



fecha de presentación: 15/12/2025, fecha de aceptación: 11/01/2026, fecha de publicación: 01/02/2026

Karen Brigitte Irigoyen-Correa

E-mail: kirigoyen1@utmachala.edu.ec

Orcid: <https://orcid.org/0009-0007-5265-2675>

Ginger Dayana Cruz-Cruz.

E-mail: gcruz3@utmachala.edu.ec

Orcid: <https://orcid.org/0009-0004-9398-7496>

Zaida Patricia Morocho-Román

E-mail: zmorocho@utmachala.edu.ec

Orcid: <https://orcid.org/0000-0003-3964-843X>

Universidad Técnica de Machala, Facultad de Administración. Machala, Ecuador

Cita sugerida (APA, séptima edición).

Irigoyen-Correa, K. B., Cruz-Cruz, G. D., & Morocho-Román, Z. P. (2026). Relación entre ciberseguridad y confiabilidad de la información financiera en Cooperativas de Ahorro y Crédito. *Revista Sociedad & Tecnología*, 9(S1), 60-79, DOI: <https://doi.org/10.51247/st.v9iS1.706>.

==== o =====

Relación entre ciberseguridad y confiabilidad de la información financiera en Cooperativas de Ahorro y Crédito

RESUMEN

Este estudio analiza la relación entre la ciberseguridad y la confiabilidad de la información financiera en las Cooperativas de Ahorro y Crédito, pilares del sistema financiero popular y solidario. Se empleó un enfoque cualitativo, de tipo exploratorio-descriptivo a través de una revisión sistemática de literatura (SLR), bajo el protocolo PRISMA 2020, abordando riesgos cibernéticos, principios de ciberseguridad, marcos regulatorios como ISO 27001, COBIT, COSO y COSO ERM, debilidades organizacionales y similares; permitiendo comprender la ciberseguridad como un elemento esencial de transparencia y gobernanza financiera y no solo como un componente técnico. Los hallazgos indican que la ausencia de controles automatizados, la baja cultura digital y la falta de gobernanza de TI incrementan el riesgo de fraude, pérdida de datos, decisiones económicas erróneas y pérdida de confianza de los socios; en cambio, la implementación de políticas de seguridad, garantiza el fortalecimiento de la integridad, la disponibilidad y la autenticidad de la información financiera. Se concluye que la ciberseguridad incluida en los sistemas de control interno y en la gestión de riesgos, es fundamental para asegurar la fiabilidad contable y la sostenibilidad de las cooperativas en un entorno digital cada vez más vulnerable.

Palabras clave: Ciberseguridad, Información financiera, Cooperativas de Ahorro y Crédito, Gobernanza tecnológica, Control interno, Normas contables internacionales.

==== o =====

Relationship between cybersecurity and reliability of financial information in Savings and Credit Cooperatives

ABSTRACT

This study analyzes the relationship between cybersecurity and the reliability of financial information in Savings and Credit Cooperatives, pillars of the popular and solidarity-based financial system. A qualitative, exploratory-descriptive approach was used, employing a

systematic literature review (SLR) under the PRISMA 2020 protocol. This approach addressed cybersecurity risks, cybersecurity principles, regulatory frameworks such as ISO 27001, COBIT, COSO, and COSO ERM, organizational weaknesses, and similar factors. This allowed for an understanding of cybersecurity as an essential element of transparency and financial governance, and not merely as a technical component. The findings indicate that the absence of automated controls, low digital literacy, and a lack of IT governance increase the risk of fraud, data loss, erroneous economic decisions, and loss of member trust. Conversely, the implementation of security policies guarantees the strengthening of the integrity, availability, and authenticity of financial information. It is concluded that cybersecurity, included in internal control systems and risk management, is fundamental to ensuring the accounting reliability and sustainability of cooperatives in an increasingly vulnerable digital environment.

Keywords: Cybersecurity, financial information, savings and credit cooperatives, Technology governance, internal control, international accounting standards.

==== o =====

Relação entre cibersegurança e fiabilidade da informação financeira em cooperativas de crédito e poupança

RESUMO

Este estudo analisa a relação entre a cibersegurança e a fiabilidade da informação financeira nas cooperativas de crédito e poupança, pilares do sistema financeiro popular e solidário. Utilizou-se uma abordagem qualitativa, exploratória-descritiva, empregando uma revisão sistemática da literatura (RSL) sob o protocolo PRISMA 2020. Esta abordagem abordou os riscos de cibersegurança, princípios de cibersegurança, quadros regulamentares como a ISO 27001, COBIT, COSO e COSO ERM, fragilidades organizacionais e fatores similares. Isto permitiu compreender a cibersegurança como um elemento essencial da transparência e da governação financeira, e não meramente como uma componente técnica. Os resultados indicam que a ausência de controlos automatizados, o baixo nível de literacia digital e a falta de governação das TI aumentam o risco de fraude, perda de dados, decisões económicas erradas e perda de confiança dos associados. Por outro lado, a implementação de políticas de segurança garante o reforço da integridade, disponibilidade e autenticidade da informação financeira. Conclui-se que a cibersegurança, integrada nos sistemas de controlo interno e na gestão de riscos, é fundamental para assegurar a fiabilidade contabilística e a sustentabilidade das cooperativas num ambiente digital cada vez mais vulnerável.

Palavras-chave: Cibersegurança, informação financeira, Cooperativas de crédito e poupança, governação tecnológica, controlo interno, normas internacionais de contabilidade.

==== o =====

INTRODUCCIÓN

El origen de la ciberseguridad se remonta a finales de la década de 1980, cuando se evidenció uno de los primeros incidentes graves de seguridad informática en la Universidad de Delaware de Estados Unidos, que ocasionó el colapso de múltiples sistemas y evidenció la vulnerabilidad de las redes digitales emergentes, en otras palabras, podrían ser fácilmente afectadas por ataques informáticos; es por ello, que la protección de la información financiera se ha vuelto uno de las prioridades para las instituciones financieras, especialmente para las Cooperativas. (Calle y Andrade, 2024, p. 89)

Actualmente, las Cooperativas de Ahorro y Crédito, elementos esenciales del Sistema Popular y Solidario, enfrentan situaciones vulnerables crecientes debido a los riesgos

cibernéticos derivados del avance de la tecnología, los cuales afectan directamente la confiabilidad de la información financiera. El avance digital, aunque ha optimizado la gestión contable, ha generado un aumento a la exposición de ataques informáticos como fraudes electrónicos, accesos no autorizados y alteración de datos, lo cual puede arriesgar la integridad, disponibilidad y confidencialidad de la información financiera. (Ojeda et al., 2020, p. 194)

La falta de controles cibernéticos robustos en las Cooperativas, causa mayores riesgos de alteración de registros contables y de pérdida de trazabilidad de los estados financieros, lo que como consecuencia, afecta la credibilidad de la institución y la confianza de los socios. En este sentido, la ciberseguridad se convierte en una herramienta esencial de la gobernanza financiera y la transparencia informativa, y no solo es considerada un componente propiamente técnico (Ojeda et al., 2020, p.194).

La ciberseguridad se considera como el conjunto de tecnologías, prácticas, procesos y estrategias orientadas a la protección de sistemas informáticos, programas, redes y datos frente a ataques, accesos no autorizados o actividades maliciosas. A pesar de la importancia que recibe la ciberseguridad en la banca tradicional, la literatura académica respecto a su vinculación con la economía popular y solidaria y la relación con la confiabilidad e integridad de la información financiera, presenta aún vacíos teóricos significativos debido a que a medida que la tecnología avanza, las probabilidades de sufrir ataques cibernéticos son mayores (Quirumbay et al., 2022, p.58).

Desde este punto de vista, la hipótesis de trabajo que subyace a este estudio es el concepto de que existe un vínculo teórico entre la ciberseguridad y la fiabilidad financiera; comienza con la premisa de que las medidas y políticas de seguridad afectan directamente la integridad de la información, haciendo de la protección digital un factor determinante para asegurar la transparencia y credibilidad de esta en las cooperativas de ahorro y crédito.

También se investiga en este marco de referencia cómo los controles de ciberseguridad afectan la integridad de la información, qué debilidades tecnológicas y organizativas potenciales afectan la calidad de los registros contables y cómo los marcos de gobernanza regulatoria y tecnológica ayudan a establecer la fiabilidad de dicha información; tales preguntas nos permiten delimitar el campo de análisis y guiar la revisión de acuerdo con las dimensiones más pertinentes de la relación entre la seguridad digital y la gestión contable.

Apoyando la afirmación anterior, el objetivo de la presente investigación es analizar la relación de la ciberseguridad y la confiabilidad de la información financiera en las Cooperativas de Ahorro y Crédito, a través de perspectivas teóricas que permitan identificar los fundamentos conceptuales que estructuran dicho vínculo en los sistemas contables cooperativos.

Para explorar cómo los mecanismos de seguridad influyen en la precisión de las cuentas y la confianza obtenida por la institución se emplea una revisión de literatura y una síntesis de investigación de nicho; finalmente este debate se estructura en torno a tres ejes analíticos, en primer lugar corresponde a los principios de normativos y directrices internacionales sobre políticas de ciberseguridad, la siguiente sección aborda conceptos contables relacionados con la representación fiel, integridad y fiabilidad de los datos financieros, que sirven como base de la transparencia institucional.

A su vez el tercero se centra en modelos de gobernanza tecnológica, que se entienden como estructuras que proporcionan una plataforma para que las organizaciones definan políticas, controles y procedimientos de evaluación; además dicho marco de análisis permite una comprensión integral de la relación entre ciberseguridad y la fiabilidad contable, así como su influencia en la gestión financiera del sector cooperativo.

REVISIÓN DE LITERATURA

Ciberseguridad en el sector financiero

La ciberseguridad es un conjunto de tecnologías y procesos diseñados para proteger equipos, redes, aplicaciones y datos de posibles amenazas, y pues, una de las obligaciones que mantienen las cooperativas de ahorro y crédito, es proteger la confidencialidad de los datos sensibles, ya sean personales, financieros y transaccionales, con la finalidad de mantener la confianza de sus clientes y socios (Quirumbay et al., 2022, p. 58).

Según Aguilar y Balseca (2024), diariamente surgen ciberamenazas tales como malware, ransomware o phishing que cada vez se vuelven más sofisticadas, exigiendo mecanismos de seguridad que garanticen la prevención de infracciones y la reducción del impacto de posibles ataques. Por esta razón, las cooperativas deben visualizar a la ciberseguridad como una inversión y no como un gasto, ya que de esta manera se podrá garantizar la transparencia, sostenibilidad y el desarrollo seguro de todas sus operaciones (p. 519).

Principios de la Ciberseguridad

Según Hernández y Baquero (2025), existen cuatro principios fundamentales de la ciberseguridad, los cuales son los siguientes:

- 1) Confidencialidad:** Se encarga de garantizar que la información sea accesible únicamente para personas, sistemas o entidades que cuenten con la debida autorización, es decir, protege los datos financieros, personales o estratégicos frente a divulgaciones indebidas, accesos no autorizados o filtraciones que puedan comprometer la seguridad y privacidad de las entidades financieras (p. 8-9).
- 2) Integridad:** Según Calle y Andrade (2024), la integridad garantiza la confianza de los socios y la transparencia institucional; bajo esta perspectiva, resguardar los datos contables es una prioridad, dado que la ciberseguridad actúa como una barrera fundamental frente a los ataques cibernéticos que podrían arriesgar la confidencialidad de la información financiera (p.89).
- 3) Disponibilidad:** Esta permite que los servicios y la información sean accesibles cuando los usuarios los necesitan, lo que lleva a procesos financieros ininterrumpidos. La redundancia tecnológica, los programas de recuperación ante desastres y la resiliencia organizacional son prácticas recomendadas para mantener las operaciones disponibles (Ojeda et al., 2020).

De manera similar, la disponibilidad está correlacionada con la capacidad de responder a incidentes de ciberseguridad, en América Latina, esta falta de disponibilidad de servicios causada por los ataques de denegación de servicio (DDoS) ha enfatizado la importancia de mejorar las infraestructuras críticas para proteger los servicios frente a amenazas (Aguilar, 2021).

- 4) Autenticidad:** Según Machín y Gazapo (2016), la autenticidad consiste en garantizar que la información provenga de fuentes legítimas y verificadas para evitar el fraude y el robo de la identidad, lo cual se logra mediante certificados electrónicos, protocolos de autenticación multifactor y firmas digitales que garantizan la legitimidad de las operaciones.
- 5) Responsabilidad:** Este se presenta cuando una institución financiera junto con sus altos mandos son completamente responsables de la protección de sistemas y datos, y las políticas de seguridad se implementan de manera transparente y coherente.

Sánchez et al. (2024), argumentan que la auditoría de riesgos de ciberseguridad es una herramienta crucial para evaluar la responsabilidad institucional, ya que

identifica debilidades y permite el establecimiento de planes de acción para aumentar la confianza en la información financiera.

Normativas

Norma ISO 27001: Seguridad de la Información

Esta norma es el estándar internacional más reconocido para la gestión de la seguridad de la información, se adopta en las instituciones financieras como un marco de referencia para proporcionar la gestión de seguridad de la información, su función principal es establecer, implementar, mantener y mejorar sistemas de gestión de seguridad de la información (ISMS) que permitan a las organizaciones proteger sus activos digitales de amenazas internas y externas, es el aspecto financiero este estándar se vuelve vital, ya que las instituciones procesan grandes cantidades de datos sensibles como la información personal del cliente, transacciones electrónicas, registros contables, entre otros.

Según De la Cruz et al. (2023), este estándar proporciona garantía de seguridad mientras mejora el rendimiento empresarial en el mundo electrónico al establecer confianza entre los usuarios, la norma ISO 27001 también se integra en marcos como el Marco de Ciberseguridad NIST, que también permite una gestión de riesgos más robusta y que las organizaciones soporten factores de riesgo de ciberataques de manera aún más efectiva.

COBIT: Gobernanza y Control de las Tecnologías de la Información (TI)

El marco COBIT (Objetivos de Control para la Información y Tecnologías Relacionadas) es un conjunto de mejores prácticas desarrolladas por la ISACA (Asociación de Auditoría y Control de Sistemas de Información) que proporciona orientación sobre la gobernanza y gestión de la tecnología digital. Su objetivo es alinear las metas tecnológicas con la dirección estratégica de la organización; por lo tanto, la información debe ser confiable, segura y significativa para la toma de decisiones.

Coronel y Quirumbay (2022), argumentan que COBIT proporciona un enfoque holístico que permite la evaluación de aspectos de seguridad de TI en aplicaciones web, que al incorporar metodologías y estándares aborda mejor la gestión de riesgos y la protección de datos en los espacios más sensibles. Por ejemplo, basado en COBIT, Torres (2024), presentó un modelo de planificación estratégica de TIC para entidades financieras en el contexto ecuatoriano que mejora la gobernanza tecnológica, maximiza la efectividad en la toma de decisiones y mejora la ciberresiliencia.

A diferencia de la norma ISO 27001, que aborda la gestión de la seguridad de la información, COBIT se considera una gobernanza de TI más amplia, por lo que puede ser una herramienta estratégica que las instituciones financieras pueden aprovechar no solo para la protección de datos, sino también para asegurar que la tecnología cumpla con las necesidades corporativas.

Confiabilidad de la Información Financiera

Según lo mencionan Ruiz y Villacís (2024), la confiabilidad de la información financiera es el grado en que los estados financieros son considerados veraces, completos, precisos y reflejen de manera adecuada la situación económica y real de la entidad, con el objetivo de que la información presentada pueda ser utilizada de manera segura por los usuarios para la toma de decisiones estratégicas, la evaluación del desempeño, y la capacidad operativa y financiera de la misma.

Uzhca y Montero (2024) mencionan que la información financiera es considerada confiable cuando brinda una representación fiel de los estados financieros, que permita evaluar correctamente el desempeño y la posición financiera de las entidades. Además, mencionan que la confiabilidad está vinculada a la capacidad técnica de los encargados de emitir la información financiera, ya que demanda formación profesional y procesos sólidos de

coordinación, y no solo mejora la calidad de los informes generados, sino que también se fortalece la transparencia y la confianza de los organismos de control.

Específicamente, en las cooperativas de ahorro y crédito, la confiabilidad de la información financiera es importante, ya que se encargan de administrar recursos de sus socios y están sujetas a un marco regulatorio establecido por los organismos de control. Debido a la naturaleza jurídica de las cooperativas, en ellas se aplican NIIF, cuyas normas garantizan que la información sea transparente y comparable, generando confianza en los socios, la Superintendencia de Economía Popular y Solidaria y otros usuarios interesados.

Cooperativas de Ahorro y Crédito

Las CAC son fundamentales para garantizar la inclusión de la información financiera, especialmente en los países de América Latina, donde los bancos tradicionales no llegan a todos los sectores; Luque y Peñaherrera (2021) afirman que estas organizaciones se han consolidado como actores clave en Ecuador al proporcionar servicios financieros accesibles y fomentar la participación democrática de sus miembros; además, no solo contribuyen al desarrollo socioeconómico local al financiar proyectos comunitarios y promover el ahorro responsable, sino que también fomentan la confianza social al encarnar la solidaridad y el beneficio colectivo, diferenciándose de los bancos, puesto que están organizadas de manera colaborativa.

Riesgos Cibernéticos

Los riesgos cibernéticos son aquellos vinculados con el robo de información confidencial de los clientes y socios por parte de hackers ciberdelincuentes y organizaciones criminales, que tienen la finalidad de apropiarse de estos datos para realizar fraudes electrónicos (Ojeda et al., 2020).

Según Calle y Andrade (2024), la gestión de los riesgos consiste en un proceso estratégico y continuo que permite a las instituciones identificar, evaluar y afrontar amenazas potenciales que puedan afectar sus operaciones, recursos o activos; cuyo proceso analiza la probabilidad de que ocurran eventos y el impacto que tendrán si llegan a realizarse, para de esta manera establecer controles adecuados que reduzcan los efectos negativos.

Ataques Cibernéticos

Los ataques cibernéticos son acciones intencionales llevadas a cabo por parte de personas, grupos o instituciones con la finalidad de dañar, robar, interrumpir o acceder de manera no autorizada a los sistemas informáticos, redes digitales o bases de datos, los cuales son perjudiciales para las cooperativas de ahorro y crédito. (Aguilar y Balseca, 2024)

Tipos de Ataques Cibernéticos

Según Guaña y demás autores (2022), los ataques cibernéticos más comunes son:

- **Phishing:** Es uno de los ataques más frecuentes en el país, ya que consiste en engañar a los usuarios mediante correos electrónicos falsos para obtener credenciales de acceso.

En cooperativas de ahorro y crédito donde no se ha implementado eficientemente la capacitación del personal, es muy probable que abran enlaces maliciosos sin saberlo, pensando que provienen de bancos, proveedores o incluso de la Superintendencia de Economía Popular y Solidaria, pero en realidad no es así, y una vez que los atacantes cibernéticos tienen acceso, pueden ingresar al sistema contable aplicado en las cooperativas, modifica registros o transferir dinero a otras cuentas sin autorización, es decir, robar dinero de manera digital. (Izaguirre Olmedo y León Gavilánez, 2018)

- **Ransomware:** Este cifra los datos financieros de las CAC y exige un pago para desbloquearlos, y esto se da especialmente si las cooperativas no cuentan con copias de seguridad periódicas o mecanismos de recuperación de datos o información.

- **Malware:** Corresponde a cualquier programa malicioso que ingresa al sistema informático como troyanos, virus o spyware, los cuales pueden recopilar información confidencial y alterar los datos financieros sin ningún rastro.
- **Ataques de denegación de servicio:** Este ataque es aquel que inunda los servidores de las cooperativas con tráfico masivo desde diversos dispositivos, hasta que colapsan y dejan de funcionar; a pesar de que no roban la información directamente, interrumpen completamente las operaciones (Maldonado Montenegro, 2024).

Causas y Consecuencias de la Deficiente Implementación de la Ciberseguridad

Según Ramirez y Pereda (2023), las causas y consecuencias de la deficiente implementación de la ciberseguridad son:

Causas

- **Falta de asignación presupuestaria para seguridad financiera digital:** En ciertos casos, las cooperativas destinan sus recursos económicos en gran mayoría solo a sus operaciones básicas, minimizando u omitiendo en su totalidad la inversión en infraestructura tecnológica, cuya omisión impide adquirir herramientas esenciales de protección de datos.
- **Desconocimiento de los riesgos financieros asociados a incidentes cibernéticos:** Cuando la administración financiera de las cooperativas no integra los riesgos tecnológicos dentro de su análisis financiero, se especula que todo está correcto o en orden, generando una falsa sensación de estabilidad que puede resultar perjudicial.
- **Carencia de controles automatizados en los sistemas informáticos de gestión financiera:** Si estos controles no están implementados eficientemente, los registros financieros corren el riesgo de padecer de manipulaciones intencionales o errores involuntarios por parte de los usuarios.
- **Déficit de capacitación del personal financiero en ciberseguridad:** Las personas encargadas del área financiera pueden tener conocimientos básicos, pero no sobre amenazas cibernéticas, lo cual es negativo para la seguridad de las cooperativas, ya que es posible que se incurran en prácticas riesgosas.

Consecuencias

Según Andrade y Cobos (2025), las consecuencias son:

- **Pérdida de confiabilidad en los estados financieros:** Los estados financieros dejan de reflejar la situación económica real de las cooperativas si la información financiera es manipulada o alterada por personal no autorizado, lo cual afecta de manera directa la credibilidad ante socios, auditores y entidades de control.
- **Riesgo de fraudes financieros y pérdidas económicas:** Tener una deficiente ciberseguridad, facilita la ejecución de fraudes internos y externos, tales como la modificación de registros de crédito, la creación de cuentas falsas, transferencias de fondos sin autorización o la eliminación de evidencias financieras; cuyos actos fraudulentos afectan el capital, aumentan las pérdidas operativas y pueden afectar la continuidad financiera de las cooperativas de ahorro y crédito.
- **Toma de decisiones financieras en base a datos alterados:** El personal que se encarga de la planificación financiera, análisis de rentabilidad, otorgamiento de créditos o inversión de recursos opera en base a información contable precisa y verídica; si dicha información ha sido alterada sin detección, se produce un grave riesgo en la toma de decisiones estratégicas; lo cual puede derivar en decisiones

desacertadas, créditos mal otorgados, presupuestos más asignados, inversiones poco rentables, causando la afectación directa al desempeño económico y financiero de la cooperativa a corto y largo plazo.

- **Pérdida de confianza de los socios:** Cabe recalcar que la confianza de los socios es uno de los elementos fundamentales de las cooperativas, pero cuando ocurre una falla en la ciberseguridad que provoque la pérdida de datos y fondos, interrupciones en los servicios o modificaciones en los saldos, dicha confianza puede verse muy afectada, generando retiros masivos de depósitos, cierre de cuentas y reducción en la captación de nuevos socios, y por consiguiente, impactando negativamente la liquidez, la reputación y el volumen de las operaciones.

La Ciberseguridad y su Relación con la Confiabilidad Financiera Según el Modelo COSO, COSO ERM y Gobernanza TI

La relación de la ciberseguridad con la confiabilidad de la información financiera, radica en que la protección eficiente de los datos financieros es una condición fundamental para que la información financiera sea confiable y útil para la toma de decisiones. Es decir, la ciberseguridad se encarga de la protección de la integridad, exactitud y disponibilidad de los datos financieros utilizados en el proceso contable; cuya protección consiste en la prevención de alteraciones, pérdidas de datos o accesos no autorizados, con la finalidad de garantizar la presentación de los estados financieros de manera verídica, precisa y confiable, reflejando la situación económica real de la entidad.

En las Cooperativas de Ahorro y Crédito, en donde los sistemas informáticos soportan las transacciones, registros contables y reportes financieros, la presencia de los riesgos cibernéticos pueden afectar directamente la credibilidad de la información financiera; por ello, para abordar esta relación, el modelo COSO, el marco ERM y gobernanza de Tecnologías de la Información brindan información complementaria que permite vincular la confiabilidad de la información financiera con la gestión oportuna de riesgos informáticos.

- **Modelo del Comité de Organizaciones Patrocinadoras de la Comisión Treadway (COSO)**

El Modelo COSO de Control Interno expresa que uno de sus principales objetivos es garantizar la confiabilidad de la información financiera; además establece que la entidad tiene que encargarse de diseñar y aplicar políticas, procedimientos y controles que permitan que la información financiera esté completa, precisa y confiable. (Catagua et al., 2023, p.154)

Desde la perspectiva del modelo COSO, la ciberseguridad se convierte en un elemento fundamental del sistema de control interno, debido a que se encarga de identificar, prevenir y mitigar los riesgos que podrían afectar la calidad de la información financiera, es por ello, que la ciberseguridad se la incorpora en las entidades para la seguridad la generación, procesamiento y reporte de datos precisos y confiables.

- **Enterprise Risk Management (ERM)**

Mejía y Vásconez (2025) expresan que Enterprise Risk Management, marco de gestión integral de riesgos desarrollado por el modelo COSO, incluye específicamente los riesgos cibernéticos dentro de la planificación, evaluación y respuesta al riesgo, los cuales deben ser analizados en base al impacto que tienen sobre el logro de los objetivos estratégicos, financieros y operativos de la entidad.

En el caso de las Cooperativas de Ahorro y Crédito, una deficiencia en la gestión del riesgo cibernético puede comprometer la confiabilidad de los estados financieros, afectar la toma

de decisiones y debilitar la confianza de los socios y de los organismos de control; por ello, COSO ERM permite comprender la ciberseguridad como un riesgo organizacional clave y no solo como un problema de naturaleza técnica.

- **Gobernanza de las Tecnologías de la Información (TI)**

Según Flores y Lopez (2025), la gobernanza TI complementa los marcos anteriormente mencionados al establecer las estructuras claras de responsabilidad, autoridad y supervisión, asegurando que la tecnología, la seguridad de la información financiera y los objetivos financieros y operativos se alineen correctamente. Además, a través de marcos como COBIT, la Gobernanza de las TI define principios y prácticas mediante los cuales la gestión de la seguridad de los datos financieros y el control de riesgo tecnológicos, contribuyen de manera directa a la confiabilidad de la información financiera.

METODOLOGÍA

La naturaleza de esta investigación es cualitativa, de carácter teórico-documental y descriptivo; revisa la literatura científica, normativa y técnica sobre la relación entre la ciberseguridad y la confiabilidad de la información financiera en cooperativas de ahorro y crédito; este diseño metodológico se complementa con una Revisión Sistemática de Literatura (SLR) bajo el protocolo PRISMA 2020, que garantiza rigor, transparencia y replicabilidad en el proceso de búsqueda, selección y análisis de fuentes científicas (Page et al.,2021).

EL MÉTODO

Tipo de estudio

El estudio es exploratorio-descriptivo, la naturaleza exploratoria se debe a la limitada literatura específica sobre ciberseguridad aplicada a Cooperativas de Ahorro y Crédito, mientras que el aspecto descriptivo permite la identificación de conceptos clave, marcos teóricos, riesgos, y factores que afectan la fiabilidad de la información financiera (Ojeda et al.,2020).

Enfoque metodológico

La metodología PRISMA 2020 es uno de los métodos que tiene como objetivo analizar sistemáticamente las características claves del diseño del estudio, la implementación y el análisis para producir información exacta, abierta y verificable, se utiliza particularmente en revisiones sistemáticas y es útil para crear procesos claros de búsqueda, obtención y reporte de fuentes científicas que son más propensos a ser replicados.

Adopta un enfoque organizado basado en cuatro fases cruciales que garantizan la integridad y responsabilidad de esta revisión, la primera que es la identificación permite establecer estudios relevantes para la relación entre la ciberseguridad y la fiabilidad de la información financiera en cooperativas de ahorro y crédito, basándose en el uso de palabras clave que delimitaron el área temática, después está la fase del cribado para eliminar estudios que no tenían relevancia con dicha temática, la tercera fase de elegibilidad en la que los artículos fueron revisados y evaluados para su inclusión según los criterios, y por último la fase de inclusión que corresponde al instante final del proceso de revisión sistemática, aquí se determina qué estudios, artículos o documentos formarán parte del análisis final, esto permitirá abordar las preguntas de investigación que son:

¿Cómo se relaciona la ciberseguridad con la confiabilidad financiera?

¿Qué marcos regulatorios y tecnológicos apoyan esta relación?

¿Qué riesgos y brechas impactan la transparencia financiera en las cooperativas?

De manera resumida, siguiendo las fases del protocolo PRISMA, se empleó una Revisión Sistemática de Literatura (SLR):

- **Identificación:** búsqueda exhaustiva en bases de datos especializadas
- **Cribado:** eliminación de duplicados y selección preliminar a través de títulos y resúmenes.
- **Elegibilidad:** análisis detallado del texto completo
- **Inclusión:** formación del corpus final para el análisis temático.

Este paso hace posible consolidar una colección de fuentes científicas recientes y más relevantes que pueden ayudar a describir cómo la ciberseguridad se relaciona con la fiabilidad financiera en el entorno cooperativo (Sánchez et al.,2022).

Fuentes utilizadas

Se utilizaron fuentes confiables, tales como normas internacionales (ISO 27001), marcos de gobernanza tecnológica (COSO, COBIT), e informes técnicos de organizaciones como IFAC, NIST Y Basilea. Así como también, artículos científicos indexados en Scopus, Web of Science, Scielo y EBSCOhost, tesis académicas, y literatura gris institucional como Google Scholar.

Se incluyeron publicaciones realizadas en los últimos 5 años, revisadas por pares y de acuerdo con los avances regulatorios y tecnológicos que mantienen relación con la temática; excepcionalmente se admitieron documentos anteriores que se refieren a marcos regulatorios esenciales como (ISO 27001,COSO ERM) debido a su relevancia estructural; por ende los criterios de inclusión fueron que las fuentes consultadas sean publicaciones recientemente del periodo antes mencionado, y que el alcance se limite al sector financiero con un enfoque especial en las cooperativas de ahorro y crédito; por su parte se excluyeron las publicaciones que carecían de validez científica, artículos técnicos simplemente no relacionados directamente con la información financiera, textos repetitivos o artículos con problemas de integridad.

Además de ello el proceso de análisis y categorización de datos para este análisis se desarrollaron en tres pasos; en la etapa inicial se identificaron los conceptos claves como la integridad de los datos contables, las amenazas cibernéticas, los controles tecnológicos, la gobernanza y el cumplimiento normativo; como segundo paso se realizó una agrupación temática dividida en cuatro partes, que son riesgos cibernéticos aplicados al sector financiero, controles de seguridad digital relevantes para los sistemas contables, impacto de los incidentes cibernéticos en la fiabilidad de la información financiera y factores organizacionales que afectan la implementación de la ciberseguridad en las cooperativas de ahorro y crédito; finalmente como tercer paso se estableció una síntesis interpretativa o análisis integrador que permitió la identificación de tendencias, de brechas de investigación, la comparación de marcos regulatorios y una perspectiva sobre el papel de la ciberseguridad en la fiabilidad de la información financiera.

RESULTADOS



Gráfico 1. Proceso de Elaboración del Estudio de Revisión Sistemática de Literatura Nota. Etapas del proceso metodológico de la elaboración del presente artículo de revisión sistemática de Literatura.

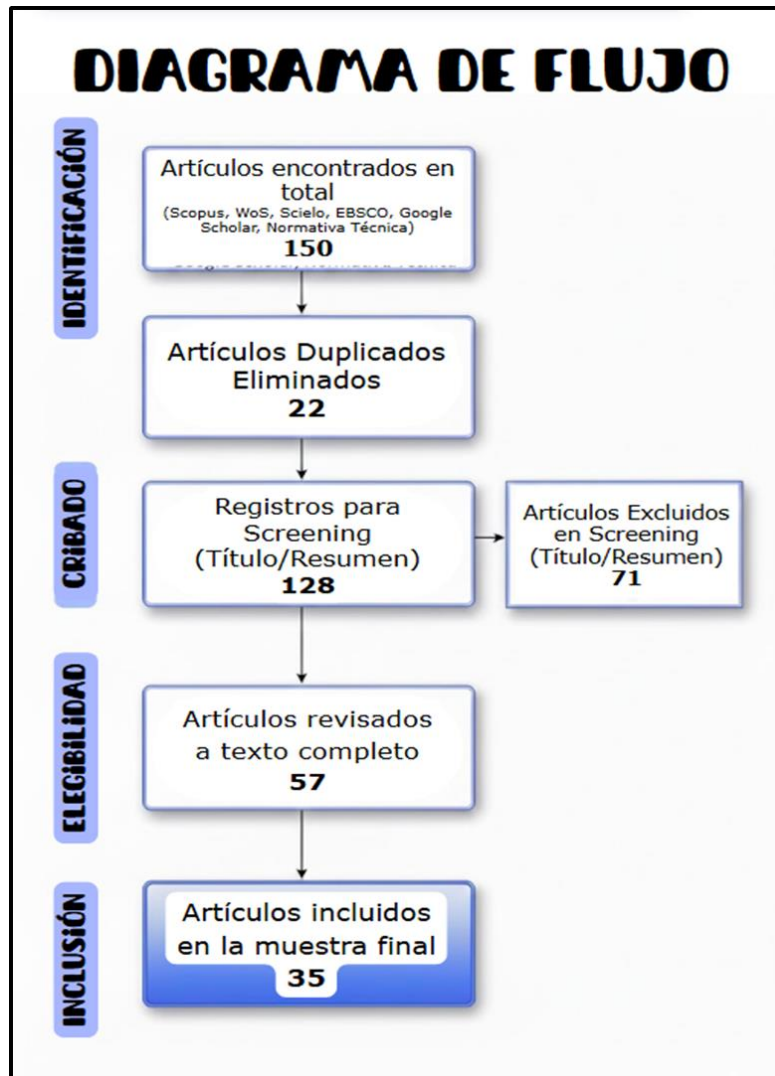


Figura 1. Diagrama de Flujo de la Metodología Prisma 2020

Nota. Representación gráfica de la metodología PRISMA 2020 aplicada al presente artículo.

Este diagrama de flujo PRISMA representa el proceso de búsqueda y recopilación de la literatura utilizada en la revisión teórica; como primera fase está la identificación, en la cual se localizaron 150 artículos proveniente de algunas bases de datos académicas tales como Scopus, Web of Science, Scielo, EBSCO, Google Scholar y normativas técnicas. En la fase de cribado, se realizó la eliminación de 22 documentos duplicados y se realizó la revisión de títulos y resúmenes de 128 artículos; de dicho total, se hizo el descarte de 71 estudios ya que no se alineaban con los criterios establecidos, quedando 57 artículos para la fase de elegibilidad, en donde fueron analizados a texto completo; de los cuales se excluyeron 22 artículos por la falta de cumplimiento de los criterios esenciales de pertinencia o carecían de conceptos significativos de ciberseguridad.

Finalmente, la base de inclusión permitió conformar un corpus definitivo de 35 artículos, los cuales respaldan el desarrollo del análisis de la relación entre ciberseguridad y la confiabilidad de la información financiera en las cooperativas de ahorro y crédito; además, garantizan la estructuración de conclusiones coherentes y fundamentadas con el propósito del estudio.

Análisis de la Literatura

El análisis de la literatura identificada evidencia un principal hallazgo: la confiabilidad de la información financiera en cooperativas de ahorro y crédito depende de manera directa del grado de protección tecnológica implementado en sus sistemas contables; puesto que los estudios examinados previamente, concuerdan en que los ciberataques, la falta de inversión en infraestructura de seguridad y las fallas del control interno informático provocan riesgos significativos de pérdida o alteración de los datos financieros. De igual manera, la evidencia teórica indica que la capacitación del personal, la gobernanza TI y la estandarización de normativas son condiciones fundamentales para fortalecer la integridad de los estados financieros.

Tendencias Generales en la Literatura Sobre Ciberseguridad

La revisión sistematizada permitió evidenciar varias tendencias importantes en el ámbito financiero. En primer lugar, se manifestó una gran preocupación por los riesgos digitales que afectan directamente los sistemas financieros, puesto que dichos riesgos son caracterizados por comprometer la integridad, disponibilidad y autenticidad de los datos financieros; y los fenómenos más frecuentes son los ataques de ransomware destinados a plataformas de gestión financiera, la manipulación de registros contables y las técnicas de ingeniería informática brindadas al personal administrativo.

De igual manera, se identifica una tendencia a vincular las normativas financieras con estándares internacionales de seguridad, tales como ISO 27001 y COSO ERM; cuya integración evidencia que la ciberseguridad ya no es considerada como un componente complementario, sino que es factor determinante clave para garantizar la transparencia contable y la calidad de los reportes financieros. Además, la literatura hace énfasis en el rol del factor humano, indicando que la deficiente capacitación y la baja cultura digital representan causas frecuentes que afectan la calidad de la información financiera.

Evidencia Empírica en Cooperativas de Ahorro y Crédito

Los estudios aplicados a cooperativas y entidades de microfinanzas revelan debilidades estructurales que amplían la relación entre ciberseguridad y confiabilidad financiera. Entre los hallazgos más recurrentes se encuentran las limitaciones presupuestarias, que se evidencian en infraestructuras tecnológicas deficientes, sistemas contables desactualizados y carencia de mecanismo de seguimiento en tiempo real. Por ejemplo, según Maliza (2021), el caso de la Cooperativa 1 de Julio en Tema evidenció que la ausencia de un plan de seguridad alineado a la norma ISO 27001 aumenta el riesgo de pérdida de datos financieros.

También, Rodríguez et al. (2020) evidenciaron que la aplicación de la norma ISO 27001 en una empresa privada permitió mejorar la seguridad de la información y consolidar una cultura organizacional diseñada para la protección digital, lo cual es relevante para el sector financiero, ya que demuestra que esta norma no solo aumenta la confianza interna, sino que también brinda credibilidad frente a reguladores y auditores externos.

De igual manera Ojeda et al. (2020) analizaron el sector financiero popular y solidario y concluyeron que la baja cultura digital, las limitaciones presupuestarias y la carencia de capacitación del personal son factores graves que afectan la confiabilidad de la información financiera.

La literatura así mismo señala una creciente exposición a fraudes ya sea internos como externos, específicamente en organizaciones donde no hay una adecuada segregación de funciones o los roles tecnológicos y financieros se superponen; por dichas razones, se facilita la alteración de historiales financieros, la modificación de saldos contables y la eliminación de evidencias fundamentales para la ejecución de auditorías internas y externa; por ello, estos hallazgos respaldan la idea de que el fortalecimiento de los controles

informáticos es una garantía directa de la confiabilidad de los estados financieros en este tipo de entidades.

Por ejemplo, Guachimposa (2024) demostró que los fraudes internos y externos en las Cooperativas de Ahorro y Crédito impactan directamente en su desempeño financiero, específicamente en entidades con roles superpuestos y controles deficientes.

Categorías Emergentes del Análisis Temático

El análisis cualitativo proveniente de los estudios revisados permitió la identificación de las siguientes categorías centrales que explican la relación entre ciberseguridad e integridad de la información financiera:

- Impacto de los ataques cibernéticos en los sistemas contables, donde se evidencia que amenazas como phishing financiero, ransomwares o accesos no autorizados provocan distorsiones en los estados financieros, inconsistencias en los registros y saldos contables y, por consiguiente, pérdidas significativas para procesos de auditoría.
- Relación entre inversión tecnológica y confianza financiera, indicando que las entidades que destinan mayores recursos económicos a la seguridad digital, tienen menos incidentes, mayor trazabilidad de la información financiera y más confianza de los socios, auditores y organismos de control.
- Riesgos estructurales en el entorno cooperativo, vinculados al personal incapacitado y no especializado en ciberseguridad, ineficiencia en los controles manuales y escasa automatización.
- Factores organizacionales, asociados a la carencia de una cultura de seguridad, deficiente formación del talento humano y ausencia de estructuras formales de gobernanza de la tecnología de la información.

Estas categorías indican que la ciberseguridad funciona como un componente fundamental del sistema de control interno que regula la calidad y confiabilidad de la información financiera.

Síntesis del Marco Conceptual

La evidencia recopilada proveniente de los diversos estudios revisados indica que los sistemas de ciberseguridad contribuyen significativamente al fortalecimiento de la integridad de la información financiera, ya que permiten mantener la trazabilidad, autenticidad y disponibilidad de los registros contables. Además, la implementación de las políticas de seguridad informática, los controles de acceso, el cifrado de datos y las auditorías digitales contribuyen a la reducción de la probabilidad de fraudes o manipulaciones, mientras que la inversión en infraestructura tecnológica y la capacitación eficiente del personal minimizan las vulnerabilidades operativas.

De esta manera, la literatura confirma la existencia de una relación directa y sostenida entre la ciberseguridad y la confiabilidad de la información financiera de las cooperativas de ahorro y crédito.

Tabla 1.

Dimensiones de Ciberseguridad y su Incidencia en la Confiabilidad de la Información Financiera

Dimensión de Ciberseguridad	Condición de Vulnerabilidad Identificada	Efecto en la Información Financiera	Ejemplo Aplicado en Cooperativas
Gestión de control de accesos	Privilegios mal definidos y falta de segregación de funciones	Alteración no autorizada de registros contables	Un empleado modifica saldos sin controles jerárquicos
Integridad de bases de datos	Ausencia de controles de validación y auditoría	Inconsistencias en estados financieros	Historiales financieros incompletos o alterados
Monitoreo y sistemas de alertas	Falta de supervisión continua y alertas automáticas	Pérdida de evidencia para auditoría	Movimientos atípicos no detectados
Cifrado de la información	Protección insuficiente de datos en tránsito o reposo	Exposición de información financiera sensible	Datos transmitidos sin cifrado
Respaldo y recuperación	Inexistencia de copias de seguridad automatizadas	Pérdida irreversible de información contable	Caída del sistema y pérdida de reportes
Capacitación del personal	Bajo nivel de concientización en seguridad informática	Registro fraudulento de transacciones	Phishing dirigido al área contable

Nota. Relación representativa entre dimensiones de ciberseguridad y sus efectos en la confiabilidad de la información financiera proveniente de la revisión de literatura.

DISCUSIÓN

Los resultados de la revisión indican que la fiabilidad de la información financiera en las Cooperativas de Ahorro y Crédito está directamente afectada por el nivel de protección tecnológica implementada en sus sistemas contables; un apoyo adicional proviene o se refuerza por varias investigaciones que ilustran que los ciberataques, la falta de inversión en infraestructura digital y las debilidades en el control interno de TI causan un gran riesgo de pérdida, manipulación o distorsión de los datos financieros (García et al., 2021).

Este resultado también coincide con lo que establecen Alassuli et al. (2025), ya que creen que para que ocurra la transformación contable digital, debe haber una función de gobernanza efectiva para promover la transparencia financiera; esto implica que, sin la infraestructura de protección adecuada detrás de ellos, los registros serán incapaces de rastrear y carecerán de credibilidad. Candau (2021), también advierte sobre la ciberseguridad como un problema importante a resolver no sólo como un problema técnico, sino como una parte transversal de la resiliencia institucional, particularmente en las organizaciones cooperativas donde la confianza de los miembros es una fortaleza intangible importante.

La revisión de la literatura sugiere un aumento en la sociedad de los marcos contables con estándares internacionales de seguridad (como ISO 27001 y COSO ERM), enfatizando aún más que la ciberseguridad ha evolucionado de un complemento operativo a un pilar fundamental de la gobernanza financiera, (Torres y Zúñiga, 2025). Esta convergencia regulatoria permite la creación de mecanismos formales que mejoran la integridad, autenticidad y disponibilidad de la información financiera, como lo evidencia el informe de la NCUA (2024), que muestra que las cooperativas de ahorro y crédito con mayor madurez digital tienen menos casos de fraude y más estabilidad institucional.

En una etapa temprana los estudios realizados en el campo empírico específicamente sobre cooperativas muestran debilidades estructurales que magnifican la correlación presupuestaria, la fragmentación del sistema, la ausencia de monitoreo en tiempo real y la mala segregación de funciones promueven mutaciones de balance y eliminación de evidencias y la implementación de fraudes internos y externos (García et al., 2021).

Estos resultados corroboran lo que León y Murillo (2021) identificó, refiriéndose a que la falta de automatización y cultura digital lleva a una mayor exposición en la forma de operar

y la calidad de la información; el análisis temático permitió que sugieran cuatro nuevas categorías que explican esta relación:

Efectos de los ciberataques en los sistemas contables: Phishing, ransomware y acceso no autorizado causan distorsiones en los registros financieros; la relación entre la inversión en tecnología y la confianza en las cuentas bancarias, indicando que aquellas organizaciones que asignan recursos a la seguridad digital pueden ofrecer más trazabilidad y confianza a los miembros y auditores; riesgos en la estructura de la situación cooperativa, resultantes de la falta de personal especializado, controles manuales ineficientes y baja automatización; y riesgo organizacional como la falta de cultura de seguridad, desarrollo inadecuado del talento humano y falta de gobernanza de TI estandarizada.

La ciberseguridad, en este sentido, puede interpretarse como un aspecto del mecanismo de control interno utilizado para mantener la calidad e integridad de la información financiera, por último, los hallazgos teóricos y cualitativos, junto con la evidencia empírica observada, nos ayudan a afirmar que la adopción de políticas y controles de seguridad de TI, el cifrado de datos y las auditorías digitales tienen un impacto significativo en la disminución del fraude y los errores contables.

Así se confirma la relación directa y duradera entre la ciberseguridad y la confiabilidad de la información financiera en las cooperativas de ahorro y crédito; lo que significa la necesidad de mejorar los sistemas de protección digital como una prioridad clave para la sostenibilidad y la confianza pública.

CONCLUSIONES

La revisión teórica realizada permite afirmar que efectivamente existe una relación directa y sustancial entre la ciberseguridad y la confiabilidad de la información financiera en las cooperativas de ahorro y crédito, puesto que los hallazgos muestran que aunque está instituciones han avanzado en la digitalización de sus procesos, aún enfrentan debilidades significativas debido a la creciente sofisticación de los ciberataques y a la limitada cultura de ciberseguridad presente en muchos de sus entornos operativos.

Los principios de confidencialidad, integridad, disponibilidad, autenticidad y responsabilidad constituyen elementos fundamentales para asegurar registros contables consistentes, completos y comprobables, especialmente en entidades que gestionan información sensible y dependen mayormente de la confianza de sus socios.

La carencia de controles de seguridad, la escasa capacitación del personal y la limitada inversión en infraestructura tecnología aumentan la posibilidad de manipulación de datos, fraudes financieros e interrupción de servicios, afectando la transparencia de los estados financieros y minimizando la credibilidad institucional; de igual manera, se identificó que la implementación de marcos normativos como ISO 27001, COBIT, NIIF, NICSP brindan lineamientos importantes que garantizan el fortalecimiento de la gobernanza tecnológica y la calidad de la información.

En relación con la hipótesis planteada, la evidencia recopilada respalda que la aplicación de medidas de ciberseguridad influye de manera significativa en la fiabilidad contable; además, las cooperativas que implementan estándares internacionales, promueven una cultura organizacional destinada a la seguridad y realizan evaluaciones de riesgos informáticos, muestran mayor transparencia y consistencia en sus registros contables e informes financieros.

La contribución principal del presente estudio es en la integración de perspectivas teóricas de ciberseguridad, normativas contables y gobernanza de tecnologías de la información para enfocar la importancia de una gestión digital fortalecida en el sector financiero, popular y solidario, ya que la seguridad de los sistemas contable no solo es un requisito técnico que cumplir, sino que se posiciona como un factor estratégico que mantiene la confianza los usuarios y garantiza la sostenibilidad financiera de las cooperativas de ahorro y crédito.

LIMITACIONES Y ESTUDIOS FUTUROS

El presente estudio a pesar de que aporta una comprensión sólida sobre la relación de la ciberseguridad y la confiabilidad de la información financiera, se basó únicamente en la revisión de literatura, limitando la posibilidad de medir empíricamente el impacto real de la ciberseguridad dentro de las cooperativas de ahorro y crédito.

Respecto al alcance futuro, el presente estudio encamina a futuras investigaciones a que complementen la revisión teórica y los casos documentados con metodologías cualitativas y cuantitativas tales como entrevistas a directivos y encuestas a usuarios o clientes, además de ampliar el análisis sobre la evaluación de riesgos informáticos específicos y la comparación entre modelos de gobernanza de tecnologías de la información y el desarrollo de indicadores que le permitan evaluar la efectividad de la implementación de controles de la ciberseguridad en las cooperativas y la incidencia que tiene en la calidad de sus estados financieros.

RECONOCIMIENTOS

Las autoras agradecen a la Universidad Técnica de Machala por el apoyo institucional que estuvo disponible durante la realización de este proyecto de investigación, de manera especial agradecen la asistencia metodológica y el apoyo académico brindado por la Ingeniera Zaida Patricia Morocho Román, tutora especialista, cuya experiencia fue fundamental para el rigor técnico del estudio, de igual manera destacan la cooperación mutua en cada etapa del trabajo de grado, lo que mejoró el análisis y la calidad de los resultados. Además, agradecen grandemente a Dios por la fortaleza, sabiduría y guía espiritual que recibieron de él durante su trabajo, y sin excepción agradecen a sus queridos padres por el apoyo incondicional, motivación y confianza en ellas y por su fe en la capacidad de ver este trabajo académico aprobado. Aprecian el arduo trabajo que forma parte de esta búsqueda; representando no solo un logro académico, sino también un esfuerzo compartido que está respaldado por familiares, institución y respaldo espiritual.

CONTRIBUCIÓN DE LOS COAUTORES

- **Karen Brigitte Irigoyen Correa:** Desarrolló la problemática, la investigación de trabajos anteriores en la introducción y contribuyó con la formulación del objetivo; la búsqueda de información de libros, artículos científicos y académicos para el desarrollo de la mitad de los conceptos abordados en la revisión de la literatura y para la evidencia de los resultados; diagrama de flujo de la metodología PRISMA; las conclusiones; y las limitaciones y estudios futuros.
- **Ginger Dayana Cruz Cruz:** Realizó el resumen; la formulación de la hipótesis, la relevancia y justificación del estudio, junto con el detalle de la organización del artículo; la búsqueda de información de fuentes confiables como artículos de revistas científicas y académicas, libros y normativas contables para la mitad de los temas de la revisión de la literatura; la metodología; y la discusión.
- **Zaida Patricia Morocho Román:** Se desempeñó como tutora de investigación, la cual proporcionó la estructura metodológica para la realización del presente artículo. Además, acompañó todo el proceso académico mediante revisiones y correcciones pertinentes, asegurando la rigurosidad y calidad de la investigación.

REFERENCIAS

- Alassuli, A., Thuneibat, N. S., Eltweri, A., Al-Hajaya, K., & Alghraibeh, K. (2025). The Impact of Accounting Digital Transformation on Financial Transparency: Mediating Role of Good Governance. *Journal of Risk and Financial Management*, 18(5), 272. <https://doi.org/10.3390/jrfm18050272>
- 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*, 53(198), pp. 169-197. <https://doi.org/10.5354/0719-3769.2021.57067>
- Aguilar Molina, P. L., & Balseca Manzano, J. M. (2024). Tendencias, Desafíos y Vulnerabilidades de los Ataques Cibernéticos en Ambientes de Desarrollo. Revisión Sistemática. *Estudios Y Perspectivas Revista Científica Y Académica*, 4(4), 517-539. <https://doi.org/10.61384/r.c.a.v4i4.689>
- Andrade-Logroño, F., & Cobos-Torres, J. C. (2025). Vulnerabilidades y ciberseguridad en sistemas SCADA: Análisis de riesgos y estrategias de protección en infraestructuras críticas. *MQRInvestigar*, 9(1). <https://doi.org/10.56048/MQR20225.9.1.2025.e289>
- Calle-Tenesaca, M. E., & Andrade-Amoroso, R. P. (2024). Ciberseguridad en contabilidad: protegiendo la integridad de los datos financieros en empresas comerciales. *Revista Metropolitana De Ciencias Aplicadas*, 7(S2), 87-98. <https://remca.umet.edu.ec/index.php/REMCA/article/view/734>
- Candau Romero, J. (2021). Ciberseguridad Evolución y tendencias. *Boletín IEEE (Instituto Español de Estudios Estratégicos)*, 23, 460-494. Dialnet. <file:///C:/Users/HP/Downloads/Dialnet-Ciberseguridad-8175398.pdf>
- Catagua Briones, M. L., Pinargote Macías, M. F., & Mendoza Vincas, M. E. (2023). Control interno y modelo COSO en la gestión administrativa y financiera empresarial. *Podium*, (44), 151-166. http://scielo.senescyt.gob.ec/scielo.php?pid=S2588-09692023000200151&script=sci_arttext
- Coronel, I., & Quirumbay, D. (2022). Seguridad informática, metodologías, estándares y marco de gestión en un enfoque hacia las aplicaciones web. *Revista Científica y Tecnológica UPSE (RCTU)*, 9(2), 97-108. Scielo. <https://doi.org/10.26423/rctu.v9i2.672>
- De la Cruz Rodríguez, G. R., Méndez, R. A., & Mendoza de los Santos, A. C. (2023). Seguridad de la información en el comercio electrónico basado en ISO 27001: Una revisión sistemática. *Dialnet*, 4(1), 219-236. <https://www.redalyc.org/journal/6738/673874721015/673874721015.pdf>
- Flores Cedeño, P. R., & Lopez Paz, C. R. (2025). Gobernanza de las tecnologías de la información en el desarrollo corporativo. *Revista InveCom*, 5(1), e501052. <https://doi.org/10.5281/zenodo.11374432>
- García, M. E., Hurtado, K. d. R., Ponce, V., & Sánchez, J. M. (2021). Analysis of the internal control process in savings and credit cooperatives. *COODES Cooperativismo y Desarrollo*, 9(1), 227-242. Scielo. http://scielo.sld.cu/pdf/cod/v9n1/en_2310-340X-cod-9-01-227.pdf
- Guachimbosa Santiago, C. E. (2024). Riesgo de fraude y el desempeño financiero en las cooperativas de ahorro y crédito del Ecuador. *Polo del Conocimiento*, 9(4), 1089-1102. <https://doi.org/10.23857/pc.v9i4.6983>
- Gualpa Guamán, A., & Urbina-Poveda, M. A. (2021). Determinantes del desempeño financiero de las cooperativas de ahorro y crédito del Ecuador. *Revista Economía y Política*, (34), 112-129. http://scielo.senescyt.gob.ec/scielo.php?pid=S2477-90752021000100112&script=sci_arttext
- Guaña-Moya, J., Sánchez-Zumba, A., Chérrez-Vintimilla, P., Chulde-Obando, L., Jaramillo-Flores, P., & Pillajo-Rea, C. (2022, Noviembre). Ataques informáticos más comunes en el mundo digitalizado. *Revista Ibérica de Sistemas e Tecnologias de Informação*, 87-100. Proquest. <https://www.proquest.com/docview/2812112763?fromopenview=true&pq-origsite=gscholar&sourcetype=Scholarly%20Journals>

- Izaguirre Olmedo, J., & León Gavilánez, F. (2018, Septiembre 7). Análisis de los ciberataques realizados en América Latina. *INNOVA Research Journal*, 3(9), 172-181. <https://doi.org/10.33890/innova.v3.n9.2018.837>
- Hernández Bejarano, M., & Baquero Rey, L. E. (2025). *Fundamentos de Ciberseguridad*. Escuela Tecnológica Instituto Técnico Central. <https://repositorio.itc.edu.co/bitstream/handle/20.500.14329/1581/01.%20Fundamentos%20de%20Ciberseguridad.pdf?sequence=1&isAllowed=y>
- León-Bermeo, S. R., & Murillo-Párraga, D. Y. (2021). Análisis Financiero: Gestionar los riesgos en las Cooperativas de Ahorro y Crédito segmento 1. *Revista Arbitrada Interdisciplinaria Koinonía*, 6(12), 242-272. <https://doi.org/10.35381/r.k.v6i12.1289>
- Luque, A., & Peñaherrera, J. (2021). Cooperativas de ahorro y crédito en Ecuador: el desafío de ser cooperativas. *REVESCO. Revista de Estudios Cooperativos*, 138, 1-20. Dialnet. <https://doi.org/10.5209/reve.73870>
- Machín, N., & Gazapo, M. (2016). LA CIBERSEGURIDAD COMO FACTOR CRÍTICO EN LA SEGURIDAD DE LA UNIÓN EUROPEA. *Revista UNISCI*, (42), 47-68. <https://www.redalyc.org/articulo.oa?id=76747805002>
- Maliza Malisa, A. S. (2021, Enero). *Plan de seguridad informática alineado a la Norma ISO 27001 para fortalecer las seguridades del data center en la cooperativa de ahorro y crédito 1 de julio de la ciudad del Tena*. Repositorio Digital Uniandes. <https://dspace.uniandes.edu.ec/handle/123456789/12752>
- Maldonado Montenegro, C. D. (2024). Análisis sobre la integración de la inteligencia artificial en la lucha contra la ciberdelincuencia en el Ecuador: desafíos y perspectivas. *Revista Criminalidad*, 66(3), 27-44. <https://doi.org/10.47741/17943108.660>
- Mejía-Buri, E. I., & Vásquez-Acuña, L. G. (2025). Fortalecimiento de la gestión operativa en cooperativas de ahorro y crédito mediante auditoría de riesgos [Strengthening operational management in credit unions through risk auditing]. *Revista Multidisciplinaria Perspectivas Investigativas*, 5(economica), 248-260. <https://doi.org/10.62574/rmpi.v5ieconomica.359>
- Montes Vera, Z. M., & Bravo Cedeño, J. G. (2024). La confiabilidad de la información contable y financiera. *Sinergia Académica*, 7(Especial 5), 626-644. <http://sinergiaacademica.com/index.php/sa/article/view/291>
- NCUA. (2024). Cybersecurity and Credit Union System Resilience Annual Report to Congress. <https://ncua.gov/news/publication-search/cybersecurity/cybersecurity-and-credit-union-system-resilience-annual-report-congress-2>
- Ojeda-Contreras, F. I., Moreno-Narváez, V. P., & Torres-Palacios, M. M. (2020, Octubre 1). Gestión del riesgo y la ciberseguridad en el sector financiero popular y solidario del Ecuador. *CIENCIAMATRIA Revista Interdisciplinaria de Humanidades, Educación, Ciencia y Tecnología*, 6(2), 192-219. <https://dialnet.unirioja.es/servlet/articulo?codigo=8316317>
- Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., ... Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *Journal of Clinical Epidemiology*, 134, 178-189. <https://doi.org/10.1016/j.jclinepi.2021.03.001>
- Quirumbay Yagual, D. I., Castillo Yagual, C. A., & Coronel Suárez, I. A. (2022). Una revisión del aprendizaje profundo aplicado a la ciberseguridad. *Revista Científica y Tecnológica UPSE (RCTU)*, 9(1), 57-65. <https://doi.org/10.26423/rctu.v9i1.671>

- Ramirez Vargas, J. A., & Pereda Otero, L. R. (2023, Noviembre 16). Propuesta de implementación de un modelo de ciberseguridad para la defensa contra ataques cibernéticos en la Oficina de Estadística e Informática del Instituto Nacional de Salud del Niño basado en el marco NIST v1.1. Repositorio Academico UPC. <https://repositorioacademico.upc.edu.pe/handle/10757/672290>
- Rodriguez Baca, L. S., Cruzado Puente de la Vega, C. F., Mejía Corredor, C., y Alarcón Diaz, M. A. (2020). Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana. *Propósitos Y Representaciones*, 8(3), e786. 2310-4635-pyr-8-03-e786.pdf
- Ruiz-Ruiz, E. G., & Villacís-Yank, J. A. (2024). NORMAS INTERNACIONALES DE INFORMACIÓN FINANCIERA EN LA GESTIÓN CONTABLE HOSPITALARIA. *KAIRÓS, Revista De Ciencias económicas, jurídicas Y Administrativas*, 7(13), 46-65. <https://doi.org/10.37135/kai.03.13.03>
- Sanchez, I. D., Rea, A. M., San, T., & Calvo, J. A. (2024). Auditoría de riesgos de ciberseguridad: Revisión de Literatura, propuesta y aplicación. *Scielo Revista Ibérica de Sistemas e Tecnologias de Informação*, 53, 69-87. Scielo. <https://doi.org/10.17013/risti.53.69-87>
- Sánchez, S., Pedraza, I., & Donoso, M. (2022). How to conduct a systematic review under PRISMA protocol? Uses and fundamental strategies for its application in the educational field through a practical case study. *Bordón: Revista de pedagogía*, 74(3), 51-66. Dialnet. <https://doi.org/10.13042/Bordon.2022.95090>
- Torres Gamarra, N., & Zúñiga Carnero, M. (2025). Panorama actual de la ciberseguridad: amenazas, legislación y brechas estructurales desde una revisión sistemática. <https://doi.org/10.5281/zenodo.15605545>
- Torres, J. D. R. (2024). Propuesta de modelo de planeación estratégica de TICs-gobernanza con COBIT para empresas del sector financiero bancario en el Ecuador, un enfoque ejemplar en una institución financiera. *Repositorio Nacional PUCE*. <https://repositorio.puce.edu.ec/handle/123456789/45157>
- Uzhca Corte, C. V., & Montero Cobo, M. A. (2024). Impacto de las NICSP en la calidad de la información financiera en instituciones públicas ecuatorianas. *PACHA. Revista de Estudios Contemporáneos del Sur Global*, 5(16). <https://doi.org/10.46652/pacha.v5i16.301>