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

Jesús Herney Fuenmayor Tobar[1]
Derly Katherine Torres Lozano[1]
Leydy Dayana Monsalve Pérez[1]
Anyi Marcela Becerra Moreno[1]

Resumen

En la era de la información existe un desafío latente para las organizaciones y quienes quieren mantenerse a la vanguardia en la optimización de sus servicios y controles, sobre todo en el campo de la ciberseguridad, a causa del aumento de delitos a infraestructuras informáticas, lo cual ha afectado a la ciudadanía y sus organizaciones. Por tanto, el propósito de este estudio es analizar los efectos que la inteligencia artificial (IA) y el *blockchain* (cadena de bloques) 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. El frecuente aumento en los ciberataques en Colombia obliga a una actualización de las medidas de seguridad actuales. En ese caso, la combinación de *blockchain* y la inteligencia artificial podrían ser decisivas gracias a los atributos que las hacen complementarias entre sí, 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

1 Estudiantes de la Fundación Universitaria del Área Andina.

sospechosos. En cuanto a *blockchain*, graba todas las transacciones y modificaciones de la información. Por consiguiente, se permite que los datos sean íntegros y confidenciales. La combinación de *blockchain* e inteligencia artificial puede beneficiar aún más la defensa de datos. La inteligencia artificial puede hacer posible la identificación y prevención de las amenazas.

Palabras clave: amenazas cibernéticas, *blockchain*, ciberseguridad, inteligencia artificial, protección de datos.

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.

Keywords: artificial intelligence, blockchain, cybersecurity, cyber threats, data protection,

Introducción

En el 2022, Colombia fue catalogado como el segundo país con más intentos de ataques informáticos en América Latina, a pesar de que los ataques de *ransomware* (*software* malicioso) en todo el mundo disminuyeron de forma considerable. Así, 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* están redefiniendo de forma radical 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 (Infobae, 2024).

Grigera (2022) subraya 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, 2018).

Las empresas deben mantenerse al día con diversas actualizaciones en ciberseguridad para protegerse de amenazas emergentes y vulnerabilidades; tal protección incluye la instalación regular de parches de seguridad y actualizaciones de *software* y sistemas operativos, y 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 (Gómez *et al*., 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 (Yadav *et al*., 2019). La infraestructura de red, incluso *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 (Hassani, 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 , 2023) (Velasco, 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 (Bedecarratz, 2018).

No obstante, la convergencia de la IA y el *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 (Aguilar-Antonio, 2021). Esta sociedad tiene el potencial de transformar diversas industrias, como la atención médica, las cadenas de suministro y los servicios financieros (AbdelSalam, 2023). La IA ha aumentado su importancia; la medicina, las finanzas y el campo en general han experimentado la influencia de esta. Salas-Pilco y 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 y los juegos, entre otras (Díaz *et al*., 2020). La enseñanza personalizada es "[l]a 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 de manera significativa su rendimiento académico y su experiencia de aprendizaje (Barrientos-Hernán *et al*., 2020).

Una forma de comprender estas dinámicas es mediante modelos, ya que un modelo representa propiedades o relaciones pertinentes de la realidad, copiando su naturaleza original (Berryhill *et al*., 2019,) Cuando nos referimos a estos elementos, aludimos tanto a las propiedades como a las relaciones de la realidad modelada, "[y]a 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" (Manrique-Villavicencio, 2003, p. 8).

En el caso del sector salud, en el que la implementación de la IA ha sido crucial en optimizar servicios y

diagnósticos, se debe tener en cuenta que también esta ha introducido riesgos de ciberseguridad, ya que los sistemas de salud, al almacenar datos sensibles, son objetivos de ciberdelincuentes; así pues, la tríada CIA (confidencialidad, integridad y disponibilidad) es fundamental para abordar estos desafíos (Díaz, 2022).

A pesar de que el aumento en el uso de tecnología genera un gran efecto positivo, también implica riesgos significativos desde el punto de vista de seguridad cibernética (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, 2021).

De acuerdo con Cervera-García y Goussens (2024), la importancia de la implementación de las tecnologías de la información en sectores de vital importancia, como el de la medicina, ha generado un efecto extremadamente positivo. Hacen referencia sobre todo a la IA como la herramienta que ha permitido que muchos procesos sean automatizados, lo cual trae resultados óptimos a partir 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, una de la cuales 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, 2018).

Desde una perspectiva ética, la ciberseguridad en salud es esencial, si se consideran principios como no maleficencia, beneficencia, autonomía y justicia (Andino-Acosta, 2015). Financiación, ética en negociaciones posciberataque y un modelo integral de ciberseguridad son clave (Carlise y Roque, 2021). La formación del personal, políticas sólidas, tecnologías avanzadas y conciencia emergen como fundamentales para abordar desafíos en la intersección de IA, *blockchain* y atención médica (Corvalán, 2017).

Díaz *et al*. (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, entre los que destacan la necesidad de evaluar de forma cuidadosa el riesgo y

el beneficio de estas tecnologías para garantizar la privacidad y los derechos de los individuos.

A pesar de su reciente llegada al país, la irrupción del *blockchain* y la IA ha causado un efecto tecnológico a gran escala, al llevar las tecnologías a un nivel más allá y producir un crecimiento positivo en el sector económico y social (Muñoz, 2023).

Método

En este estudio sobre el efecto de la IA y *blockchain* en la ciberseguridad se utilizó una metodología mixta en la que se adoptó el método PICO, que se emplea con frecuencia en investigaciones médicas y tesis universitarias y que sirvió para organizar estudios y recopilar datos pertinentes. Este método, que incluye preguntas precisas a partir de 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. Además, se llevó a cabo una revisión documental y se contrastó la información mediante una encuesta web dirigida a profesionales en tecnología de la información (TI), lo cual permitió una estructuración sistemática y objetiva del estudio sobre la influencia de la IA y *blockchain* en la ciberseguridad.

Fase 1: revisión documental

Se llevó a cabo una revisión documental exhaustiva de artículos indexados (Cielo, Scopus Redalyc, Google Academico, Research GATE), publicaciones como *El Tiempo*, Kaspersky y MINTIC, y siguiendo las directrices del portocolo PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) con el uso de términos de búsqueda relacionados con el objeto de estudio, identificaron patrones, tendencias y lagunas 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 procedió a implementar el instrumento de recolección de datos, en este caso, una encuesta diseñada para capturar las percepciones y experiencias de los

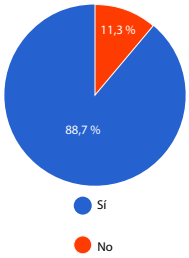
participantes respecto del tema de estudio. El instrumento se validó antes para asegurar su fiabilidad y consistencia interna. La encuesta se distribuyó de manera electrónica en una plataforma en línea, que se publicó en un lapso de veinte días, lo cual permitió un acceso amplio y eficiente a la muestra seleccionada.

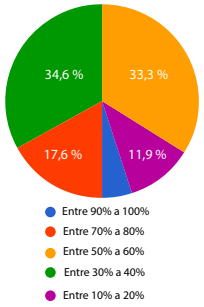
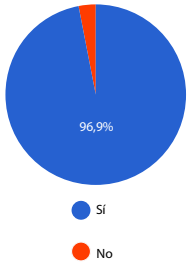
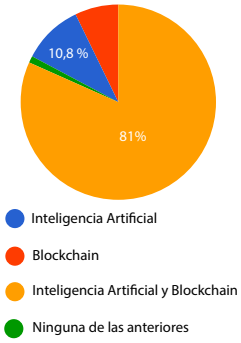
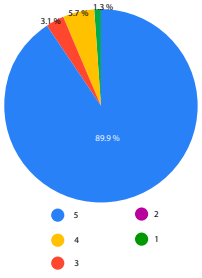
Fase 3: análisis de resultados y emisión de juicios

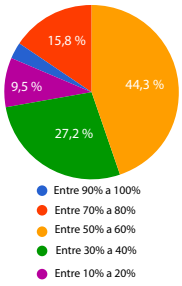
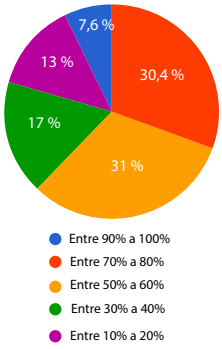
Se llevó a cabo u análisis detallado de los datos recolectados y se procesó la emisión de juicios sobre los hallazgos de la investigación. Los datos obtenidos en la encuesta se sometieron a un proceso de análisis estadístico. Estos resultados se presentaron en forma de tablas y gráficos que facilitaron la visualización de las tendencias observadas al examinar hallazgos estadísticos. De forma paralela, los resultados de la revisión sistemática se sintetizaron y contrastaron con los datos empíricos de la encuesta, lo que permitió contextualizar los hallazgos dentro del cuerpo que ya existía de literatura científica.

Resultados

A partir de las preguntas realizadas mediante la encuesta en el instrumento, la cual se refiere a la investigación en curso, se obtuvieron las siguientes preguntas:

N.º	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 atribuirse 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 nacional y corporativa.	

N.º	Pregunta	Análisis de respuesta	Gráfica
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 e indica 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 el *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 IA y *blockchain* puede mejorar la seguridad de sus empresas. Esta gran 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 enorme 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 la ve en extremo importante el 89,9 % de los encuestados, lo cual indica 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 mediante la capacitación continua puede ayudar a mitigar riesgos cibernéticos.	

N.º	Pregunta	Análisis de respuesta	Gráfica
6	En lo que se refiere a 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 abordarse. Es crucial realizar mejoras continuas en la infraestructura de ciberseguridad, sobre todo 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 en la que usted trabaja para enfrentar un ataque cibernético?	Las respuestas indican una variabilidad en la preparación de las empresas para enfrentar ataques cibernéticos, con muchas empresas que aún necesitan 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 desde el punto de vista de conocimiento y conciencia sobre ciberseguridad entre la población TI en Colombia. Pero 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 la *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 (Muñoz, 2023). Esta convergencia tiene el potencial de transformar diversas industrias, como la atención médica, las cadenas de suministro y los servicios financieros La inteligencia artificial ha aumentado su importancia en la medicina, las finanzas y otros campos. Según Salas-Pilco y Yang (2022), la industria y el entretenimiento han experimentado la influencia de la IA. Esta puede mejorar el rendimiento y aprendizaje de los estudiantes mediante tecnologías como la realidad virtual, la realidad aumentada y los

juegos (Barrientos-Hernán *et al*., 2020; Rivero-Albarrán, 2019). Los modelos representan propiedades o relaciones pertinentes de la realidad, promoviendo la construcción colectiva y una comprensión mejorada de los procesos de aprendizaje (Berryhill *et al*., 2019).

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 de ciberdelincuentes. La tríada CIA (confidencialidad, integridad y disponibilidad) es fundamental para abordar estos desafíos (Díaz, 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 Cervera-García y Goussens (2024), la implementación de tecnologías de la información en sectores como la medicina ha generado un efecto muy 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, 2018). Desde una perspectiva ética, la ciberseguridad en salud es esencial, considerando principios como no maleficencia, beneficencia, autonomía y justicia (Andino-Acosta, 2015). La financiación, la ética en negociaciones posciberataque y un modelo integral de ciberseguridad son clave (Carlise y Roque, 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 (Corvalán, 2017).

A pesar de su reciente llegada al país, la irrupción de la *blockchain* y la inteligencia artificial ha generado un efecto 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 (Alide, 2022).

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, que incluyen la evolución de las técnicas de los atacantes y la expansión de la superficie de ataque por el aumento de la digitalización.

La implementación de IA en ciberseguridad ha demostrado ser una herramienta valiosa para la detección y prevención de amenazas. Los encuestados en la investigación señalaron 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 con más rapidez a las amenazas, reduciendo el tiempo de respuesta y mitigando el efecto 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 de forma considerable la alteración de los datos, proporcionando una capa adicional de seguridad. Los encuestados subrayaron que la combinación de IA y *blockchain* puede dar como resultado 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 la 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, que incluyen 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 actualizarse y adaptarse de forma continua. Por

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.

Conclusiones

- La investigación concluye que la implementación de tecnologías de IA y *blockchain* en las estrategias de ciberseguridad puede transformar de manera significativa 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, resalta la necesidad de inversiones constantes en tecnologías emergentes y en la capacitación del personal para enfrentar con eficacia las amenazas cibernéticas actuales y futuras.
- La investigación subraya 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. Aun así, para maximizar su efectividad es esencial abordar los desafíos de adopción y garantizar una formación continua del personal e implementar también políticas de seguridad robustas y actualizadas.

Referencias

AbdelSalam, F. (2023). *Blockchain Revolutionizing Healthcare Industry: A Systematic Review of Blockchain Technology Benefits and Threats. Perspect Health Inf Manag*. https://pmc.ncbi.nlm.nih.gov/articles/PMC10701638/

Aguilar-Antonio, J. M. (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://doi.org/10.5354/0719-3769.2021.57067

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

Asociación Latinoamericana de Instituciones Financieras para el Desarrollo (Alide). (2022). *Estudio básico Alide 52: La banca de desarrollo y la transformación digital*. Alide.

Barrientos-Hernán, E. J., López-Pastor, V. M., y 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

Bedecarratz, F. (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

Berryhill, A., Heang, K., Clogher, R y McBride, K. *et al*. (2019). Hello, World: Artificial intelligence and its use in the public sector. *OECD Working Papers on Public Governance* 36, OECD Publishing. https://doi.org/10.1787/726fd39d-en.

Carlise, N. y Roque, J. (2021). *Seguridad del paciente y aspectos éticos: revisión de alcance. Bioética, 29*(2). 304-316. https://doi.org/10.1590/1983-80422021292468

Cano M., J. (2018). Seguridad y ciberseguridad en los dispositivos médicos. *Sistemas, 149*. 55-67. https://doi.org/10.29236/sistemas.n149a7

Cervera-García, A., y Goussens, A. (2024). Ciberseguridad y uso de las TIC en el sector salud. *Atención Primaria*, *56*(3), 102854. https://doi.org/10.1016/j.aprim.2023.102854

Corvalán, J. G. (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.

Díaz, L. L. (2022, 5 de 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

Drnas de Clément, Z. (2022). Inteligencia artificial en el derecho Internacional, Naciones Unidas y Unión Europea. *Estudios Jurídicos. Segunda Época*, *22*. https://doi.org/10.17561/rej.n22.7524

Díaz, J., Saldaña, C., & Ávila. (2020). Virtual World as a Resource for Hybrid Education. *International Journal of Emerging Technologies in Learning (iJET)*, *15*(15), 94-109. https://doi.org/10.3991/ijet.v15i15.13025

Finck, M. (2018). Blockchains: Regulating the Unknown. *German Law Journal*, *19*(4), 665-692. https://doi.org/10.1017/S2071832200022847

Gómez, J., Castaño, N., y Correa, L. (2023). Sistemas de detección y prevención de intrusos: una taxonomía experimental basada en código abierto orientada a la industria 4.0*. *Ciencia e Ingeniería Neogranadina, 33*(1), 75-86. https://doi.org/10.18359/rcin.6534

Greenleaf, G. (2021). Global Tables of Data Privacy Laws and Bills (7th Ed, January 2021) (February 11, 2021*). 169 Privacy Laws & Business International Report*, 6-19. https://ssrn.com/abstract=3836261 or http://dx.doi.org/10.2139/ssrn.3836261 .

Grigera del Campillo. S. (2022). Ciberseguridad y Blockchain. *Blockchain e Inteligencia Artificial*, *2*(3). https://doi.org/10.22529/rbia.2021(3)05

Hassani, H. (2024). A Comprehensive Survey on Cybersecurity Threats, Attacks, and Countermeasures. *Electronics, 13*(13), 2499. https://doi.org/10.3390/electronics13132499

Infobae (2024, 21 de febrero). *IBM alerta del aumento de ataques con credenciales válidas y la falta de seguridad básica en infraestructuras críticas*. https://www.infobae.com/america/agencias/2024/02/21/ibm-alerta-del-aumento-de-ataques-con-credenciales-validas-y-la-falta-de-seguridad-basica-en-infraestructuras-criticas/ Primera

López, Y (s. f.). 5 famosas empresas que usan la tecnología blockchain. *conquerblocks*. https://www.conquerblocks.com/post/5-famosas-empresas-que-usan-la-tecnologia-blockchain

Manrique-Villavicencio, L. (2003). *El aprendizaje autónomo en la educación a distancia.* Pontificia Universidad Católica del Perú. https://files.pucp.education/departamento/educacion/2020/02/21174038/lileya-manrique-el-aprendizaje-autonomo-en-la-educacion-a-distancia.pdf

Muñoz, O. (2023, enero-junio). La inteligencia artificial (IA) y la tecnología *blockchain* como grandes innovaciones del siglo XXI. *FULL investiga, 36-41.* https://repository.libertadores.edu.co/items/50f71145-89a0-48ef-a2e8-fceb2de6f696

Rivero-Albarrán, D. (2019). Adaptive agent for teaching in intelligent environments. *RISTI : Revista Ibérica de Sistemas e Tecnologias de Informação*, *2019*(19), 694-707.

Salas-Pilco, S., & Yang, Y. (2022). Artificial intelligence applications in Latin American higher education: a systematic review. *Int. J. Educ Technol High Educ.,* 19, 21. https://doi.org/10.1186/s41239-022-00326-w

Vega, W. (2023, 2 de 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

Velasco-Magalhaes, M. (2023). *El presente y futuro de la tecnología Blockchain y su potencial en el almacenamiento en la nube*. [Trabajo de grado Ingeniería Informática, Universidad Politécnica de Madrid]. Archivo digital UPM. https://oa.upm.es/75434/.

Yadav, R., Kashyap, G., Kumawat, A., & Sharma, D. (2019). Cybersecurity: Protecting Networks, Systems, and Data from Cyberattacks. *Turkish Journal of Computer and Mathematics Education (Turcomat)*, *10*(3), 1565-1568. https://doi.org/10.61841/turcomat.v10i3.14395