**Texto

Descripción generada automáticamente**

Estudiantes

Luis Pablo Chavarria Morales

Curso

Inteligencia en Redes de Datos [202403\_001\_BIT-31\_1]

Profesor

Carlos Andres Mendez Rodriguez

Proyecto

Detección de anomalías en redes con IA

Tabla de contenido

[Tema de Investigación 3](#_Toc183625361)

[Objetivo General 3](#_Toc183625362)

[Implementar un sistema basado en inteligencia artificial para la detección de anomalías en redes de telecomunicaciones, mejorando la capacidad de identificación de posibles amenazas. 4](#_Toc183625363)

[Objetivos Específicos 4](#_Toc183625364)

[ Investigar diferentes algoritmos de IA que son efectivos para la detección de anomalías en redes. 4](#_Toc183625365)

[ Implementar un prototipo de sistema de detección de anomalías utilizando algoritmos de IA seleccionados, evaluando su rendimiento en un entorno simulado. 4](#_Toc183625366)

[ Evaluar la efectividad del sistema de IA en relación con métodos tradicionales de detección, midiendo métricas como la precisión, la sensibilidad y la tasa de falsos positivos. 4](#_Toc183625367)

[ Investigar mejoras en la metodología utilizada y en la configuración de los algoritmos para aumentar la eficacia del sistema. 4](#_Toc183625368)

[Plan de Trabajo Detallado 4](#_Toc183625369)

[Metodología de Investigación 5](#_Toc183625370)

[Recursos para la Implementación 5](#_Toc183625371)

[1- Python 5](#_Toc183625372)

[2- Google Colab 5](#_Toc183625373)

[3- Matplotlib y Seaborn para visualizaciones de datos y resultados. 5](#_Toc183625374)

### Tema de Investigación

El proyecto se enfocará en la detección de anomalías en redes con IA, con el objetivo es detección automática de patrones inusuales en el tráfico de red, con el fin de mejorar la seguridad en redes de telecomunicaciones, con el fin de identificar comportamientos anómalos que indiquen posibles amenazas, como ataques cibernéticos o accesos no autorizados.

### Objetivo General

### Implementar un sistema basado en inteligencia artificial para la detección de anomalías en redes de telecomunicaciones, mejorando la capacidad de identificación de posibles amenazas.

### Objetivos Específicos

### Investigar diferentes algoritmos de IA que son efectivos para la detección de anomalías en redes.

### Implementar un prototipo de sistema de detección de anomalías utilizando algoritmos de IA seleccionados, evaluando su rendimiento en un entorno simulado.

### Evaluar la efectividad del sistema de IA en relación con métodos tradicionales de detección, midiendo métricas como la precisión, la sensibilidad y la tasa de falsos positivos.

### Investigar mejoras en la metodología utilizada y en la configuración de los algoritmos para aumentar la eficacia del sistema.

### Plan de Trabajo Detallado

Para la simulación del trabajo se manejar dos opciones;

1. Selección del Dataset o Entorno de Simulación

Se utilizará un dataset de tráfico de red que contenga tanto tráfico normal como tráfico anómalo o malicioso. Basándonos en bibliografías consultadas algunas se pueden utilizar las siguientes para la simulación:

* CICIDS 2017: Contiene tráfico de red normal y varias categorías de ataques (DoS, phishing, etc.). Este es uno de los más utilizados para la evaluación de sistemas de detección.
* UNSW-NB15: Proporciona un conjunto de datos diverso con características detalladas del tráfico de red, incluyendo tráfico normal y anómalo.

1. Entorno de Simulación Alternativo:

Para capturar tráfico en tiempo real se puede implementar Wireshark para y generar un dataset propio.

1. Lenguaje de programación

* Python se utilizará por sus bibliotecas de Machine Learning e IA.

1. Documentación de Resultados

### Metodología de Investigación

Buscar artículos académicos, libros y publicaciones recientes sobre técnicas de IA (aprendizaje supervisado, no supervisado, redes neuronales, etc.) aplicadas a la seguridad en redes.

Herramientas: Google Scholar, IEEE Xplore, SpringerLink, bases de datos académicas.

Configuración del entorno de pruebas (entorno simulado o dataset).

Implementación del algoritmo.

Documentar el proceso de investigación.

### Recursos para la Implementación

### Python

### Google Colab

### Matplotlib y Seaborn para visualizaciones de datos y resultados.