

UNIVERSIDAD DEL BIO-BIO

FACULTAD CIENCIAS EMPRESARIALES

**SOLICITUD INSCRIPCIÓN ACTIVIDAD DE TITULACIÓN**

**1. Identificación Alumno**

|  |  |  |
| --- | --- | --- |
| Nombre | : | Tomás Antileo Jara |
| Dirección | : | Valle Grande 2420 San Pedro de la Paz |
| Teléfono | : | +56 952253200 |
| E-Mail | : | tomas.antileo1801@alumnos.ubiobio.cl |
| Carrera | : | Ingeniería Civil Informática |
| Depto. | : | Sistemas de Información |

**2. Evaluadores**

**2.1 Profesor guía**

|  |  |  |  |
| --- | --- | --- | --- |
| Nombre | : | Juan Carlos Parra | Firma: |

**3. Proyecto**

**3.1 Título Que Identificará La Actividad De Titulación.**

|  |
| --- |
| Investigación sobre el papel de la inteligencia artificial en la detección temprana de ataques cibernéticos. |

**3.2 Objetivos Generales Y Específicos De La Actividad De Titulación.**

**3.2.1 Objetivos General**

|  |
| --- |
| Desarrollar una investigación sobre el papel de la inteligencia artificial en la detección temprana de ataques cibernéticos, con el fin de comprender su impacto en la mejora de la ciberseguridad, mediante el análisis de su eficacia y su aplicación en entornos de seguridad informática. |

**3.2.1 Objetivos Específicos**

|  |
| --- |
| 1. Realizar un estudio del estado del arte en detección de ataques cibernéticos y tecnologías de inteligencia artificial. 2. Analizar las soluciones de detección de ataques cibernéticos basadas en inteligencia artificial. 3. Evaluar el rendimiento de algoritmos de inteligencia artificial en la detección temprana de ataques cibernéticos. 4. Implementar un algoritmo con el propósito de llevar a cabo pruebas y recopilar datos. 5. Recopilar datos de pruebas de ataques cibernéticos y evaluar el rendimiento del algoritmo, mediante tasa de detección, falso positivos y otros indicadores. 6. Analizar los datos recopilados para evaluar la eficacia del algoritmo en la detección temprana de ataques cibernéticos. 7. Proponer recomendaciones y mejoras basadas en la investigación para optimizar la implementación del algoritmo de Inteligencia Artificial en la detección temprana de ataques cibernéticos. |

**3.4 Actividades a realizar**

|  |
| --- |
| Objetivo 1:   1. Revisión de la literatura. 2. Recopilación de información 3. Síntesis de información relevante.   Objetivo 2:   1. Análisis de soluciones de detección de ataques cibernéticos basadas en inteligencia artificial   Objetivo 3:   1. Selección de algoritmo de Inteligencia Artificial para detección temprana de ataques cibernéticos 2. Diseño de pruebas para comparar algoritmos de Inteligencia Artificial 3. Análisis de rendimiento de algoritmos de Inteligencia Artificial.   Objetivo 4:   1. Implementación de algoritmo de Inteligencia Artificial para detección temprana de ataques cibernéticos   Objetivo 5:   1. Ejecución de pruebas de detección 2. Recopilación de datos de pruebas 3. Evaluación de tasas de detección y falsos positivos.   Objetivo 6:   1. Evaluación del algoritmo 2. Identificación de patrones y tendencias   Objetivo 7:   1. Formulación de recomendaciones y mejoras basadas en resultados de la investigación. |

**3.3 Justificación Del Proyecto Propuesto.**

|  |
| --- |
| La justificación del proyecto de investigación sobre el papel de la inteligencia artificial en la detección temprana de ataques cibernéticos se fundamenta en las principales tendencias en ciberseguridad en un mundo cada vez más digital y conectado. La situación actual es que los ataques cibernéticos representan una amenaza constante para individuos, empresas, gobiernos y organizaciones en todo el mundo. Los métodos tradicionales de seguridad y detección de intrusiones se han vuelto insuficientes para hacer frente a la evolución constante de las amenazas cibernéticas. Los ataques “día cero” y tácticas de evasión desafían las defensas convencionales, lo que genera la necesidad de soluciones más efectivas. La creciente cantidad de información sensible que se almacena y transmite en línea ha hecho que sea más importante que nunca protegerse contra ataques cibernéticos. Una de las tendencias en el futuro de la ciberseguridad es el uso de la inteligencia artificial (IA) y el aprendizaje automático (ML), mediante algoritmos capaces de analizar gran cantidad de datos y detectar anomalías que puedan derivar en amenazas. Esto permite responder rápidamente a ataques, reduciendo el riesgo de daño y minimizando el impacto ataques. También pueden utilizarse para automatizar tareas de seguridad y predecir futuras amenazas basadas en tendencias históricas, lo que se traduce en una defensa proactiva contra las amenazas del futuro.  La propuesta de esta investigación se basa en la utilización de la inteligencia artificial para mejorar la detección temprana de ataques cibernéticos. La IA tiene el potencial de identificar patrones y anomalías en los datos de tráfico de red y sistemas informáticos que pueden ser indicativos de un ataque. Además es flexible, se puede adapta y aprende de nuevas amenazas, por lo que es una herramienta necesaria para los problemas de hoy en día.  La detección temprana de ataques cibernéticos con inteligencia artificial tiene un impacto positivo en la seguridad, protección de datos y privacidad, lo que se traduce en beneficios económicos, sociales y tecnológicos para nuestra sociedad. |

**3.5 Plan De Trabajo A Desarrollar**

|  |  |
| --- | --- |
| **Actividad** | **Rango de fechas** |
| **OBJ1: ACT1** | **28/08/2023-28/09/2023** |
| **OBJ1: ACT 2** | **28/08/2023-28/09/2023** |
| **OBJ1: ACT 3** | **28/08/2023-28/09/2023** |
| **OBJ2: ACT 1** | **20/09/2023-30/09/2023** |
| **OBJ3: ACT 1** | **01/10/2023-7/10/2023** |
| **OBJ3: ACT 2** | **07/10/2023-20/10/2023** |
| **OBJ3: ACT 3** | **20/10/2023-31/10/2023** |
| **OBJ4: ACT 1** | **01/11/2023-30/11/2023** |
| **OBJ5: ACT 1** | **01/03/2024-07/03/2024** |
| **OBJ5: ACT 2** | **07/03/2024-20/03/2024** |
| **OBJ5: ACT 3** | **20/03/2024-30/03/2024** |
| **OBJ6: ACT 1** | **01/04/2024-7/04/2024** |
| **OBJ6: ACT 2** | **07/04/2024-14/04/2024** |
| **OBJ7: ACT 1** | **14/04/2024-30/04/2024** |

**3.6 Trabajos Similares Realizados Previamente.**

|  |
| --- |
| Dentro de la Universidad del Bío Bío existen trabajos similares respecto al área de seguridad informática. El proyecto titulo Desarrollo de un sistema de monitoreo para un servidor honeypot en apoyo al curso de seguridad informática se relaciona con la detección de ataques mediante un servidor web configurado para detectar intrusos mediante la duplicación de un sistema vulnerable, desviando a los atacantes de los servidores reales.  Por otra parte, fuera de la Universidad del Bío Bío existen investigaciones similares en el campo de la ciberseguridad. Algunos trabajos son:  Aplicación de técnicas de aprendizaje automático (no supervisado) para la detección de anomalías en infraestucturas críticas cibernéticas. Trata sobre la importancia de proteger las Infraestructuras Críticas (ICs) debido a su papel fundamental en el funcionamiento de servicios esenciales. A medida que estas infraestructuras se han vuelto más conectadas a nuevas tecnologías, han aumentado sus vulnerabilidades a los ciberataques, lo que plantea una amenaza significativa para la seguridad. Se menciona que los ciberataques se han vuelto más sofisticados y que los criminales pueden evadir fácilmente los sistemas de seguridad convencionales. Por lo tanto, se propone utilizar técnicas de aprendizaje automático (ML) para abordar estas amenazas. El ML tiene la capacidad de detectar una amplia variedad de ataques, incluidos los ataques "día cero" que son previamente desconocidos.  Machine Learning Based Intrusion Detection System. Conferencia internacional que trata del campo de la detección de intrusiones en redes y sistemas informáticos. Se menciona que la detección de intrusiones es esencial para identificar actividad maliciosa en una red o sistema. Dado el aumento de la conectividad entre computadoras, se destaca la importancia de esta tecnología para garantizar la seguridad de las redes. Se menciona que se han utilizado diversas técnicas de aprendizaje automático y estadísticas para desarrollar sistemas de detección de intrusiones. El enfoque principal de la investigación se centra en mejorar la precisión de estos sistemas para reducir falsas alarmas y aumentar la tasa de detección. Para lograr esto, se aplican técnicas de aprendizaje automático, como Support Vector Machine (SVM) y Naive Bayes, en un enfoque de clasificación organizado. Además, se utiliza el conjunto de datos NSL-KDD para evaluar el rendimiento de los sistemas, y se concluye que SVM funciona mejor que Naïve Bayes en esta aplicación. En resumen, el resumen habla sobre la importancia de la detección de intrusiones, las técnicas utilizadas para mejorarla y los resultados de la evaluación de sistemas de detección de intrusos.  Deep Learning for Cybersecurity Intrusion Detection: Appreaches, Datasets, and Comparative Study. Es un estudio comparativo de enfoque basados en aprendizaje profundo para la detección de intrusiones en ciberseguridad. Examina cómo diferentes técnicas de Inteligencia Artificial pueden contribuir a la detección temprana de ataques.  Artificial intelligence, cyber-threats and Industry 4.0: challenges and opportunities. Este estudio aborda las oportunidades y amenazas en la aplicación de la inteligencia artificial (IA) en la industria manufacturera, considerando sus usos tanto en la defensa como en la ofensa. Comienza con una introducción a la Industria 4.0 y el rol de la IA en este contexto, destacando la importancia de la seguridad en los sistemas de fabricación. Luego, se examinan las técnicas de detección de intrusiones basadas en IA, evaluando sus fortalezas y debilidades en el contexto de la tecnología operativa (OT) en la manufactura. Además, se exploran las implicaciones de la IA en la supervisión, optimización y control de la producción, con ejemplos prácticos. El informe aborda desafíos técnicos, operativos y de seguridad, así como la transición hacia la Industria 4.0. Finalmente, se discuten temas como la orquestación de técnicas de detección distribuidas, la IA adversaria/robusta y la supervisión del comportamiento humano-máquina en el contexto de la seguridad en la Industria 4.0.  Survey On The Applications Of Artificial Intelligence In Cyber Security aborda el desafío creciente de la ciberseguridad en un mundo digitalizado y la necesidad de proteger información personal y financiera de los ciberataques. La investigación se centra en el uso de la Inteligencia Artificial (IA) como una herramienta transformadora para mejorar la seguridad cibernética. A través de una análisis de la literatura existente, el estudio destaca que la aplicación de la IA en la detección y mitigación de ciberataques presenta ventajas significativas en comparación con métodos convencionales. Se menciona que la tecnología de IA tiene el potencial de elevar la protección tanto de clientes como de empresas en el ciberespacio, y se destaca el aumento en el uso de motores de IA en lugar de motores de exploración tradicionales en el ámbito de la ciberseguridad. En resumen, el artículo explora cómo la IA está revolucionando la ciberseguridad y ofrece un enfoque prometedor para hacer frente a la creciente amenaza de ciberataques. |

**3.6 Descripción De Los Aspectos Fundamentales De: la Metodología de desarrollo de SW o la metodología de Investigación a utilizar.**

|  |
| --- |
| El diseño de la investigación se llevará a cabo utilizando datos de investigaciones anteriores.  El problema central de esta investigación es determinar el impacto y la efectividad de la inteligencia artificial en la detección temprana de ataques cibernéticos. Se busca comprender cómo las soluciones basadas en inteligencia artificial han mejorado la ciberseguridad y cuáles son los desafíos asociados.  La población objetivo incluye expertos en seguridad cibernética, investigadores de inteligencia artificial y profesionales de la industria de la ciberseguridad.  La recopilación de datos se realizará con una revisión a la literatura, artículos actuales y entrevistas a profesionales expertos del área de ciberseguridad e inteligencia artificial.  Se desarrollarán cuestionarios y entrevistas para la recopilación de datos. Se utilizarán herramientas de análisis de datos.  Las variables principales incluyen la eficacia de la inteligencia artificial en la detección temprana de ataques cibernéticos, los desafíos en la implementación de soluciones basadas en inteligencia artificial y la percepción de los expertos en ciberseguridad sobre la adopción de esta tecnología.  Se realizará validación cruzada utilizando diferentes fuentes de datos para garantizar la validez de los resultados. Además, se realizarán pruebas de fiabilidad para los cuestionarios.  El proyecto se desarrollará en un período de 12 meses, comenzando en septiembre de 2023 y finalizando en agosto de 2024.  Las limitaciones potenciales incluyen la disponibilidad de participantes y la calidad de los datos secundarios disponibles en la literatura existente. |

**4. Bibliografía**

**4.1 Referencia bibliografica**

|  |
| --- |
| 1. Goodfellow, I., Bengio, Y., Courville, A., "Deep Learning", The MIT Press, 2016 2. Gómez Vietes, Á., Enciclopedia de la Seguridad Informática 2a Edición Actualizada, RA-MA, 2016 3. Bishop, C. M., "Pattern Recognition and Machine Learning", Springer, 2006. 4. LeCun, Y., Bengio, Y., Hinton, G. , "Deep learning", Nature, 521(7553), 436-444, 2015 5. Russell, S. J., Norvig, P., "Artificial Intelligence: A Modern Approach", Pearson, 2016. 6. Anderson, R., Moore, T., "Information Security: The Complete Reference", McGraw-Hill Education, 2009. |

**4.2 Linkografía**

|  |
| --- |
| 1. Repositorio Digital – Sistema de Bibliotecas Universidad del Bío-Bío, Desarrollo de un sistema de monitoreo para un servidor honeypot en apoyo al curso de seguridad informática, [http://repobib.ubiobio.cl](http://repobib.ubiobio.cl/jspui/bitstream/123456789/3132/1/Carvajal%20Vergara%2c%20Jean%20Carlos.pdf) 2. Repositorio Universidad de los Andes, Colombia, Aplicación de técnicas de aprendizaje automático (no supervisado) para la detección de anomalías en infraestructuras críticas cibernéticas, 04-09-2023,   <https://repositorio.uniandes.edu.co/handle/1992/68449>   1. IEEE, Machine Learning Based Intrusion Detection System,   04-09-2023, <https://ieeexplore.ieee.org/document/8862784>   1. ScienceDirect, Deep learning for cyber security intrusión detection: Approaches, datasets, and comparative study, 04-09-2023,   <https://www.sciencedirect.com/science/article/abs/pii/S2214212619305046>   1. Springer, Artificial intelligence, cyber-threats and Industry 4.0: challenges and opportunities,   04-09-2023,<https://link.springer.com/article/10.1007/s10462-020-09942-2>   1. Research Gate, Survey on the applications of artificial intelligence in cyber security,   04-09-2023, [survey-on-applications-of-artificial-intelligence-in-cyber-security](https://www.researchgate.net/profile/Aaron-Achi/publication/355119649_Survey_On_The_Applications_Of_Artificial_Intelligence_In_Cyber_Security/links/623c6b5991e0810f44d62f22/Survey-On-The-Applications-Of-Artificial-Intelligence-In-Cyber-Security.pdf)   1. ScienceDirect, A machine learning-based intrusión detection for detecting   internet of things network attacks, 04-09-2023,  <https://www.sciencedirect.com/science/article/pii/S1110016822001570>   1. ScienceDirect, A survey of intrusion detection in Internet of Things, 04-09-2023, <https://www.sciencedirect.com/science/article/abs/pii/S1084804517300802> 2. ScienceDirect, Scalable machine learning-based intrusión detection system of IoT-enable   smart cities, 04-09-2023,  <https://www.sciencedirect.com/science/article/abs/pii/S221067072030545X>   1. Springer, Machine Learning Based Intrusion Detection Systems for IoT Applications,   04-09-2023, <https://link.springer.com/article/10.1007/s11277-019-06986-8>   1. CSIRT, IBM Ciberamenazas en redes industriales, 04-09-2023,   <https://www.csirt.gob.cl/media/2021/09/Amenzas-Cibernetica-28-Redes-industriales.pdf>   1. BBVA Open Mind, El futuro de la ciberseguridad. Previsiones y tendencias, 06-09-2023,   [https://www.bbvaopenmind.com/tecnologia/mundo-digital/futuro-ciberse0guridad-previsiones-tendencias/](https://www.bbvaopenmind.com/tecnologia/mundo-digital/futuro-ciberseguridad-previsiones-tendencias/#:~:text=Una%20de%20las%20mayores%20tendencias,puedan%20indicar%20una%20amenaza%20potencial.) |

Texto, Carta

Descripción generada automáticamente

**LA PRESENTE SOLICITUD DE INSCRIPCIÓN DE LA ACTIVIDAD DE TITULACIÓN SIGNIFICA UN COMPROMISO DE CUMPLIR LO ESTIPULADO EN ELLA.**

**………………………………….**

**FIRMA ALUMNO**

**………………………………….**

**FIRMA ALUMNO**

**FECHA PRESENTACIÓN SOLICITUD: ....... 06-09-2023 ................................**

|  |
| --- |
| **RESOLUCIÓN DIRECTOR DE ESCUELA/JEFE DE CARRERA** |
| **APROBADO**   * **REPROBADO**   **OBSERVACIONES: ……………………………………………………………………….........................................................................................................................................................................................................................................................................................................................................................................................................**  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **FIRMA DIRECTOR DE ESCUELA**  **/JEFE DE CARRERA**  **FECHA RESOLUCIÓN: ………………………………………** |