Management (Montevideo). 2025; 3:116
doi: 10.62486/agma2025116
ISSN: 3046-4048

REVISIÓN

AI and cybersecurity, business protection in an interconnected world: systematic literature review

IA y ciberseguridad, protección empresarial en un mundo interconectado: revisión sistemática de literatura

Iris María Cantillo Velásquez[1], Jhon Wolfgang Echeverry David[1], Yerlis Patricia Martínez Taborda[1], Rubén Santiago Ramírez Piraquive[1]

[1]Corporación Unificada Nacional de Educación Superior. Bogotá, Colombia.

Citar como: Cantillo Velásquez IM, Echeverry David JW, Martínez Taborda YP, Ramírez Piraquive RS. AI and cybersecurity, business protection in an interconnected world: systematic literature review. Management (Montevideo).2025; 3:116. https://doi.org/10.62486/agma2025116

Recibido: 18-02-2024 **Revisado:** 10-06-2024 **Aceptado:** 04-10-2024 **Publicado:** 01-01-2025

Editor: Misael Ron

ABSTRACT

In an increasingly interconnected world, cyber threats are constantly evolving, with malicious actors developing sophisticated methods to attack enterprise systems. Traditional cybersecurity methods, such as firewalls and antivirus software, are insufficient to protect organizations from these advanced threats. A more proactive approach is needed to identify and stop threats before they cause significant damage. This research seeks to understand the current state of artificial intelligence (AI) in enterprise cybersecurity, identify best practices and methodologies for implementing effective AI solutions. To do this, the authors were based on a systematic review of the literature, adopting AI, cybersecurity, business protection and threats as fundamental categories. The search was mainly based on databases and search engines such as Scopus, Science Direct and Redalyc. The processed information was graphed through the VOSviewer software and the Lens.org platform. The usefulness and applications of AI for cybersecurity were evident. This entails the challenge of constantly updating cyber tools in order to achieve greater protection and security for users.

Keywords: Cyber Threats; Cybersecurity; Artificial Intelligence; Business Protection; Cyber Resilience; Business Systems.

RESUMEN

En un mundo cada vez más interconectado, las amenazas cibernéticas evolucionan constantemente, con actores maliciosos que desarrollan métodos sofisticados para atacar sistemas empresariales. Los métodos tradicionales de ciberseguridad, como los firewalls y el software antivirus, son insuficientes para proteger a las organizaciones de estas amenazas avanzadas. Es necesario adoptar un enfoque más proactivo que identifique y detenga las amenazas antes de que causen daños significativos. Esta investigación busca comprender el estado actual de la inteligencia artificial (IA) en la ciberseguridad empresarial, identificar las mejores prácticas y metodologías para implementar soluciones de IA efectivas. Para ello los autores se basaron en una revisión sistemática a la literatura, adoptaron como categorías fundamentales la IA, ciberseguridad, protección empresarial y amenazas. La búsqueda se basó fundamentalmente en bases de datos y buscadores como Scopus, Science Direct y Redalyc. La información procesada se graficó a través del software VOSviewer y la plataforma Lens.org. Se evidenció la utilidad y aplicaciones de la IA para la ciberseguridad. Ello conlleva el reto de actualizar de forma constante las herramientas cibernéticas con el fin de lograr mayor protección y seguridad a los usuarios.

Palabras clave: Amenazas Cibernéticas; Ciberseguridad; Inteligencia Artificial; Protección Empresarial; Resiliencia Cibernética; Sistemas Empresariales.

INTRODUCCIÓN

En la era digital actual, las empresas enfrentan un panorama de amenazas cibernéticas cada vez más complejo.[1,2,3,4,5,6,7,8] Se exponen a riesgos significativos como pérdidas financieras, daños a la reputación e interrupciones operativas. La sofisticación creciente de los ataques cibernéticos ha superado la capacidad de los métodos tradicionales de ciberseguridad, como los firewalls y el software antivirus, para proteger eficazmente los sistemas empresariales. Esto destaca la necesidad de adoptar enfoques más proactivos y avanzados en el sector de los negocios y empresas.[9,10,11,12,13,14,15,16]

Un desafío crucial es la escasez de recursos y personal capacitado en ciberseguridad, lo que limita la capacidad de las organizaciones para defenderse adecuadamente.[17,18,19] Además, la integración de tecnologías emergentes, como la computación en la nube y el Internet de las Cosas (IoT) aumenta la vulnerabilidad y requiere estrategias de seguridad específicas. La detección tardía de intrusiones y la falta de sistemas de monitoreo efectivos agravan estos problemas, comprometen la capacidad de recuperación y continuidad del negocio.

La inteligencia artificial (IA) ofrece una solución prometedora, capaz de analizar grandes volúmenes de datos para detectar patrones de amenazas, automatizar respuestas a incidentes y explorar en diferentes áreas que permitan dinamizar procesos comerciales, sociales, de salud, económicos, urbanísticos, educativos, entre otros.[20,21,22,23,24]

No obstante, la implementación efectiva de IA en ciberseguridad exige una comprensión profunda de las mejores prácticas y la superación de barreras técnicas y éticas.

En este artículo se revisa sistemáticamente la literatura sobre el uso de IA en ciberseguridad empresarial,[25,26,27] se exploraron aplicaciones prácticas en las funciones de identificar, proteger, detectar, responder y recuperar. Al analizar oportunidades y desafíos, se pretende proporcionar una guía para investigadores, profesionales y decisores, a la vez que se facilita la adopción de tecnologías de IA para fortalecer la seguridad empresarial.

MÉTODO

Este artículo presenta una revisión sistemática sobre la IA para la ciberseguridad en conjunto de otras revisiones literarias que sirvieron como base a este estudio.[28,29,30,31,32,33,34,35,36,37,38] Además, se consultaron varios artículos con metodologías basadas en análisis bibliométricos como modelo a la presente investigación.[39,40] Para el desarrollo de la metodología, se llevaron a cabo las siguientes fases. En primera instancia, se realizó una investigación exhaustiva referente al tema "IA para la ciberseguridad", se utilizaron las bases de datos académicas como: Scopus, Science Direct y Redalyc, con un periodo de análisis comprendido entre 2019-2024.

Luego se realizó proceso de filtrado y exclusiones para analizar el contenido enfocados en la identificación de patrones temáticos en cuanto a IA para la ciberseguridad. Este procedimiento radicó en filtrar las siguientes áreas: ingeniería, computación, ciencias de la información y administración y contabilidad. Los resultados de esta fase se representaron de manera gráfica, lo cual evidencia el número de artículos encontrados en las diferentes subáreas de estudios.

Como tercera fase, se seleccionaron algunos artículos relacionados con la temática, se revisó y analizó su contenido, y de esta manera se pudo presentar discusiones de los resultados al tener en cuenta que estas revisiones sistemáticas son importantes porque facilitan información detallada del tema. El proceso fue una secuencia de pasos que incluyen la planeación y la búsqueda de la información.

Al buscar las fuentes relevantes en las bases de datos seleccionadas, se utilizaron palabras clave flexibles y relevantes y operadores booleanos para formular cadenas de búsqueda. La combinación de palabras clave se realizó de tal manera que se centrara en el interés de la investigación. Se realizó un análisis de los principales temas identificados, el cual estuvo compuesto por el total de publicaciones que se visualizan gráficamente. Se encontraron 24842 artículos en la base de datos Redalyc, 4345 en Science Direct y 194 en Scopus. Posteriormente, a partir de los artículos hallados, se analizaron y se plantearon discusiones del contexto de la IA en la ciberseguridad empresarial, se identificaron ventajas, desventajas, oportunidades, barreras y desafíos.

RESULTADOS Y DICUSIÓN

Criterios de inclusión y exclusión

La revisión sistemática de la literatura acerca del uso de la inteligencia artificial (IA) en la ciberseguridad empresarial, basada en búsquedas en Redalyc, Science Direct y Scopus de los últimos cinco años (2019-2024), ha revelado un notable volumen de investigaciones. Los filtros aplicados en Administración, Ingeniería, Computación y Ciencias de la Información permitieron identificar las principales tendencias y enfoques

temáticos. A continuación, se presentan los resultados en forma de gráficos. Estos ilustran la cantidad de publicaciones y su distribución por subáreas, proporcionan una visión detallada del panorama actual de la investigación y destacan los avances y áreas que requieren mayor atención.

La figura 1 muestra la frecuencia de publicaciones por subáreas en el periodo estudiado. Destacan las Ciencias de la Computación, Inteligencia Artificial, Seguridad Informática, Negocios, Ingeniería, fundamentalmente con una frecuencia mayor a 450.

108 Algorithm	899 Artificial intelligence	125 Artificial neural network	143 Big data	238 Biology
86 Blockchain	647 Business	77 Chemistry	156 Cloud computing	123 Computer network
1,887 Computer science	906 Computer security	90 Context (archaeology)	298 Data mining	286 Data science
138 Deep learning	78 Digital transformation	262 Economics	457 Engineering	81 Engineering ethics
85 Epistemology	156 Finance	98 Health care	127 Internet of Things	121 Internet privacy
145 Intrusion detection system	199 Knowledge management	365 Law	107 Linguistics	376 Machine learning
165 Marketing	273 Mathematics	96 Mechanical engineering	168 Medicine	379 Operating system
95 Paleontology	80 Pattern recognition (psychology)	215 Philosophy	206 Physics	460 Political science
111 Process (computing)	94 Process management	145 Programming language	203 Psychology	110 Quantum mechanics
127 Risk analysis (engineering)	170 Sociology	80 Telecommunications	212 The Internet	351 World Wide Web

Figura 1. Tabla de frecuencias de publicaciones entre 2019-2024

En este sentido, el número de publicaciones por tipos de documentos asciende en el período. Es singular el valor numérico de los artículos científicos, el cual alcanzó su punto máximo en 2024 con un total de 603, al cierre del primer semestre del año. La figura 2, representa un gráfico con lo antes expresado.

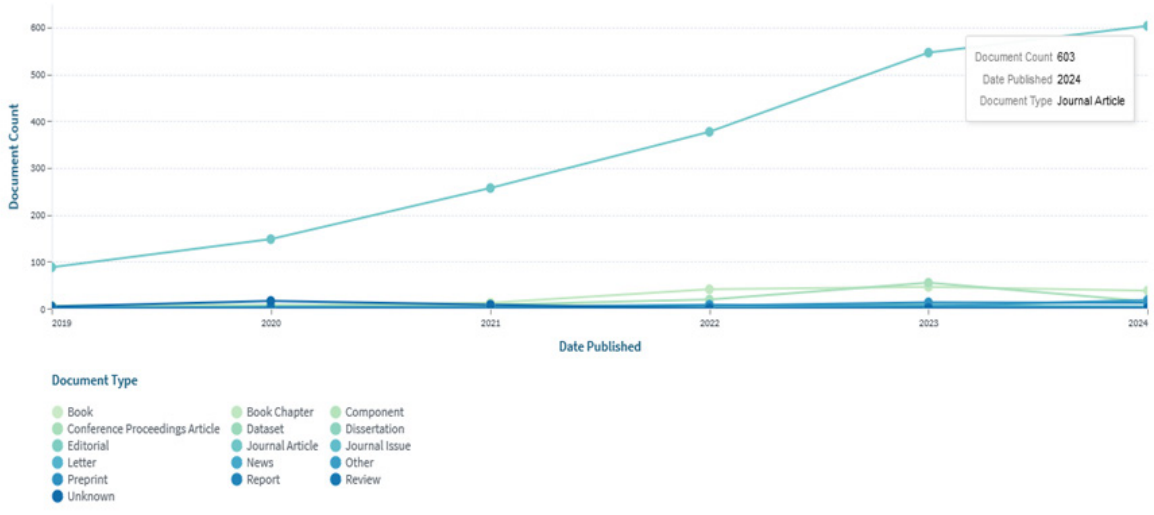

Figura 2. Tipos de publicaciones entre 2019-2024

Como se puede observar en las figuras 3 y 4, las publicaciones realizadas en tema de IA en las empresas han aumentado de forma exponencial, en comparación a los años 2019-2023, en el 2024 ha tenido un crecimiento de las publicaciones en las subáreas de Administración y Contabilidad y Computación, lo que afirma es que es un tema emergente en las empresas; a su vez, han disminuido el número de publicaciones en las Ingenierías.

En la figura 3, se muestra la distribución de publicaciones por subárea en Redalyc, destacan las áreas de Administración y Contabilidad (verde), Ingeniería (naranja), Computación (azul claro) y Ciencias de la

Información (azul oscuro).

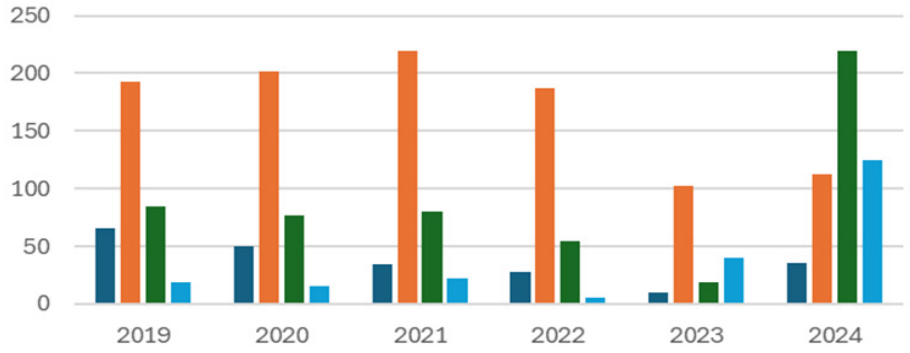

Figura 3. Revisión de Literatura en Redalyc

En esta gráfica (figura 4), se presenta la distribución de publicaciones por subárea obtenidas a través de Science Direct. Se puede observar la relevancia de cada área temática, con un ascenso considerable en las tres subáreas seleccionadas. El año 2024, se ve afectado hasta el momento porque solo se tuvo en cuenta el primer semestre del mismo, pero se puede aseverar que de igual forma, ascenderán sus valores de forma sobresaliente.

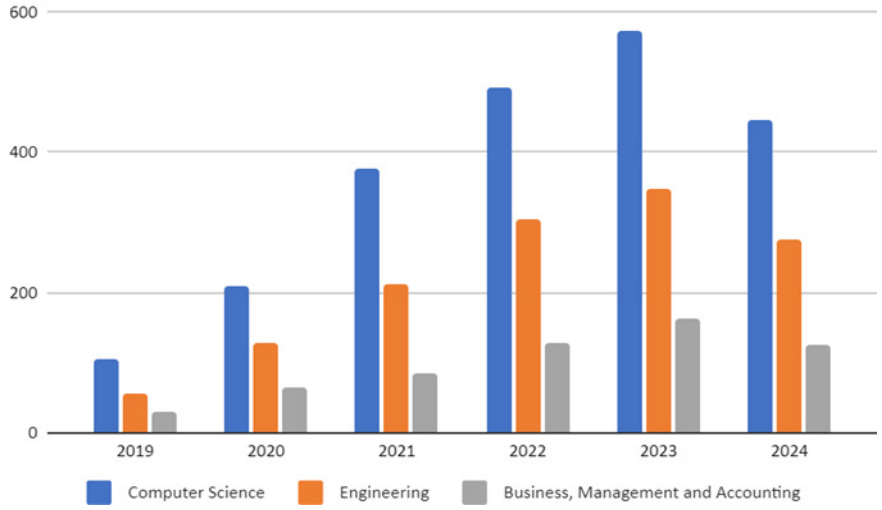

Figura 4. Revisión de Literatura en Science Direct

En la figura 5, se ilustra la distribución de publicaciones por subárea en Scopus, proporciona una visión comparativa con las otras bases de datos. El número de publicaciones es menor y se nota un ascenso singular en el año 2023. Los pronósticos al cierre del primer semestre de 2024, indican que no superará al año anterior, pero sí al resto del quinquenio.

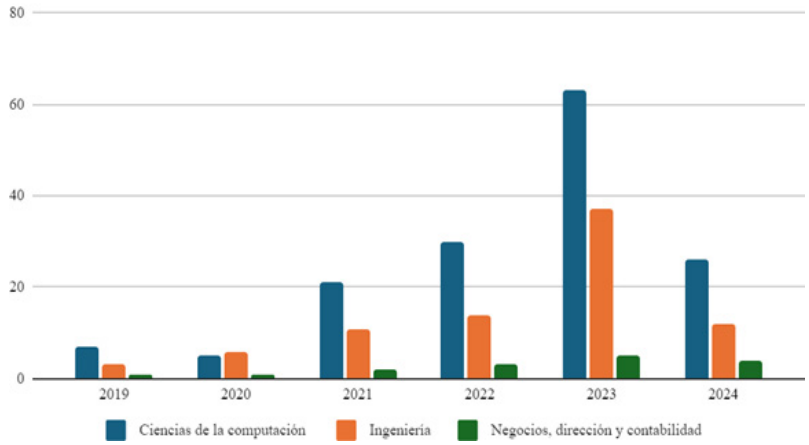

Figura 5. Revisión de Literatura en Scopus

Resultados revisión de literatura

En el marco teórico para la investigación sobre IA y ciberseguridad en las empresas, es necesario abordar en primera instancia, el concepto de ciberseguridad en el contexto de la Inteligencia Artificial.[41] Así mismo, desde la problemática de análisis, discutir de manera integral, los aspectos generales de las soluciones basadas en IA en la ciberseguridad organizacional. Se debe considerar en este análisis tanto los impactos positivos como los negativos.[42,43,44] Además, para obtener una comprensión de oportunidades y desafíos de implementación en las organizaciones.

Ante lo anterior, cabe exponer que la ciberseguridad protege los sistemas de información y comunicación conectados a Internet contra ataques y amenazas maliciosos.

La Cuarta Revolución Industrial y el Internet industrial de las cosas (IIoT) han ampliado el alcance de la ciberseguridad desde la seguridad de redes y aplicaciones hasta la infraestructura, la nube y la seguridad de la información, haciéndola multidimensional. La ciberseguridad abarca varios componentes y tecnologías interrelacionados en el ciberespacio en lugar de limitarse únicamente a la seguridad del sistema. En un contexto organizacional, la ciberseguridad implica proteger todas las dimensiones relevantes del ciberespacio de forma simultánea.

El concepto de "Inteligencia Artificial" surgió en 1956 y desde entonces ha evolucionado hacia soluciones prácticas utilizadas en diversos campos. El papel del aprendizaje automático en la ciberseguridad se remonta a la década de 1990 con el desarrollo de sistemas de detección de anomalías (ADS) y sistemas de detección de intrusos (IDS), aunque el progreso se vio obstaculizado por limitaciones informáticas y de datos. Hoy día, la IA es parte integral de la ciberseguridad y trasciende la jerga corporativa. Puede simular la inteligencia y los comportamientos humanos, lo que da como resultado una automatización de la seguridad cibernética más allá de la capacidad humana, que puede detectar una brecha de seguridad de una red en segundos.

La pandemia de COVID-19 aceleró la transformación digital e impulsó que las empresas dependieran de tecnologías como la inteligencia artificial, el aprendizaje automático (ML) y los big data. Sin embargo, esto provocó un aumento de los delitos cibernéticos al poner en peligro a personas y organizaciones establecidas. Los delitos cibernéticos podrían costar 10,5 billones de dólares para 2025. Debido a su dependencia de estas tecnologías, las empresas enfrentan riesgos operativos y de continuidad. Vale la pena explorar el uso de la IA en la ciberseguridad para que las organizaciones puedan comprender las capacidades de la IA en el espacio de la ciberseguridad en beneficio de su organización.

Las grandes cantidades de datos generados por las organizaciones brindan oportunidades para una amplia gama de aplicaciones de aprendizaje automático en el ciberespacio, incluida la inteligencia de amenazas, la detección de anomalías y la automatización de tareas relacionadas

con la ciberseguridad. La relación entre la IA y la ciberseguridad se denomina ciberIA.

Esta revisión de la literatura permite analizar cómo la IA puede aplicarse en la ciberseguridad desde una perspectiva organizacional y cuáles son esos aspectos positivos y negativos, así como las oportunidades y barreras de implementación.[45,46,47,48,49,50] Al analizar las publicaciones sobre IA y ciberseguridad en las empresas, se halla que la IA se aplica en gran medida en las organizaciones en cuanto a ciertos procesos administrativos y operativos; pero que son pocas las que lo utilizan para aumentar las medidas de ciberseguridad y preservar computadoras, redes, programas y datos de los depredadores e invasiones. Las declaraciones que aquí se enumeran describen los diferentes aspectos de este campo de investigación. Entre los beneficios de la ciberseguridad impulsada por la IA destacan los métodos comunes de IA como aprendizaje automático, aprendizaje profundo, procesamiento del lenguaje natural y representación y razonamiento del conocimiento.

Otros aportes son el valor de la IA en la seguridad inteligente del ciberespacio y en la gestión de esta tecnología, la utilización de métodos combinados, teoremas factoriales y multinomiales, métodos computacionales en aprendizaje automático, criptología y ciberseguridad. Estos ejemplos demuestran el valor de la investigación matemática y combinatoria para aumentar la importancia del análisis de datos y seguridad contra ciberataques.

En la era moderna, las organizaciones están preocupadas por el tema de la ciberseguridad. Si bien los proyectos suelen priorizar la innovación, existe el riesgo de comprometer la ciberseguridad cuando las organizaciones priorizan las características de ventas y el tiempo de comercialización, lo que resulta en evaluaciones limitadas de riesgo y recursos asignados para la ciberseguridad. Reforzar la seguridad de una red interna de la organización puede resultar insuficiente, ya que la dependencia de terceros puede crear nuevas vías, para que los ciberdelincuentes los exploten. Por lo tanto, las organizaciones deben considerar la gestión de riesgo cibernético de terceros (C-TPRM) para mitigar estos riesgos.

Si se trata de ciberseguridad, las organizaciones deberían explorar nuevos mecanismos y utilizar las medidas de ciberseguridad existentes. Para tomar decisiones informadas sobre inversiones en ciberseguridad, las organizaciones deben evaluar las compensaciones entre riesgo y recompensa.

Mejorar la ciberseguridad requiere auditorías y controles internos. Además, las organizaciones deben considerar los beneficios y desafíos asociados con el intercambio de información. en ciberseguridad. Para la infraestructura de red, las organizaciones normalmente emplear redes de área local (LAN) o LAN inalámbrica

para perímetros internos, mientras se utiliza el acceso a Internet para perímetros externos. En el contexto de la Industria 4.0, donde la comunicación en red y las comunicaciones inalámbricas son fundamentales, es crucial cumplir con las pautas de ciberseguridad y las mejores prácticas.

Es importante tener en cuenta el análisis exhaustivo de los desafíos y estrategias relacionados con la ciberseguridad en las redes móviles de telecomunicaciones, centrándose en la gestión de riesgos. Entre sus resultados se encuentran la identificación de amenazas específicas como ataques de denegación de servicio (DoS), intercepciones de comunicaciones y fraudes por suplantación de identidad. Se evaluaron vulnerabilidades en la infraestructura de telecomunicaciones, desde estaciones base hasta dispositivos de usuario final, para priorizar acciones correctivas. Por otra parte, se encontró un modelo integral de gestión de riesgos que abarca identificación, evaluación y mitigación, basado en estándares internacionales y mejores prácticas.

Otros aspectos analizados fueron la implementación de tecnologías como autenticación multifactorial, encriptación de extremo a extremo e inteligencia artificial para detección y respuesta a incidentes. Se hallaron recomendaciones para la implementación de políticas de seguridad y programas de capacitación específicos para las redes móviles de telecomunicaciones.

Las investigaciones existentes indican que el aumento de las amenazas y ataques cibernéticos ha obligado a las organizaciones a adoptar tecnologías basadas en inteligencia artificial para salvaguardar sus activos digitales. Se considera que el impulso inicial para esta adopción es la implementación de la IA en entornos organizacionales y que su aplicación a la ciber protección genera importantes ventajas competitivas para las organizaciones. Además, se cree que traerá un cambio revolucionario en la ciber protección moderna y su alcance.

En el análisis de la literatura realizada se hallaron temas relacionados con los efectos beneficiosos de la utilización de la IA en el contexto de la detección de malware, así como en la identificación de otros incidentes de intrusión en la red o el sistema. Además, la influencia favorable de la IA se extiende al ámbito de la administración de la ciberseguridad, simplifica los procedimientos operativos y mejora la comodidad general.

Mediante la identificación de patrones de datos y la detección de comportamientos anormales, el sistema puede identificar riesgos potenciales. En consecuencia, esta automatización permite a las organizaciones adoptar un enfoque proactivo para reconocer, anticipar y abordar amenazas familiares y desconocidas en lugar de depender únicamente de medidas reactivas después de una infracción cibernética. La automatización de las tareas de ciberseguridad reduce la necesidad de intervención humana, minimiza la interacción humana y, posteriormente, reduce el potencial de error humano durante todo el ciclo de vida de la seguridad.

En términos de ciberseguridad organizacional, no se trata solo de software avanzado y soluciones de protección. La salvaguardia de la seguridad física y de los componentes vitales del hardware y la infraestructura es crucial para que una organización logre una ciber protección integral y madura. La naturaleza multifacética de la inteligencia artificial (IA) puede tener un impacto positivo en la seguridad del hardware y la infraestructura al optimizar y monitorear los centros de datos, servidores y procesadores responsables de esta protección.

Las soluciones impulsadas por IA emplean técnicas de aprendizaje automático para monitorear aspectos como la temperatura del hardware, los sistemas de enfriamiento, el consumo de energía y las copias de seguridad de energía. Al analizar estos datos unidos a la información histórica, se puede afirmar que estas soluciones mejoran el rendimiento del hardware y la eficiencia general de la infraestructura. Además, la implementación de la IA ayuda a minimizar la carga financiera de los costos de mantenimiento de hardware e infraestructura necesarios para proteger una organización. Lo logra al notificar de manera inteligente a las organizaciones sobre el mantenimiento programado o al predecir fallas potenciales de componentes de hardware específicos, lo que permite el reemplazo proactivo antes de que ocurra una avería completa. En última instancia, la integración de tecnologías de IA con el mantenimiento de hardware e infraestructura puede proporcionar ahorros financieros para las organizaciones y reducir el consumo general de energía de los componentes de hardware.

Otro impacto positivo del uso de la ciberIA destacado en la literatura revisada fue la escalabilidad y la interconectividad de las soluciones de IA a un nivel más avanzado. La protección de la red mediante sistemas de análisis de red (NAS) y sistemas de protección de red (NPS) impulsados por IA puede garantizar la seguridad y disponibilidad de las redes informáticas dentro de una organización, no solo para una sola computadora sino para todo un sistema de red informática simultáneamente. Estas soluciones de IA se pueden implementar en cada etapa del ciclo de vida de la seguridad, lo que permite una solución más completa, integral e interconectada.

Aunque la implementación de la IA en la ciberseguridad organizacional es reconocida por su capacidad para lograr eficiencias más allá de las capacidades humanas, existen varios inconvenientes asociados con su adopción, particularmente a nivel organizacional.

La mayor adopción de la IA ha provocado un aumento de los ataques adversarios, lo que aumenta la amenaza de ciberataques. La existencia o ausencia de regulaciones y estándares relevantes puede impedir la adopción de la IA dentro de una organización. Estos efectos negativos obstaculizan o aplazan la aceptación generalizada de las soluciones de IA como un enfoque generalizado de ciberseguridad. Según la literatura actual, uno de los principales obstáculos para la adopción generalizada de la IA en el ámbito cibernético es su impacto en los

requisitos de infraestructura y hardware.

Para implementar de forma eficaz, soluciones impulsadas por IA a nivel organizacional, se necesita una potencia computacional, capacidades de procesamiento y memoria significativas. Además, los modelos de IA más grandes y avanzados exigen unidades centrales de procesamiento (CPU) modernas que puedan funcionar diez veces más rápido que los procesadores tradicionales, lo que genera costos de implementación sustanciales.

Otro desafío radica en los problemas de compatibilidad causados por el uso continuo de sistemas, lenguajes de programación e infraestructura tecnológica generales obsoletos en muchas organizaciones. Estos sistemas heredados no logran soportar adecuadamente los requisitos de las técnicas de IA y aprendizaje automático (ML). Por ejemplo, el análisis de grandes cantidades de datos complejos, un paso crítico en la implementación exitosa de IA y ML, se ve obstaculizado por la falta de escalabilidad que ofrecen las bases de datos heredadas y los sistemas obsoletos. En esencia, implementar soluciones de IA en las organizaciones no es una tarea sencilla, ya que muchas veces requiere una revisión completa de la infraestructura tecno tecnológica.

La literatura destaca constantemente un tema recurrente de disponibilidad insuficiente de datos limpios, libres de errores y de alta calidad. Las soluciones de IA se basan en amplios conjuntos de datos para entrenar modelos y lograr resultados precisos. Como resultado, obtener una gran cantidad de datos es esencial para entrenar modelos de IA de forma eficaz. Además, implementar una solución de ciberIA requiere un proceso de gestión de datos organizacional más complejo debido a los diversos volúmenes y tipos de datos almacenados, la velocidad a la que se acumulan, la necesidad de mantener la confidencialidad de los datos y la necesidad constante de datos adicionales. Este aspecto es particularmente crucial porque la inteligencia de las soluciones de IA depende únicamente de la calidad de los conjuntos de datos utilizados para entrenar los modelos.

No existe una solución universal de ciberIA que se adapte a todas las situaciones, ya que la mayoría de los sistemas de IA deben personalizarse de alguna manera para organizaciones específicas. Aunque algunas soluciones se pueden poner en práctica con relativa rapidez, se ha observado que el tiempo necesario para implementar la mayoría de las soluciones ciberIA a nivel organizacional afecta negativamente su adopción. Este retraso puede atribuirse a la complejidad inherente de la propia IA moderna e incluso la solución de IA más simple puede tardar meses o incluso años en implementarse completamente dentro de una organización.

Además del largo tiempo de implementación, se descubrió que implementar ciberIA presenta un desafío debido a su naturaleza multidisciplinaria, que requiere una variedad de profesionales especializados como científicos de datos, analistas de datos, expertos en inteligencia artificial, especialistas en aprendizaje automático, desarrolladores, especialistas en ciberseguridad y gerentes de proyectos, cada uno con diferentes niveles de experiencia técnica. Se señala que esta amplia necesidad de personal calificado plantea una dificultad para las organizaciones, dada la actual escasez de profesionales calificados y experimentados en estos campos especializados que puedan implementar y gestionar eficazmente soluciones de ciberIA a nivel organizacional. Las organizaciones a menudo **enfrentan** importantes cargas financieras al contratar a estos escasos profesionales.

Para evaluar plenamente el impacto de la IA en la ciberseguridad organizacional, se determinó que era necesario hacer una comparación entre los enfoques tradicionales de ciberseguridad y los enfoques impulsados por la IA. Se identificó que existe una literatura limitada pero que esta explora directamente la diferencia entre la IA y los medios tradicionales de ciberprotección. Además, se afirma que cada solución de IA debe adaptarse a una organización específica y utilizar datos internos y externos propios de la organización. Esto requiere un mayor compromiso financiero, de mano de obra y de implementación de hardware e infraestructura en comparación con los enfoques tradicionales.

La implementación de soluciones de IA a nivel organizacional está sujeta a leyes y regulaciones más estrictas en comparación con los enfoques tradicionales de ciberseguridad. Si bien la IA se utiliza principalmente con fines defensivos en la ciberseguridad organizacional, ciertos gobiernos y organismos reguladores han regulado las aplicaciones de IA de alto riesgo para garantizar el uso responsable de una tecnología tan poderosa.

Este estudio proporciona información sobre el impacto de la IA en la ciberseguridad organizacional, pero tiene limitaciones. Adopta una visión amplia de la influencia de la ciberIA en las organizaciones, pasa por alto las variaciones entre tipos, tamaños, sectores y regiones de organizaciones, que pueden producir diferentes efectos. No profundiza en herramientas específicas de IA, lo que restringe la comprensión de sus diversos impactos. Las limitaciones de tiempo delimitaron la búsqueda de literatura otras bases de datos, excluyeron potencialmente materiales relevantes de otras fuentes. Además, los criterios de inclusión/exclusión limitaron la selección de literatura pertinente, centrándose en publicaciones en el periodo entre 2019 e inicios del 2024.

Se debe señalar que la mayor parte de la literatura existente en este campo se ha concentrado en organizaciones grandes y bien establecidas, por lo que es necesario prestar más atención a las pequeñas y medianas empresas (PYME). Además, los impactos de la IA en la ciberseguridad identificados en esta revisión son amplios y no específicos de ninguna solución de ciberseguridad impulsada por la IA. Por lo tanto, futuras investigaciones podrían explorar los efectos de soluciones y herramientas específicas de IA en la ciberseguridad de una organización.

CONCLUSIONES

La literatura existente destaca un interés creciente en el empleo de la inteligencia artificial (IA) para la ciberseguridad, lo que genera debates en curso sobre la eficacia de los métodos de IA para fortalecer la ciberseguridad en varios dominios. En particular, se ha puesto énfasis en la investigación en la utilización de IA para la detección de intrusiones, así como para mejorar la protección e identificar malware. A medida que crece la adopción de tecnología dentro de las organizaciones, también aumenta la aparición de amenazas y ataques cibernéticos. La literatura existente indica un requisito apremiante para métodos mejorados y seguros de ciberseguridad organizacional que utilicen soluciones impulsadas por IA para protegerse contra amenazas en constante evolución. Por lo tanto, el objetivo de esta investigación de revisión de literatura, permitió analizar la influencia general de las soluciones impulsadas por la IA en la ciberseguridad organizacional. Se examinaron las ventajas y desventajas de implementar soluciones cibernéticas basadas en IA en las organizaciones.

Con esta revisión de la literatura, se determinó que la utilización de soluciones impulsadas por IA afecta la seguridad cibernética de las organizaciones durante todo el ciclo de vida de la seguridad. En el lado positivo, la IA contribuye a la ciberseguridad organizacional al automatizar procesos, analizar y predecir amenazas, mejorar la seguridad del hardware y la infraestructura, gestionar vulnerabilidades, ayudar en la toma de decisiones y en general, mejorar la solidez y resiliencia de la seguridad del sistema. Por el contrario, la IA tiene implicaciones negativas para la ciberseguridad organizacional. Estos incluyen importantes requisitos de datos, la necesidad de profesionales capacitados, demandas de hardware e infraestructura, desafíos en la implementación y la amenaza potencial que representa para los puestos de trabajo relacionados con la ciberseguridad. Además, dado que los propios piratas informáticos utilizan la IA para sus ataques, varios de estos se han vuelto resistentes a las medidas de protección basadas en la IA. Lo cual potencia un enfoque proactivo de la ciberseguridad e introduce vulnerabilidades adicionales que deben considerarse antes de implementarla a nivel organizacional. Deben considerarse factores como la ausencia de soluciones universales basadas en IA y la necesidad de regulaciones más estrictas en comparación con los enfoques tradicionales de ciberseguridad.

A pesar de algunas desventajas, la incorporación de soluciones de IA a la ciberseguridad organizacional tiene un efecto predominantemente beneficioso. Básicamente, el uso de la IA ofrece un nivel de ciberprotección eficaz, avanzado y elevado. Este resultado establece teóricamente una base para estudios futuros, que pueden profundizar en factores específicos como el tamaño y el tipo de organización y evaluar el impacto de la IA. Desde un punto de vista práctico, estos hallazgos pueden ayudar a las organizaciones a tomar decisiones mejor informadas con respecto a las soluciones de IA al proporcionar una evaluación imparcial de los impactos asociados.

REFERENCIAS BIBLIOGRÁFICAS

1. Arranz CFA, Arroyabe MF, Arranz N, de Arroyabe JCF. Digitalisation dynamics in SMEs: An approach from systems dynamics and artificial intelligence. Technological Forecasting and Social Change. 2023; 196:122880. https://doi.org/10.1016/j.techfore.2023.122880

2. Cepa K, Schildt H. What to teach when we teach digital strategy? An exploration of the nascent field. Long Range Planning. 2023;56(2):102271. https://doi.org/10.1016/j.lrp.2022.102271

3. Guatemala A, Martínez G. Capacidades tecnológicas en empresas sociales emergentes: una ruta de impacto social. Región Científica. 2023;2(2):2023111. https://doi.org/10.58763/rc2023111

4. Chang V, Doan LMT, Ariel Xu Q, Hall K, Anna Wang Y, Mustafa Kamal M. Digitalization in omnichannel healthcare supply chain businesses: The role of smart wearable devices. Journal of Business Research. 2023; 156:113369. https://doi.org/10.1016/j.jbusres.2022.113369

5. Dunsin D, Ghanem MC, Ouazzane K, Vassilev V. A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response. Forensic Science International: Digital Investigation. 2024; 48:301675. https://doi.org/10.1016/j.fsidi.2023.301675

6. Grosu V, Cosmulese CG, Socoliuc M, Ciubotariu M-S, Mihaila S. Testing accountants' perceptions of the digitization of the profession and profiling the future professional. Technological Forecasting and Social Change. 2023; 193:122630. https://doi.org/10.1016/j.techfore.2023.122630

7. Acero AM, Ordoñez BA, Toloza HP, Vega B. Análisis estratégico para la empresa Imbocar, seccional Valledupar – Colombia. Región Científica. 2023;2(2):202395. https://rc.cienciasas.org/index.php/rc/article/view/95

8. Hanisch M, Goldsby CM, Fabian NE, Oehmichen J. Digital governance: A conceptual framework and research agenda. Journal of Business Research. 2023; 162:113777. https://doi.org/10.1016/j.jbusres.2023.113777

9. Hartley N, Kunz W, Tarbit J. The corporate digital responsibility (CDR) calculus: How and why organizations reconcile digital and ethical trade-offs for growth. Organizational Dynamics. 2024;53(2):101056. https://doi.org/10.1016/j.orgdyn.2024.101056

10. Kaplan, A., & Haenlein, M. (2019). Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence. Business horizons, 62(1), 15-25. https://doi.org/10.1016/J.BUSHOR.2018.08.004

11. **Çipi** A, Fernandes ACRD, Ferreira FAF, Ferreira NCMQF, Meidutė-Kavaliauskienė I. Detecting and developing new business opportunities in society 5.0 contexts: A sociotechnical approach. Technology in Society. 2023; 73:102243. https://doi.org/10.1016/j.techsoc.2023.102243

12. Climent RC, Haftor DM, Staniewski MW. AI-enabled business models for competitive advantage. Journal of Innovation & Knowledge. 2024;9(3):100532. https://doi.org/10.1016/j.jik.2024.100532

13. Cosma S, Rimo G. Redefining insurance through technology: Achievements and perspectives in Insurtech. Research in International Business and Finance. 2024; 70:102301. https://doi.org/10.1016/j.ribaf.2024.102301

14. Muñoz HA, Menassa IS, Rojas L, Espinosa MA. La innovación en el sector servicios y su relación compleja con la supervivencia empresarial. Región Científica. 2024;3(1):2024214. https://rc.cienciasas.org/index.php/rc/article/view/214

15. del Val Núñez MT, de Lucas Ancillo A, Gavrila Gavrila S, Gómez Gandía JA. Technological transformation in HRM through knowledge and training: Innovative business decision making. Technological Forecasting and Social Change. 2024; 200:123168. https://doi.org/10.1016/j.techfore.2023.123168

16. Kowalkowski C, Ulaga W. Subscription offers in business-to-business markets: Conceptualization, taxonomy, and framework for growth. Industrial Marketing Management. 2024; 117:440-56. https://doi.org/10.1016/j.indmarman.2024.01.014

17. Maggie Wang Y, Matook S, Dennis AR. Unintended consequences of humanoid service robots: A case study of public service organizations. Journal of Business Research. 2024; 174:114509. https://doi.org/10.1016/j.jbusres.2024.114509

18. Sarker, I. H.; Furhad, M. H.; Nowrozy, R. AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. SN Computer Science, 2021, 2. https://doi.org/10.1007/s42979-021-00557-0

19. García M, López LS, Romero R. Control interno de inventario y la gestión de resultados de un emporio comercial de la región de San Martín - Perú. Región Científica. 2023;2(2):202392. https://rc.cienciasas.org/index.php/rc/article/view/92

20. Arroyabe MF, Arranz CFA, Fernandez De Arroyabe I, Fernandez de Arroyabe JC. Exploring the economic role of cybersecurity in SMEs: A case study of the UK. Technology in Society. 2024; 78:102670. https://doi.org/10.1016/j.techsoc.2024.102670

21. Hoong Y, Rezania D, Baker R. When traditional SME managers encounter cybersecurity: Discourse analysis of opportunities and dilemmas in meeting the demands. Technology in Society. 2024; 78:102650. https://doi.org/10.1016/j.techsoc.2024.102650

22. Jada I, Mayayise TO. The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. Data and Information Management. 2024;8(2):100063. https://doi.org/10.1016/j.dim.2023.100063

23. Debortoli DO, Brignole NB. Inteligencia empresarial para estimular el giro comercial en el microcentro de una ciudad de tamaño intermedio. Región Científica. 2024;3(1):2024195. https://doi.org/10.58763/rc2024195

24. Ali O, Murray PA, Momin M, Dwivedi YK, Malik T. The effects of artificial intelligence applications in educational settings: Challenges and strategies. Technological Forecasting and Social Change. 2024; 199:123076. https://doi.org/10.1016/j.techfore.2023.123076

25. Ghobakhloo M, Asadi S, Iranmanesh M, Foroughi B, Mubarak MF, Yadegaridehkordi E. Intelligent automation implementation and corporate sustainability performance: The enabling role of corporate social responsibility strategy. Technology in Society. 2023;74:102301. https://doi.org/10.1016/j.techsoc.2023.102301

26. Fiorentin FA, Llorca L, Suarez DV, Goren NJ. The advancement of Industry 4.0 and the transformations in the labor market Closing gender gaps? Policies under debate. Región Científica. 2024;3(2):2024290. https://doi.org/10.58763/rc2024290

27. Giordano V, Spada I, Chiarello F, Fantoni G. The impact of ChatGPT on human skills: A quantitative study on twitter data. Technological Forecasting and Social Change. 2024; 203:123389. https://doi.org/10.1016/j.techfore.2024.123389

28. Gómez CA, Sánchez V, Pérez AJ. El turismo como dinamizador del desarrollo económico: una revisión mixta de la producción científica. Dictamen Libre. 2024;35. https://doi.org/10.18041/2619-4244/dl.35.12114

29. Acciarini C, Cappa F, Boccardelli P, Oriani R. How can organizations leverage big data to innovate their business models? A systematic literature review. Technovation. 2023; 123:102713. https://doi.org/10.1016/j.technovation.2023.102713

30. Raudales EV, Acosta JV, Aguilar PA. Economía circular: una revisión bibliométrica y sistemática. Región Científica. 2024;3(1):2024192. https://doi.org/10.58763/rc2024192

31. Han H, Shiwakoti RK, Jarvis R, Mordi C, Botchie D. Accounting and auditing with blockchain technology and artificial Intelligence: A literature review. International Journal of Accounting Information Systems. 2023; 48:100598. https://doi.org/10.1016/j.accinf.2022.100598

32. Gómez CA, Sánchez V, Pérez AJ, Castillo W, Vitón AA, Gonzalez J. Internet of Things and Health: A literature review based on Mixed Method. EAI Endorsed Trans IoT. 2024;10. https://publications.eai.eu/index.php/IoT/article/view/4909

33. Ali O, Abdelbaki W, Shrestha A, Elbasi E, Alryalat MAA, Dwivedi YK. A systematic literature review of artificial intelligence in the healthcare sector: Benefits, challenges, methodologies, and functionalities. Journal of Innovation & Knowledge. 2023;8(1):100333. https://doi.org/10.1016/j.jik.2023.100333

34. Attard-Frost B, Brandusescu A, Lyons K. The governance of artificial intelligence in Canada: Findings and opportunities from a review of 84 AI governance initiatives. Government Information Quarterly. 2024;41(2):101929. https://doi.org/10.1016/j.giq.2024.101929

35. Velásquez LA, Paredes JA. Revisión sistemática sobre los desafíos que enfrenta el desarrollo e integración de las tecnologías digitales en el contexto escolar chileno, desde la docencia. Región Científica. 2024;3(1):2024226. https://doi.org/10.58763/rc2024226

36. Guler N, Kirshner SN, Vidgen R. A literature review of artificial intelligence research in business and management using machine learning and ChatGPT. Data and Information Management. 2024;8(3):100076. https://doi.org/10.1016/j.dim.2024.100076

37. Raman R, Pattnaik D, Hughes L, Nedungadi P. Unveiling the dynamics of AI applications: A review of reviews using scientometrics and BERTopic modeling. Journal of Innovation & Knowledge. 2024;9(3):100517. https://doi.org/10.1016/j.jik.2024.100517

38. Roppelt JS, Kanbach DK, Kraus S. Artificial intelligence in healthcare institutions: A systematic literature review on influencing factors. Technology in Society. 2024;76:102443. https://doi.org/10.1016/j.techsoc.2023.102443

39. Sánchez V, Pérez AJ, Gómez CA. Trends and evolution of Scientometric and Bibliometric research in the

SCOPUS database. Bibliotecas. Anales de Investigacion. 2024;20(1):1-22. http://revistas.bnjm.sld.cu/index.php/BAI/article/view/834

40. Liao a-T, Pan C-L, Wu Z. Digital Transformation and Innovation and Business Ecosystems: A Bibliometric Analysis for Conceptual Insights and Collaborative Practices for Ecosystem Innovation. International Journal of Innovation Studies. 2024. https://doi.org/10.1016/j.ijis.2024.04.003

41. Al Dhaheri MH, Ahmad SZ, Papastathopoulos A. Do environmental turbulence, dynamic capabilities, and artificial intelligence force SMEs to be innovative? Journal of Innovation & Knowledge. 2024;9(3):100528. https://doi.org/10.1016/j.jik.2024.100528

42. Ramón A, García AD, Estrada HG. Transformaciones e impactos de la innovación financiera y el auge de las Fintech en México. Región Científica. 2024;3(2):2024311. https://doi.org/10.58763/rc2024311

43. Kumar V, Ashraf AR, Nadeem W. AI-powered marketing: What, where, and how? International Journal of Information Management. 2024;77:102783. https://doi.org/10.1016/j.ijinfomgt.2024.102783

44. Nahar S. Modeling the effects of artificial intelligence (AI)-based innovation on sustainable development goals (SDGs): Applying a system dynamics perspective in a cross-country setting. Technological Forecasting and Social Change. 2024; 201:123203. https://doi.org/10.1016/j.techfore.2023.123203

45. González DIN, Garzón DP, Sánchez V. Cierre de las empresas del sector turismo en el municipio de Leticia: una caracterización de los factores implicados. Región Científica. 2023;2(1):202342. https://rc.cienciasas.org/index.php/rc/article/view/42

46. Jiang T, Sun Z, Fu S, Lv Y. Human-AI interaction research agenda: A user-centered perspective. Data and Information Management. 2024:100078. https://doi.org/10.1016/j.dim.2024.100078

47. Niet I, Van den Berghe L, van Est R. Societal impacts of AI integration in the EU electricity market: The Dutch case. Technological Forecasting and Social Change. 2023; 192:122554. https://doi.org/10.1016/j.techfore.2023.122554

48. Papagiannidis E, Mikalef P, Conboy K, Van de Wetering R. Uncovering the dark side of AI-based decision-making: A case study in a B2B context. Industrial Marketing Management. 2023; 115:253-65. https://doi.org/10.1016/j.indmarman.2023.10.003

49. Popkova EG, Bogoviz AV, Ekimova KV, Sergi BS. Will Russia become a blueprint for emerging nations' high-tech reforms? evidence from a 26-countries dataset. International Journal of Innovation Studies. 2023;7(4):294-306. https://doi.org/10.1016/j.ijis.2023.05.001

50. Rodgers W, Cardenas JA, Gemoets LA, Sarfi RJ. A smart grids knowledge transfer paradigm supported by experts' throughput modeling artificial intelligence algorithmic processes. Technological Forecasting and Social Change. 2023; 190:122373. https://doi.org/10.1016/j.techfore.2023.122373

FINANCIACIÓN

Los autores no recibieron financiación para el desarrollo de la presente investigación.

CONFLICTO DE INTERESES

Los autores declaran que no existe conflicto de intereses.

CONTRIBUCIÓN DE AUTORÍA

Conceptualización: Iris María Cantillo Velásquez, Jhon Wolfgang Echeverry David, Yerlis Patricia Martínez Taborda, Rubén Santiago Ramírez Piraquive.

Curación de datos: Iris María Cantillo Velásquez, Jhon Wolfgang Echeverry David, Yerlis Patricia Martínez Taborda, Rubén Santiago Ramírez Piraquive.

Análisis formal: Iris María Cantillo Velásquez, Jhon Wolfgang Echeverry David, Yerlis Patricia Martínez Taborda, Rubén Santiago Ramírez Piraquive.

Investigación: Iris María Cantillo Velásquez, Jhon Wolfgang Echeverry David, Yerlis Patricia Martínez Taborda, Rubén Santiago Ramírez Piraquive.

Metodología: Iris María Cantillo Velásquez, Jhon Wolfgang Echeverry David, Yerlis Patricia Martínez Taborda, Rubén Santiago Ramírez Piraquive.

Administración del proyecto: Iris María Cantillo Velásquez, Jhon Wolfgang Echeverry David, Yerlis Patricia Martínez Taborda, Rubén Santiago Ramírez Piraquive.

Recursos: Iris María Cantillo Velásquez, Jhon Wolfgang Echeverry David, Yerlis Patricia Martínez Taborda, Rubén Santiago Ramírez Piraquive.

Software: Iris María Cantillo Velásquez, Jhon Wolfgang Echeverry David, Yerlis Patricia Martínez Taborda, Rubén Santiago Ramírez Piraquive.

Supervisión: Iris María Cantillo Velásquez, Jhon Wolfgang Echeverry David, Yerlis Patricia Martínez Taborda, Rubén Santiago Ramírez Piraquive.

Validación: Iris María Cantillo Velásquez, Jhon Wolfgang Echeverry David, Yerlis Patricia Martínez Taborda, Rubén Santiago Ramírez Piraquive.

Visualización: Iris María Cantillo Velásquez, Jhon Wolfgang Echeverry David, Yerlis Patricia Martínez Taborda, Rubén Santiago Ramírez Piraquive.

Redacción – borrador original: Iris María Cantillo Velásquez, Jhon Wolfgang Echeverry David, Yerlis Patricia Martínez Taborda, Rubén Santiago Ramírez Piraquive.

Redacción – revisión y edición: Iris María Cantillo Velásquez, Jhon Wolfgang Echeverry David, Yerlis Patricia Martínez Taborda, Rubén Santiago Ramírez Piraquive.