Revista Colón Ciencias, Tecnología y Negocios
ISSN L: 2313-7819
revistas.up.ac.pa/index.php/revista_colon_ctn
Vol. 12, Nº 1 Enero – Junio 2025

pp. 32 - 48

Introducción a la Inteligencia Artificial y el Aprendizaje Automático en Ciberseguridad

Introduction to Artificial Intelligence and Machine Learning in Cybersecurity

Abimelec Antek Arias Ariza[1], Miguel Vargas-Lombardo[2]

[1] Universidad Tecnológica de Panamá, Facultad de Ingeniería de Sistemas Computacionales, Panamá. abimelec.arias@utp.ac.pa. https://orcid.org/0009-0007-3902-8261
[2] Universidad Tecnológica de Panamá, Facultad de Ingeniería de Sistemas Computacionales, Panamá. miguel.vargas@utp.ac.pa. https://orcid.org/0000-0002-2074-2939

Recibido: 28 de junio de 2024 Aceptado: 9 de octubre de 2024

DOI https://doi.org/10.48204/j.colonciencias.v12n1.a6824

Resumen

La ciberseguridad juega un papel vital en la protección de activos digitales y la privacidad de los individuos en la era de la información. En este contexto, la inteligencia artificial (IA) y el aprendizaje automático (ML) han emergido como herramientas poderosas para mejorar la detección y prevención de amenazas cibernéticas. Este articulo analiza la utilización de la IA y el ML en ciberseguridad, examinando su evolución histórica, ventajas y limitaciones, así como su impacto social y consideraciones éticas. Se realiza una revisión de la literatura científica y técnica mediante palabras clave “"Inteligencia Artificial en ciberseguridad", "Machine Learning en seguridad informática" y "IA y ML en detección de amenazas" en las bases de datos IEEE Xplore, ScienceDirect y ACM Digital Library seleccionando 30 referencias útiles de un total 150 artículos identificados. Se aplicó un cuestionario a 12 ingenieros de sistemas de diversas empresas del país que cuentan con al menos una maestría en ciberseguridad con el propósito de conocer si logran implementar la técnica PICOC en entornos de ciberseguridad. La inteligencia artificial y el machine

learning han revolucionado la ciberseguridad al permitir la detección automatizada de amenazas, el análisis de comportamientos anómalos, y la generación de respuestas más rápidas y precisas ante potenciales ataques cibernéticos.

Palabras clave: Amenazas cibernéticas; protección de datos; detección de amenazas; ataques informáticos; tecnologías de la información.

Abstract

Cybersecurity plays a vital role in protecting digital assets and the privacy of individuals in the information age. In this context, artificial intelligence (AI) and machine learning (ML) have emerged as powerful tools to improve the detection and prevention of cyber threats. This article analyzes the use of AI and ML in cybersecurity, examining its historical evolution, advantages and limitations, as well as its social impact and ethical considerations. A review of scientific and technical literature is carried out using keywords "Artificial Intelligence in cybersecurity", "Machine Learning in computer security" and "AI and ML in threat detection" in the IEEE Xplore, ScienceDirect and ACM Digital Library databases, selecting 30 useful references from a total of 150 articles identified. A questionnaire was applied to 12 systems engineers from various companies in the country who have at least a master's degree in cybersecurity in order to find out if they can implement the PICOC technique in cybersecurity environments. Artificial intelligence and machine learning have revolutionized cybersecurity by allowing the automated detection of threats, the analysis of abnormal behavior, and the generation of faster and more accurate responses to potential cyber-attacks.

Keywords: Cyber threats; data protection; threat detection; computer attacks; information technologies.

Introducción

La ciberseguridad se ha vuelto una preocupación cada vez más relevante en un mundo hiperconectado y dependiente de la tecnología. En este contexto, la inteligencia artificial (IA) y el aprendizaje automático o *machine learning* (ML), en idioma inglés, han emergido como herramientas clave para fortalecer la protección de la información digital y combatir las crecientes amenazas cibernéticas. Este artículo propone explorar la evolución, desafíos, consideraciones éticas y el impacto social de la IA y el ML en la ciberseguridad, analizando cómo estas tecnologías avanzadas están siendo utilizadas para proteger redes, sistemas y datos críticos en un entorno digital cada vez más complejo y peligroso (Swinfen Green, 2015).

Tanto la inteligencia artificial (IA) y el machine learning (ML) han revolucionado el campo de la ciberseguridad brindando nuevas herramientas y enfoques para la detección y mitigación de amenazas cibernéticas. La inteligencia artificial y el machine learning son dos ramas de la computación que buscan imitar la inteligencia humana y aprender de los datos, respectivamente. En el contexto de la ciberseguridad, estas tecnologías se utilizan para identificar patrones, detectar anomalías y predecir posibles amenazas en tiempo real (Apruzzese et al., 2023)

Al aprovechar algoritmos sofisticados y modelos predictivos, la IA y el ML permiten a los expertos en ciberseguridad anticiparse a los ataques, responder más rápidamente y fortalecer las defensas de las organizaciones ante las crecientes amenazas en línea (Ebert & Beck, 2023). Los sistemas de IA son capaces de procesar grandes cantidades de datos en tiempo real, identificar patrones sutiles y tomar decisiones precisas para proteger activos críticos de una organización. Ejemplos de aplicaciones de IA en ciberseguridad incluyen sistemas de detección de intrusiones basados en aprendizaje profundo, análisis de comportamiento de usuarios para detectar accesos no autorizados y sistemas de autenticación biométrica para mejorar la seguridad en las redes (Al-Garadi et al., 2019).

Los beneficios que aportan la IA y el ML en ciberseguridad y su implementación presenta desafíos significativos. La falta de datos de calidad y etiquetados, la aplicabilidad de los modelos, la privacidad de los datos y la adversarialidad son algunos de los retos que enfrentan los

profesionales de la ciberseguridad al adoptar tecnologías avanzadas como la IA y el ML. Además, la escasez de talento especializado y la necesidad de capacitación continua para mantenerse al día con las últimas tendencias en IA y ML representan desafíos adicionales en la integración de estas tecnologías en los programas de ciberseguridad de las organizaciones.

A medida que la ciberdelincuencia continúa evolucionando, la inteligencia artificial y el machine learning jugarán un papel cada vez más importante en la protección de activos digitales. Se espera que las organizaciones inviertan en soluciones de IA y ML para fortalecer sus defensas cibernéticas, mejorar la detección y respuesta a incidentes, y anticiparse a las amenazas emergentes en un entorno digital en constante cambio. El futuro de la ciberseguridad estará definido en gran medida por la capacidad de las organizaciones para integrar de manera efectiva la IA y el ML en sus estrategias de seguridad, adaptándose a un panorama cada vez más desafiante y sofisticado en materia de ciberamenazas (Montasari, 2024).

La integración de tecnologías como la inteligencia artificial (IA), blockchain, eXplainable AI (XAI), aprendizaje automático (machine learning), aprendizaje incremental y aprendizaje profundo ha revolucionado diversas industrias, desde la ciberseguridad hasta la salud. En este artículo se analizarán estas técnicas, sus aplicaciones y sus implicaciones en la actualidad.

Las técnicas de inteligencia artificial (IA) en la ciberseguridad, con un enfoque especial en la técnica PICOC (*Predictive Continuous Compromise Detection*). Se analizará cómo esta técnica puede mejorar la protección de las redes y sistemas de información. La ciberseguridad es un campo en constante evolución, con ciberataques cada vez más sofisticados. La IA y el ML han demostrado ser herramientas poderosas para detectar y prevenir amenazas cibernéticas en tiempo real, gracias a su capacidad para analizar grandes cantidades de datos en tiempo real e identificar patrones anómalos en el comportamiento de los sistemas.

Algunas de las aplicaciones más comunes incluyen la detección de *malware*, el análisis de registros de seguridad y la identificación de vulnerabilidades en redes. La historia de la inteligencia artificial y el machine learning en la ciberseguridad se remonta a las décadas pasadas, con la aplicación de algoritmos de aprendizaje automático para la detección de intrusiones y análisis de

comportamiento malicioso en redes informáticas. Ejemplos específicos de investigaciones muestran cómo la IA y el ML han mejorado la detección temprana de amenazas cibernéticas, la identificación de patrones de ataque y la toma de decisiones automáticas en tiempo real.

El uso de redes neuronales convolucionales para detectar intrusiones en tiempo real en sistemas informáticos es un ejemplo de investigación destacada relacionada al ciberataque. Otro caso es el desarrollo de algoritmos de aprendizaje automático para predecir ataques de *phishing* y *malware* con alta precisión.

Investigaciones recientes han demostrado el potencial de la IA y el ML en la ciberseguridad, destacando casos donde algoritmos de aprendizaje automático han mejorado la detección de malware, la identificación de ataques de denegación de servicio distribuidos (DDoS, por sus siglas en inglés) y la predicción de comportamientos maliciosos en redes corporativas.

La inteligencia artificial es el campo de la informática que se enfoca en crear sistemas capaces de realizar tareas que requieren inteligencia humana. Entre las técnicas clave se encuentran el aprendizaje automático, el aprendizaje profundo y el aprendizaje incremental. Las técnicas como blockchain, XAI, machine learning, aprendizaje profundo e incremental permiten a los sistemas aprender, mejorar y adaptarse a medida que se exponen a más datos. Como bien lo indica Tama et al. (2017) sobre la blockchain es una estructura de datos que garantiza la integridad y seguridad de la información almacenada en bloques en una red distribuida. Su uso va más allá de las criptomonedas, abarcando contratos inteligentes, trazabilidad y transacciones segura.

Por otra parte, XAI se refiere a la capacidad de los sistemas de IA para explicar sus decisiones de manera comprensible para los humanos. Esto es crucial en campos como la salud y la toma de decisiones críticas según Narasimhan (2017) y el aprendizaje automático es una rama de la inteligencia artificial que permite a las máquinas aprender y mejorar a partir de datos sin intervención explícita. Las técnicas de ML incluyen el aprendizaje supervisado, no supervisado, y por refuerzo (Salamanca Rativa, 2021). De igual forma, el aprendizaje incremental es una técnica que implica la actualización continua de un modelo de ML a medida que se introducen nuevos datos, lo que permite una adaptación constante a entornos cambiantes (Millán Santamaría, 2023).

El aprendizaje profundo, o deep learning, es una técnica de ML que utiliza redes neuronales artificiales con múltiples capas para extraer características y patrones complejos de datos no estructurados (LeCun et al., 2015). La inteligencia artificial ha demostrado ser una herramienta poderosa en la detección de amenazas cibernéticas, gracias a su capacidad para procesar grandes cantidades de datos e identificar patrones y comportamientos maliciosos. Las técnicas de IA, como el aprendizaje automático, el aprendizaje profundo y la minería de datos, permiten a los sistemas de ciberseguridad adaptarse y responder de manera proactiva a las amenazas en tiempo real.

La inteligencia artificial y el machine learning son conceptos interrelacionados pero distintos dentro del campo de la tecnología. Existen diferencias clave entre ambas disciplinas, así como los requerimientos, especificaciones técnicas, procesos de implementación y migración asociados con su adopción en entornos empresariales (Alfonso Galipienso et al., 2003). Diferenciación entre inteligencia artificial y machine learning se refiere a la capacidad de las máquinas para realizar tareas que normalmente requieren inteligencia humana, como el razonamiento, el aprendizaje y la resolución de problemas (Russell, 2004).

El machine learning es una subdisciplina de la inteligencia artificial que se enfoca en el desarrollo de algoritmos y modelos que permiten a las máquinas aprender .de los datos y mejorar su rendimiento sin una programación explícita (Goodfellow et al., 2016). Requerimientos y especificaciones técnicas se necesita definir los requisitos de hardware y software necesarios para implementar soluciones de inteligencia artificial y machine learning, como potencia de cálculo, capacidad de almacenamiento y acceso a datos, esta selección de herramientas y plataformas de desarrollo que sean compatibles con los algoritmos y modelos utilizados, así como con los requisitos de seguridad y privacidad de la información. Se deben establecer criterios de evaluación de desempeño y métricas de éxito para medir la eficacia de las soluciones implementadas (Hastie et al., 2009).

Siendo el entrenamiento de modelos, y su validación de resultados, y optimización de algoritmos mejora la precisión y la eficiencia de las soluciones de inteligencia artificial y machine learning (Chollet, 2021). La diferencia fundamental entre inteligencia artificial y machine learning,

así como los requerimientos, especificaciones técnicas, procesos de implementación y migración relevantes para la adopción exitosa de estas tecnologías en entornos empresariales. Al comprender estas diferencias y consideraciones, las organizaciones pueden tomar decisiones informadas para implementar soluciones de inteligencia artificial y machine learning que impulsen la innovación y la eficiencia en sus operaciones (Geron, 2022).

La inteligencia artificial (IA) y el machine learning (ML) son áreas interconectadas que tienen como objetivo capacitar a las máquinas para llevar a cabo tareas de manera autónoma. Poseen las similitudes fundamentales entre la IA y el ML, así como los requerimientos, especificaciones técnicas, procesos de implementación y migración asociados con su aplicación en entornos empresariales (Bishop, 2006). Las similitudes entre la inteligencia Artificial y el machine learning ambas son disciplinas buscan capacitar a las máquinas para aprender de los datos y tomar decisiones autónomas, tanto la IA como el ML utilizan algoritmos y modelos para analizar patrones, extraer información y predecir resultados y se basan en el procesamiento de grandes volúmenes de datos para mejorar la precisión y eficiencia de las aplicaciones (Sutton & Barto, 2018).

También existen requerimientos y especificaciones técnicas para establecer necesidades de hardware y software adecuadas para admitir soluciones de inteligencia artificial y machine learning, como capacidad de procesamiento, memoria y almacenamiento, escoger adecuadamente las herramientas y plataformas que sean compatibles con los algoritmos utilizados, así como con los requisitos de seguridad y complican de la organización, definir métricas de evaluación de desempeño y criterios de éxito para medir la eficacia de las soluciones implementadas (Domingos, 2015). Los procesos de implementación y migración para evaluar los casos de uso pertinentes, para la implementar soluciones de IA y ML dentro de la organización, requiere de identificar y preparar una serie de conjuntos de datos relevantes para el entrenamiento de los modelos de aprendizaje automático y su desarrollo, mejoran con su entrenamiento y validación de modelos, así como su integración en los procesos empresariales existentes (Murphy, 2012). Al hacerlo, podrán mejorar la eficiencia, la precisión y la innovación en sus procesos empresariales (Murillo Tovar, 2021).

Según Dasgupta et al. (2022), Russell (2004) y Chen (2012), es necesario describir los requerimientos del software en ciberseguridad para implementar IA o ML deberá conocer de vectores de ataques, comportamiento de usuarios, los protocolos de seguridad y de disponer de herramientas automatizadas para el contraataque; también deben ser profesionales con experiencia en patrones de tráfico y comportamiento de sistemas software anómalos; además de contar con las capacidades de procesamiento dentro de una infraestructura tecnológica (*cloud computing*) altamente escalable.

En esta investigación, se plantea la técnica PiCoc o *Predictive Continuous Compromise Detection*, la cual se centra en la detección temprana de vulnerabilidades de seguridad en entornos informáticos. Utilizando algoritmos avanzados de Machine Learning y análisis de comportamiento anómalo PiCoc es capaz de identificar posibles amenazas incluso antes de que se materialicen totalmente, permitiendo una respuesta más rápida y efectiva a los incidentes de seguridad.

Metodología

Se realizó una revisión exhaustiva de la literatura científica y técnica relacionada con la aplicación de IA y ML en ciberseguridad. Se utilizaron bases de datos académicas como IEEE Xplore, ScienceDirect y ACM Digital Library para identificar estudios relevantes. Se emplearon palabras clave como "Inteligencia Artificial en ciberseguridad", "Machine Learning en seguridad informática" y "IA y ML en detección de amenazas". Se analizaron diferentes estudios y casos de éxito en los que se han implementado estas tecnologías, así como sus metodologías y resultados obtenidos. En total 150 artículos de las fuentes señalas anteriormente (mayo-junio, 2024) y de las cuales se obtuvieron 30 referencias útiles (ver referencias) para esta actividad de investigación que apenas inicia con este estudio.

La aplicación de IA y ML en ciberseguridad plantea importantes implicaciones conceptuales, ya que permite mejorar la eficiencia y la efectividad de los sistemas de protección. Además, estas tecnologías pueden ayudar a anticipar y mitigar posibles riesgos, contribuyendo a la

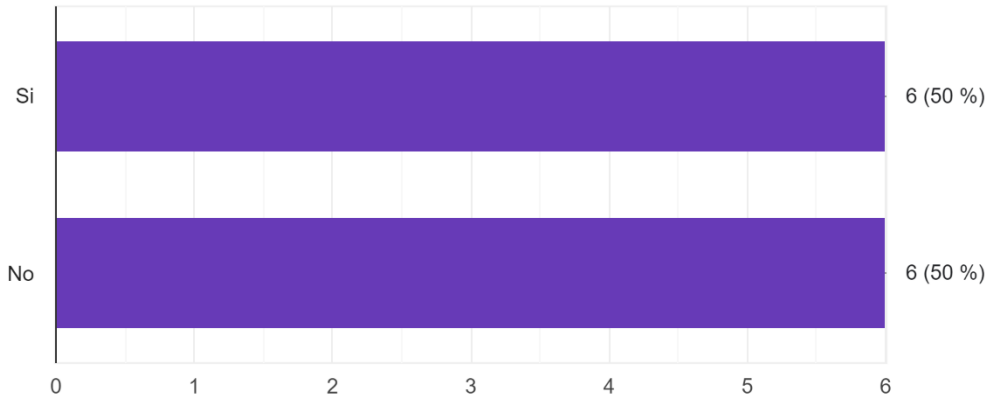
seguridad de la información. Se ha elaborado un cuestionario a 12 ingenieros de sistemas de diversas empresas del país y cuentan con al menos una maestría en ciberseguridad, con ello buscamos conocer si logran implementar la técnica PiCoc en entornos de ciberseguridad puede llevar a una detección más proactiva de amenazas, reduciendo el tiempo de respuesta a los incidentes y minimizando el impacto de posibles ataques.

Resultados

Los especialistas que se tomaron como muestra para la encuesta indica lo siguiente sobre el tema. En la primera pregunta de la encuesta podemos validar que se solo el 50% de las empresas de los encuestados para algunos de sus procesos utilizan la IA-ML en su ciberseguridad, el resto de los encuestados desconocen su uso (Figura 1).

Figura 1.

Porcentaje de empresas que lo utiliza IA o ML en sus sistemas de ciberseguridad

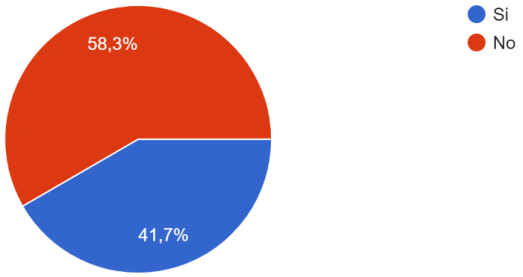


En la segunda pregunta seleccionada se puede comprobar que menos de la mitad, sólo el 41.7% de las empresas en Panamá utilizan como medida de seguridad para prevenir ciberataques la IA-ML (Véase Figura 2).

Revista Colón Ciencias, Tecnología y Negocios
ISSN L: 2313-7819
revistas.up.ac.pa/index.php/revista_colon_ctn
Vol. 12, Nº 1 Enero – Junio 2025

Figura 2.

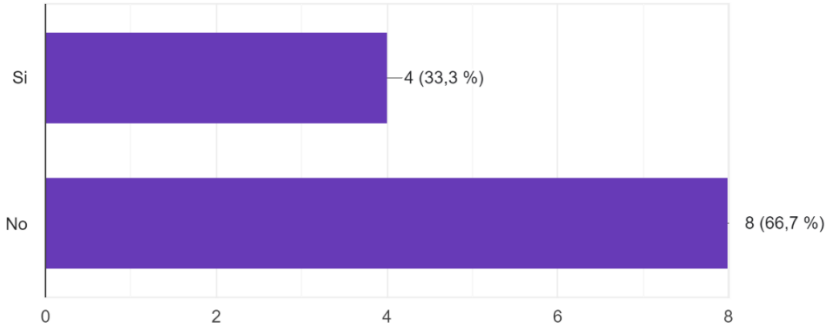
Muestra prevención de ataques



En la pregunta 3 se puede validar que para temas sobre ciberseguridad no se está utilizando IA-ML, sólo el 33% de las empresas en Panamá lo utilizan (Figura 3).

Figura 3.

Muestra el uso de IA – ML para temas regulatorios de ciberseguridad

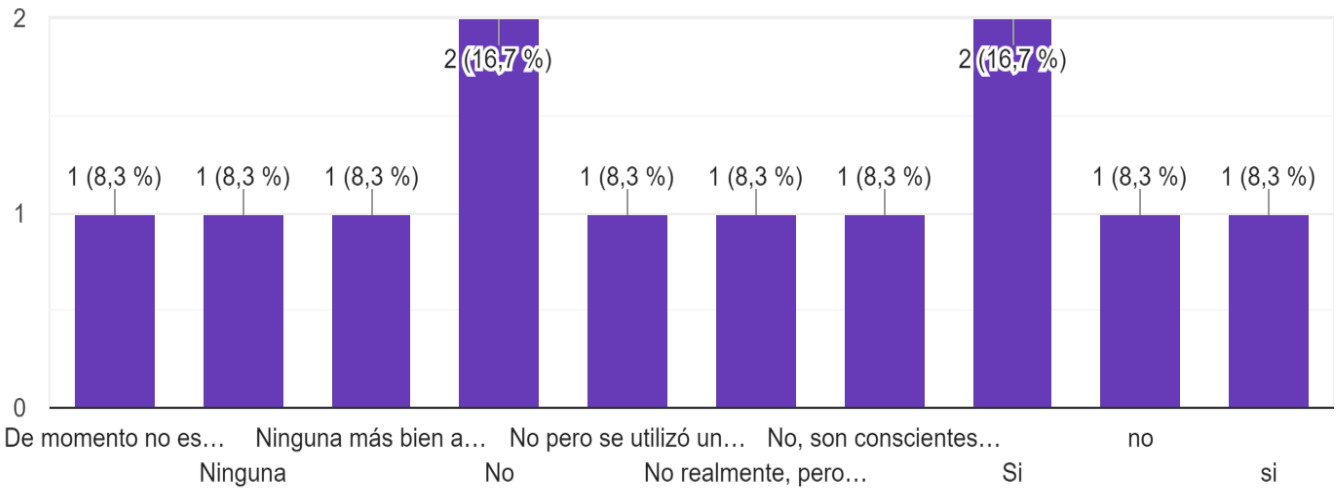


En la Figura 4, las respuestas a la siguiente pregunta muestran la casi nula utilización de las herramientas que nos ofrece la inteligencia artificial y machine learning en temas de ciberseguridad en Panamá, la resistencia de las compañías al cambio en temas de su ciberseguridad.

Revista Colón Ciencias, Tecnología y Negocios
ISSN L: 2313-7819
revistas.up.ac.pa/index.php/revista_colon_ctn
Vol. 12, Nº 1 Enero – Junio 2025

Figura 4.

Nivel de implementación de IA-ML en ciberseguridad en Panamá

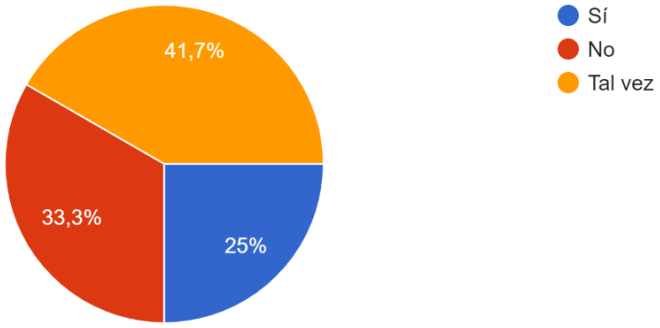


La pregunta 5 aborda el tema de externalizar la gestión de ciberseguridad a una empresa tercera para que realice la migración además del uso de inteligencia artificial y machine learning, se puede validar que solo el 25 % estaría dispuesto (Figura 5).

Figura 5.

Utilizar proveedores externos de ciberseguridad en empresas en Panamá

Revista Colón Ciencias, Tecnología y Negocios
ISSN L: 2313-7819
revistas.up.ac.pa/index.php/revista_colon_ctn
Vol. 12, Nº 1 Enero – Junio 2025



Resultados adicionales muestran que solamente el 33% utilizan la inteligencia artificial y machine learning para los procesos de análisis forense de sistemas cibernéticos. Sin embargo, los encuestados mantienen una opinión del 92% que la inteligencia artificial y el machine learning en ciberseguridad facilita el monitoreo de comportamientos anómalos en la red.

Al comparar los métodos tradicionales de ciberseguridad con aquellos donde se implementan la inteligencia artificial y machine learning, el 83% de los profesionales que se desempeñan en el área de ciberseguridad en Panamá indican que los procesos y los temas de ciberseguridad mejora con su uso.

La encuesta realizada sobre la implementación de IA y ML en ciberseguridad en las empresas en Panamá arroja una consideración preocupante, que la adopción de estas tecnologías aún es limitada. A pesar del potencial de la IA y el ML para mejorar la seguridad cibernética, la mayoría de las empresas encuestadas no las están utilizando de forma significativa. Esto sugiere que existe una brecha considerable entre el conocimiento de estas tecnologías y su aplicación práctica. La falta de conocimiento afecta a muchas empresas ya que no tienen el conocimiento técnico necesario para implementar IA y ML en sus sistemas de seguridad. Esto agravado por los costos de la implementación de IA y ML requiere inversiones significativas en hardware, software y personal especializado. La falta de confianza de las empresas aún no confía en las capacidades de la IA y el ML para detectar y responder a amenazas cibernéticas de forma efectiva.

Conclusiones

La aplicación de IA y ML en ciberseguridad ofrece oportunidades significativas para mejorar la protección de nuestros sistemas y datos, permitiendo detectar y prevenir amenazas de forma más eficiente y precisa. Sin embargo, es necesario abordar desafíos como el sesgo en los algoritmos y la protección de la privacidad de los datos para garantizar un uso ético y responsable de estas tecnologías.

La integración de la inteligencia artificial y el machine learning en ciberseguridad ha demostrado ser un avance significativo en la detección y prevención de amenazas cibernéticas. A pesar de los desafíos existentes, estas tecnologías prometen mejorar la seguridad digital en el futuro. La inteligencia artificial y el machine learning han demostrado ser herramientas valiosas para que las organizaciones fortalezcan su ciberseguridad y hagan frente a las amenazas digitales cada vez más sofisticadas. Al implementar soluciones basadas en estas tecnologías, las empresas pueden mejorar la detección, prevención y respuesta a incidentes, optimizar la gestión de riesgos y mantener una postura de seguridad más sólida y adaptable.

La integración de la IA y ML en sistemas de seguridad existentes puede requerir cambios significativos en la infraestructura, lo cual es complejo. Esto y la falta de casos de éxito claros y medibles puede dificultar la justificación de la inversión en IA y ML para la ciberseguridad. Educar y capacitar es fundamental invertir en programas de educación y capacitación para que las empresas comprendan el potencial de la IA y el ML en ciberseguridad. Incentivos y apoyo Se necesitan incentivos y apoyo gubernamental para promover la adopción de IA y ML en ciberseguridad, incluyendo programas de subvenciones y financiamiento. Casos de éxito de la implementación de IA y ML en ciberseguridad para demostrar su eficacia. Herramientas y Plataformas accesibles de IA y ML más fáciles de usar para que las empresas puedan implementar estas tecnologías de forma más sencilla. La encuesta pone de manifiesto la necesidad de un mayor esfuerzo para promover la adopción de IA y ML en ciberseguridad. Las empresas deben invertir en conocimiento, capacitación y herramientas para aprovechar el potencial de estas tecnologías y mejorar la seguridad de sus sistemas.

Sin embargo, es crucial abordar los desafíos y consideraciones clave para una adopción exitosa y responsable de la IA y el ML en el ámbito de la ciberseguridad (Nolasco-Mamani et al., 2023). La técnica PiCoc, basada en la predicción continua de compromisos de seguridad, se presenta como una herramienta prometedora en la lucha contra las amenazas cibernéticas. Su capacidad de detectar posibles ataques antes de que se materialicen completamente ofrece nuevas oportunidades para fortalecer la seguridad informática. Sin embargo, es fundamental abordar los desafíos técnicos y éticos asociados con su implementación para garantizar su eficacia y aceptación.

En conclusión, la inteligencia artificial y el machine learning representan un avance significativo en la ciberseguridad, proporcionando herramientas poderosas para combatir las amenazas cibernéticas en un entorno digital cada vez más complejo. Sin embargo, es indispensable abordar las limitaciones, desafíos, consideraciones éticas y el impacto social de la integración de la IA y el ML en la ciberseguridad para garantizar su uso efectivo y responsable en beneficio de la sociedad.

Conflicto de interés

Los autores declaran que no existe conflicto de interés en la redacción de este artículo.

Agradecimiento

A la Secretaría Nacional de Ciencia y Tecnología (SENACYT) y al Sistema Nacional de Investigación (SNI) por los fondos destinados a esta investigación en su primera fase.

Referencias Bibliográficas

Alfonso Galipienso, M.I., Cazorla Quevedo, M.A., Colomina Pardo, O., Escolano Ruiz, F., Lozano Ortega, M.A. (2003). *Inteligencia Artificial: modelos, técnicas y áreas de aplicación*. Ediciones Paraninfo, S.A. Madrid, España.

Al-Garadi, M. A., Hussain, M.R., Khan, N., Murtaza, G., Nweke, H. & Ali, I. (2019). Predicting Cyberbullying on Social Media in the Big Data Era Using Machine Learning Algorithms: Review of Literature and Open Challenges. *IEEE Access*, 7, 70701-70718. https://ieeexplore.ieee.org/document/8720155

Apruzzese, G., Laskov, P., Montes, E., et al. (2023). The Role of Machine Learning in Cybersecurity. *Digital Threats: Research and Practice*, 4 (1), 1-38. https://doi.org/10.1145/3545574

Bishop, C. M. (2006). *Pattern Recognition and Machine Learning*. Springer, 2, 1122-1128. https://link.springer.com/book/9780387310732

Chen, H. C. (2012). Business Intelligence and Analytics: From Big Data to Big Impact. *MIS Quarterly*, 36(4), 1165–1188. https://doi.org/10.2307/41703503.

Chollet, F. (2021). *Deep Learning with Python*. Shelter Island, NY, USA: Manning Publications Co. https://www.manning.com/books/deep-learning-with-python

Dasgupta, D., Akhtar, Z. & Sen, S. (2022). Machine learning in cybersecurity: a comprehensive survey. *The Journal of Defense Modeling and Simulation*, 19 (1), 57-106. https://doi.org/10.1177/1548512920951275

Domingos, P. (2015). The Master Algorithm: How the Search for the Ultimate Learning Machine Will Remake Our World. *Computer and Technology Magazine*, 15 (02). https://www.redalyc.org/comocitar.oa?id=638067264018

Ebert, C. & Beck, M. (2023). Artificial Intelligence for Cybersecurity. *IEEE Software*, 40 (6), 27-34. https://doi.org/10.1109/MS.2023.3305726

Geron, A. (2022). *Hands-On Machine Learning with Scikit-Learn, Keras & TensorFlow.* O´Reilly Media Inc. California, U.S.A. https://books.google.com.pa/books?id=HHetDwAAQBAJ&printsec=frontcover&redir_esc=y#v=onepage&q&f=false

Goodfellow, I., Bengio, Y. & Courville, A. (2016). *Deep Learning*. MIT press. Cambridge, AM, U.S.A.

Hastie, T., Tibshiriani, R. & Friedman, J. (2009). *The Elements of Statistical Learning Data Mining, Inference and Prediction.* Springer Science, Second Edition, New York, U.S.A.

LeCun, Y., Bengio, Y, & Hinton, G. (2015). Deep learning. *Nature*, 521, 436-444. https://doi.org/10.1038/nature14539

Millán Santamaría, S. (2023). *Machine Learning Operations (MLOps): contexto actual y tendencias futuras*. [Trabajo de Fin de Máster - Universidad de La Rioja]. https://investigacion.unirioja.es/documentos/655c98b6da93c5320dbe7690/f/655c98b6da93c5320dbe768f.pdf

Montasari, R. (2024). Addressing Ethical, Legal, Technical, and Operational Challenges in Counterterrorism with Machine Learning: Recommendations and Strategies. In: *Cyberspace, Cyberterrorism and the International Security in the Fourth Industrial Revolution*. Springer, Cham. https://doi.org/10.1007/978-3-031-50454-9_10

Murillo Tovar, L. P. (2021). *Implementación de la industria 4.0 en el sector de tecnologías de información*. [Trabajo de Máster - Instituto Tecnológico de Mérida]. Repositorio Institucional – ITM. https://rinacional.tecnm.mx/handle/TecNM/4517

Murphy, K. P. (2012). *Machine learning: a probabilistic perspective*. MIT Press. Cambridge,

MA, U.S.A.

Narasimhan, K. S. (2017). Economic efficiency of adaptive trading algorithms: A case study with XAI. *Journal of Machine Learning Research*, 18 (1), 123-135.

Nolasco-Mamani, M.A, Espinosa, S. & Choque-Salcedo, R. (2023). Innovación y Transformación Digital en la Empresa. ACVENISPROH Académico, 67. https://doi.org/10.47606/ACVEN/ACLIB0039

Russell, S. J. (2004). *Inteligencia Artificial: un enfoque moderno*. Pearson Prentice Hall. México. https://www.academia.edu/49826989/Inteligencia_artificial_un_enfoque_moderno_stuart_j_russell

Salamanca Rativa, I. N. (2021). Técnicas de aprendizaje automático aplicadas en los sistemas de predicción. *Tecnología, Investigación y Academia*, 8(1), 37–53. https://revistas.udistrital.edu.co/index.php/tia/article/view/17325

Sutton, R. & Barto, A.G. (2018). *Reinforcement Learning: an Introduction*. MIT Press. Cambridge, MA, U.S.A.

Swinfen Green, J. (2015). *Cyber security: An introduction for non-technical managers.* Gower Publishing Limited. Burlington, VT, U.S.A.

Tama, B. A., Kweka, B. J., Park, Y., & Rhee, K. H. (2017). *A critical review of blockchain and its current applications.* International Conference on Electrical Engineering and Computer Science, IEEE Xplore, 109-113. https://doi.org/10.1109/ICECOS.2017.8167115.