**Sistematización del Proyecto**

**LÍNEA DE INVESTIGACIÓN:**

Inteligencia Artificial aplicada a la Ciberseguridad.

**Tema General:**

Servidor Linux. 2025

**Temas Particulares:**

Logs en Servidor Linux. 2025

Servicios en Servidor Linux. 2025

Procesos en Servidor Linux. 2025

**Temas Específicos:**

Ineficiente detección de ataques de fuerza bruta en logs en Servidor Linux. 2025

Inexacto análisis de intentos de acceso no autorizado en logs en Servidor Linux. 2025

Limitada detección de patrones anómalos en logs en Servidor Linux. 2025

**Problema de Estudio:**

Ineficiente detección de ataques de fuerza bruta en logs en Servidor Linux. 2025

**Título Preliminar de la Tesis:**

Detección de ataques de fuerza bruta en logs en Servidor Linux. 2025

**Variable Dependiente:** Detección de ataques de fuerza bruta

**Objeto de Estudio:** Logs

**Alcance Espacial:** Servidor Linux

**Alcance Temporal:** 2025

**Antecedentes Bibliográficos**

Mehmmod, A., Batool, K., Sajid, A., Alam, M. M., Su’ud, M. M., & Khan, I. U. (2025). ERBM: A machine learning-driven rule-based model for intrusion detection in IoT environments. *Computers, Materials & Continua*, 81(1), 1017–1036. <https://doi.org/10.32604/cmc.2025.062971>

Kasongo, S. M. (2023). A deep learning technique for intrusion detection system using a Recurrent Neural Networks based framework. *Computer Communications*, 195, 145–158. <https://doi.org/10.1016/j.comcom.2022.12.010>

Otoom, A. F., Eleisah, W., & Abdallah, E. E. (2023). Deep learning for accurate detection of brute force attacks on IoT networks. *Procedia Computer Science*, 215, 157–164. <https://doi.org/10.1016/j.procs.2023.03.038>

Park, J., Kim, J., Gupta, B. B., & Park, N. (2021). Network log-based SSH brute-force attack detection model. *Complexity*, 2021, Article ID 6617592. <https://doi.org/10.32604/cmc.2021.015172>

Sarantos, P., Violos, J., & Leivadeas, A. (2025). Enabling semi-supervised learning in intrusion detection systems. *Journal of Parallel and Distributed Computing*, 179, 27–40. <https://doi.org/10.1016/j.jpdc.2024.105010>

**Título Tentativo de la Tesis:**

Modelo de inteligencia artificial para mejorar la detección de ataques de fuerza bruta en logs en Servidor Linux. 2025

**Variable Independiente:** Modelo de inteligencia artificial

**Variable Dependiente:** Detección de ataques de fuerza bruta

**Objeto de Estudio:** Logs

**Alcance Espacial:** Servidor Linux

**Alcance Temporal:** 2025

**ANEXO 1: MATRIZ DE CONSISTENCIA**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Título:**  Modelo de inteligencia artificial para mejorar la detección de ataques de fuerza bruta en logs en Servidor Linux. 2025 | | | | | | |
| **LINEA DE**  **INVESTIGACIÓN** | **PROBLEMA DE ESTUDIO** | **PROBLEMAS** | **OBJETIVOS** | **HIPÓTESIS** | **VARIABLES Y DIMENSIONES** | **DISEÑO**  **METODOLÓGICO** |
| Inteligencia Artificial aplicada a la Ciberseguridad | Ineficiente detección de ataques de fuerza bruta en logs en Servidor Linux. 2025 | **Problema general:**  ¿De qué manera la aplicación de modelo de inteligencia artificial se relaciona con la detección de ataques de fuerza bruta en logs en Servidor Linux en 2025? | **Objetivo general:**  Determinar la relación entre la aplicación de un modelo de inteligencia artificial y el nivel de detección de ataques de fuerza bruta en los logs en un Servidor Linux en el año 2025. | **Hipótesis general:**  Existe una relación directa y significativa entre la aplicación de un modelo de inteligencia artificial y el nivel de detección de ataques de fuerza bruta en los logs en un Servidor Linux en el año 2025. | **Variable independiente:**  Modelo de inteligencia artificial (Cuantitativo)  **Dimensiones**  - Interpretabilidad  - Arquitectura y Complejidad  - Eficiencia Computacional  - Robustez y Generalización | **Enfoque:** Cuantitativo  **Tipo de**  **Investigación:**  Aplicada  **Nivel de**  **Investigación:**  Correlacional  **Diseño:**  Experimental, Transversal |
| **OBJETO DE ESTUDIO** |
| Logs | **Problemas específicos:** | **Objetivos específicos:** | **Hipótesis específicas:** | **Variable dependiente:** |  |
| 1. ¿De qué manera la arquitectura de optimización y selección de características del algoritmo de aprendizaje adaptativo se relaciona con el reconocimiento de port-scan en el tráfico de red de una Universidad Peruana en 2025?  2. ¿Qué relación existe entre la precisión de los modelos de análisis automatizado y la identificación de intentos de acceso no autorizado en los logs en Servidor Linux en el año 2025?  3. ¿Cómo se relaciona el uso de técnicas de inteligencia artificial interpretables con la detección de patrones anómalos en los logs en Servidor Linux durante el año 2025? | O.E. 1: Determinar la relación entre la precisión del modelo de inteligencia artificial y la detección de ataques de fuerza bruta en los logs en un Servidor Linux en el año 2025.  O.E. 2: Determinar la relación entre la capacidad de generalización del modelo de inteligencia artificial y la detección de ataques de fuerza bruta en los logs en un Servidor Linux en el año 2025.  O.E. 3: Determinar la relación entre la eficiencia computacional del modelo de inteligencia artificial y la detección de ataques de fuerza bruta en los logs en un Servidor Linux en el año 2025. | H.E. 1: Existe una relación directa y significativa entre la precisión del modelo de inteligencia artificial y la detección de ataques de fuerza bruta en los logs en un Servidor Linux.  H.E. 2: Existe una relación directa y significativa entre la capacidad de generalización del modelo de inteligencia artificial y la detección de ataques de fuerza bruta en los logs en un Servidor Linux.  H.E. 3: Existe una relación directa y significativa entre la eficiencia computacional del modelo de inteligencia artificial y la detección de ataques de fuerza bruta en los logs en un Servidor Linux | Detección de ataques de fuerza bruta (Cuantitativo)  **Dimensiones**  - Precisión y Exactitud de la Detección  - Cobertura y Alcance  - Caracterización y Severidad del Ataque  - Resiliencia y Adaptabilidad de la Detección |