Journal of Multidisciplinary Novel Journeys & Explorations

Vol. 2 Num. 1 (2024)

JMNJE V.2 N.1 004

Artículo de Investigación

Elevando la Resiliencia Cibernética en Universidades: IA para la Detección Proactiva de Amenazas

Elevating Cyber Resilience in Universities: AI for Proactive Threat Detection

Autores:
Rosa María Vera Molina
Universidad Técnica de Babahoyo
Babahoyo – Ecuador
alexrosado1996@gmail.com
https://orcid.org/0009-0004-1127-1057

Corresponding Author: *Rosa María Vera Molina*, alexrosado1996@gmail.com

Reception date: 5-Agosto-2024 **Acceptance:** 29-Septiembre-2024 **Publication:** 9-Octubre-2024

How to cite this article:

Vera Molina, R. M. (2024). Elevando la Resiliencia Cibernética en Universidades: IA para la Detección Proactiva de Amenazas. *Journal of Multidisciplinary Novel Journeys & Explorations*, *2*(1). https://sagespherejournal.com/index.php/JMNJE/article/view/56

RESUMEN

Las instituciones de educación superior enfrentan crecientes desafíos en ciberseguridad debido al aumento de amenazas cibernéticas. En este contexto, la inteligencia artificial (IA) se ha convertido en una herramienta clave para la detección y prevención de intrusiones. Sin embargo, su implementación en entornos universitarios aún presenta diversas barreras. Este estudio tuvo como objetivo analizar la implementación de sistemas de IA para la detección de intrusiones y su impacto en la resiliencia cibernética de las universidades. Para ello, se realizaron encuestas a 200 estudiantes y entrevistas semiestructuradas a 10 docentes de la Escuela Superior Politécnica de Chimborazo (ESPOCH). Las encuestas evaluaron el nivel de conocimiento sobre ciberseguridad, la percepción sobre el uso de IA en la detección de amenazas y la factibilidad de su implementación. Las entrevistas exploraron desafíos, oportunidades y limitaciones en este proceso.Los resultados mostraron una percepción positiva sobre la integración de la IA en la ciberseguridad universitaria, con un alto nivel de aceptación tanto de estudiantes como de docentes. No obstante, se identificaron desafíos como la falta de infraestructura tecnológica, la necesidad de capacitación y las preocupaciones sobre la privacidad de los datos. A pesar de estas barreras, la mayoría de los participantes consideró factible su implementación a mediano plazo, siempre que se garantice inversión en recursos y formación especializada.

Palabras clave: Inteligencia artificial, ciberseguridad, detección de intrusiones, educación superior, resiliencia cibernética.

ABSTRACT

Higher education institutions face increasing cybersecurity challenges due to the rise of cyber threats. In this context, artificial intelligence (AI) has become a key tool for detecting and preventing intrusions. However, its implementation in university environments still presents various barriers. This study aimed to analyze the implementation of AI systems for intrusion detection and their impact on the cyber resilience of universities. To achieve this, surveys were conducted with 200 students and semi-structured interviews with 10 faculty members of the Higher Polytechnic School of Chimborazo (ESPOCH). The surveys assessed the level of knowledge about cybersecurity, the perception of using AI in threat detection, and the feasibility of its implementation. The interviews explored challenges, opportunities, and limitations in this process.The results showed a positive perception of the integration of AI in university cybersecurity, with high acceptance from both students and faculty. Nevertheless, challenges such as the lack of technological infrastructure, the need for training, and concerns about data privacy were identified. Despite these barriers, the majority of participants considered its implementation feasible in the medium term, provided that investment in resources and specialized training is ensured.

Keywords: Artificial intelligence, cybersecurity, intrusion detection, higher education, cyber resilience.

1. INTRODUCCIÓN

En la era digital, las instituciones de educación superior son blancos de ciberataques que ponen en riesgo la seguridad de la información académica y administrativa. La creciente sofisticación de estos ataques, como ransomware y phishing, requiere de estrategias avanzadas de ciberseguridad. La inteligencia artificial (IA) se ha mostrado eficaz para la detección y mitigación de intrusiones, permitiendo una respuesta temprana y automatizada ante amenazas (Diana Olivia et al., 2025). Este estudio busca evaluar el impacto del uso de sistemas de IA en la mejora de la resiliencia cibernética en universidades, asegurando la protección de datos y la continuidad operativa. Se

analizarán modelos basados en machine learning y deep learning aplicados a la detección de anomalías en redes universitarias.

Actualmente, las instituciones de educación superior enfrentan desafíos cibernéticos cada vez más complejos que amenazan la integridad y confidencialidad de sus sistemas de información. Estas organizaciones manejan una vasta cantidad de datos sensibles, que incluye información académica y personal de estudiantes y docentes, así como datos esenciales para la investigación (Logroño León, 2023). Además, su funcionamiento depende en gran medida de la infraestructura tecnológica utilizada para la gestión administrativa, la enseñanza, el aprendizaje y la investigación. Por tanto, cualquier afectación en sus sistemas de información puede tener consecuencias significativas y de gran alcance (Griffiths, 2019).

Los ciberataques dirigidos a estas instituciones pueden manifestarse de diversas formas, como ransomware que bloquea datos esenciales, robo de propiedad intelectual o interrupción de servicios en línea (Heylighen et al., 2022). Estos incidentes no solo comprometen la operatividad de las universidades, sino que también pueden debilitar la confianza de estudiantes, profesores, investigadores y otros actores clave. Con la expansión del uso de dispositivos interconectados y la digitalización de procesos educativos, las amenazas cibernéticas se vuelven más sofisticadas, demandando enfoques innovadores y preventivos en seguridad informática (Cote et al., 2024).

En este contexto, la ciberresiliencia ha ganado relevancia en el ámbito de la educación superior. Este concepto se refiere a la capacidad de una institución para anticiparse, resistir, adaptarse y recuperarse de incidentes cibernéticos, garantizando la continuidad operativa y la protección de sus activos digitales (Griffiths, 2019). A diferencia de la ciberseguridad convencional, que se enfoca en evitar ataques, la ciberresiliencia asume que estos son inevitables y, por lo tanto, busca reducir su impacto y optimizar los tiempos de recuperación (Lionel F. Gonzalez Casanova & Lin, 2023).

El uso de inteligencia artificial (IA) para la detección de intrusiones representa una estrategia eficaz para mejorar la ciberresiliencia en las universidades (Heylighen et al., 2022). Estos sistemas emplean algoritmos avanzados de aprendizaje automático y análisis de datos para detectar patrones anómalos y comportamientos maliciosos en tiempo real, facilitando la detección temprana y permitiendo una respuesta inmediata ante posibles amenazas (Diana Olivia et al., 2025).

El objetivo principal de este estudio es analizar la implementación de sistemas de inteligencia artificial para la detección de intrusiones y su impacto en la resiliencia cibernética de instituciones de educación superior. La pregunta de investigación que guía este estudio es: ¿Cómo la implementación de inteligencia artificial en la detección de intrusiones puede fortalecer la resiliencia cibernética en universidades?

Se plantea que la aplicación de sistemas de inteligencia artificial para la detección proactiva de intrusiones en universidades fortalecerá su resiliencia cibernética. La automatización de la detección y respuesta ante amenazas reducirá la vulnerabilidad a ciberataques, mejorará la capacidad de recuperación ante incidentes y garantizará la integridad de los datos académicos y administrativos. Además, el uso de machine learning optimizará la identificación de patrones anómalos, permitiendo una reacción temprana y efectiva. Esto contribuirá a la seguridad informática en el ámbito educativo, minimizando riesgos y promoviendo un entorno digital más seguro para docentes, estudiantes y personal administrativo.

2. METODOLOGÍA

Este estudio emplea una metodología mixta, combinando el análisis de datos obtenidos a través de encuestas y entrevistas con la interpretación de percepciones y opiniones. Es una investigación descriptiva y exploratoria, centrada en examinar la implementación de sistemas de inteligencia artificial para la detección de intrusiones y su impacto en la resiliencia cibernética de universidades, sin intervenir directamente en la aplicación de estas tecnologías.

Población y Muestra

La población objetivo incluye estudiantes y docentes universitarios. Para recolectar datos, se utilizó una muestra de 200 estudiantes de diversas carreras en la Escuela Superior Politécnica de Chimborazo (ESPOCH), quienes participaron mediante encuestas en línea, y 10 docentes universitarios, seleccionados por su experiencia en ciberseguridad y tecnologías de la información, quienes fueron entrevistados.

Técnicas e Instrumentos de Recolección de Datos

Encuestas: Aplicadas a 200 estudiantes mediante Google Forms, incluyeron preguntas en escala de Likert para evaluar el conocimiento sobre ciberseguridad, el uso de herramientas de inteligencia artificial en la detección de amenazas y la percepción sobre la factibilidad de implementar estos sistemas en su institución. Entrevistas: Realizadas a 10 docentes mediante Zoom, estas entrevistas semiestructuradas ofrecieron una visión profunda sobre los desafíos, oportunidades y limitaciones de integrar sistemas de inteligencia artificial en la ciberseguridad universitaria.

Procedimiento de Recolección de Datos

Se diseñaron y validaron los instrumentos de recolección (encuesta y guía de entrevista). Las encuestas se distribuyeron mediante Google Forms y se recopiló la información durante dos semanas. Las entrevistas con los docentes fueron agendadas y realizadas a través de Zoom, registrando y transcribiendo las respuestas para su análisis posterior.

Análisis de Datos

Los datos cuantitativos de las encuestas se procesaron con herramientas estadísticas para identificar tendencias y frecuencias en las respuestas de los estudiantes. Las respuestas cualitativas de las entrevistas fueron analizadas mediante categorización temática, identificando opiniones recurrentes sobre la viabilidad y efectividad de los sistemas de inteligencia artificial en la detección de intrusiones.

Consideraciones Éticas

Se garantizó la confidencialidad y el anonimato de los participantes, asegurando que la

información recopilada se utilizaría únicamente con fines investigativos. Además, todos los participantes dieron su consentimiento informado antes de responder las encuestas o participar en las entrevistas.

DESARROLLO

Importancia de la resiliencia cibernética en las universidades

Impacto de los ciberataques en la educación superior

Las universidades gestionan una vasta cantidad de información sensible, incluidos datos personales de estudiantes y profesores, investigaciones en curso y registros administrativos. Los ciberataques pueden comprometer la integridad y confidencialidad de estos datos, afectando la operatividad de las instituciones y generando pérdidas económicas significativas (Samaniego Campoverde, 2024). Además, las interrupciones causadas por ataques como el ransomware pueden impedir el acceso a plataformas educativas, perjudicando el desarrollo académico de los estudiantes y ralentizando los procesos administrativos esenciales (Gohar et al., 2022).

Necesidad de fortalecer la seguridad digital en instituciones académicas

Las universidades dependen en gran medida de la tecnología para la enseñanza, la investigación y la administración. Sin embargo, muchas instituciones carecen de estrategias de seguridad digital robustas que les permitan resistir y recuperarse de los ataques. La implementación de medidas proactivas es crucial para garantizar la continuidad de las operaciones y proteger los activos digitales de la comunidad universitaria (Ebady Manaa et al., 2024).

Ciberamenazas en el entorno universitario

Tipos de ataques más frecuentes en universidades Los ataques a instituciones académicas incluyen ransomware, que cifra archivos y exige un rescate para su liberación; phishing, que engaña a los usuarios para obtener credenciales de acceso; e intrusiones en redes para robar información confidencial (López González et al., 2024). Además, la digitalización del aprendizaje ha incrementado los ataques de suplantación de identidad, donde ciberdelincuentes acceden a plataformas educativas con credenciales robadas (Wei et al., 2020).

Consecuencias de los ciberataques en la gestión académica y la investigación Los ciberataques pueden paralizar actividades universitarias, desde la imposibilidad de acceder a sistemas de gestión de estudiantes hasta la pérdida de datos críticos en investigaciones científicas. La falta de medidas preventivas puede generar una crisis institucional, afectando la reputación de la universidad y disminuyendo la confianza de estudiantes y docentes en la seguridad digital de la institución (Zubeidat et al., 2024).

Inteligencia artificial como herramienta para la detección de amenazas

Funcionamiento de los sistemas de IA en la ciberseguridad Los sistemas de inteligencia artificial (IA) aplicados a la ciberseguridad utilizan algoritmos de aprendizaje automático y análisis de comportamiento para detectar patrones anómalos en el tráfico de red y en el uso de plataformas digitales (Russell Belk, 2019). Estos sistemas pueden identificar amenazas emergentes antes de que se conviertan en ataques efectivos, permitiendo una respuesta rápida y minimizando el daño potencial (Jayavanth et al., 2024).

Beneficios de la detección proactiva mediante IA El uso de IA en ciberseguridad ofrece ventajas significativas, como la capacidad de detectar amenazas en tiempo real, reducir la carga de trabajo de los equipos de seguridad informática y mejorar la respuesta ante incidentes. Además, la automatización permite identificar vulnerabilidades antes de que sean explotadas, fortaleciendo la resiliencia cibernética de las universidades (Ala-Laurinaho et al., 2017).

Factores que influyen en la implementación de IA en ciberseguridad universitaria

Infraestructura tecnológica y recursos disponibles La adopción de sistemas de IA para la ciberseguridad en universidades depende en gran medida de la infraestructura tecnológica disponible. Instituciones con sistemas obsoletos o limitados pueden enfrentar dificultades para integrar estas soluciones, mientras que aquellas con mayor inversión en tecnología pueden aprovechar al máximo su potencial (Samaniego Campoverde, 2024).

Capacitación del personal y resistencia al cambio Para que la implementación de IA en ciberseguridad sea efectiva, es fundamental que el personal académico y administrativo reciba formación en el uso y gestión de estas tecnologías. Sin embargo, la resistencia al cambio es un desafío común en muchas universidades, lo que dificulta la adopción de nuevas herramientas digitales (Kar-Han & Boon Pang, 2018). La capacitación continua y la concienciación sobre los riesgos cibernéticos son clave para garantizar una transición exitosa hacia sistemas de seguridad basados en IA.

3. RESULTADOS

Se presentan los resultados obtenidos de las encuestas aplicadas a 200 estudiantes de la institución, con el objetivo de evaluar su nivel de conocimiento sobre ciberseguridad, su percepción sobre el uso de inteligencia artificial (IA) para la detección de amenazas cibernéticas y su opinión sobre la factibilidad de implementar estos sistemas en el entorno educativo. Los resultados proporcionan una visión general sobre el grado de familiaridad y disposición de los estudiantes hacia la incorporación de tecnologías avanzadas como la IA en la mejora de la seguridad cibernética y la resiliencia de la institución. Las respuestas obtenidas permiten identificar áreas clave para el fortalecimiento de la infraestructura de ciberseguridad y la necesidad de capacitación continua en

este ámbito.

Fig. 1:
Nivel de familiaridad con los conceptos básicos de ciberseguridad entre los estudiantes.

Nota: Los resultados indican que el 70% de los estudiantes se considera al menos algo familiarizado con los conceptos básicos de ciberseguridad. Esto sugiere un nivel moderado de conocimiento, lo que podría representar una oportunidad para implementar programas educativos en el área para mejorar la comprensión general. Fuente: Elaboración propia.

La mayoría de los estudiantes tiene un conocimiento básico o algo avanzado sobre ciberseguridad, lo que demuestra que existe una base sobre la que se pueden construir programas de capacitación más especializados. Sin embargo, una proporción considerable aún tiene un conocimiento limitado, lo que señala la necesidad de más educación en este campo.

Fig. 2:
Percepción de los estudiantes sobre la adecuación del uso de IA para la detección de amenazas cibernéticas.

Nota: El 80% de los estudiantes considera que la implementación de IA para detectar amenazas cibernéticas es una opción adecuada para la institución. Esto sugiere una actitud favorable hacia el uso de tecnologías avanzadas en la mejora de la seguridad. Fuente: Elaboración propia.

La mayoría de los estudiantes ve la inteligencia artificial como una herramienta adecuada para la detección de amenazas, lo que refleja una actitud positiva hacia la adopción de nuevas tecnologías. Esta percepción favorable es crucial para la viabilidad de la implementación de IA en la institución, ya que el apoyo de los estudiantes puede facilitar el proceso.

Fig. 3:
Opinión de los estudiantes sobre la mejora de la seguridad cibernética a través de la implementación de IA.

Nota: Un alto porcentaje (85%) de los estudiantes opina que la IA podría mejorar en alguna medida la seguridad cibernética. Esto indica un alto nivel de confianza en las tecnologías emergentes y su impacto potencial en la protección contra ciberamenazas. Fuente: Elaboración propia.

Los resultados muestran una visión positiva sobre el impacto de la IA en la seguridad cibernética. La mayoría cree que su implementación mejoraría significativamente la protección de la institución, lo que refleja un alto nivel de confianza en las capacidades de la IA para detectar y prevenir amenazas.

Fig. 4:
Percepción de los estudiantes sobre la factibilidad de implementar sistemas de IA para la detección

de amenazas.

Nota: El 70% de los estudiantes considera que la implementación de sistemas de IA para la detección de amenazas es al menos algo factible. Esto refleja una actitud realista y positiva sobre la posibilidad de adoptar dicha tecnología. Fuente: Elaboración propia.

Aunque la mayoría de los estudiantes percibe la implementación como factible, una proporción significativa aún tiene dudas sobre su viabilidad. Esto puede ser un indicio de preocupaciones sobre recursos, infraestructura o capacitación necesarias para una integración efectiva de IA.

Fig. 5:
Disposición de los estudiantes para aprender sobre el uso de IA en la mejora de la seguridad cibernética.

Nota: Un alto porcentaje (80%) de los estudiantes muestra disposición para aprender sobre el uso de la IA en seguridad cibernética. Este interés puede ser aprovechado para desarrollar programas educativos que aumenten la conciencia y la capacitación en IA. Fuente: Elaboración propia.

La disposición de los estudiantes para aprender sobre IA es un factor positivo, ya que su participación activa en el aprendizaje de estas tecnologías fortalecerá la efectividad de la implementación de sistemas de IA en la institución. La educación en esta área podría facilitar la integración y el uso correcto de estas herramientas.

Fig. 6:
Opinión de los estudiantes sobre el impacto de la IA en el fortalecimiento de la resiliencia cibernética institucional.

Nota: El 85% de los estudiantes está de acuerdo o totalmente de acuerdo en que la IA fortalecería la resiliencia cibernética de la institución, lo que resalta la percepción positiva de esta tecnología como un medio para mejorar la seguridad a largo plazo. Fuente: Elaboración propia.

La mayoría de los estudiantes cree que la IA tiene el potencial de fortalecer significativamente la resiliencia cibernética de la institución. Este respaldo podría facilitar la adopción de estos sistemas, contribuyendo a una mayor seguridad y protección frente a las ciberamenazas.

Resultados de las entrevistas a los docentes universitarios
Las entrevistas semiestructuradas permitieron explorar la percepción de los docentes respecto a la integración de sistemas de inteligencia artificial (IA) en la ciberseguridad universitaria. A continuación, se presentan los principales hallazgos organizados en categorías clave:
1. Nivel de conocimiento sobre inteligencia artificial en ciberseguridad
- 7 de los 10 docentes manifestaron tener un conocimiento básico o intermedio sobre el uso de IA en ciberseguridad.
- 3 docentes reconocieron que su conocimiento en este ámbito es limitado y que sería necesario capacitarse para comprender mejor su aplicación.
- Se destacó la necesidad de programas de formación dirigidos al personal docente y

administrativo para fortalecer su competencia en el uso de estas tecnologías.

2. Percepción sobre los beneficios de la IA en la ciberseguridad universitaria

- 8 docentes afirmaron que la IA puede mejorar significativamente la detección y prevención de amenazas cibernéticas, reduciendo el tiempo de respuesta ante incidentes de seguridad.
- 6 docentes resaltaron que el uso de IA facilitaría la identificación de patrones de ataque y comportamientos sospechosos, mejorando la seguridad de la institución.
- 4 docentes señalaron que la IA podría optimizar la gestión de la seguridad informática, automatizando procesos de monitoreo y análisis de datos.

3. Desafíos para la implementación de IA en ciberseguridad

- 9 docentes mencionaron que uno de los principales desafíos es la falta de recursos tecnológicos y financieros para integrar sistemas de IA en la infraestructura universitaria.
- 7 docentes indicaron que la falta de capacitación y la resistencia al cambio podrían dificultar la adopción de estas tecnologías.
- 5 docentes expresaron preocupación por la privacidad y el manejo ético de los datos que procesaría la IA en un entorno académico.

4. Factibilidad de implementación de IA en la universidad

- 6 docentes consideran que la implementación de IA en la ciberseguridad universitaria es factible a mediano plazo, siempre que exista inversión en tecnología y capacitación.
- 4 docentes creen que, aunque es una opción viable, su adopción será lenta debido a limitaciones presupuestarias y falta de personal especializado.
- Se resaltó la importancia de establecer colaboraciones con instituciones y expertos en el área para facilitar la integración de estas tecnologías.

5. Propuestas para mejorar la ciberseguridad con IA

- 8 docentes recomendaron el desarrollo de cursos y talleres sobre ciberseguridad y el uso de IA en el ámbito universitario.
- 6 docentes sugirieron la creación de un laboratorio de ciberseguridad que permita realizar pruebas y simulaciones con sistemas de IA.
- 5 docentes destacaron la importancia de generar políticas institucionales que regulen el uso de IA en la seguridad informática.

Los resultados de la entrevista con los 10 docentes de la Escuela Superior Politécnica de Chimborazo (ESPOCH) evidencian un interés significativo en la implementación de inteligencia artificial (IA) para mejorar la ciberseguridad universitaria. La mayoría de los docentes reconoce el potencial de la IA para fortalecer la detección y prevención de amenazas, optimizar la gestión de seguridad informática y mejorar la resiliencia cibernética institucional. Sin embargo, también identifican desafíos importantes, como la falta de recursos tecnológicos y financieros, la necesidad de capacitación especializada y las preocupaciones sobre la privacidad y el manejo ético de los datos.

A pesar de estos desafíos, los docentes consideran que la implementación de IA es factible a mediano plazo, siempre que la universidad invierta en formación, infraestructura y políticas claras para su uso. Destacan la importancia de desarrollar programas educativos sobre ciberseguridad, crear laboratorios de prueba y establecer alianzas estratégicas con expertos en la materia.

4. CONCLUSIÓN

Estudiantes y docentes de la Escuela Superior Politécnica de Chimborazo (ESPOCH) muestran una actitud favorable hacia la implementación de inteligencia artificial (IA) para la detección de amenazas cibernéticas. Los resultados indican un alto nivel de aceptación y un reconocimiento generalizado del potencial de la IA para mejorar la seguridad informática y reforzar la resiliencia cibernética de la institución.

Aunque su conocimiento sobre IA y ciberseguridad es básico o intermedio, la mayoría de los estudiantes y docentes reconoce la necesidad de una capacitación adicional para comprender mejor su aplicación. La implementación exitosa de estos sistemas requiere la incorporación de programas educativos específicos que permitan desarrollar habilidades en el uso de la IA para detectar y prevenir amenazas cibernéticas.

Se identificaron la falta de infraestructura tecnológica, los recursos financieros limitados y la resistencia al cambio como los principales obstáculos para la adopción de IA en la ciberseguridad universitaria. Superar estos desafíos exige un compromiso institucional que incluya inversiones en tecnología, el desarrollo de políticas de seguridad y la promoción de una cultura de ciberseguridad dentro de la comunidad universitaria.

Aunque la implementación de IA en la detección de intrusiones es viable a mediano plazo, su éxito dependerá de una estrategia integral que combine tecnología, capacitación y normativas claras. Es fundamental establecer alianzas con expertos y desarrollar laboratorios de investigación para experimentar y validar estos sistemas en entornos académicos, garantizando así su efectividad y sostenibilidad en la protección de la infraestructura digital universitaria.

REFERENCIAS BIBLIOGRÁFICAS

Ala-Laurinaho, A., Kurki, A. L., & Abildgaard, J. S. (2017). Supporting Sensemaking to Promote a Systemic View of Organizational Change – Contributions from Activity Theory. *Journal of Change Management*, *17*(4), 367–387. https://doi.org/10.1080/14697017.2017.1309566

Cote, C, Kawalek, P., Jackson, T.: Navegando por la incertidumbre con principios cibernéticos: una revisión del alcance de las estrategias de resiliencia interdisciplinarias para sistemas ferroviarios. *IET Intell. Transp. Syst.* 18 (Suppl. 1), 2814 – 2826 (2024). https://doi.org/10.1049/itr2.12598

Diana Olivia, Khan, Z., & Shetty, S. (2025). Un enfoque de aprendizaje automático e inteligencia artificial explicable para la clasificación de fraudes en seguros. *Inteligencia Artificial* , *28* (75), 140–169. https://doi.org/10.4114/intartif.vol28iss75pp140-169

Ebady Manaa, M., Hussain, SM ., Suad A. Alasadi, & Hussein AA Al-Khamees. (2024). Detección de ataques DDoS basados en algoritmos de aprendizaje automático en entornos IoT. *Inteligencia Artificial* , *27* (74),

152–165. https://doi.org/10.4114/intartif.vol27iss74pp152-165

Gohar Sargsyan (ed.), Dimitrios Kavallieros (ed.), Nicholas Kolokotronis (ed.) (2022), "Tecnologías y métodos de seguridad para la detección, mitigación e inteligencia avanzadas de amenazas cibernéticas", Boston-Delft: ahora publicado por la editorial, http://dx.doi.org/10.1561/9781680838350

Griffiths, D. (2019), "Resiliencia y transparencia en los sistemas sociales", Kybernetes , Vol. 48 No. 4, pp. 715-726. https://doi.org/10.1108/K-01-2018-0032

Heylighen, F., Beigi, S., & Busseniers, E. (2022). The role of self-maintaining resilient reaction networks in the origin and evolution of life. *Biosystems, 219*, 104720. https://doi.org/10.1016/j.biosystems.2022.104720

Jayavanth Shenoy, Patrick Grinaway, Shriphani Palakodety (2024), "Inteligencia artificial de alto rendimiento que preserva la privacidad", Boston-Delft: ahora publicado, http://dx.doi.org/10.1561/9781638283454

Kar-Han Tan y Boon Pang Lim (2018), "El renacimiento de la inteligencia artificial: aprendizaje profundo y el camino hacia la inteligencia artificial a nivel humano", APSIPA Transactions on Signal and Information Processing: Vol. 7: No. 1, e6. http://dx.doi.org/10.1017/ATSIP.2018.6

Lionel F. Gonzalez Casanova y Po-Chiang Lin (2023), "Detección de tráfico de red malicioso para DNS sobre HTTPS mediante algoritmos de aprendizaje automático", APSIPA Transactions on x

Logroño León, E. J. (2023). Open Source Intelligence para inteligencia de amenazas de seguridad informática (Master's thesis, Quito, Ecuador: Universidad Tecnológica Israel). http://repositorio.uisrael.edu.ec/handle/47000/3955

López González, A., Moreno, M., Moreno Román, AC, Hadfeg Fernández, Y., & Cepero Pérez, N. (2024). Ética en Inteligencia Artificial: una aproximación a la Ciberseguridad. *Inteligencia Artificial* , *27* (73), 38–54. https://doi.org/10.4114/intartif.vol27iss73pp38-54

Russell Belk (2019), "Máquinas e inteligencia artificial", Journal of Marketing Behavior: vol. 4: n.º 1, págs. 11-30. http://dx.doi.org/10.1561/107.00000058

Samaniego Campoverde, J. E. (2024). SEGURIDAD CIBERNÉTICA: AMENAZAS EMERGENTES Y ESTRATEGIAS DE DEFENSA. Revista SOCIENCYTEC, 3(1).https://doi.org/10.61396/s5hje696

Russell Belk (2019), "Máquinas e inteligencia artificial", Journal of Marketing Behavior: vol. 4: n.º 1, págs. 11-30. http://dx.doi.org/10.1561/107.00000058

Wei Cao, Qinan Wang, Asma Sbeih y FHA Shibly (2020). Marco de aprendizaje inteligente y eficiente basado en inteligencia artificial para plataformas educativas. *Inteligencia Artificial* , *23* (66), 112–123. https://doi.org/10.4114/intartif.vol23iss66pp112-123

Zubeidat, I., Dallasheh, W., Khalil, A. E., & Masri, A. S. (2024). Personal resilience among novice teachers and teacher-interns in Arab society in Israel: demographic, socio-emotional and educational characteristics. International Journal of Inclusive Education, 1–27. https://doi.org/10.1080/13603116.2024.2303155

FINANCIACIÓN

Declarar fuente de financiación; caso contrario colocar “Ninguna” o “Los autores no recibieron financiación para el desarrollo de la presente investigación”.

CONFLICTO DE INTERESES

Declarar potenciales conflictos de interés; caso contrario declarar “Ninguno” o “Los autores declaran que no existe conflicto de intereses”.