**DETECCIÓN DE ATAQUES DDOS EN REDES IOT UTILIZANDO MODELO DE DEEP LEARNING BASADO EN EL**

**PROTOCOLO DE RED NETFLOW**



Autor

**JOHAN ANDRÉS HERRERA REYES**

**DANIEL EDUARDO CABIATIVA FELACIO**

**UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS**

**Facultad Tecnológica**

**Ingeniería en Telecomunicaciones**

Bogotá D.C. Septiembre, 2023

**DETECCIÓN DE ATAQUES DDOS EN REDES IOT UTILIZANDO MODELO DE DEEP LEARNING BASADO EN EL**

**PROTOCOLO DE RED NETFLOW**



Autor

**JOHAN ANDRÉS HERRERA REYES 20212373001**

**johaherrerar@udistrital.edu.co**

**DANIEL EDUARDO CABIATIVA FELACIO 20202373014**

**decabiativaf@udistrital.edu.co**

Modalidad

**Monografía**

**Presentado para optar al título de: Ingeniero en Telecomunicaciones**

**Director:**

**Ing. Henry Alberto Hernández Martínez, MSc.**

**UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS**

**Facultad Tecnológica**

**Ingeniería en Telecomunicaciones**

Bogotá D.C. Septiembre, 2023

Dedicatoria

*A Dios, por iluminar nuestro camino y darnos fortaleza. A nuestros padres y compañeros, por su inquebrantable apoyo y enseñanzas. Y a Henry Alberto Hernández, nuestro director de proyecto cuya dirección meticulosa y experta fue esencial para la culminación de este proyecto. A todos, nuestra profunda gratitud.*

Índice

[Dedicatoria 3](#_Toc150408529)

[Índice 4](#_Toc150408530)

[Índice de Figuras 6](#_Toc150408531)

[Índice de Tablas 7](#_Toc150408532)

[Índice de Anexos 8](#_Toc150408533)

[Glosario 9](#_Toc150408534)

[Lista de Abreviaturas y Siglas 10](#_Toc150408535)

[Resumen 11](#_Toc150408536)

[1. Introducción 1](#_Toc150408537)

[2. Planteamiento del problema 2](#_Toc150408538)

[3. Justificación 3](#_Toc150408539)

[4. Objetivos 4](#_Toc150408540)

[4.1. Objetivo General 4](#_Toc150408541)

[4.2. Objetivos específicos 4](#_Toc150408542)

[5. Marco de referencia 5](#_Toc150408543)

[5.1. Antecedentes 5](#_Toc150408544)

[Detección de amenazas en Redes IoT empleando modelo híbrido de Machine Learning y Deep Learning [3]. 5](#_Toc150408545)

[Diseño De Un Modelo De Detección De Intrusos En Entornos Iot Usando Inteligencia Artificial [10]. 5](#_Toc150408546)

[Modelo De Detección De Ataques DDoS (Distributed Denial Of Services), Con Base En El Clasificador Decision Tree [11]. 5](#_Toc150408547)

[Las amenazas de seguridad a las que se enfrenta IoT y las soluciones en desarrollo [12]. 6](#_Toc150408548)

[Mecanismos de seguridad en el internet de las cosas [13]. 6](#_Toc150408549)

[Un método para la identificación y prevención temprana de incidentes de ciberseguridad en dispositivos del Internet de las Cosas [14]. 6](#_Toc150408550)

[Defensa contra intrusos en redes de dispositivos IoT usando técnicas de Blockchain y Machine Learning [15]. 6](#_Toc150408551)

[NetFlow Datasets for Machine Learning-Based Network Intrusion Detection Systems [5]. 7](#_Toc150408552)

[Towards a Standard Feature Set for Network Intrusion Detection System Datasets [9]. 7](#_Toc150408553)

[Medición de desempeño de sistema de monitoreo de redes con protocolo Netflow en modelo Big Data [16] 7](#_Toc150408554)

[Evaluación de modelos de machine learning para sistemas de detección de intrusos en Redes IoT [17] 8](#_Toc150408555)

[Implementación de análisis de tráfico y de flujos de red con tecnologías netflow y sflow en equipos de red de la UNAM utilizando software libre [18] 8](#_Toc150408556)

[Sistema preventivo contra ataques de Denegación de servicio web utilizando Deep Learning [19] 8](#_Toc150408557)

[The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 dataset [20] 8](#_Toc150408558)

[Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review [6] 9](#_Toc150408559)

[5.2. Marco teórico 9](#_Toc150408560)

[Internet de las cosas (IOT) 9](#_Toc150408561)

[Ataques de denegación de servicio DOS Y DDOS 10](#_Toc150408562)

[Machine learning y Deep learning 11](#_Toc150408563)

[Modelos de Deep Learning 13](#_Toc150408564)

[Algoritmos no supervisados en Deep Learning: 14](#_Toc150408565)

[Sistemas de Detección de intrusos con Machine learning y Deep learning 14](#_Toc150408566)

[Datasets 15](#_Toc150408567)

[Métricas para evaluar capacidad 15](#_Toc150408568)

[Análisis de tráfico 15](#_Toc150408569)

[Cisco Net Flow 16](#_Toc150408570)

[Herramientas de para machine learning y Deep learning 16](#_Toc150408571)

[6. Marco Legal 17](#_Toc150408572)

[7. Metodología 18](#_Toc150408573)

[Herramientas Y Plataformas De Deep Learning Apropiadas Para El Desarrollo 19](#_Toc150408574)

[Tensor Flow 19](#_Toc150408575)

[Keras 19](#_Toc150408576)

[Scikit-learn 20](#_Toc150408577)

[NF-UQ-NIDS-v2 20](#_Toc150408578)

[7.1. Preprocesamiento Y Acondicionamiento Conjunto De Datos Para Determinar Las Características De Un Ataque DDoS En Una Red IOT Utilizando El Dataset NF-UQ-NIDS. 21](#_Toc150408579)

[ANALISIS EXPLORATORIO DE LOS DATOS 22](#_Toc150408580)

[CARGA Y REDUCCION DATASET 22](#_Toc150408581)

[LIMPIEZA DE DATOS 25](#_Toc150408582)

[VALORES ATIPICOS(OUTLIERS) 27](#_Toc150408583)

[MUESTREO ESTRATIFICADO 28](#_Toc150408584)

[SELECCIÓN DE CARACTERISTICAS 29](#_Toc150408585)

[GRUPOS DE CARACTERISTICAS 29](#_Toc150408586)

[CLASIFICACION Y CODIFICACION VARIABLES CATEGORICAS Y NUMERICAS 30](#_Toc150408587)

[Categóricas: 31](#_Toc150408588)

[Numéricas: 31](#_Toc150408589)

[INSPECCION VISUAL 34](#_Toc150408590)

[Características Categóricas: 34](#_Toc150408591)

[Características Numéricas: 34](#_Toc150408592)

[CORRELACION DE PEARSON 34](#_Toc150408593)

[INFORMACION MUTUA 35](#_Toc150408594)

[ELIMINACIÓN DE CARACTERÍSTICAS RECURSIVA (RFE) 37](#_Toc150408595)

[NORMALIZACIÓN 37](#_Toc150408596)

[7.2. Implementación De Un Algoritmo De Aprendizaje Supervisado Basado En Una Red Neuronal Para Modelar El Conjunto De Datos. 37](#_Toc150408597)

[7.3. Análisis Estadístico De Los Resultados Obtenidos Utilizando El Modelo Y Comparación De Su Desempeño Frente A Otra Técnica Reportada En El Estado Del Arte. 37](#_Toc150408598)

[8. Resultados 37](#_Toc150408599)

[9. Conclusiones y Recomendaciones 39](#_Toc150408600)

[10. Referencias 40](#_Toc150408601)

[11. Anexos 41](#_Toc150408602)

Índice de Figuras

Índice de Tablas

Índice de Anexos

Glosario

|  |  |
| --- | --- |
| **Concepto** | **Explicación breve y detallada del concepto** |
| DDoS (Distributed Denial of Service) | Es un ataque informático en el cual se utiliza una red de computadoras comprometidas para inundar un sistema con tráfico malicioso, lo que ocasiona indisponibilidad en el servicio. |
| IoT (Internet of things) | Se refiere a la interconexión de dispositivos físicos por medio de internet, lo cual les permite obtener y compartir datos del mundo real. |
| Netflow | Protocolo de red desarrollado por Cisco que se utiliza para recopilar información sobre el tráfico de red y facilitar la monitorización y el análisis del mismo |
| Deep learning | Es una rama del aprendizaje automático (machine learning) que involucra redes neuronales profundas para resolver tareas complejas de procesamiento de datos. |
| Modelo de detección | Es un conjunto de algoritmos y técnicas utilizadas para identificar patrones de comportamiento malicioso o anormal en una red. |
| Tensor | Estructura de datos multidimensional que se utiliza en el aprendizaje automático profundo para representar información como imágenes. |
| Aprendizaje profundo | Rama de la inteligencia artificial que utiliza redes neuronales profundas para aprender y realizar cierto tipo de tareas a partir de datos, pudiendo así simular el procesamiento de un humano. |
|  |  |

Lista de Abreviaturas y Siglas

|  |  |
| --- | --- |
| **Sigla/Abreviatura** | **Significado** |
| IoT | Internet of Things |
| DoS | Denial of Service |
| DDoS | Distributed Denial of Service |
| DL | Deep learning |
| Netflow | Netflow network protocol |
| IP | Internet Protocol |
| ML | Machine Learning |
| TCP | Transmission Control Protocol |
| UDP | User Datagram Protocol |
| AI | Artificial Intelligence |
| IDS | Intrusion Detection System |
| IPS | Intrusion Prevention System |
| NIDS | Network Intrusion Detection System |
| NN | Neural Networks |
| P2P | Peer to Peer |
| PCA | Principal Component Analysis |
| EDA | Exploratory Data Analysis |

Resumen

Los ataques cibernéticos han experimentado un aumento alarmante en la región de América Latina y el Caribe sufriendo 137 mil millones intentos de ciberataques entre enero del 2022 y junio del mismo año, lo que representa un incremento del 50% en comparación con el mismo período del año anterior, que registró 91 mil millones de intentos [1]. Además de este aumento en la frecuencia, la sofisticación de estos ataques continúa en aumento, ya que los ciberatacantes permanecen a la vanguardia y desarrollan técnicas cada vez más elaboradas, incluyendo el uso de inteligencia artificial [2]. Esta creciente complejidad plantea la posibilidad de que el volumen y la sofisticación de los ciberataques superen la capacidad de detección humana en un futuro cercano.

En este contexto, la inteligencia artificial (IA) emerge como un multiplicador de fuerza esencial. No solo permite a los equipos de seguridad responder de manera más rápida que los atacantes cibernéticos, sino que también brinda la capacidad de anticipar sus movimientos. En respuesta a este desafío, este proyecto propone diseñar e implementar un modelo de Deep Learning para la detección y prevención de ataques DDoS en redes IoT. Este enfoque se basa en el análisis de conjuntos de datos estandarizados que capturan características cruciales mediante el protocolo Netflow.

Es importante destacar que la estandarización de características a partir de cuatro conjuntos de datos de referencia en el campo de la ciberseguridad de IoT facilita la medición del rendimiento del modelo entrenado en un conjunto de datos específico y su aplicabilidad en entornos reales [3]. Este enfoque contribuirá a fortalecer la seguridad en las redes IoT, en un momento en que la ciberseguridad se ha convertido en una prioridad crítica.

*Palabras clave: Ciberataque, Aprendizaje profundo, Ciberseguridad, Redes Neuronales, Estandarización, Internet de las Cosas.*

1. Introducción

La digitalización fomenta en la vida cotidiana y de las industrias un aumento exponencial en el tráfico de redes. El informe de Deloitte 2022 destaca este fenómeno, revelando que después de la pandemia, el espacio digital está experimentando un crecimiento sin precedentes. Este aumento ha dado lugar a un panorama donde una variedad de servicios, desde transacciones hasta soluciones en la nube para infraestructuras comerciales y el almacenamiento de información crítica, exigen un nivel eficiente y robusto de seguridad [2]. Además, el despliegue de las redes 5G ha contribuido al incremento de dispositivos conectados a internet en constante expansión, lo que conocemos como el Internet de las cosas (IoT). Según las proyecciones de Statista, se espera que para 2030 haya más de 29.000 millones de dispositivos IoT en todo el mundo, en comparación con los 19.000 millones proyectados para 2025 [3].

Este aumento en la interconexión digital ha generado la necesidad de garantizar la seguridad de las redes, ya que los ciberatacantes continúan evolucionando y desarrollando métodos cada vez más sofisticados para vulnerar sistemas. Entre estas amenazas, los ataques de Denegación de Servicio Distribuido (DDoS) se han convertido en uno de los más comunes y desafiantes de detectar. Su variabilidad y las características cambiantes del tráfico lo convierten en un adversario formidable [4].

Esta creciente amenaza es abordada desde el punto de vista del aprendizaje automático (machine learning), y más específicamente en el Deep Learning (DL). Esta técnica ha demostrado ser una herramienta eficaz y precisa en la detección y protección de redes contra ciberataques [5]. Sin embargo, para que estos modelos de DL sean eficientes y versátiles, es esencial estandarizar la captura de características en los conjuntos de datos de entrenamiento, lo que permitirá evaluarlos en diferentes contextos y facilitará su implementación en diversos escenarios.

En este contexto, el presente trabajo se propone diseñar, implementar y evaluar un modelo de Deep Learning que detecta y previene ataques DDoS en redes IoT. Este modelo utilizará un conjunto de datos basado en el protocolo de red Netflow, que registra flujos de red para detectar comportamientos anómalos y actividades maliciosas, como accesos no autorizados, intrusiones y otras amenazas a la seguridad de la información.

1. Planteamiento del problema

Las redes IoT están experimentando un crecimiento exponencial, impulsado por la proliferación de dispositivos de bajo costo que se conectan a Internet, como cámaras, grabadoras de video y electrodomésticos. Este aumento en la escala y complejidad de las redes IoT ha llevado a un incremento significativo en los ataques cibernéticos, cuya magnitud a menudo supera la capacidad de detección humana [1]. Los dispositivos IoT, en muchos casos, carecen de medidas de seguridad adecuadas, presentando una variedad de vulnerabilidades, como contraseñas débiles, falta de actualizaciones, servicios de red no seguros y componentes obsoletos, lo que da lugar a amenazas como la suplantación de identidad y la manipulación de datos [6].

Entre las tácticas de ataque más utilizadas se encuentran las botnets, que facilitan los ataques distribuidos de denegación de servicio (DDoS) para sobrecargar el tráfico de acceso y tomar el control de los dispositivos [4]. Esta problemática se agrava debido a la creciente cantidad de dispositivos IoT conectados a la red sin suficiente seguridad [7]. Los ataques DDoS se han mantenido en el centro de atención, siendo uno de los principales tipos de ciberataques entre 2013 y 2020, según una revisión de seguridad en IoT realizada en 2021 [6]. Además, son conocidos los ataques a servicios y empresas de renombre, como Amazon Web Services, GitHub, CNN y muchas otras [8].

El Deep Learning, ha demostrado ser eficaz para la detección y protección de estas redes contra ciberataques, su implementación en entornos reales presenta desafíos significativos [5]. La IA depende en gran medida de la disponibilidad de datos de red, que a menudo son difíciles de obtener debido a preocupaciones de seguridad y privacidad. Por lo tanto, se recurre al desarrollo de bancos de pruebas para la captura de datos que conformen los datasets para el entrenamiento de modelos de IA. Sin embargo, la falta de estandarización en la captura de características en estos datasets da como resultado modelos diseñados para entornos de prueba específicos, lo que limita su aplicabilidad en diferentes situaciones. Además, las técnicas de extracción, recopilación y almacenamiento de datos utilizadas en los datasets existentes suelen ser complejas y poco adecuadas para redes reales con alto tráfico. Se requiere, por tanto, una metodología más sencilla y eficaz para capturar características de tráfico de red y aplicar el aprendizaje profundo de manera efectiva [9].

1. Justificación

La seguridad en las redes IoT es un tema crítico que requiere una solución efectiva y escalable. A medida que la cantidad de dispositivos IoT aumenta, también lo hacen las vulnerabilidades y los ataques cibernéticos, lo que puede tener consecuencias graves en términos de privacidad, seguridad y economía.

La detección y prevención de ataques DDoS es particularmente difícil debido a la gran cantidad de dispositivos IoT que se conectan a la red con poca o ninguna seguridad. La aplicación de técnicas de Inteligencia Artificial para crear IDS (Sistemas de Detección de Intrusiones) ha demostrado ser una solución prometedora, pero aún existen desafíos importantes que deben superarse para implementarla de manera efectiva en entornos reales. Por lo tanto, investigar formas de mejorar la precisión y escalabilidad de los IDS basados en IA para redes IoT puede tener un impacto significativo en la seguridad y confiabilidad de estas redes, y en última instancia, en la protección de la privacidad y seguridad de los usuarios [6].

En la realización de este proyecto se aplicarán los conocimientos de redes, específicamente en cuanto a redes de paquetes e ingeniería de tráfico. Se utilizarán las herramientas de desarrollo de software y programación adquiridas, entre otras, utilizando el lenguaje de programación Python, y se aplicarán las habilidades para el modelamiento matemático adquiridas durante la carrera, además de los conocimientos sobre seguridad informática en cuanto a tipos de ataques. Con esto se busca contribuir a la investigación de la universidad en el campo de la Inteligencia Artificial aplicada a redes de datos.

1. Objetivos

## Objetivo General

Proponer un algoritmo de detección de ataques DDoS basado en Deep Learning utilizando

redes neuronales para redes IoT a partir de conjuntos de datos NF-UQ-NIDS basado en el

protocolo de red Netflow.

## Objetivos específicos

* Realizar un preprocesamiento y acondicionamiento de la información contenida en el conjunto de datos para determinar las características de un ataque DDoS en una red IOT utilizando el dataset NF-UQ-NIDS.
* Implementar un algoritmo de aprendizaje supervisado basado en una red neuronal para modelar el conjunto de datos.
* Realizar un análisis estadístico de los resultados obtenidos utilizando el modelo y comparar su desempeño frente a otra técnica reportada en el estado del arte.

# Marco de referencia

Párrafo de introducción para conocer el contenido del capitulo

## Antecedentes

La contribución de esos trabajos al de ustedes

#### Detección de amenazas en Redes IoT empleando modelo híbrido de Machine Learning y Deep Learning [3]: Se realizó la construcción del modelo híbrido es decir utilizando algoritmos de Machine Learning y Deep Learning que posean métricas de desempeño favorables para la clasificación correcta de los ataques DoS, evaluando una serie de algoritmos con base en las métricas de Exactitud, Precisión y Sensibilidad se eligieron los algoritmos Random Forest y la Red Neuronal Convolucional para crear el sistema de detección de amenazas en redes IoT.

#### Diseño De Un Modelo De Detección De Intrusos En Entornos Iot Usando Inteligencia Artificial [10].

En este trabajo se planteó el diseño de un modelo capaz de detectar intrusiones en entornos de red IoT mediante el uso de aprendizaje automático o aprendizaje profundo y lenguaje de programación de fuente abierta como Python o matlab con el fin de contribuir a la solución de actuales problemas de seguridad en las redes emergentes IoT.

En este caso se diseñó un Sistemas De Detección De Intrusiones Basados En Red (Nids) estos sistemas Monitorean el tráfico en la red para detectar intrusiones y pueden trabajar de forma secuencial o paralela detectando datos anómalos, inapropiados u otros que puedan considerarse no autorizados y dañinos en una red. Para el diseño de tal sistema se utilizó un conjunto de datos del tráfico real de una cámara de seguridad auténticamente infectada por Mirai y BASHLITE el cual se compone de 11 subconjuntos de datos y se realizó el análisis de estos datos mediante libreria de python 3.7 y probando varios algoritmos de machine learning: Logistic Regression,K-Nearest-Neighbor. Random Forest, Support Vector Machine, Gradient Boosting Classifiers.

#### Modelo De Detección De Ataques DDoS (Distributed Denial Of Services), Con Base En El Clasificador Decision Tree [11].

En este proyecto se desarrolló un modelo efectivo de detección de intrusos mediante la técnica de Machine Learning de clasificación supervisada Decisión Tree (Árbol de decisiones), comparándola a su vez con otras técnicas de aprendizaje supervisado (Random Forest, Logistic Regression, K Nearest Neighbor Algorithm, Support Vector Machines SVM) con el fin de identificar patrones anormales en las conexiones a una red, tomando como referencia un dataset de datos llamado CIC-IDS-2017, que fue elegido por tener un tráfico de red completo y actualizado acorde a la tendencia de navegación de un usuario común, usando protocolos como HTTP, HTTPS, FTP, SSH y email. En este trabajo se centraron principalmente en ataques de tipo DDoS (ataque distribuido de negación de servicio).

#### Las amenazas de seguridad a las que se enfrenta IoT y las soluciones en desarrollo [12].

En este este artículo se realiza una descripción de los principales problemas de seguridad que afronta IoT, detallando cómo afectan estos problemas al usuario final también algunas de las soluciones que están siendo utilizadas para solventar estos problemas de seguridad, entre otras soluciones basadas en Blockchain, Fog computing, Machine learning, y edge computing.

#### Mecanismos de seguridad en el internet de las cosas [13].

En este artículo se realizó un análisis de algunos métodos de seguridad que se emplean en el internet de las cosas, teniendo en cuenta sus características, funcionamiento, beneficios y esquemas de vanguardia, así como las buenas prácticas de seguridad, generando estrategias de control y protección en tecnologías de hardware y software. Se presentan características y funcionalidades de los mecanismos de seguridad de IoT sirviendo para analizar e identificar los problemas de seguridad en los dispositivos conectados a internet.

#### Un método para la identificación y prevención temprana de incidentes de ciberseguridad en dispositivos del Internet de las Cosas [14].

En este trabajo se propuso un método basado en la unión de redes neuronales convolucionales y redes neuronales recurrentes para la detección y clasificación de ataques

de denegación de servicios en entornos IoT. Para este método se transforman los flujos de datos a un formato de imágenes de tres canales. Para realizar este trabajo el autor exploró y evaluar distintos conjuntos de datos con datos reales o simulados de un ataque de denegación de servicios en una red IoT con el fin de consolidar el más óptimo para implementar el modelo de aprendizaje profundo, posteriormente Implementó los modelos de red neuronal seleccionadas durante el al conjunto de datos e hizo una revisión de la literatura para encontrar trabajos donde se hayan abordado problemas similares que den solución a la detección de ataques DoS en IoT y hayan utilizado el conjunto Bot IoT, para realizar la comparación y validación de los resultados generados por el modelo entrenado

#### Defensa contra intrusos en redes de dispositivos IoT usando técnicas de Blockchain y Machine Learning [15].

Esta tesis describe cómo las redes de IoT se han integrado en la infraestructura industrial y cómo esto puede presentar riesgos de seguridad para las compañías. Para contrarrestar este riesgo, se utilizaron algoritmos de blockchain y técnicas de machine learning para identificar y bloquear amenazas. El proyecto propone integrar estas soluciones para crear un mecanismo de protección integral para las redes de dispositivos IoT que permita identificar amenazas y activar mecanismos seguros de transferencia de información. El objetivo final es el afinamiento de un algoritmo que permita implementar la solución propuesta, que se adecue a las capacidades computacionales de IoT industrial. La solución propuesta logra detectar y contener intrusos en una red de IoT y supera en algunos casos los mecanismos de detección tradicionales. El algoritmo es escalable y permite la interconectividad de grandes cantidades de nodos.

#### NetFlow Datasets for Machine Learning-Based Network Intrusion Detection Systems [5].

Este documento aborda la dificultad de comparar los sistemas de detección de intrusos en la red (NIDS) basados en el aprendizaje automático (ML) en diferentes conjuntos de datos, lo que genera una brecha entre la investigación académica y las implementaciones prácticas. Para cerrar esta brecha, el documento proporciona cinco conjuntos de datos NIDS con un conjunto de características comunes basado en NetFlow, un formato ampliamente implementado en redes de producción. Estos conjuntos de datos están etiquetados para experimentos de clasificación de ataques y tráfico binario y multiclase y están disponibles para la comunidad de investigación. El documento presenta una evaluación de un clasificador de conjunto Extra Trees en estos conjuntos de datos como un caso de uso y un escenario de aplicación. NetFlow tiene los beneficios de que tiene una gran relevancia práctica, su amplia implementación y que permite un fácil escalamiento.

#### Towards a Standard Feature Set for Network Intrusion Detection System Datasets [9].

Este documento analiza la importancia de los sistemas de detección de intrusos en la red (NIDS) para proteger las redes informáticas contra los ataques cibernéticos, con esfuerzos recientes centrados en el desarrollo de NIDS basados en aprendizaje automático (ML). Sin embargo, la falta de un conjunto de características estándar en conjuntos de datos disponibles públicamente dificulta la comparación del rendimiento de diferentes clasificadores de tráfico basados en ML en diferentes conjuntos de datos, lo que limita la capacidad de evaluar la generalización de estos sistemas. Para abordar esta limitación, el documento propone y evalúa conjuntos de funciones NIDS estándar basados en el sistema y el protocolo de recopilación de metadatos de la red NetFlow. El conjunto de funciones de NIDS basado en NetFlow propuesto, junto con cuatro conjuntos de datos de referencia, se pone a disposición de la comunidad de investigación para permitir una evaluación más rigurosa y completa de los NIDS basados en ML. Los resultados muestran que el conjunto más grande con 43 funciones de NetFlow logra un rendimiento de clasificación consistentemente más alto en comparación con el conjunto de funciones original, que se adaptó a cada uno de los conjuntos de datos NIDS considerados.

#### Medición de desempeño de sistema de monitoreo de redes con protocolo Netflow en modelo Big Data [16]

Este documento analiza y evalúa la cadena de procesos que limita la capacidad en un canal de información utilizando el protocolo Netflow. Se identifican las aplicaciones de mayor consumo y se determina la causa de la saturación del canal. Se utiliza el modelo Ergódico, un modelo matemático que evalúa el comportamiento promedio, para identificar los procesos que causan la saturación del servicio. Se implementó la tecnología AVC "Application Visibility and Control" en los dispositivos muestreados y se diseñó un código en MATLAB para el proyecto. Con este software, se evaluó si el canal de comunicaciones es Ergódico o no. Se busca responder la pregunta ¿se puede optimizar el servicio?

#### Evaluación de modelos de machine learning para sistemas de detección de intrusos en Redes IoT [17]

Este trabajo aborda la importancia de la seguridad en las redes IoT y cómo los Sistemas de Detección de Intrusos son fundamentales para enfrentar los desafíos de seguridad. Se entrenan dos modelos de Machine Learning, Support Vector Machine y TabNet, para detectar ataques de tipo DoS, Backdoor y Reconnaissance. Los modelos son evaluados con la métrica de recall y se comparan entre sí. El modelo de mejor desempeño (TabNet) logra detectar cerca del 100% de los ataques, pero tiene un alto número de falsas alarmas (50%) y tiene dificultades para identificar el tipo exacto de ataque.

#### Implementación de análisis de tráfico y de flujos de red con tecnologías netflow y sflow en equipos de red de la UNAM utilizando software libre [18]

La propuesta busca implementar el análisis de tráfico de red en la UNAM utilizando tecnologías como NetFlow y sFlow. El objetivo es apoyar la resolución de incidentes y permitir el monitoreo en tiempo real y almacenamiento estadístico del tráfico en los enlaces de la UNAM. La solución deberá operar continuamente y notificar al Centro de Operación de RedUNAM mediante correo elec

Dataset CICDDoS2019. El sistema Dique tiene una interfaz gráfica que permite cambiar entre modo de detección y modo de prevención y muestra la información de los paquetes y su respectiva clasificación.

#### Sistema preventivo contra ataques de Denegación de servicio web utilizando Deep Learning [19]

El documento describe el proceso de investigación para crear un sistema preventivo contra ataques DDoS en servidores web y el diseño y construcción de un software que integra una interfaz gráfica de usuario con el modelo de clasificación. El sistema Dique clasifica los paquetes que ingresan a la red en dos tipos: Maligno y NoMaligno, utilizando un algoritmo de Deep Learning con la red neuronal artificial Deep Feed Forward y se entrenó con el Dataset CICDDoS2019. El sistema Dique tiene una interfaz gráfica que permite cambiar entre modo de detección y modo de prevención y muestra la información de los paquetes y su respectiva clasificación.

#### The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 dataset [20]

Este documento analiza la importancia de los sistemas de detección de anomalías (ADS) en la detección de nuevos ataques en los sistemas de detección de intrusos en la red (NIDS). Sin embargo, la evaluación de los NIDS utilizando conjuntos de datos de referencia existentes no arroja resultados satisfactorios. Para abordar esto, se generó el conjunto de datos UNSW-NB15, que incluye estilos de ataque modernos de bajo impacto y nuevos patrones de tráfico normal. En este documento se muestra la complejidad del conjunto de datos UNSW-NB15 en tres aspectos: análisis estadístico, correlaciones entre características y evaluación utilizando cinco clasificadores existentes. Los hallazgos revelan que el conjunto de datos UNSW-NB15 es más complejo que el conjunto de datos KDD99, lo que lo convierte en un nuevo punto de referencia para evaluar los sistemas de detección de intrusiones en red (NIDS).

#### Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review [6]

Este articulo analiza los desafíos y riesgos asociados con la tecnología IoT, incluida la gestión de la seguridad, la heterogeneidad, la escalabilidad y la calidad del servicio. La falta de seguridad en los dispositivos IoT supone un riesgo importante y puede dar lugar a ataques de seguridad y pérdidas financieras. El texto también se centra en los ataques de denegación de servicio distribuido (DDoS) y su impacto en el mundo cibernético. Se analizan diferentes tipos de ataques DDoS, impactos y soluciones de mitigación, con una comparación de los modelos de detección y prevención de intrusiones para mitigar los ataques DDoS. El texto también cubre varias técnicas de aprendizaje automático y aprendizaje profundo para el preprocesamiento de datos y la detección de malware. Finalmente, el texto analiza los desafíos de investigación y las soluciones propuestas para el futuro de la seguridad de IoT.

## Marco teórico

En esta seccion, se exploraron los conceptos y teorías relacionadas con la detección de ataques DDoS utilizando algoritmos basados en Deep Learning y redes neuronales. Se examinará la importancia de los conjuntos de datos NF-UQ-NIDS, que son datasets estandarizados basados en el protocolo de red Netflow, y cómo pueden ser utilizados para entrenar y evaluar los modelos de detección.

#### Internet de las cosas (IOT)

Es una red de dispositivos interconectados que se comunican entre sí y con servidores en la nube. Esto ha sido posible gracias a microchips económicos y una infraestructura de comunicaciones de alta velocidad. Como resultado, ha habido un aumento en dispositivos conectados, desde cepillos de dientes hasta automóviles y maquinaria industrial, todos equipados con sensores para recopilar datos y tomar decisiones inteligentes.[x1]

IoT tuvo sus inicios en los años 90 cuando ingenieros comenzaron a incorporar sensores y unidades de procesamiento en objetos cotidianos. A pesar de que la evolución fue inicialmente lenta debido al tamaño de los microchips, la miniaturización y el desarrollo de chips de radiofrecuencia de baja potencia, como las etiquetas RFID, redujeron significativamente el tamaño y el costo de integrar capacidades computacionales en objetos pequeños.[x1]

Un ejemplo de esta tendencia es la adición de funciones de conectividad mediante asistentes de voz como Alexa a dispositivos con menos de 1MB de memoria RAM, como interruptores de luz. Todo esto ha dado lugar a una industria que llena los entornos, desde hogares hasta oficinas, con dispositivos de IoT que pueden enviar datos automáticamente a Internet. En conjunto, estos "dispositivos de cómputo discretos" y las tecnologías que los respaldan se conocen como Internet de las cosas.[x1]

#### Ataques de denegación de servicio DOS Y DDOS

Un ataque de Denegación de servicios DoS es un tipo de ataque que tiene como objetivo sobrecargar un servidor, una red o una página web para que los servicios que estos prestan sean inaccesibles para los usuarios reales o legítimos. Los ataques DoS se realizan sobrecargando el servicio o recurso que se quiere denegar mediante un gran volumen de tráfico o solicitudes de modo que las solicitudes de los usuarios reales no puedan ser procesadas. Estos Ataques se realizan para causar pérdidas económicas o de reputación para la organización afectada. [6] Los métodos más comunes son:

* **Ataque de inundación de tráfico:** el atacante envía una gran cantidad de tráfico falso al servicio o recurso objetivo con el fin de agotar sus recursos de red.
* **Ataque de amplificación:** el atacante envía solicitudes al servidor de un tercero que responderán con paquetes de datos mucho más grandes, lo que puede sobrecargar el servicio o recurso objetivo.
* **Ataque de reflexión:** el atacante falsifica la dirección IP de la solicitud para que parezca que proviene de un tercero. Luego, envía la solicitud a un servidor de ese tercero, que responde con una gran cantidad de datos al servicio o recurso objetivo, lo que puede sobrecargarlo.
* **Ataque de consumo de recursos:** el atacante aprovecha vulnerabilidades en el software o hardware del servicio o recurso objetivo para agotar sus recursos, como el uso excesivo de CPU o memoria.

Un ataque DDoS (Denegación de Servicio Distribuido) es una variante avanzada de un ataque DoS (Denegación de Servicio), en el que se utilizan múltiples dispositivos comprometidos en diferentes lugares para sobrecargar una red, sistema o servidor específico. El objetivo es hacer que el servicio sea inaccesible para usuarios legítimos. La diferencia clave entre DDoS y DoS radica en que en DDoS participan varios dispositivos controlados por una o varias personas, mientras que en DoS un solo dispositivo realiza el ataque.

Los atacantes suelen infectar numerosos dispositivos previamente con malware para crear una red de bots llamada botnet. Luego, utilizan esta botnet para enviar tráfico malicioso a la víctima, saturando su infraestructura de red y volviéndola inaccesible.

Los atacantes pueden aprovechar dispositivos IoT para llevar a cabo ataques DDoS masivos, ya que incluso unos pocos dispositivos comprometidos pueden generar suficiente tráfico para interrumpir un servicio en línea. Por lo tanto, es esencial asegurar y proteger los dispositivos IoT contra accesos no autorizados para prevenir su uso en ataques maliciosos.

Podemos clasificar los ataques DDoS según las siguientes categorías:

* **Basados en volumen:** se enfocan en inundar la red del objetivo con una gran cantidad de tráfico, lo que puede saturar la capacidad de la red y hacer que los servicios sean inaccesibles. Algunos ejemplos de ataques basados en volumen son los ataques de inundación UDP, SYN Flood, Ping Flood, entre otros.
* **Basados en la capa de aplicación:** buscan explotar vulnerabilidades en aplicaciones específicas, como servidores web, para agotar los recursos del servidor y hacer que sea inaccesible. Ejemplos de ataques de capa de aplicación incluyen el ataque HTTP Flood, el ataque Slowloris, entre otros.
* **Basados en amplificación:** estos ataques aprovechan la capacidad de algunos servicios para amplificar el tráfico de los atacantes. Por ejemplo, un atacante puede enviar una solicitud falsa a un servidor DNS que hace que el servidor responda con una gran cantidad de datos a la víctima. Los ataques de amplificación incluyen el ataque DNS Amplification, NTP Amplification, entre otros.
* **Basados en vulnerabilidades:** aprovechan las vulnerabilidades específicas en dispositivos conectados a Internet de las cosas (IoT) para crear botnets y lanzar ataques DDoS. Los atacantes pueden aprovechar contraseñas predeterminadas débiles o vulnerabilidades conocidas en dispositivos IoT para tomar el control de ellos y utilizarlos para lanzar ataques DDoS.
* **Ataques combinados:** Los ataques DDoS también pueden combinar varias técnicas para hacer que el ataque sea más difícil de mitigar. Por ejemplo, un atacante puede lanzar un ataque de inundación de la capa de red al mismo tiempo que un ataque de amplificación de DNS para maximizar el impacto del ataque.

#### Machine learning y Deep learning

El aprendizaje automático, o Machine Learning, es un subcampo de la inteligencia artificial que se enfoca en desarrollar algoritmos que permiten a las máquinas aprender a partir de datos, sin necesidad de programarlas explícitamente. Se emplea para llevar a cabo diversas tareas, como clasificación, regresión, agrupación, detección de anomalías, reconocimiento de patrones y toma de decisiones.

El aprendizaje profundo, o Deep Learning, es una subdisciplina del aprendizaje automático que se especializa en aprender y extraer características de datos complejos mediante el uso de redes neuronales artificiales profundas. Estas redes constan de múltiples capas y se aplican en la detección de patrones, el reconocimiento de imágenes y voz, el procesamiento del lenguaje natural, entre otros. Se entrenan con grandes conjuntos de datos y han tenido un impacto significativo en la resolución de problemas de inteligencia artificial, impulsando avances notables en áreas como la visión artificial, la robótica y la conducción autónoma.

|  |  |  |
| --- | --- | --- |
|  | Machine Learning (ML) | Deep Learning (DL) |
| Estructura de datos | Requiere datos estructurados y definidos con características definidas. | Puede manejar datos estructurados y no estructurados. |
| Algoritmos | Utiliza algoritmos supervisados, no supervisados y de refuerzo. | Utilizan redes neuronales profundas, tales como las redes neuronales convolucionales (CNN) y también las redes neuronales recurrentes (RNN). |
| Representación de características | Requiere que las características se extraigan manualmente. | Puede extraer automáticamente las características de los datos. |
| Capacidad de generalización | Menos propenso a la sobreajuste y puede generalizar bien para datos nuevos. | Más propenso al sobreajuste, pero puede generalizar bien para datos nuevos si se entrena adecuadamente. |
| Escalabilidad | Limitado en la escalabilidad, requiere mucho tiempo para entrenar grandes conjuntos de datos. | Es altamente escalable y puede entrenar grandes conjuntos de datos en paralelo utilizando GPUs. |

Tabla No. 1 Comparación entre Machine Learning VS Deep Learning

Apruzze y Colajanni[21] propusieron una taxonomía original dirigida específicamente a los operadores de seguridad. Esta clasificación distingue el aprendizaje profundo (DL) moderno de los algoritmos tradicionales de aprendizaje automático, llamado aprendizaje superficial (SL). Mientras que SL requiere que los expertos en el dominio identifiquen las características relevantes de los datos antes de ejecutar el algoritmo, DL permite que la selección de características sea autónoma mediante el aprendizaje de la representación.

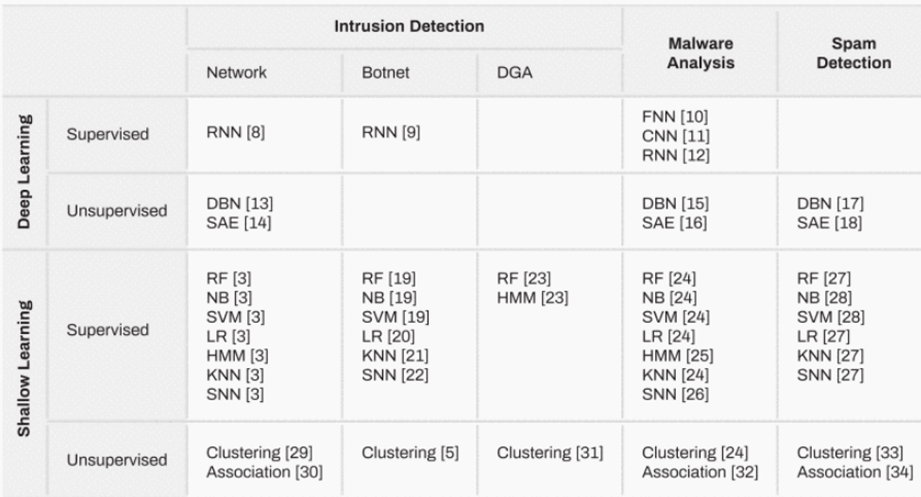


Imagen No. 1 Aplicaciones de ML y DL en problemas de seguridad.

#### Modelos de Deep Learning

Los algoritmos supervisados en Deep Learning son una rama de la inteligencia artificial que se enfoca en el aprendizaje automático. Los algoritmos supervisados son aquellos que se entrenan con un conjunto de datos etiquetados y luego se utilizan para predecir la etiqueta de nuevos datos.

* **Las Redes Neuronales Convolucionales, o CNN en inglés**, son un tipo de red neuronal profunda ampliamente empleado en la visión por computadora, especialmente en la clasificación de imágenes. Su concepto principal consiste en procesar la imagen de entrada mediante capas de convolución y agrupación para extraer sus características, y posteriormente utilizar estas características en capas completamente conectadas para llevar a cabo la clasificación.
* **Las redes neuronales recurrentes (RNN)** son un tipo de red neuronal que se utiliza principalmente para el procesamiento de lenguaje natural. Estas redes son capaces de procesar secuencias de datos y recordar información anterior para predecir la siguiente palabra o frase.
* **Las redes neuronales profundas** son un tipo de red neuronal que se utiliza para procesar grandes conjuntos de datos. Estas redes tienen muchas capas ocultas y son capaces de detectar patrones complejos en los datos.
* **Las redes neuronales de alimentación** hacia adelante son un tipo de red neuronal que se utiliza principalmente para clasificación y regresión. Estas redes tienen una estructura simple y están compuestas por una capa de entrada, una o varias capas ocultas y una capa de salida.

#### Algoritmos no supervisados en Deep Learning:

* **Autoencoders:** son redes neuronales que aprenden a comprimir datos en una representación de menor dimensión, llamada "codificación", y luego reconstruyen los datos de la codificación. Se utilizan en aplicaciones como la reducción de la dimensionalidad, la eliminación de ruido y la generación de nuevas muestras.
* **Redes neuronales generativas (GAN):** son redes que generan muestras de datos sintéticos similares a los datos de entrenamiento. Una red GAN consta de dos partes: un generador que produce datos sintéticos y un discriminador que evalúa la autenticidad de los datos. Se utilizan en aplicaciones como la generación de imágenes y la síntesis de voz.
* **Redes neuronales convolucionales 3D (3DCNN):** son extensiones de las redes neuronales convolucionales (CNN) que se utilizan para datos tridimensionales, como videos y volúmenes de datos médicos. Utilizan filtros 3D para extraer características espaciales y temporales.
* **Redes neuronales de flujo:** son redes que modelan la distribución de probabilidad de los datos de entrada mediante el uso de transformaciones de flujo inverso. Utilizan la regla de cambio de variables para calcular la densidad de probabilidad del espacio de entrada y se utilizan en aplicaciones como la generación de imágenes y el modelado de la densidad de probabilidad de los datos.

#### Sistemas de Detección de intrusos con Machine learning y Deep learning

Los sistemas de prevención de ataques DDoS se dividen en dos categorías: sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS). Los IDS emiten alertas en caso de intrusión sin tomar medidas, mientras que los IPS toman medidas de penalización.

Los IDS son herramientas de seguridad utilizadas después de los firewalls y se dividen en IDS basados en host y en red. Los basados en host monitorean un host específico, mientras que los basados en red supervisan todo el tráfico de red, detectan y responden a ataques. Los IDS también se dividen en basados en firmas (comparan con una base de datos de firmas conocidas) y en anomalías (detectan comportamientos anómalos en relación con el comportamiento normal del sistema).

Los IDS tienen ventajas como la detección temprana y la recopilación de información detallada, pero presentan debilidades como la fragmentación de paquetes y la dificultad para distinguir entre comunicaciones normales y ataques. Un IDS consta de tres componentes principales: recopilación de datos, selección/conversión de características y un motor de decisiones que determina si se ajusta a la definición de una intrusión, pudiendo ser basado en firmas o anomalías. Este motor es crucial para la eficiencia del sistema de IDS. [22]

#### Datasets (Conjunto de datos)

En el campo de la ciberseguridad, se han identificado 15 conjuntos de datos (datasets) para entrenar sistemas de detección de intrusos, según una encuesta de 2019 [17]. Estos datasets presentan diversas características seleccionadas por los autores en función de sus conocimientos y experiencias, pero análisis posteriores han revelado que muchas de estas características carecen de relevancia y su diversidad dificulta la generalización del rendimiento de los modelos en un dataset específico [11]. Además, estos datasets se generan a partir de entornos virtuales, lo que crea una brecha entre los modelos desarrollados con ellos y los sistemas IDS utilizados en entornos del mundo real.

#### Métricas para evaluar capacidad

La Matriz de Confusión (CM) es una herramienta comúnmente utilizada para evaluar la corrección de un modelo de clasificación. Si bien no es una medida de rendimiento en sí misma, la mayoría de las otras métricas se derivan de sus parámetros. Para reducir los errores, la CM proporciona dos estrategias: disminuir los Falsos Negativos o los Falsos Positivos. Qué estrategia utilizar depende del contexto; por ejemplo, en la clasificación de spam de correo electrónico, se deben minimizar los Falsos Positivos, mientras que en la clasificación de pacientes con cáncer se deben minimizar los Falsos Negativos.[6]

Hay varias métricas de rendimiento derivadas de la CM, que incluyen la Exactitud, la Precisión, la Sensibilidad/Recall, el Puntaje F-1, la Especificidad y la Curva AUC-ROC.

* **La exactitud** mide el número de predicciones correctas sobre el total de predicciones, pero es más adecuada para conjuntos de datos balanceados.
* **La precisión** determina la precisión de un modelo en encontrar el número de positivos reales de los positivos totales predichos, y es útil cuando los Falsos Positivos son costosos, como en la detección de spam de correo electrónico.
* **El recall** mide la precisión de un modelo en encontrar el número de positivos de los positivos reales totales y es útil cuando los Falsos Negativos son costosos, como en la detección de fraude.
* **El Puntaje F-1** se calcula como la Media Armónica de la Precisión y el Recall, otorgando igual importancia a ambas métricas, y es útil para evaluar el rendimiento de un conjunto de datos desequilibrado.
* **La especificidad** es el opuesto del Recall y mide la tasa de Falsos Positivos.

La Curva AUC-ROC es una medida de la estabilidad entre la Precisión y el Recall al variar los umbrales y se representa por el Área Bajo la Curva (AUC), siendo una mayor AUC indicativa de un mejor modelo de clasificación.

Otras métricas, como la métrica KAPPA y el Error Cuadrático Medio (RMSE), también pueden utilizarse según los requisitos específicos.

#### Análisis de tráfico

El monitoreo y análisis de redes involucra la captura de todo el tráfico de red o un resumen en forma de flujos. Para prevenir ataques DDoS con dispositivos IoT, es esencial analizar patrones de tráfico y mitigar el tráfico malicioso que podría sobrecargar la red. Estos ataques suelen originarse en dispositivos IoT infectados. Las técnicas incluyen la inspección de paquetes y la detección de patrones inusuales, además del uso de soluciones como el filtrado de paquetes para bloquear el tráfico malicioso antes de llegar a la red de destino.

#### Cisco Net Flow

NetFlow de Cisco es un protocolo desarrollado por Cisco Systems para recopilar información sobre el tráfico de red, como el origen, el destino, el tipo de protocolo y el tiempo. Este protocolo ayuda en la gestión y solución de problemas de redes al recopilar estos datos a través de routers y switches, enviándolos a un colector de NetFlow para su análisis.[16]

El NetFlow se usa para diversas finalidades, como detectar problemas de red, monitorear la actividad, planificar la capacidad e identificar tráfico malicioso. También sirve para analizar el comportamiento del usuario y mejorar el rendimiento de la red según las necesidades de la organización.

Los sistemas de detección de intrusos en red (NIDS) basados en aprendizaje automático (ML) son prometedores en la ciberseguridad, pero enfrentan desafíos en la implementación práctica debido a la falta de conjuntos de datos comunes. La idea de crear conjuntos de datos NIDS basados en NetFlow con características relevantes es una solución potencial. Utilizar NetFlow como formato común ofrece ventajas prácticas y de escalabilidad, mejorando la seguridad cibernética en redes del mundo real. [5]

#### Herramientas de para machine learning y Deep learning

* **Jupyter Notebook:** Una aplicación web de código abierto que permite crear documentos interactivos con código, ecuaciones, visualizaciones y texto narrativo.
* **Scikit-Learn:** Una biblioteca en Python para algoritmos de clasificación, regresión y clustering, aunque no está diseñada para aprendizaje profundo.
* **TensorFlow:** Ampliamente utilizado para aprendizaje profundo en Python, ofrece una amplia gama de herramientas y es altamente personalizable.
* **Keras:** Interfaz de aprendizaje profundo en Python compatible con TensorFlow, que simplifica la construcción de redes neuronales.
* **PyTorch:** Biblioteca de aprendizaje profundo en Python enfocada en la facilidad de uso y flexibilidad, especialmente en problemas de aprendizaje profundo.

# Marco Legal

NTC 27001:2006c es una norma técnica colombiana que establece los requisitos para un sistema de gestión de seguridad de la información.

Ley 1273 de 5 de enero de 2009 es una ley colombiana que modifica el Código Penal y crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos” - y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

CONPES 3701 de 2011 es un documento que establece los lineamientos de política para ciberseguridad y ciberdefensa en Colombia.

Resolución 500 del 2021 es una resolución del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) que establece los requisitos técnicos para la implementación del Sistema Nacional de Ciberseguridad.

# Metodología

Presentación del cómo se llevó a cabo el proyecto. Se puede presentar por actividades o fases del proyecto de acuerdo con el proyecto de grado aprobado. Se debe incluir un análisis del porqué de la selección de los métodos, técnicas, estándares y normas empleadas.

En este capitulo se presenta el enfoque y las técnicas adoptadas para abordar cada uno de los objetivos para la detección de ataques DDoS en redes IoT. Nuestro enfoque se centra en proponer un algoritmo basado en el aprendizaje profundo y específicamente, en redes neuronales, para afrontar este problema. Este algoritmo se construirá sobre el conjunto de datos NF-UQ-NIDS, que se basa en el protocolo de red Netflow.

Para lograr este objetivo principal, comenzaremos por un preprocesamiento y acondicionamiento del conjunto de datos, con el fin de destacar y comprender las características intrínsecas de un ataque DDoS en el contexto de una red IoT. Posteriormente, nos adentraremos en el diseño e implementación de un algoritmo supervisado basado en una arquitectura de red neuronal para modelar y clasificar estos datos. Finalmente, para validar y evaluar la eficacia de nuestro modelo propuesto, llevaremos a cabo un análisis estadístico de los resultados, y contrastaremos su desempeño con otras técnicas presentes en el estado del arte. A través de estos pasos meticulosos, aspiramos a ofrecer una solución robusta y precisa para la detección de ataques DDoS en entornos IoT.

Se presenta una serie de tareas detalladas y exhaustivas para cumplir con los objetivos planteados:

* Fase 1.

Realizar un preprocesamiento y acondicionamiento de la información del conjunto de datos para determinar las características de un ataque DDoS en una red IoT.

* Carga y exploración inicial del dataset NF-UQ-NIDS.
* Identificación y tratamiento de valores faltantes o atípicos.
* Selección de características relevantes y eliminación de aquellas no esenciales.
* Normalización y escalado de las características numéricas.
* Codificación de variables categóricas si es necesario.
* División del conjunto de datos en conjuntos de entrenamiento, prueba y validacion.
* Fase 2:

Implementar un algoritmo de aprendizaje supervisado basado en una red neuronal para modelar el conjunto de datos.

* Diseño de la arquitectura de la red neuronal (número de capas, nodos, funciones de activación, etc.).
* Definición de hiperparámetros y criterios de parada.
* Entrenamiento del modelo usando el conjunto de datos de entrenamiento.
* Validación y ajuste del modelo utilizando un subconjunto de validación.
* Pruebas de detección de ataques DDoS con el conjunto de datos de prueba.
* Evaluación del rendimiento del modelo (precisión, recall, F1-score, etc.).
* Fase 3:

Realizar un análisis estadístico de los resultados obtenidos y comparar su desempeño frente a otra técnica reportada en el estado del arte.

* Revisión de técnicas reportadas en la literatura relacionadas con la detección de ataques DDoS en IoT.
* Aplicación de métricas de rendimiento sobre el modelo propuesto.
* Comparación cuantitativa y cualitativa de los resultados obtenidos con los reportados en el estado del arte.
* Documentación de los hallazgos y conclusiones obtenidas.
* Propuestas de mejoras y trabajos futuros basados en los resultados del análisis.

Con estas tareas, se busca llevar a cabo de manera organizada y metódica el desarrollo y análisis de un algoritmo de detección de ataques DDoS en redes IoT, desde la adquisición y preprocesamiento de datos hasta la evaluación y comparación con técnicas existentes.

## Herramientas Y Plataformas De Deep Learning Apropiadas Para El Desarrollo

#### Tensor Flow

TensorFlow, una biblioteca de código abierto concebida por Google Brain, se destaca por su habilidad en la construcción y entrenamiento de modelos de aprendizaje profundo, además de otras técnicas de aprendizaje automático. Una de sus principales fortalezas radica en ofrecer una plataforma de cálculo numérico eficaz basada en gráficos de flujo de datos. Además, su escalabilidad es notable, permitiendo entrenar modelos no solo en CPU, sino también en GPU y en clusters que engloban múltiples GPUs. A pesar de que su nivel de abstracción pueda ser más complejo en comparación con otras herramientas, esta característica concede al usuario una amplia flexibilidad, esencial para diseñar modelos a medida.

#### Keras

Por otro lado, Keras actúa como una interfaz de alto nivel destinada específicamente para redes neuronales, y opera encima de TensorFlow. Esta herramienta se diseñó pensando en simplificar y acelerar la experimentación. Ofrece bloques de construcción ya predefinidos, lo que optimiza notablemente el proceso de diseño de modelos. Cabe destacar que, desde la versión 2.0 de TensorFlow, Keras se ha integrado directamente en éste, permitiendo así que los usuarios aprovechen la intuitiva interfaz de Keras a la par que se benefician del poder y capacidad de TensorFlow en segundo plano. Por todo ello, la elección de estas herramientas se alinea con el objetivo de garantizar una implementación robusta, eficiente y flexible para el proyecto.

#### Scikit-learn

Para la fase inicial de nuestro proyecto, hemos decidido emplear Scikit-learn, una biblioteca consagrada en el mundo del aprendizaje automático. A pesar de que está diseñada principalmente para el aprendizaje automático clásico y no para el aprendizaje profundo, Scikit-learn se erige como una herramienta altamente valiosa en las etapas preliminares de cualquier proyecto relacionado con la ciencia de datos. Esto se debe a que Scikit-learn ofrece herramientas simples pero potentes para el análisis predictivo de datos. Su diseño intuitivo permite un rápido despliegue y experimentación, lo que es crucial durante las etapas iniciales de exploración y preprocesamiento de datos. Esta biblioteca proporciona una gama extensa de algoritmos de clasificación, regresión, clustering y reducción de dimensionalidad. Tal variedad nos permitirá tener una visión completa y un entendimiento profundo de nuestros datos antes de avanzar a etapas posteriores.

Dado que no está diseñada para modelar redes neuronales profundas ni para trabajar en GPU, Scikit-learn se presenta como la herramienta ideal para la fase inicial donde el enfoque está en comprender, limpiar y preparar los datos, más que en modelar soluciones de aprendizaje profundo.

En resumen, al optar por Scikit-learn para las primeras etapas del proyecto, buscamos garantizar una exploración y un preprocesamiento de datos eficientes y robustos, creando así una base sólida para las fases subsecuentes de modelado y análisis más profundos.

## NF-UQ-NIDS-v2

En la página web de nuestro conjunto de datos encontramos la siguiente descripción del conjunto de datos:

Un conjunto de datos **NF-UQ-NIDS-v2** fusiona los siguientes conjuntos de datos: **NF-UNSW-NB15-v2, NF-ToN-IoT-v2, NF-BoT-IoT-v2, NF-CSE-CIC-IDS2018-v2.** El conjunto de datos recientemente publicado representa los beneficios de los conjuntos de características de conjuntos de datos compartidos, donde es posible fusionar múltiples conjuntos de datos más pequeños. Esto eventualmente conducirá a un conjunto de datos NIDS más grande y universal que contenga flujos de múltiples configuraciones de red y diferentes configuraciones de ataque.

Incluye una función de etiqueta adicional, que identifica el conjunto de datos original de cada flujo. Esto se puede utilizar para comparar los mismos escenarios de ataque realizados en dos o más redes de prueba diferentes. Las categorías de ataque se han modificado para combinar todas las categorías principales. Los ataques denominados ataques DoS-Hulk, ataques DoS-SlowHTTPTest, ataques DoS-GoldenEye y ataques DoS-Slowloris han cambiado de nombre a la categoría principal DoS.

Los ataques denominados ataque DDoS-LOIC-UDP, ataque DDoS-HOIC y ataques DDoS-LOIC-HTTP han cambiado de nombre a DDoS. Los ataques denominados FTP-BruteForce, SSH-Bruteforce, Brute Force -Web y Brute Force -XSS se han combinado como una categoría de fuerza bruta. Finalmente, los ataques de inyección SQL se han incluido en la categoría de ataques de inyección. El conjunto de datos NF-UQ-NIDS tiene un total de 75.987.976 registros, de los cuales 25.165.295 (33,12%) son flujos benignos y 50.822.681 (66,88%) son ataques. La siguiente tabla enumera la distribución de las categorías de ataque finales.

|  |  |
| --- | --- |
| **Class** | **Count** |
| Benign | 25165295 |
| DDoS | 21748351 |
| Reconnaissance | 2633778 |
| Injection | 684897 |
| DoS | 17875585 |
| Brute Force | 123982 |
| Password | 1153323 |
| XSS | 2455020 |
| Infilteration | 116361 |
| Exploits | 31551 |
| Scanning | 3781419 |
| Fuzzers | 22310 |
| Backdoor | 18978 |
| Bot | 143097 |
| Generic | 16560 |
| Analysis | 2299 |
| Theft | 2431 |
| Shellcode | 1427 |
| MITM | 7723 |
| Worms | 164 |
| Ransomware | 3425 |

## Preprocesamiento Y Acondicionamiento Conjunto De Datos Para Determinar Las Características De Un Ataque DDoS En Una Red IOT Utilizando El Dataset NF-UQ-NIDS.

* Carga y exploración inicial del “Dataset” NF-UQ-NIDS.
* Identificación y tratamiento de valores faltantes o atípicos.
* Selección de características relevantes y eliminación de aquellas no esenciales.
* Normalización y escalado de las características numéricas.
* Codificación de variables categóricas si es necesario.
* División del conjunto de datos en conjuntos de entrenamiento, prueba y validación.

A continuación, investigaremos la integridad de los datos, buscando valores nulos y evaluando su impacto en la utilidad del conjunto. Identificar si los datos son discretos o continuos, y obtener información sobre los tipos de datos subyacentes, nos ayudará a planificar futuras etapas de preprocesamiento. Si estamos abordando un problema supervisado, identificaremos la columna de "salida" y determinaremos si la distribución de clases está balanceada. Exploraremos las características en busca de importancia, veremos si siguen alguna distribución específica y analizaremos la correlación entre ellas. Si es un problema de visión artificial, evaluaremos la cantidad de muestras por clase. También buscaremos outliers y decidiremos si eliminarlos o conservarlos, considerando su impacto y si representan errores de carga o datos reales. Finalmente, estudiaremos posibles sesgos de datos para garantizar que nuestro modelo de aprendizaje automático no discrimine clases minoritarias. Este plan de análisis exploratorio nos permitirá comprender completamente nuestro conjunto de datos y tomar decisiones informadas en la próxima etapa del proyecto.

### ANALISIS EXPLORATORIO DE LOS DATOS

El análisis exploratorio de datos es un paso fundamental en cualquier proyecto de ciencia de datos y puede proporcionar una visión integral de la calidad y la estructura de tu conjunto de datos.

Comenzamos evaluando las características de nuestro conjunto de datos incluyendo la cantidad de registros disponibles y determinaremos si es adecuada para nuestros objetivos. Si los registros son insuficientes, consideraremos la capacidad de recursos (CPU y RAM) necesaria para el procesamiento.

#### CARGA Y REDUCCION DATASET

En la descripción del conjunto de datos observamos que este compuesto de una cantidad muy grande de datos que no es posible procesar además de que hay una variedad de datos que no son relevantes para el desarrollo del modelo el cual solo va a estar enfocado en ataques DDoS como vemos hay una cantidad de 21748351 de registros solamente para ataques DDoS y una cantidad similar de registros de flujos benignos: 25165295. Como nuestro modelo se va enfocar en detectar ataques DDoS debemos saber si se va a descartar o no los otros tipos de ataques en el conjunto de datos final con el cual se entrenará el modelo de aprendizaje profundo.

La evaluación de la selección de datos para el entrenamiento del modelo se hizo teniendo en cuenta los siguientes criterios:

Descartar todos los otros tipos de ataques y enfocarse exclusivamente en los ataques DDoS puede tener algunas ventajas en situaciones específicas, dependiendo de los objetivos y las limitaciones del proyecto. Aquí hay algunas razones por las que podrías considerar esta estrategia:

* Enfoque Específico: Al centrarse en un tipo específico de ataque, como los ataques DDoS, se puede desarrollar un modelo altamente especializado y ajustado a ese tipo de amenaza.
* Menor Complejidad: Al eliminar registros de otros tipos de ataques, puedes simplificar el problema y reducir la complejidad del modelo.
* Mejora de la Eficiencia: Si estás trabajando en un entorno donde los ataques DDoS son la principal preocupación y se desea una solución de detección altamente eficiente.
* Riesgo de Ruido Reducido: Al eliminar registros de otros tipos de ataques, se reduce el riesgo de ruido en tus datos. Los modelos de aprendizaje automático pueden confundirse si tienen que distinguir entre múltiples clases de ataques, especialmente si algunas son raras o tienen patrones similares.

Sin embargo, también es importante considerar las desventajas de descartar otros tipos de ataques:

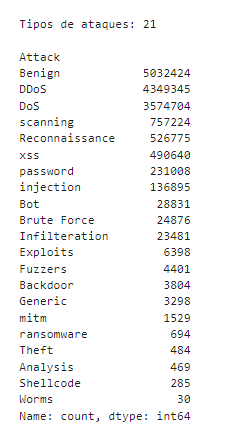
* Pérdida de Información: Descartar datos de otros tipos de ataques significa perder información valiosa que podría ser relevante en un contexto más amplio de seguridad cibernética. Podrías estar ignorando señales de otros tipos de amenazas que podrían surgir en el futuro.
* Limitación en la Detección: Centrarse exclusivamente en un tipo de ataque puede llevar a un modelo que es ciego a otras amenazas. Si bien puede ser muy eficiente en la detección de DDoS, podría ser ineficaz en la detección de otros tipos de ataques.
* No se refleja en la Realidad: En la realidad, las redes y sistemas enfrentan una variedad de amenazas. Descartar registros de otros tipos de ataques puede no reflejar con precisión el panorama de seguridad real.

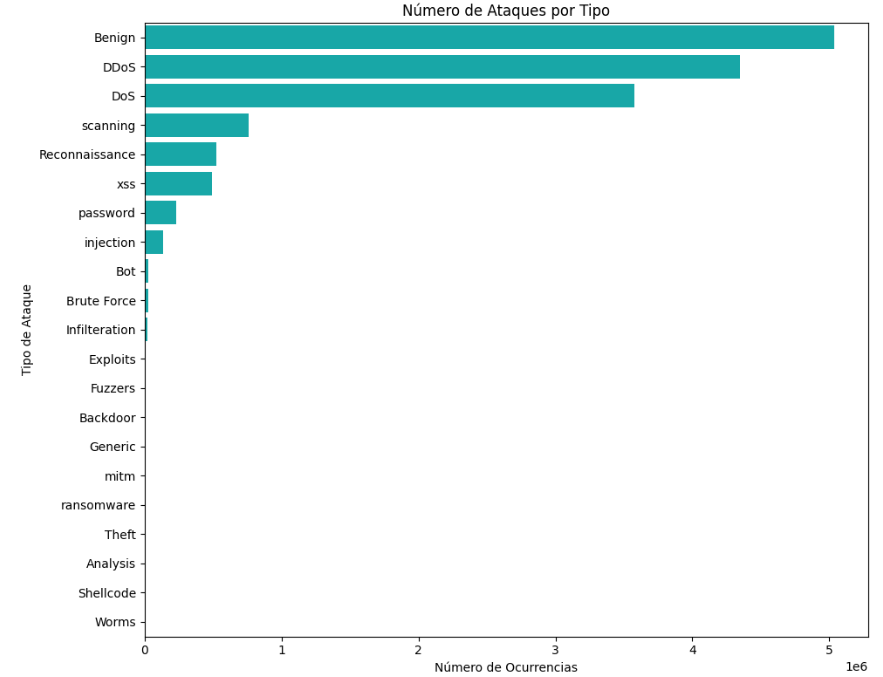
Teniendo en cuenta lo mencionado anteriormente se seleccionaron todos los distintos ataques del conjunto de datos con el fin de crear un modelo más robusto de detección de ataques, que se ajuste más a un escenario real donde un sistema tiene una variedad amplia de amenazas y se debe ser capaz de lidiar con todas estas.

Por otra es necesaria la reducción del tamaño del conjunto de datos debido a limitaciones de capacidad de RAM y recursos computacionales lo que puede dificultar el procesamiento de conjuntos de datos extremadamente grandes. Además, la reducción del tamaño del conjunto de datos puede acelerar significativamente el tiempo de entrenamiento y evaluación del modelo, lo que es esencial en aplicaciones en tiempo real. Asimismo, al eliminar datos redundantes o menos relevantes, se puede simplificar el análisis y aumentar la eficiencia del modelo. Sin embargo, es crucial garantizar que la reducción del tamaño no comprometa la representatividad del conjunto de datos y que se conserve la calidad de los datos relevantes para los objetivos del proyecto. En última instancia, la reducción del conjunto de datos debe considerarse cuidadosamente en función de los recursos disponibles y los requisitos específicos del proyecto, equilibrando la eficiencia computacional con la capacidad de lograr resultados precisos y útiles.

Para la reducción de conjunto de datos se tuvo en cuenta la distribución de las características y la estructura del conjunto de datos. Esto con el fin de identificar qué características son más informativas y cuáles son redundantes o menos relevantes. La utilización de técnica de selección de características para identificar las características más importantes. También se realizó un muestreo estratificado asegurando que todas las clases y subgrupos estén representados proporcionalmente en la muestra. Después del entrenamiento del modelo se realizará la validación cruzada para evaluar cómo afecta la calidad del modelo. Y se realizaran múltiples experimentos con diferentes tamaños de conjunto de datos reducido y evalúa su rendimiento en términos de métricas de evaluación. Se considero si la reducción inicial del conjunto de datos afecta negativamente la calidad del modelo, ajustar el proceso y revisar qué características o ejemplos de datos son esenciales.

Se toma primero el 20% del Dataset original el cual tiene una representación de cada uno de los 21 ataques.





#### LIMPIEZA DE DATOS

Un conjunto de datos limpios es un conjunto de información que ha sido procesado, organizado y depurado de manera que esté libre de errores, inconsistencias y duplicados. Estos datos están en un formato que es fácil de entender y utilizar para el análisis, la minería de datos o cualquier otro propósito específico.

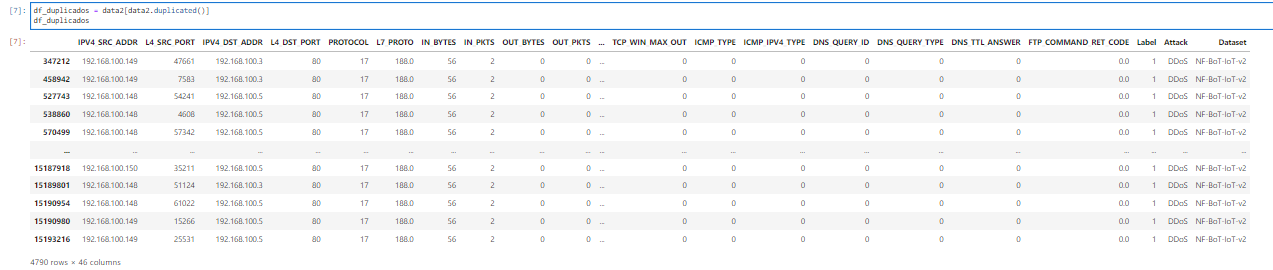
La limpieza de datos es un paso crítico en el proceso de gestión de datos y análisis de datos, y es necesario por varias razones: Los datos limpios son precisos y confiables. Esto significa que reflejan con exactitud la realidad que representan, lo que permite tomar decisiones informadas basadas en ellos, La limpieza de datos garantiza que los datos sigan un formato y una estructura coherentes. Esto facilita su comparación y análisis, ya que los datos son uniformes y no varían en su presentación, La limpieza de datos elimina errores como valores atípicos, valores faltantes o información incorrecta. Esto ayuda a evitar que se tomen decisiones incorrectas debido a datos corruptos o inexactos, Los conjuntos de datos limpios se procesan de manera más eficiente, lo que acelera el análisis y reduce el tiempo necesario para extraer información valiosa. Los datos limpios son más fáciles de representar visualmente en gráficos y tablas, lo que facilita la comunicación de resultados y tendencias a diferentes audiencias, La calidad de los datos ayudan a tomar decisiones más acertadas y fundamentadas.

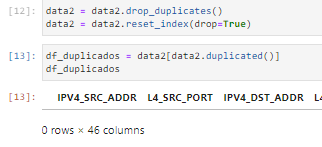
En resumen, un conjunto de datos limpios es esencial para obtener información precisa y confiable a partir de los datos, lo que a su vez es fundamental para la toma de decisiones, la investigación, el análisis y muchas otras aplicaciones en el ámbito empresarial y científico. Teniendo en cuenta esto se realizaron las siguientes tareas durante el proceso de limpieza de los datos:

* La gestión adecuada de valores faltantes y registros duplicados.
* Tratamiento de columnas tipo float y object.
* Transformación de las características tipo float64 a valores int32 e Int64.
* Codificacion Ordinal de Columnas Attack y Dataset

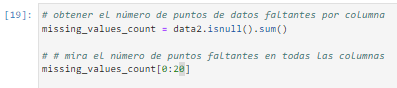
La gestión adecuada de valores faltantes y registros duplicados es esencial para mantener la integridad y la precisión de cualquier análisis de datos. Además, la presencia de datos duplicados puede inflar artificialmente la importancia de ciertas observaciones, distorsionando estadísticas descriptivas y el desempeño de modelos predictivos. Eliminar o tratar adecuadamente estos valores no solo optimiza el almacenamiento y el rendimiento computacional, sino que también garantiza que los insights extraídos del conjunto de datos sean representativos y fiables. Por lo tanto, dedicar tiempo a la identificación y gestión de valores faltantes y duplicados es una inversión crítica en la calidad y credibilidad del análisis.

Una búsqueda con la función duplicates() de pandas arroja 4790 duplicados. Debido a que son irrelevantes para el desarrollo del modelo puesto que tienen los mismos valores en todas las columnas son eliminados.





Los valores faltantes pueden introducir sesgos y alterar los resultados, llevando a conclusiones erróneas y a decisiones mal informadas. Debido a esto debemos tratar los datos faltantes o nulos.



|  |  |
| --- | --- |
|  |  |

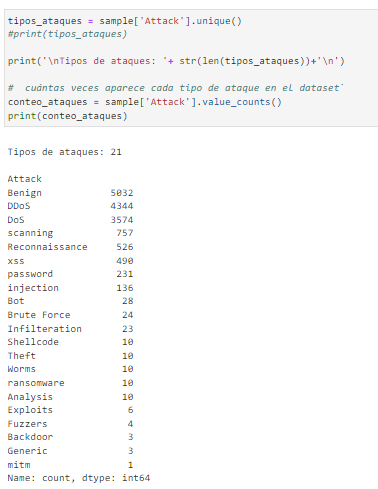
Como se puede ver no se encuentran datos faltantes en el conjunto de datos.

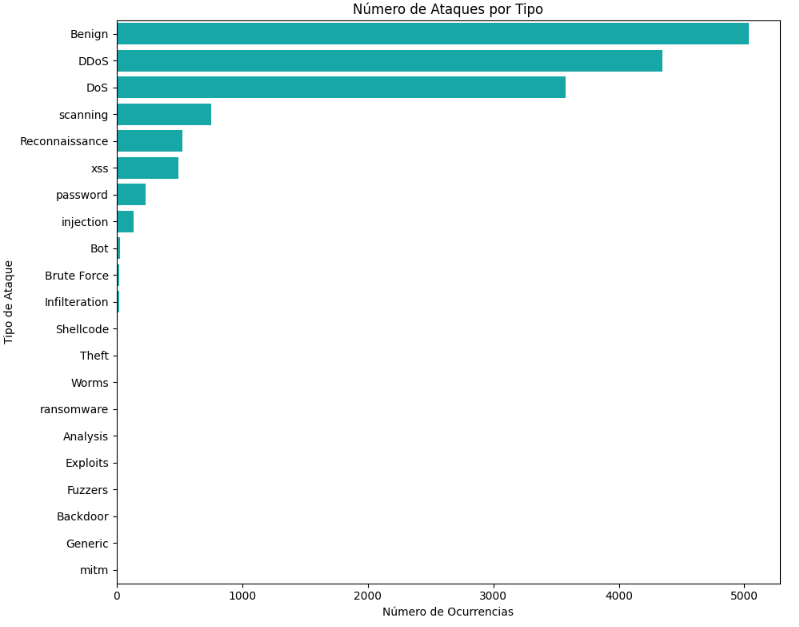
#### VALORES ATIPICOS(OUTLIERS)

El tratamiento de los valores atípicos en Aprendizaje profundo es crucial para mejorar el rendimiento del modelo, prevenir el sobreajuste y asegurar la estabilidad en su entrenamiento. Los valores atípicos pueden distorsionar procesos de normalización y escalado de datos, impactando negativamente la interpretación de resultados y la robustez del modelo. Además, gestionar adecuadamente estos valores puede optimizar la eficiencia computacional, reduciendo el ruido y facilitando un aprendizaje más efectivo. Sin embargo, es importante analizar si los ‘outliers’ reflejan patrones significativos antes de decidir cómo manejarlos, ya que no siempre su eliminación es la mejor opción.

#### MUESTREO ESTRATIFICADO

Haciendo uso de la función “sample()” de Python se realiza un muestreo estratificado. Este es un método de muestreo en el que se divide la población total en subgrupos homogéneos (o estratos) y se extraen muestras aleatorias de cada estrato. El objetivo es garantizar que cada subgrupo esté adecuadamente representado en la muestra final. Se toman subgrupos del conjunto de datos en subconjuntos equivalente al 0.1% ciento de los datos originales es decir aproximadamente 15202 registros.





### SELECCIÓN DE CARACTERISTICAS

La selección de características es el proceso de elegir características de un conjunto de datos con el objetivo de que estos se ajusten de manera más adecuada al problema en cuestión. Se realiza la selección de características con el fin de mejorar el rendimiento predictivo de un modelo al reducir la influencia del ruido originado por características que no son necesarias para la predicción. Esto, a su vez, contribuye a disminuir las demandas computacionales y a mejorar la interpretabilidad y comprensión de los resultados obtenidos.

La selección de características se realiza con una variedad de técnicas una de las mas comunes es construir una clasificación con una métrica de utilidad de característica, una función que mide las asociaciones entre una característica y el objetivo. Mediante esta métrica se puede elegir un conjunto más pequeño de las características más útiles para desarrollar inicialmente.

#### GRUPOS DE CARACTERISTICAS

Para reducir la dimensionalidad del conjunto de datos con 46 características y prepararlo para entrenar un modelo de detección de ataques DDoS, se pueden utilizar varios métodos de selección y reducción de características se hará uso de métodos de filtro y envoltura con el fin de crear varios grupos de características y evaluar el rendimiento del modelo con cada uno de estos.

**Correlación de Pearson:** La correlación de Pearson es una medida estadística que evalúa la relación lineal entre dos variables continuas. Se utiliza para cuantificar cuán fuerte y en qué dirección se relacionan dos variables. El coeficiente de correlación de Pearson, denotado como "r", varía en el rango de -1 a 1.

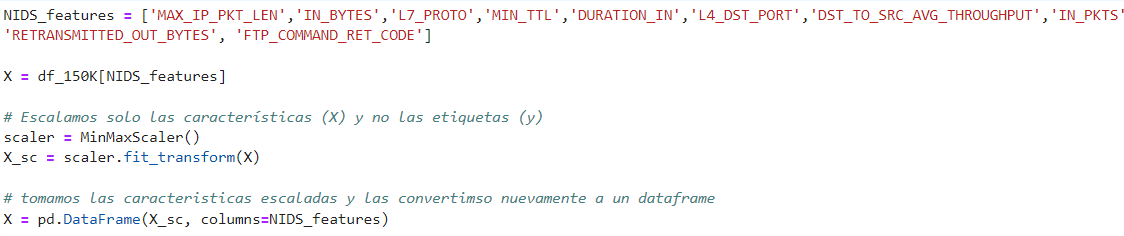
**Información Mutua:** Es una métrica univariable que se utiliza en una variedad de aplicaciones, como selección de características, análisis de datos, clasificación y clustering. Tiene la ventaja de poder detectar cualquier tipo de relación, mientras que la correlación sólo detecta relaciones lineales. La información mutua (IM) entre dos cantidades es una medida de hasta qué punto el conocimiento de una cantidad reduce la incertidumbre sobre la otra. La incertidumbre se mide utilizando una cantidad de la teoría de la información conocida como "entropía".

**Eliminación de Características Recursiva (RFE):** es una técnica de selección de características en aprendizaje automático que comienza entrenando un modelo con todas las características, calcula la importancia de cada una y elimina la menos importante en cada iteración. Este proceso se repite hasta alcanzar un criterio de parada, lo que resulta en un conjunto final de características óptimas que permiten un modelo más eficiente y preciso.

**PCA:** El análisis de componentes principales es una técnica de selección de características que reduce la dimensionalidad de un conjunto de datos al identificar y eliminar la información redundante o menos relevante. PCA transforma las características originales en un nuevo conjunto de características no correlacionadas, llamadas componentes principales, que capturan la mayor variabilidad en los datos. PCA normalmente se aplica a datos estandarizados. PCA solo funciona con funciones numéricas, como cantidades o recuentos.

#### NORMALIZACIÓN

Se realiza el Escalado de características utilizando la función MinMaxScaler de la librería ScikitLearn. Usualmente, se escalan las características para que todas tengan el mismo rango, típicamente [0,1], para que ninguna característica domine sobre las otras simplemente debido a su escala. Este proceso puede ayudar a ciertos algoritmos (como las redes neuronales, SVM, K-means, etc.) a converger más rápidamente y/o a actuar de manera más eficiente. Cuando se trabaja con características que tienen escalas muy diferentes, algunos algoritmos pueden tener dificultades para converger. Esto significa que pueden requerir más iteraciones o tiempo para llegar a una solución óptima o pueden no converger en absoluto. La normalización también se realiza para realizar el análisis de componentes de componente principales PCA para reducir la dimensionalidad del Dataset.



#### CLASIFICACION Y CODIFICACION VARIABLES CATEGORICAS Y NUMERICAS

Diferenciar entre variables categóricas y numéricas en un dataset es esencial para un análisis adecuado y la modelización. Las categóricas representan etiquetas sin un orden específico, como género o color, mientras que las numéricas son valores medibles en una escala, ya sean continuos o discretos. Estas distinciones guían la elección de técnicas de visualización, preprocesamiento y análisis estadístico. Por ejemplo, las categóricas pueden necesitar codificación para algoritmos de machine learning, y los tests estadísticos varían según el tipo de variable. Asimismo, la interpretación de resultados en modelos depende del tipo de variable, haciendo fundamental su correcta identificación y tratamiento.

Clasificaremos las variables en dos categorías principales: categóricas y numéricas. Dividir las variables de un dataset en categóricas y numéricas es crucial por diversas razones relacionadas con la naturaleza de los datos, el análisis y la modelización. Por lo general, las direcciones y puertos IP son tratadas como categóricas, aunque técnicamente son numéricas. Pero debido a su naturaleza y uso, se manejan comúnmente como categóricas. Las demás variables que se relacionan con conteos, tamaños, velocidades, y duraciones son consideradas numéricas.

#### Categóricas:

|  |  |  |
| --- | --- | --- |
| **Feature** | **Description** | **Feature,Description** |
| IPV4\_SRC\_ADDR | IPv4 source address | Las direcciones IP actúan como etiquetas únicas, no valores numéricos. |
| IPV4\_DST\_ADDR | IPv4 destination address | Las direcciones IP actúan como etiquetas únicas, no valores numéricos. |
| L4\_SRC\_PORT | IPv4 source port number | Aunque son números, representan tipos de servicios y aplicaciones específicas. |
| L4\_DST\_PORT | IPv4 destination port number | Similar al puerto de origen, indica servicios y no tiene un valor numérico inherente. |
| PROTOCOL | IP protocol identifier byte | Identifica protocolos específicos, no tiene un significado cuantitativo. |
| L7\_PROTO | Layer 7 protocol (numeric) | Aunque es numérico, identifica protocolos específicos. |
| ICMP\_TYPE | ICMP Type \* 256 + ICMP code | Representa tipos específicos de mensajes ICMP. |
| ICMP\_IPV4\_TYPE | ICMP Type | Identifica tipos de mensajes ICMP. |
| DNS\_QUERY\_ID | DNS query transaction Id | Es una etiqueta única para transacciones DNS. |
| DNS\_QUERY\_TYPE | DNS query type (e.g. 1=A, 2=NS..) | Representa tipos específicos de consultas DNS. |
| FTP\_COMMAND\_RET\_CODE | FTP client command return code | Representa respuestas específicas a comandos FTP. |

#### Numéricas:

|  |  |  |
| --- | --- | --- |
| **Feature** | **Description** | **Feature,Description** |
| IN\_BYTES | Incoming number of bytes | Representa una cantidad cuantificable de bytes entrantes. |
| OUT\_BYTES | Outgoing number of bytes | Representa una cantidad cuantificable de bytes salientes. |
| IN\_PKTS | Incoming number of packets | Cuantifica los paquetes entrantes. |
| OUT\_PKTS | Outgoing number of packets | Cuantifica los paquetes salientes. |
| FLOW\_DURATION\_MILLISECONDS | Flow duration in milliseconds | Mide el tiempo de duración del flujo en milisegundos |
| TCP\_FLAGS | Cumulative of all TCP flags | Representa una suma acumulada de indicadores TCP. |
| CLIENT\_TCP\_FLAGS | Cumulative of all client TCP flags | Suma acumulada de indicadores TCP del cliente. |
| SERVER\_TCP\_FLAGS | Cumulative of all server TCP flags | Suma acumulada de indicadores TCP del servidor. |
| DURATION\_IN | Client to Server stream duration (msec) | Esta variable representa la duración de una conexión o flujo en una dirección, probablemente del cliente al servidor. Es numérica porque es una medida cuantificable en milisegundos o segundos. |
| DURATION\_OUT | Client to Server stream duration (msec) | Al igual que DURATION\_IN, esta representa la duración pero en la dirección opuesta, probablemente del servidor al cliente. También es numérica debido a su naturaleza cuantificable. |
| MIN\_TTL | Min flow TTL | Mide el tiempo mínimo de vida del paquete. |
| MAX\_TTL | Max flow TTL | Mide el tiempo máximo de vida del paquete. |
| LONGEST\_FLOW\_PKT | Longest packet (bytes) of the flow | Tamaño en bytes del paquete más largo del flujo. |
| SHORTEST\_FLOW\_PKT | Shortest packet (bytes) of the flow | Tamaño en bytes del paquete corto del flujo. |
| MIN\_IP\_PKT\_LEN | Len of the smallest flow IP packet observed | Tamaño en bytes del paquete IP más pequeño observado. |
| MAX\_IP\_PKT\_LEN | Len of the largest flow IP packet observed | Tamaño en bytes del paquete IP más grande observado. |
| SRC\_TO\_DST\_SECOND\_BYTES | Src to dst Bytes/sec | Representa la tasa de transferencia de bytes de origen a destino por segundo. |
| DST\_TO\_SRC\_SECOND\_BYTES | Dst to src Bytes/sec | Representa la tasa de transferencia de bytes de destino a origen por segundo. |
| RETRANSMITTED\_IN\_BYTES | Number of retransmitted TCP flow bytes (src->dst) | Cuantifica los bytes TCP retransmitidos del origen al destino. |
| RETRANSMITTED\_IN\_PKTS | Number of retransmitted TCP flow packets (src->dst) | Cuantifica los paquetes TCP retransmitidos del origen al destino. |
| RETRANSMITTED\_OUT\_BYTES | Number of retransmitted TCP flow bytes (dst->src) | Cuantifica los bytes TCP retransmitidos del destino al |
| RETRANSMITTED\_OUT\_PKTS | Number of retransmitted TCP flow packets (dst->src) | Cuantifica los bytes TCP retransmitidos del destino al |
| SRC\_TO\_DST\_AVG\_THROUGHPUT | Src to dst average thpt (bps) | Tasa promedio de transferencia de origen a destino en bits por segundo. |
| DST\_TO\_SRC\_AVG\_THROUGHPUT | Dst to src average thpt (bps) | Tasa promedio de transferencia de destino a origen en bits por segundo. |
| NUM\_PKTS\_UP\_TO\_128\_BYTES | Packets whose IP size <= 128 | Cuantifica los paquetes según su tamaño, en este caso aquellos cuyo tamaño IP es menor o igual a 128 bytes. |
| NUM\_PKTS\_128\_TO\_256\_BYTES | Packets whose IP size > 128 and <= 256 | Cuantifica los paquetes cuyo tamaño IP es mayor que 128 bytes pero menor o igual a 256 bytes. |
| NUM\_PKTS\_256\_TO\_512\_BYTES | Packets whose IP size > 256 and <= 512 | Cuantifica los paquetes cuyo tamaño IP está entre 256 y 512 bytes. |
| NUM\_PKTS\_512\_TO\_1024\_BYTES | Packets whose IP size > 512 and <= 1024 | Cuantifica los paquetes cuyo tamaño IP está entre 512 y 1024 bytes. |
| NUM\_PKTS\_1024\_TO\_1514\_BYTES | Packets whose IP size >1024 and <= 1514 | Cuantifica los paquetes cuyo tamaño IP está entre 512 y 1024 bytes. |
| TCP\_WIN\_MAX\_IN | Max TCP Window (src->dst) | Representa el tamaño máximo de la ventana TCP desde el origen al destino. |
| TCP\_WIN\_MAX\_OUT | Max TCP Window (dst->src) | Representa el tamaño máximo de la ventana TCP desde el destino al origen. |
| DNS\_TTL\_ANSWER | TTL of the first A record (if any) | Representa el tiempo de vida (TTL) en un registro DNS de respuesta. Es numérico porque el TTL es una medida de tiempo en segundos. |

#### INSPECCION VISUAL

#### Características Categóricas:

* **IPv4 source address y IPv4 destination address**: Estas direcciones IP pueden ayudar a identificar patrones de tráfico inusuales o fuentes de ataque.
* **IPv4 source port number y IPv4 destination port number**: Monitorear los puertos involucrados puede ayudar a detectar ataques dirigidos a servicios específicos.
* **IP protocol identifier byte**: Puede ayudar a identificar el protocolo de capa de red utilizado en la comunicación.
* **ICMP Type y ICMP code**: Estas características pueden ser útiles para detectar ataques ICMP, como ataques de ping de la muerte.
* **DNS query transaction Id y DNS query type**: Pueden proporcionar información sobre consultas DNS anómalas que podrían ser parte de un ataque.

#### Características Numéricas:

* **Flow duration in milliseconds**: Puede indicar la duración de un flujo, y una duración inusualmente corta o larga puede ser indicativa de un ataque.
* **Cumulative of all TCP flags, Cumulative of all client TCP flags y Cumulative of all server TCP flags**: Estas características pueden ayudar a identificar patrones inusuales en las banderas TCP, como un gran número de conexiones SYN.
* **Number of retransmitted TCP flow bytes y Number of retransmitted TCP flow packets**: La detección de retransmisiones excesivas podría indicar un ataque de inundación SYN.
* **Src to dst average thpt (bps) y Dst to src average thpt (bps):** Estas características pueden ayudar a detectar patrones de tráfico inusuales o picos de uso de ancho de banda.
* **Max TCP Window (src->dst) y Max TCP Window (dst->src):** Pueden indicar problemas en la comunicación TCP, como ventanas de congestión inusuales.
* **TTL of the first A record**: Puede ser útil para detectar consultas DNS inusuales o intentos de resolver nombres de dominio maliciosos.

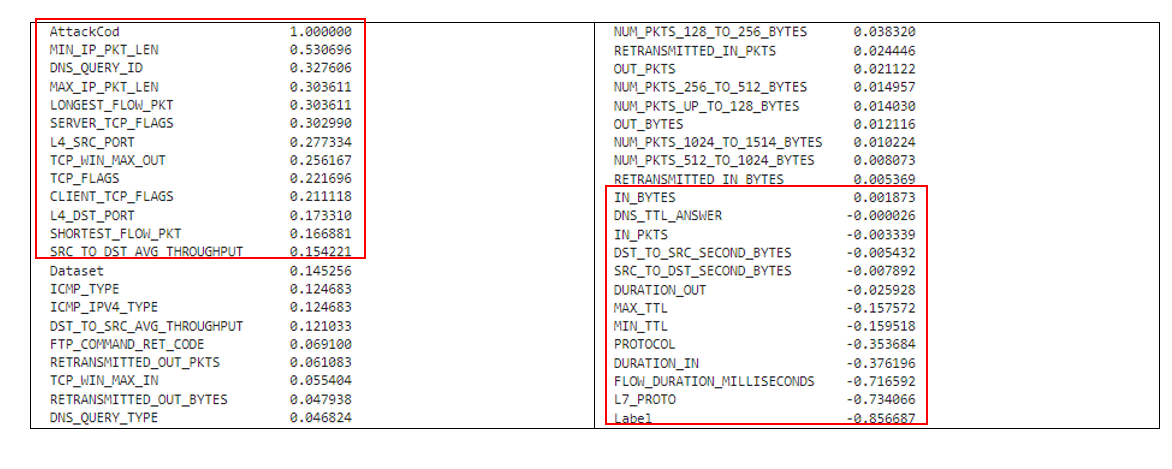
#### CORRELACION DE PEARSON

Un gráfico de correlación, típicamente visualizado como un mapa de calor, puede ser una herramienta útil al decidir qué características (features) incluir en un modelo de deep learning o cualquier otro modelo de machine learning. Una correlación cercana a 1 o -1 sugiere una fuerte relación lineal entre dos características. Una correlación cercana a 0 indica una débil relación lineal.

Si dos características están altamente correlacionadas (es decir, cerca de 1 o -1), es posible que contengan información redundante. En tales casos, puede considerarse eliminar una de las dos características para reducir la dimensionalidad y evitar la multicolinealidad, que puede hacer que el modelo sea inestable o más difícil de interpretar. Cada característica se correlaciona con la variable objetivo (la que se desea predecir). Las características que tienen una correlación muy baja con la variable objetivo podrían no ser muy útiles para la predicción y podrían ser candidatas a eliminarse. Sin embargo, se debe tener cuidado con este enfoque, ya que la correlación lineal no captura relaciones no lineales.

Al imprimir la tabla de correlaciones con la variable objetivo AttackCod podemos observar las características con mayor correlación positiva y negativa.

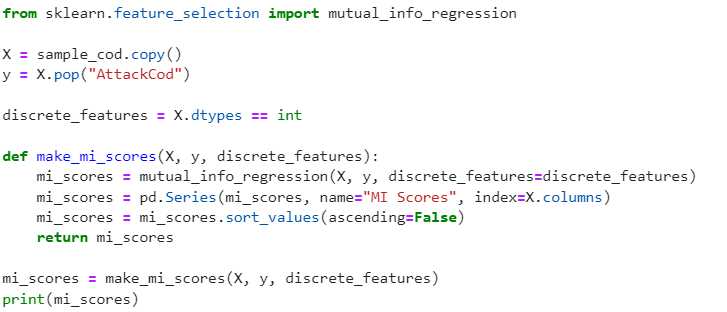
|  |  |
| --- | --- |
|  |  |



#### INFORMACION MUTUA

Se realiza el cálculo de la información mutua para todas las características respecto a la variable objetivo que en este caso son los ataques. La información mutua es una cantidad o métrica de la teoría de la información que tiene ciertas ventajas respecto a la correlación debido a que permite encontrar relaciones lineales y no lineales entre dos variables. Para la implementación de este algoritmo se utilizó el método mutual\_info\_regression de Scikit-learn el cual permite calcular la información mutua para variables discretas y continuas en nuestro caso todas las características fueron transformadas a entero por lo se utiliza solo para este caso.

Se creo una función para el cálculo de la información mutua, esta función tiene como parámetros las variables que fueron asignadas A ‘X’ y la variable objetivo ‘y’.



|  |  |
| --- | --- |
|  |  |

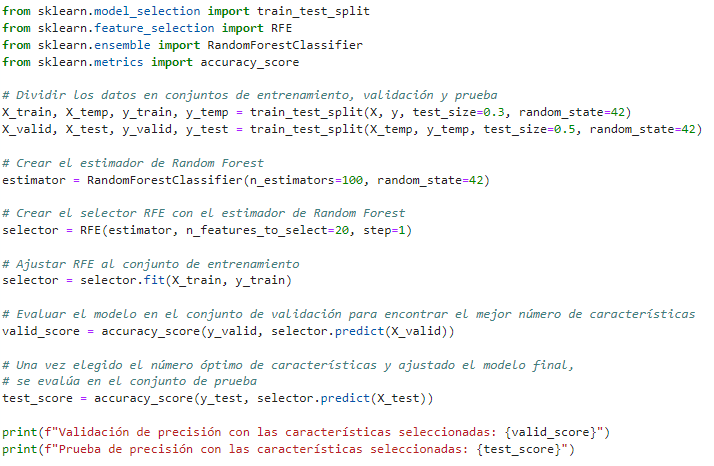
La selección de características es un proceso fundamental en la preparación de datos para el entrenamiento de modelos de aprendizaje automático. Esta etapa implica identificar aquellas variables que proporcionan la mayor cantidad de información útil para la predicción de una variable objetivo. En el contexto de estos resultados de Información Mutua (MI Scores), podemos observar que características como MAX\_IP\_PKT\_LEN, LONGEST\_FLOW\_PKT y SRC\_TO\_DST\_SECOND\_BYTES tienen los valores más altos de información mutua. Esto sugiere que estas variables tienen una mayor relación con la variable objetivo y, por tanto, podrían ser más relevantes para el modelo. La alta puntuación indica que los cambios en estas características tienen una gran influencia en la capacidad del modelo para predecir correctamente el resultado deseado. Por otro lado, algunas características como FTP\_COMMAND\_RET\_CODE y DURATION\_OUT tienen valores más bajos de información mutua, lo que indica que proporcionan menos información predictiva sobre la variable objetivo.

#### ELIMINACIÓN DE CARACTERÍSTICAS RECURSIVA (RFE)

Se utilizoel algoritmo Recursive Feature Elimination (RFE) junto con un clasificador de bosque aleatorio (Random Forest Classifier) para mejorar un modelo predictivo de clasificación.El uso de RFE puede capturar la importancia de las características en un problema de clasificación complejo y RFE puede iterativamente optimizar el conjunto de características para mejorar la precisión del modelo. El proceso de eliminación de características recursiva tiene una serie de pasos:

1. Entrenar Modelo Base: se entrena un modelo con todas las características del conjunto de datos. El tipo de modelo utilizado depende del problema y puede ser cualquier algoritmo de aprendizaje automático.
2. Ranking de Características: Después de entrenar el modelo base, se obtiene una puntuación o ranking de importancia para cada característica.
3. Eliminación de Características: Se elimina la característica menos importante según el ranking obtenido en el paso anterior.
4. Entrenamiento Iterativo: El modelo se vuelve a entrenar con el conjunto de datos reducido, que ahora contiene una característica menos. Este proceso se repite de manera iterativa, eliminando una característica en cada iteración, hasta que se alcanza un criterio de parada predefinido.
5. Evaluación del Rendimiento: Se evalúa el rendimiento del modelo en un conjunto de validación o prueba en cada iteración. Esto permite determinar si la eliminación de características ha mejorado o degradado el rendimiento del modelo.
6. Selección de Características Óptimas: Finalmente, se selecciona el conjunto óptimo de características que proporciona el mejor rendimiento en función del criterio de evaluación establecido.

Para la implementación de este algoritmo primero se realiza una división de los datos en conjuntos de entrenamiento, validación y prueba con un tamaño de prueba del 30% para el conjunto de entrenamiento y validación y luego divide el restante 70% por la mitad para la validación y prueba. Ajusta RFE al conjunto de entrenamiento para encontrar el mejor conjunto de características. Evalúa el modelo en el conjunto de validación para encontrar el mejor número de características utilizando la precisión como métrica. Evalúa el modelo final en el conjunto de prueba para obtener la precisión de las predicciones con las características seleccionadas.



Se inicializa un clasificador de bosque aleatorio con 100 árboles y una semilla aleatoria para la reproducibilidad (random\_state=42). Configura RFE con el clasificador de bosque aleatorio como el estimador base y especifica que se desean seleccionar las 20 características más importantes. El parámetro step=1 indica que RFE eliminará una característica en cada iteración para determinar el conjunto de características más importantes. Ajusta RFE al conjunto de datos completo X y y para obtener el ranking de las características.

Imprime la precisión de validación y la precisión de prueba para ver cómo se desempeña el modelo con el número de características seleccionado por RFE. Finalmente se obtiene y muestra las características seleccionadas por RFE.

### 

#### PCA

El Análisis de Componentes Principales (PCA) es una técnica estadística utilizada en proyectos de aprendizaje profundo principalmente para la reducción de dimensionalidad. En el contexto de el proyecto que se está realizando el conjuntos de datos contiene un gran número de variables o características en total 43, muchas de las cuales pueden estar correlacionadas o no ser relevantes para el problema en cuestión. PCA ayuda a simplificar estos conjuntos de datos al transformar las variables originales en un nuevo conjunto de variables, llamadas componentes principales, que son ortogonales (no correlacionadas) entre sí. Esto se logra al encontrar las direcciones (componentes) que maximizan la varianza en los datos. Reducir la cantidad de variables no solo facilita la visualización y el análisis de los datos, sino que también puede mejorar el rendimiento del modelo de aprendizaje profundo al reducir el ruido y la complejidad, acelerar el entrenamiento y evitar el sobreajuste.

## Implementación De Un Algoritmo De Aprendizaje Supervisado Basado En Una Red Neuronal Para Modelar El Conjunto De Datos.

## Análisis Estadístico De Los Resultados Obtenidos Utilizando El Modelo Y Comparación De Su Desempeño Frente A Otra Técnica Reportada En El Estado Del Arte.

.

# Resultados

Se esperan 4 sub-secciones de resultados: Propuesta definitiva (Diseño definitivo) de solución al problema planteado; Restricciones de la Solución; validación de la solución (resultados de pruebas hechas a la solución propuesta para verificar el cumplimiento de los requerimientos); y Evaluación del impacto de la solución propuesta

# Conclusiones y Recomendaciones

Presentación resumida de los aspectos encontrados en el proyecto que van más allá de los aspectos factuales y específicos del mismo. Esta sección se nutre de las implicaciones del proyecto en la práctica, de las lecciones metodológicas aprendidas en la ejecución del proyecto, de las limitaciones del proyecto, de los aspectos no resueltos del proyecto y nuevas preguntas creadas a partir del mismo, propuestas de nuevos proyectos a partir de los resultados actuales.

# Referencias

[x1] Amazon Web Services. (n. d.). ¿Qué es el Internet de las cosas (IoT)? Recuperado de https://aws.amazon.com/es/what-is/iot/

# Anexos

De ser necesario, se pueden preparar Anexos en orden alfabético (Anexo 1, Anexo 2, etc.). Pueden ser utilizados para presentar mayor detalle sobre algún aspecto del documento sin romper el hilo conductor del texto principal. Por ejemplo, se puede usar para presentar el formato de encuesta que se espera usar en el proyecto, o un protocolo de observación, etc.

**PAUTAS PARA LA REDACCIÓN DEL DOCUMENTO**

Se propone el seguimiento de las normas de la APA o IEEE. En general se espera que la ortografía sea impecable (no confiarse del corrector de MS Word). Las propuestas deben estar bien presentadas; se debe cuidar: la unidad del estilo del texto, títulos y sub-títulos a lo largo del documento.

Cada capítulo debe comenzar en una nueva página. El fin de una sección y el encabezado de la próxima no deben ser separados por espacios adicionales. Cuándo una sección comienza al final de la página, ésta debe ser trasladada a la página siguiente si el primer párrafo de la sección no alcanza a tener dos líneas de texto.

La extensión del documento no debe superar las 60 páginas sugerido (70 páginas máximo) sin incluir los preliminares (portada, contraportada, índices, dedicatoria, glosario, siglas); Listado de referencias bibliográficas ni Anexos

**Estilo y formato:**

***Redacción****:* La propuesta debe ser redactada en tercera persona.

***Texto y formato de los párrafos:***La letra del documento es Times New Roman tamaño 12 o equivalente, el interlineado es sencillo. Además, se deben parametrizar el párrafo con los siguientes valores:

* Alineación: Justificada.
* Espaciado: Anterior: 12 pto, Posterior: 12 pto, Interlineado: 1,0
* Viñetas y significado de variables y parámetros de fórmulas: Espaciado (Anterior: 6 pto, Posterior: 6 pto)

***Títulos:*** A continuación, una descripción de los tipos de títulos y sus características:

* Título 1 (Sección primaria o Capítulo): Times New Roman Negrita tamaño 14
* Titulo 2 (sección secundaria o Sub-capítulo): Times New Roman Negrita tamaño 13.
* Título 3 (sección terciaria): Times New Roman Negrita tamaño 12

***Número de Página***Todas las páginas deben estar numeradas excepto la portada. Las páginas previas al capítulo de introducción deben ser numeradas en números romanos (i, ii, iii, iv, v,…) en minúsculas, mientras que a partir de la introducción debe ser arábiga (1,2,3…).

***Notas al pie de página****.* Las notas al pie de página tienen por finalidad brindar una información extra o aclarar un concepto dentro del cuerpo principal. Son una herramienta útil para agregar contenido que para un lector lego puede ser de utilidad para interpretar o entender lo que se está presentando. Las notas al pie de página deberán ser referenciadas utilizando un superíndice y la nota al pie de página deberán tener un tamaño de letra entre 10 a 8. Utilizar la funcionalidad pie de página para esta parte del texto.

***Figuras y Tablas en el texto.***La resolución adecuada de fotos y figuras que permitan leer y entender el mensaje que se desea entregar. Toda tabla y figura debe tener un título. Además, toda tabla y figura debe ser anunciada en el texto del documento antes de aparecer en el mismo, no olvide referenciarla

*Ejemplo:*

Se evaluó la simulación de la marcha normal, al igual que las diferentes fases de un ciclo, trazando la flexión y extensión de la cadera contra la flexión y extensión de la rodilla. La cadera está en el eje *x* y la rodilla está en el eje *y*; La magnitud de los gráficos se indica en ángulos. El resultado del ciclograma mostrado en la Figura 6 concuerda con los resultados reportados en la literatura, ya que los ángulos de rodilla y cadera están dentro de los límites de los valores observados en estudios previos.

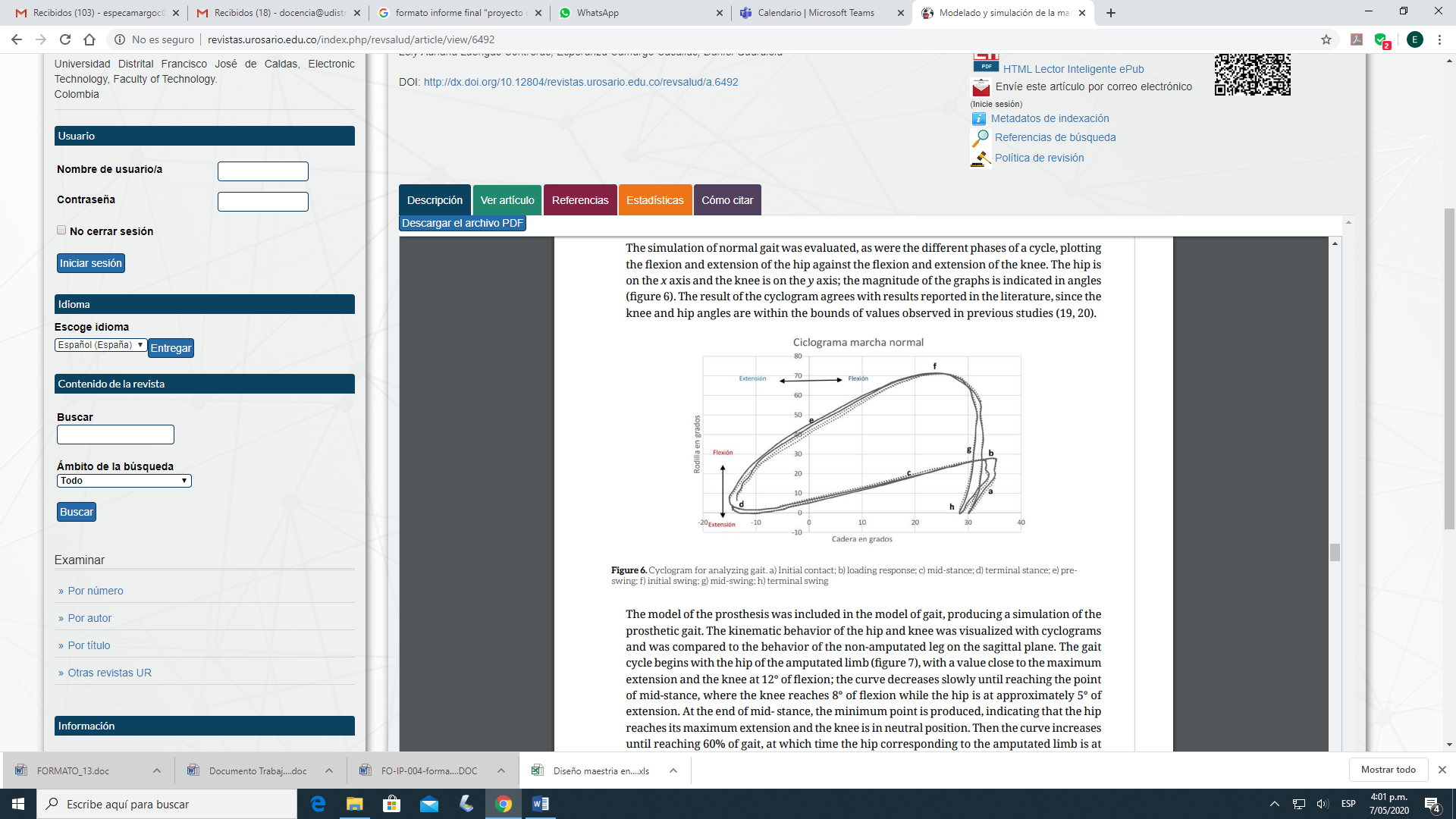


Figura 6. Ciclograma para analizar la marcha. a) Contacto inicial; b) Respuesta de carga; c) Apoyo media; d) Apoyo terminal; e) Prebalanceo f) Balanceo inicial; g) Balanceo medio; h) Balanceo terminal. (Camargo, 2018)

En el caso de las tablas se sigue un criterio similar a las figuras, el tamaño mínimo de la letra al interior de la tabla es 11.

Ejemplo:

Como se muestra en la Tabla 1, los valores de *t* para un nivel de confidencia del 95%, depende de los grados de libertad asociados con la desviación estándar.

|  |  |
| --- | --- |
| **Grados de Libertad** | **Nivel de confidencia** |
| 2 | 4.303 |
| 4 | 2.776 |
| 6 | 2.447 |

Tabla 3. Variables de medición. Fuente: El Autor

***Ecuaciones y Fórmulas.***Las ecuaciones deben ser elaboradas en un editor de ecuaciones apropiado. Si utiliza Word, use o bien Microsoft Editor de Ecuaciones o MathType. Numere las ecuaciones consecutivamente, deben estar centradas, por orden de aparición, con números arábigos entre paréntesis justificado al margen derecho. Las ecuaciones al igual que las figuras y tablas deben ser anunciadas en el texto del documento antes de aparecer en el mismo.

Ejemplo:

La curva de frecuencia (1) de los valores medios está centrada alrededor del valor límite medioy tiene un factor de escala

|  |  |
| --- | --- |
|  | (1) |

***Citaciones***Las citaciones son referencias a textos realizados por otras personas, las podemos clasificar en tres grandes grupos:

* Formales: donde se transcriben literalmente textos. Es imprescindible que éstas sean colocadas entre comillas e indicar su fuente.
* Conceptuales: en este caso se reproduce el concepto utilizando palabras propias, es una síntesis personal de una idea basándose en otra idea, es necesario referenciar usando normas APA o IEEE.

***Referencias*** Las referencias bibliográficas constituyen una parte importante del texto donde se detallan todas las fuentes consultadas en el trabajo que se está presentando. Es importante detallarlo adecuadamente para que posteriormente otros lectores puedan realizar búsquedas de esas referencias.

Las referencias deberán ser ordenadas considerando el apellido del primer autor, en caso de que el autor tenga más de un artículo o trabajo referenciado en el informe se debe ordenar por el año de publicación. Para mayor información sobre la forma de referenciar se les sugiere que revisen las normas APA o IEEE.

***Especificando las referencias***

Considere los siguientes ejemplos que se detallan a continuación para realizar las referencias. El autor debe dejar un espacio entre una y otra referencia.

**Referencias de libros:**

Apellido autor, Iniciales nombre autor, (Año), *Título en cursiva,*Ciudad y país, Editorial.

Hacyan, S., (2004), *Física y metafísica en el espacio y el tiempo. La filosofía en el laboratorio*, México DF, México: Fondo nacional de cultura económica.

**Referencia de páginas web:**

Apellido, A. A. (Fecha). Título de la página. Lugar de publicación: Casa publicadora. Dirección de donde se extrajo el documento (URL).

Argosy Medical Animation. (2007-2009). Visible body: Discover human anatomy. New York, EU.: Argosy Publishing. Recuperado de <http://www.visiblebody.com>.

Nombre del artículo, (s. f). En xxxxx. Recuperado el X de MES de AÑO de <http://xxx.xxxxxxxxxx.xx/xxxx/xxx>.

**Referencia revistas científicas:**

Apellido autor1, Iniciales nombre autor1., Apellido autor2, Iniciales nombre autor2., …y Apellido autorN, Iniciales nombre autor. (Año). Nombre del trabajo, revista, volumen(número del volumen), paginas.

Coruminas, M., Ronecro, C., Bruguca, E., y Casas, M. (2007). Sistema dopaminérgico y adicciones, *Rev Mukuel*, 44(1), 23-31.

Arshinder, K., Kanda, A., y Deshmukh, S. G. (2011). A Review on Supply Chain Coordination: Coordination Mechanisms, Managing Uncertainty and Research Directions. In T.-M. Choi & T. C. E. Cheng (Eds.), Supply Chain Coordination under Uncertainty SE - 3 (pp. 39–82). Springer Berlin Heidelberg. doi:10.1007/978-3-642-19257-9\_3.

**Referencias congresos y seminarios:**

Autor, A., & Autor, A. (año). Título de la ponencia, Título del simposio o congreso. Simposio o conferencia llevado a cabo en el congreso Nombre de la organización, Lugar.

Rojas, C., y Vera, N. (2013). ABMS Automatic BLAST for Massive Sequencing), 2° Congreso Colombiano de Biologia Computacional y Bioinformática CCBCOL. Congreso llevado a cabo en Manizales, Colombia.