Imagen que contiene Texto

Descripción generada automáticamente

**Desarrollo de un sistema de detección de intrusos en redes utilizando técnicas de inteligencia artificial**

Grado en Ingeniería Informática

2024 - 2025

|  |
| --- |
| **ALFONSO GALOCHA SANCHEZ**  **ALUMNO** |

|  |
| --- |
| **ALBERTO BALLESTEROS RODRIGUEZ**  **TUTOR** |

Índice de Contenidos

[Resumen y Palabras Clave. 2](#_Toc1883459593)

[Agradecimientos. 3](#_Toc329744947)

[1. Introducción 4](#_Toc1857871230)

[2. Metodología. 4](#_Toc1954701149)

[3. Resultados. 4](#_Toc1808679833)

[4. Conclusiones 5](#_Toc1188207844)

[5. Limitaciones y Líneas futuras 5](#_Toc501976075)

[6. Bibliografía 5](#_Toc930442683)

# Resumen y Palabras Clave.

# Agradecimientos.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nunc porttitor, diam at ornare pretium, eros ipsum mattis purus, non blandit lectus dui eu felis. Quisque gravida, lacus id aliquet pulvinar, dui diam luctus eros, vitae bibendum magna velit ut lorem. Proin sed nunc libero, sit amet adipiscing dolor. Integer tempus pretium quam, tristique commodo nunc mattis et. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Aenean nisl sapien, sagittis ut ultricies eget, ultrices at ante. Mauris porta sagittis consectetur. Donec pellentesque, purus sed fringilla rutrum, leo nulla pellentesque nunc, quis imperdiet nisi tortor vel nisl. Vestibulum suscipit pellentesque condimentum. Aliquam dignissim, enim quis molestie feugiat, neque quam viverra urna, a cursus mauris metus eleifend lacus. Vivamus sit amet erat ante. Phasellus a vehicula felis. Morbi ullamcorper luctus gravida. Duis imperdiet, turpis et bibendum venenatis, velit lectus porta massa, eu fringilla risus velit sit amet lectus. Duis ac mauris enim, at dictum velit.

# Introducción

La ciberseguridad ha despertado un notable interés en los últimos años, tanto por sus implicaciones técnicas como por el reto que representa la detección de comportamientos anómalos en sistemas o redes. El análisis de datos, la identificación de patrones inusuales y la comprensión de cómo estos pueden utilizarse para prevenir incidentes antes de que ocurran constituyen elementos clave en este ámbito. El entorno actual, altamente digitalizado, plantea la necesidad de aplicar conocimientos técnicos en soluciones que generen un impacto real, como la protección de infraestructuras frente a ciberataques.

Este Trabajo de Fin de Grado se ha orientado hacia la ciberseguridad no solo por el interés que suscita el área, sino también por su relevancia como uno de los grandes desafíos tecnológicos contemporáneos. A partir de la formación académica y la experiencia práctica del autor, se ha identificado que muchos sistemas de detección de intrusos (IDS) actuales se basan en firmas o reglas predefinidas. Esta aproximación presenta una limitación importante: la incapacidad para detectar ataques desconocidos o que han sido modificados mínimamente respecto a sus versiones conocidas. En un contexto donde las amenazas evolucionan constantemente, esta limitación representa un riesgo considerable.

En paralelo, se ha observado una tendencia creciente en el uso de técnicas de inteligencia artificial por parte de atacantes para generar amenazas más sofisticadas, capaces de adaptarse y evadir mecanismos de detección tradicionales. Esta situación refuerza la necesidad de incorporar la inteligencia artificial también en los sistemas defensivos, no solo para mejorar la detección, sino con el objetivo de anticiparse a los ataques.

Actualmente, existen múltiples investigaciones y desarrollos que exploran la aplicación de algoritmos de aprendizaje automático y redes neuronales en la detección de intrusiones. No obstante, muchos de estos trabajos se enfocan en entornos específicos o presentan dificultades para su implementación práctica. Además, algunos modelos continúan enfrentándose a desafíos como elevadas tasas de falsos positivos, limitada capacidad de adaptación ante nuevas amenazas y una fuerte dependencia de datos etiquetados con precisión.

El objetivo principal de este proyecto es diseñar un sistema de detección de intrusos funcional, basado en técnicas de inteligencia artificial, capaz de identificar tráfico malicioso en redes. Aunque no se pretende desarrollar una solución definitiva que abarque todos los tipos de ataque, el propósito es contribuir a una mejora en la capacidad de detección respecto a sistemas tradicionales. En particular, se abordarán ataques frecuentes y de alto impacto, como los escaneos de puertos o los ataques de denegación de servicio. Para ello, se emplearán datasets públicos del ámbito de la ciberseguridad, herramientas de análisis de red y librerías de aprendizaje automático, con el fin de construir una solución práctica, funcional y orientada a su aplicabilidad en entornos reales.

# Metodología.

Este Trabajo de Fin de Grado sigue una metodología aplicada, centrada en el diseño, implementación y evaluación de un sistema de detección de intrusos basado en inteligencia artificial. El objetivo es desarrollar un modelo capaz de identificar tráfico malicioso en redes, utilizando técnicas de análisis de datos y aprendizaje automático. El proceso se ha dividido en varias fases que incluyen: selección y preparación del dataset, análisis exploratorio de datos, entrenamiento de modelos de IA, validación de resultados y evaluación de su rendimiento.

**2.1. Limpieza del Dataset**

Para comenzar el desarrollo del sistema, se seleccionó un dataset público de ciberseguridad. La limpieza de datos es una fase crítica en cualquier proyecto de análisis, ya que asegura la calidad de los datos que se utilizarán para el entrenamiento del modelo. En esta etapa se han llevado a cabo tareas como:

* Eliminación de columnas irrelevantes o redundantes.
* Conversión de variables categóricas en valores numéricos.
* Tratamiento de valores nulos o mal formateados.
* Revisión de duplicados y errores evidentes en los registros.
* Normalización o escalado de características, en caso necesario.
* Estas acciones han permitido dejar el conjunto de datos preparado para realizar un análisis más profundo y posteriormente entrenar modelos de IA de forma más eficaz.

**2.2. Análisis Exploratorio de Datos (EDA)**

El análisis exploratorio permite comprender mejor la estructura del dataset y detectar posibles problemas o patrones interesantes antes de aplicar modelos predictivos. En esta fase se han generado:

* Gráficos de distribución de clases (por ejemplo, proporción entre tráfico normal y tráfico malicioso).
* Análisis de correlación entre características.
* Estudio de la frecuencia y comportamiento de las principales variables.
* Identificación de posibles outliers y tendencias en los datos.
* El EDA también ayuda a tomar decisiones sobre qué características utilizar en el modelo final y cómo balancear el dataset si existe un desbalance entre clases.

**2.3. Fases Pendientes**

Aunque las dos fases anteriores ya se han completado, el proyecto continuará con los siguientes pasos:

* **Selección y entrenamiento de modelos de IA:** Se probarán distintos algoritmos de clasificación como Decision Trees, Random Forest, y modelos basados en redes neuronales, evaluando cuál ofrece mejor rendimiento para la detección de intrusos.
* **Validación y ajuste del modelo:** Se aplicarán técnicas como validación cruzada, matrices de confusión y métricas como precisión, recall y F1-score para analizar el comportamiento del modelo.
* **Implementación del sistema IDS:** Una vez entrenado, se integrará el modelo en un sistema que sea capaz de recibir tráfico de red y emitir alertas en caso de detectar actividad sospechosa.
* **Evaluación del sistema en escenarios simulados:** Se realizarán pruebas para comprobar su rendimiento en diferentes tipos de ataques.

# Resultados.

Responde a la pregunta ¿qué se ha encontrado? En esta sección se presentan de forma descriptiva (no interpretada o discutida) los resultados obtenidos de la investigación descrita en el apartado anterior, mediante texto, y en su caso tablas y figuras.

# Conclusiones

Responde a la pregunta ¿qué significa? El apartado final del cuerpo del TFM debe contener las conclusiones que dan respuesta a las preguntas planteadas en la introducción del trabajo -particularmente el objetivo, con el que deben mantener una coherencia- a partir del análisis e interpretación de los datos presentados en el apartado anterior. Opcionalmente puede incluirse un apartado de discusión, que será reflexión final basada en los argumentos expuestos en el trabajo, que tenga una aportación personal del autor, aunque sin cargas subjetivas -ideológica o moral, por ejemplo- que valore los resultados alcanzados, reconozca las limitaciones y dificultades encontradas, y esboce una propuesta de una hipotética investigación futura.

# Limitaciones y Líneas futuras

Responde a la pregunta ¿Con qué limitaciones me he encontrado? Y ¿Qué se debería de seguir investigando de aquí en adelante?

# Bibliografía

Normativa APA

Servidio, R., Bartolo, M. G., Palermiti, A. L., & Costabile, A. (2021). Fear of COVID-19, depression, anxiety, and their association with Internet addiction disorder in a sample of Italian students. *Journal of Affective Disorders Reports*, *4*, 100097.