



Ciencia Latina Revista Científica Multidisciplinar, Ciudad de México, México.
ISSN 2707-2207 / ISSN 2707-2215 (en línea), septiembre-octubre 2026,
Volumen 10, Número 5.

https://doi.org/10.37811/cl_rcm.v10i5

**INTELIGENCIA ARTIFICIAL, CIBERSEGURIDAD Y
SU RELACIÓN CON LOS SISTEMAS DE
INFORMACIÓN CONTABLE DEL SECTOR
TRANSPORTE INTERPROVINCIAL, HUANCAYO
2024**

**ARTIFICIAL INTELLIGENCE, CYBERSECURITY, AND THEIR
RELATIONSHIP WITH ACCOUNTING INFORMATION
SYSTEMS IN THE INTERPROVINCIAL TRANSPORTATION
SECTOR, HUANCAYO 2024**

Flor de María Jara Espinoza
Universidad Nacional Federico Villarreal

Inteligencia artificial, ciberseguridad y su relación con los sistemas de información contable del sector transporte interprovincial, Huancayo 2024

Flor de María Jara Espinoza ¹

2021006694@unfv.edu.pe

<https://orcid.org/0000-0002-3061-0497>

Universidad Nacional Federico Villarreal

RESUMEN

El estudio tuvo por objetivo determinar la correlación entre la inteligencia artificial, ciberseguridad y los sistemas de información contable en sector transporte interprovincial, Huancayo 2024. Metodología, de enfoque cuantitativo, tipo aplicada, nivel explicativa, diseño no experimental de corte transversal. La muestra del estudio fue de 100 personas conocedores y especialistas en inteligencia artificial, ciberseguridad y sistemas de información contable, seleccionados a través de muestreo no probabilístico por conveniencia. Resultados, revelaron existencia de coeficiente de correlación de ($Rho = 0.906$), de acuerdo con baremos de interpretación metodológica, el valor demuestra de manera contundente correlación positiva muy fuerte entre las variables en estudio. Colusión, combinación estratégica de herramientas algorítmicas y seguridad digital resulta fundamental para elevar eficiencia, precisión y transparencia en los procesos contables.

Palabras clave: Inteligencia artificial; ciberseguridad; sistemas de información contable; datos contables.

¹ Autor principal.

Correspondencia: 2021006694@unfv.edu.pe

Artificial Intelligence, Cybersecurity, and Their Relationship with Accounting Information Systems in the Interprovincial Transportation Sector, Huancayo 2024

ABSTRACT

The objective of the study was to determine the correlation between artificial intelligence, cybersecurity, and accounting information systems in the interprovincial transportation sector in Huancayo in 2024. Methodology: quantitative approach, applied type, explanatory level, non-experimental cross-sectional design. The study sample consisted of 100 experts and specialists in artificial intelligence, cybersecurity, and accounting information systems, selected through non-probabilistic convenience sampling. The results revealed a correlation coefficient of ($Rho = 0.906$); according to methodological interpretation standards, this value strongly indicates a very strong positive correlation among the variables under study. The strategic combination of algorithmic tools and digital security is essential for enhancing efficiency, accuracy, and transparency in accounting processes.

Keywords: Artificial intelligence; cybersecurity; accounting information systems; accounting data.

*Artículo recibido 06 septiembre 2026
Aceptado para publicación: 07 octubre 2026*



INTRODUCCIÓN

La transformación digital en sector transporte mundial plantea importantes desafíos en la gestión financiera y contable. La adopción creciente de plataformas digitales facilitó registro de operaciones; sin embargo, incrementa la vulnerabilidad frente a riesgos informáticos. En este contexto, la inteligencia artificial y la ciberseguridad emergen como factores determinantes para salvaguardar integridad de los datos y optimizar el procesamiento contable.

Para la Organización de las Naciones Unidas (ONU, 2024) alertó sobre diversos riesgos que representa la inteligencia artificial sin adecuada supervisión. La Asociación Interamericana de Contabilidad (AIC, 2024) el alto grado de interconexión global han dejado expuestas cerca del 92% de organizaciones de América Latina a múltiples riesgos cibernéticos, capaces de afectar la integridad, reserva y acceso oportuno de información, estos ciberataques no solo pueden generar considerables pérdidas económicas, sino también dañar seriamente la imagen de la corporación. ONU (2021) las amenazas que son más comunes reportadas provienen de las actividades maliciosas que son dirigidas tanto a usuarios de los sistemas de información, como llamados “phishing”, el robo de identidad o tácticas basadas en la figura del intermediario, como a propia infraestructura tecnológica, a través de software maliciosos, ataques de DDoS y otros que son métodos similares a los mencionados.

El ese contexto, aporta a literatura académica al analizar convergencia de tecnologías emergentes como el IA y ciberseguridad. Asimismo, contribuye a entender cómo la seguridad digital actúa como variable moderadora o determinante para la adopción confiable de inteligencia artificial en los sistemas de información contable, minimizando riesgos de pérdidas financieras por ciberataques o manipulaciones del sistema.

Antecedente al estudio, Pilay y marcos (2024) la automatización ofrece beneficios para modernizar la contabilidad, pero para aprovechar plenamente se requiere mentalidad abierta al cambio. Santiago y Páramo (2024) inteligencia artificial como tecnología influye significativamente en la forma y plantea importantes desafíos en cuanto a la integridad educativa contable. Calle y Andrade (2024) es esencial mejorar la formación en ciberseguridad y aumentar el presupuesto destinado para proteger los sistemas mitigando riesgos. Caminos-Manjarrez et al. (2023) la incorporación del software contable permite



optimizar los procesos contables, agilizar el trabajo, minimizar errores, alcanzar los objetivos empresariales con mayor facilidad y también mejorar la toma de decisiones.

Teoría del conexionismo de Edward Lee Thorndike 1949, sostiene que la inteligencia artificial no depende de reglas ni símbolos explícitos, sino que emerge de redes complejas de unidades conectadas, parecidas al de un cerebro humano, en este enfoque el conocimiento se encuentra más distribuido en sus vínculos (o pesos sinápticos) entre estas unidades, y el aprendizaje se produce al modificar dichas conexiones según los datos que la red recibe. La IA hace referencia a la capacidad que poseen los sistemas para aplicar algoritmos, los datos brindados y ese conocimiento en procesos de toma de decisiones de manera similar a la capacidad humana. (Lasse, 2018), se entiende como la habilidad que tiene un sistema computacional para imitar el funcionamiento del cerebro de los seres humanos, procesando diversas informaciones del entorno, aprendiendo a través del entrenamiento y utilizando ese aprendizaje para alcanzar fines para lo que está diseñado. (Brazdil y Jorge, 2001), son programas informáticos capaces de realizar diversas tareas que requieren de inteligencia y lógica, abarca uso de computadoras para comprender el funcionamiento de la inteligencia humana, sí que esto implique imitar procesos biológicos observables. (McCarthy, 2007) son sistemas informáticos diseñados básicamente para aprender y realizar predicciones. Estos sistemas toman decisiones basadas en datos con los que fueron entrenados, así como las nuevas informaciones que reciben a tiempo real. (Cárdenas, 2023).

El principio del Menor Privilegio de Jerome Saltzer 1966, fortalece la seguridad general de los sistemas y permite tener visibilidad y control preciso sobre el entorno digital. La ciberseguridad es el conjunto de diversas prácticas, medidas que son orientadas a proteger las redes, dispositivos, aplicaciones, sistemas y datos frente a las amenazas digitales. (Systemanalyse Programmentwicklung [SAP], 2024), son acciones tanto preventivas como reactivas, llevadas a cabo por personas, instituciones y sistemas tecnológicos con el propósito de proteger la información y asegurar que se mantenga confidencial, íntegra y de manera auténtica. (De Freitas, 2009), abarca el conjunto de tecnologías, práctica y política orientadas a prevenir los ciberataques o lo que sería ideal reducir drásticamente las consecuencias negativas, el propósito principal es proteger los sistemas informáticos, los dispositivos, datos y recursos financieros y las personas frente a amenazas como el ransomware, el phishing, el robo de información y otros tipos de software malicioso. (Matt, 2024).



Teoría de la información de Claude Shannon 1948. Constituye un enfoque interdisciplinario orientado al estudio de la cuantificación, almacenamiento y transmisión de la información. Sistema de información contable es conjunto de procedimientos, técnicas y herramientas utilizadas para recopilar, registrar, almacenar y procesar datos contables para producir información útil para tomadores de decisiones (Romney y Steinbart, 2018), es subsistema funcional dentro de un sistema de información de negocios que recopila y procesa datos relacionados con transacciones económicas de organizaciones para producir informes financieros y otros útiles para usuarios (Laudon y Laudon, 2016), aplicación informática integrada por procedimientos y técnicas orientados a generar información confiable, a partir del procesamiento, organización, clasificación, síntesis y registro de las operaciones económicas. (Prieto, 2024), información contable es fundamental para analizar las estrategias empresariales, de negocios, ya que facilita la comprensión del sistema económico de la corporación tanto cualitativos como cuantitativos. (Rueda y Arias, 2009).

El estudio tiene por objetivo, determinar la correlación entre la inteligencia artificial, ciberseguridad y los sistemas de información contable en sector transporte interprovincial, Huancayo 2024, aportando convicción científica en proteger y modernizar gestión contable que garantice continuidad operativa, competitividad comercial y transparencia en toma de decisiones por parte de líderes empresariales del sector transporte interprovincial.

METODOLOGÍA

La investigación se efectuó bajo enfoque cuantitativo, tipo aplicada, nivel explicativa, diseño no experimental de corte transversal. La muestra del estudio fue de 100 personas conocedores y especialistas en inteligencia artificial, ciberseguridad y sistemas de información contable, seleccionados a través de muestreo no probabilístico por conveniencia.

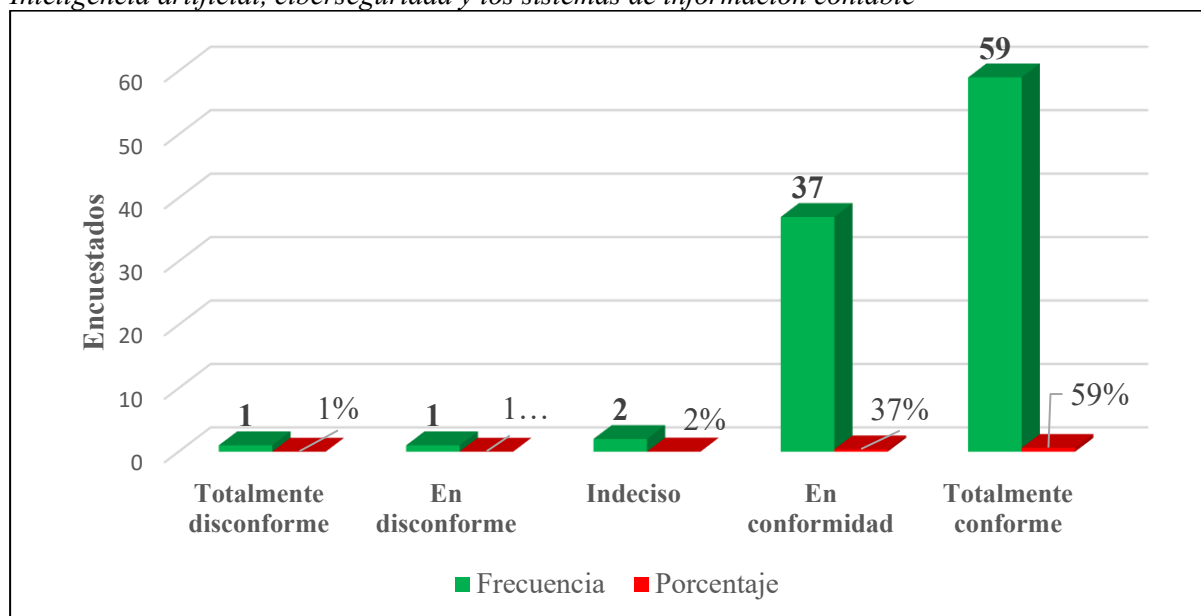
La técnica que se empleó fue la encuesta y se aplicó el instrumento del cuestionario tipo likert orientado a ejecutivos del sector servicio, la información se recabó por Google forms, con consentimiento informado y cuestionarios definidos, para analizar los datos se utilizó Excel 2016, que facilitó efectuar sumatorias de las tabulaciones de las respuestas por preguntas, dimensiones y variables, determinar límite inferior y máximo, cuadros y gráficos y otro análisis que requiera el estudio, para el análisis descriptivo e inferencial de datos se utilizó software SPSSv27.

RESULTADOS

Resultados descriptivos

Figura 1

Inteligencia artificial, ciberseguridad y los sistemas de información contable



Nota. Los resultados descriptivos obtenidos tras evaluar la percepción de muestra ($N = 100$) respecto a la variable vinculada a la inteligencia artificial, ciberseguridad y los sistemas de información contable. Al analizar la distribución de frecuencias, se observa marcada tendencia hacia valoraciones positivas por parte de los evaluados. El 59% ($n = 59$) de los participantes manifestó estar totalmente conforme, mientras que el 37% ($n = 37$) se ubicó en categoría en conformidad. De manera integrada, el porcentaje acumulado revela que el 96% de la muestra percibe de forma favorable la convergencia o el estado actual de estas herramientas tecnológicas y de seguridad en el ámbito contable. En contraste, niveles de neutralidad o insatisfacción resultaron estadísticamente marginales. Únicamente el 2% ($n = 2$) se declaró Indeciso, el 1% ($n = 1$) se mostró en disconformidad, y otro 1% ($n = 1$) seleccionó la opción Totalmente disconforme.

Hallazgos sugieren de forma contundente que usuarios profesionales perciben los sistemas de información contable respaldados por inteligencia artificial y ciberseguridad como herramientas altamente confiables, eficientes o alineadas con expectativas positivas, la baja presencia de posturas críticas o dudosas refuerza la viabilidad técnica y aceptación operativa de estas tecnologías en contexto de estudio, lo cual aporta base sólida para análisis correlacionales posteriores.

Resultados inferenciales

Hipótesis General

Tabla 1

Inteligencia artificial, ciberseguridad y los sistemas de información contable

	Inteligencia artificial, ciberseguridad	Coeficiente de correlación	de	Inteligencia artificial, ciberseguridad	Sistemas de información contable
Rho de Spearman	Inteligencia artificial, ciberseguridad	Coeficiente de correlación	de	1,000	,906**
		Sig. (bilateral)			,000
		N		100	100
	Sistemas de información contable	Coeficiente de correlación	de	,906**	1,000
		Sig. (bilateral)		,000	
		N		100	100

Nota. Se exponen resultados de prueba inferencial no paramétrica de Rho de Spearman, ejecutada con propósito de determinar el grado de relación entre variables predictor (Inteligencia artificial y ciberseguridad) y la variable dependiente (Sistemas de información contable), a partir de muestra válida de 100 profesionales del sector transporte interprovincial de Huancayo. Los datos estadísticos revelan existencia de coeficiente de correlación de (Rho = 0.906). De acuerdo con baremos de interpretación metodológica, el valor demuestra de manera contundente correlación positiva muy fuerte entre las variables en estudio. El signo positivo del coeficiente indica relación directamente proporcional, lo cual significa que a medida que se incrementa desarrollo, adopción y madurez de la inteligencia artificial y los protocolos de ciberseguridad en las organizaciones, se eleva significativamente el nivel de eficiencia, consistencia y optimización de sus sistemas de información contable.

DISCUSIÓN

Los resultados obtenidos en la investigación demuestran de manera contundente existencia de una relación directamente proporcional y significativamente alta entre la inteligencia artificial (IA), la ciberseguridad y la optimización de los sistemas de información contable en el sector de transporte interprovincial de Huancayo. El coeficiente de correlación de Spearman arrojado ($Rho = 0.906$, $p < 0.001$) evidencia asociación positiva muy fuerte, respaldada por percepción favorable del 96% de los especialistas encuestados. Este hallazgo sostiene de manera empírica que la modernización tecnológica contable en las organizaciones no puede concebirse como esfuerzo aislado, sino como convergencia estratégica donde el procesamiento algorítmico y la ciberprotección actúan en profunda sinergia.

Resultados concuerdan sustancialmente con lo planteado por Caminos-Manjarrez et al. (2023), quienes enfatizan que la adopción de herramientas tecnológicas avanzadas optimiza los procesos contables, minimiza el margen de error y facilita la toma de decisiones ejecutivas. Sin embargo, la presente investigación va un paso más allá al integrar a la ciberseguridad como factor indisoluble del ecosistema digital. Al respecto, los hallazgos dialogan críticamente con las advertencias de la Asociación Interamericana de Contabilidad (AIC, 2024) y la ONU (2021) respecto al alto nivel de vulnerabilidad institucional ante amenazas como el phishing y el ransomware. En tal sentido, los datos respaldan la postura de Calle y Andrade (2024), quienes sostienen que la asignación presupuestaria en seguridad digital y la capacitación continua son imprescindibles para mitigar riesgos financieros y operativos durante la automatización.

Desde perspectiva teórica, fuerte correlación hallada encuentra sólido respaldo en el marco conceptual analizado. Por, la Teoría del Conexionismo de Thorndike (1949) explica cómo los modelos algorítmicos basados en IA aprenden y adaptan sus flujos de datos a partir de interacciones complejas en tiempo real, imitando la resolución de problemas lógicos. Por otro lado, la incorporación del Principio del Menor Privilegio de Saltzer (1966) y la Teoría de la Información de Shannon (1948) justifican operativamente por qué la integridad, confidencialidad y transmisión eficiente de la información financiera dependen directamente de políticas de acceso estricto y salvaguardas cibernéticas. Tal como sostiene Matt (2024), la protección activa de la infraestructura es el pilar que permite que la automatización de datos contables se despliegue con confianza operativa.



En contexto específico del transporte interprovincial, donde la digitalización de la facturación, el rastreo de pasajes y la gestión de flotas generan volúmenes masivos de datos en tiempo real, este estudio demuestra que la ciberseguridad actúa como variable determinante para la madurez de los sistemas contables. En conclusión, la integración coordinada de tecnologías algorítmicas inteligentes y protocolos de protección informática informados constituye el motor principal para elevar la eficiencia, precisión y transparencia en las empresas del sector. Las futuras líneas de investigación podrían explorar el impacto de estas herramientas mediante metodologías cualitativas o modelos longitudinales para evaluar la resiliencia financiera a largo plazo.

CONCLUSIONES

La integración coordinada de tecnologías algorítmicas inteligentes y protocolos de protección informática robustos constituye factor determinante y directamente proporcional para la optimización, eficiencia y transparencia de los sistemas contables organizacionales. Con ello, se valida empíricamente que la modernización tecnológica no puede concebirse de manera aislada de blindaje cibernético efectivo si se desea garantizar la fiabilidad institucional.

El despliegue de soluciones inteligentes orientadas al procesamiento masivo de datos contables y la automatización de procesos operativos genera, de forma inherente, dependencia proporcional de salvaguardas digitales. Por lo tanto, para que la inteligencia artificial opere de manera resiliente, las empresas del sector transporte deben codesarrollar políticas rigurosas de gestión del riesgo cibernético y mitigación de vulnerabilidades que protejan los flujos interactivos humano-máquina.

REFERENCIAS BIBLIOGRÁFICAS

- Asociación Interamericana de Contabilidad (2024). Fortaleciendo la Resiliencia Digital: Estrategias de Ciberseguridad para los Contadores de las Américas desde el Aula Virtual de AIC. <https://goo.su/uUJNqT>
- Brazdil, P., y Jorge, A. (Eds.). (2001). Progress in Artificial Intelligence: Knowledge Extraction, Multi-agent Systems, Logic Programming, and Constraint Solving. Berlin, Heidelberg: Springer Berlin Heidelberg. <https://link.springer.com/book/10.1007/3-540-45329-6>



- Calle-Tenesaca, M., y Andrade-Amoroso, R. (2024). Ciberseguridad en contabilidad: protegiendo la integridad de los datos financieros en empresas comerciales. *Revista Metropolitana De Ciencias Aplicadas*, 7(S2), 87-98. <https://doi.org/10.62452/bdc3pg66>
- Caminos-Manjarrez, W., Guerrero-Arrieta, K., Pérez-Salas, F., y Córdova-Ponce, B. (2023). Los sistemas contables y su incidencia en la dirección empresarial en el Ecuador. *LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades*, 4(2), 5528–5544. <https://doi.org/10.56712/latam.v4i2.998>
- De Freitas, V. (2009). Análisis y evaluación del riesgo de la información: caso de estudio Universidad Simón Bolívar. *Revista enlace*. 6(1),43-55. https://ve.scielo.org/scielo.php?pid=S1690-75152009000100004&script=sci_abstract
- Lasse, P. (2018) Inteligencia artificial 101 cosas que debes saber hoy sobre nuestro futuro. Primera edición. <https://goo.su/rhwM>
- Laudon, KC, y Laudon, JP (2016). Sistemas de información gerencial: Gestión de la empresa digital (14.ª ed.). Pearson Education.
- Matt, R. (2024). ¿Qué es la ciberseguridad?. IBM. <https://www.ibm.com/mx-es/topics/cybersecurity>
- McCarthy, J. (2007) What is Artificial Intelligence? Stanford University, Computer Science Department. EEUU <http://wwwformal.stanford.edu/jmc/whatisai/>
- Organización de las Naciones Unidas (ONU, 2021). La ciberseguridad en las organizaciones del sistema de las Naciones Unidas. <https://goo.su/VyRP>
- Organización de las Naciones Unidas (ONU, 2024). La inteligencia artificial sin gobernanza es una amenaza para la democracia. Día Internacional de la Democracia. <https://surl.li/jfozys>
- Pilay - Asunción, D. D., & Marcos - Rodríguez, K. L. (2024). Los desafíos tecnológicos y el rol del contador en la automatización de procesos contables. *Journal of Economic and Social Science Research*,5(1), 306–329. <https://doi.org/10.55813/gaea/jessr/v5/n1/178>
- Prieto, E. (2024). Sistemas de información contable: ¿Qué son y cuáles son sus funciones? <https://es.snhu.edu/blog/aprende-sobre-los-sistemas-de-informacion-contable>
- Romney, MB, y Steinbart, PJ (2018). *Sistemas de información contable* (14ª ed.). Pearson Educación.



Rueda-Delgado, Gabriel; Arias-Bello, Martha Liliana (2009). Los sistemas de información contable en la administración estratégica organizacional. *Cuadernos de Contabilidad*, 10 (27), 247-268.

http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722009000200003

Systemanalyse Programmentwicklung (2024). SAP. ¿Qué es la ciberseguridad?

<https://www.sap.com/latinamerica/products/financial-management/what-is-cybersecurity.html>

