Fundación Universitaria del Área Andina

La inteligencia artificial y Blockchain, dos elementos decisivos en el futuro de la ciberseguridad

Artificial intelligence and Blockchain, two decisive elements in the future of cybersecurity.

Jesus Herney Fuenmayor Tobar
Derly Katherine Torres Lozano
Leydy Dayana Monsalve Pérez
Anyi Marcela Becerra Moreno

RESUMEN

En la era de la información existe un desafío latente para las organizaciones y quienes quieren mantenerse a la vanguardia sobre la optimización de sus servicios y controles, principalmente en el campo de la ciberseguridad, por causa al aumento de delitos a infraestructuras informáticas, lo que ha afectado a la ciudadanía y sus organizaciones, es por esto que **e**l propósito de este estudio fue el de analizar los efectos que la Inteligencia Artificial (IA) y Blockchain pueden tener en la ciberseguridad. se ha empleado un método que integra un instrumento implementado en el campo mencionado, la revisión de literatura especializada y el análisis de informes de ciberataques. Como resultado, el frecuente aumento en los ciberataques en Colombia lleva a la necesidad de una actualización de las medidas de seguridad actuales. En ese caso, la combinación de Blockchain y la inteligencia artificial podrían ser decisivas gracias a sus atributos que las hacen complementarias entre si principalmente en el campo de la salud y movimientos financieros.

Se puede imaginar la ciberseguridad como un escudo que protege nuestras infraestructuras y datos esenciales. La inteligencia artificial es un guardián astuto que puede analizar una gran cantidad de datos y descubrir comportamientos y patrones sospechosos. En cuanto a Blockchain, graba todas las transacciones y modificaciones de la información. Por lo tanto, se permite que los datos sean íntegros y confidenciales. La combinación de blockchain e inteligencia artificial puede aprovechar aún más la defensa de datos. La inteligencia artificial puede hacer posible la identificación y prevención de las amenazas.

ABSTRACT

In the information age there is a latent challenge for organizations and those who want to stay ahead on the optimization of their services and controls, mainly in the field of cybersecurity, due to the increase of crimes to computer infrastructure, which has affected citizens and their organizations, which is why the purpose of this study was to analyze the effects that Artificial Intelligence (AI) and Blockchain can have on cybersecurity. a method that integrates an instrument implemented in the mentioned field, the review of specialized literature and the analysis of cyber-attack reports has been employed. As a result, the frequent increase in cyber-attacks in Colombia leads to the need for an update of current security measures. In that case, the combination of Blockchain and artificial intelligence could be decisive thanks to their attributes that make them complementary to each other mainly in the field of health and financial movements.

Cybersecurity can be imagined as a shield protecting our critical infrastructures and data. Artificial intelligence is an astute guardian that can analyze a large amount of data and discover suspicious behaviors and patterns. As for Blockchain, it records all transactions and modifications of information. Therefore, the data is allowed to remain integral and confidential. The combination of blockchain and artificial intelligence can further leverage data defense. Artificial intelligence can make it possible to identify and prevent threats.

Las palabras clave: ciberseguridad, inteligencia artificial, Blockchain, protección de datos,

amenazas cibernéticas.

Keywords: Cybersecurity, artificial intelligence, Blockchain, data protection, cyber threats.

INTRODUCCIÓN

En el 2022, Colombia fue catalogado como el segundo país con más intentos de ataques informáticos a nivel de América Latina, esto a pesar de que los ataques de Ransomware (software malicioso) a nivel mundial disminuyeron considerablemente, el país CO fue listado como uno de los que fue contra la tendencia siendo blanco de muchos ciberdelincuentes. (Vega, 2023).

En el dinámico paisaje tecnológico contemporáneo, los avances en inteligencia artificial (aprendizaje automático)y Blockchain (cadena de bloques) están redefiniendo radicalmente la seguridad informática y la infraestructura digital, sin embargo, en medio de este panorama de innovación, las recientes alertas de IBM (Multinacional de desarrollo tecnológico) sobre el creciente número de ataques con credenciales válidas y la preocupante falta de seguridad básica en infraestructuras críticas arrojan luces sobre desafíos urgentes que enfrenta la comunidad tecnológica. (Danitza Moran, 2024)

De acuerdo con Grigera lopez enfatiza la necesidad de robustecer las medidas de protección en un ecosistema digital que no deja de evolucionar, el autor ilustra cómo la implementación de Blockchain puede potenciar la confidencialidad, integridad y disponibilidad de la información, características fundamentales para salvaguardar datos en el vasto dominio del ciberespacio. (Finck, M. (2018)

Las empresas deben mantenerse al día con diversas actualizaciones en ciberseguridad para protegerse contra amenazas emergentes y vulnerabilidades, esto incluye la instalación regular de parches de seguridad y actualizaciones de software y sistemas operativos, así como mantener todas las aplicaciones en sus versiones más recientes. Además, es esencial actualizar las bases de datos de virus y malware en las soluciones antivirus y antimalware, y utilizar herramientas de seguridad avanzadas. Los firewalls y sistemas de detección y prevención de intrusiones (IDS/IPS) deben tener sus configuraciones y firmware actualizados **Stallings, W.**

(2021) **FortiGuard Labs.** (2023). También es fundamental revisar y actualizar las políticas de seguridad, como las contraseñas y acceso, y proporcionar formación continua al personal sobre prácticas de ciberseguridad y cómo identificar amenazas. Divyanshu. (2019). La infraestructura de red, incluyendo routers y switches, debe actualizarse con las últimas versiones de firmware y ajustarse la segmentación de la red para limitar el alcance de posibles ataques.Enrique Alanis Hernández, (2024) las empresas deben asegurar que las copias de seguridad se realicen regularmente y se almacenan en ubicaciones seguras, y revisar y actualizar los planes de recuperación ante desastres para garantizar una respuesta rápida y efectiva a incidentes de seguridad. Marcos Velasco Magalhaes 2023 Implementar estas actualizaciones y mantener una postura proactiva en ciberseguridad ayuda a las empresas a proteger su información y minimizar el riesgo de ataques cibernéticos.Francisco Javier Bedecarratz Scholz 2021

Sin embargo, la convergencia de la inteligencia artificial (IA) y Blockchain ofrece nuevas oportunidades para las empresas al combinar la transparencia y seguridad de esta tecnología con la automatización y análisis avanzado de la IA. (Antonio, C. (2023), Esta Sociedad tiene el potencial de transformar diversas industrias, como la atención médica, las cadenas de suministro y los servicios financieros. (IBM, 2024) La inteligencia artificial ha aumentado su importancia, la medicina, las finanzas y el campo en general han experimentado su impacto. Salas-Pilco & Yang (2022) mencionan que la industria y el entretenimiento son derechos, se puede aprovechar la inteligencia artificial en el ámbito educativo para mejorar el rendimiento y aprendizaje de los estudiantes mediante diversas tecnologías como la realidad virtual, la realidad aumentada, los juegos, entre otras. La enseñanza personalizada es “La adaptación del currículo y los entornos de aprendizaje para satisfacer las necesidades y el aprendizaje de cada estudiante” (Rivero-Albarrán., 2019, p. 698). Esto asegura que al atender de manera específica

las particularidades de cada alumno, el proceso educativo sea más efectivo, lo que puede mejorar significativamente su rendimiento académico y su experiencia de aprendizaje. (Barrientos-Hernán, E. J., 2020)

Una forma de comprender estas dinámicas es a través de los modelos, ya que “un modelo representa propiedades o relaciones pertinentes de la realidad, copiando su naturaleza original. (Berryhill, J., 2019) Cuando nos referimos a estos elementos, estamos haciendo referencia tanto a las propiedades como a las relaciones de la realidad modelada "Ya que esto promueve la construcción colectiva de los participantes y contribuye a una comprensión y adaptación mejorada de los procesos de aprendizaje, también puede resultar en un aprendizaje más efectivo y personalizado”. (Ibáñez Bernal, 2007).

En el caso del sector salud, en donde la implementación de las IA (Inteligencia artificial) ha sido crucial en optimizar servicios y diagnósticos. Se debe tener en cuenta que también ha introducido riesgos de ciberseguridad, ya que los sistemas de salud, al almacenar datos sensibles, son objetivos para ciberdelincuentes, la tríada CIA (Confidencialidad, Integridad y Disponibilidad) es fundamental para abordar estos desafíos. (Díaz, L. L. (2022).
A pesar de que el aumento en el uso de tecnología genera un gran impacto positivo también conlleva riesgos significativos en términos de seguridad cibernética. (Zlata Drnas de Clément, 2022) La interconexión de dispositivos médicos, registros electrónicos de salud y sistemas de información hospitalaria crea una superficie de ataque expandida que requiere una protección sólida contra amenazas cibernéticas. (Greenleaf, G. (2021)

En el punto de vista de Alejandro Cervera García y Alyson Goussens, se nos da a entender que la importancia de la implementación de las tecnologías de la información en sectores de vital importancia como lo es la medicina, ha generado un impacto altamente positivo, sobre todo

hacen referencia a la inteligencia artificial como la herramienta que ha permitido que muchos procesos sean automatizados, generando así resultados óptimos en términos de tiempo de respuesta y sobre todo prioriza la seguridad de la información de los pacientes, pero como todas las implementaciones estas tienen sus desventajas y una de esas grandes desventajas es el hecho de que se pueden generar nuevas brechas de seguridad u oportunidad de ciberataques, los cuales al no darles la atención que se requiere pueden llegar a ser muy peligrosas. (Cano M., (2018). Desde una perspectiva ética, la ciberseguridad en salud es esencial, considerando principios como no maleficencia, beneficencia, autonomía y justicia.(Carlos Andrés Andino Acosta, 2015) Financiación, ética en negociaciones post-ciberataque y un modelo integral de ciberseguridad son clave.(Carlise Rigon Dalla Nora, 2021) La formación del personal, políticas sólidas, tecnologías avanzadas y conciencia emergen como fundamentales para abordar desafíos en la intersección de inteligencia artificial, blockchain y atención médica (Juan Guatavo Corvalán, 2017).

Según Diaz Marquez (2020) analiza la importancia de estas tecnologías disruptivas para generar sinergias que permitan sistemas más avanzados de estudio y análisis, facilitando la toma de decisiones en el ámbito de la salud además, se discuten aspectos éticos y de seguridad de la información relacionados con la manipulación masiva de datos de pacientes, destacando la necesidad de evaluar cuidadosamente el riesgo y el beneficio de estas tecnologías para garantizar la privacidad y los derechos de los individuos.(Díaz, J. E. M. (2020))

A pesar de su reciente llegada al país, la irrupción del Blockchain y la inteligencia artificial ha generado un impacto tecnológico a gran escala llevando las tecnologías a un nivel más allá, generando un crecimiento en el sector económico y social de manera positiva (MINTIC Colombia,2023)

I. MÉTODO

En este estudio sobre el impacto de la IA y Blockchain en la ciberseguridad, se utilizó una metodología mixta, donde se adopta el método PICO, comúnmente empleado en investigaciones médicas y tesis universitarias, sirvió para organizar estudios y recopilar datos pertinentes. Este método, que incluye preguntas precisas basadas en los componentes P (problema o paciente), I (Intervención), C (comparación) y O (resultados), facilitó la unificación de criterios de búsqueda y la obtención de respuestas específicas. La investigación se estructuró en varias etapas: formulación de la pregunta, búsqueda exhaustiva de referencias, selección de estudios relevantes, extracción y síntesis de datos, y evaluación crítica. Adicionalmente, se llevó a cabo una revisión documental y se contrastó la información mediante una encuesta web dirigida a profesionales de TI, permitiendo una estructuración sistemática y objetiva del estudio sobre la influencia de la IA y Blockchain en la ciberseguridad.

Fase 1: **Revisión documental**

Se lleva a cabo una revisión documental exhaustiva de artículos indexados (cielo, scopus redalyc, google academico, research GATE) publicaciones como El Tiempo, Kaspersky y MINTIC, y que siguiendo las directrices del portocolo PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) con el uso de terminos de busqueda relacionados al objeto de estudio identificaron patrones tendencias y laguna que proporcionaron una base sólida para entender las aplicaciones y desafíos de estas tecnologías emergentes la IA y Blockchain en el ámbito de la ciberseguridad.

Fase 2: Aplicación del instrumento

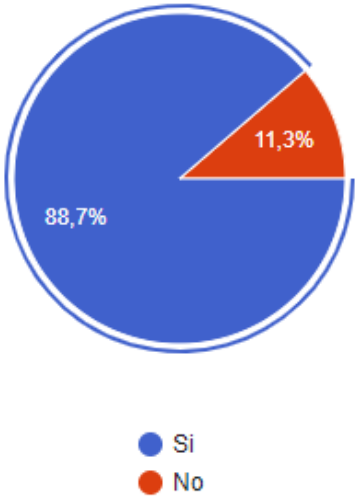
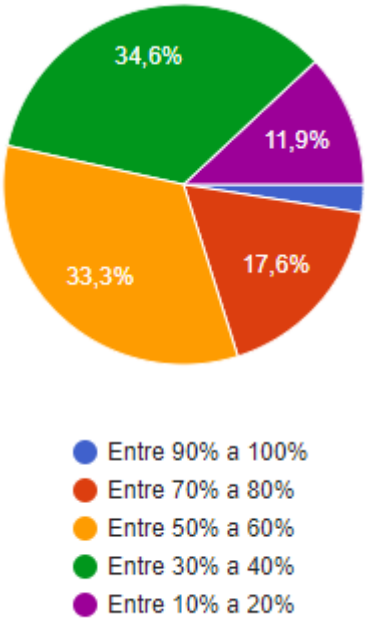
En la segunda fase del estudio, se procede a la implementación del instrumento de recolección de datos, en este caso, una encuesta diseñada para capturar las percepciones y experiencias de los participantes en relación con el tema de estudio. El instrumento fue validado previamente para asegurar su fiabilidad y consistencia interna. La encuesta se distribuyó electrónicamente a través de una plataforma en línea, dejando esta publicada en un rango de 20 dias , permitiendo un acceso amplio y eficiente a la muestra seleccionada.

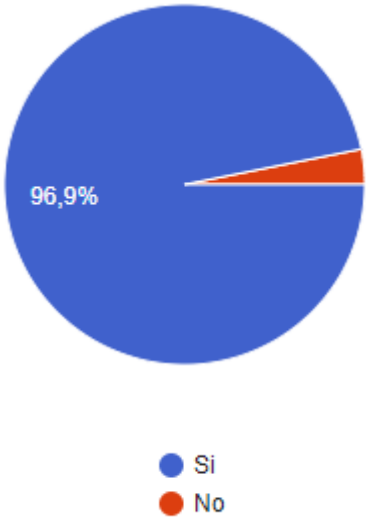
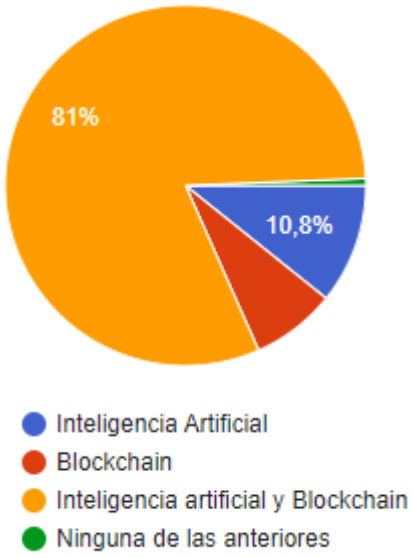
Fase 3: Análisis de resultados y emisión de juicios explicar

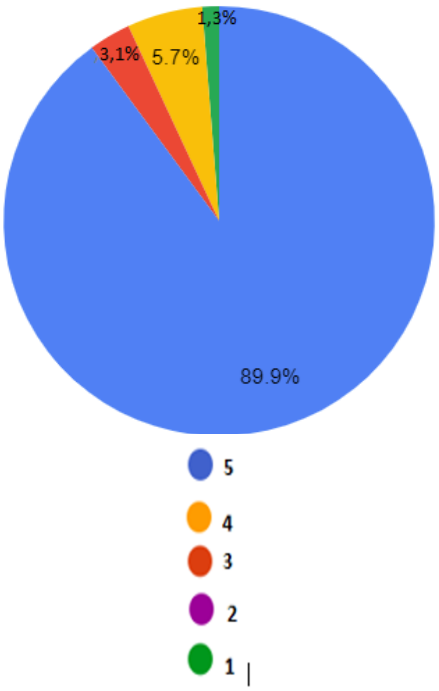
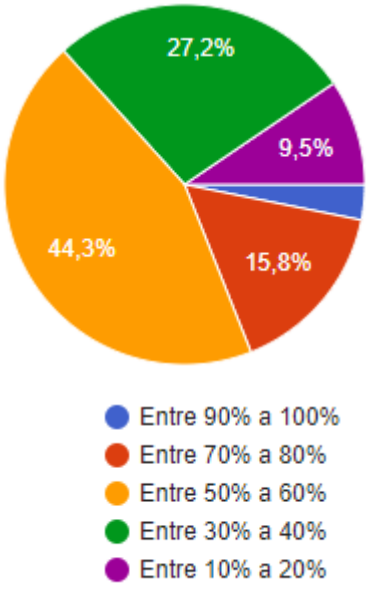
Se llevo a cabo u análisis detallado de los datos recolectados y se procesó a la emisión de juicios sobre los hallazgos de la investigación. Los datos obtenidos a la encuesta fueron sometidos a un proceso de análisis estadístico, estos resultados fueron presentados en forma de tablas y gráficos que facilitaron la visualización de las tendencias observadas al examinar hallazgos estadísticos, en paralelo los resultados de la revisión sistemática fueron sintetizados y contrastados con los datos empíricos de la encuesta, que permitió contextualizar los hallazgos dentro del cuerpo existente de literatura científica

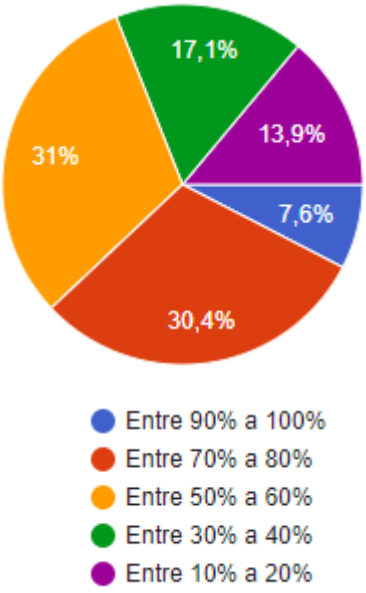
III RESULTADOS

Según las preguntas realizadas mediante la encuesta en el instrumento, la cual es referente a la investigación en curso en donde se las siguientes preguntas:

No	PREGUNTA	ANÁLISIS DE RESPUESTA	GRÁFICA
1	¿Tiene conocimiento sobre los ataques cibernéticos que afectan los sistemas de información?	La encuesta reveló que un 88.7% de los encuestados tiene conocimiento sobre los ataques cibernéticos. Este alto porcentaje sugiere una conciencia generalizada sobre los riesgos de ciberseguridad entre los usuarios de sistemas de información. Este nivel de conocimiento puede ser atribuido a capacitaciones en el trabajo, experiencias personales, y una creciente cobertura mediática de incidentes de ciberseguridad. Sin embargo, el 11.3% que no está informado representa un grupo vulnerable que necesita ser abordado con programas de educación y concienciación específicos para cerrar esta brecha de conocimiento. De igual forma consideramos que es crucial desarrollar e implementar programas de educación y concienciación en ciberseguridad dirigidos al 11.3% que carece de conocimiento. Políticas públicas y corporativas: Estos resultados pueden servir como base para diseñar políticas que fortalezcan la seguridad cibernética a nivel nacional y corporativo.	
2	¿Qué tan preparado cree que está el país para hacer frente a los desafíos actuales en materia de ciberseguridad?	Las percepciones sobre la preparación del país para enfrentar desafíos de ciberseguridad varían. Una mayoría significativa se inclina hacia una percepción positiva, sugiriendo confianza en la infraestructura y políticas de ciberseguridad del país. No obstante, hay un grupo que percibe que la preparación es insuficiente, indicando áreas que requieren mejora. Es esencial llevar a cabo evaluaciones regulares de la infraestructura y políticas de ciberseguridad del país para identificar y abordar áreas de mejora. Aumentar las inversiones en tecnología y capacitación puede mejorar la percepción y la realidad de la preparación del país en ciberseguridad.	

3	¿Cree usted que la Inteligencia Artificial y Blockchain pueden servir de apoyo para mejorar la seguridad de su empresa?	Un 96.9% de los encuestados cree que la implementación de tecnologías de Inteligencia Artificial (IA) y Blockchain puede mejorar la seguridad de sus empresas. Esta fuerte aceptación sugiere una tendencia hacia la adopción de estas tecnologías emergentes en el sector empresarial colombiano. Las empresas deben considerar la implementación de IA y Blockchain para fortalecer sus estrategias de ciberseguridad. La minoría que no está convencida de la eficacia de estas tecnologías necesita más información y capacitación para comprender sus beneficios.	
4	¿Qué tecnologías emergentes pueden servir de apoyo para mejorar la seguridad de la información en las organizaciones?	La mayoría de los encuestados (81%) considera que una combinación de IA y Blockchain es la mejor solución emergente para mejorar la seguridad de la información en las organizaciones. Esto refleja una fuerte confianza en la sinergia de estas tecnologías. Las organizaciones deben explorar y aprovechar la combinación de IA y Blockchain para mejorar sus medidas de seguridad.	

5	¿Qué tan importante considera usted la capacitación del personal en la prevención de ataques cibernéticos?	La capacitación del personal es vista como extremadamente importante por el 89.9% de los encuestados, indicando un consenso sobre la relevancia crítica de la educación en ciberseguridad para prevenir ataques. Las organizaciones deben implementar y mantener programas robustos de capacitación en ciberseguridad para todos los empleados. Fomentar una cultura de seguridad a través de la capacitación continua puede ayudar a mitigar riesgos cibernéticos.	
6	En relación con la capacidad de nuestro país para prevenir y mitigar los ataques cibernéticos, ¿Cuál de las siguientes opciones refleja mejor su opinión sobre la robustez de nuestra infraestructura actual?	Las opiniones sobre la robustez de la infraestructura de ciberseguridad del país varían, con una inclinación hacia un rango intermedio (50%-60%), lo que sugiere que aunque hay fortalezas, también existen debilidades que deben ser abordadas. Es crucial realizar mejoras continuas en la infraestructura de ciberseguridad, especialmente en áreas identificadas como vulnerables. Comparar la infraestructura con estándares internacionales puede proporcionar una guía para mejorar las capacidades de ciberseguridad.	

7	¿Qué tan preparada cree que está la empresa donde labora para hacer frente a un ataque cibernético?	Las respuestas indican una variabilidad en la preparación de las empresas para enfrentar ataques cibernéticos, con muchas empresas aún necesitando mejoras significativas en sus medidas de seguridad. Las empresas deben realizar evaluaciones de seguridad exhaustivas y regulares para identificar y remediar vulnerabilidades. Es necesario implementar mejores prácticas y seguir estándares reconocidos en ciberseguridad puede aumentar la preparación empresarial. La encuesta realizada muestra un panorama positivo en términos de conocimiento y conciencia sobre ciberseguridad entre la población TI en Colombia. Sin embargo, también revela áreas críticas que necesitan atención, como la educación continua, la mejora de infraestructuras y la adopción de tecnologías emergentes. Estos resultados pueden guiar el desarrollo de políticas públicas y estrategias corporativas para fortalecer la ciberseguridad en el país.	

Resultados de revisión sistemática

La convergencia de la inteligencia artificial (IA) y Blockchain ofrece nuevas oportunidades para las empresas al combinar la transparencia y seguridad de esta tecnología con la automatización y análisis avanzado de la IA (Antonio, C., 2023). Esta convergencia tiene el potencial de transformar diversas industrias, como la atención médica, las cadenas de suministro y los servicios financieros (IBM, 2024). La inteligencia artificial ha aumentado su importancia en la medicina, las finanzas y otros campos. Según Salas-Pilco & Yang (2022), la industria y el entretenimiento han experimentado su impacto. La IA puede mejorar el rendimiento y aprendizaje de los estudiantes mediante tecnologías como la realidad virtual, la realidad aumentada y los juegos (Rivero-Albarrán, 2019; Barrientos-Hernán, 2020). Los modelos representan propiedades o relaciones pertinentes de la realidad, promoviendo la

construcción colectiva y una comprensión mejorada de los procesos de aprendizaje (Berryhill, 2019; Ibáñez Bernal, 2007).

En el sector salud, la implementación de IA ha sido crucial para optimizar servicios y diagnósticos, pero también ha introducido riesgos de ciberseguridad, ya que los sistemas de salud, al almacenar datos sensibles, son objetivos para ciberdelincuentes. La tríada CIA (Confidencialidad, Integridad y Disponibilidad) es fundamental para abordar estos desafíos (Díaz, L. L., 2022). La interconexión de dispositivos médicos, registros electrónicos de salud y sistemas de información hospitalaria crea una superficie de ataque expandida que requiere una protección sólida contra amenazas cibernéticas (Greenleaf, 2021).

Según Alejandro Cervera García y Alyson Goussens, la implementación de tecnologías de la información en sectores como la medicina ha generado un impacto altamente positivo, automatizando procesos y priorizando la seguridad de la información de los pacientes. Sin embargo, esto también genera nuevas brechas de seguridad y oportunidades de ciberataques (Cano M., 2018). Desde una perspectiva ética, la ciberseguridad en salud es esencial, considerando principios como no maleficencia, beneficencia, autonomía y justicia (Carlos Andrés Andino Acosta, 2015). La financiación, la ética en negociaciones post-ciberataque y un modelo integral de ciberseguridad son clave (Carlise Rigon Dalla Nora, 2021). La formación del personal, políticas sólidas, tecnologías avanzadas y conciencia emergen como fundamentales para abordar desafíos en la intersección de inteligencia artificial, blockchain y atención médica (Juan Gustavo Corvalán, 2017).

A pesar de su reciente llegada al país, la irrupción del Blockchain y la inteligencia artificial ha generado un impacto tecnológico a gran escala, llevando las tecnologías a un nivel más allá y generando un crecimiento en el sector económico y social de manera positiva (MINTIC Colombia, 2023).

IV DISCUSIÓN

Los resultados preliminares de la investigación indican un alarmante aumento en la frecuencia y sofisticación de los ciberataques en Colombia y España. Estos países han experimentado un incremento significativo en las actividades maliciosas dirigidas a infraestructuras críticas y datos sensibles, lo que subraya la urgencia de actualizar y reforzar las medidas de seguridad existentes. Esta tendencia creciente de ciberataques puede atribuirse a varios factores, incluyendo la evolución de las técnicas de los atacantes y la expansión de la superficie de ataque debido al aumento de la digitalización.

La implementación de inteligencia artificial (IA) en ciberseguridad ha demostrado ser una herramienta valiosa para la detección y prevención de amenazas. Los encuestados en la investigación resaltaron la capacidad de la IA para analizar grandes volúmenes de datos en tiempo real, identificar patrones anómalos y predecir posibles ataques. Este análisis avanzado permite a las organizaciones reaccionar más rápidamente a las amenazas, reduciendo el tiempo de respuesta y mitigando el impacto potencial de los ataques. Además, la automatización proporcionada por la IA facilita una gestión más eficiente de los incidentes de seguridad, permitiendo a los equipos de ciberseguridad enfocarse en tareas más estratégicas.

Blockchain, por su parte, ofrece una solución robusta para garantizar la confidencialidad, integridad y trazabilidad de la información. Su estructura descentralizada y su capacidad para crear registros inmutables dificultan considerablemente la alteración de los datos, proporcionando una capa adicional de seguridad. Los encuestados destacaron que la combinación de IA y Blockchain puede resultar en una protección de datos significativamente

más fuerte, aprovechando las ventajas de ambas tecnologías para crear un sistema de seguridad más resiliente.

La encuesta también reveló que una gran mayoría de los profesionales en seguridad informática creen en el potencial de la combinación de IA y Blockchain para mejorar la seguridad cibernética. Sin embargo, también se identificaron desafíos en la adopción de estas tecnologías, incluyendo la necesidad de una mayor comprensión y capacitación sobre su uso efectivo, así como la inversión en infraestructura adecuada para soportarlas.

Aunque los resultados son prometedores, también se identificaron varios desafíos. La implementación de tecnologías avanzadas como IA y Blockchain requiere inversiones significativas en infraestructura y capacitación del personal. Además, la rápida evolución de las amenazas cibernéticas implica que las soluciones tecnológicas deben ser continuamente actualizadas y adaptadas. Por lo tanto, es crucial que las organizaciones no solo adopten estas tecnologías, sino que también implementen políticas de ciberseguridad sólidas y proporcionen formación continua a su personal para mantener la efectividad de las medidas de seguridad.

V CONCLUSIONES

- La investigación concluye que la implementación de tecnologías de IA y Blockchain en las estrategias de ciberseguridad puede transformar significativamente la protección de infraestructuras críticas y datos sensibles. Es crucial que las organizaciones desarrollen y mantengan una estrategia de ciberseguridad sólida y actualizada, que incluya la formación continua del personal y la implementación de políticas efectivas.
- La sinergia entre IA y Blockchain ofrece una defensa robusta y avanzada, adaptada a las necesidades de un entorno digital en constante evolución. Además, se destaca la necesidad de inversiones constantes en tecnologías emergentes y en la capacitación del personal para enfrentar eficazmente las amenazas cibernéticas actuales y futuras.
- La investigación destaca la necesidad crítica de integrar tecnologías avanzadas como la IA y Blockchain en las estrategias de ciberseguridad para enfrentar los crecientes desafíos en el ámbito digital. La combinación de estas tecnologías ofrece una solución prometedora para mejorar la protección de infraestructuras críticas y datos sensibles. Sin embargo, para maximizar su efectividad, es esencial abordar los desafíos de adopción y garantizar una formación continua del personal, junto con la implementación de políticas de seguridad robustas y actualizadas.

VI REFERENCIAS

- Quintero, L. N. (2023, 21 septiembre). Cómo chat GPT: Alexa de Amazon va a estar impulsada por inteligencia artificial. *El Tiempo*. https://www.eltiempo.com/tecnosfera/inteligencia-artificial-la-nueva-version-de-alexa-lanzada-por-amazon-808134
- Paola, D. B. J. (2023, 1 enero). *FULL investiga enero a junio de 2023 número 7*. https://repository.libertadores.edu.co/handle/11371/6054#:~:text=FULL%20Investiga%20Enero%20a%20Junio%20de%202023%20N%C3%BAmero%207
- *5 famosas empresas que usan la tecnología blockchain (ejemplos reales)*. (s. f.). https://www.conquerx.com/post/5-famosas-empresas-que-usan-la-tecnologia-blockchain
- *¿Qué son los NFT y cómo funcionan?* (2023, 19 abril). latam.kaspersky.com. https://latam.kaspersky.com/resource-center/definitions/what-is-an-nft
- Vega, W. (2023, 2 marzo). Colombia, el segundo país de América Latina con más ciberataques en 2022, según IBM. Xataka Colombia. https://www.xataka.com.co/seguridad/colombia-segundo-pais-america-latina-ciberataques-2022-ibm
- Eset. (2023). ESET THREAT REPORT. https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset-threat-report-h22023

- Díaz, L. L. (2022, diciembre 4). *Keralty, la nueva víctima de los ataques de 'ransomware'*. El Tiempo. https://www.eltiempo.com/tecnosfera/novedades-tecnologia/keralty-detalles-del-ataque-de-ransomware-a-eps-sanitas-723175
- MINTIC Colombia. Recuperado 12 de marzo de 2024, de https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/327002:La-tecnologia-blockchain-llega-para-innovar-la-seguridad-y-eficiencia-de-los-procesos-gubernamentales-y-el-sector-empresarial
- Blockchain e inteligencia artificial (IA). (s. f.). Ibm.com. Recuperado 11 de marzo de 2024, de https://www.ibm.com/es-es/topics/blockchain-ai
- García, A. C., & Goussens, A. (diciembre 2023). Ciberseguridad y uso de las TIC en el Sector Salud. ELSEVIER, 56(2024), 7. https://www.elsevier.es/es-revista-atencion-primaria-27-articulo-ciberseguridad-uso-tic-el-sector-S0212656723002871
- Ciberseguridad y Blockchain. (2022). *Revista Blockchain E Inteligencia Artificial*, *3*. https://doi.org/10.22529/rbia.2021(3)05
- Márquez Díaz, J. (2020). Inteligencia artificial y Big Data como soluciones frente a la COVID-19. *Revista de Bioetica y Derecho*, *50*, 315–331. https://scielo.isciii.es/scielo.php?pid=S1886-58872020000300019&script=sci_arttext

- Ciberseguridad y Blockchain. (2022). *Revista Blockchain E Inteligencia Artificial*, *3*. https://doi.org/10.22529/rbia.2021(3)05

- Díaz, L. L. (2022, 5 diciembre). Keralty, la nueva víctima de los ataques de 'ransomware'. *El Tiempo*. https://www.eltiempo.com/tecnosfera/novedades-tecnologia/keralty-detalles-del-ataque-de-ransomware-a-eps-sanitas-723175

- Parra-Sánchez, J. (2022). Potencialidades de la Inteligencia Artificial en Educación Superior: Un Enfoque desde la Personalización. Revista Tecnológica Educativa Docentes 2.0, 14(1), 19-27. https://doi.org/10.37843/rted.v14i1.296
- Graciela Maribel Fajardo Aguilar Diana Catalina Ayala Gavilanes Edison Manuel Arroba Freire Martha López Quincha (Ed.). (2023). January 2023 Magazine de las Ciencias Revista de Investigación e Innovación. https://www.researchgate.net/publication/373010274_Inteligencia_Artificial_y_la_Educacion_Universitaria_Una_revision_sistematica
- Valle, M. (2023, marzo 24). *Josep Albors sobre el auge del phishing: "los delincuentes están usando inteligencia artificial para generar mensajes más convincentes"*. Bit Life Media. https://bitlifemedia.com/2023/03/josep-albors-sobre-el-auge-del-phishing-los-delincuentes-estan-usando-inteligencia-artificial-para-generar-mensajes-mas-convincentes/
- Pablo-Martí, Federico & Mir Fernández, Carlos. (2024). Enseñando economía con inteligencia artificial. Una propuesta para dinamizar las aulas de la Generación Z, DOI:10.13140/RG.2.2.23320.16649
- Berryhill, J., et al. (2019), "Hello, World: Artificial intelligence and its use in the public sector", *OECD Working Papers on Public Governance*, No. 36, OECD Publishing, Paris, https://doi.org/10.1787/726fd39d-en.
- Inteligencia artificial en el Derecho Internacional, Naciones Unidas y Unión Europea. (2022). *Revista Estudios Jurídicos. Segunda Época*, *22*. https://doi.org/10.17561/rej.n22.7524
- PESQUISA • Rev. Bioét. 29 (2) • Apr-Jun 2021, https://doi.org/10.1590/1983-80422021292468

- Finck, M. (2018). Blockchains: Regulating the Unknown. *German Law Journal*, *19*(4), 665–692. doi:10.1017/S2071832200022847
- Barrientos-Hernán, E. J., López-Pastor, V. M., & Pérez-Brunicardi, D. (2020). Evaluación Auténtica y Evaluación Orientada al Aprendizaje en Educación Superior. Una Revisión en Bases de Datos Internacionales. *Revista Iberoamericana De Evaluación Educativa*, *13*(2), 67–83. https://doi.org/10.15366/riee2020.13.2.004
- Greenleaf, Graham, Global Tables of Data Privacy Laws and Bills (7th Ed, January 2021) (February 11, 2021). (2021) 169 Privacy Laws & Business International Report. 6-19, Available at SSRN: https://ssrn.com/abstract=3836261 or http://dx.doi.org/10.2139/ssrn.3836261 .
- Cano M., Jeimy. (2018). Seguridad y Ciberseguridad en los dispositivos médicos. 149. 55-67. 10.29236/sistemas.n149a7.
- JUAN GUSTAVO CORVALÁN,2017, Artificial intelligence: challenges and opportunities - Prometea: the first artificial intelligence of Latin America at the service of the Justice System, https://doi.org/10.5380/rinc.v5i1.55334.
- Andino Acosta, C. A. (2015). Bioética y humanización de los servicios asistenciales en la salud. *Revista Colombiana De Bioética*, *10*(1), 38–64. https://doi.org/10.18270/rcb.v10i1.684
- Díaz, J. E. M., Saldaña, C. A. D., & Ávila, C. A. R. (2020). Virtual World as a Resource for Hybrid Education. *International Journal of Emerging Technologies in Learning (iJET)*, *15*(15), pp. 94–109. https://doi.org/10.3991/ijet.v15i15.13025
- La tecnología blockchain llega para innovar la seguridad y eficiencia de los procesos gubernamentales y el sector empresarial - La tecnología blockchain

llega para innovar la seguridad y eficiencia de los procesos gubernamentales y el sector empresarial. (s/f). MINTIC Colombia. Recuperado el 17 de julio de 2024, de https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/327002:La-tecnologia-blockchain-llega-para-innovar-la-seguridad-y-eficiencia-de-los-procesos-gubernamentales-y-el-sector-empresarial

- Bedecarratz Scholz, F. J. (2018). Riesgos delictivos de las monedas virtuales: Nuevos desafíos para el derecho penal. *Revista Chilena De Derecho Y Tecnología*, *7*(1), 79–105. https://doi.org/10.5354/0719-2584.2018.48515
- Aguilar Antonio, Juan Manuel. (2021). Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior. *Estudios internacionales (Santiago)*, *53*(198), 169-197. https://dx.doi.org/10.5354/0719-3769.2021.57067
- Bedecarratz Scholz, Francisco. (2018). Riesgos delictivos de las monedas virtuales: Nuevos desafíos para el derecho penal. *Revista chilena de derecho y tecnología*, *7*(1), 79-105. https://dx.doi.org/10.5354/0719-2584.2018.48515