso de una persona están relacionados, y las personas más altas tienden a ser más pesadas que las personas más bajas.

2.1.12. Visualización de Datos

Hoy en día vivimos inundado de información, la habilidad de comprender y comunicar de manera efectiva los patrones y tendencias que yacen en conjuntos de datos complejos

se ha vuelto esencial. Según (Tableau, 2023) la visualización de datos es la ilustración gráfica de información y datos. Mediante el uso de componentes visuales como diagramas, gráficos y mapas, las herramientas de visualización de datos ofrecen un método fácil de interpretar y entender las tendencias, anomalías y patrones en los datos. Además (Tableau, 2023), proporciona una excelente manera para que los empleados o propietarios de empresas presenten datos a audiencias no técnicas sin confusión.

2.1.13. Mapa de calor

Los mapas de calor son visualizaciones de datos que emplean códigos de colores para representar la información. Su propósito principal es mejorar la visualización del volumen de ubicaciones o eventos en un conjunto de datos y guiar a los observadores hacia las áreas de datos más relevantes (Insight Software, 2022).

2.1.14. Evaluación de Modelos

En el emocionante campo de la ciencia de datos, donde se extraen ideas valiosas de datos complejos y diversas fuentes, la construcción de modelos es una de las tareas fundamentales. Estos modelos, que pueden variar desde algoritmos de aprendizaje automático hasta modelos estadísticos, sirven como herramientas poderosas para predecir, clasificar, optimizar y comprender una amplia variedad de fenómenos. Sin embargo, la creación de un modelo no es el final del viaje; es aquí donde entra en juego la evaluación de modelos. Según (Domino, 2023), la evaluación de modelos es el proceso de usar diferentes métricas de evaluación para comprender el rendimiento de un modelo de aprendizaje automático, así como sus fortalezas y debilidades. La evaluación del modelo es importante para evaluar la eficacia de un modelo durante las fases iniciales de investigación, y también desempeña un papel en el seguimiento del modelo.

2.2. FUNDAMENTACIÓN TEÓRICA

En la investigación realizada por (TÜRK, 2023) que tiene como nombre, busca analizar la detección de ataques de red mediante algoritmos de aprendizaje automático, aplicaron una fase de distribución aleatoria en ambos conjuntos de datos y extrajeron características básicas utilizando el método de correlación de Pearson para la selección de características. Además, realizaron una comparativa con los algoritmos de aprendizaje automático que aplicaron, en los resultados obtuvo una precisión del 98,6 % y 98,3 % para dos clases y clases múltiples, respectivamente, y una precisión del 97,8 % y 93,4 % en el conjunto de datos NSL-KDD.

El trabajo realizado por (Kasongo & Sun, 2020), presenta un análisis del conjunto de datos de detección de intrusiones UNSW NB15 que se utilizan para entrenar y probar técnicas de aprendizaje automático. El trabajo aplica metodologías de ML supervisadas para Los sistemas de detección de intrusiones (IDS): k vecino más cercano (kNN), regresión logística (LR), red neuronal artificial (ANN), máquina de vectores de soporte (SVM) y árbol de decisión (DT). Los resultados de esta investigación demuestran que el método de selección de características basado en XGBoost permite que métodos como el árbol de decisión aumenten la precisión de su prueba del 88,13 % al 90,85 % para el esquema de clasificación binaria.

El proyecto de investigación de (Wei et al., 2022), propone un sistema de detección de intrusos para el bus Controller Area Network (CAN). Este sistema, basado en una red neuronal adversaria de dominio, puede lograr un alto rendimiento de detección en datos de ataques variantes no aprendidos. Los métodos utilizados en la investigación son algoritmos de clasificación. Además, los resultados demuestran que el sistema de detección de intrusos para vehículos logró un alto rendimiento de detección, con valores

de recuperación, precisión y puntuación F1 superiores al 99 % en un conjunto de datos de ataque variante no entrenado.

En el siguiente trabajo también se centra en el método de clasificación. En la investigación realizada por (Shitharth et al., 2022), desarrolló una metodología de clasificación basada en agrupaciones para detectar con precisión intrusiones de los diferentes tipos de conjuntos de datos de detección. Utiliza un interesante grupo de metodologías, como agrupación, optimización y clasificación, para procesar los conjuntos de datos en orden. Además, utiliza la clasificación para procesar los conjuntos de datos y predecir las intrusiones. Los resultados en esta investigación muestran que el modelo ADC-DBScan-LNB propuesto supera a las otras técnicas, con mejores resultados de rendimiento.

Por otro lado, en la investigación de (Athipalli et al., 2022), plantea un sistema de detección de intrusiones que utiliza Máquinas de Vector Soporte (SVM) de manera computacionalmente eficiente, basado en la agrupación de prototipos K. El propósito es proponer un nuevo modelo de aprendizaje automático híbrido para la detección de intrusos, que utiliza agrupación en clústeres de prototipos K y Máquinas de Vectores de Soporte. El modelo propuesto en esta investigación reduce la cantidad de muestras de entrenamiento, lo que a su vez reduce la cantidad de vectores de soporte. Esto reduce el tiempo necesario para entrenar SVM y, al mismo tiempo, produce resultados impresionantes.

En la investigación de (Malathi & Padmaja, 2023), realiza la identificación de ciberataques mediante aprendizaje automático en redes IoT, que tiene como objetivo investigar y evaluar la eficacia de los algoritmos de aprendizaje automático en la protección contra

ataques de ciberseguridad, con un enfoque particular en los ataques de denegación de servicio en el contexto del Internet de las cosas, recopilando metadatos únicos del entorno IoT, específicamente utilizando el conjunto de datos Bot-IoT. La investigación se centró en evaluar la eficiencia y la confiabilidad de algoritmos de aprendizaje automático para la detección y mitigación de riesgos cibernéticos en un entorno IoT. Se consideraron múltiples factores novedosos y se utilizaron técnicas de vanguardia para mejorar la precisión de los resultados. Los resultados de esta investigación sugieren que la implementación de algoritmos de aprendizaje automático puede fortalecer eficazmente la seguridad de los dispositivos IoT interconectados, ofreciendo una defensa más sólida contra amenazas cibernéticas en constante evolución.

Según el estudio realizado por (Dalal et al., 2023), se menciona el uso de la predicción de ciberataques de próxima generación para sistemas de Internet de las Cosas. Aprovechando SVM multiclase y árbol de decisión CHAID optimizado, el estudio busca identificar los atributos más relevantes que contribuyen a la categorización de ataques y, por lo tanto, mejorar la precisión del modelo SVM. La metodología propuesta comienza con la clasificación del tráfico de IoT utilizando una máquina de vectores de soporte de múltiples clases para identificar varios tipos de ataques. Los resultados de la evaluación de *Multistep Cyber-Attack Dataset* (MSCAD) indican que el árbol de decisión CHAID propuesto puede predecir ataques cibernéticos de múltiples etapas con una impresionante precisión del 99.72 %.

Por otra parte, en la investigación de (Mumtaz et al., 2023), utilizan algoritmos de clasificación y predicción para Significant Cyber Incidents (SCI) mediante minería de datos y aprendizaje automático (DM-ML), con el propósito en explorar la importancia de la ciberseguridad y su relación con los SCI, además de analizar el impacto de la

pandemia de COVID-19 en la ciberseguridad. El estudio utiliza técnicas de minería de datos y aprendizaje automático (DM-ML) para predecir, prevenir y detectar. La metodología se basa en la aplicación de técnicas de minería de datos (DM) para la extracción de características relevantes de los datos y el uso de clasificadores de aprendizaje automático bien conocidos, como Naïve Bayes (NB), Support Vector Machine (SVM), Logistic Regression (LR) y Random Forest (RF), para la clasificación de SCI. Los resultados en este estudio indican que los clasificadores SVM y RF son más efectivos que otros en la predicción de SCI. Además, se concluye que Asia es el continente que probablemente se vea más afectado por los SCI.

En la investigación de (Rustagi & Goel, 2022), se resalta la importante del análisis predictivo, las ventajas y aplicación que tienen en diversas industrias, el objetivo de este estudio es proporcionar una visión futura desarrollada en el área de análisis de datos a través de la ciencia de análisis predictivo. La metodología utilizada en este estudio es el análisis predictivo. Los resultados obtenidos indican que el análisis predictivo facilita la visualización del futuro y es más confiable y preciso que las herramientas anteriores.

Según en el estudio de (Alharbi et al., 2022), realiza un modelo predictivo para la detección de software malicioso con el propósito de reducir las vulnerabilidades utilizando técnicas de aprendizaje automático y minería de datos. La metodología utilizada en este estudio es el análisis predictivo basado en técnicas de aprendizaje automático y minería de datos. Los resultados de este estudio muestran que el clasificador Random Forest (RF) logró una precisión de clasificación del modelo predictivo del 0.9714%.

Por otro lado, en el trabajo de (Lal et al., 2023), desarrollan un modelo efectivo de identificación de ciberseguridad basado en IoT que pueda predecir y clasificar vulnerabilidades de manera precisa y oportuna. En este trabajo se utilizaron técnicas de aprendizaje automático, para identificar características relevantes de las vulnerabilidades y se emplearon diversos modelos de aprendizaje automático, como KNN (K-Nearest Neighbors), NBSVM (Naive Bayes Support Vector Machine), LSTM-ANN (Long Short-Term Memory Artificial Neural Network), MLP (Multilayer Perceptron), LR (Logistic Regression). Los resultados de este trabajo indican que la combinación de diferentes modelos de aprendizaje automático, como LSTM, NBSVM, MLP, entre otros, contribuyó a mejorar la precisión y eficacia en la identificación y clasificación de vulnerabilidades en entornos de ciberseguridad basados en IoT.

En la investigación de (Saheed & Arowolo, 2021), también utilizan algoritmos de aprendizaje automático para la detección eficiente de ciberataques en *Internet of Medical Things.* En este trabajo, proponen un enfoque innovador para mejorar la ciberseguridad en entornos médicos inteligentes. Utilizan técnicas avanzadas como Redes Neuronales Recurrentes Profundas y Algoritmos de Aprendizaje Automático para detectar y prevenir ataques cibernéticos en el Internet de las Cosas Médicas (IoMT). Su investigación destaca la importancia de proteger la privacidad y la integridad de los datos de los pacientes en un entorno donde la tecnología desempeña un papel crucial en la atención médica. Además, exploran métodos de optimización como la Optimización por Enjambre de Partículas (PSO) para seleccionar atributos relevantes y mejorar la eficiencia del sistema de detección de intrusiones.

En el trabajo de (Li et al., 2019), proponen un marco de aprendizaje automático para identificar y detectar dominios generados por algoritmos (DGA) para mitigar la

amenaza. Los autores recopilan datos de amenazas en tiempo real del tráfico real durante un período de un año. También proponen un modelo de aprendizaje profundo para clasificar una gran cantidad de dominios DGA. El marco de aprendizaje automático propuesto consta de un modelo de dos niveles y un modelo de predicción que utiliza serie temporal para predecir las características del dominio entrante basándose en el modelo oculto de Markov (HMM). Los resultados de esta investigación muestran una precisión del 95,89% para la clasificación en el marco y del 97,79% para el modelo DNN, del 92,45% para la agrupación de segundo nivel y del 95,21% para la predicción HMM en el marco.

2.3. FUNDAMENTACIÓN LEGAL

Para entender la estructura técnico - legal que sostiene el (Ministerio De Telecomunicaciones Y De La Sociedad De La Información, 2020), según el Acuerdo Ministerial No. 011 -2020, cuyo objetivo es establecer el marco jurídico y normativo que regula la apertura y el uso de datos gubernamentales en formato abierto.

2.3.1. Ministro de Telecomunicaciones y de la Sociedad de la Información

En la Constitución de la República del Ecuador, el derecho al acceso a la información está reconocido en el numeral 2 del artículo 18, que establece lo siguiente: "Acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas. No existirá reserva de información excepto en los casos expresamente establecidos en la ley. En caso de violación a los derechos humanos, ninguna entidad pública negará la información". Además, el artículo 226 (Ministerio De Telecomunicaciones Y De La Sociedad De La Información, 2020) de la Constitución indica que las instituciones del Estado, sus organismos y dependencias, así como las personas que actúen en virtud de una potestad estatal, tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución.

2.3.2. Ley Del Sistema Nacional De Registro De Datos Públicos

La (Ley Orgánica del Sistema Nacional de Registro de Datos Públicos, s.f.) en su artículo 1 establece que su propósito es asegurar la seguridad jurídica, organizar, regular, sistematizar y conectar la información. Además, busca garantizar la eficacia y eficiencia en su manejo, su divulgación, transparencia, acceso e implementación de tecnologías emergentes.

Art. 13.- En este artículo indica que los registros de datos públicos incluyen el Registro Civil, de la Propiedad, Societario, Mercantil, Vehicular, de naves y aeronaves, patentes, de propiedad intelectual y cualquier otro que la Dirección Nacional de Registro de Datos Públicos determine ahora o en el futuro, todo ello en conformidad con lo establecido en la Constitución de la República y las leyes en vigor.

Art. 23.- Sistema Informático: El sistema informático es la digitalización y actualización de los registros, utilizando tecnologías de información, bases de datos y lenguajes de programación estandarizados, así como protocolos seguros de intercambio de datos. Esto permite una gestión adecuada de la información que incluye la recepción, captura, almacenamiento, codificación, protección, intercambio, reproducción, verificación, certificación o procesamiento tecnológico de los datos registrados.

Art. 24.- Interconexión: Para la correcta implementación del sistema de control cruzado a nivel nacional, es obligatorio que los registros y bases de datos se interconecten, con el objetivo de simplificar los procesos y controlar adecuadamente la información de las instituciones pertinentes. El sistema de control cruzado comprende una serie de componentes técnicos e informáticos, que están integrados e interrelacionados, y que interactúan y se nutren mutuamente.

Art. 26.- Seguridad, cada base de datos informática debe tener su correspondiente archivo de respaldo, adherirse a los estándares técnicos y tener un plan de contingencia que prevenga la interrupción del sistema, el hurto de datos, la alteración o cualquier otro evento que pueda perjudicar la información pública.

Art. 31.- Atribuciones y facultades: La Dirección Nacional de Registro de Datos Públicos tendrá las siguientes atribuciones y facultades:

2. Emitir las resoluciones y regulaciones necesarias para la estructuración y operación del sistema.
4. Fomentar, emitir y llevar a cabo, a través de los distintos registros, las políticas públicas mencionadas en esta Ley, así como las normas generales para su seguimiento y control.
5. Unificar, normalizar y gestionar la base de datos única de todos los Registros Públicos. Para ello, todos los miembros del Sistema deben proporcionar información digitalizada de sus archivos, actualizada y de manera simultánea a medida que se produzca.
6. Establecer los programas informáticos y otros aspectos técnicos que todas las dependencias de registro de datos públicos deben implementar para el sistema de interconexión y control cruzado de datos, y mantenerlo funcionando correctamente.
9. Establecer que los datos generados en cada oficina de registro se ingresen a una misma base de datos, en el lenguaje y plataforma determinados por la autoridad.

2.3.3. Dirección Nacional De Registro De Datos Públicos

Resulta crucial considerar diversos artículos legales y normativas vigentes en la RESOLUCIÓN No. 005-NG-DINARDAP-2019, según lo considerado por (Christian Fabián Espinosa Velarde, 2019), Director Subrogante De Registro De Datos Públicos. Dicha resolución se encarga de regular la protección de datos personales, el acceso a la información y la seguridad en el manejo de datos en entornos digitales.

- **Artículo 18 de la Constitución de la República del Ecuador** - Este artículo consagra el derecho a indagar, obtener, compartir, generar y propagar información precisa, así como el acceso a la información producida por organismos públicos.
- **Artículo 66 numeral 19 de la Constitución de la República del Ecuador** - Reconoce el derecho a la salvaguarda de los datos personales y el consentimiento del propietario para la recopilación, almacenamiento, tratamiento y divulgación de dichos datos.

Decreto Ejecutivo No. 1384 - Establece la política pública de interoperabilidad gubernamental, que conlleva la transferencia de datos entre organismos a través de tecnologías de información y comunicación.

CAPÍTULO III

METODOLOGÍA DE LA INVESTIGACIÓN

3.1. TIPOS DE INVESTIGACIÓN

Para la presente investigación se utilizó los siguientes tipos de investigación:

3.1.1. Investigación Descriptiva

Este tipo de investigación que se aplicó con la finalidad de observar, interpretar y analizar patrones de ataques en entornos de Internet de las Cosas. Este enfoque fue esencial para identificar los protocolos de seguridad más vulnerados por los ciberdelincuentes en los dispositivos de Internet de las Cosas. Además, la investigación descriptiva sirvió de base para la selección del algoritmo más adecuado para predecir los ciberataques en estos entornos.

3.2. MÉTODOS UTILIZADOS EN LA INVESTIGACIÓN

Los métodos de investigación que se presentan se aplicarán en función de los objetivos de la investigación, tal como se detalla a continuación:

3.2.1. Método cuantitativo

En este estudio, se optó por el análisis cuantitativo como el método de investigación debido a su capacidad para ofrecer resultados precisos y objetivos. En el contexto de los ciberataques en entornos de Internet de las Cosas, resultó esencial cuantificar y medir con precisión los patrones de ataques y las vulnerabilidades de seguridad. Además, este enfoque proporcionó una base para establecer correlaciones y realizar predicciones. En este caso, la utilización de este método facilitó la comprensión de la frecuencia y el tipo de ciberataques, la gravedad de las vulnerabilidades de seguridad y el rendimiento de los algoritmos predictivos.

3.2.2. Método Deductivo

El método deductivo se utilizó en esta investigación debido a su enfoque sistemático y lógico. Para el efecto, se partió de una teoría general, seguida de su aplicación a un caso particular para finalmente llegar a su confirmación. En este caso, la teoría general fue que ciertos patrones y tendencias podrían indicar la probabilidad de ciberataques. A partir de esta teoría, se especuló sobre qué algoritmos de predicción podrían ser más efectivos. Luego, se recopilaron y analizaron datos para observar si los resultados empíricos respaldaban estas premisas. Finalmente, se confirmó la premisa inicial al identificar el algoritmo de predicción más efectivo. Por lo tanto, el uso del método deductivo permitió una investigación rigurosa y sistemática, lo que resultó en decisiones informadas y fundamentadas para conseguir un modelo eficiente.

3.3. CONSTRUCCIÓN METODOLÓGICA DEL OBJETO DE INVESTIGACIÓN

3.2.1. Técnicas de investigación

Las siguientes técnicas de investigación fueron las que se utilizaron para cumplir con el desarrollo del estudio, permitiendo así alcanzar los objetivos propuestos:

Estadística descriptiva: La estadística descriptiva permitió entender los datos para proporcionarte resúmenes sobre las muestras y las medidas. Además, facilitó la identificación de tendencias, patrones y relaciones que podrían no ser evidentes a simple vista.

Aprendizaje Automático (Machine Learning): Esta técnica permitió aplicar algoritmos de clasificación para predecir la probabilidad de variables categóricas multiclases.

Análisis predictivo: El análisis predictivo permitió utilizar datos históricos para hacer predicciones sobre eventos o resultados futuros, aplicando técnicas de clasificación, regresión o series temporales.

Visualización de Datos: Se utilizó gráficos y representaciones visuales para comunicar patrones y tendencias en los datos, ayudando a las personas a entender mejor los resultados del análisis.

3.2.2. Instrumentos de Investigación

En este estudio se ha optó por emplear herramientas de análisis, visualización y manipulación de datos, necesarias para su desarrollo. Los instrumentos utilizados son los siguientes:

Herramientas de manipulación de datos:

- **MS Excel:** Es un programa de hoja de cálculo que usó para organizar los datos y la información que contiene el conjunto de datos CICIOT2023.

Lenguaje de programación y librerías:

- **Python:** Python permite trabajar de forma muy versátil y flexible. Dispone de una gran cantidad de librerías para desarrollar proyectos referentes a Ciencia de Datos, por ejemplo, panda, numpy y scikit-learn
- **Visual Studio Code:** Es un editor de código abierto, que ofrece una amplia gama de funciones y es utilizado por desarrolladores en una variedad de campos y tecnologías debido a su versatilidad y capacidad de personalización

Herramientas de visualización:

- **Power BI**: Esta herramienta permite realizar análisis y gestión de grandes volúmenes de datos.
- **Matplotlib y Seaborn**: Son librerías de Python para crear gráficos y visualizaciones.

3.4. ELABORACIÓN DEL MARCO TEÓRICO

El marco teórico de esta investigación consiste en proporcionar un contexto intelectual y conceptual necesario para comprender y abordar el problema de investigación. Además, incluye conceptos clave y relaciones entre variables relevantes, lo que contribuye a situar el estudio en un contexto académico más amplio, aumentando así su relevancia y su contribución al avance del conocimiento en el campo del tema investigación.

Revisión de antecedentes: Se realizó una revisión bibliográfica de trabajos existentes que abordaran el mismo problema de este estudio o que tuvieran relación con la investigación. Al revisar trabajos previos, se pudo entender mejor el estado actual de conocimiento sobre el campo de estudio. Esto permitió identificar las brechas en la literatura existente que la investigación podría llenar. Además, la revisión de los antecedentes permitió realizar un trabajo original evitando duplicar otros trabajos ya existentes.

Lluvia de ideas con las variables clave: Se creó un borrador y se empezó a escribir todos los conceptos o temas que se deseaban indagar, ya que la lluvia de ideas ayudó a identificar y explorar diversas variables, conceptos y teorías que eran relevantes para este estudio. Además, la lluvia de ideas permitió fomentar el pensamiento creativo y crítico, lo cual era esencial en la investigación.

Organiza la información: Se organizó la información recopilada de manera lógica y coherente, lo cual era esencial para mantener el orden y la claridad en el proceso de investigación y permitir el acceso rápido a los recursos necesarios, analizar datos de manera eficiente y mantener un enfoque coherente en la construcción del marco teórico.

Desarrollo del Marco Conceptual: Se definieron y detallaron los conceptos relevantes para la investigación con base en el análisis previo. Este proceso me permitió establecer una base sólida de conocimientos teóricos sobre el tema de estudio.

Desarrollo del Marco Legal: Se desarrolló un marco legal en mi investigación, lo cual era esencial para garantizar la legalidad, ética y validez de mi estudio. Ayudó a proteger los derechos de los autores y proporcionó directrices claras para la conducción de la investigación de manera ética y conforme a la ley. Esto, a su vez, contribuyó a la credibilidad y el rigor de mi investigación.

3.5. RECOLECCIÓN DE LA INFORMACIÓN

3.5.1. Fuentes secundarias

Como fuentes secundarias se emplearon documentos científicos pertinentes como libros, artículos, textos, etc. que garantizan la correcta aplicación de la metodología de la investigación.

3.5.2. Fuentes Primarias

El sitio web del Instituto Canadiense de Ciberseguridad (CIC) se utilizó como fuente primaría de información para la investigación. Este conjunto de datos, de nombre CICIOT2023, abarca una amplia gama de dispositivos y sistemas en entornos de Internet de las Cosas. El conjunto de datos está compuesto 33 tipos de ataques

segmentados en siete familias que se clasifican en categorías: DDoS, DoS, Recon, basados en Web, Fuerza Bruta, Spoofing y Mirai. Todos los ataques son ejecutados en una red de dispositivos de Internet de las Cosas compuestos por equipos reales en los cuales adoptan dispositivos IoT como atacantes y víctimas.

Para este trabajo, se utilizaron todos los registros contenidos en el conjunto de datos CICIOT2023, porque permitió realizar un análisis, maximizando la capacidad del estudio para identificar patrones, analizar vulnerabilidades y predecir futuros ciberataques. A continuación, se describen las variables pertenecientes al conjunto de datos.

Tabla 1 - Descripción de variables del conjunto de datos
Fuente: Autor

Variables	Concepto	Indicadores
Ts	Timestamp (Marca de tiempo) que indica cuándo ocurrió el evento en la red.	Marca de tiempo
flow_duration	Duración de una comunicación de red o flujo de datos, medida en segundos o milisegundos.	Duración del flujo del paquete
Header_Length	Longitud del encabezado de un paquete de datos en bytes. Representa la cantidad de información de control antes de los	Longitud del encabezado

	datos reales.	
Protocol type	Tipo de protocolo de red utilizado en la comunicación.	encabezado IP, UDP, TCP, IGMP, ICMP, desconocido (enteros)
Duration	Duración de un evento específico, como una conexión o una transacción, medida en segundos o milisegundos.	Tiempo de vida (ttl)
Rate	Tasa o velocidad de transferencia de datos, generalmente medida en bits por segundo (bps) o paquetes por segundo (pps).	Tasa de transmisión de paquetes en un flujo
Srate	Tasa de transferencia de datos en dirección de origen (source), medida en bits por segundo (bps) o paquetes por segundo (pps).	Tasa de transmisión de paquetes salientes en un flujo
Drate	Tasa de transferencia de datos en dirección de destino (destination), medida en bits por segundo (bps) o paquetes por segundo (pps).	Tasa de transmisión de paquetes entrantes en un flujo

fin_flag_number	Número de veces que se estableció la bandera FIN en los paquetes, indicando el cierre de una conexión TCP.	Valor de la bandera de aleta
syn_flag_number	Número de veces que se estableció la bandera SYN en los paquetes, indicando la solicitud de una nueva conexión TCP.	Valor del indicador de sincronización
rst_flag_number	Número de veces que se estableció la bandera RST en los paquetes, indicando el reinicio de una conexión TCP o la respuesta a una solicitud inválida.	Valor del primer indicador
psh_flag_number	Número de veces que se estableció la bandera PSH en los paquetes, indicando la solicitud de un procesamiento inmediato de datos en TCP.	Valor de la bandera psh
ack_flag_number	Número de veces que se estableció la bandera ACK en los paquetes, indicando el reconocimiento de	Valor del indicador de confirmación

	datos en una conexión TCP.	
ece_flag_number	Número de veces que se estableció la bandera ECE (Explicit Congestion Notification Echo) en los paquetes, utilizada en TCP para la notificación de congestión en la red.	Valor de la bandera Ece
cwr_flag_number	Número de veces que se estableció la bandera CWR (Congestion Window Reduced) en los paquetes, también utilizada en TCP para la notificación de congestión en la red.	Valor de la bandera Cwr
ack_count	Conteo total de paquetes con la bandera ACK establecida en la comunicación.	Número de paquetes con indicador de confirmación configurado en el mismo flujo
syn_count	Conteo total de paquetes con la bandera SYN establecida en la comunicación.	Número de paquetes con el indicador syn configurado en el mismo flujo

fin_count	Conteo total de paquetes con la bandera FIN establecida en la comunicación.	Número de paquetes con el indicador fin configurado en el mismo flujo
urg_count	Conteo total de paquetes con la bandera URG (Urgent) establecida en la comunicación, indicando datos urgentes en TCP.	Número de paquetes con el indicador urg configurado en el mismo flujo
rst_count	Conteo total de paquetes con la bandera RST establecida en la comunicación.	Número de paquetes con el primer indicador establecido en el mismo
HTTP	Indicación de la presencia de tráfico HTTP (Hypertext Transfer Protocol), utilizado para la transferencia de datos en la web.	flujo Indica si el protocolo de la capa de aplicación es HTTP
HTTPS	Indicación de la presencia de tráfico HTTPS (Hypertext Transfer Protocol Secure), una versión segura de HTTP que utiliza cifrado SSL/TLS.	Indica si el protocolo de la capa de aplicación es HTTPS

DNS	Indicación de la presencia de tráfico DNS (Domain Name System), que resuelve nombres de dominio en direcciones IP y viceversa.	Indica si el protocolo de la capa de aplicación es DNS
Telnet	Indicación de la presencia de tráfico Telnet, un protocolo de acceso remoto que permite la administración de dispositivos a través de la red.	Indica si el protocolo de capa de aplicación es Telnet
SMTP	Indicación de la presencia de tráfico SMTP (Simple Mail Transfer Protocol), utilizado para el envío de correo electrónico.	Indica si el protocolo de capa de aplicación es SMTP
SSH	Indicación de la presencia de tráfico SSH (Secure Shell), un protocolo seguro para la administración remota de sistemas.	Indica si el protocolo de capa de aplicación es SSH
IRC	indicación de la presencia de tráfico IRC (Internet Relay Chat), utilizado para la comunicación en tiempo real en salas de chat en línea.	Indica si el protocolo de capa de aplicación es IRC

TCP	Conteo o indicación de la presencia de tráfico TCP (Transmission Control Protocol), un protocolo de comunicación confiable y orientado a la conexión.	Indica si el protocolo de la capa de transporte es TCP
UDP	Conteo o indicación de la presencia de tráfico UDP (User Datagram Protocol), un protocolo de comunicación no confiable y sin conexión.	Indica si el protocolo de la capa de transporte es UDP
DHCP	Conteo o indicación de la presencia de tráfico DHCP (Dynamic Host Configuration Protocol), utilizado para asignar direcciones IP dinámicas a dispositivos en una red.	Indica si el protocolo de la capa de aplicación es DHCP
ARP	Conteo o indicación de la presencia de tráfico ARP (Address Resolution Protocol), que asocia direcciones IP a direcciones MAC en una red local.	Indica si el protocolo de capa de enlace es ARP
ICMP	Conteo o indicación de la presencia de tráfico ICMP (Internet Control Message Protocol), utilizado para el	Indica si el protocolo de capa de red es ICMP

	diagnóstico y control de red, incluyendo ping.	
IPv	Conteo o indicación de la presencia de tráfico IPv4 o IPv6, que son las dos versiones principales del Protocolo de Internet.	Indica si el protocolo de capa de red es IP
LLC	Conteo o indicación de la presencia de tráfico LLC (Logical Link Control), una subcapa de control de enlace de datos en la arquitectura de redes OSI.	Indica si el protocolo de capa de enlace es LLC
Tot sum	Suma total de los valores de una variable específica en un conjunto de datos, indicando la suma de todas las observaciones.	Suma de longitudes de paquetes en flujo
Min	El valor mínimo (más bajo) registrado en una variable o conjunto de datos, representando el valor más pequeño observado.	Longitud mínima del paquete en el flujo
Max	El valor máximo (más alto) registrado en una variable o	Longitud máxima del

	conjunto de datos, representando el valor más grande observado.	paquete en el flujo
AVG	Promedio (media) de los valores de una variable o conjunto de datos, calculado como la suma total dividida por el número de observaciones.	Longitud promedio de paquetes en el flujo
Std	Desviación estándar, una medida de dispersión que indica cuán dispersos están los valores con respecto a la media.	Desviación estándar de la longitud de paquetes en el flujo
Tot size	Tamaño total, que puede referirse al tamaño total de los datos transmitidos en una comunicación de red o al tamaño total de un conjunto de datos.	Longitud del paquete
IAT	Inter-Arrival Time (Tiempo entre llegadas), que mide el tiempo transcurrido entre la llegada de dos eventos consecutivos en una secuencia de datos o eventos.	La diferencia horaria con el paquete anterior.

Number	Número total de observaciones o eventos en un conjunto de datos o secuencia.	El número de paquetes en el flujo.
Magnitue	Magnitud de un valor o evento en una escala específica.	(Promedio de las longitudes de los paquetes entrantes en el flujo
Radius	Representa el radio de una esfera o círculo en un contexto geométrico o la distancia máxima desde un punto central en un conjunto de datos multidimensional.	+ Promedio de las longitudes de los paquetes salientes en el flujo) ** 0,5
Covariance	Medida de la relación entre dos variables en un conjunto de datos. Indica cómo cambian juntas dos variables.	(Varianza de las longitudes de los paquetes entrantes en el flujo +
Variance	Medida de la dispersión de los valores de una variable con respecto a su media.	Tasa de transmisión de paquetes en un flujo
Weight	Se refiere al valor asignado a una observación o variable en un cálculo	Tasa de transmisión de paquetes salientes en un

	ponderado o en un análisis estadístico.	flujo
Label	Variable categórica de clasificación multiclase.	Todos los tipos de ataques recibidos

Para la captura de los datos que conforman el conjunto de datos fue realizado en un laboratorio del Instituto Canadiense de Ciberseguridad (CIC) utilizando Wireshark para la captura de tráfico. A su vez, cuentan con una red IoT dedicada para fomentar el desarrollo de soluciones de seguridad de IoT. Los atacantes y las víctimas se encuentran dentro de esta misma red; por lo tanto, es un ambiente controlado donde se ejecutaron los distintos tipos de ataques a diversos dispositivos IoT.

A continuación, se muestra la lista de dispositivos domésticos inteligentes, cámaras, sensores y microcontroladores que fueron conectados y configurados para permitir la ejecución de varios ataques y capturar el tráfico de ataque correspondiente.

Tabla 2 - Dispositivos IoT utilizados para formar el conjunto de datos
Fuente: Autor

	Nombre de Dispositivos IoT	Categoría	Nombre de Dispositivos IoT	Categoría
Víctimas	Amazon Alexa Echo Dot 1	Audición	Bombilla Lumiman	Iluminación
	Amazon Alexa Echo Dot 2	Audición	Puente Philips Hue	Concentrador

	Amazon Alexa Echo Spot	Audición	Pizarra inteligente	Domótica
	Amazon Alexa Echo Studio	Audición	Tira de luz Teckin	Iluminación
	Espectáculo de Amazon Echo	Audición	Enchufe Teckin 1	Tomacorriente
	Altavoz Google Nest Mini	Audición	Enchufe Teckin 2	Tomacorriente
	harman kardon (Ampak Technology)	Audición	Enchufe inteligente Wemo 1 (Wemo id: Wemo.Mini.AD3)	Tomacorriente
	Altavoz Sonos One	Audición	Enchufe inteligente Wemo 2 (Wemo id: Wemo.Mini.4A3)	Tomacorriente
	Cámara WiFi AMCREST	Cámara	Enchufe Yutron 1	Tomacorriente
	Estación base Arlo	Cámara	Enchufe Yutron 2	Tomacorriente
	Cámara interior Arlo Q	Cámara	Televisor inteligente LG	Domótica
	Cámara	Cámara	Estación	Domótica

	Borun/Sichuan-AI		meteorológica Netatmo	
	DCS8000LHA1 Mini cámara D-Link	Cámara	Raspberry Pi 4: 2 GB	NextGen
	Cámara WiFi inteligente HeimVision	Cámara	Raspberry Pi 4: 2 GB	NextGen
	Cámara de ojo para el hogar	Cámara	Raspberry Pi 4: 2 GB	NextGen
	Perro de cámara Luohe	Cámara	Fibaro Sensor de puerta/ventana 1	Sensor
	Cámara interior Nest	Cámara	Fibaro Sensor de Puerta/Ventana 2	Sensor
	Cámara Netatmo	Cámara	Fibaro Sensor de puerta/ventana 3	Sensor
	Cámara Rbcior	Cámara	Sensor de inundación Fibaro 1	Sensor
	SIMCAM 1S (AMPAKTec)	Cámara	Sensor de inundación Fibaro 2	Sensor
	Cámara TP-Link	Cámara	Sensor de	Sensor

	Tapo		movimiento Fibaro 1	
	Cámara Wyze	Cámara	Sensor de movimiento Fibaro 2	Sensor
	Cámara interior Yi	Cámara	Sensor de movimiento Fibaro 3	Sensor
	Cámara Yi Indoor 2	Cámara	Sensor de movimiento Fibaro 4	Sensor
	Cámara para exteriores Yi	Cámara	Sensor de movimiento Fibaro 5	Sensor
	Eufy HomeBase 2	Concentrador	Enchufe de pared Fibaro 1	Tomacorriente
	Enchufe de Amazon	Tomacorriente	Enchufe de pared Fibaro 2	Tomacorriente
	Cafetera Atomi	Domótica	Teclado de alarma de timbre	Domótica
	Ventilador HVAC inteligente Cocoon	Domótica	Extensor de rango de anillo	Domótica
	Lámpara de globo	Iluminación	Sensor de contacto de anillo (1)	Sensor

	ESP_B1680C			
	Bombilla GoSund	Iluminación	Sensor de contacto de anillo (2)	Sensor
	Regleta Gosund (1)	Tomacorriente	AeoTec TriSensor	Sensor
	Regleta GoSund (2)	Tomacorriente	Timbre AeoTec 6	Domótica
	Enchufe inteligente GoSund WP2 (1)	Tomacorriente	Sirena interior AeoTec	Domótica
	Enchufe inteligente GoSund WP2 (2)	Tomacorriente	Interruptor inteligente AeoTec 7	Domótica
	Enchufe inteligente GoSund WP2 (3)	Tomacorriente	Sensor de agua AeoTec 6	Sensor
	Enchufe inteligente GoSund WP3 (1)	Tomacorriente	AeoTec NanoMote Quad	Domótica
	Enchufe inteligente	Tomacorriente	AeoTec Sensor de puerta/ventana 7 Pro	Sensor

	Gosund WP3 (2)			
	Humidificador inteligente Govee	Domótica	Sensor de temperatura y humedad AeoTec	Sensor
	Radio/Lámpara HeimVision SmartLife	Iluminación	Philips Hue Blanco 1	Iluminación
	iRobot Roomba	Domótica	Philips Hue Blanco 2	Iluminación
	LampUX RGB	Iluminación	Bombilla inteligente SmartThings 1	Iluminación
	Purificador de aire Levoit	Domótica	Bombilla inteligente SmartThings 2	Iluminación
	Bombilla LIFX	Iluminación	Botón Aeotec	Domótica
	Centro de SmartThings	Concentrador	Sensor de movimiento AeoTec	Sensor
	Concentrador de hogar inteligente AeoTec	Concentrador	Sensor multipropósito AeoTec	Sensor
	Enchufe inteligente Sengled 2	Tomacorriente	Sensor de fugas de agua AeoTec	Sensor

	Botón SmartThings	Domótica	Enchufe inteligente Sengled 1	Tomacorriente
	Bombilla inteligente SmartThings 3	Iluminación	Enchufe inteligente Sonoff 2	Tomacorriente
	Enchufe inteligente Sonoff 1	Tomacorriente	Cámara exterior Arlo Ultra 2	Cámara
Atacantes	Raspberry Pi 4: 4 GB	NextGen	Raspberry Pi 4: 2 GB	NextGen
	Raspberry Pi 4: 8 GB	NextGen	Raspberry Pi 4: 2 GB	NextGen
	Raspberry Pi 4: 2 GB	NextGen	Raspberry Pi 4: 2 GB	NextGen
	Raspberry Pi 4: 2 GB	NextGen	Estación base de anillo	Concentrador
	Fibaro Home Center Lite	Concentrador	Cámara de timbre Eufy	Cámara

3.6. PROCESAMIENTO Y ANÁLISIS

Se detallaron los mecanismos utilizados para el procesamiento de la información, donde se empleó la metodología KDD (Knowledge Discovery in Databases) de (Maimon & Rokach, 2005). Este procedimiento abarcó distintas etapas, incluyendo la selección de datos pertinentes, el preprocesamiento, la transformación, la minería de datos y la evaluación e implementación de los hallazgos resultantes.

Antes de pasar por cada una de las fases de la metodología KDD es importante seleccionar la infraestructura a utilizar para aplicar cada uno de los procesos del modelo. A continuación, se describen las alternativas que existen para poder ejecutar el proyecto de investigación.

La infraestructura local consiste en el uso de un equipo computacional, el cual se empleó en este proyecto de investigación debido al bajo costo que representa para generar el modelo. Sin embargo, la desventaja radicaba en su velocidad para producir los resultados. Por otro lado, se cotizo el costo de la infraestructura en la nube de (Microsoft Azure, 2024), el cual observamos que tiene un costo significativamente mayor, podría generar resultados mucho más rápidos; no obstante, esta opción resulta viable principalmente a nivel empresarial.

Tabla 3 - Infraestructura local - Equipo Computacional
Fuente: Autor

Infraestructura Local
• Procesador i3 9100F • Memoria RAM 16GB a 2666mhz • Almacenamiento SSD 500GB

• Tarjeta Madre Asus H310 • Tarjeta gráfica Nvidia RTX 2070 8GB • Case
Total: $650

Tabla 4 - Infraestructura en la nube - Microsoft Azure
Fuente: Autor

Infraestructura en la nube – Costo mensual	Infraestructura en la nube – Costo Anual
• Azure Machine Learning – 8 vCPUs / 32GB RAM / 300GB Storage	• Azure Machine Learning – 8 vCPUs / 32GB RAM / 300GB Storage
Total: $329.96	Total: $3,959.52

El proceso KDD consta de varias fases:

- **Selección:** Determinar las metas y seleccionar el conjunto de datos objetivo.
- **Preprocesamiento:** Limpieza y procesamiento de la información.
- **Transformación:** Cambiar los datos a una forma adecuada para la minería.
- **Minería de datos:** Uso de técnicas específicas para extraer patrones a partir de los datos.
- **Evaluación e implantación:** Interpretación y análisis de los patrones encontrados y utilización del conocimiento obtenido para la toma de decisiones.

Ilustración 1 - Metodología Knowledge Discovery in Databases (KDD)
Fuente: Autor

3.6.1. Selección

En esta fase, se seleccionaron las variables más relevantes del conjunto de datos CICIOT2023 (Brunswick, 2023), proporcionado por el Instituto Canadiense de Ciberseguridad (CIC). Este conjunto de datos, que abarca una amplia gama de dispositivos y sistemas en entornos de Internet de las Cosas, consta de 33 tipos de ataques segmentados en siete familias. Se planteó seleccionar todas las variables del conjunto de datos, que consta de un total de 46686747 instancias y 47 atributos. Dada la gran cantidad de variables, se planteó categorizarlas para organizar y comprender mejor los datos. Esta selección y categorización de variables permitieron un análisis más eficiente y efectivo en las siguientes etapas de la metodología KDD. Además, se realizó un análisis adicional para identificar y seleccionar las variables más relevantes para la

predicción de ciberataques. Esto permite mejorar la eficiencia de los algoritmos de predicción en las etapas posteriores de la investigación.

3.6.2. Preprocesamiento

Se realiza un proceso ETL (Extract, Transform, Load) (García Del Río & López Contreras, 2018) para consolidar los 169 archivos CSV del conjunto de datos en un solo archivo, ya que el conjunto de datos se encuentra fragmentado en varias partes. Este proceso implica la extracción de los datos de cada archivo CSV, seguido de su carga en un solo archivo CSV y en un servidor de MS SQL Server. Esto permitió una integración de la información de los archivos originales, facilitando un acceso más sencillo y un análisis unificado de todos los datos recolectados.

3.6.3. Transformación

Se realizó la búsqueda de características para representar los datos en función de los objetivos planteados. Se aplicaron técnicas de reducción como agregaciones, compresión de datos, segmentación, discretización basada en entropía, muestreo, entre otros. Se realizó la transformación de la variable dependiente Label, que contiene el nombre de los ataques, creando una nueva variable con la segmentación de las siete familias para definir el tipo o la categoría del ciberataque. Esto se planteó con el fin de mejorar los tiempos de respuesta y precisión de los resultados durante el modelamiento.

3.6.4. Minería de datos

Durante esta fase se realizó el proceso de modelamiento o minería de datos. Se buscó descubrir patrones de interés mediante técnicas supervisadas. Esta fase se ejecutó en la plataforma Google Colab, utilizando Python. Se trabajó con 6 algoritmos: *Random*

Forest, *Decision Tree*, SVM (Support Vector Machine), KNN (K-Nearest Neighbors), *Gradient Boosting* y *Naive Bayes*. Se seleccionaron diversos algoritmos de aprendizaje automático para abordar el problema de ciberataques en entornos de Internet de las cosas. La selección de los algoritmos mencionados anteriormente se basa acorde con la investigación de (Alharbi et al., 2022), en donde muestra la eficacia que tienen estos algoritmos de aprendizaje automático para realizar predicciones. Además, empresas como (The MathWorks Inc, 2023), sugieren utilizar este tipo de algoritmos, ya que frecuentemente suelen ser utilizados cuando se refiere a aprendizaje automático supervisado.

Además, cada algoritmo se entrenó utilizando el conjunto de datos preparado y se ajustaron sus parámetros para optimizar el rendimiento. Se llevaron a cabo evaluaciones utilizando técnicas como la validación cruzada. Según (Berrar, 2018) cuando se trabaja con validación cruzada se recomienda un rango de 20 % a 30 % para prueba y 70 % a 80 % para entrenamiento, en este trabajo se dividió un 70 % de los datos para entrenamiento y un 30 % para prueba, y así medir la eficacia de cada modelo. La elección de estos algoritmos se basó en su idoneidad para el problema específico de prever ciberataques en entornos de IoT y su capacidad para manejar la complejidad y la dimensionalidad de los datos involucrados. Los resultados obtenidos en esta fase fueron fundamentales para seleccionar el modelo final que mejor se ajusta a los objetivos del proyecto.

3.6.5. Métricas de evaluación

La evaluación de diferentes algoritmos y configuraciones se lleva a cabo en función de métricas de evaluación. Dado que TP representa los Verdaderos Positivos, TN los

Verdaderos Negativos, FP los Falso Positivos y FN los Falsos Negativos, las métricas utilizadas en esta investigación son:

- **Accuracy:** se encarga de evaluar los modelos de clasificación representando la proporción de predicciones correctas en un conjunto de datos determinado y se basa en la siguiente expresión:

$$\text{Acc} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}}$$

- **Recall:** la relación entre las etiquetas correctamente identificadas y el número total de apariciones de esa etiqueta en particular:

$$Rec = \frac{TP}{TP + FN}$$

- **Precision:** la relación entre las etiquetas correctamente identificadas y el número total de clasificaciones positivas:

$$Pre = \frac{TP}{TP + FP}$$

- **F1-Score:** promedio geométrico de precisión y recuperación:

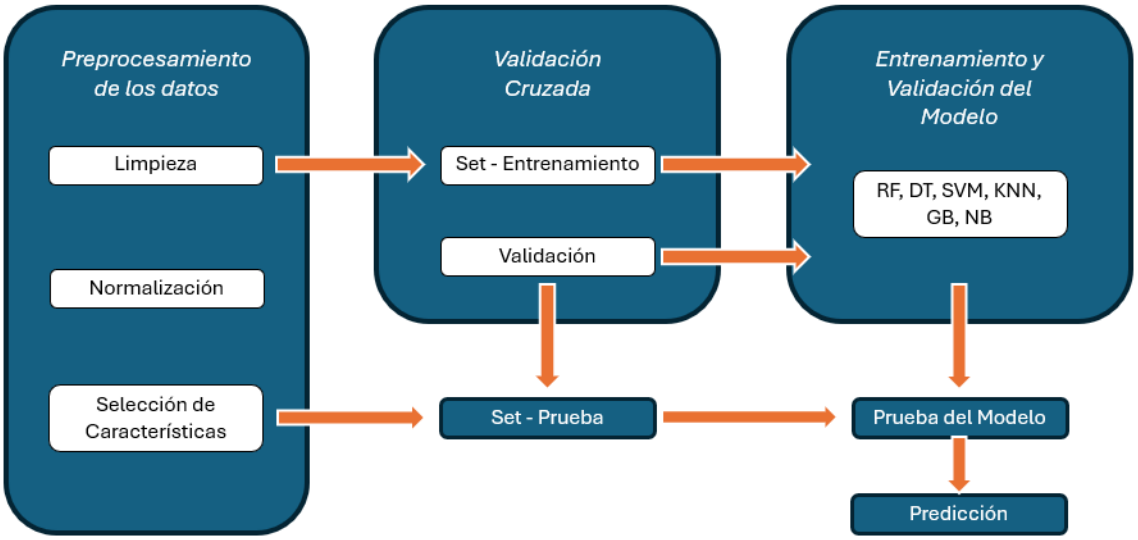
$$F1 = 2 \times \frac{Pre \times Rec}{Pre + Rec}$$

3.6.6. Evaluación

En esta última fase, se ejecutan y evalúan los resultados de los algoritmos que se utilizaron para el modelo predictivo, posteriormente se compararon los resultados utilizando las siguientes métricas de evaluación: Accuracy, Precision, Recall, F1-Score y R-Squared. Finalmente, luego de obtener los resultados se realizó una interpretación y

discusión de los resultados, esto permitió seleccionar el algoritmo con mejores resultados para el modelo predictivo.

Ilustración 2 - Arquitectura del Modelo Predictivo de Ciberataques
Fuente: Autor



CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

4.1. Identificación de patrones de ataques en entornos de Internet de las Cosas

Para identificar los patrones de ataques, se realizó la selección de todas las variables del conjunto de datos, que consta de un total de 46686747 instancias y 47 atributos. Al haber una gran cantidad de variables, estas fueron categorizadas en la siguiente tabla para organizar y comprender de mejor forma los datos.

Tabla 5 - Categorización para reducir la dimensionalidad de las variables
Fuente: Autor

Categoría	Variables	Descripción
Duración	'flow_duration', 'Duration', 'IAT'	Variables relacionadas con la duración y tiempos entre eventos
Características de Flujo	'Header_Length', 'Rate', 'Srate', 'Drate', 'Tot size'	Características específicas del flujo de datos
Flags de Control	'fin_flag_number', 'syn_flag_number', 'rst_flag_number', 'psh_flag_number', 'ack_flag_number', 'ece_flag_number', 'cwr_flag_number'	Número de ocurrencias de diferentes flags de control TCP
Contadores de	'ack_count', 'syn_count', 'fin_count',	Contadores de ocurrencias de

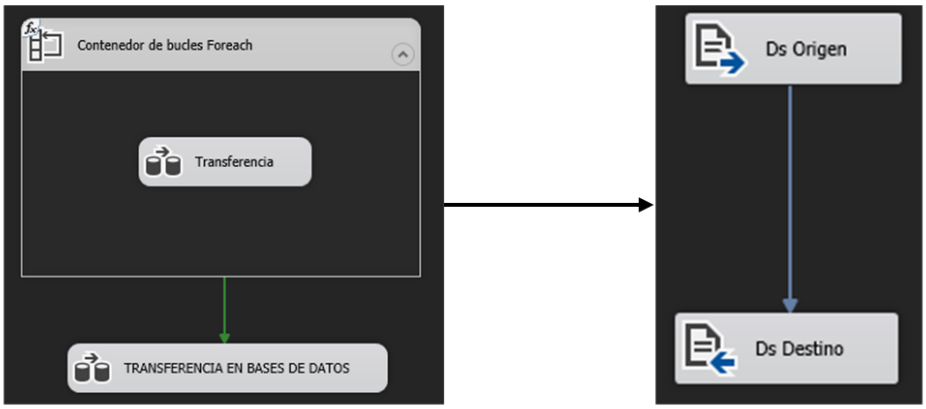
Flags	'urg_count', 'rst_count'	diferentes flags TCP
Protocolos	'HTTP', 'HTTPS', 'DNS', 'Telnet', 'SMTP', 'SSH', 'IRC', 'TCP', 'UDP', 'DHCP', 'ARP', 'ICMP', 'IPv', 'LLC'	Variables binarias que indican la presencia de ciertos protocolos
Estadísticas Básicas	'Min', 'Max', 'AVG', 'Std'	Estadísticas básicas de las variables numéricas
Magnitud y Distancia	'Number', 'Magnitue', 'Radius'	Variables relacionadas con la magnitud y distancia
Propiedades de Datos	'Covariance', 'Variance', 'Weight'	Propiedades estadísticas de los datos
Etiqueta	'label'	Variable de etiqueta que indica la clase o categoría

Se realizó un proceso ETL, inicialmente se cargaron múltiples archivos CSV desde una carpeta y se consolidaron en un único archivo en formato CSV. Posteriormente, se cargan los datos a un servidor de MS SQL Server correspondiendo así a una integración de la información de los archivos originales, permitiendo un acceso más sencillo y un

análisis unificado de la totalidad de los datos recolectados. Este proceso garantiza la coherencia y la consolidación de la información dispersa en diferentes archivos en una sola fuente de datos consolidada.

La Ilustración 3 representa el flujo de proceso automatizado de integración de datos desarrollado mediante la herramienta de MS SQL Server Integration Services (SSIS).

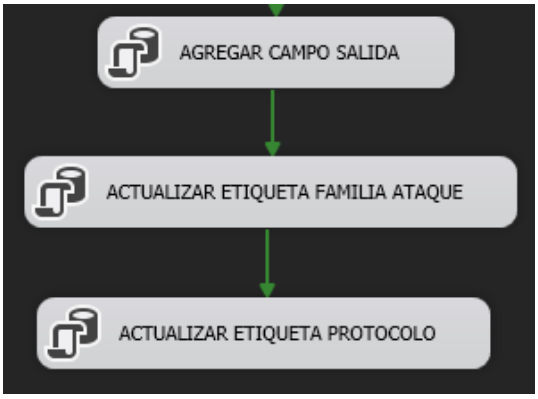
Ilustración 3 - Flujo de proceso de integración de datos
Fuente: Autor



Posteriormente se realizó la búsqueda de patrones en las variables, se utilizaron métodos de reducción de dimensiones o de transformación con el fin de preparar la data para el modelamiento. Para ello, se emplearon técnicas de reducción como agregaciones, compresión de datos, histogramas, segmentación, discretización basada en entropía, muestreo, etcétera. En el flujo de proceso se transforma la variable dependiente *Label*. Esta variable contiene el nombre de los ataques como DDoS-RSTFINFlood o Recon-OSScan. Se procedió a crear una nueva variable con la segmentación de las siete familias para definir el tipo o la categoría del ciberataque. Esto con el fin de que durante el modelamiento los tiempos de respuesta y los resultados mejoren.

La Ilustración 4 representa el flujo del proceso explicado anteriormente.

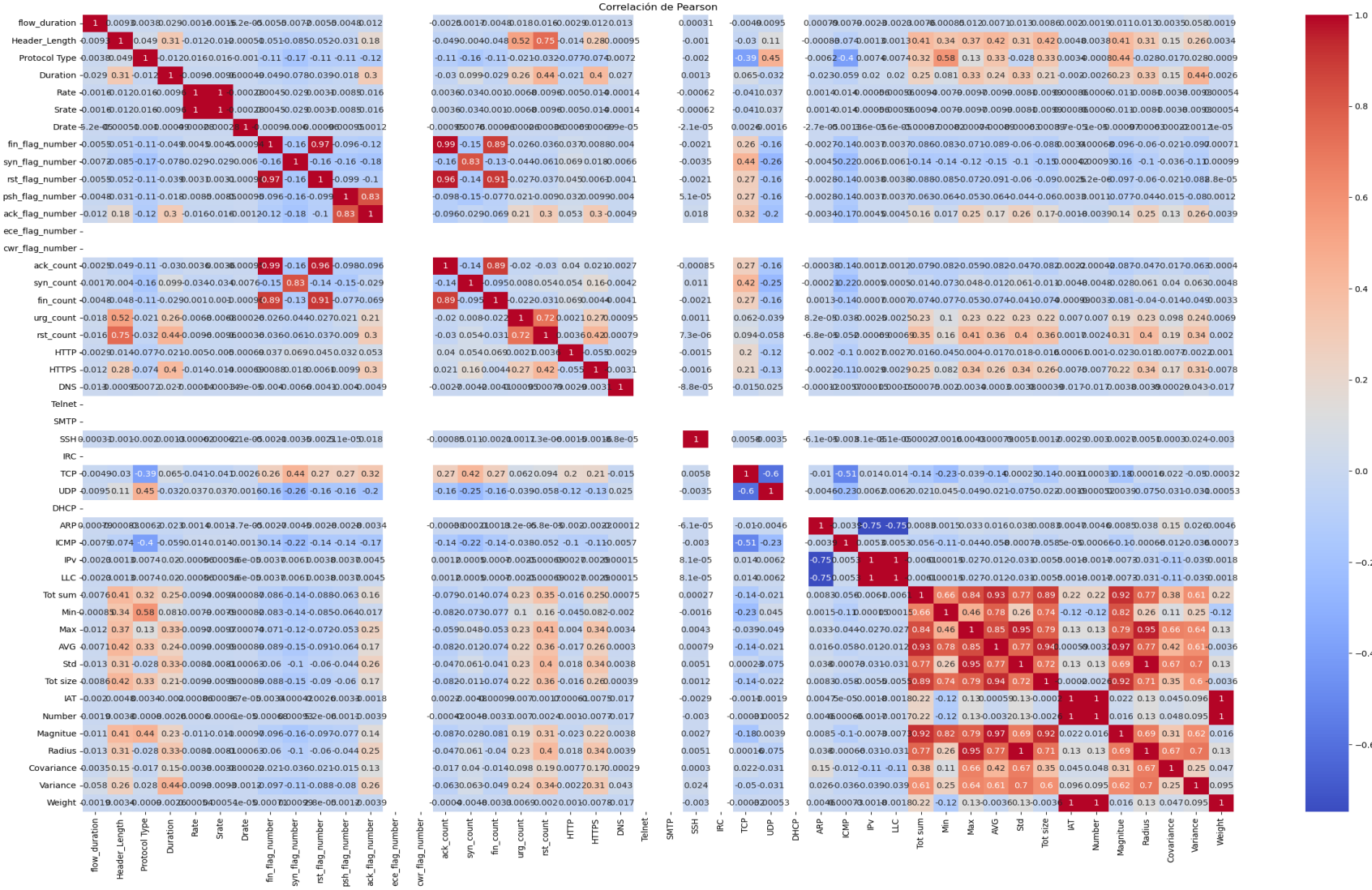
Ilustración 4 - Flujo de proceso de integración de datos - Categorización
Fuente: Autor



Además, con el fin de explorar las relaciones entre variables, se procede a validar la correlación que tienen las variables entre sí, a través de una matriz. Aquellas variables que tienen alta correlación son eliminadas del modelo porque no hacen aporte alguno; por el contrario, produce ruido.

La Ilustración 5 muestra la matriz de correlación entre las variables. Mientras el color rojo o azul sea más intenso, la correlación será mayor lineal o inversamente. En el mapa, se evidencia una conexión a través de líneas blancas entre ciertas variables, indicando la presencia exclusiva de valores cero en esas variables. Por ende, la ausencia de correlación entre dichas variables es clara.

Ilustración 5 - Matriz de correlación de Pearson
Fuente: Autor



4.1.1. Discusión

La identificación de patrones de ataques entorno a los resultados obtenidos demuestran que el uso de todas las variables seleccionadas ayuda a mejorar la precisión de los resultados. La capacidad de identificar estos patrones y tendencias en los datos permitió una comprensión más profunda del conjunto de datos. Sin embargo, es importante tener en cuenta que los patrones identificados son específicos del conjunto de datos utilizado y pueden no ser generalizables a otros entornos de IoT. Por otro lado, la creación de una variable que contiene las familias de los tipos de ataques permitió mejorar los resultados del modelo, porque se redujo significativamente el número de variables a predecir.

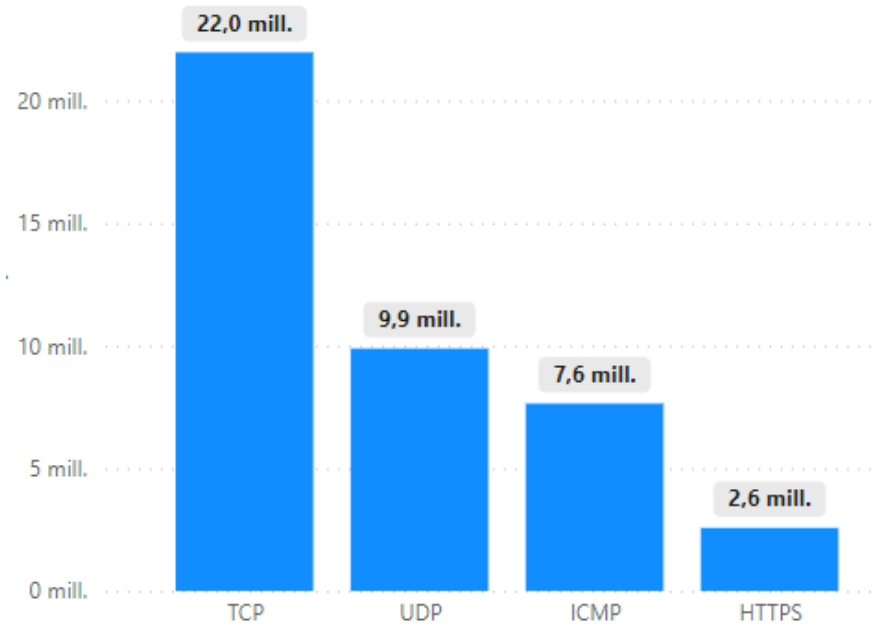
La investigación realizada por (Bilal et al., 2022) evidencia que el uso de una matriz de correlación de Pearson ayuda a identificar aquellas variables con mayor impacto en trabajos que contienen un gran número de variables. Además, se utilizó la librería de Python, Seaborn, para crear una matriz de correlación y visualizar todas las variables del conjunto de datos. Esta visualización reveló que existen variables, como Telnet, SMTP, IRC, DHCP, ece_flag_number y cwr_flag_number, que no tienen ninguna correlación entre sí. Sin embargo, durante el desarrollo del modelo, observo que la precisión mejoraba cuando no excluíamos estas variables. Por lo tanto, se pudo concluir que estas variables actúan como un patrón fundamental que permite a los algoritmos mejorar la precisión de sus resultados.

4.2. Análisis de los protocolos más vulnerados por ciberataques en entornos de Internet de las Cosas

En este apartado, se utilizó Power BI para realizar un análisis de frecuencia y poder evidenciar aquellos protocolos que frecuentemente se encuentran bajo ataque. Una vez completada la fase de preparación de los datos, se precedió a cargar todo el conjunto de datos, y mediante gráficos estadísticos se logró encontrar datos importantes con respecto a los protocolos de red atacados por los distintos tipos de malware.

En la Ilustración 6. Representa un gráfico de barras de los diferentes protocolos. Visualmente se identifica el TCP, como el protocolo más atacado y con bastante diferencia en comparación con los otros protocolos que le siguen como UDP y ICMP.

Ilustración 6 - Gráfica de Frecuencia - Ataques/Protocolos
Fuente: Autor



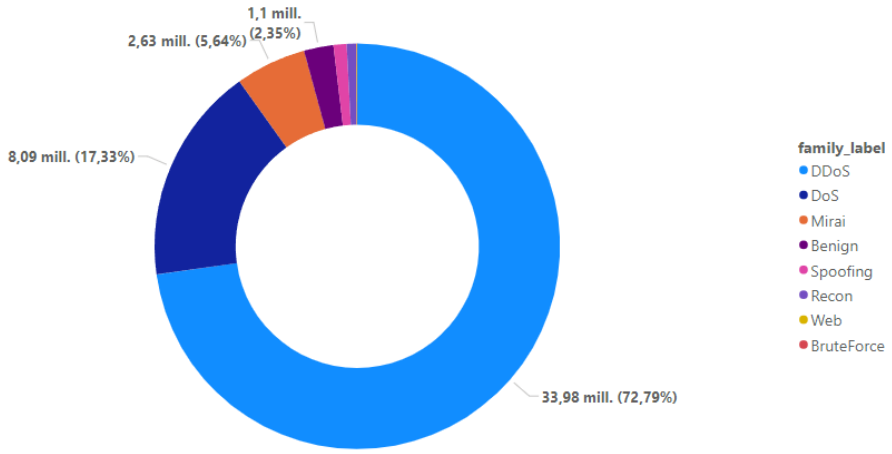
La siguiente Ilustración 7 representa una tabla visual donde se dimensiona con frecuencias y frecuencia porcentual de los protocolos más atacados según el conjunto de datos implementado en la realización del presente trabajo.

Ilustración 7 - Frecuencias y porcentajes de Ataques/Protocolo
Fuente: Autor

protocolo	Recuento de protocolo	%TG Recuento de protocolo
TCP	21964152	47,05%
UDP	9887606	21,18%
ICMP	7643600	16,37%
HTTPS	2572394	5,51%
	2355991	5,05%
HTTP	2251891	4,82%
DNS	6101	0,01%
ARP	3090	0,01%
SSH	1911	0,00%
IRC	7	0,00%
SMTP	3	0,00%
Telnet	1	0,00%
Total	**46686747**	**100,00%**

Por otro lado, la siguiente Ilustración muestra un gráfico de pastel que se representa en la Ilustración 8, identifica el porcentaje que corresponde a las familias atacantes con relación al conjunto de datos CICIOT2023.

Ilustración 8 - Gráfico de anillo - Ataques/Familia
Fuente: Autor



4.2.2. Discusión

En cuanto al análisis de los protocolos de seguridad más vulnerados en entornos de Internet de las Cosas, los resultados indican que el protocolo TCP es el más atacado representando el 47.05 %, seguido por UDP e ICMP con un 21.18 % y 16.37 %. Esta información es crucial para los esfuerzos de mitigación de ciberataques, ya que proporciona una dirección clara sobre dónde se deben concentrar los esfuerzos de seguridad.

Por otro lado, aunque el protocolo TCP fue identificado como el más atacado en este trabajo, es importante recordar que los ciberataques pueden variar en función de una serie de factores, incluyendo el tipo de dispositivo IoT, el entorno de red, y las tácticas y técnicas específicas utilizadas por los ciberdelincuentes. Además, mediante el uso de gráficos estadísticos en Power Bi se determinó que la familia de ataques DDoS es la más frecuente dentro del tráfico de la red conformada por dispositivos de IoT, esta información es bastante relevante y de alto impacto en cuanto a seguridad de redes se refiere, y de acuerdo con trabajos recientes como el de (Uddin et al., 2024), los ataques DDoS son una preocupación realmente importante entornos a dispositivos IoT, y sugiere la aplicación de algoritmos de aprendizaje automático como medio de prevención para este tipo de ataques.

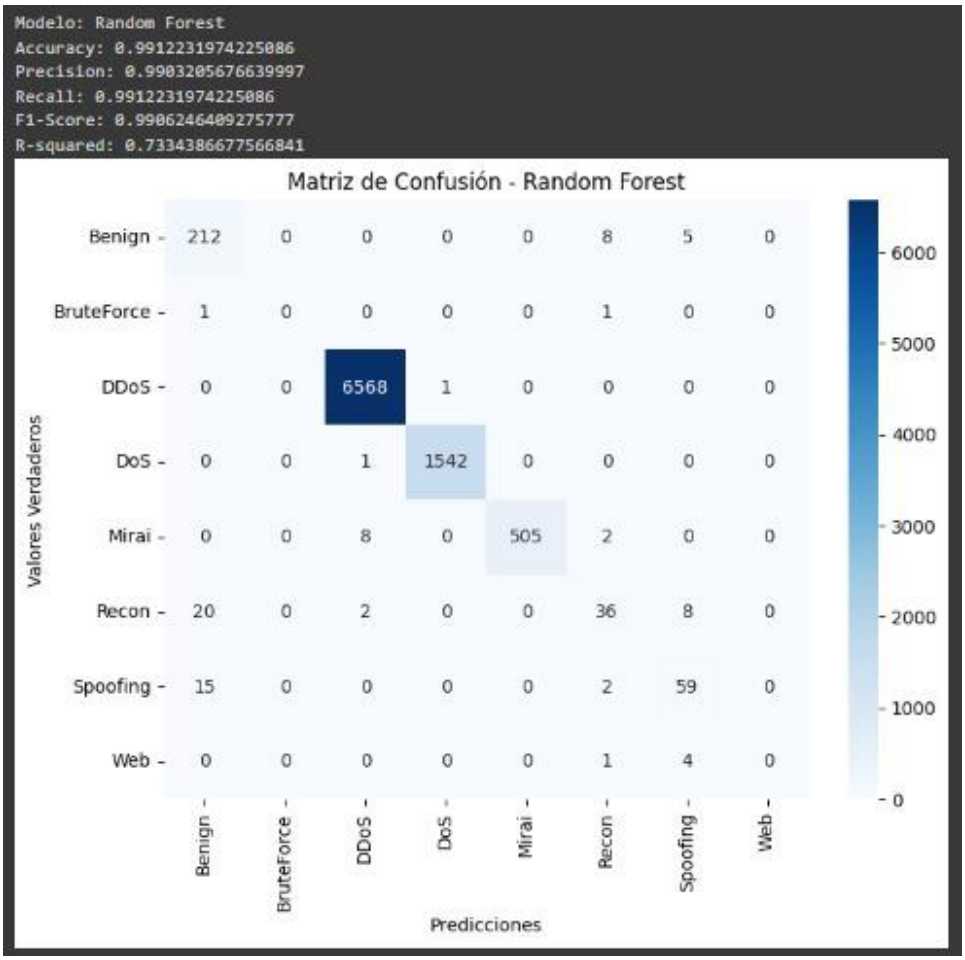
4.3. Selección de algoritmos para predicción de ciberataques en entornos de Internet de las Cosas

En esta sección se evalúa el rendimiento del proceso implementado en un ambiente controlado denominado “TEST”. Para lograr este objetivo, implementamos los siguientes algoritmos de aprendizaje supervisado como: Random Forest, Decision Tree,

SVM, Knn, Gradient Boosting y Naive Bayes. Los 6 algoritmos fueron ejecutados en la plataforma Google Colab, en Python.

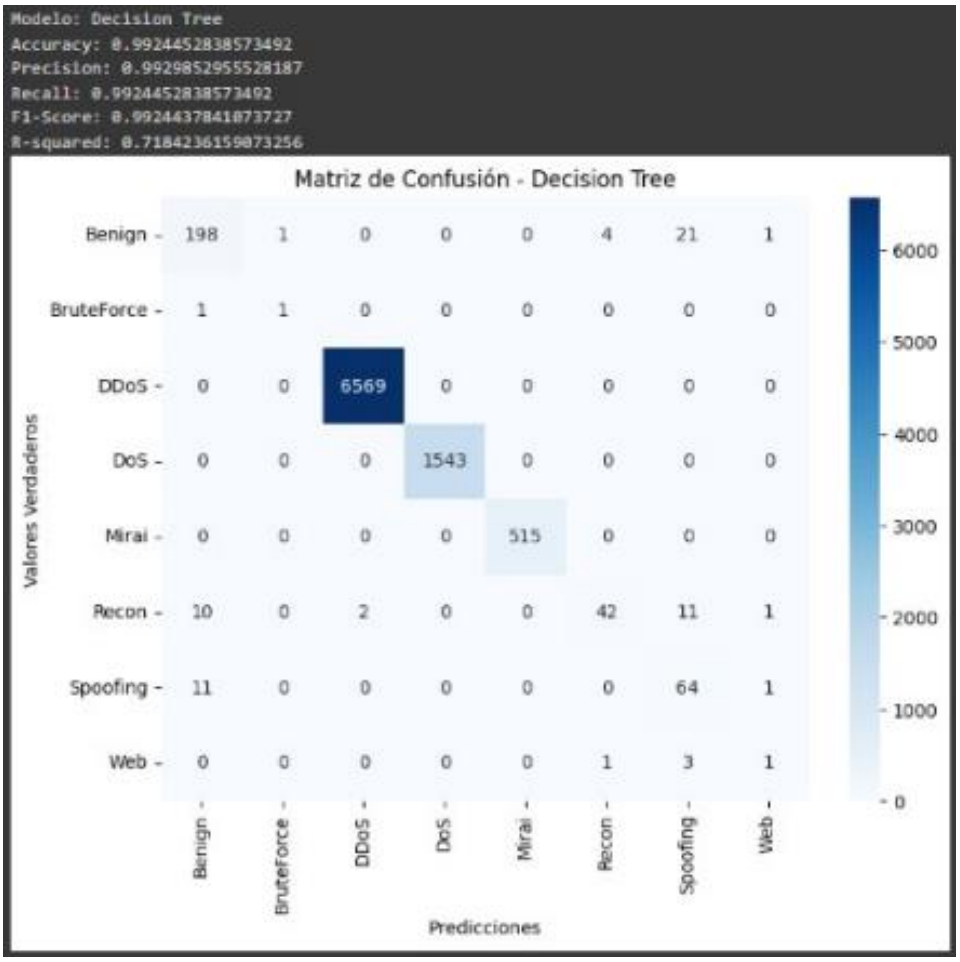
El modelo Random Forest, se obtuvo una precisión de 0.993367. La Ilustración 9 muestra la matriz de confusión donde se visualiza los aciertos y los falsos positivos.

Ilustración 9 - Matriz de confusión – Random Forest
Fuente: Autor



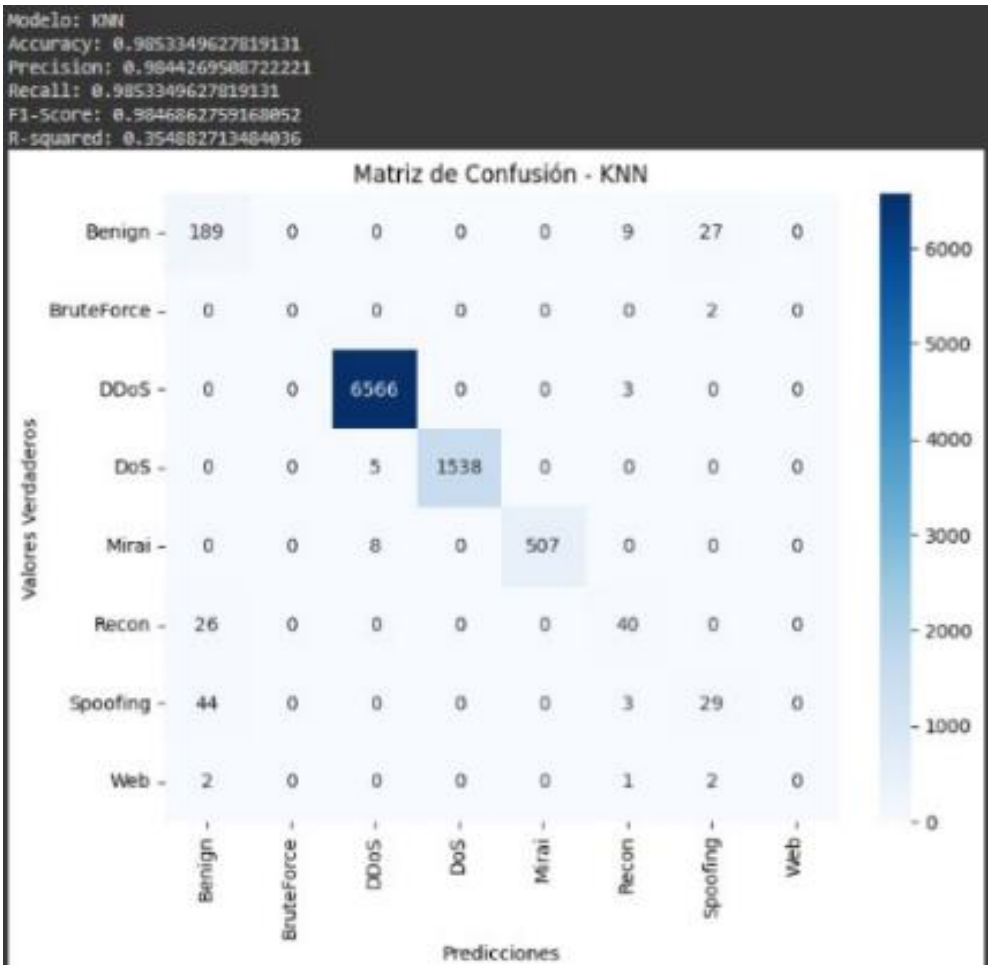
El algoritmo de Decision tree, se obtuvo una exactitud de 0.993646. La Ilustración 10 muestra la matriz de confusión donde se visualiza la clasificación de las familias de ataques.

Ilustración 10 - Matriz de confusión – Decision Tree
Fuente: Autor



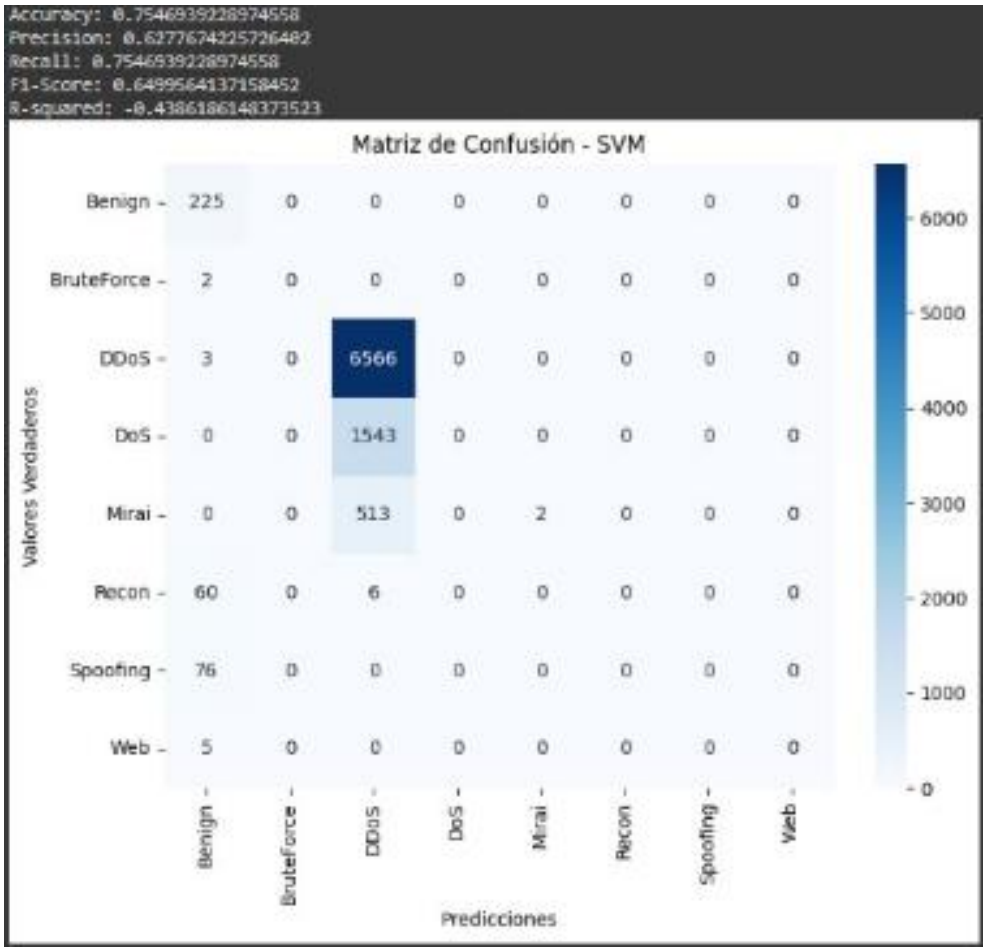
El algoritmo, Vecinos cercanos (KNN), se obtuvo una exactitud de 0.988004. Este algoritmo agrupó las instancias según su comportamiento etiquetándolos en clusters con alta similitud a las familias de ataques definidos en el conjunto de datos. La Ilustración 11 muestra la matriz de confusión donde se visualiza la clasificación de las familias de ataques.

Ilustración 11 - Matriz de confusión – KNN
Fuente: Autor



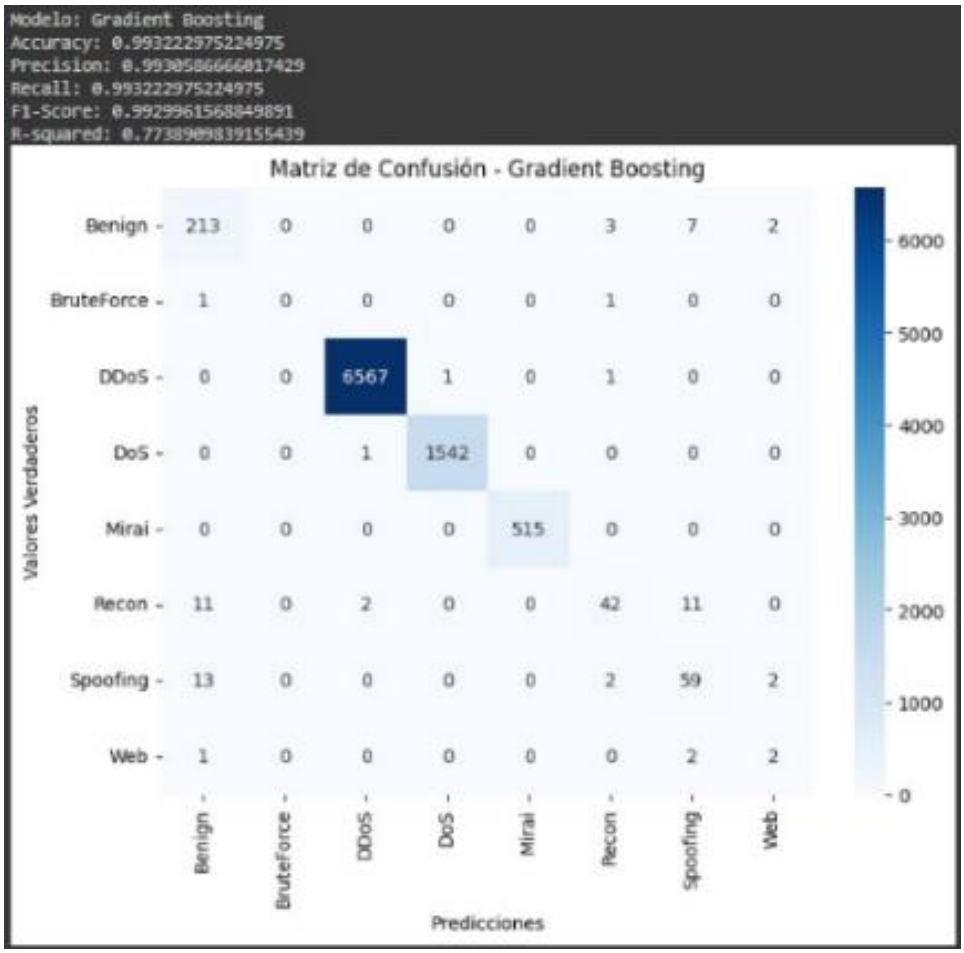
La Ilustración 12, representa la matriz de confusión del algoritmo Soporte vector máquina (SVM). La precisión del este modelo es de 0.6277. Se puede observar que existe una clasificación errónea entre las familias DDoS y Dos, lo que hace que sus métricas sean bajas.

Ilustración 12 - Matriz de confusión – SVM
Fuente: Autor



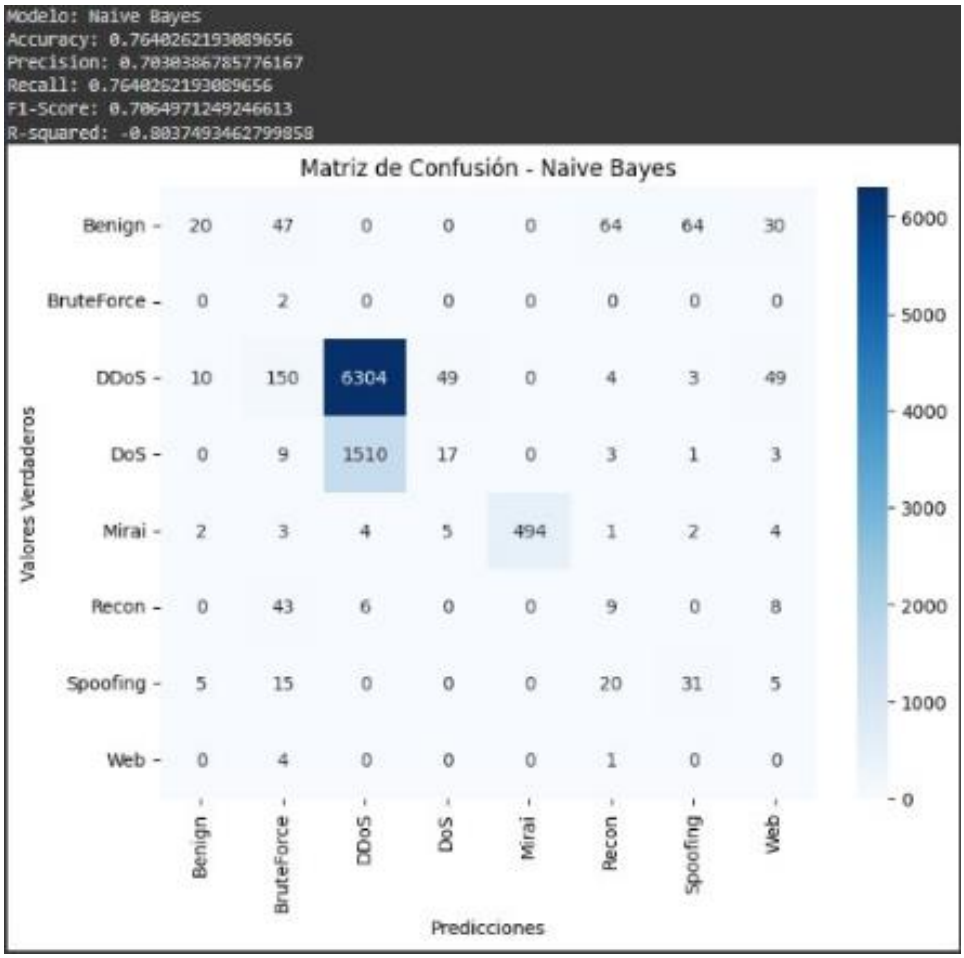
La siguiente Ilustración 13 detalla la matriz de confusión del algoritmo Gradient Boosting. Con una precisión de 0.993 es uno de los modelos que mejor se adaptó a los datos durante el entrenamiento.

Ilustración 13 - Matriz de confusión – Gradient Boosting
Fuente: Autor



La Ilustración 14 detalla la matriz de confusión del algoritmo probabilístico de Naive Bayes. Con una exactitud de 0.76, su clasificación errónea de las familias recae en los ataques DDoS, DoS y Mirai.

Ilustración 14 - Matriz de confusión – Naive Bayes
Fuente: Autor



A continuación, se presentan los resultados de los algoritmos utilizados para el desarrollo del presente proyecto de investigación. En la siguiente tabla 6 se observan los resultados obtenidos por cada uno de los algoritmos de predicción. Además, en la tabla 7 podemos observar el tiempo que se toma cada algoritmo en cada uno de sus resultados.

Tabla 6 - Resultados de los algoritmos de predicción
Fuente: Autor

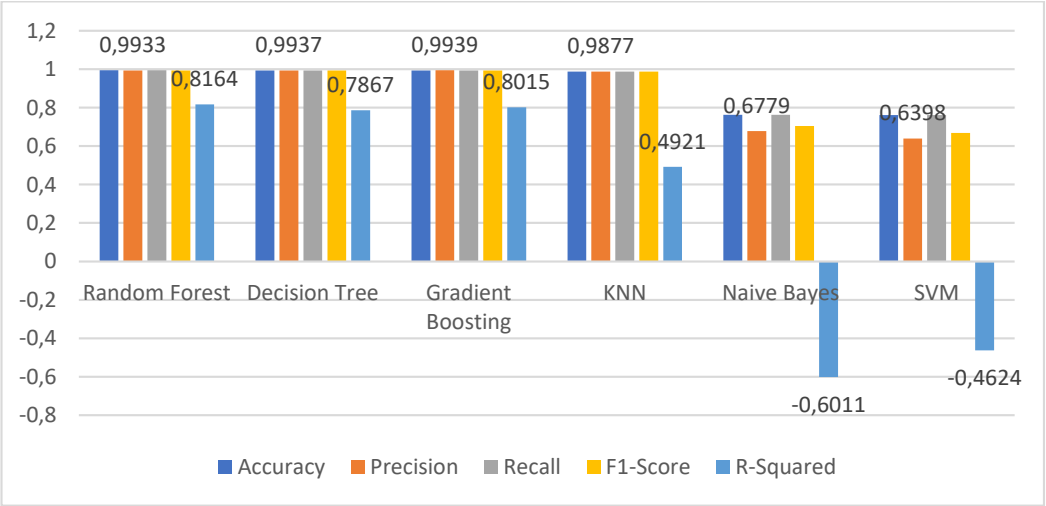
Model	Accuracy	Precision	Recall	F1-Score	R-Squared
Random Forest	0.9941	0.9933	0.9941	0.9936	0.8164
Decision Tree	0.9936	0.9937	0.9936	0.9936	0.7867
Gradient Boosting	0.9929	0.9939	0.9929	0.9932	0.8015
KNN	0.9880	0.9877	0.9880	0.9874	0.4921
Naive Bayes	0.7626	0.6779	0.7626	0.7045	-0.6011
SVM	0.7619	0.6398	0.7619	0.6678	-0.4624

Tabla 7 - Tiempo de ejecución de los algoritmos
Fuente: Autor

Random Forest	00:24:37
Decision Tree	00:34:08
Gradient Boosting	00:28:33
KNN	00:48:05
Naive Bayes	00:27:35
SVM	01:08:12

En la siguiente ilustración 15 podemos apreciar de mejor forma los resultados mediante un gráfico de barras en donde se destacan los resultados de la precisión y R cuadrado, se observa que Random Forest, Decision Tree y Grandient Boosting son los que tienen mejores resultados.

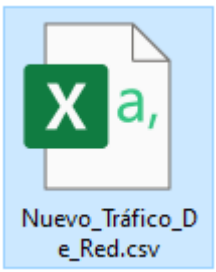
Ilustración 15 - Gráfico de barras con los resultados de los algoritmos
Fuente: Autor



4.3.1. Prueba del modelo predictivo

Una vez encontrado el algoritmo más adecuado para nuestro modelo, creamos una carpeta en donde se van a almacenar los conjuntos de datos que van a pasar a través del modelo predictivo.

Ilustración 16 - Carpeta que contiene los nuevos conjuntos de datos a predecir
Fuente: Autor



Luego en Python seleccionamos la ruta, donde se encuentra nuestro nuevo conjunto de datos a predecir, el cual debe estar en formato CSV.

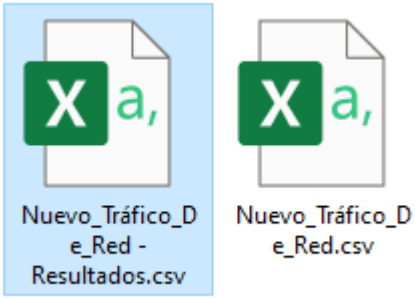
Ilustración 17 - Ubicación de los conjuntos de datos a predecir
Fuente: Autor

```
nueva_predict = pd.read_csv('D:\\CICIoT2023\\Prueba\\Nuevo_Tráfico_De_Red.csv'
                            , engine= 'python', index_col=0, sep=';')

nueva_predict
```

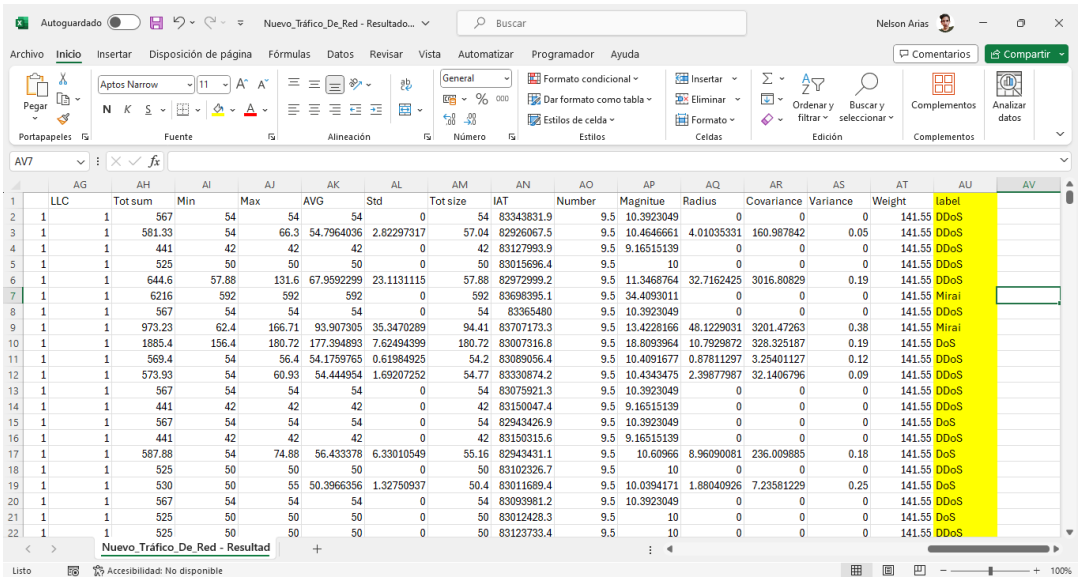
A continuación, una vez ajustados los parámetros necesarios para realizar la predicción con el modelo, ejecutamos y obtenemos un nuevo conjunto de datos con las etiquetas que poseen sus respectivas predicciones realizadas por nuestro modelo predictivo.

Ilustración 18 - Nuevo archivo CSV con las predicciones
Fuente: Autor



Por último, en la siguiente ilustración 18, podemos observar las predicciones realizadas por el modelo de manera exitosa.

Ilustración 19 - Resultados del modelo predictivo
Fuente: Autor



	LLC	Tot sum	Min	Max	AVG	Std	Tot size	IAT	Number	Magnitue	Radius	Covariance	Variance	Weight	label
2	1	567	54	54	54	0	54	83343831.9	9.5	10.3923049	0	0	0	141.55	DDoS
3	1	581.33	54	66.3	54.7964036	2.82297317	57.04	82926067.5	9.5	10.4646661	4.01035331	160.987842	0.05	141.55	DDoS
4	1	441	42	42	42	0	42	83127993.9	9.5	9.16515139	0	0	0	141.55	DDoS
5	1	525	50	50	50	0	50	83015696.4	9.5	10	0	0	0	141.55	DDoS
6	1	644.6	57.88	131.6	67.9592299	23.1131115	57.88	82972999.2	9.5	11.3468764	32.7162425	3016.80829	0.19	141.55	DDoS
7	1	6216	592	592	592	0	592	83698395.1	9.5	34.4093011	0	0	0	141.55	Mirai
8	1	567	54	54	54	0	54	83365480	9.5	10.3923049	0	0	0	141.55	DDoS
9	1	973.23	62.4	166.71	93.907305	35.3470289	94.41	83707173.3	9.5	13.4228166	48.1229031	3201.47263	0.38	141.55	Mirai
10	1	1885.4	156.4	180.72	177.394893	7.62494399	180.72	83007316.8	9.5	18.8093964	10.7929872	328.325187	0.19	141.55	DoS
11	1	569.4	54	56.4	54.1759765	0.61984925	54.2	83089056.4	9.5	10.4091677	0.87811297	3.25401127	0.12	141.55	DDoS
12	1	573.93	54	60.93	54.444954	1.69207252	54.77	83330874.2	9.5	10.4343475	2.39877987	32.1406796	0.09	141.55	DDoS
13	1	567	54	54	54	0	54	83075921.3	9.5	10.3923049	0	0	0	141.55	DDoS
14	1	441	42	42	42	0	42	83150047.4	9.5	9.16515139	0	0	0	141.55	DDoS
15	1	567	54	54	54	0	54	82943426.9	9.5	10.3923049	0	0	0	141.55	DoS
16	1	441	42	42	42	0	42	83150315.6	9.5	9.16515139	0	0	0	141.55	DDoS
17	1	587.88	54	74.88	56.433378	6.33010549	55.16	82943431.1	9.5	10.60966	8.96090081	236.009885	0.18	141.55	DoS
18	1	525	50	50	50	0	50	83102326.7	9.5	10	0	0	0	141.55	DDoS
19	1	530	50	55	50.3966356	1.32750937	50.4	83011689.4	9.5	10.0394171	1.88040926	7.23581229	0.25	141.55	DoS
20	1	567	54	54	54	0	54	83093981.2	9.5	10.3923049	0	0	0	141.55	DDoS
21	1	525	50	50	50	0	50	83012428.3	9.5	10	0	0	0	141.55	DoS
22	1	525	50	50	50	0	50	83123733.4	9.5	10	0	0	0	141.55	DDoS

4.3.2. Discusión

En relación con la selección del algoritmo más apropiado para predecir ciberataques en entornos del Internet de las Cosas, es importante destacar que los algoritmos de Random Forest, Decision Tree y Gradient Boosting muestran un alto rendimiento en todas las métricas evaluadas (precisión, recall, F1-Score). Esto indica que son capaces de predecir correctamente la mayoría de los ciberataques. Además, el hecho de que estos tres algoritmos posean un valor de R-cuadrado positivo sugiere que pueden explicar una gran proporción de la variabilidad en los datos. Sin embargo, un factor crucial a considerar es el tiempo de ejecución de los algoritmos. En este aspecto, Random Forest destaca por ser el algoritmo con mejor tiempo de ejecución en comparación con los demás.

Finalmente, podemos afirmar que Random Forest es el algoritmo idóneo para nuestro modelo predictivo. Un algoritmo que es más rápido y tiene la mejor precisión, es decir, la capacidad de hacer predicciones más acertadas, fue precisamente lo que buscaba conseguir en esta investigación. Además, en trabajos de investigación como el de (TÜRK, 2023), muestran que Random Forest tiene muy buenos resultados entorno a modelos de predicción multiclase.

Por otro lado, observando los resultados del algoritmo KNN también muestra un alto rendimiento en términos de precisión, recall y F1-Score, su R-cuadrado es significativamente más bajo que los de Decision Tree, Random Forest y Gradient Boosting. Esto señala que, aunque KNN es capaz de predecir correctamente muchos ciberataques, puede no ser tan eficaz para explicar la variabilidad en los datos. También tenemos a Naive Bayes, SVM y Logistic Regression, estos tres algoritmos muestran un rendimiento significativamente más bajo en todas las métricas en comparación con los

otros algoritmos. Además, todos tienen un R-cuadrado negativo, lo que indica que estos modelos no son capaces de explicar la variabilidad en los datos. Los resultados demuestran que estos algoritmos son inadecuados para conseguir un buen modelo y no se ajustan bien a la variabilidad de los datos.

Finalmente, aunque los resultados obtenidos son prometedores, es importante recordar que la predicción de ciberataques es un campo de investigación desafiante y en constante evolución. Los ciberataques son cada vez más sofisticados y cambiantes, y los modelos predictivos deben adaptarse en consecuencia. Por lo tanto, aunque los algoritmos Random Forest y Gradient Boosting mostraron un buen rendimiento en este estudio, es crucial que se tomen en cuenta y se apliquen este tipo de trabajos como medidas para ayudar a reforzar la seguridad frente a los constantes ataques de ciberdelincuentes.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

En el presente estudio, se analizó el conjunto de datos CICIOT2023, referente a los ciberataques a dispositivos IoT, con el objetivo de identificar patrones, protocolos más atacados y los tipos de ataques realizados. Además, se evaluaron diferentes algoritmos de clasificación, predicción y probabilísticos con el fin de obtener un modelo que explique el comportamiento de los datos estudiados.

La identificación de patrones en los datos facilitó una comprensión más detallada del conjunto de datos. Esto permitió organizar y minimizar la cantidad de atributos presentes en la variable objetivo, lo cual resultó en una mejora significativa del rendimiento del modelo.

Conforme a los datos analizados, se identificó que el protocolo más atacado es el TCP, representando el 47.05% del total de paquetes enviados. Le siguen el protocolo UDP e ICMP, con porcentajes del 21.18% y 16.37%, respectivamente. Además, los ataques pertenecientes a la familia DDoS son los que representan el mayor número de ataques en relación con el conjunto de datos estudiados, alcanzando el 72.79%. Mientras que los ataques por fuerza bruta constituyen solo el 0.03%, convirtiéndose en la familia con el menor número de ataques realizados.

En los resultados obtenidos de los algoritmos que han sido entrenado, se demuestra que Random Forest y Gradient Boosting sobresalen en términos de rendimiento para realizar predicciones precisas. Estos algoritmos exhiben una precisión excepcional y una puntuación de R cuadrado positivo muy bueno, lo que indica un ajuste sólido para el modelo a los datos. Además, al trabajar con un conjunto de datos de gran tamaño, notamos que estos dos algoritmos son notablemente más rápidos en generar resultados

en comparación con los demás algoritmos. Por lo tanto, Random Forest y Gradient Boosting se destacan no solo en precisión, sino también en los tiempos para generar resultados.

Las reglas de clasificación de algoritmos supervisados son las que dieron mejores resultados y permiten una mejor adaptación del modelo a los datos estudiados en el presente proyecto de investigación. Por otro lado, los algoritmos Naive Bayes, SVM y Logistic Regression no logaron ajustarse de manera correcta al conjunto de datos, como lo indica su baja precisión y el R cuadrado negativo.

5.2. RECOMENDACIONES

En este proyecto de investigación se trabajó con una gran cantidad de datos. Durante las pruebas, resulta bastante lento terminar de ejecutar un modelo. Por lo tanto, en estos casos, es recomendable migrar todo el proyecto a una nube, como por ejemplo Google Cloud, Amazon Web Services o Microsoft Azure. Esto podría ayudar a obtener los resultados de manera más rápida, además, la posibilidad de acceder de manera remota. Un punto importante para considerar son los costos asociados con los servicios en la nube. Por ello, se recomienda aplicarlo en casos de empresas u organizaciones que puedan cubrir los costos para mantener la infraestructura en la nube.

Dado que el protocolo TCP es el más atacado por los distintos tipos de ataques, se considera investigar más a fondo las vulnerabilidades específicas asociadas con este protocolo. Puede ser útil implementar medidas de seguridad específicas para proteger los dispositivos IoT que utilizan TCP. Además, a través de este estudio se demostró que los ataques tipo DDoS y DoS son los más frecuentes en entornos IoT. En base a esto, las empresas podrían implementar medidas contra este tipo de ataques en sus empresas u organizaciones.

Se podría desarrollar una aplicación web alojada en un servidor, que funcione como un servicio en donde los usuarios interactuarán con la página web para ingresar datos y ver las predicciones generadas desde cualquier lugar. Esto puede beneficiar múltiples empresas u organizaciones que requieran este tipo de servicios.

6. REFERENCIAS

Avast. (2023). *Avast*. Obtenido de https://www.avast.com/c-b-what-is-cybersecurity

Bharath Reddy, G. S. (12 de Agosto de 2022). Intrusion Detection System Using Computationally Efficient SVM based on K-Prototype Clustering. *IEEE*.

Brunswick, U. o. (2023). *Canadian Institute for Cybersecurity*. Recuperado el 12 de 2023, de https://www.unb.ca

Canadian Institute for Cybersecurity. (2023). *CIC IoT Dataset 2023.* Obtenido de https://www.unb.ca/cic/datasets/iotdataset-2023.html

Cisco. (2023). *¿Cuáles son los ciberataques más comunes?* Obtenido de https://www.cisco.com/c/es_mx/products/security/common-cyberattacks.html#~tipos-de-ciberataques

Consejo Nacional Electoral. (20 de Agosto de 2023). *Pulzo*. Recuperado el 15 de Septiembre de 2023, de https://www.pulzo.com/mundo/elecciones-ecuador-hoy-denuncian-ciberataques-sistema-votos-exterior-PP2978287

Deepai. (2023). *Deepai*. Obtenido de https://deepai.org/machine-learning-glossary-and-terms/supervised-learning

Diazgranados, H. (31 de Agosto de 2021). *Kaspersky.* Recuperado el 17 de Septiembre de 2023, de https://latam.kaspersky.com/blog/ciberataques-en-america-latina-crecen-un-24-durante-los-primeros-ocho-meses-de-2021/22718/

Domino. (2023). *Domino*. Obtenido de https://domino.ai/data-science-dictionary/model-evaluation

Express Analytics. (2023). *Express Analytics*. Obtenido de https://www.expressanalytics.com/what-is-predictive-modeling/

Fernández, R. (20 de Marzo de 2023). *statista*. Recuperado el 15 de Septiembre de 2023, de https://es.statista.com/temas/6976/el-internet-de-las-cosas-iot/#editorsPicks

Fernández, R. (28 de Marzo de 2023). *Statista.* Obtenido de https://es.statista.com/estadisticas/541451/penetracion-mundial-de-internet-por-region-del-mundo/

García Del Río, A., & López Contreras, I. (2018). IMPLEMENTACIÓN DE HERRAMIENTAS DE EXTRACCIÓN, TRANSFORMACIÓN Y CARGA DE DATOS ESTRUCTURADOS EN BIG DATA. *Recursos Electrónicos UACJ*.

Gohar Mumtaz, S. A. (27 de Febrero de 2023). Classification and Prediction of Significant Cyber Incidents (SCI) Using Data Mining and Machine Learning (DM-ML).

Google. (2023). *Google Cloud*. Obtenido de https://cloud.google.com/learn/artificial-intelligence-vs-machine-learning?hl=es

Horowitz, M. (2023). *Check Point.* Obtenido de https://resources.checkpoint.com/report/2023-check-point-cyber-security-report

Insight Software. (2022). *Insight Software*. Obtenido de https://insightsoftware.com/blog/when-and-why-to-use-heat-maps/#:~:text=By%20definition%2C%20Heat%20Maps%20are,data%20visualizations%20that%20matter%20most.

Institute for Cybersecurity. (2023). *Institute for Cybersecurity*. Obtenido de https://www.unb.ca/cic/about/index.html

International Business Machines. (2023). *What is internet of things?* Obtenido de https://www.ibm.com/topics/internet-of-things

Jingwen Wei, y. c. (Noviembre de 2022). Domain Adversarial Neural Network-Based Intrusion Detection System for In-Vehicle Network Variant Attacks. págs. 2547 - 2551.

Kasongo, S. M. (25 de Noviembre de 2020). *Performance Analysis of Intrusion Detection Systems Using a Feature Selection Method on the UNSW-NB15 Dataset.* Obtenido de https://journalofbigdata.springeropen.com/articles/10.1186/s40537-020-00379-6

Ley Orgánica del Sistema Nacional de Registro de Datos Públicos. (s.f.). *Ley Del Sistema Nacional De Registro De Datos Públicos*. Obtenido de https://www.registrospublicos.gob.ec/marco-legal-s-n-r-p/

Malathi C, I. N. (2023). Identification of cyber attacks using machine learning in smart IoT networks. págs. 2518-2523. Obtenido de https://www-sciencedirect-com.translate.goog/science/article/abs/pii/S2214785321047945?_x_tr_sl=auto&_x_tr_tl=es&_x_tr_hl=es

Microsoft. (2023). *Microsoft*. Obtenido de https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-are-databases

Ministro De Telecomunicaciones Y De La Sociedad De La Información. (17 de Abril de 2020). *Ministro De Telecomunicaciones Y De La Sociedad De La Información*. Obtenido de https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/04/Acuerdo-Poli%CC%81tica-Datos-Abiertos-17.04.20-v4-signed.pdf

Oracle Cloud Infrastructure. (2023). *OCI*. Obtenido de https://www.oracle.com/big-data/what-is-data-mining/

S. Shitharth, P. R. (2 de Mayo de 2022). An Innovative Perceptual Pigeon Galvanized Optimization (PPGO) Based Likelihood Naïve Bayes (LNB) Classification Approach for Network Intrusion Detection System. *IEEE*, págs. 46424 - 46441.

Statistical Analysis System. (2023). *SAS*. Obtenido de https://www.sas.com/es_mx/insights/big-data/what-is-big-data.html

Surjeet Dalal, U. K. (29 de Septiembre de 2023). Next-generation cyber attack prediction for IoT systems: leveraging multi-class SVM and optimized CHAID decision tree. pág. 137.

Tableau. (2023). Obtenido de https://www.tableau.com/learn/articles/data-visualization

Turk, F. (27 de Junio de 2023). *Análisis de sistemas de detección de intrusiones en conjuntos de datos UNSW-NB15 y NSL-KDD con algoritmos de aprendizaje automático.* Obtenido de https://doi.org/10.17798/bitlisfen.1240469

ANEXOS

Anexo 1. Certificado Urkund

PARA: Dr. Byron Oviedo Bayas
Decano de Posgrado
DE: Ing. Emilio Zhuma Mera, Ms.C
ASUNTO: Informe Proyecto de Investigación
FECHA: 5 de junio del 2024

Adjunto al presente sírvase encontrar el documento final del proyecto de investigación titulado: **MODELO PREDICTIVO DE CIBERATAQUES EN ENTORNOS DE INTERNET DE LAS COSAS**, elaborado por el **ING. NELSON GERMAN ARIAS CHEVEZ** posgradista de la **MAESTRÍA EN CIENCIA DE DATOS**. El proyecto de investigación fue elaborado bajo mi dirección según lo asignado en el contrato Nro. UTEQ-RUTEQ- 2023-4194-M de fecha 27 de noviembre de 2023, el mismo que cumple el informe de la herramienta COMPILATIO, el cual avala los niveles de originalidad, en un 98 % del trabajo investigativo.

Atentamente,

EMILIO RODRIGO ZHUMA MERA
Firmado digitalmente por EMILIO RODRIGO ZHUMA MERA

Ing. Emilio Zhuma Mera, Ms.C.
Director de Proyecto de Investigación

Anexo 2. Código de Python

```
#!/usr/bin/env python

# coding: utf-8

# In[2]:

import pandas as pd

import matplotlib.pyplot as plt

import seaborn as sns

import numpy as np

from sklearn.cluster import KMeans

from sklearn.preprocessing import StandardScaler

import warnings

warnings.filterwarnings('ignore')

# In[3]:

dataset = pd.read_csv('D:\\CICIoT2023\\TEST.csv',  sep=';')

dataset.head(5)

# In[4]:

df = dataset.loc[:, ['flow_duration', 'Header_Length', 'Protocol Type', 'Duration', 'Rate',

'Srate', 'Drate',
```

```
                'fin_flag_number', 'syn_flag_number', 'rst_flag_number',
'psh_flag_number', 'ack_flag_number',
                'ece_flag_number', 'cwr_flag_number', 'ack_count', 'syn_count', 'fin_count',
'urg_count', 'rst_count',
                'HTTP', 'HTTPS', 'DNS', 'Telnet', 'SMTP', 'SSH', 'IRC', 'TCP', 'UDP',
'DHCP', 'ARP', 'ICMP', 'IPv', 'LLC',
                'Tot sum', 'Min', 'Max', 'AVG', 'Std', 'Tot size', 'IAT', 'Number', 'Magnitue',
'Radius', 'Covariance',
                'Variance', 'Weight', 'label'
]]
df.head(10)



# In[5]:
from sklearn.preprocessing import StandardScaler, RobustScaler
features = df.drop('label', axis=1)
scaler = StandardScaler()
scaled_features = pd.DataFrame(scaler.fit_transform(features),
columns=features.columns)
df = pd.concat([scaled_features, df['label']], axis=1)
```

```
df.info()


# In[6]:

df.head(5)

# In[7]:

remap_labels = {
    'DDoS-RSTFINFlood': 'DDoS',
    'DDoS-PSHACK_Flood': 'DDoS',
    'DDoS-SYN_Flood': 'DDoS',
    'DDoS-UDP_Flood': 'DDoS',
    'DDoS-TCP_Flood': 'DDoS',
    'DDoS-ICMP_Flood': 'DDoS',
    'DDoS-SynonymousIP_Flood': 'DDoS',
    'DDoS-ACK_Fragmentation': 'DDoS',
    'DDoS-UDP_Fragmentation': 'DDoS',
    'DDoS-ICMP_Fragmentation': 'DDoS',
    'DDoS-SlowLoris': 'DDoS',
    'DDoS-HTTP_Flood': 'DDoS',
    'DoS-UDP_Flood': 'DoS',
```

'DoS-SYN_Flood': 'DoS',

'DoS-TCP_Flood': 'DoS',

'DoS-HTTP_Flood': 'DoS',

'Mirai-greeth_flood': 'Mirai',

'Mirai-greip_flood': 'Mirai',

'Mirai-udpplain': 'Mirai',

'Recon-PingSweep': 'Recon',

'Recon-OSScan': 'Recon',

'Recon-PortScan': 'Recon',

'VulnerabilityScan': 'Recon',

'Recon-HostDiscovery': 'Recon',

'DNS_Spoofing': 'Spoofing',

'MITM-ArpSpoofing': 'Spoofing',

'BenignTraffic': 'Benign',

'BrowserHijacking': 'Web',

'Backdoor_Malware': 'Web',

'XSS': 'Web',

'Uploading_Attack': 'Web',

'SqlInjection': 'Web',

```
    'CommandInjection': 'Web',
    'DictionaryBruteForce': 'BruteForce'
}
df['label'] = df['label'].apply(lambda x : remap_labels[x])
df['label'].value_counts()
# In[8]:
df.head(5)
# In[9]:
from sklearn.model_selection import train_test_split
from sklearn.ensemble import RandomForestClassifier
from sklearn.tree import DecisionTreeClassifier
from sklearn.metrics import accuracy_score, precision_score, recall_score, f1_score,
r2_score, confusion_matrix



# In[10]:
from sklearn.preprocessing import LabelEncoder
label_encoder = LabelEncoder()
df['label_encoded'] = label_encoder.fit_transform(df['label'])
```

```
# Se dividen los datos en conjuntos de entrenamiento y prueba

X_train, X_test, y_train, y_test = train_test_split(df.drop(['label', 'label_encoded'],
axis=1), df['label_encoded'], test_size=0.3, random_state=42)

# In[11]:

# Inicializan los modelos

models = {

    'Random Forest': RandomForestClassifier(),



}

# In[12]:

# Se crear un DataFrame para almacenar las métricas

results_df = pd.DataFrame(columns=['Model', 'Accuracy', 'Precision', 'Recall', 'F1-
Score', 'R-squared'])

# Iterar sobre los modelos

for model_name, model in models.items():

    # Entrenar el modelo

    model.fit(X_train, y_train)

    # Predecir con el conjunto de prueba

    y_pred = model.predict(X_test)
```

```
# Calcula las métricas

accuracy = accuracy_score(y_test, y_pred)

precision = precision_score(y_test, y_pred, average='weighted')

recall = recall_score(y_test, y_pred, average='weighted')

f1 = f1_score(y_test, y_pred, average='weighted')

r2 = r2_score(y_test, y_pred)



# Mostrar métricas

print(f"\nModelo: {model_name}")

print(f"Accuracy: {accuracy}")

print(f"Precision: {precision}")

print(f"Recall: {recall}")

print(f"F1-Score: {f1}")

print(f"R-squared: {r2}")

# Almacenar métricas en el DataFrame

results_df = results_df.append({

    'Model': model_name,

    'Accuracy': accuracy,

    'Precision': precision,
```

```
        'Recall': recall,
        'F1-Score': f1,
        'R-squared': r2
    }, ignore_index=True)
    # Mostrar matriz de confusión con seaborn
    label_encoder = LabelEncoder()
    label_encoder.fit(df['label'])
    conf_matrix = confusion_matrix(y_test, y_pred)
    conf_matrix_df = pd.DataFrame(conf_matrix, index=label_encoder.classes_,
columns=label_encoder.classes_)
    plt.figure(figsize=(8, 6))
    sns.heatmap(conf_matrix_df, annot=True, fmt='d', cmap='Blues')
    plt.title(f"Matriz de Confusión - {model_name}")
    plt.xlabel("Predicciones")
    plt.ylabel("Valores Verdaderos")
    plt.show()



# In[13]:
```

```
# Mostrar DataFrame con métricas de todos los modelos

print("\nComparación de Métricas:")

print(results_df)

# # Guardar el Modelo Predictivo

# In[1]:

modelo_predict = open('Modelo Random Forest.sav', 'wb')

# In[14]:

from pickle import dump

dump(model, modelo_predict)

# In[20]:

nueva_predict = pd.read_csv('D:\\CICIoT2023\\Prueba\\Nuevo_Tráfico_De_Red.csv'

                            , engine= 'python', index_col=0, sep=';')

nueva_predict

# In[ ]:

from pickle import load

modelo_cargardo = load(open('Modelo Random Forest.sav', 'wb'))
```