Revista de investigación de sistemas e informática
16(1): 71-80 (2023)
DOI: https://doi.org/10.15381/risi.v16i1.25390

ISSN: 1815-0268 (Impreso) / ISSN: 1816-3823 (Electrónico)
Facultad de Ingeniería de Sistemas e Informática - UNMSM

El papel de la inteligencia artificial en la seguridad de la información: Una revisión de su aplicación en la industria cibernética

The role of artificial intelligence in information security: a review of its application in the cyber industry

Josue Eduardo David Chavez Flores
https://orcid.org/0000-0002-6648-2052
jochavezf@unitru.edu.pe

Jean Carlos Joel Pacheco Guzmán
https://orcid.org/0000-0002-8699-5461
jcpachecog@unitru.edu.pe

Alberto Carlos Mendoza de los Santos
https://orcid.org/0000-0002-0469-915X
amendozad@unitru.edu.pe

Universidad Nacional de Trujillo. Trujillo, Perú

Recibido: 23/05/2023 - Aceptado: 14/06/2023 - Publicado: 21/08/2023

RESUMEN

En la actualidad, la implementación de las tecnologías de la información en las organizaciones es cada vez más común, ya que beneficia el desarrollo y automatización de los procesos que realizan; sin embargo, es importante tener en cuenta que la incorporación de estas soluciones tecnológicas pueden afectar en la seguridad de sus sistemas y de la información contenida en ellos. Es aquí donde la inteligencia artificial puede ayudar a las organizaciones a mejorar su capacidad para proteger su información sensible ante posibles amenazas de ciberseguridad, al mismo tiempo que reduce la carga de trabajo en los equipos encargados de ello; no obstante, la ejecución de esta estrategia acarrea consigo sus propias desventajas, las cuales deberán abordar las organizaciones que la implementen. El presente artículo tiene como objetivo determinar y analizar los beneficios y limitaciones que ofrece la inteligencia artificial aplicada en la seguridad de la información, para lo cual se realizó una revisión sistemática de los artículos y papers publicados en las bases de datos Scopus, Scielo y Alicia durante los últimos 5 años (2019 – 2023), con la intención de brindar prioridad a las publicaciones de actualidad sobre el tema. Los resultados obtenidos nos muestran que la Inteligencia Artificial (IA) brinda beneficios en cuanto a la detección de ataques en tiempo real y en la prevención de amenazas, teniendo como limitaciones su complejidad de implementación, la necesidad de un amplio acceso a los datos, la desconfianza generada por su interpretación independiente y la poca privacidad hacia los datos del usuario.

Palabras clave: Seguridad de la información, inteligencia artificial, tecnologías de la información, ciberseguridad.

ABSTRACT

At present, the implementation of information technologies in organizations is increasingly common, since it benefits the development and automation of the processes they carry out; however, it is important to take into account that the incorporation of these technological solutions may affect the security of your systems and the information contained in them. This is where artificial intelligence can help organizations improve their ability to protect their sensitive information against possible cybersecurity threats, while reducing the workload on the teams in charge of it; however, executing this strategy comes with its own drawbacks, which organizations implementing it will need to address. The objective of this article is to determine and analyze the benefits and limitations offered by artificial intelligence applied to information security, for which a systematic review of the articles and papers

published in the Scopus, Scielo and Alicia databases was carried out. during the last 5 years (2019 - 2023), with the intention of giving priority to current publications on the subject. The results obtained show us that Artificial Intelligence (AI) provides benefits in terms of detecting attacks in real time and preventing threats, having as limitations its implementation complexity, the need for broad access to data, the distrust generated by its independent interpretation and the lack of privacy towards user data.

Keywords: Information security, artificial intelligence, information technologies, cybersecurity.

I. INTRODUCCIÓN

En el campo de la seguridad de la información existen brechas tecnológicas que requieren investigación (Misra, Srivastava, & Rajeshwari, 2019), teniendo en cuenta que es fundamental en el mundo digital actual. Con el aumento constante de los riesgos y amenazas cibernéticas, es crucial estar protegido. La inteligencia artificial (IA) ha demostrado ser una herramienta valiosa en la protección contra estos peligros y en la defensa de los datos sensibles (Tu & Sun, 2020). La capacidad de la IA para detectar patrones y reconocer anomalías en el comportamiento de las aplicaciones y los usuarios es particularmente útil para identificar intrusiones y prevenir ataques (Huang & Li, 2019). Además, la capacidad de la IA para aprender y adaptarse continuamente brinda a las organizaciones la posibilidad de mantenerse actualizadas en la protección contra nuevas amenazas de seguridad (Kshetri & Voas, 2020).

En este artículo de revisión, examinamos el papel de la inteligencia artificial en la protección de la seguridad de la información y su impacto en la defensa cibernética. Exploramos la utilidad de la IA en la identificación y prevención de intrusiones, así como en la adaptación a nuevas amenazas. También analizamos algunas preocupaciones éticas y de privacidad asociadas con el uso de la IA en la seguridad de la información.

II. MATERIALES Y MÉTODOS

Tipo De Estudio

Se realizó una revisión sistemática de la literatura científica, siguiendo las bases dictaminadas por la metodología PRISMA (Preferred Reporting Items for Systematic reviews and Meta-Analyses) y haciendo uso de su diagrama de flujo de cuatro fases (Quispe, Hinojosa, Miranda, & Sedano, 2021). Durante dicho proceso, se estableció la siguiente pregunta de investigación: ¿Cómo se ha aplicado la inteligencia artificial en la industria cibernética para mejorar la seguridad de la información?

Fundamentación de la metodología

La revisión sistemática es la evaluación comprehensiva, reproducible, crítica y explícita de la mejor evidencia disponible en respuesta a una pregunta de investigación específica, haciendo uso de una metodología clara y sistemática para reducir sesgos en la identificación, selección, síntesis y resumir los estudios. Sus hallazgos son confiables, por ello las conclusiones ayudan en la toma de decisiones clínicas (Quispe, Hinojosa, Miranda, & Sedano, 2021).

La metodología PRISMA son pautas que orientan a los autores en la preparación de protocolos, en la planificación de revisiones sistemáticas y metaanálisis, a través de un conjunto mínimo de ítems de inclusión en el protocolo. El objetivo del protocolo es proporcionar la justificación y el enfoque metodológico con antelación y el análisis de la revisión (Quispe, Hinojosa, Miranda, & Sedano, 2021).

Proceso de recolección de información

Cabe recalcar que nuestra búsqueda de información aborda a la pregunta de investigación en su totalidad y a nuestros objetivos de estudio como lo indican (Quispe, Hinojosa, Miranda, & Sedano, 2021); es por ello que identificamos los siguientes términos clave establecidos en la pregunta para una mayor precisión de búsqueda: “Gestión de servicios de TI”, “Seguridad de la Información”, “Inteligencia Artificial”.

Para el desarrollo de la revisión, delimitamos la fuente de búsqueda a la base de datos SCOPUS, SciELO, Alicia.

Criterios de inclusión y exclusión

De acuerdo con (Quispe, Hinojosa, Miranda, & Sedano, 2021), nuestros criterios de inclusión/exclusión deben estar en base a nuestro método de búsqueda y a la pregunta de investigación; elaborando para ello una lista de verificación buscando una mayor facilidad de control sobre ellos.

Basándonos en esto y en nuestros propósitos de investigación, establecimos los siguientes criterios de inclusión y exclusión:

Criterios de inclusión

- Se incluyeron los artículos publicados tanto en inglés como en español.
- Se incluyeron únicamente documentos académicos del tipo artículo y conference paper.

Criterios de exclusión

- Se excluyeron los artículos que no hayan sido publicados entre los años 2019 y 2023.
- Se excluyeron los artículos que no se encuentren disponibles públicamente en línea.
- Se excluyeron los artículos pertenecientes a áreas no relevantes a nuestra investigación.
- Se excluyeron los artículos repetidos.

Catálogos y Bases de Datos

En la búsqueda realizada para nuestra revisión, encontramos un total de 97 documentos originales, divididos de la siguiente forma: SCOPUS: 78 documentos, SciELO: 5 documentos, Alicia: 14 documentos; todos ellos relacionados con el tema del presente artículo.

Para obtener dichos resultados, se realizaron las siguientes consultas según la fuente de información.

Alicia:

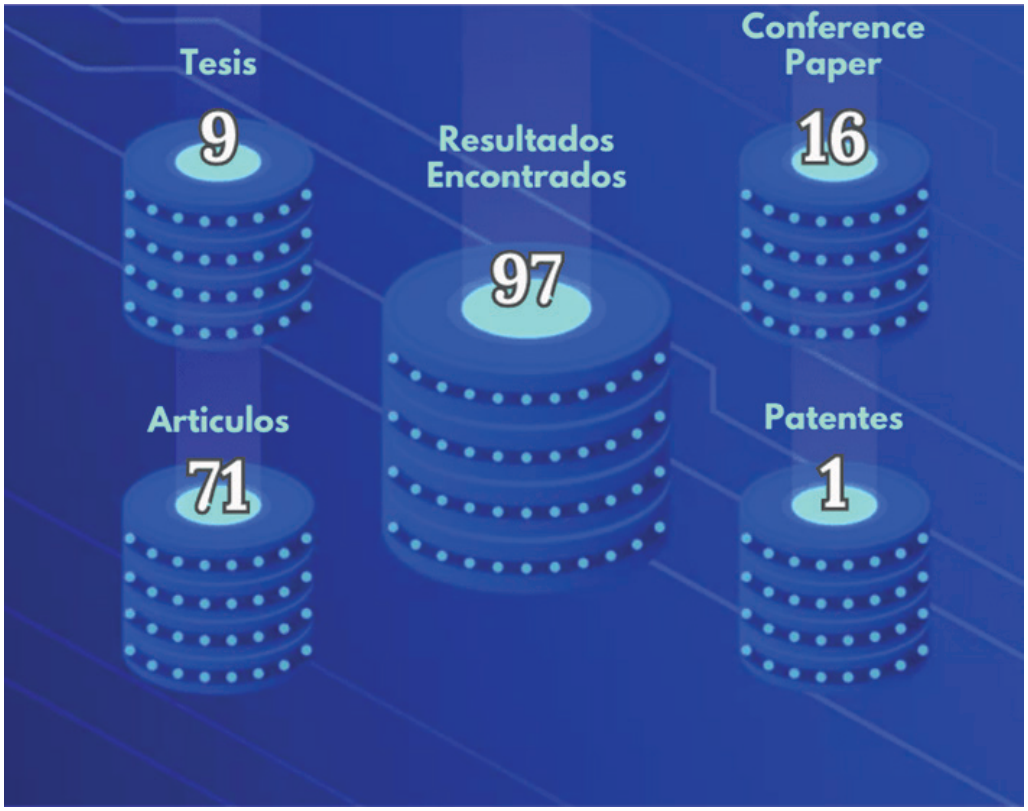
'inteligencia artificial y seguridad de la información'

SciELO:

"Information security" AND "artificial intelligence"

Figura 1

Resultados de la búsqueda



Fuente: Elaboración propia

SCOPUS:

> TITLE-ABS-KEY (" service management " OR "information security" AND "artificial intelligence") AND (LIMIT-TO (SUBJAREA,"COMP") OR LIMIT-TO (SUBJAREA,"ENGI")) AND (LIMIT-TO (DOCTYPE,"cp") OR LIMIT-TO (DOCTYPE,"ar")) AND (LIMIT-TO (PUBYEAR,2019) OR LIMIT-TO (PUBYEAR,2020) OR LIMIT-TO (PUBYEAR,2021) OR LIMIT-TO (PUBYEAR,2022) OR LIMIT-TO (PUBYEAR,2023)) AND (LIMIT-TO (LANGUAGE,"English")) AND (LIMIT-TO (EXACTKEYWORD,"Artificial Intelligence") OR LIMIT-TO (EXACTKEYWORD,"Security Of Data") OR LIMIT-TO (EXACTKEYWORD,"Information Security")) AND (LIMIT-TO (OA,"all"))

Es así que, habiendo realizado las consultas mencionadas, procedimos a aplicar los criterios de inclusión y exclusión a las búsquedas obtenidas, lo cual está explicado gráficamente en el flujograma de la metodología PRISMA (Figura 2).

III. RESULTADOS

Una vez realizado el proceso de filtrado, listamos los 12 documentos seleccionados y rescatamos los resultados obtenidos en la tabla 1.

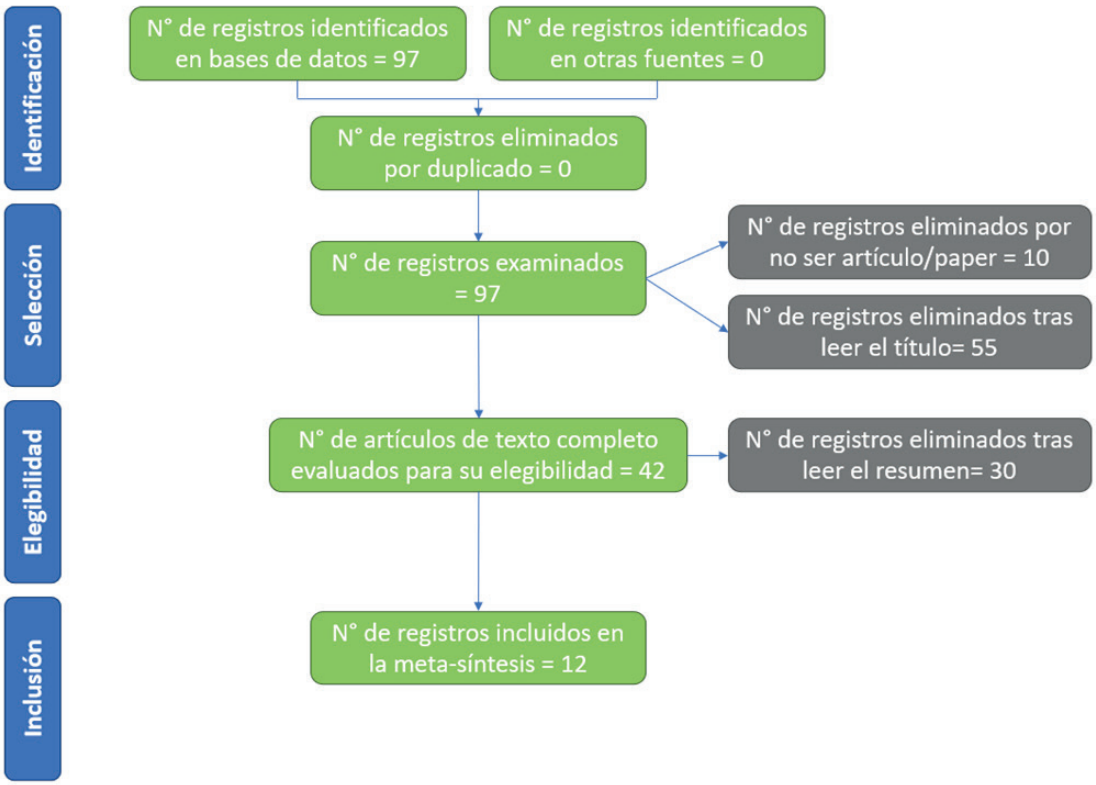
La figura 3 ilustra un gráfico que nos muestra la cantidad de autores que redactaron los documentos incluidos en la presente revisión distribuidos por países, resaltando que no se tiene en cuenta a los artículos que tienen autores de países diferentes.

Ahora, en la figura 4, veremos la ilustración de los documentos incluidos para la presente revisión, divididos en un gráfico circular según su año de publicación, entre el 2019 y 2023, siendo el año 2022 el que más publicaciones tuvo.

A continuación, mostraremos las técnicas, propuestas y/o métodos utilizados por los 12 artículos revisados en la tabla 2.

Figura 2

Diagrama de Flujo PRISMA



Fuente: Page M. y otros (2021).

Tabla 1

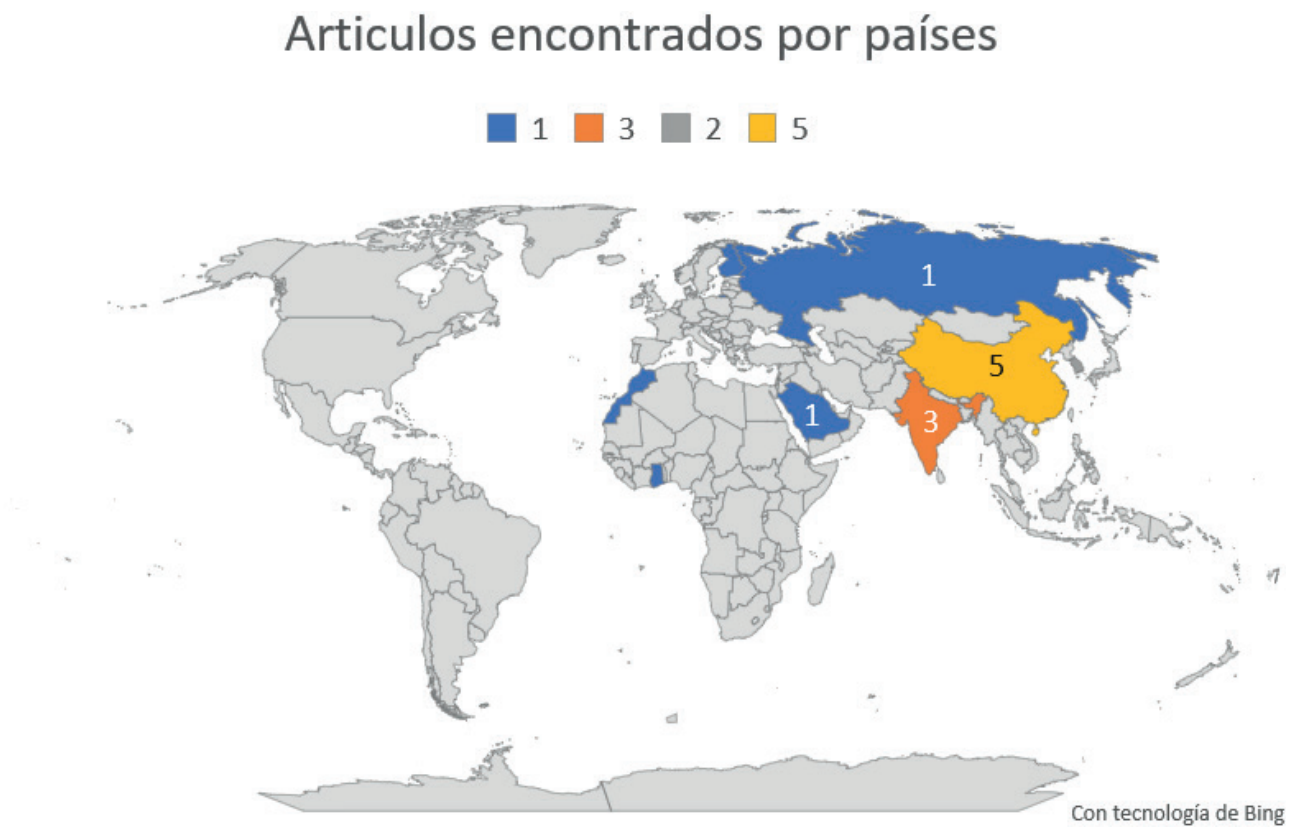
Documentos escogidos para la revisión sistemática

#	Tipo	Autores	Pais de Procedencia	Fuente	Año	Título de Investigación	Resultados
1	Articulo	Ayachi, Yassine; Mellah, Youssef; Saber, Mohammed; Rahmoun, Noureddine; Kerrakchou, Imane; Bouchentouf, Toumi.	Morocco	Scopus	2022	A survey and analysis of intrusion detection models based on information security and object technology-cloud intrusion dataset	Los modelos de detección de intrusos inteligentes descritos en este documento mejoran significativamente el rendimiento de los métodos de detección y logran una sensibilidad perfecta en el conjunto de datos ISOT-CID.
2	Articulo	Singh, Shailendra Pratap; Alotaibi, Youseef; Kumar, Gyanendra; Rawat, Sur Singh.	India	Scopus	2022	Intelligent Adaptive Optimisation Method for Enhancement of Information Security in IoT-Enabled Environments	Los resultados de varias funciones de referencia muestran que la técnica propuesta funciona mucho mejor que las versiones anteriores del algoritmo DE en variantes máximas, lo cual es muy alentador. El método propuesto se aplica y prueba en aplicaciones de comercio electrónico IoTenabled, pero en el futuro se puede extender a otras aplicaciones incorporando los parámetros de entrada de acuerdo con los requisitos.
3	Articulo	Moon, Jaewoong; Kim, Subin; Jangyong, Park.; Lee, Jieun; Kim, Kyungshin; Song, Jaeseung.	South Korea	Scopus	2022	MalDC: Malicious Software Detection and Classification using Machine Learning	La investigación sobre el análisis de malware mediante ML requiere la consideración de dos factores principales. En primer lugar, debe desarrollarse el método para convertir malware en imágenes. En segundo lugar, se puede aumentar la precisión mejorando la cantidad y la calidad del conjunto de datos de imágenes de malware.
4	Articulo	Ding, Jun; Alroobaea, Roobaea; Baqasah, Abdullah M; Althobaiti, Anas; Miglani, Rajan; Gill, Harsimranjit Singh.	China,Saudi Arabia y India	Scopus	2022	Big Data Intelligent Collection and Network Failure Analysis Based on Artificial Intelligence	La aplicación efectiva de la tecnología de big data e inteligencia artificial puede mejorar la precisión y la precisión del procesamiento de la información, evaluar de manera integral el estado de riesgo de seguridad del sistema de información y lograr la operación segura y ordenada de las empresas.
5	Conference Paper	Jo, Hyeon	South Korea	Scopus	2022	Impact of Information Security on Continuance Intention of Artificial Intelligence Assistant	La intención de permanencia de los usuarios de AIA con un enfoque en la seguridad de la información. Para considerar varios aspectos dentro de la seguridad de la información, el modelo de investigación incluyó preocupaciones de seguridad sobre AIA, confianza en el nivel de seguridad de AIA y preocupaciones sobre la exposición de la información al entorno.
6	Articulo	Han, Yubiao; Wang, Lei; He, Dianhong.	China	Scopus	2022	Differential Privacy Technology of Big Data Information Security based on ACA-DMLP	Se propone un esquema de preservación de la privacidad de aprendizaje automático distribuido resistente a la colusión (ACA-DMLP).
7	Articulo	Sun, Hongbin; Bai, Shizhen.	China	Scopus	2022	Enterprise Information Security Management Using Internet of Things Combined with Artificial Intelligence Technology	Se diseña una plataforma de gestión de seguridad de la información empresarial moderna basada en IoT el cual logara que el tiempo de respuesta promedio a un evento es inferior a 0,25 s, el uso de la CPU no supera el 20 % y el requisito de memoria no es grande. Por lo tanto, el sistema construido en este trabajo tiene un mejor efecto en la gestión de la seguridad de la información empresarial.
8	Articulo	Wang, Na; Wang, Kai.	China	Scopus	2022	Internet Financial Risk Management in the Context of Big Data and Artificial Intelligence	La aplicación de tecnologías de inteligencia artificial y big data en la gestión de riesgos en el sector de las finanzas en línea es esencial para abordar los problemas que han surgido con la rápida expansión de este modelo de negocio.
9	Articulo	Guan, Yi; Chen, Qian.	China	Scopus	2021	Research on Intelligent Perception and Cognitive Computing of Information Security System Based on Computer Big Data	La variedad de redes neuronales y métodos de entrenamiento que sirven como herramientas para la investigación y el desarrollo de sistemas de seguridad, siendo la red perceptrón multicapa la más importante para la computación perceptual.
10	Articulo	Wiafe, Isaac; Koranteng, Felix Nti; Obeng, Emmanuel Nyarko; Assyne, Nana; Wiafe, Abigail; Gulliver, Stephen R..	Ghana,Finland y United Kingdom	Scopus	2020	Artificial Intelligence for Cybersecurity: A Systematic Mapping of Literature	La inteligencia artificial es prometedora en ciberseguridad, permitiendo reducir complejidad en los procesos de la misma; también se cree que seguirá ofreciendo oportunidades en esta rama, pero se necesita adoptar nuevos enfoques y nuevas investigaciones.
11	Articulo	Misra, Tripti; Srivastava, Kingshuk; Rajeshwari.	India	Scopus	2019	Challenges of information security in the contemporary cyber threat perception	La existencia de grandes brechas tecnológicas que necesitan investigación, las cuales se pueden mitigar con la disponibilidad de Inteligencia Artificial, implementando un enfoque novedoso de protección proactiva y análisis en tiempo real de patrones de intrusión.
12	Conference Paper	Kirillova A.D.; Vasilyev V.I.; Nikonov A.V.; Berkholts V.V.	Russian Federation	Scopus	2019	Decision support system in the task of ensuring information security of automated process control systems	La solución que brindan los sistemas de control de procesos automatizados basados en un algoritmo de soporte de decisiones que utilizan una red neuronal modular (ensamblada), permiten resolver el problema de evaluación de riesgos y el cumplimiento de los requisitos para garantizar la seguridad de la información de un APCS e identificar las amenazas actuales a un objeto de protección específico.

Fuente: Elaboración propia

Figura 3

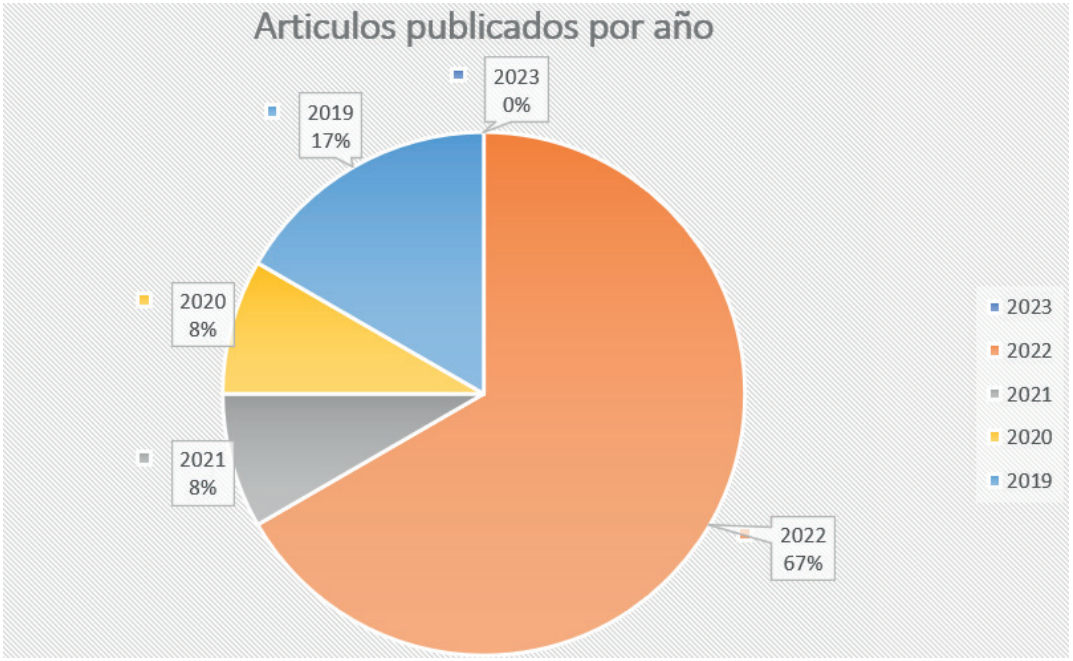
Publicaciones según la nacionalidad de los autores



Fuente: Elaboración propia

Figura 4

Artículos publicados por año



Fuente: Elaboración propia

Tabla 2

Técnicas de la IA aplicados en la seguridad de la información

Autor(es)	Nombre Articulo	Técnica / Propuesta / Modelo de la IA en Seguridad de la Información
Ayachi, Yassine; Mellah, Youssef; Saber, Mohammed; Rahmoun, Noureddine; Kerrakchou, Imane; Bouchentouf, Toumi.	A survey and analysis of intrusion detection models based on information security and object technology cloud intrusion dataset	Modelo de redes neuronales artificiales usando la técnica de machine Learning y Natural Language Processing.
Singh, Shailendra Pratap; Alotaibi, Youseef; Kumar, Gyanendra; Rawat, Sur Singh.	Intelligent Adaptive Optimisation Method for Enhancement of Information Security in IoT-Enabled Environments	Método de optimización inteligente y adaptativo, utilizando técnicas de aprendizaje automático y optimización multiobjetivo.
Moon, Jaewoong; Kim, Subin; Jangyong, Park.; Lee, Jieun; Kim, Kyungshin; Song, Jaeseung.	MalDC: Malicious Software Detection and Classification using Machine Learning	Un método de detección y clasificación de software malicioso utilizando técnicas de aprendizaje automático
Ding, Jun; Alroobaea, Roobaea; Baqasah, Abdullah M; Althobaiti, Anas; Miglani, Rajan; Gill, Harsimranjit Singh.	Big Data Intelligent Collection and Network Failure Analysis Based on Artificial Intelligence	Propuesta de sistema para la recolección inteligente de datos y el análisis de fallas en redes utilizando aprendizaje automático y minería de datos.
Jo, Hyeon	Impact of Information Security on Continuance Intention of Artificial Intelligence Assistant	Un modelo de ecuaciones estructurales de mínimos cuadrados parciales (PLS-SEM).
Han, Yubiao; Wang, Lei; He, Dianhong.	Differential Privacy Technology of Big Data Information Security based on ACA-DMLP	Propuesta de tecnología de privacidad diferencial con las técnicas de Machine Learning, Data Mining, Natural Language Processing y Computer Vision.
Sun, Hongbin; Bai, Shizhen.	Enterprise Information Security Management Using Internet of Things Combined with Artificial Intelligence Technology	Sistema de gestión de seguridad de la información empresarial para la implementación usan el aprendizaje automático y la minería de datos.
Wang, Na; Wang, Kai.	Internet Financial Risk Management in the Context of Big Data and Artificial Intelligence	Técnica de indicadores de riesgos mediante algoritmos de inteligencia artificial para la administración de riesgos financieros en internet.
Guan, Yi; Chen, Qian.	Research on Intelligent Perception and Cognitive Computing of Information Security System Based on Computer Big Data	Método de implementación de Big Data y un algoritmo de IA para la construcción del sistema de conciencia sobre la situación de la seguridad de la información empresarial.
Wiafe, Isaac; Koranteng, Felix Nti; Obeng, Emmanuel Nyarko; Assyne, Nana; Wiafe, Abigail; Gulliver, Stephen R..	Artificial Intelligence for Cybersecurity: A Systematic Mapping of Literature	Técnica de máquina de vectores de apoyo para la detección y prevención de intrusos.
Misra, Tripti; Srivastava, Kingshuk; Rajeshwari.	Challenges of information security in the contemporary cyber threat perception	Implementación de reglas de decisión en la composición del DSS basado en el uso de modelos neuro-fuzzy.
Kirillova A.D.; Vasilyev V.I.; Nikonov A.V.; Berkholts V.V.	Decision support system in the task of ensuring information security of automated process control systems	Técnica de aprendizaje automático que puede predecir y distinguir rápidamente entre amenazas.

Fuente: Elaboración propia

IV. DISCUSIÓN

Inteligencia Artificial

La inteligencia artificial ha revolucionado el mundo tecnológico en la actualidad, causando que muchas organizaciones busquen automatizar sus procesos mediante esta herramienta, la cual es definida como la rama de la informática que se centra en la creación de algoritmos y sistemas que pueden realizar tareas que normalmente requerirían inteligencia humana, como el reconocimiento de patrones, la toma de decisiones y la resolución de problemas (Wiafe, y otros, 2020).

Esta herramienta también brinda un valor agregado a los servicios ofrecidos por una organización, puesto que permite que estos se desarrollen de manera automatizada, disminuyendo la carga de trabajo ocasionada por dichos servicios, además de hacerlo tal cual lo haría un experto en la materia relacionada con en el servicio en cuestión

(Wang & Wang, 2022). Es aquí donde entra el servicio de seguridad de la información, puesto que la automatización de procesos que brinda la inteligencia artificial puede ofrecer beneficios en cuanto a la detección de amenazas (Jo, 2022).

Seguridad de la Información

La seguridad de la información se refiere a la protección de los sistemas y la información de una organización contra amenazas y riesgos de seguridad. En los entornos IoT, donde hay una gran cantidad de dispositivos conectados a la red y una enorme cantidad de datos generados y procesados, la seguridad de la información se vuelve aún más crítica (Pratap, Alotaibi, Kumar, & Singh, 2022).

Otros autores como es el caso de (Moon, y otros, 2022), abordan el concepto de seguridad de la información en el contexto de la detección y clasificación de software malicioso, asegurando que el término seguridad de la información se describe como la protección de los sistemas y la información de una organización contra posibles riesgos y amenazas de seguridad. En el contexto de la detección y clasificación de software malicioso, la seguridad de la información se vuelve aún más crítica debido al constante aumento de amenazas de malware y la complejidad de los ataques cibernéticos. En un artículo reciente, se propone un método para la detección y clasificación de software malicioso utilizando técnicas de aprendizaje y control de procesos automático basados en un algoritmo de soporte de decisiones (Kirillova, Vasilyev, Nikonov, & Berkholts, 2019), y se destaca la importancia de una detección temprana y una clasificación precisa de las amenazas de malware para proteger la información y los sistemas de las organizaciones.

Influencia de la IA en la Seguridad de la Información

Conociendo ya los 2 términos, que son a su vez palabras clave de la presente revisión, podemos analizar la influencia que tiene la IA sobre la seguridad de la información, en qué la beneficia y qué limitaciones acarrea consigo. Comenzaremos con los autores (Ayachi, y otros, 2022), quienes hicieron un estudio sobre el entrenamiento de distintos modelos de defensa implementados con Inteligencia Artificial (IA) para la detección de intrusos en tiempo real, los cuales mostraron una excelente precisión, reduciendo considerablemente el número de falsos positivos.

Por otra parte, los autores (Guan & Chen, 2021) realizaron un análisis de rendimiento de la red neuronal Perceptrón, del cual obtuvieron que este algoritmo muestra una mejora en el tiempo de duración del entrenamiento, el cual es más corto y le permite a la defensa estar preparada en un menor tiempo, además de que este recorte de tiempo no influye en la cantidad de falsos positivos detectados.

Mediante estos estudios podemos conocer que la inteligencia artificial se ha aplicado en la implementación de la seguridad de la información en el campo de detección de amenazas en tiempo real en los sistemas, permitiendo así tomar acciones sobre las intrusiones de manera inmediata (Ding, Alroobaea, Baqash, Althobaiti, & Miglani, 2022).

Además, la IA no solo permite actuar cuando la amenaza ya se encuentra en el sistema, sino que también puede estudiar y predecir patrones de intrusión, permitiéndole así a los tomadores de decisiones establecer medidas ante posibles futuros ataques de robo de información, todo esto de forma automatizada (Ayachi, y otros, 2022).

Como se indicó previamente, una de las características de la IA es aprender sobre la marcha, es así que esta característica es muy aprovechada por los desarrolladores del servicio de seguridad de la información, puesto que la inteligencia artificial puede aprender nuevos patrones que sugieran un posible futuro ataque, autoperfeccionándose a sí misma en su labor (Ayachi, y otros, 2022).

Sin embargo, la aplicación de la IA en seguridad de la información también tiene sus limitaciones, tal y como lo indica el autor (Jo, 2022), quien nos dice que la implementación de esta dependerá mucho del nivel de conocimiento del responsable de dicha instalación, puesto que representa un nivel de complejidad considerable.

Además, nos dice que el nivel de confiabilidad por parte de los usuarios se puede ver afectado, esto debido al nivel de accesibilidad que se le debe otorgar a la IA para que pueda realizar su entrenamiento, lo cual puede afectar la privacidad de los datos; asimismo, la IA interpreta por sí sola los datos obtenidos, clasificando las amenazas automáticamente, por lo que, en caso de error, será responsabilidad única del sistema de defensa, lo que también influye en los niveles de confiabilidad.

V. CONCLUSIONES

La protección de los datos es un gran problema en muchas empresas y más aun las que cuentan con una gran cantidad de información. Teniendo en cuenta la evidencia, concluimos en que la inteligencia artificial es muy usada para la protección de información en diferentes contextos y organizaciones ya que muchas empresas tienen que proteger sus sistemas y datos de los ciberataques. Con lo cual recordaremos nuestra pregunta planteada al comienzo del articulo ¿Cómo se ha aplicado la inteligencia artificial en la industria cibernética para mejorar la seguridad de la información?

La inteligencia artificial (IA) se ha aplicado en la industria cibernética en la mejora de la seguridad de la información de varias maneras, como la detección de ataques maliciosos de seguridad en tiempo real, mediante la utilización de algoritmos de aprendizaje automático, buscando así reducir la predictibilidad de la defensa, y permitiendo crear softwares y plataformas de seguridad con un tiempo de respuesta muy bajo.

Además, la inteligencia artificial se utiliza en la prevención de ataques, donde se pueden utilizar técnicas de modelado predictivo para analizar los datos almacenados, y así prever las posibles amenazas. También se puede utilizar la inteligencia artificial para realizar análisis de vulnerabilidades en los sistemas y redes, lo que ayuda a las empresas a identificar y corregir debilidades antes de que sean aprovechadas por los atacantes.

Sin embargo, también damos a conocer que el implementar esta tecnología trae consigo limitaciones que pueden representar desafíos y riesgos para las organizaciones, las cuales van relacionadas principalmente a la dificultad técnica que significa su implementación, la poca accesibilidad a los datos que suelen ofrecer las organizaciones obstruiría el análisis adecuado, la interpretación de los datos realizada propiamente por la IA puede causar desconfianza entre los usuarios, y los derechos de privacidad de los datos con los que se trabaja pueden no ser respetados. Como recomendación a las distintas empresas y organizaciones, deben aprovechar los beneficios que les ofrece la IA en la seguridad de la información, pero gestionando cuidadosamente los riesgos involucrados.

Para finalizar, se espera que el presente artículo de revisión sistemática sirva como base para futuras investigaciones científicas, brindando una visión amplia y actualizada sobre el papel de la inteligencia artificial en la seguridad de la información. Además, esperamos que los hallazgos y conclusiones presentados en este artículo sean de utilidad para profesionales y expertos en el campo de la seguridad de la información, así como para las organizaciones que deseen implementar soluciones basadas en inteligencia artificial en sus estrategias de protección y prevención de riesgos.

REFERENCIAS

[1] Tu, C., & Sun, J. (2020). Artificial Intelligence and Cybersecurity. Journal of Network and Computer Applications, 159, 102631.

[2] Huang, J.*, & Li, T. (2019). A Survey on Deep Learning for Cybersecurity. ACM Computing Surveys, 52(6), 1-38.

[3] Kshetri, N., & Voas, J. (2020). An Exploratory Study of Artificial Intelligence (AI) in Cybersecurity: A Machine Learning Perspective. IEEE Transactions on Engineering Management, 67(4), 991-1002.

[4] Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., McGuinness, L. A., Stewart, L. A., Thomas, J., Tricco, A. C., Welch, V. A., Whiting, P., & Moher, D. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. doi: 10.1136/bmj.n71

[5] Ayachi, Y., Mellah, Y., Saber, M., Noureddine, R., Kerrakchou, I., & Bouchentouf, T. (2022). A survey and analysis of intrusion detection models based on information security and object technology-cloud intrusion dataset. Retrieved from http://doi.org/10.11591/ijai.v11.i4.pp1607-1614

[6] Ding, J., Alroobaea, R., Baqash, A., Althobaiti, A., & Miglani, R. (2022). Big Data Intelligent Collection and Network Failure Analysis Based on Artificial Intelligence. Retrieved from https://doi.org/10.31449/inf.v46i3.3866

[7] Guan, Y., & Chen, Q. (2021). Research on Intelligent Perception and Cognitive Computing of Information Security System Based on Computer Big Data. Retrieved from https://doi.org/10.1155/2021/3281825

[8] Han, Y., Wang, L., & He, D. (2022). Differential Privacy Technology of Big Data Information Security based on ACA-DMLP.

Retrieved from https://dx.doi.org/10.14569/IJACSA.2022.0130905

[9] Jo, H. (2022). Impact of Information Security on Continuance Intention of Artificial Intelligence Assistant. Retrieved from https://doi.org/10.1016/j.procs.2022.08.093

[10] Kirillova, A., Vasilyev, V., Nikonov, A., & Berkholts, V. (2019). Decision support system for ensuring information security of an automated process control system. Retrieved from http://repo.ssau.ru/bitstream/Informacionnye-tehnologii-i-nanotehnologii/Decision-support-system-for-ensuring-information-security-of-an-automated-process-control-system-75670/1/paper48.pdf

[11] Misra, T., Srivastava, K., & Rajeshwari. (2019). Challenges of Information Security in the Contemporary Cyber Threat Perception. Retrieved from http://dx.doi.org/10.35940/ijitee.J1060.08810S19

[12] Moon, J., Kim, S., Jangyong, P., Lee, J., Kim, K., & Song, J. (2022). MalDC: Malicious Software Detection and Classification using Machine Learning. Retrieved from http://doi.org/10.3837/tiis.2022.05.004

[13] Pratap, S., Alotaibi, Y., Kumar, G., & Singh, S. (2022). Intelligent Adaptive Optimisation Method for Enhancement of Information Security in IoT-Enabled Environments. Retrieved from https://doi.org/10.3390/su142013635

[14] Quispe, A., Hinojosa, Y., Miranda, H., & Sedano, C. (2021). Serie de Redacción Científica: Revisiones Sistemáticas. Retrieved from http://cmhnaaa.org.pe/ojs/index.php/rcmhnaaa/article/view/906

[15] Sun, H., & Bai, S. (2022). Enterprise Information Security Management Using Internet of Things Combined with Artificial Intelligence Technology. Retrieved from https://doi.org/10.1155/2022/7138515

[16] Wang, N., & Wang, K. (2022). Internet Financial Risk Management in the Context of Big Data and Artificial Intelligence. Retrieved from https://doi.org/10.1155/2022/6219489

[17] Wiafe, I., Koranteng, F., Obeng, E., Assyne, N., Wiafe, A., & Gulliver, S. (2020). Artificial Intelligence for Cybersecurity: A Systematic Mapping of Literature. Retrieved from https://doi.org/10.1109/ACCESS.2020.3013145

Fuentes de financiamiento:

Propia.

Conflictos de interés:

Los autores declaran no tener conflictos de interés.