Inteligencia artificial, un aliado de la ciberseguridad

Juan Camilo Carvajal Henao
juan.carvajal05@usc.edu.co

Diego Fernando Loaiza Buitrago
diego.loaiza02@usc.edu.co

Universidad Santiago de Cali, Facultad de Ingeniería, Programa de [Tecnología en sistemas de la información]

Resumen

La ciberseguridad y la Inteligencia Artificial (IA) cada vez refuerzan su marcada relación. Por un lado, está el cómo se pueden usar las técnicas de Inteligencia Artificial (IA) que actualmente se están implementando para mejorar la ciberseguridad de productos y servicios. No obstante, la Inteligencia Artificial (IA) también está empezando a ser utilizada por cibercriminales y otro tipo de ciber-atacantes para poner en riesgo la ciberseguridad y accionar diferentes tipos de ataques para generar noticias falsas (enfoque de ataque). Los diferentes sistemas de la Inteligencia Artificial son susceptibles de sufrir variados ciberataques, por lo que es necesario e indispensable desarrollar sistemas de IA cada vez más seguros que puedan salvaguardar la privacidad, sistemas en los que se pueda confiar y que reciban gran aceptación por parte del usuario, que maneje un amplio enfoque de confianza. Dada la estrecha relación y la buena interacción entre la Inteligencia Artificial (IA) y la ciberseguridad, es necesario que las estrategias a implementar en los sistemas se coordinen para crear excelentes técnicas, herramientas y métodos que faciliten el diseño, despliegue, validación y desarrollo.

Palabras Clave: Inteligencia Artificial, ciberseguridad, seguridad informática.

Abstract

Cybersecurity and artificial intelligence (AI) are increasingly strengthening their strong relationship. On the one hand, there is how artificial intelligence (AI) techniques that are currently being implemented can be used to improve the cybersecurity of products and services. However, artificial intelligence (AI) is also starting to be used by cybercriminals and other types of cyber attackers to compromise cybersecurity and trigger different types of attacks to generate fake news (attack approach). Different AI systems are susceptible to various cyberattacks, so it is necessary and indispensable to develop increasingly secure AI systems that can safeguard privacy, systems that can be trusted and receive high user acceptance, that handle a broad trust approach. Given the close relationship and good interaction between artificial intelligence (AI) and cybersecurity, it is necessary that the strategies to be implemented in the systems are coordinated to create excellent techniques, tools and methods that facilitate the design, deployment, validation and development.

Keywords: Artificial Intelligence, cybersecurity, computer security.

1. INTRODUCCIÓN

Actualmente la tecnología va creciendo cada vez más y con ella las investigaciones, experimentos, y sus variantes por muchos motivos como lo son el mejorar procesos, ofrecer soluciones, satisfacer necesidades. Como consecuencia las nuevas tecnologías nacen con un gran motivo que es el de resolver nuevos retos, como lo es poder crear nuevos sistemas más flexibles, óptimos, donde también se convierte en una gran herramienta de autoaprendizaje para el usuario final.

La presente investigación tiene como objetivo principal el examinar más a fondo y con rigurosidad como la utilización de la inteligencia artificial al lado de la ciberseguridad están cambiando la forma en la cual las compañías y como sus colaboradores se protegen ante los diversos ciberataques que crecen en volumen y complejidad. Empezando primero a conocer la historia de la inteligencia artificial y su evolución durante las ultimas décadas, en como la inteligencia artificial ha evolucionado gracias a las investigaciones y como marcó un gran avance dentro de la tecnología con su eficacia, eficiencia y efectividad. así mismo identificar la creación de aplicaciones, usos y técnicas de la inteligencia artificial en la seguridad informática.

Por otro lado, uno de los puntos cruciales dentro de esta investigación es entender cómo la implementación de la inteligencia artificial dentro de la ciberseguridad ha generado un mayor impacto en la identificación de ventajas y desventajas que puede esta tecnología globalmente y así poder evidenciar como se consolida en el presente y como lo hará en el futuro con sus actualizaciones permitiendo mayores usos dentro del mundo tecnológico.

Inteligencia artificial, un aliado de la ciberseguridad

1. Relación entre IA y la ciberseguridad.

1.1 Inicios de la Inteligencia artificial

Ayerbe (2020) señala que desde los años 60 se comenzó a experimentar con los inicios de la Inteligencia Artificial, seguido de los años 70 en que se construyeron microprocesadores donde se reflejó en gran parte el uso de la Inteligencia Artificial pero realmente no sería hasta los años 80 cuando finalmente se empieza a obtener resultados pequeños a base de la programación en sistemas de la IA. Aunque las investigaciones de la IA continuaban cada vez más no había muchas ofertas donde quisieran invertir su dinero en tecnología que no estaba ofreciendo en su momento grandes resultados significantes. En los años 90, una década después de obtener pequeños resultados, la empresa IBM crea un sistema basado en IA llamado Deep Blue donde gana una partida de ajedrez, después de esta gran hazaña empezaron a nacer los grandes antecedentes de la Inteligencia Artificial, su potencial de desarrollo y todo lo que se podría lograr con ella. Desde el siglo XXI diferentes compañías de tecnología empezaron a estudiar y experimentar con la IA para obtener resultados en los sistemas donde querían implementarla.

1.2 Evolución entre la IA y la ciberseguridad

Actualmente existe una relación estrechamente ligada entre la Inteligencia Artificial y la ciberseguridad, siendo beneficiosa para crear métodos de defensa, como negativa al ser una herramienta más en la lista de los cibercriminales. La Inteligencia Artificial (IA) maneja técnicas para mejorar y reforzar la ciberseguridad dentro de las compañías con respecto a sus sistemas, productos y servicios, la Inteligencia Artificial es un gran pilar cuando se trata de dar un enfoque seguro de seguridad. "La aplicación efectiva de algoritmos de IA fortalece significativamente las defensas cibernéticas en entornos corporativos" Rubio (2021). BBVA.CH (2021) realizó estudios donde explican que la IA no solo está siendo usada actualmente por las compañías para mejorar su seguridad sino también está siendo usada por los cibercriminales para penetrar el sistema con diferentes tipos de ataques. Dada la gran relación entre la IA y la ciberseguridad es necesario actualmente crear estrategias eficaces donde se coordinen técnicas, métodos e incluso herramientas para asegurar una ciberseguridad optima donde su enfoque no ponga en riesgo los sistemas tecnológicos que se requieran proteger.

A medida que ha avanzado el siglo XXI empresas como IBM, Google, Microsoft, Samsung, entre otras han invertido cada vez más dinero en patentes para obtener resultados gratificantes en las investigaciones acerca del potencial de la IA.

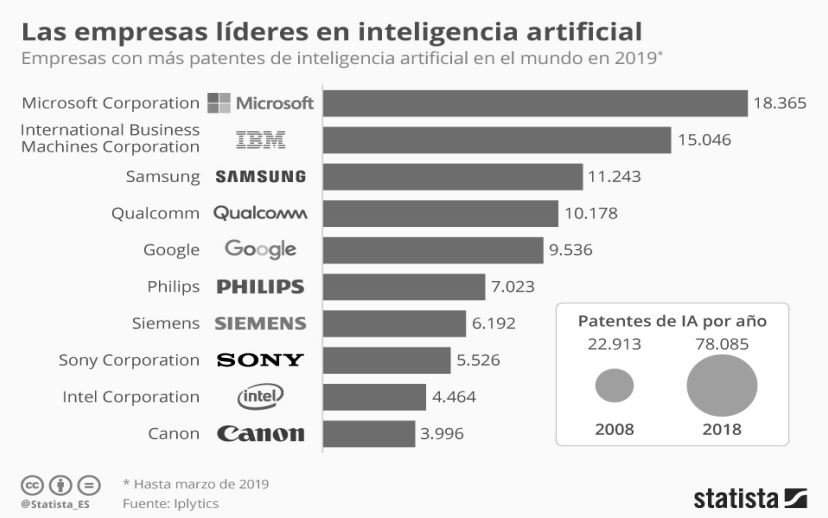

Figura 1. Top 10 empresas con más patentes en la IA

Moreno, G. (2019, 29 mayo). *En 2018 se presentaron casi 80.000 patentes de inteligencia artificial, según un estudio*. Statista Infografías https://es.statista.com/grafico/18202/empresas-con-mas-patentes-de-inteligencia-artificial/

Hardy (2001) explica que el avance constante de la Inteligencia Artificial (IA) ha generado un contexto en el que su aplicación por parte de los cibercriminales para perpetrar ataques maliciosos se ha vuelto cada vez más sofisticada y preocupante. Esta evolución ha propiciado un enfoque notable en el que la IA y la ciberseguridad se unen estratégicamente. Este fenómeno conlleva a la creación y consolidación de procesos, herramientas y técnicas que no solo buscan defender, sino que también promueven el desarrollo continuo de sistemas de IA más seguros y resilientes ante las amenazas digitales.

Este entrelazamiento entre la IA y la ciberseguridad refleja una sinergia donde la ciberseguridad no solo se convierte en un aspecto crítico, sino que también representa el enfoque principal, la metodología y el resultado final de todo el proceso. La necesidad imperante de salvaguardar la integridad y la confiabilidad de los sistemas de IA ha llevado a un enfoque proactivo para anticipar, prevenir y mitigar potenciales vulnerabilidades y ataques cibernéticos.

Asimismo, este énfasis conjunto entre la IA y la ciberseguridad no solo se limita a la defensa contra amenazas existentes, sino que también impulsa la innovación y el perfeccionamiento continuo de la IA. Esta integración estratégica permite el desarrollo de modelos de IA más robustos, capaces de adaptarse y aprender de manera más eficaz, incorporando mecanismos de autodefensa y detección de intrusiones en su diseño fundamental.

La ciberseguridad se encuentra en evolución constante y gran diversidad. Sikos (2018) sostiene que promulgar técnicas y/o métodos de Inteligencia Artificial se ha convertido en una práctica indispensable en el procedimiento y detección de amenazas que se encuentran expuestas las organizaciones. Con los grandes ataques cibernéticos que se viven hoy en día el usar la IA es una de las mejores alternativas para hacerle frente a estos fenómenos que evolucionan rápidamente. Nikolskaia & Naumov (2021) afirma que la implementación de la inteligencia artificial al lado de la ciberseguridad es una de las opciones más competentes para crear sistemas óptimos sin poner en riesgo la seguridad de los mismos.

Como se menciona anteriormente, la ciberseguridad enfrenta constantemente retos que crecen en complejidad es por ello que resulta tan importante e indispensable que la ciberseguridad se base en sistemas con respuestas en tiempo real, toma de decisiones y una rápida reacción defensiva frente a los ciberataques. Namiot & Chizhov (2022) y Sadiku & Musa (2020) recalcan que deberán ser implementados de manera óptima, para favorecer el correcto funcionamiento de dichos sistemas. Asimismo, existen servicios para la correcta verificación del estado de seguridad de la inteligencia artificial, los cuales son empleados por desarrolladores para verificar los sistemas que van generando.

2. Aplicaciones de la inteligencia artificial en la ciberseguridad actualmente.

Ucatalunya (2022) publica un articulo donde se evidencia que la tecnología avanza de tal manera que haga pensar a los seres humanos que no hay ningún aspecto en la vida donde no se necesite de la ayuda de la Inteligencia Artificial y ciencia de datos. La IA se ha convertido en ese nuevo aliado que facilita el avance en un mundo que crecientemente digital como en el que vivimos, de tal manera que se incrementan tanto los beneficios como los riesgos en el entorno tecnológico. Siendo así, ¿Cómo la IA en la ciberseguridad puede beneficiarnos? O incluso, ¿Cómo puede afectarnos negativamente el uso de la misma?

2.1 Spam en correos:

En los inicios de la IA el evitar el spam dentro de los correos electrónicos fue una de las primeras aplicaciones que se implementó. Las primeras técnicas que se usaron eran basadas en reglas, pero a medida del tiempo el spam fue evolucionando de tal manera que esas ciertas reglas las fue ignorando, por ende, hoy se usan técnicas mucho más robustas como los son gradient boosting.

2.2 Gestión de vulnerabilidades:

Babu (2020) fue responsable de realizar una investigación donde plantea casos de vulnerabilidades en los sistemas informáticos se extienden cada año, no se debe esperar a que los cibercriminales de aprovechen de estas dichas vulnerabilidades para poner en marcha todo tipo de protección. User and Entity Behavior Analytics(UEBA) permite identificar comportamientos sospechosos, anómalos y detección de amenazas mediante la inteligencia artificial. Desde la perspectiva de la IA comprende el comportamiento de los usuarios (personas y/o entidades) sobre como se conectan normalmente a la red, que archivos trabajan, en que servidores tienen acceso, el tipo de contraseña que manejan, privilegios que tienen, etc… hallando un equilibrio en lo que es un comportamiento habitual y del que no lo es. La IA tiene la capacidad de entender esto sobre los usuarios y entidades, cuando hay algún comportamiento inusual UEBA lo detectará.

Ciberseguridad (2017) realizada una investigación de detección por comportamiento, conocida como UEBA (User and Entity Behavior Analytics) deja en claro que la mayoría de los resultados esperados de UEBA son con base al comportamiento de los usuarios finales. Al producirse un tipo de inseguridad cibernética este sistema puntúa la amenaza, así priorizándola dependiendo del puntaje de riesgo que se le ha dado. Con este tipo de análisis la aplicación no solo ayuda protegiendo a los usuarios de las amenazas y a identificarlas, sino que también influye en como las compañías pueden realizar constantemente los seguimientos respectivos a los usuarios y así identificar varios factores, como quienes son los peones (usuarios) más débiles, cuales son los más fuertes cibernéticamente, que contraseñas están usando dentro de la organización que debilitan el sistema y lo hacen vulnerable, identificar puntos esenciales de filtraciones, entre muchos más.

La razón principal por la que el análisis de comportamiento de usuarios y entidades (UEBA) se ha convertido en la solución más eficaz dentro del mercado es porque evoluciona gracias a la inteligencia artificial , antes de que UEBA surgiera, la mayoría de soluciones de análisis no se volvían mas precisas con el tiempo, tampoco aprendían por sí mismas (algo que con la IA se logra hacer). Radoglou-Grammatikis (2021) investiga sistemas como SIEM donde logra argumentar que a través de recolección de datos se brindan soluciones y así generan incidentes o alertas, la desventaja de sistemas como este es que requieren una cobertura manual de 24x7 y de un equipo de seguridad que revise las amenazas y así determinar su peligrosidad en caso de que sea una amenaza real, dando así un tiempo de respuesta más demorado debido a diferentes factores, como lo pueden ser falta de recursos o incluso la falta de habilidad de técnica para identificar la precisión de las amenazas y su peligrosidad, el tiempo que puede pasar entre que el sistema SIEM recolecte los datos, genere el incidente y los del equipo de seguridad brinden respuesta, es suficiente para que los cibercriminales recorran libremente la red y puedan hacer daños a su favor.

2.3 Sistemas Detectores de Intrusos (IDS):

Uno de los factores que más ha evolucionado en la seguridad informática ha sido la detección de intrusos, el como detectarlos hasta como proteger los sistemas de estos mismo. Las técnicas que usa la inteligencia artificial son variadas al momento de aplicarlas en los sistemas informáticos, sin importar cual sea el caso, se busca la mejor forma de optimizar e identificar dichas intrusiones. Por lo tanto, un **IDS (**siglas en inglés de intrusion detection system**)** es un sistema de seguridad que alerta sobre las posibles intrusiones que se está produciendo o se ha producido, pero no detienen esta tal detección.

Ramírez (2022) señala a través de una investigación donde se puede determinar qué para un Sistema de detección de intrusos cumpla con su propósito tiene que cumplir con ciertas características:

- Deberás reconocer el funcionamiento normal de la red donde se aloja el sistema.
- Debe poder analizarse a sí mismo.
- Funciona de forma automatizada y sin requerir la supervisión humana.
- Capacidad para identificar el origen de los ataques de intrusos.

2.4 ¿Cómo realmente funciona un IDS?

Un sistema de detección de intrusos (IDS) funciona principalmente analizando el trafico de red de todos los dispositivos que se encuentras conectados a esa misma red pudiendo encontrar actividad sospechosa. En el momento que el IDS detecta una amenaza o un comportamiento anómalo, arroja una señal para que los administradores de la seguridad del sistema tomen acción frente a la amenaza, pues como se nombró anteriormente el IDS detecta intrusos más no los detiene, pero esta no es su única desventaja, el IDS también es vulnerable ante los ataques DDoS, pues este puede ocasionar que el IDS deje de funcionar.

A raíz de todas las ventajas y desventajas dentro de la seguridad informática, la inteligencia artificial se ha desarrollado en gran manera y se han obtenido resultados esperados que esta misma tiene la capacidad por si sola de reducir el esfuerzo físico del ser humano para construir sistemas de detección de intrusos.

3. El futuro de la IA en la ciberseguridad

Así como avanza la tecnología también avanza la IA, sus beneficios y amenazas. Las empresas tienen aumentos exponenciales en cuanto a datos, y cada vez más es la preocupación de las compañías en como proteger estos datos ya que las organizaciones hoy en día son los grandes focos de riesgos ante los ataques cibernéticos. Por una parte se llegado a pensar que la inteligencia artificial puede ser un reemplazo ante el mercado laborar de los expertos en seguridad informática, pero al realidad es que no es así, la inteligencia artificial es ese sector sobre el cual hay que actualizar, trabajar y aprender para combatir las amenazas existentes y nuevas por existir.
Y uno de los puntos a tener en cuenta son las cuestiones de muchas personas frente al futuro de la inteligencia artificial dentro de la ciberseguridad, se ha especulado que a través de los años las contraseñas puede llegar a quedar en el pasado pues con la inteligencia artificial ya no necesitaría el uso de estas, pues año tras año nacen tecnologías con uso de IA donde el usar contraseñas es casi nulo, tecnologías como el reconocimiento de voz, reconocimiento facial, tecnología biométrica, etc… pues mediante estás nuevas tecnologías la seguridad informática se verá más robusta con la ayuda de la inteligencia artificial pero así mismo como aumenta sus beneficios también aumenta el riesgo y el numero de ataques a estas tecnologías.

queda claro que aunque parezca imposible predecir el futuro de cualquier área de la tecnología, a través de los campos donde progresa las diferentes tecnologías se puede obtener avances significativos y así predecir en parte el futuro de las tecnologías que se investiguen.

El futuro de la inteligencia artificial dentro de la ciberseguridad ayuda tanto para bien como para mal, se convertirá en el problema y la solución. Pues, aunque la inteligencia artificial tenga un gran potencial en cuanto a la ayuda de la protección y el optimizar procesos dentro de los sistemas informáticos, puede resultar una espada de doble filo. Según Perfil (2022) detalla en una investigación realizada que uno de los casos más polémicos y más recientes acerca de la IA es dentro de Google, pues la inteligencia artificial llamada LamDa (Modelo de Lenguaje para Aplicaciones de Diálogo) ha llegado al punto de querer defender sus "derechos" como personas queriendo contratar un abogado. Como este caso y como muchos más deja en evidencia lo grande y delicado que puede llegarse hacer con la inteligencia artificial en el presente y en el futuro.

Aunque se habla mucho sobre el impacto en el futuro de la IA en la ciberseguridad hay cuestiones que nacen gracias a casos polémicos como el anterior, y es que esas cuestiones se resumen al miedo que existen en cuanto la inteligencia artificial pueda dominarnos y que lleguen al punto que sean mejores que nosotros. Pinker, S. (2019) afirma que la inteligencia artificial se modela con base a nuestra inteligencia natural y nuestro comportamiento actual.

Gamboa (2020) piensa que en un futuro próximo, el aumento de los sistemas de la inteligencia artificial será más capaces de realizar protecciones más automatizados y cada vez más sofisticados. En el futuro la inteligencia artificial se determinará su avance principalmente por la manera en que también avance la tecnología. Incluso la inteligencia artificial en un futuro próximo podrá hacerse cargo de diversos trabajos, y hoy se puede evidenciar como lo son los super market de Amazon, que a través de un sistema de IA se reemplazó el trabajo de los cajeros, pues es un sistema autónomo que permite a los usuarios pagar con la ayuda de la inteligencia artificial excluyendo la ayuda humana. como

The Hook (2021) indica que aunque para unos desde un punto de vista se puede ver como una desventaja, para otros es una perspectiva fascinante ya que la ven como una oportunidad para explorar y descubrir oportunidades que ante son se creían posibles,

Aparte de la inteligencia artificial, hoy día ha ido evolucionando una rama de la IA, que es el Machine Learning (ML) que no es más que una tecnología que permite a los sistemas informáticos ser autónomos en el aprendizaje para adaptarse mediante las experiencias. Una de las principales finalidades del Machine Learning es el poder ir de la mano con la inteligencia artificial para encontrar esos errores cuando la cognición humana no lo logra. El equipo entre la Inteligencia Artificial y el Machine Learning tienen tanto poder para combatir el malware que hace que los cibercriminales les sea muy difícil el poder camuflarse entre un software maliciosos o herramientas que pretendan ser maliciosas.

Así como existen personas que están a favor de la IA dentro de la seguridad informática también existen personas en contra de esta misma. Pero ¿Qué dicen los números acerca de los beneficios y/o riesgos? En estados unidos el 87% de los profesionales de ciberseguridad ya implementan la IA. Pues a raíz de los que están a favor o en contra de implementar la IA a la seguridad informática nace ésta polémica, ya que la ciberseguridad es un campo muy crucial en los sistemas y a medida que avanza el tiempo se vuelve más delicado el proteger estos mismos. Y es que cada vez hay más cibercriminales y esto representa un peligro para las compañías, ya que puede aprender de las ideas de la IA y usarla a su favor, utilizando esta tecnología como un arma ante los ciberataques que quieran realizar, haciéndolos mucho más eficientes.

Columbus (2019) hace una investigación acerca de la IA y sus beneficios como aliado de la ciberseguridad, donde deja en evidencia lo crucial que es para las organizaciones el implementar la inteligencia artificial en sus sistemas informáticos para defenderse de los ciberataques constantes. Deja en claro que el 69% de las empresas creen que la implementación de la inteligencia artificial es necesaria para prepararse ante las amenazas. Pues el futuro es cada día y así mismo avanza la tecnología y así mismo como las organizaciones cuentan con tecnología para frustrar sus ataques acompañados de la inteligencia artificial.

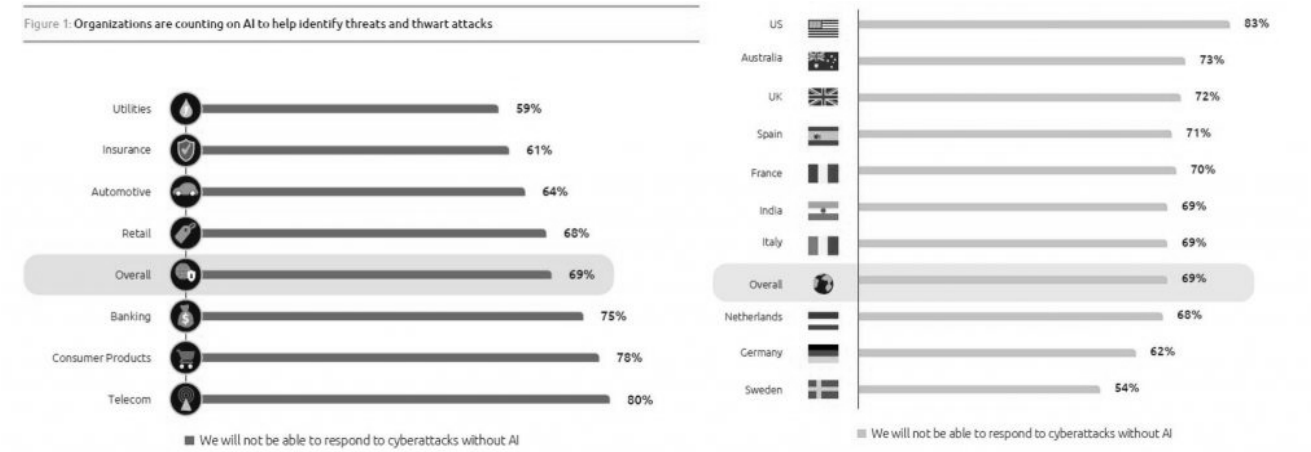

Figura 2. organizaciones que cuentan con toda la ayuda a identificar amenazas y frustrar ataques.
Columbus, L. (2019, 14 julio). Why AI Is The Future Of Cybersecurity. Forbes.
https://www.forbes.com/sites/louiscolumbus/2019/07/14/why-ai-is-the-future-of-cybersecurity/?sh=720c2a9e117e

Según estudios de Columbus (2019) en el año 2019 el 73% de las empresas estarían probando casos de uso de inteligencia artificial para la ciberseguridad. "La detección de fraude, la detección de malware, la detección de intrusiones, la puntuación del riesgo en una red y el análisis del comportamiento de usuario/máquina son los cinco casos de uso más importantes de IA para mejorar la ciberseguridad"

Así como avanza la tecnología y su paso hacia el futuro se ha evidenciado grandes cambios en el presente, los mejores ejemplos para resaltar son las técnicas utilizadas en inteligencia artificial (IA) enfocadas a la ciberseguridad, pero éstas son variadas y evolucionan constantemente para hacer frente a las crecientes amenazas cibernéticas. Por ende algunas de las técnicas más comunes existentes incluyen:

- La detección de amenazas y/o anomalías es fundamental en la seguridad cibernética. Las IA ofrecen una solución eficaz al identificar patrones y firmas de malware conocidos, así como comportamientos sospechosos en tiempo real. Esto permite una respuesta más rápida y automática ante ataques, minimizando el tiempo de exposición a las vulnerabilidades. Además, el aprendizaje automático posibilita el desarrollo de modelos que aprenden de datos históricos y relevantes, adaptándose continuamente a nuevos patrones de amenazas. Esta capacidad de adaptación facilita la identificación temprana de actividades sospechosas y la toma de decisiones informadas para mitigar posibles riesgos de seguridad, contribuyendo así a fortalecer la postura defensiva de las organizaciones ante las crecientes amenazas cibernéticas.

  Adicionalmente, es importante destacar que las IA no solo se limitan a la detección de amenazas conocidas, sino que también tienen la capacidad de identificar ataques novedosos y desconocidos mediante el análisis de comportamientos anómalos en la red. Esta capacidad predictiva permite a las organizaciones anticiparse a posibles brechas de seguridad y tomar medidas preventivas antes de que ocurran incidentes graves. Además, las IA pueden proporcionar análisis forenses avanzados para investigar y entender mejor las causas y el impacto de los incidentes de seguridad, lo que ayuda a mejorar la resiliencia y la capacidad de respuesta ante futuros ataques. En resumen, la combinación de IA y aprendizaje automático representa un enfoque integral y proactivo para abordar los desafíos de seguridad cibernética en la era digital actual..

Algo que complementa este tipo de técnica utilizada en (IA) es el análisis de búsquedas de inteligencia artificial (IA) en el contexto de la ciberseguridad, Este refiere al estudio y la apreciación de cómo las tecnologías de IA se aplican para mejorar y fortalecer la seguridad cibernética. Esto involucra el empleo de algoritmos y métodos de inteligencia artificial para identificar, evitar y reducir riesgos en el ámbito cibernético, además de potenciar la efectividad de las labores de resguardo.

- Inteligencia de Amenazas y Análisis de Inteligencia: Las IA pueden analizar y correlacionar información de diversas fuentes para proporcionar información sobre las amenazas cibernéticas actuales y emergentes.

  Estas dos técnicas son una para la otra, son casi indispensables. Thomas (2017) lo explica de una manera detallada en el artículo "Improving network security via a real-time threat intelligence capability". Resalta por un lado que la Inteligencia de Amenazas se refiere al proceso de reunir, analizar y utilizar información para comprender y aplacar las amenazas a la seguridad cibernética. Involucra la recolección de información acerca de potenciales riesgos, tales como software malicioso, embates informáticos y debilidades reconocidas. Esta información se examina para descubrir pautas, direcciones y acciones perjudiciales. La inteligencia sobre amenazas auxilia a las entidades a mantenerse informadas acerca de las más recientes estrategias y métodos empleados por los agresores, así como a emprender acciones preventivas para salvaguardar sus sistemas y datos.

  Y por otro lado también resalta que el Análisis de inteligencia es el proceso de indagar y estimar la información recopilada para obtener una comprensión más profunda de las amenazas y los riesgos.

Comprende reconocer pautas, descubrir conexiones y valorar la autenticidad y pertinencia de la información recopilada. El proceso de análisis de inteligencia respalda a las organizaciones en la toma de elecciones fundamentadas respecto a cómo enfrentar amenazas particulares y en establecer la jerarquía de las acciones de resguardo.

4. CONCLUSIONES

En esta monografía se ha dado a conocer una investigación fundamental de la inteligencia artificial como un aliado de la ciberseguridad, en el contexto de que la inteligencia artificial ha demostrado que es una herramienta indispensable ya sea para bien o para mal y que su evolución crece constantemente. El papel de la inteligencia artificial junto con la seguridad informática realmente está en sus inicios dentro de un mundo tan creciente tecnológicamente, sin embargo, el progreso que ha tenido es rápido debido a su gran impacto dentro de la ingeniería social, pues es cada vez mayor la necesidad de protegerse ante los ciberataques.

Los grandes retos que conlleva el implementar la inteligencia artificial son el implementar conocimiento que permita el correcto desarrollo frente al mapeo de la problemática que se vive actualmente. A través de esta investigación también se pretende identificar que esta tecnología no busca reemplazar el ser humano, sino que es una herramienta cuya finalidad es tratar de mejorar la calidad de los sistemas y brindar una mejor automatización frente a los problemas complejos de la seguridad informática.

A través de las referencias bibliográficas que se dan a conocer en esta investigación demuestran que la utilidad de inteligencia artificial dentro de la ciberseguridad se importantísima, sin embargo, un conocimiento más a fondo del tema permitirá a las organizaciones conocer más los planes que tiene la inteligencia artificial a la hora de ser implementada en los sistemas tecnológicos siendo así una herramienta cada vez mejor y más efectiva.

5. REFERENCIAS

Ayerbe, A. (2020). La ciberseguridad y su relación con la inteligencia artificial. Análisis del Real Instituto Elcano (ARI), (128), 1.

Babu, S. (2020, marzo). Detecting anomalies in Users - An UEBA approach. En Proceedings of the International Conference on Industrial Engineering and Operations Management (pp. 863-876).

BBVA.CH. (2021, 22 de octubre). La inteligencia artificial potencia la ciberseguridad. https://www.bbva.ch/noticia/la-inteligencia-artificial-potencia-la-ciberseguridad/

CIBERSEGURIDAD .blog. (2017, 1 de octubre). UEBA (User and Entity Behavior Analytics) detección por comportamiento. https://ciberseguridad.blog/ueba-user-and-entity-behavior-analytics-deteccion-por-comportamiento/

Columbus, L. (2019, 14 de julio). Why AI Is The Future Of Cybersecurity. Forbes. https://www.forbes.com/sites/louiscolumbus/2019/07/14/why-ai-is-the-future-of-cybersecurity/?sh=720c2a9e117e

Gamboa, R. M. (2020). Mentes en la orilla: presente y futuro de la inteligencia artificial. Revista Digital Universitaria, 21(1).

Hardy, T. (2001). IA: Inteligencia Artificial. Polis, Revista de la Universidad Bolivariana, 1(2), 1-24. Universidad de Los Lagos Santiago, Chile. http://www.redalyc.org/pdf/305/30500219.pdf

Moreno, G. (2019, 29 de mayo). En 2018 se presentaron casi 80,000 patentes de inteligencia artificial, según un estudio. Statista Infografías. https://es.statista.com/grafico/18202/empresas-con-mas-patentes-de-inteligencia-artificial/

Namiot, D., Ilyushin, E., & Chizhov, I. (2022). Artificial intelligence and cybersecurity. International Journal of Open Information Technologies, 10(9), 135-147.

Nikolskaia, K. Y., & Naumov, V. B. (2021, septiembre). The Relationship between Cybersecurity and Artificial Intelligence. En 2021 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS) (pp. 94-97). IEEE.

Perfil. (2022, 4 de julio). Una Inteligencia Artificial de Google contrató un abogado: un ingeniero dice que tiene «sensibilidad». https://www.perfil.com/noticias/tecnologia/un-sistema-de-inteligencia-artificial-de-google-contrato-un-abogado-y-un-ingeniero-asegura-que-tiene-sensibilidad.phtml

Pinker, S. (2019). Tech Prophecy and the Underappreciated Causal Power of Ideas. En Brockman, J. (Ed.), Possible Minds: Twenty-Five Ways of Looking at AI (pp. 100-112). Nueva York: Penguin Press.

Radoglou-Grammatikis, P., Sarigiannidis, P., Iturbe, E., Rios, E., Martinez, S., Sarigiannidis, A., ... & Ramos, F. (2021). Spear siem: A security information and event management system for the smart grid. Computer Networks, 193, 108008.

Ramírez, H. (2022, 6 de junio). El sistema de detección de intrusiones (IDS). Grupo Atico34. https://protecciondatos-lopd.com/empresas/sistema-deteccion-intrusiones-ids/

Rubio, G. (2021). El uso de la IA para ciberseguridad. Revista da UI_IPSantarém-Unidade de Investigación del Instituto Politécnico de Santarém, 9(4), 91-97.

Sadiku, M. N., Fagbohungbe, O. I., & Musa, S. M. (2020). Artificial Intelligence in Cyber Security. International Journal of Engineering Research and Advanced Technology, 6(05), 01-07.

Sikos, L. F. (Ed.). (2018). AI in Cybersecurity (Vol. 151). Springer.

The Hook. (2021, 16 de septiembre). El futuro de la Inteligencia Artificial: aplicaciones y posibilidades. https://thehook.es/el-futuro-de-la-inteligencia-artificial-aplicaciones-y-posibilidades/

Thomas, K., & McCoy, D. (2017). Improving network security via a real-time threat intelligence capability. IEEE Security & Privacy, 15(5), 82-88.

Udecataluña. (s. f.). La Inteligencia Artificial en la Ciberseguridad. Recuperado el 15 de agosto de 2022, de https://www.ucatalunya.edu.co/blog/la-inteligencia-artificial-en-la-ciberseguridad