UNIVERSIDAD DISTRITAL

**“Francisco José de Caldas”**

**Facultad Tecnológica**



**Formato para Propuesta de Proyecto de Grado de Tecnología Electrónica**

|  |
| --- |
| **Modalidad**  x  **PASANTÍA MONOGRAFÍA INVESTIGACIÓN** |

|  |
| --- |
| TITULO PROPUESTA Detección de ataques DDoS en redes IOT utilizando modelo de Deep Learning basado en el protocolo de red Netflow. |

|  |
| --- |
| **PROPONENTES**  Johan Andrés Herrera Reyes – 20212373001 Daniel Eduardo Cabiativa Felacio - 20202373014 |

|  |
| --- |
| **DIRECTOR**  Ing. Henry Alberto Hernandez |

|  |
| --- |
| REFERENCIA AL CONSEJO Los ataques cibernéticos han aumentado según el periódico el tiempo entre el primer periodo del año 2021 y el mismo periodo del 2022 en un 50%[1] , pero además la complejidad de estos ataques debido a que los ciber atacantes se mantienen a la vanguardia, creando técnicas de ataque cada vez más sofisticadas que utilizan incluso inteligencia artificial. Por esto es posible que pronto, el gran volumen, la sofisticación y la dificultad de detectar ciberataques sobrepase la capacidad humana. La IA es un multiplicador de fuerza, que permite que los equipos de seguridad no solo responder más rápido de lo que pueden moverse los atacantes cibernéticos, sino que también anticipar sus movimientos.  Teniendo en cuenta este panorama se plantea diseñar e implementar un modelo de Deep learning para la detección y prevención de ataques DDoS en redes IOT utilizando un conjunto de datasets estandarizados. En estos datasets se estandarizaron las características capturadas de cuatro datasets de referencia en el campo de la ciberseguridad de IOT, utilizando el protocolo Netflow. Esta estandarización permite medir el desempeño del modelo entrenado con un dataset especifico y aplicarlo en otro diferente para aplicar este tipo de modelos en entornos reales más fácilmente. |

# DATOS DE ENLACE

E-mail: decabiativaf@correo.udistrital.edu.co Teléfonos: 3162736281  
E-mail: johaherrerar@correo.udistrital.edu.co Teléfonos: 3132873456

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Espacio Exclusivo Consejo Curricular**

**APROBADO MODIFICAR RECHAZADO**

# HOJA DE ACEPTACIÓN

**TITULO**

**Detección de ataques DDoS en redes IOT utilizando modelo de Deep Learning basado en el protocolo de red Netflow.**

Observaciones.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_



\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Director del Proyecto

Henry Alberto Hernández Martinez

C:\Users\ECM\Pictures\firma.jpg

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Evaluador del Proyecto

Ernesto Cadena Muñoz

Fecha de presentación: Mayo de 2023

**INFORMACIÓN GENERAL DEL PROYECTO**

**Título:** Modelo de detección de ataques DDos para las redes IoT usando deep learning.

**Estudiantes Proponentes:**

Johan Andrés Herrera Reyes,

Daniel Eduardo Cabiativa Felacio

Total, de Estudiantes: 2

**Línea de Investigación**: Redes y sistemas de telecomunicaciones

**Descriptores / Palabras claves:** Modelo, Ciberataques, DDoS, Deep learning

**Modalidad**

Pasantía: Monografía: X Investigación:

**Lugar de Ejecución del Proyecto:** Bogotá D.C

**Nombre de la Entidad:** Universidad Distrital Francisco José de Caldas.

Entidad Pública: X Entidad Privada:

Empresa agrícola Empresa Industrial Empresa servicios

Grupo investigación Otras (Indicar cuál)

Ciudad: Bogotá DC Departamento: Bogotá

Dirección: [Carrera 7 # 40B - 53](https://www.google.com.co/maps/place/Cra.+7+%2340b-53,+Bogot%C3%A1/@4.6280856,-74.0674698,17z/data=!3m1!4b1!4m5!3m4!1s0x8e3f9a287591013f:0x5cce5fbab6b77b9b!8m2!3d4.6280856!4d-74.0652811?hl=es)

Teléfono:(601)3239300 ext:1421 Fax:

Correo Electrónico: tecelectronica@udistrital.edu.co

Sede de la Entidad: Facultad Tecnológica Nit: 899999230-7

**Duración del Proyecto (meses): 6**

**Valor total del proyecto: $ 14’509.000**

**Modalidad - Investigación**

**Modalidad - Pasantía:**

Observaciones:

## 

|  |
| --- |
| RESUMEN EJECUTIVO Según el informe Deloitte 2022 hay un aumento del tráfico de redes después de la pandemia y un crecimiento exponencial del espacio digital donde se brindan cada vez más servicios que requieren de una seguridad más eficiente y robusta, como transacciones, servicios en la nube para infraestructura de negocios, o almacenamiento de información sensible que puede ser robada[2] . Adicionalmente, con el despliegue de las redes 5g hay un aumento de dispositivos de todo tipo conectados a internet cada año, lo que se denomina el Internet de las cosas se prevé según el portal de estadísticas Statista que en 2030 habrá más de 29.000 millones de dispositivos conectados en todo el mundo y tan solo 19.000 millones de dispositivos en 2025 [3] . Con este crecimiento y despliegue de redes de dispositivos IOT a nivel comercial e industrial se requiere un gran esfuerzo para que estas cuenten con la debida seguridad porque los atacantes se encuentran en una búsqueda constante de nuevos métodos para vulnerar los sistemas y entre estas amenazas, los ataques DDoS (Distributed Denial of Service) son los más comunes y son bastante difíciles de detectar debido a su variedad y características del tráfico [4].  La IA incluyendo machine learning y más específicamente Deep learning ha probado ser una herramienta eficaz y altamente precisa para detectar y proteger las redes contra los ciberataques [5]. Sin embargo, debe avanzarse en una forma estandarizada de captura de características en los datasets de entrenamiento para que los modelos puedan ser evaluados utilizando diferentes datasets y puedan ser implementados en escenarios diversos de forma más sencilla.  En el presente trabajo se propone el diseño, la implementación y evaluación de un modelo de Deep learning que detecta y previene ataques DDoS utilizando un dataset basado en el protocolo de red Netflow el cual toma ráfagas de red en forma de flujos, y mediante estos se puede detectar los comportamientos de la red que están fuera de lo “normal” y que son el resultado de accesos no autorizados, virus, ataques, intrusiones y otras amenazas a la seguridad de la información. El proyecto tendrá un valor aproximado de $14’509.000 de pesos. |

## 2.0 DESCRIPCIÓN DEL PROYECTO

|  |
| --- |
| 2.1. Planteamiento del Problema Las redes IOT son cada vez más grandes por la gran cantidad de dispositivos de bajo coste que son capaces de conectarse a internet como cámaras, grabadoras de video, electrodomésticos también en el sector industrial sobre todo sensores y con esto aumenta la complejidad de los ataques a estas redes y también su volumen por lo que la dificultad de detectar ciberataques es cada vez mayor y sobrepasa la capacidad humana [1].  Los dispositivos IOT no están siendo diseñados para ser seguros y cuentan con una variedad de vulnerabilidades como contraseñas débiles o codificadas, falta de un proceso o mecanismos de actualización, servicios de red e interfaces de ecosistema no seguros, componentes de la aplicación IoT obsoletos o no seguros, almacenamiento y transferencia de datos no seguros a partir de estas vulnerabilidades se crean amenazas como suplantación de identidad, divulgación de información, manipulación de datos, elevación de privilegios[6].  Entre los principales ataques que explotan están vulnerabilidades están los que se realizan mediante botnets (conjunto o red de robots informáticos), que se caracterizan porque permiten realizar ataques distribuidos de denegación de servicio (DDoS), que sobresaturan el tráfico de acceso con el fin de inhabilitar o tomar el control de los dispositivos [4]. El problema de los ataques de DDoS se vuelve cada vez más difícil debido a la gran cantidad de dispositivos de IOT que se conectan a la red con poca o ninguna seguridad [7]. Los ataques DDoS estuvieron entre los principales ciberataques entre el año 2013 y 2020 como lo indica una revisión hecha en 2021 sobre la seguridad en IOT [6]. Y son bastante conocidos los ataques DDoS a servicios como Amazon web services, GitHub o también a empresas como CNN, Dell, E-TRADE, eBay Spamhaus o el proveedor de nombres de dominio DYN [8] .  La IA (Inteligencia Artificial) para crear IDS (sistemas de detección de intrusos por sus siglas en inglés) ha probado ser una herramienta eficaz y altamente precisa para detectar y proteger estas redes contra los ciberataques convirtiéndose en un multiplicador de fuerza para los grupos de ciberseguridad, sin embargo, su implementación en entornos reales tiene una serie de dificultades [5].  La IA es posible gracias a la captura de una gran cantidad de datos. Los datos de red reales son difíciles de obtener debido a cuestiones de seguridad y privacidad por lo que se desarrollan bancos de prueba para obtenerlos y mediante estos se capturan los datos que conforman los datasets para el entrenamiento de los modelos de Inteligencia artificial. Pero esta captura no es estandarizada por lo que se crean datasets de entrenamiento con características muy diferentes.  Las características de los conjuntos de datos determinan el desempeño de los modelos por lo que no se puede medir el desempeño de un modelo creado con un dataset en otro dataset ya que se crean modelos para dataset específicos y por lo tanto para entornos de prueba específicos por lo que no se pueden utilizar estos modelos en otros dataset y en otros entornos.  Por otra parte, se dan otras dificultades en los dataset existentes que se deben a la utilización de complejas técnicas de extracción, recopilación y almacenamiento que no son viables de utilizar en redes reales con un alto tráfico por lo que se necesitan utilizar formas más sencillas de capturar características de tráfico de red para crear datasets a lo que se le pueda aplicar aprendizaje profundo [9]. |
| 2.2 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 ha demostrado ser una solución prometedora, pero aún hay 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 utilizarán los conocimientos de redes específicamente en cuanto a redes de paquetes e ingeniería de tráfico, se utilizarán las herramientas en desarrollo de software y programación adquiridas entre otras utilizando el lenguaje de programación Python, y se utilizarán las habilidades para el modelamiento matemático adquiridos durante la carrera, además de los conocimientos sobre seguridad informática en cuanto a tipos de ataques. Con esto se busca aportar a la investigación de la universidad en el campo de la Inteligencia artificial para su en redes de datos. |
| **3. Estado del Arte**  **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.  Mediante el dataset UNSW-NB15 de la Universidad de Nueva Gales del Sur en Australia se construyó un conjunto de datos balanceado enfocado a los ataques DoS para después ser limpiados, normalizados, caracterizados permitan una mejora en cuenta al desempeño del modelo.  **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 set 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 electrónico o mensaje de celular en caso de detectar actividades sospechosas. La propuesta abarca todos los equipos que interconectan a la UNAM con sus dependencias externas e Internet y busca identificar rápidamente la causa de los incidentes.  **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 data set** [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. |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 4 Marcos de referencia **4.1. Marco Teórico**  En este marco teórico, 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 se define como una infraestructura que permite ofrecer servicios avanzados mediante la interconexión de objetos (físicos y virtuales) a internet y entre sí. [6] IoT utiliza plenamente las "objetos" para ofrecer servicios a todo tipo de aplicaciones aprovechando las capacidades de identificación, adquisición de datos, procesamiento y comunicación, garantizando a su vez el cumplimiento de los requisitos de seguridad y privacidad.  Los dispositivos IOT tienen una serie de características que incluyen; conectividad por WIFI, bluetooth, NFC y otras; la identificación, la adquisición y el procesamiento de datos para la toma de decisiones o para alerta; capacidad de comunicación inalámbrica con protocolos MQTT, CoAP, HTTP y otros; Sensores para capturar datos sobre movimiento, temperatura, movimientos; también escalabilidad para manejar gran cantidad de datos y un sistema de seguridad para proteger la conexión y transmisión de los datos. Además, IoT hace uso de tecnologías avanzadas como la comunicación máquina a máquina, las redes autónomas, la minería de datos y la toma de decisiones, la protección de la seguridad y la privacidad y la computación en la nube, así como tecnologías avanzadas de detección y accionamiento.  La arquitectura IOT se compone de cuatro capas principales: la capa de dispositivos, capa de servicios, capa de red y la capa de aplicaciones. La capa de dispositivos se compone de dispositivos de transporte de datos, dispositivos de adquisición de datos, de detección y accionamiento y dispositivos genéricos. La capa de servicios se compone de servicios de gestión de dispositivos, servicios de gestión de datos, servicios de gestión de seguridad y servicios de gestión de aplicaciones. La capa de red se compone de capacidades de red y capacidades de transporte. La capa de aplicaciones se compone de aplicaciones de usuario, aplicaciones de servicio y aplicaciones de gestión. 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 ataques DoS se pueden realizar de diversas maneras. Algunos de los métodos comunes son:  **Ataque de inundación de tráfico**: el atacante envía una gran cantidad de tráfico falso al servicio o recurso objetivo con el objetivo 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.  Los **Ataques de Denegación de servicios distribuidos** o (DDoS por sus siglas en inglés) son una versión más moderna de los ataques DoS. En estos ataques se utilizan múltiples dispositivos comprometidos y distribuidos geográficamente para saturar el tráfico de red de un servidor, sistema o red en particular, por esto se vuelve más difícil su detección, con el fin de hacer que el servicio sea inaccesible para los usuarios legítimos. La principal diferencia entre un ataque DDoS y un ataque DoS (Denial of Service) es que en el primero, los dispositivos utilizados para el ataque son controlados por una o varias personas, mientras que, en el segundo, el ataque se realiza desde un solo dispositivo o computadora.  El objetivo de un ataque DDoS puede variar, desde interrumpir la actividad normal de un sitio web o servicio en línea, hasta extorsionar a la víctima para que pague un rescate para detener el ataque. Para protegerse contra los ataques DDoS, es importante contar con firewalls y sistemas de detección y prevención de intrusos (IDS/IPS), así como contar con planes de contingencia y respuesta ante incidentes.  En un ataque DDoS, los atacantes suelen infectar previamente una gran cantidad de dispositivos a través de malware, creando una red de bots conocida como botnet. Luego, los atacantes utilizan esta botnet para enviar tráfico malicioso a la víctima, sobrecargando su infraestructura de red y haciéndola inaccesible. Debido a que los dispositivos IoT se están volviendo cada vez más comunes y accesibles, y muchos de ellos se conectan a Internet sin una seguridad adecuada. Esto los convierte en objetivos atractivos para los atacantes que buscan crear redes botnet, que son redes de dispositivos comprometidos que pueden ser utilizados para realizar ataques DDoS.  Los atacantes pueden usar botnets de dispositivos IoT para lanzar ataques DDoS masivos, inundando un sitio web o servicio en línea con una cantidad abrumadora de tráfico. Debido a que los dispositivos IoT a menudo tienen una capacidad limitada para procesar y transmitir datos, incluso un pequeño número de dispositivos comprometidos puede generar una gran cantidad de tráfico que puede ser suficiente para interrumpir un servicio en línea. Por lo tanto, es importante asegurar los dispositivos IoT y protegerlos contra el acceso no autorizado para evitar su uso en ataques malintencionados.  Podemos clasificar los ataques DDoS según las siguientes categorías:  **Basados en volumen**: Estos ataques 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**: Estos ataques 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**: Estos ataques se aprovechan de 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. Sistemas de Detección de Intrusos Los sistemas de detección de seguridad (IDS) y los sistemas de prevención de intrusos (IPS) son tecnologías de seguridad diseñadas para monitorear y proteger las redes informáticas de posibles ataques y amenazas. IDS monitorea el tráfico de la red en busca de patrones sospechosos y alerta a los equipos de seguridad cuando detecta actividad maliciosa, pero no toma medidas activas para detenerla. En cambio, IPS puede ir más allá y tomar medidas proactivas para bloquear o mitigar la actividad maliciosa, incluido el bloqueo de direcciones IP o la reconfiguración de las reglas del firewall [6].  Los IDS/IPS pueden funcionar en modo promiscuo, lo que significa que pueden ver todo el tráfico de red, o pueden funcionar en modo en línea, lo que significa que se encuentran en la ruta de tráfico de red y pueden detener o bloquear el tráfico sospechoso.  Los IDS/IPS utilizan diferentes métodos para detectar la actividad malintencionada. Uno de ellos es la detección basada en firmas, que compara los paquetes de datos con una base de datos de firmas conocidas de ataques. Si se encuentra una coincidencia, el IDS/IPS puede tomar medidas para bloquear el tráfico. Otro método es la detección basada en anomalías, que busca patrones de tráfico inusual o anormal que puedan indicar un ataque. Los IDS/IPS pueden aprender el comportamiento normal del tráfico de red y alertar al administrador de red cuando se detecta actividad inusual.  Los sistemas de prevención de intrusos también pueden tomar medidas activas para bloquear el tráfico malintencionado. Pueden usar técnicas como la mitigación de DDoS, que bloquea el tráfico proveniente de fuentes sospechosas y reduce la cantidad de tráfico que llega al destino. También pueden usar firewalls de aplicación web para bloquear ataques a aplicaciones específicas.  Los IDS/IPS generalmente se basan en reglas y patrones conocidos para detectar y bloquear actividades maliciosas, pero también pueden usar técnicas de análisis de comportamiento para detectar patrones inusuales en el tráfico de la red. IDS/IPS es una parte importante de la seguridad cibernética y es ampliamente utilizado por empresas y organizaciones para detectar y prevenir ataques e intrusiones en la red. Machine learning y Deep learning El aprendizaje automático o Machine learning es un subcampo de la inteligencia artificial que se centra en la creación de algoritmos que permiten que las máquinas aprendan de los datos sin tener que programarlas. El aprendizaje automático se utiliza para realizar tareas como clasificación, regresión, agrupación, detección de anomalías, reconocimiento de patrones y toma de decisiones.  El aprendizaje profundo o Deep Learning es un subcampo del aprendizaje automático que se centra en aprender y extraer características de datos complejos utilizando redes neuronales artificiales profundas. Estas redes neuronales constan de múltiples capas y se utilizan para la detección de patrones, el reconocimiento de imágenes y voz, el procesamiento del lenguaje natural y más. Entrene con grandes conjuntos de datos para realizar tareas como El aprendizaje profundo ha tenido un gran impacto en la resolución de problemas de inteligencia artificial y ha dado lugar a avances significativos en áreas como la visión artificial, la robótica y la conducción autónoma.  En la siguiente realizamos una comparación resumida de las características mas importantes de Machine Learning y Deep learning:   |  |  |  | | --- | --- | --- | |  | **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 al 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 1. Tabla comparativa ML y DL** [19].  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.  Las aplicaciones de ML y DL en problemas de seguridad según el análisis de los autores se da de la siguiente manera:   |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | | **Detección de Intrusos** | | | **Análisis de**  **Malware** | **Detección de Spam** | | **Red** | **Botnet** | **DGA** | | **Aprendizaje Profundo (DL)** | Supervisado | RNN | RNN |  | FNN  CNN  RNN |  | | No supervisado | DBN  SAE |  |  | DBN  SAE | DBN  SAE |   **Tabla 2. Técnicas de Deep learning para uso en ciberseguridad** [19]. Modelos de Deep Learning **Algoritmos supervisados en 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** por sus siglas en inglés, son un tipo de red neuronal profunda que se utiliza comúnmente en la tarea de visión por computadora, como la clasificación de imágenes. La idea detrás de una CNN es procesar la imagen de entrada a través de varias capas de convolución y pooling para extraer características de la imagen y luego alimentar estas características a capas completamente conectadas para realizar la clasificación.  Las **redes neuronales recurrentes (RNN**) son un tipo de red neuronal que se utiliza principalmente para 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.  Las **redes neuronales de memoria a largo plazo (LSTM)** son un tipo especializado de red neuronal recurrente que se utiliza para procesamiento de lenguaje natural. Estas redes son capaces de recordar información anterior durante períodos más largos y evitar el problema del desvanecimiento del gradiente.  **GRU (Gated Recurrent Unit):** Es otra variante de las RNN que también aborda el problema de las dependencias a largo plazo. Las GRU tienen una estructura simplificada en comparación con las LSTM, lo que las hace más fáciles de entrenar y computacionalmente más eficientes.  **FNN (Feedforward Neural Network**): También conocida como red neuronal de propagación hacia adelante, es la arquitectura básica de una red neuronal artificial. Consiste en múltiples capas de unidades neuronales, donde las conexiones solo se propagan en una dirección, desde las capas de entrada hasta las capas de salida. Se utiliza para tareas de clasificación y regresión.  **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 variacionales (VAE):** son redes que aprenden a modelar la distribución de los datos de entrada. Utilizan una capa de codificación que produce un vector de medias y desviaciones estándar para cada muestra de entrada. A continuación, se muestrea de la distribución para generar muestras nuevas. Se utilizan en aplicaciones como la generación de texto y la síntesis de imágenes.  **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.  **Boltzmann Machine**: Es un tipo de red neuronal estocástica que se utiliza en aprendizaje no supervisado. Las Boltzmann Machines modelan la distribución de probabilidad conjunta de los datos de entrada y aprenden a reconstruir los datos de entrada.  **DBN (Deep Belief Network):** Es una arquitectura de red neuronal que se compone de múltiples capas de unidades de restricción de Boltzmann. Cada capa se entrena de manera no supervisada y luego las capas se combinan para formar una red completa. Se utiliza principalmente para tareas de aprendizaje no supervisado, como la extracción de características.  **SAE (Stacked Autoencoder):** Es una arquitectura de red neuronal en la que múltiples capas de autoencoders se apilan de manera secuencial. Cada autoencoder aprende a reconstruir su capa de entrada y se utiliza para extraer características no lineales de los datos. Los SAE se utilizan comúnmente en tareas de aprendizaje no supervisado y pre-entrenamiento de redes neuronales profundas. Sistemas de Detección de intrusos con Machine learning y Deep learning Las dos soluciones principales utilizadas para prevenir ataques DDoS son: sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS). IDS es una precaución que no toma ninguna acción si el sistema en sí está comprometido. En su lugar, se activa una alarma. IPS es una acción de penalización en caso de que haya una intrusión.  IDS significa Sistemas de detección de intrusos. Son herramientas de seguridad de software o hardware que juegan un papel crucial para aumentar el nivel de seguridad de un sistema. Los IDS son la segunda línea de defensa después de los firewalls y se utilizan para identificar y responder a los ataques.  Los IDS se pueden clasificar en función de varios criterios. Una forma de clasificar los IDS se basa en su ubicación, que puede estar basada en el host o en la red. Los IDS basados en host detectan ataques al escuchar el tráfico, los archivos de registro y las transacciones en un host específico. Los IDS basados en red escuchan todo el tráfico dirigido a la red, registran el contenido de cada paquete de datos que pasa por la red, cortan los ataques cuando es necesario y crean informes.  Los IDS también se pueden clasificar según sus técnicas, que pueden basarse en firmas o anomalías. Los IDS basados en firmas detectan tipos de ataques conocidos al comparar el tráfico entrante con una base de datos de firmas de ataques conocidas. Los IDS basados en anomalías detectan ataques ocultos aprendiendo el comportamiento normal del sistema y marcando cualquier desviación de ese comportamiento como ataques potenciales. Los IDS también se pueden clasificar según el tiempo de procesamiento de los datos, la estructura arquitectónica y el tipo de sistema que protegen.  Algunas ventajas de un sistema de detección de intrusos (IDS) incluyen: Detección temprana: IDS puede detectar ataques que otros mecanismos de seguridad no pueden prevenir; Recopilar información detallada: IDS proporciona información detallada sobre un ataque, incluido el tipo de ataque, el origen del ataque y el objetivo del ataque; Calidad de la evidencia: IDS proporciona evidencia de alta calidad que se puede utilizar para enjuiciar a un atacante. Sin estos sistemas también tienen alguna debilidad como la fragmentación de paquetes y los ataques de sincronización, la combinación de órdenes de escaneo y el secuestro de paquetes. Puede ser difícil entender si un paquete que llega a la computadora es para un ataque o para una comunicación normal. La detección de ataques es difícil y computacionalmente intensiva.  Los IDS constan de tres componentes principales: 1. Recopilación de datos: este componente es responsable de rastrear los flujos de la red y recopilar datos. 2. Selección/conversión de características: los datos recopilados se utilizan para identificar las características y se crea un vector de características. 3. Motor de decisiones: este componente es la parte crítica de un sistema IDS, que decide si el vector de características convertido se ajusta a la definición de una intrusión. El motor de decisiones se puede implementar como sistemas de detección basados ​​en firmas o en anomalías. El motor de decisiones es la parte más crítica de un sistema IDS, ya que afecta directamente la eficiencia del sistema. El motor de decisiones decide si el flujo rastreado se identifica como normal o como una intrusión según el conocimiento previo. El motor de clasificación del sistema IDS es responsable de esta decisión y puede implementarse como basado en firmas o basado en anomalías [22]. Datasets En el campo de la ciberseguridad existen 15 conjuntos de datos(datasets) disponibles para el entrenamiento de sistemas de para detección de intrusos esto según una encuesta de datasets del año 2019. [17]. Estos “Datasets” tienen diferentes características elegidas por los autores según sus conocimientos y experiencias en el campo, sin embargo, como se ha evidenciado en varios análisis muchas de estas características son irrelevantes y su disparidad imposibilita una generalización del desempeño de los modelos utilizado en un dataset especifico [11]. Estos Datasets son creados a partir de bancos de pruebas virtuales lo que crea una brecha entre los modelos implementados utilizando estos conjuntos de datos y sistemas IDS en sistemas reales. 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.   * + 1. **Análisis de trafico**   Es necesario recopilar y registrar el tráfico de la red para monitorear y analizar redes Hay dos tendencias principales para este proceso, capturando la totalidad tráfico de red, es decir, paquetes de tráfico, y captura de un resumen de los paquetes de red en forma de flujos.  El análisis de tráfico para evitar ataques DDoS con dispositivos IoT involucra el monitoreo y análisis de los patrones de tráfico de la red para identificar y mitigar el tráfico malicioso que podría estar destinado a inundar y sobrecargar la red, causando una interrupción en el servicio. Los ataques DDoS a menudo se originan a partir de dispositivos IoT infectados, que pueden formar parte de una botnet y ser controlados por un atacante remoto.  Para evitar estos ataques, se utilizan técnicas de análisis de tráfico, como la inspección profunda de paquetes y la identificación de patrones anormales en el tráfico de red. También se pueden implementar soluciones de mitigación de DDoS, como el filtrado de paquetes, para bloquear el tráfico malicioso antes de que llegue a la red de destino. Cisco Net Flow NetFlow de Cisco es un protocolo desarrollado por Cisco Systems para recolectar información de tráfico de red. Fue creado para solucionar el problema de la falta de visibilidad en el tráfico de la red y para ayudar en la gestión de la red y la resolución de problemas.  Funciona mediante la recolección de información sobre el tráfico de red, incluyendo detalles sobre el origen, el destino, el tipo de protocolo, el tiempo, entre otros. La información se recopila a través de routers y switches de red, y se envía a un colector de NetFlow, donde se procesa y analiza [16].  El NetFlow se utiliza para una variedad de propósitos, incluyendo la identificación de problemas de red, el monitoreo de la actividad de la red, la planificación de capacidad y la detección de tráfico malicioso. También puede ser utilizado para analizar el comportamiento del usuario y optimizar el rendimiento de la red en función de las necesidades de la organización.  Los sistemas de detección de intrusos en la red (NIDS) basados en el aprendizaje automático (ML) son una herramienta prometedora para proteger las redes contra los ataques cibernéticos. Sin embargo, existe una brecha entre la investigación académica y las implementaciones prácticas en las redes del mundo real debido a la falta de conjuntos de datos comunes y relevantes. La propuesta de generar conjuntos de datos NIDS con un conjunto de características común y prácticamente relevante basado en NetFlow es una solución prometedora para abordar esta brecha. Utilizar NetFlow como formato común tiene muchos beneficios, como su relevancia práctica y sus propiedades de escalado. La creación de conjuntos de datos comunes y relevantes para la evaluación de NIDS basados en ML es un paso importante para mejorar la seguridad cibernética en las redes del mundo real [5].   * + 1. **Dataset NF-UQ-NIDS**   El dataset NF-UQ-NIDS (Network Forensic - University of Queensland - Network Intrusion Detection System) es un conjunto de datos estandarizado con el protocolo Netflow utilizado en el ámbito de la detección de intrusos en redes. Este dataset se creó específicamente para la evaluación y desarrollo de algoritmos y sistemas de detección de intrusos.  El dataset NF-UQ-NIDS contiene capturas de tráfico de red correspondientes a diferentes tipos de actividades de red, incluyendo tanto tráfico normal como tráfico malicioso o sospechoso. Estas capturas de tráfico se obtuvieron a partir de un entorno de red real o se generaron en laboratorio para simular diferentes escenarios y tipos de ataques.  El objetivo principal del dataset NF-UQ-NIDS es proporcionar a los investigadores y profesionales de seguridad una colección de datos representativa que les permita probar y evaluar la efectividad de los sistemas de detección de intrusos. El dataset incluye información detallada sobre los paquetes de red, como direcciones IP de origen y destino, puertos, protocolos y otros atributos relevantes para el análisis de tráfico y la detección de ataques.  Este conjunto de datos toma cinco conjuntos de datos NIDS que comparten un conjunto de características comunes y relevantes, basados en NetFlow. Estos conjuntos de datos se generaron a partir de cuatro conjuntos de datos NIDS de referencia existentes: UNSW-NB15, BoT-IoT, ToN-IoT y CSE-CIC-IDS2018. Se tomaron los archivos de captura de paquetes sin procesar de estos conjuntos de datos y se convirtieron al formato NetFlow, utilizando un conjunto de características compartido.  Según los creadores del conjunto de datos se eligió el formato NetFlow como estándar porque ofrece varios beneficios: relevancia práctica, amplio uso en redes de producción y su capacidad de escalado. Los conjuntos de datos de NetFlow generados han sido etiquetados para permitir experimentos de clasificación de ataques y tráfico binario y multiclase [5]. Herramientas de para machine learning y Deep learning **Jupyter Notebook** es una aplicación web de código abierto que permite crear y compartir documentos interactivos que contienen código en vivo, ecuaciones, visualizaciones y texto narrativo. Se utiliza ampliamente en la ciencia de datos y el aprendizaje automático, ya que permite a los usuarios escribir, ejecutar y compartir código de manera fácil y accesible. Jupyter Notebook es compatible con una amplia gama de lenguajes de programación, incluidos Python, R, Julia.  **Scikit-Learn**: es una biblioteca de aprendizaje automático en Python que proporciona una variedad de algoritmos de clasificación, regresión y clustering. Sin embargo, Scikit-Learn no está diseñado específicamente para el aprendizaje profundo, por lo que su capacidad para abordar problemas de detección de ataques DDoS en redes IoT utilizando Deep Learning puede ser limitada. Aunque puede ser útil para algunas tareas de preprocesamiento de datos, Scikit-Learn .  **TensorFlow**: es una de las bibliotecas más populares para el aprendizaje profundo en Python. Proporciona una amplia gama de herramientas para la creación de redes neuronales y modelos de aprendizaje automático, incluyendo capas, optimizadores y funciones de activación. TensorFlow es una excelente opción para el desarrollo del modelo, ya que es altamente personalizable y escalable.  **Keras**: es una biblioteca de aprendizaje profundo en Python que proporciona una interfaz fácil de usar para construir redes neuronales. Keras es compatible con TensorFlow, lo que significa que se pueden utilizar todas las herramientas y características de TensorFlow en combinación con la sintaxis más sencilla y legible de Keras. Keras es una buena ya que es una biblioteca más intuitiva y de fácil uso que TensorFlow.  **PyTorch:** es una biblioteca de aprendizaje profundo en Python que se centra en la facilidad de uso y la flexibilidad. Al igual que TensorFlow, PyTorch proporciona una amplia gama de herramientas para la creación de redes neuronales, pero su sintaxis es más cercana a Python que a una interfaz específica de aprendizaje automático. PyTorch es una buena ya que es una biblioteca más flexible y más fácil de depurar que TensorFlow.  **Microsoft Cognitive Toolkit (CNTK**): Microsoft Cognitive Toolkit (CNTK) es una biblioteca de aprendizaje automático en C++ y Python que proporciona herramientas para la creación de redes neuronales y modelos de aprendizaje automático. Es especialmente útil para problemas de aprendizaje profundo y se centra en la escalabilidad y la eficiencia. CNTK es una buena opción si estás trabajando en un proyecto a gran escala.  **Torch:** es una biblioteca de aprendizaje profundo de código abierto basada en Lua. Es una herramienta muy popular para el procesamiento de lenguaje natural, la visión por computadora y la investigación en aprendizaje profundo. La documentación es buena y tiene una amplia comunidad de usuarios y desarrolladores. Torch podría ser una buena opción si se está familiarizado con Lua y se quiere una biblioteca de aprendizaje profundo de alta calidad.  **H2O.ai**: es una plataforma de aprendizaje automático de código abierto con una interfaz fácil de usar y amplias capacidades de análisis de datos. Se puede usar para una variedad de problemas de aprendizaje automático, incluida la clasificación, la regresión y la agrupación. H2O.ai es una plataforma fácil de usar y permite explorar una variedad de algoritmos de aprendizaje automático.  **Apache Mahout**: Mahout es una biblioteca de aprendizaje automático de código abierto que se ejecuta en la plataforma Hadoop. Ofrece una amplia variedad de algoritmos de aprendizaje automático, incluidos los algoritmos de clustering, clasificación y recomendación. Mahout es una buena opción si se utiliza Hadoop como plataforma de big data y desea implementar algoritmos de aprendizaje automático en su entorno.  **RapidMiner**: es una plataforma de análisis de datos que ofrece una amplia variedad de técnicas de aprendizaje automático. Ofrece una interfaz de usuario gráfica fácil de usar y una amplia gama de conectores de datos. RapidMiner podría ser una buena opción si desea una plataforma fácil de usar para el análisis de datos y la construcción de modelos de aprendizaje automático.  **KNIME Analytics Platform**: plataforma de análisis de datos de código abierto que ofrece una amplia variedad de técnicas de aprendizaje automático. Ofrece una interfaz de usuario gráfica fácil de usar y una amplia gama de conectores de datos. KNIME podría ser una buena opción si desea una plataforma fácil de usar para el análisis de datos y la construcción de modelos de aprendizaje automático.  **Google Cloud AutoML**: plataforma de aprendizaje automático que permite crear modelos personalizados sin experiencia previa en aprendizaje automático. Es útil para proyectos en los que se desea una solución rápida y eficiente en la nube, y ofrece una variedad de modelos preentrenados. Es útil para acelerar el proceso de entrenamiento del modelo y reducir la complejidad de la implementación.  **DataRobot**: plataforma de aprendizaje automático que automatiza el ciclo de vida completo de la creación de modelos. Permite la selección de algoritmos y la optimización de hiperparámetros, lo que puede ser útil para acelerar el proceso de desarrollo de modelos. Además, DataRobot también ofrece la posibilidad de integrar modelos personalizados en su plataforma. Puede ser útil para acelerar el proceso de entrenamiento del modelo y optimizar su rendimiento.  **IBM Watson Studio**: plataforma de aprendizaje automático basada en la nube que permite crear y desplegar modelos de aprendizaje automático personalizados. Ofrece una variedad de herramientas y recursos para el análisis de datos y el modelado, lo que puede ser útil en proyectos de aprendizaje automático complejos. Puede ser útil para acelerar el proceso de entrenamiento del modelo y para mejorar la eficiencia de la implementación.  **4.2 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. |

|  |
| --- |
| 5. Objetivos **5.1 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.  **5.2 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 neuronales 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. |

|  |
| --- |
| 6. Alternativa de Solución   **Figura 1. Diagrama de Bloques para alternativa de solución.**  **6.1 Diagrama de bloques de la solución**  En este apartado se explican cada uno de los bloques que componen la alternativa de solución propuesta:  **Preparación de datos**: Este bloque se encarga de recolectar y almacenar los datos de red IoT a través del protocolo Netflow. Esto puede implicar el uso de dispositivos de captura de tráfico de red o la conexión directa a los dispositivos IoT para recopilar los datos necesarios.  **Preprocesamiento de datos**: Este bloque implica la limpieza, normalización y transformación de los datos crudos de la red IoT para prepararlos para el entrenamiento del modelo. Esto puede incluir la eliminación de valores atípicos, la normalización de los datos y la selección de características relevantes.  **Entrenamiento del modelo**: Este bloque implica el entrenamiento del modelo de detección de ataques DDoS utilizando los datos preprocesados. Este proceso se basa en la aplicación de técnicas de aprendizaje profundo, como redes neuronales convolucionales o redes neuronales recurrentes.  **Evaluación del modelo**: En este bloque, se evalúa el rendimiento del modelo entrenado utilizando diferentes métricas de evaluación, como precisión, recall y F1-score. Además, se comparará el desempeño del modelo con otros algoritmos de detección de ataques DDoS previamente reportados en la literatura.  **Implementación del modelo**: En este bloque, se implementará el modelo entrenado en un entorno real de red IoT y se realizarán pruebas para evaluar su capacidad para detectar ataques DDoS en tiempo real.  **Análisis de resultados**: Finalmente, en este bloque, se realizará un análisis detallado de los resultados obtenidos durante todo el proceso, incluyendo el rendimiento del modelo y su capacidad para detectar ataques DDoS en tiempo real. Además, se discutirán las limitaciones del modelo y las posibles mejoras y futuras investigaciones. |

|  |
| --- |
| 7. Metodología Propuesta La metodología descrita a continuación según su estructura y los pasos involucrados es consistente con una metodología de investigación aplicada mixta es decir combinando elementos de investigación cualitativa y cuantitativa, esta metodología es ampliamente utilizada en informática y en el desarrollo de la inteligencia artificial [23]. La metodología de investigación aplicada se refiere al enfoque y conjunto de pasos que se siguen para abordar un problema específico en un campo de estudio particular y generar conocimiento práctico y aplicable.  **Investigación**: Se analizará la literatura existente sobre la detección de ataques DDoS basada en Deep Learning y su aplicación en redes IoT. También se analizarán los algoritmos de Deep Learning existentes que podrían aplicarse para la detección de ataques DDoS en redes IoT.  **Preparación de los datos**: Descargar los datasets estandarizados NF-UQ-NIDS y el protocolo de red Netflow. Preprocesar los datos para asegurar que sean adecuados para el análisis. Realizar una exploración de los datos para entender su estructura y características.  **Desarrollo del modelo**: Seleccionar y configurar el modelo de Deep Learning que se utilizará para la detección de ataques DDoS en redes IoT. Entrenar el modelo utilizando los datos preparados. Evaluar el modelo utilizando medidas de desempeño apropiadas.  Comparación y análisis: Comparar el desempeño del modelo desarrollado con otros modelos de detección de ataques DDoS basados en Deep Learning reportados en la literatura.  Analizar las fortalezas y debilidades del modelo propuesto.  **Análisis de resultados, optimización y conclusiones**: Presentar las conclusiones del proyecto. Proporcionar recomendaciones para mejorar el modelo y para futuras investigaciones.  **Documentación y Trabajo final:** se realizarán las correcciones finales al documento y se realizara la socialización del proyecto ante los jurados. |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8. cronograma de Actividades.  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | **Actividad/Mes** | **Mes 1** | | | | **Mes 2** | | | | **Mes 3** | | | | **Mes 4** | | | | **Mes 5** | | | | **Mes 6** | | | | | | Semana | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | | **Investigación Modelos DL** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | **Selección de Datasets** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | **Preprocesamiento de datos** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | **Entrenamiento del modelo** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | **Evaluación del modelo** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | **Optimización del modelo** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | **Pruebas finales** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |   **Figura 2. Diagrama de Gantt.** |

|  |
| --- |
| 9. Impacto Esperado. Este proyecto tiene como objetivo el desarrollo de un modelo de Deep learning que contribuya a la investigación en auge en este campo más específicamente para su uso en la seguridad de las redes de datos.  Esto debido a que las redes de nueva generación cuentan cada vez con mayor cantidad de dispositivos conectados, lo que aumenta la su complejidad y también la cantidad de datos que generan. El Deep learning será en el futuro una herramienta cada vez más eficaz y necesaria para procesar y analizar estos datos y encontrar patrones ocultos que podrían no ser detectados por técnicas de análisis más tradicionales, esto con el fin de ayudar a mejorar la seguridad y el rendimiento de las redes.  **9.1 Impacto Social**  Crear y dominar nuevas técnicas de ciberseguridad que no dependan solamente de la capacidad humana solamente es fundamental ya que podemos ver este ámbito como un campo de batalla donde atacantes como defensores utilizaran las mejores armas a su disposición. Además, teniendo en cuenta que es cada vez más posible atacar la información personal y financiera de las personas, así como la propiedad intelectual y los activos de las empresas. Además, las violaciones de seguridad pueden tener un impacto significativo en la reputación y la confianza de la organización, así como en su responsabilidad legal y financiera.  **9.2 Impacto Económico**  El uso de tecnologías de inteligencia artificial (IA) puede mejorar la capacidad de detección y protección contra amenazas, así como predecir y responder rápidamente ante ataques, disminuyendo la necesidad de especialistas en seguridad cibernética, los cuales son escasos en la actualidad. La IA puede aprender de los analistas de seguridad y mejorar su desempeño gradualmente, lo que permite un ahorro de tiempo y la toma de decisiones más acertadas. La necesidad de capacidades en inteligencia es crucial debido al aumento constante en volumen y complejidad de los ciberataques.  **9.3 Impacto Tecnológico**   En el contexto de las redes de nueva generación, como las redes 5G, la importancia de la ciberseguridad se vuelve aún más crítica. Estas redes están diseñadas para soportar un número mucho mayor de dispositivos y conexiones, lo que aumenta la superficie de ataque y la complejidad de la seguridad. Además, las redes de nueva generación tienen la capacidad de habilitar nuevas aplicaciones y servicios, lo que significa que es necesario proteger una variedad de datos críticos en tiempo real, como los datos de salud y de tráfico. Por lo tanto, la ciberseguridad se vuelve esencial para garantizar la confidencialidad, integridad y disponibilidad de los datos y sistemas en estas redes de alta velocidad y complejidad. |

|  |
| --- |
| 10. Resultados Esperados 1- Modelo de Deep learning que mejore en la precisión y eficacia de la detección de actividades maliciosas en comparación con métodos tradicionales de Machine Learning.  2- Documento con la descripción del desarrollo de este modelo en las etapas de recopilación de datos, preprocesamiento, entrenamiento, evaluación del modelo. |

|  |
| --- |
| 11. Estrategia de Comunicación **Documento para el repositorio**  Documento técnico que documentará el problema abordado, la metodología de investigación, así como los recursos, y conocimientos empleados para el desarrollo del proyecto y finalmente las pruebas realizadas de la solución planteada.  **Socialización**  Sustentación ante los jurados del proyecto en donde se dan a conocer la problemática abordada, y el desarrollo de la solución planteada detallando el proceso investigativo y experimental realizado, así como la experiencia y los conocimientos adquiridos. |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **12. PRESUPUESTO**   |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | PRESUPUESTO GLOBAL DE LA PROPUESTA POR FUENTES DE FINANCIACIÓN(En miles de $) | | | | | | | | | RUBROS | FUENTES | | | | | | TOTAL | | 1 Univ. Distrital | | 2 recursos propios | | 3 empresa | | |  | Especie | Dinero | Especie | Dinero | Especie | Dinero |  | | PERSONAL | $100 | $0 | $900 | $0 | $0 | $0 | $1000 | | EQUIPO | $1000 | $0 | $0 | $300 | $0 | $0 | $1300 | | MATERIALES | $0 | $0 | $0 | $300 | $0 | $0 | $300 | | SALIDAS DE CAMPO | $0 | $0 | $0 | $0 | $0 | $0 | $0 | | VIAJES | $0 | $0 | $0 | $0 | $0 | $0 | $0 | | BIBLIOGRAFÍA | $0 | $0 | $0 | $0 | $0 | $0 | $0 | | SOFTWARE | $0 | $0 | $0 | $0 | $0 | $0 | $0 | | PUBLICACIONES | $0 | $0 | $0 | $0 | $0 | $0 | $0 | | SERVICIOS TÉCNICOS | $0 | $0 | $0 | $0 | $0 | $0 | $0 | | CONSTRUCCIONES | $0 | $0 | $0 | $0 | $0 | $0 | $0 | | MANTENIMIENTO | $0 | $0 | $0 | $0 | $0 | $0 | $0 | | ADMINISTRACIÓN | $0 | $0 | $0 | $0 | $0 | $0 | $0 | | TOTAL |  |  |  |  |  |  | $1600 |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | | DESCRIPCIÓN DE LOS GASTOS DE PERSONAL (En miles de $) | | | | | | | | | | INVESTIGADOR/AUXILIAR | FORMACIÓN | FUNCIÓN DENTRO DEL PROYECTO | DEDICACIÓN | RECURSOS | | | | TOTAL | | 1 | 2 | 3 | | | Henry Alberto Hernández | Profesional especializado | Director | 50 | $1562 |  | |  | $1562 | | Ernesto cadena | Profesional especializado | Codirector | 50 | $1562 |  | |  | $1562 | | Daniel Cabiativa | Estudiante | Investigador | 160 |  | $4500 | |  | $4500 | | Johan Herrera | Estudiante | Investigador | 160 |  | $4500 | |  | $4500 | | TOTAL | | | | | | |  | $12124 |   1 🡪 Universidad Distrital Francisco José de Caldas  2 🡪 Recursos propios  3 🡪 Empresa  Técnico o estudiante de tecnología: 2,5 SMLV POR 160 HORAS.  Tecnólogo: 3 SMLV POR 160 HORAS  Profesional: 4,5 SMLV POR 160 HORAS  Profesional especializado: 5 SMLV POR 160 HORAS   |  |  |  |  | | --- | --- | --- | --- | | DESCRIPCIÓN Y CUANTIFICACIÓN DE LOS EQUIPOS DE USO PROPIO  (En miles de $) | | | | | EQUIPO | 1 | 2 | 3 | | PC | $0 | $750 | $0 | | SMARTPHONE | $0 | $35 | $0 | |  |  |  |  | | TOTAL | $$0 | $$785 | $$0 | |

**BIBLIOGRAFIA**

[1] C. Aubley, D. Golden, M. Morris, y K. Norton, «The future of cybersecurity and AI | Deloitte Insights», 2022. https://www2.deloitte.com/us/en/insights/focus/tech-trends/2022/future-of-cybersecurity-and-ai.html (accedido 16 de febrero de 2023).

[2] «¿Cuántos ciberataques sufrió Colombia en 2022? - Novedades Tecnología - Tecnología - ELTIEMPO.COM», agosto de 2022. Accedido: 16 de febrero de 2023. [En línea]. Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/cuantos-ciberataques-sufrio-colombia-en-2022-695772

[3] E. V. Jaimes Bastidas, «Detección de amenazas en redes IoT empleando modelo híbrido de Machine Learning y Deep Learning», Universidad de los Andes, 2022. Accedido: 16 de febrero de 2023. [En línea]. Disponible en: https://repositorio.uniandes.edu.co/handle/1992/58981

[4] J. M. Díaz, «Riesgos y vulnerabilidades de la denegación de servicio distribuidos en internet de las cosas», 2019, Accedido: 2 de marzo de 2023. [En línea]. Disponible en: www.bioeticayderecho.ub.edu

[5] M. Sarhan, S. Layeghy, N. Moustafa, y M. Portmann, «NetFlow Datasets for Machine Learning-Based Network Intrusion Detection Systems», *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, vol. 371 LNICST, pp. 117-135, 2021, doi: 10.1007/978-3-030-72802-1\_9/COVER.

[6] N. Mishra y S. Pandya, «Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review», *IEEE Access*, vol. 9, pp. 59353-59377, 2021, doi: 10.1109/ACCESS.2021.3073408.

[7] B. Schneier, «TR10: Ejércitos de las cosas zombi | MIT Technology Review», 23 de febrero de 2017. https://www.technologyreview.es/s/6823/tr10-ejercitos-de-las-cosas-zombi (accedido 6 de marzo de 2023).

[8] «Ataques DDoS más conocidos | Los mayores ataques DDoS de la historia | Cloudflare». https://www.cloudflare.com/es-es/learning/ddos/famous-ddos-attacks/ (accedido 9 de marzo de 2023).

[9] M. Sarhan, S. Layeghy, y M. Portmann, «Towards a Standard Feature Set for Network Intrusion Detection System Datasets», *Mobile Networks and Applications*, vol. 27, n.o 1, pp. 357-370, feb. 2022, doi: 10.1007/S11036-021-01843-0/METRICS.

[10] Cortés Cabezas Edison, «Diseño de un modelo de detección de intrusos en entornos IoT usando inteligencia artificial.», 2021. Accedido: 16 de febrero de 2023. [En línea]. Disponible en: https://repository.udistrital.edu.co/handle/11349/29671

[11] C. A. Carvajal Hoyos y J. S. Susa Velandia, «Modelo de detección de ataques DDoS (distributed denial of services), con base en el clasificador decisión tree. - hdl:11349/30117», UDJC, Bogotá D.C, 2022.

[12] D. Rolando, D. Patiño, E. Alexander, y S. Galindo, «Las amenazas de seguridad a las que se enfrenta IoT y las soluciones en desarrollo», 2021, Accedido: 16 de febrero de 2023. [En línea]. Disponible en: https://repository.udistrital.edu.co/bitstream/handle/11349/29310/S%C3%A1nchezGalindoEdgarAlexander2021.pdf?sequence=1&isAllowed=y

[13] A. C. M. Suárez, S. S. D. Ávila, y M. Á. L. Páez, «Mecanismos de seguridad en el internet de las cosas », *Revista Vínculos*, vol. 16, n.o 2, pp. 288-297, dic. 2019, doi: 10.14483/2322939X.15758.

[14] J. A. Parra Jiménez, «Un método para la identificación y prevención temprana de incidentes de ciberseguridad en dispositivos del Internet de las Cosas», 2021. Accedido: 16 de febrero de 2023. [En línea]. Disponible en: https://repositorio.unal.edu.co/bitstream/handle/unal/81148/1030660760.2021.pdf?sequence=1&isAllowed=y

[15] H. Fabián y V. Sánchez, «Defensa contra intrusos en redes de dispositivos IoT usando técnicas de Blockchain y Machine Learning», Universidad de los Andes, 2020. Accedido: 16 de febrero de 2023. [En línea]. Disponible en: https://repositorio.uniandes.edu.co/handle/1992/48617

[16] Diaz Pinilla Luis David, «Medición de desempeño de sistema de monitoreo de redes con protocolo Netflow en modelo Big Data. - hdl:11349/23554», Bogotá, 2019. Accedido: 21 de febrero de 2023. [En línea]. Disponible en: https://repository.udistrital.edu.co/handle/11349/23554

[17] L. A. Polanía Arias, «Evaluación de modelos de machine learning para sistemas de detección de intrusos en dedes IoT», 2021. Accedido: 22 de febrero de 2023. [En línea]. Disponible en: https://repositorio.uniandes.edu.co/handle/1992/55526

[18] E. R. Ramírez Fernández, «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». Accedido: 22 de febrero de 2023. [En línea]. Disponible en: https://repositorio.unam.mx/contenidos/implementacion-de-analisis-de-trafico-y-de-flujos-de-red-con-tecnologias-netflow-y-sflow-en-equipos-de-red-de-la-unam-util-168152?c=KY7rlW&d=true&q=\*:\*&i=1&v=1&t=search\_0&as=0

[19] F. J. García Cañola, «Sistema preventivo contra ataques de denegación de servicio web utilizando Deep Learning», Bogotá, 2020.

[20] N. Moustafa y J. Slay, «The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set», *http://dx.doi.org/10.1080/19393555.2015.1125974*, vol. 25, n.o 1-3, pp. 18-31, abr. 2016, doi: 10.1080/19393555.2015.1125974.

[21] G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido, y M. Marchetti, «On the effectiveness of machine and deep learning for cyber security», *International Conference on Cyber Conflict, CYCON*, vol. 2018-May, pp. 371-389, jul. 2018, doi: 10.23919/CYCON.2018.8405026.

[22] G. Karatas, O. Demir, y O. K. Sahingoz, «Deep Learning in Intrusion Detection Systems», *International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism, IBIGDELFT 2018 - Proceedings*, pp. 113-116, ene. 2019, doi: 10.1109/IBIGDELFT.2018.8625278.

[23] Hirsch, H. G. (2019). Research Methodology in Artificial Intelligence. In The AI Book: The Artificial Intelligence Handbook for Business Leaders. Wiley..