Facultad de Ciencias de la Administración

Carrera de Contabilidad Superior

Seguridad de la información contable en entornos digitales. Una revisión de la literatura

Trabajo de titulación previo a la obtención del grado de Ingeniera en Contabilidad y Auditoría

Autora:
Ana Valeria Alvarez Luna

Directora:
María Gabriela Chica Contreras

Cuenca – Ecuador

Año

2026

DEDICATORIA

Dedico este trabajo de titulación primeramente a mis padres, Patricio y Esperanza, por su apoyo incondicional en cada etapa de mi vida y por ser ese ejemplo de lucha constante; son merecedores de toda mi admiración y respeto.

A mi esposo, Carlos, mi compañero de vida, por confiar siempre en mi capacidad y por brindarme tu apoyo total para culminar este sueño. A mis hermosas princesas, Belén y Elisa, quienes son mi fortaleza y alegría; espero ser siempre su fuente de orgullo y que este logro les enseñe que todo sacrificio tiene su recompensa.

A mis hermanos, Dennis, María y Paola, por estar presentes y alentarme a lograr este objetivo.

Finalmente, a mi familia política, especialmente a mi suegra, María, por cuidar de mi tesoro más preciado mientras yo perseguía este sueño; gracias por ser parte fundamental de este camino.

AGRADECIMIENTO

A Dios y a la Virgen Santísima, por ser mi luz, guía y fortaleza en cada momento de mi vida, y por darme la templanza necesaria para alcanzar esta meta.

Mi gratitud a todas aquellas personas que, con un consejo o una palabra de aliento, me impulsaron a ser perseverante. Gracias por depositar su confianza en mis capacidades y por recordarme que puedo lograr todo lo que me proponga.

Un agradecimiento especial a mi directora de proyecto, la Ing. Gabriela Chica, quien con su guía constante y excepcional calidad humana supo orientarme en la culminación de este trabajo. Su apoyo ha dejado en mí una profunda admiración profesional y personal.

Índice de Contenidos

Índice de Figuras

Índice de Tablas

RESUMEN

La presente investigación realiza un análisis crítico y sistemático de la literatura académica sobre la seguridad de la información contable en entornos digitales, con el propósito de identificar los principales riesgos que afectan a los sistemas de información contable. Además, analiza las prácticas y estrategias implementadas para la protección de la información financiera. El estudio se desarrolló bajo un enfoque cualitativo, de alcance descriptivo y carácter documental, mediante una revisión bibliográfica de tipo mapeo de literatura. Para la recopilación de información se consultaron bases de datos académicas de alto impacto, como Scopus, Web of Science, IEEE Xplore y SpringerLink, seleccionándose un total de 35 artículos científicos publicados entre 2015 y 2025, en función de su pertinencia temática y rigor metodológico.

Los resultados evidencian que los riesgos más relevantes se asocian a vulnerabilidades tecnológicas, amenazas cibernéticas como phishing, malware y ransomware, debilidades en los controles organizacionales y limitaciones en la capacitación del talento humano. Asimismo, se identifica que las buenas prácticas de ciberseguridad han evolucionado hacia enfoques integrales, destacándose la formación continua del personal, la implementación de controles tecnológicos avanzados, la adopción de marcos normativos y el uso de auditorías y monitoreo permanente.

En conclusión, la literatura revisada converge en la necesidad de adoptar un enfoque sistémico e integral que articule dimensiones tecnológicas, organizacionales y humanas para garantizar la confidencialidad, integridad y disponibilidad de la información contable.

Palabras clave: ciberseguridad, control interno, información contable, riesgos digitales, seguridad de la información, sistemas de información contable.

ABSTRACT

This study provides a critical and systematic analysis of the academic literature on accounting information security in digital environments, aiming to identify the main risks affecting accounting information systems, as well as the practices and strategies implemented to safeguard financial information. The research follows a qualitative, descriptive, and documentary approach, employing a literature mapping review. Data were collected from high-impact academic databases, including Scopus, Web of Science, IEEE Xplore, and SpringerLink, resulting in the selection of 35 scientific articles published between 2015 and 2025, based on their thematic relevance and methodological rigor.

The findings reveal that the most significant risks are associated with technological vulnerabilities, cyber threats such as phishing, malware, and ransomware, organizational control weaknesses, and insufficient staff training. Furthermore, the study identifies a shift toward comprehensive cybersecurity practices, emphasizing continuous training, the implementation of advanced technological controls, the adoption of regulatory frameworks, and the use of auditing and continuous monitoring mechanisms.

In conclusion, the reviewed literature highlights the need for a systemic and integrated approach that combines technological, organizational, and human dimensions to ensure the confidentiality, integrity, and availability of accounting information.

Keywords: accounting information systems, cybersecurity, digital risks, information security, internal control, accounting information.

1. **Introducción**

En los sistemas contables tradicionales, los registros financieros se gestionaban de forma manual o mediante software local, lo que limitaba su exposición a riesgos externos y reducía la probabilidad de ataques cibernéticos. No obstante, en la actualidad, la mayoría de los Sistemas de Información Contable operan en entornos digitales interconectados y basados en la nube, lo que ha incrementado de manera significativa su vulnerabilidad frente a diversas amenazas informáticas. Dado que la información financiera constituye un activo estratégico para las organizaciones, los ciberdelincuentes la consideran un objetivo de alto valor para la explotación de vulnerabilidades tecnológicas y organizacionales (Cram et al., 2023).

En este contexto, la gestión de la seguridad de la información contable enfrenta importantes cuestionamientos respecto a su efectividad. Si bien existen modelos y estándares internacionales ampliamente adoptados, como la norma ISO/IEC 27001, la literatura evidencia que su enfoque predominantemente documental no siempre garantiza un control real de los riesgos ni una adecuada correspondencia entre el valor de los activos protegidos y las medidas de defensa implementadas. Esta brecha entre la normativa y la práctica limita la capacidad de las organizaciones para responder de manera efectiva a las amenazas del entorno digital (Boss et al., 2022).

Diversos estudios señalan que esta problemática se acentúa en las pequeñas y medianas empresas, donde la ciberseguridad suele percibirse como un gasto operativo y no como una inversión estratégica. Esta visión restringe el análisis costo-beneficio, reduce la asignación de recursos destinados a la protección de los sistemas contables y aumenta la exposición a ataques informáticos. En consecuencia, se vuelve indispensable fortalecer la conciencia organizacional, la capacitación del personal contable y la inversión en infraestructura tecnológica orientada a la mitigación de riesgos (Jiménez et al., 2018).

Asimismo, la profesión contable enfrenta un incremento constante de ciberataques, lo que resalta la necesidad de reforzar las políticas, controles internos y estrategias de ciberseguridad en las organizaciones. La creciente dependencia de sistemas digitales para el procesamiento de información financiera amplifica los riesgos asociados a accesos no autorizados, manipulación de datos y pérdidas de información crítica, afectando directamente la integridad y la confidencialidad de los registros contables (Burchi et al., 2025a).

Desde una perspectiva problemática, los sistemas de información contable se encuentran cada vez más expuestos a amenazas derivadas del uso intensivo de tecnologías digitales y del almacenamiento de datos en entornos interconectados. Estas amenazas pueden generar consecuencias significativas, como accesos indebidos, destrucción de información, fraudes financieros y sanciones regulatorias, comprometiendo la toma de decisiones empresariales y la sostenibilidad organizacional (Cram et al., 2023). De hecho, (Cele&Kwenda, 2025a), evidencian que más de 4.500 incidentes de ciberseguridad fueron reportados por empresas y organizaciones sin fines de lucro, lo que refleja la magnitud del riesgo y la creciente vulnerabilidad institucional frente a las amenazas digitales.

La literatura reciente también destaca el potencial de tecnologías emergentes, como la blockchain y los marcos de inteligencia de ciberamnezas, para mejorar la capacidad de respuesta ante incidentes y fortalecer la seguridad en plataformas digitales. Sin embargo, su adopción sigue siendo limitada y su efectividad depende en gran medida del nivel de madurez tecnológica, de la gestión del riesgo y de la disponibilidad de recursos en cada organización (Burchi et al., 2025). Esta situación resulta especialmente crítica en regiones emergentes, donde la transformación digital avanza de forma acelerada, pero sin una implementación consistente de prácticas de seguridad informática.

Adicionalmente, si bien la digitalización ha mejorado el acceso, el análisis y la eficiencia en el manejo de la información contable, también ha generado nuevos desafíos, como la desigualdad digital y la limitada disponibilidad tecnológica en comunidades y organizaciones vulnerables. Estos factores profundizan las brechas de acceso y restringen una adopción equitativa y segura de los sistemas contables digitalizados (Giang&Tam, 2023).

En este contexto, el presente estudio tiene como objetivo analizar de manera crítica la literatura académica relacionada con la seguridad de la información contable en entornos digitales, con el fin de identificar los principales riesgos asociados, así como las buenas prácticas y recomendaciones orientadas a su mitigación. Para ello, el artículo se estructura de la siguiente manera: en la primera sección se desarrolla el marco teórico y el estado del arte, donde se examinan las principales tendencias teóricas y vacíos de investigación; posteriormente, se presenta la metodología empleada para la selección y análisis de los estudios; en la sección de resultados se exponen los hallazgos más relevantes en torno a riesgos, buenas prácticas y recomendaciones; a continuación, se desarrolla la discusión, en la que se interpretan y contrastan los resultados con la literatura existente; finalmente,

se presentan las conclusiones del estudio, destacando los principales aportes y líneas futuras de investigación.

1.1 Objetivo general:

Analizar de manera crítica la literatura académica relacionada con la seguridad de la información contable en entornos digitales, identificando los principales riesgos asociados a la manipulación o pérdida de datos, así como las estrategias y medidas preventivas implementadas por las organizaciones para garantizar la integridad, confidencialidad y disponibilidad de la información contable.

1.1.2. Objetivos específicos:

- Analizar los principales riesgos de seguridad de la información financiera existentes en los sistemas contables.
- Identificar las buenas prácticas de ciberseguridad que las empresas implementan.
- Establecer recomendaciones orientadas al fortalecimiento de la seguridad contable digitalizada.

1.2 Marco teórico

El presente marco teórico se fundamenta en la definición y delimitación de los conceptos clave relacionados con los sistemas de información contable, la seguridad de la información y la ciberseguridad, con el propósito de establecer una base conceptual que sustente el análisis de la protección de la información financiera en entornos digitales.

1.2.1. Seguridad de la información

La seguridad de la información se define como el conjunto de políticas, procedimientos y controles orientados a proteger los activos de información frente a amenazas que puedan comprometer su confidencialidad, integridad y disponibilidad (Whitman y Mattord, 2022).

Este enfoque se fundamenta en el modelo CIA (Confidentiality, Integrity, Availability), el cual constituye la base para la gestión de la seguridad en las organizaciones, independientemente del medio en el que se encuentre la información.

La seguridad de la información integra dimensiones tecnológicas, organizacionales y humanas, orientadas a prevenir accesos no autorizados, alteraciones indebidas y pérdida de datos. En el ámbito contable, su aplicación resulta esencial debido a la naturaleza crítica y sensible de la información financiera.

1.2.2. Sistemas de información contable en entornos digitales

Los sistemas de información contable (SIC) se definen como un conjunto integrado de personas, procesos y tecnologías destinado a recopilar, procesar y comunicar información

financiera para apoyar la toma de decisiones organizacionales (Romney y Steinbart, 2021).

Desde una perspectiva funcional, los SIC permiten el registro de transacciones económicas, la elaboración de estados financieros y el fortalecimiento del control interno. En entornos digitales, estos sistemas se caracterizan por el uso de plataformas tecnológicas interconectadas, bases de datos centralizadas y servicios en la nube, lo que facilita el acceso, procesamiento y almacenamiento de la información (Hall, 2016).

En este contexto, los sistemas de información contable requieren mecanismos de control que aseguren la confiabilidad, integridad y disponibilidad de la información financiera.

1.2.3. Ciberseguridad

Según Shahid et al, (2022), la ciberseguridad se define como una dimensión de la seguridad de la información enfocada en la protección de sistemas digitales, redes y aplicaciones frente a amenazas del ciberespacio. Además, se diferencia de la seguridad de la información, que abarca la protección de los datos en cualquier formato, la ciberseguridad se centra en los entornos tecnológicos interconectados. Su finalidad es prevenir, detectar y responder a incidentes de seguridad mediante la implementación de controles técnicos.

En los sistemas de información contable, la ciberseguridad permite proteger la infraestructura tecnológica que soporta el procesamiento de la información financiera.

1.2.4. Riesgos cibernéticos en los sistemas de información contable

Los riesgos cibernéticos se definen como la probabilidad de que una amenaza digital explote vulnerabilidades en los sistemas tecnológicos, afectando la confidencialidad, integridad o disponibilidad de la información (Hall, 2016).

En los sistemas de información contable, estos riesgos pueden originarse en debilidades de los controles tecnológicos, errores humanos o fallas en los procesos organizacionales. En este sentido, diversos estudios destacan que la interacción entre factores técnicos y humanos incrementa significativamente la exposición a incidentes de seguridad, comprometiendo la confiabilidad de la información financiera y afectando la toma de decisiones organizacionales (Shahid et al., 2022; Whitman y Mattord, 2022).

La gestión de los riesgos cibernéticos implica su identificación, evaluación y tratamiento, con el fin de reducir su impacto en los sistemas contables digitales. Este proceso se fundamenta en enfoques estructurados de gestión del riesgo, los cuales permiten a las organizaciones anticipar amenazas, implementar controles adecuados y fortalecer la

resiliencia frente a incidentes de seguridad (ISO/IEC 27005, 2018; Sánchez-García et al., 2024).

1.2.5. Marcos normativos y modelos de gestión de la seguridad de la información

Los marcos normativos de seguridad de la información se definen como conjuntos de estándares, lineamientos y buenas prácticas orientados a gestionar y proteger los activos de información en las organizaciones.

La norma ISO/IEC 27001 establece los requisitos para la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI), basado en la identificación y tratamiento de riesgos (Sánchez-García et al., 2024). De manera complementaria, la norma ISO/IEC 27002 proporciona controles de seguridad, mientras que ISO/IEC 27005 se enfoca en la gestión de riesgos.

Por su parte, el modelo COSO ERM permite integrar la gestión de riesgos dentro del sistema de control interno, incluyendo aquellos de carácter tecnológico. Asimismo, el marco NIST proporciona lineamientos para la identificación, protección, detección, respuesta y recuperación frente a incidentes de ciberseguridad.

Estos marcos permiten estructurar la gestión de la seguridad de la información de manera sistemática y alineada con los objetivos organizacionales.

1.2.6. Buenas prácticas de ciberseguridad en el ámbito contable

Las buenas prácticas de ciberseguridad se definen como un conjunto de acciones orientadas a prevenir, detectar y mitigar riesgos en los sistemas de información contable. Entre estas prácticas se incluyen la segregación de funciones, el control de accesos basado en roles, la autenticación segura y el cifrado de la información, las cuales contribuyen a proteger la información financiera frente a accesos no autorizados y posibles alteraciones (Romney y Steinbart, 2021).

Asimismo, la auditoría de sistemas y el monitoreo de actividades permiten identificar vulnerabilidades y fortalecer los controles internos (Ramesh et al., 2025).

La aplicación de estas prácticas favorece la confiabilidad de la información contable y la continuidad de las operaciones organizacionales.

1.2.7. Tecnologías emergentes y blockchain

En el contexto de la transformación digital, la seguridad de la información contable ha evolucionado significativamente gracias a la incorporación de tecnologías emergentes que permiten optimizar los procesos de control, protección y análisis de datos financieros (Alzate et al., 2023). Estas tecnologías no solo mejoran la eficiencia operativa, sino que

también contribuyen a la mitigación de riesgos asociados al manejo de información sensible (D'Anna et al., 2023).

Entre las principales tecnologías se encuentra la inteligencia artificial (IA), la cual permite analizar grandes volúmenes de datos en tiempo real, facilitando la detección de anomalías, fraudes y patrones de riesgo en los sistemas contables. Mediante técnicas de aprendizaje automático, la IA fortalece los procesos de auditoría y mejora la toma de decisiones financieras (Alzate et al., 2023).

Por su parte, el big data posibilita la gestión y análisis de grandes cantidades de información estructurada y no estructurada, lo que contribuye a una mayor precisión en los informes financieros y en la identificación de vulnerabilidades dentro de los sistemas de información contable (Singh, 2025).

La computación en la nube (cloud computing) representa una solución eficiente para el almacenamiento y acceso remoto a la información contable, permitiendo mayor flexibilidad, escalabilidad y reducción de costos operativos. No obstante, esta tecnología también introduce riesgos relacionados con la privacidad, la confidencialidad y la integridad de los datos, lo que exige la implementación de controles de seguridad adecuados (Alharbi et al., 2021).

Asimismo, la tecnología blockchain ha emergido como una herramienta clave para garantizar la integridad, trazabilidad y transparencia de la información contable, debido a su estructura descentralizada e inmutable, que dificulta la manipulación de registros financieros (Kissoon, 2024).

Finalmente, las soluciones de ciberseguridad avanzada, como el cifrado de datos, la autenticación multifactor y los sistemas de detección de intrusos, permiten proteger la información contable frente a amenazas digitales cada vez más sofisticadas, fortaleciendo los mecanismos de control interno y la confiabilidad de los sistemas (Whitman y Mattord, 2022).

En conjunto, estas tecnologías emergentes no solo optimizan la gestión de la información contable, sino que también fortalecen los sistemas de control y seguridad, contribuyendo a la reducción de riesgos en entornos digitales complejos (Alzate et al., 2023).

Dentro de estas tecnologías, blockchain destaca por una tecnología de registro distribuido que permite almacenar información de manera descentralizada, segura e inmutable mediante el uso de bloques enlazados criptográficamente (Dai y Vasarhelyi, 2017).

En el ámbito contable, esta tecnología fortalece la integridad y trazabilidad de la información financiera, al garantizar que los registros no puedan ser alterados sin dejar evidencia.

Su aplicación en los sistemas de información contable contribuye a mejorar la confiabilidad de los datos y a reforzar los procesos de control y auditoría.

1.3 Estado del arte

El estado del arte presenta una revisión crítica de estudios nacionales e internacionales relacionados con ciberseguridad en sistemas de información contable en entornos digitales. A partir del análisis de 35 artículos científicos seleccionados, se examinan los principales enfoques teóricos, riesgos identificados, prácticas implementadas y vacíos investigativos existentes en la literatura.

En este sentido, el estado del arte no solo describe los aportes previos, sino que permite comprender cómo ha evolucionado el estudio de la seguridad de la información contable, identificando tendencias relevantes y limitaciones que justifican el desarrollo de la presente investigación.

1.3.1 Seguridad de la información contable en entornos digitales

La revisión de los estudios evidencia un creciente interés por el análisis de la ciberseguridad en el contexto de la digitalización de los sistemas contables. En particular, se observa que una proporción significativa de los artículos analizados se enfoca en la identificación de riesgos asociados a entornos tecnológicos interconectados.

Hall (2016) señala que la evolución de los sistemas de información hacia plataformas digitales ha incrementado la exposición a amenazas, lo que exige el fortalecimiento de los controles de seguridad. Este planteamiento es reforzado por Shahid et al. (2022), quienes destacan que la adopción de tecnologías como la computación en la nube ha ampliado la superficie de ataque, incrementando la probabilidad de incidentes como accesos no autorizados, pérdida de información y ataques informáticos.

Asimismo, varios estudios coinciden en que la ciberseguridad debe integrarse dentro de la gestión organizacional. Macías et al. (2020) plantean que la seguridad de la información no puede ser abordada únicamente desde una perspectiva tecnológica, sino que debe considerarse como un componente estratégico que involucra procesos, personas y tecnología.

. En esta misma línea,(Kavak et al., 2021), plantean que la ciberseguridad debe integrarse a la gestión organizacional para enfrentar tanto amenazas externas como riesgos internos.

No obstante, el análisis de los 35 artículos revela una tendencia importante: aunque existe un amplio desarrollo teórico en ciberseguridad, son limitados los estudios que abordan de manera específica su impacto en la información contable. Esta falta de articulación evidencia un vacío en la literatura, ya que la mayoría de las investigaciones analizan la seguridad digital de forma general, sin profundizar en su relación directa con la confiabilidad de los datos financieros.

1.3.2. Riesgos más estudiados en la literatura

En relación con los riesgos cibernéticos, la literatura revisada muestra una alta coincidencia en torno a las principales amenazas que afectan a los sistemas de información contable.

Los estudios analizados identifican como riesgos predominantes el phishing, malware, ransomware y ataques de denegación de servicio, los cuales impactan directamente la confidencialidad, integridad y disponibilidad de la información (Shahid et al., 2022). Estos riesgos se ven potenciados por la creciente digitalización y la interconectividad de los sistemas.

Sin embargo, los hallazgos evidencian que los riesgos no se limitan al ámbito tecnológico, ya que un número considerable de artículos destaca la presencia de vulnerabilidades organizacionales, tales como la falta de políticas de seguridad, debilidad en los controles internos y una gestión inadecuada de accesos (Faccia&Petratos, 2021). Estas condiciones incrementan la probabilidad de incidentes y reflejan deficiencias en la gobernanza de la seguridad de la información.

De igual manera, el factor humano se posiciona como una de las principales fuentes de riesgo. Diversos estudios señalan que la falta de capacitación y concienciación en ciberseguridad incrementa significativamente la vulnerabilidad de los sistemas. En este sentido, investigaciones recientes evidencian que incluso mecanismos avanzados, como la autenticación multifactor, pueden resultar insuficientes cuando los usuarios no cuentan con la formación adecuada (Nobanee et al., 2023).

Adicionalmente, se identifican riesgos técnicos asociados a la falta de actualización de sistemas, configuraciones incorrectas y debilidades en las infraestructuras digitales, los cuales son considerados críticos en entornos tecnológicos complejos (Zhang et al., 2021).

En conjunto, estos resultados reflejan que los riesgos en los sistemas de información contable responden a una interacción entre factores tecnológicos, organizacionales y humanos, lo que evidencia la necesidad de un enfoque integral de gestión de la seguridad.

1.3.3 Buenas prácticas reportadas

En respuesta a los riesgos identificados, la literatura propone diversas buenas prácticas orientadas a fortalecer la seguridad de la información contable. A partir del análisis de los artículos seleccionados, se evidencia que estas prácticas han evolucionado hacia enfoques integrales, los cuales combinan dimensiones tecnológicas, organizacionales y humanas para una gestión más efectiva de la ciberseguridad.

Uno de los aspectos más relevantes identificados en la literatura es la inversión estratégica en ciberseguridad, concebida como un elemento clave para fortalecer la resiliencia organizacional frente a amenazas digitales. En este sentido, Azrour y Mabrouki (2025) señalan que una adecuada asignación de recursos permite optimizar la protección de los sistemas, priorizando la implementación de controles en función del nivel de riesgo.

No obstante, los estudios revisados coinciden en que dicha inversión trasciende la simple adquisición de herramientas tecnológicas, abarcando también la implementación de infraestructuras seguras, la actualización continua de los sistemas, la incorporación de personal especializado y el fortalecimiento de capacidades internas en materia de ciberseguridad. En este sentido, Romney y Steinbart (2021), destacan que la integración de la seguridad dentro de la planificación estratégica permite reducir significativamente la exposición a amenazas.

(Monteiro&Cepêda, 2021) mencionan que, la capacitación del personal y la concienciación en ciberseguridad se consolidan como prácticas fundamentales. Los artículos analizados coinciden en que el fortalecimiento de las competencias del talento humano reduce la probabilidad de errores operativos y accesos no autorizados.

De igual manera, se identifican prácticas relacionadas con la implementación de marcos normativos y políticas de seguridad, las cuales permiten estructurar la gestión de la seguridad de la información de manera sistemática (Sánchez-García et al., 2024).

Finalmente, el uso de tecnologías avanzadas, como la inteligencia artificial y los sistemas de monitoreo continuo, se posiciona como una tendencia emergente para la detección y prevención de amenazas en tiempo real (Shahid et al., 2022).

1.3.4 Tecnologías emergentes y vacíos de investigación

Las tecnologías emergentes han transformado significativamente el enfoque de la ciberseguridad en los sistemas de información contable. En particular, el uso de inteligencia artificial, aprendizaje automático y análisis predictivo ha permitido mejorar la capacidad de detección de amenazas y la respuesta ante incidentes (Alzate et al., 2023).

Asimismo, el Internet de las Cosas (IoT) introduce nuevos desafíos en la protección de datos, debido a la interconexión de múltiples dispositivos que generan y comparten información en tiempo real. Zhang et al. (2021), destacan que estos entornos presentan vulnerabilidades significativas en la transmisión y almacenamiento de datos.

Existen importantes vacíos en la literatura. En primer lugar, se observa una escasez de estudios empíricos aplicados a pequeñas y medianas empresas, especialmente en países en desarrollo, donde las limitaciones tecnológicas y financieras dificultan la implementación de medidas de seguridad (Alzate et al., 2023).

En segundo lugar, se identifica una limitada investigación sobre la aplicación específica de tecnologías emergentes en los sistemas de información contable, ya que la mayoría de los estudios aborda estas herramientas desde una perspectiva general (Giang&Tam, 2023).

Otro vacío relevante corresponde a la falta de modelos prácticos de implementación adaptados a contextos organizacionales reales, lo que limita la transferencia del conocimiento teórico hacia la práctica empresarial (Romney y Steinbart, 2021).

Finalmente, se evidencia una insuficiente producción científica en contextos latinoamericanos, lo que limita la comprensión de las particularidades regionales en materia de ciberseguridad contable.

2. Metodología

La presente investigación se desarrolló bajo un enfoque cualitativo, descriptivo y documental.,

El método empleado correspondió a una revisión bibliográfica con enfoque de mapeo de la literatura (literature mapping), el cual resulta pertinente cuando se busca identificar y describir, de manera amplia, las principales líneas de investigación, enfoques teóricos, riesgos y prácticas abordadas dentro de un campo específico del conocimiento. Este tipo de revisión permite estructurar el conocimiento existente, reconocer tendencias investigativas y evidenciar vacíos en la literatura, proporcionando una visión integral del estado del arte.

Para el desarrollo de la revisión, se llevó a cabo una búsqueda sistemática de información en diversas fuentes académicas, tales como artículos científicos, capítulos de libros, informes técnicos y normativas vigentes, relacionados con la ciberseguridad y los sistemas de información contable. Las fuentes fueron seleccionadas en función de su pertinencia temática, rigor metodológico y relevancia académica, priorizando aquellos

estudios que abordan la protección de la información financiera en contextos digitales y organizacionales.

El análisis de la información se realizó mediante un proceso de lectura crítica, clasificación temática y síntesis cualitativa, lo que permitió agrupar los estudios en función de los principales ejes de discusión identificados en la literatura. Posteriormente, se efectuó una comparación de los enfoques teóricos y de las prácticas reportadas, con el fin de identificar coincidencias, divergencias y aportes relevantes, contribuyendo así a una comprensión estructurada y coherente de la seguridad de la información contable en entornos digitales.

2.1. Estrategia de búsqueda y recuperación de información

La identificación de los artículos científicos utilizados en el análisis se realizó mediante la aplicación de cadenas de búsqueda estructuradas en bases de datos académicas de alto impacto, con el propósito de garantizar la trazabilidad, calidad y pertinencia de las fuentes seleccionadas. Este procedimiento permitió recuperar información relevante de manera sistemática y replicable, evitando sesgos asociados a una selección arbitraria de la literatura.

Las principales bases de datos empleadas fueron Scopus, Web of Science, IEEE Xplore y SpringerLink, seleccionadas por su amplia cobertura en áreas como contabilidad, sistemas de información, auditoría y ciberseguridad.

Para la búsqueda, se diseñaron cadenas de palabras clave combinadas mediante operadores booleanos (AND, OR), las cuales fueron aplicadas en los campos de título, resumen y palabras clave de cada base de datos. Entre las principales cadenas de búsqueda utilizadas se incluyen:

Tabla 1 ***Cadenas de búsquedas***

BIBLIOTECA	CADENA DE BÚSQUEDA
Scopus	TITLE-ABS-KEY (CYBER RISK) AND PUBYEAR > 2018 AND PUBYEAR < 2027 AND PUBYEAR > 2018 AND PUBYEAR < 2027 AND (LIMIT-TO (EXACTKEYWORD , "Cybersecurity") OR LIMIT-TO (EXACTKEYWORD , "Blockchain")) AND (LIMIT-TO (SUBJAREA , "COMP") OR LIMIT-TO (SUBJAREA , "BUSI") OR LIMIT-TO (SUBJAREA , "ECON")) AND (LIMIT-TO (DOCTYPE , "re") OR LIMIT-TO (DOCTYPE , "bk")) AND (LIMIT-TO (SRCTYPE , "j") OR LIMIT-TO (SRCTYPE , "b"))
Web of science	TS=(("accounting information system*" OR AIS) AND (cybersecurity OR "cyber risk*" OR cyberrisk* OR "information security" OR blockchain OR "distributed ledger technolog*"))
IEEE	(("Accounting") AND ("Blockchain" OR "Artificial Intelligence" OR "Smart Contracts") AND ("Security")) Filters Applied: Journals2015 - 2026
SPRINGER	ACCOUNTING INFORMATION SYSTEMS AND CYBERSECURITY

Estas cadenas permitieron recuperar estudios relacionados con los sistemas contables digitales, los riesgos cibernéticos y las prácticas de seguridad de la información en entornos organizacionales.

Criterios de inclusión y exclusión

Para garantizar la calidad y pertinencia de la literatura analizada se establecieron los siguientes criterios:

Criterios de Inclusión:

- Estudios centrados en el tema de investigación.
- Publicaciones en idioma español e inglés.
- Documentos publicados entre 2015 y 2025
- Artículos, capítulos de libro, informes técnicos.

Criterios de Exclusión:

- Publicaciones duplicadas o sin acceso completo al texto
- Trabajos previos a 2015.
- Literatura sin respaldo técnico.
- Tesis de grado y posgrado.

2.2. Resultados de la búsqueda inicial

La aplicación de las cadenas de búsqueda permitió identificar un conjunto inicial de publicaciones científicas en las diferentes bases de datos consultadas.

Estos resultados representan el universo inicial de literatura científica vinculada con el tema de estudio.

2.3. Formulación de preguntas de clasificación

Con el propósito de organizar y analizar de manera sistemática la literatura científica recopilada, se formularon un conjunto de preguntas de clasificación, las cuales fueron diseñadas en función del objetivo general y los objetivos específicos de la investigación. Estas preguntas permitieron evaluar la pertinencia de los artículos identificados y clasificar aquellos estudios que aportan información relevante para el desarrollo del estudio.

En este sentido, cada artículo recuperado fue revisado a partir de su título, resumen y palabras clave, con el fin de determinar si respondía a las preguntas planteadas y si su contenido contribuía al cumplimiento de los objetivos del estudio. Aquellos artículos que presentaban una relación directa con el tema de seguridad de la información, ciberseguridad o riesgos digitales en sistemas de información contable fueron seleccionados para el análisis.

Por el contrario, los documentos que no abordaban estos aspectos o que se alejaban del enfoque de la investigación fueron excluidos del proceso de análisis.

De esta manera, las preguntas de clasificación permitieron filtrar, organizar y categorizar los artículos seleccionados, garantizando que el análisis bibliográfico se centre únicamente en estudios que aportan evidencia relevante para el cumplimiento del objetivo de la investigación.

2.4. Preguntas de clasificación utilizadas

Las preguntas de clasificación que orientan la presente revisión bibliográfica se estructuran en torno a tres ejes fundamentales. En primer lugar, se busca identificar cuáles son los principales riesgos de seguridad que afectan a la información financiera en los sistemas contables digitales, con el propósito de comprender las vulnerabilidades más recurrentes reportadas en la literatura académica. En segundo lugar, se analizan las buenas prácticas de ciberseguridad implementadas por las organizaciones para proteger la información contable en entornos digitales, permitiendo reconocer estrategias efectivas aplicadas en distintos contextos. Finalmente, se examinan las recomendaciones propuestas por la literatura científica para fortalecer la seguridad de la información contable en sistemas contables digitalizados, con el fin de establecer lineamientos que contribuyan a mejorar la protección, confiabilidad e integridad de los datos financieros en la era digital.

2.5. Proceso de selección de artículos

Una vez obtenidos los resultados de la búsqueda, los registros fueron revisados con base en los títulos, resúmenes y palabras clave para verificar su pertinencia con el tema de investigación. De esta manera, el mapeo bibliográfico se desarrolló a partir de un conjunto final de 35 artículos científicos, los cuales fueron analizados para identificar los principales enfoques, riesgos cibernéticos, tecnologías emergentes y buenas prácticas relacionadas con la seguridad de la información en sistemas de información contable.

Tabla 2 ***Artículos seleccionados por biblioteca***

Bibliotecas	**Artículos Identificados**	**Artículos duplicados**	**Selección de artículos**		**Total Artículos**
			SI	**NO**	
Scopus	318	1	12	305	12
Web of Science	152	1	17	134	17
IEEE Xplore	87	0	5	82	5
SpringerLink	74	0	1	73	1
Total	**631**	**2**	**35**	**594**	**35**

Nota: elaboración propia

3. RESULTADOS

En la presente sección se exponen los resultados derivados del análisis de los 35 artículos El análisis permitió identificar patrones recurrentes en torno a los riesgos de seguridad, las buenas prácticas y las recomendaciones orientadas a la protección de la información contable en entornos digitales.

3.1 ¿Cuáles son los principales riesgos de seguridad en los sistemas de información contable?

Los resultados evidencian que los riesgos asociados a la seguridad de la información contable presentan una distribución relativamente equilibrada entre factores tecnológicos, organizacionales y humanos, lo que confirma la naturaleza multidimensional de la ciberseguridad en entornos digitales. Este hallazgo es consistente con lo planteado por Weigand et al. (2020), quienes sostienen que la seguridad de la información debe abordarse desde un enfoque integral que articule tecnología, procesos y comportamiento humano.

Como se observa en la Figura 1, el 27,59% de los estudios identifica la vulnerabilidad de la seguridad como el principal riesgo. Este resultado se asocia con debilidades en la implementación de controles internos y mecanismos de protección en los sistemas contables. En este sentido, (Li&Jiang, 2025) señalan que la ausencia de controles adecuados incrementa significativamente la exposición a vulnerabilidades, especialmente en entornos digitalizados donde la información es accesible de forma remota. De manera complementaria, Ramos et al. (2024), destacan que los sistemas de información contable requieren controles robustos para garantizar la integridad, confiabilidad y disponibilidad de la información financiera.

Por su parte, el 25,00% de los artículos analizados identifica las amenazas cibernéticas como uno de los riesgos más relevantes (Alawida et al., 2025). Estas incluyen ataques como phishing, malware, ransomware y accesos no autorizados, los cuales afectan directamente la confidencialidad, integridad y disponibilidad de la información financiera. Según Saeed et al. (2023), el crecimiento de los sistemas interconectados ha ampliado la superficie de ataque, facilitando la explotación de vulnerabilidades tecnológicas por parte de ciberdelincuentes. En la misma línea, Moll & Yigitbasioglu, (2019), sostienen que la evolución de las amenazas digitales ha incrementado su complejidad y sofisticación, lo que exige la implementación de mecanismos de defensa más avanzados.

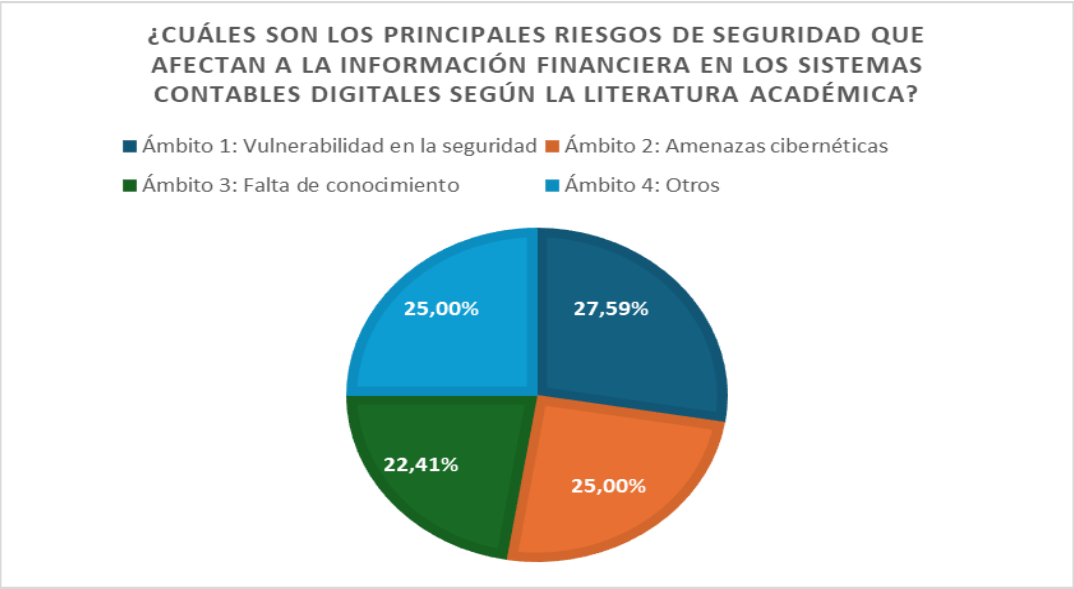
Otro 25,00% corresponde a la categoría de otros riesgos, donde se incluyen factores como fallas en la infraestructura tecnológica, problemas de interoperabilidad y deficiencias en

la gestión de sistemas. Estos resultados coinciden con lo expuesto por Giang y Tam (2023), quienes destacan que la falta de actualización de sistemas y las configuraciones incorrectas constituyen riesgos críticos en entornos digitales. Asimismo, Boonkrong (2021), enfatiza que la creciente complejidad de los sistemas contables digitales incrementa la probabilidad de errores estructurales y vulnerabilidades técnicas cuando no se gestionan adecuadamente.

Finalmente, el 22,41% de los estudios enfatiza la falta de conocimiento en ciberseguridad, evidenciando el impacto del factor humano en la generación de incidentes. En esta línea, Powell (2025), demuestra que incluso mecanismos avanzados de autenticación pueden ser vulnerables cuando los usuarios no cuentan con la formación adecuada. Este planteamiento es reforzado por Cele y Kwenda (2025), quienes sostienen que el factor humano continúa siendo uno de los principales puntos críticos en la seguridad de los sistemas contables, debido a errores operativos, negligencia y falta de capacitación.

En conjunto, estos hallazgos evidencian que los riesgos de seguridad en los sistemas de información contable no pueden ser abordados de manera aislada, sino que requieren un enfoque integral que considere simultáneamente las dimensiones tecnológica, organizacional y humana, lo cual coincide con las tendencias actuales en la literatura sobre ciberseguridad.

Figura 1: *Principales riesgos de seguridad en sistemas de información contable*



Nota: Elaboración propia

En conjunto, estos resultados evidencian que los riesgos no se limitan a factores tecnológicos, sino que también incluyen dimensiones organizacionales y humanas, lo que requiere un enfoque integral para su gestión.

3.2 ¿Cuáles son las principales buenas prácticas de ciberseguridad en sistemas contables?

Los resultados obtenidos evidencian que las buenas prácticas de ciberseguridad en los sistemas de información contable se estructuran en torno a tres ejes fundamentales: la gestión del factor humano, la protección tecnológica de los datos y el fortalecimiento de la gobernanza organizacional. Este enfoque integral refleja una evolución en la literatura hacia modelos de seguridad más holísticos y adaptativos.

De acuerdo con la Figura 2, el 28,57% de los estudios destaca la capacitación en ciberseguridad como la práctica más relevante. Este hallazgo demuestra que el fortalecimiento de las competencias del talento humano constituye un elemento clave en la prevención de incidentes. En este sentido, Giordano (2017), evidencia que los programas de concienciación en seguridad reducen significativamente los comportamientos de riesgo en los usuarios. De manera complementaria, (Ghadge et al., 2019), sostiene que los errores humanos y las malas prácticas en el uso de tecnologías continúan siendo una de las principales causas de vulnerabilidades en los sistemas digitales.

En segundo lugar, el 27,62% de los artículos enfatiza la protección de datos contables mediante la implementación de controles tecnológicos avanzados. En este contexto, Kshetri (2016) señala que el uso de cifrado, autenticación multifactor y sistemas de control de acceso permite mitigar riesgos asociados a la exposición de información sensible. También, (Parambil et al., 2024), destaca que la adecuada gestión de accesos y privilegios es fundamental para prevenir filtraciones de información y garantizar la integridad de los sistemas contables.

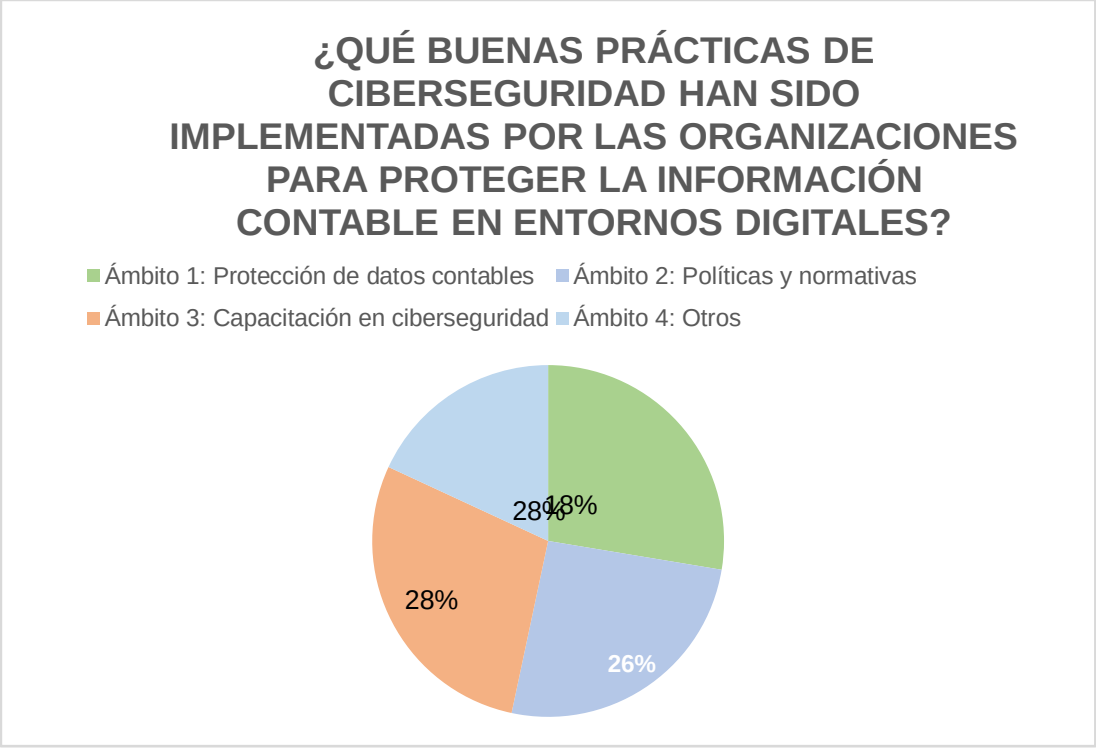
Por su parte, el 25,71% de los estudios resalta la importancia de las políticas y normativas como eje central de la ciberseguridad. En esta línea, Kissoon (2024), argumenta que la implementación de políticas formales de seguridad permite establecer lineamientos claros para la protección de la información y la gestión de riesgos. De igual manera, Das (2024), sostiene que los sistemas de gestión de seguridad basados en estándares internacionales contribuyen a mejorar la capacidad organizacional para prevenir y responder a incidentes.

Finalmente, el 18,10% corresponde a otras prácticas, entre las cuales se incluyen auditorías de seguridad, monitoreo continuo y uso de tecnologías emergentes. En este sentido, Moll - Yigitbasioglu (2019), destacan que las auditorías permiten identificar vulnerabilidades y evaluar la efectividad de los controles implementados. Asimismo,

Boss et al. (2022), señalan que el monitoreo continuo es esencial para detectar amenazas en tiempo real y fortalecer la capacidad de respuesta ante incidentes.

En conjunto, estos resultados evidencian que las buenas prácticas de ciberseguridad en los sistemas de información contable han evolucionado hacia un enfoque integral, en el cual la interacción entre tecnología, gestión organizacional y comportamiento humano resulta fundamental para garantizar la protección de la información en entornos digitales cada vez más complejos.

Figura 2*: Buenas prácticas de ciberseguridad en sistemas contables*



Nota: Elaboración propia

Estos resultados reflejan que la ciberseguridad en los sistemas contables requiere no solo de herramientas tecnológicas, sino también de una adecuada gestión organizacional y formación continua del personal.

3.3 ¿Cuáles son las principales recomendaciones para fortalecer la seguridad de la información contable?

Los resultados muestran que la literatura científica propone diversas recomendaciones orientadas a fortalecer la seguridad de la información contable, las cuales se agrupan en tres dimensiones principales: tecnológica, organizacional y formativa. Este enfoque evidencia que la protección de los sistemas contables requiere estrategias integrales que respondan a la complejidad de los entornos digitales actuales.

Como se observa en la Figura 3, el 27,45% de los estudios plantea recomendaciones tecnológicas, centradas en la implementación de herramientas avanzadas de seguridad,

como sistemas de cifrado, inteligencia artificial y soluciones de monitoreo. En este sentido, (Burchi et al., 2025b), destacan que el uso de inteligencia artificial permite detectar patrones anómalos y prevenir fraudes en tiempo real. De manera complementaria, (Ulven&Wangen, 2021), señalan que la incorporación de tecnologías emergentes fortalece la capacidad predictiva de los sistemas, permitiendo anticipar amenazas y mejorar la toma de decisiones en materia de seguridad.

En segundo lugar, el 26,47% de los artículos propone recomendaciones organizacionales, orientadas al fortalecimiento de los controles internos y la gestión del riesgo. En este contexto, el Committee of Sponsoring Organizations of the Treadway Commission (COSO, 2017) establece que la integración de la gestión de riesgos en los procesos organizacionales permite mejorar la capacidad de respuesta frente a amenazas y reducir la incertidumbre en entornos digitales. Asimismo, (Powell, 2025), sostiene que una adecuada estructura de control interno facilita la implementación de políticas de seguridad coherentes y alineadas con los objetivos estratégicos de la organización.

De igual manera, otro 26,47% enfatiza las recomendaciones formativas, destacando la importancia de la capacitación continua del personal. En esta línea, (P. Wang et al., 2025) afirma que el comportamiento del usuario influye directamente en la seguridad de los sistemas, por lo que la formación en ciberseguridad resulta clave para reducir riesgos asociados a errores humanos. De forma similar, (Monteiro&Cepêda, 2021), evidencian que los programas de concienciación contribuyen significativamente a mejorar las prácticas de seguridad dentro de las organizaciones.

Finalmente, el 19,61% de los estudios incluye otras recomendaciones, entre las que se destacan la adopción de tecnologías emergentes como blockchain y la implementación de modelos de auditoría continua. En este sentido, (Desolda et al., 2022), argumentan que el uso de blockchain en los sistemas contables permite garantizar la integridad, trazabilidad y transparencia de la información financiera. Desde este modo, Moll & Yigitbasioglu (2019), señalan que la auditoría continua mejora el control sobre los procesos contables, permitiendo detectar irregularidades de manera oportuna.

En conjunto, estos resultados evidencian que las recomendaciones para fortalecer la seguridad de la información contable no se limitan a la implementación de herramientas tecnológicas, sino que requieren un enfoque integral que articule innovación, gestión organizacional y desarrollo de capacidades humanas, con el fin de garantizar la protección de la información en entornos digitales cada vez más complejos.

Figura 3: *Recomendaciones para fortalecer la seguridad de la información contable*

Nota: Elaboración propia

En conjunto, los resultados muestran que las recomendaciones se orientan hacia un enfoque integral que combine tecnología, gestión organizacional y formación, con el fin de garantizar una protección efectiva de la información contable en entornos digitales.

4. Discusión

4.1 Interpretación de resultados

Los resultados obtenidos permiten afirmar que la seguridad de la información contable en entornos digitales constituye un fenómeno complejo, dinámico y multidimensional, caracterizado por la interacción constante entre factores tecnológicos, organizacionales y humanos. Esta interpretación se alinea con los enfoques contemporáneos de la ciberseguridad, que destacan la necesidad de abordar los riesgos desde una perspectiva sistémica e integrada (Desolda et al., 2022).

En relación con los riesgos identificados, se evidencia que las vulnerabilidades en los sistemas de información contable representan el principal foco de exposición, lo que sugiere la existencia de debilidades en los controles internos y en la arquitectura tecnológica. Este hallazgo coincide con lo planteado por (Cram et al., 2023), quienes sostienen que los sistemas contables digitalizados requieren mecanismos de control más robustos para garantizar la confiabilidad de la información financiera. En este contexto, la digitalización, si bien ha optimizado la eficiencia operativa, también ha incrementado

la superficie de ataque, generando nuevas oportunidades para la explotación de vulnerabilidades (Zheng et al., 2018).

En cuanto a las amenazas cibernéticas, los resultados reflejan su creciente sofisticación y frecuencia, lo que confirma la transición hacia un entorno de riesgo más complejo. Este escenario es consistente con lo expuesto por Saeed et al. (2023), quienes señalan que los ataques informáticos han evolucionado desde esquemas simples hacia modelos altamente estructurados y difíciles de detectar. De manera similar, Alawida et al. (2025), destacan que el incremento de ataques como ransomware y phishing está directamente relacionado con la expansión de los sistemas interconectados.

Un aspecto particularmente relevante es la incidencia del factor humano, identificado como una de las principales fuentes de riesgo. Este resultado refuerza la idea de que la seguridad de la información no depende únicamente de soluciones tecnológicas, sino también de la conducta de los usuarios. En esta línea, Weigand et al. (2020), demuestra que los comportamientos inseguros y la falta de concienciación incrementan significativamente la probabilidad de incidentes de seguridad. Esta evidencia sugiere que la gestión de la ciberseguridad debe incorporar estrategias formativas que fortalezcan las competencias del personal.

En relación con las buenas prácticas, los hallazgos evidencian una evolución hacia enfoques integrales, en los que la capacitación del personal, la protección de datos y la implementación de políticas organizacionales se posicionan como pilares fundamentales. Este resultado coincide con (Parambil et al., 2024), quienes señalan que los programas de formación en seguridad reducen significativamente los comportamientos de riesgo. De igual forma, Badhwar (2021), sostiene que la implementación de sistemas de gestión de seguridad basados en estándares internacionales mejora la capacidad organizacional para prevenir incidentes.

Por otra parte, las recomendaciones identificadas en la literatura refuerzan la necesidad de integrar tecnologías avanzadas dentro de los sistemas de seguridad. La incorporación de inteligencia artificial y análisis predictivo, por ejemplo, permite anticipar amenazas y mejorar la capacidad de respuesta (Zhang&Zhou, 2020). Esta tendencia evidencia un cambio hacia modelos de ciberseguridad más proactivos y basados en datos.

En conjunto, la interpretación de los resultados permite concluir que la seguridad de la información contable ha evolucionado desde un enfoque técnico hacia una visión estratégica e integral, en la que la articulación entre tecnología, gestión organizacional y

comportamiento humano resulta determinante para enfrentar los desafíos de los entornos digitales contemporáneos.

4.2 Comparación de similitudes y diferencias entre los artículos

El análisis comparativo de los estudios revisados permite identificar patrones de convergencia y divergencia que enriquecen la comprensión del fenómeno estudiado.

En cuanto a las similitudes, existe un consenso en la literatura respecto a la relevancia de las amenazas cibernéticas como uno de los principales riesgos para los sistemas de información contable. Diversos autores coinciden en que ataques como el phishing, ransomware y malware representan amenazas críticas que comprometen la confidencialidad y disponibilidad de la información (Wang et al., 2025). Esta coincidencia refleja una preocupación global por el impacto de la cibercriminalidad en los entornos digitales.

De igual manera, se identifica una convergencia significativa en torno al papel del factor humano. La mayoría de los estudios coincide en que los errores humanos, la falta de capacitación y la baja concienciación constituyen una de las principales fuentes de vulnerabilidad (Parambil et al., 2024). Este consenso refuerza la necesidad de incorporar estrategias formativas dentro de los modelos de ciberseguridad.

En relación con las buenas prácticas, los artículos analizados coinciden en la importancia de implementar controles tecnológicos, tales como cifrado de datos, autenticación multifactor y monitoreo continuo. Estos mecanismos son considerados esenciales para la protección de la información en entornos digitales (Radanliev et al., 2021). A esto se suma la coincidencia en la relevancia de las políticas organizacionales y los marcos normativos como elementos estructurales de la gestión de la seguridad (Cram et al., 2023).

No obstante, se identifican diferencias importantes en el enfoque de los estudios. Algunos autores priorizan una perspectiva tecnológica, centrada en el desarrollo de herramientas avanzadas de seguridad, mientras que otros adoptan un enfoque organizacional, orientado a la gestión del riesgo y el fortalecimiento del control interno. Esta diversidad refleja la complejidad del fenómeno y la necesidad de abordarlo desde múltiples perspectivas.

También se observan diferencias en función del contexto geográfico y económico. Los estudios desarrollados en países con mayor nivel de digitalización tienden a enfocarse en tecnologías emergentes, como inteligencia artificial y blockchain (Das, 2024), mientras que las investigaciones en países en desarrollo destacan limitaciones relacionadas con recursos, infraestructura y capacidades técnicas (Al-Okaily, 2025).

Finalmente, existen posturas divergentes respecto al impacto de las tecnologías emergentes. Mientras algunos estudios resaltan su potencial para fortalecer la seguridad, otros advierten sobre los nuevos riesgos asociados a su implementación, como la complejidad técnica y la aparición de nuevas vulnerabilidades.

4.3 Limitaciones de la investigación

La presente investigación presenta diversas limitaciones que deben ser consideradas al interpretar los resultados obtenidos.

En primer lugar, el análisis se basa en una muestra de 35 artículos, lo cual, aunque permite identificar tendencias relevantes, puede limitar la generalización de los hallazgos. En segundo lugar, se observa una predominancia de estudios en contextos internacionales, con una limitada representación de investigaciones en América Latina, lo que restringe la comprensión de las particularidades regionales.

Otra limitación importante radica en el carácter predominantemente teórico de muchos de los estudios revisados, lo que dificulta evaluar la aplicabilidad práctica de las recomendaciones propuestas. Esta situación evidencia la necesidad de desarrollar investigaciones empíricas que permitan validar los modelos teóricos en contextos reales.

Adicionalmente, la rápida evolución de las tecnologías digitales representa un desafío para la vigencia de los hallazgos, ya que las amenazas y soluciones en ciberseguridad cambian constantemente. Por último, la diversidad metodológica de los estudios analizados introduce variabilidad en los resultados, lo que puede dificultar la comparación directa entre investigaciones.

5. Conclusiones

La presente investigación tuvo como objetivo analizar de manera crítica la literatura académica relacionada con la seguridad de la información contable en entornos digitales, con el propósito de identificar los principales riesgos, así como las estrategias y medidas preventivas implementadas para garantizar la integridad, confidencialidad y disponibilidad de la información financiera.

En relación con el primer objetivo específico, orientado a analizar los principales riesgos de seguridad de la información financiera en los sistemas contables, se concluye que dichos riesgos presentan una naturaleza multidimensional, en la que interactúan factores tecnológicos, organizacionales y humanos. Entre los más relevantes se identifican las vulnerabilidades en los sistemas, las amenazas cibernéticas como phishing, malware y ransomware y las deficiencias en el conocimiento de ciberseguridad por parte del personal. Este hallazgo evidencia que la exposición al riesgo no depende exclusivamente

de la infraestructura tecnológica, sino también de la gestión organizacional y del comportamiento de los usuarios dentro de los sistemas digitales.

En cuanto al segundo objetivo, enfocado en identificar las buenas prácticas de ciberseguridad implementadas por las organizaciones, se determina que la literatura ha evolucionado hacia enfoques integrales que combinan la protección tecnológica de los datos, el fortalecimiento de políticas y normativas, y el desarrollo de capacidades en el talento humano. En este contexto, prácticas como el cifrado de la información, la autenticación multifactor, la implementación de marcos normativos y la capacitación continua del personal se consolidan como pilares fundamentales para reducir la exposición a riesgos y mejorar la seguridad de los sistemas contables.

Respecto al tercer objetivo, relacionado con el establecimiento de recomendaciones para fortalecer la seguridad contable digitalizada, se concluye que las estrategias más efectivas se orientan hacia la integración de tecnologías emergentes, el fortalecimiento de los sistemas de control interno y la implementación de programas formativos permanentes. La incorporación de herramientas como inteligencia artificial, sistemas de monitoreo continuo y modelos de auditoría digital permite mejorar la capacidad de detección y respuesta frente a amenazas, mientras que la formación del personal contribuye a mitigar riesgos asociados al factor humano.

De manera general, los resultados del estudio evidencian que la seguridad de la información contable en entornos digitales requiere un enfoque integral, estratégico y adaptativo, capaz de responder a la complejidad y evolución constante de los riesgos tecnológicos. En este sentido, la investigación aporta una visión estructurada que integra riesgos, prácticas y recomendaciones, contribuyendo al fortalecimiento de la gestión de la ciberseguridad en los sistemas contables.

Finalmente, se identifica la necesidad de impulsar futuras investigaciones con enfoque empírico, especialmente en contextos de países en desarrollo, donde las limitaciones tecnológicas y organizacionales pueden influir en la implementación de estrategias de ciberseguridad, lo que permitirá avanzar hacia modelos más contextualizados y aplicables a la realidad empresarial.

6. Referencias

Alawida, M., Almomani, A., & Alauthman, M. (Eds.). (2025). *Cybersecurity Insurance Frameworks and Innovations in the AI Era:* IGI Global. https://doi.org/10.4018/979-8-3373-1977-3

Alawida, M., Almomani, A., & Alauthman, M. (Eds.). (2025). *Cybersecurity Insurance Frameworks and Innovations in the AI Era:* IGI Global. https://doi.org/10.4018/979-8-3373-1977-3

Al-Okaily, M. (2025). The antecedents and outcomes of accounting information systems usage: The indirect effect of IT knowledge. *Knowledge and Information Systems*, *67*(5), 4651–4675. https://doi.org/10.1007/s10115-024-02306-0

Badhwar, R. (2021). *The CISO's Next Frontier: AI, Post-Quantum Cryptography and Advanced Security Paradigms*. Springer International Publishing. https://doi.org/10.1007/978-3-030-75354-2

Boonkrong, S. (2021). *Authentication and Access Control: Practical Cryptography Methods and Tools*. Apress. https://doi.org/10.1007/978-1-4842-6570-3

Boss, S. R., Gray, J., & Janvrin, D. J. (2022a). Accountants, Cybersecurity Isn't Just for "Techies": Incorporating Cybersecurity into the Accounting Curriculum. *Issues in Accounting Education*, *37*(3), 73–89. https://doi.org/10.2308/ISSUES-2021-001

Boss, S. R., Gray, J., & Janvrin, D. J. (2022b). Accountants, Cybersecurity Isn't Just for "Techies": Incorporating Cybersecurity into the Accounting Curriculum. *Issues in Accounting Education*, *37*(3), 73–89. https://doi.org/10.2308/ISSUES-2021-001

Burchi, A., Figà-Talamanca, G., & Musile Tanzi, P. (2025). Open banking boost and brake: An extended technology acceptance model. *International Journal of Bank Marketing*, 1–28. https://doi.org/10.1108/IJBM-03-2024-0161

Burchi, A., Figà-Talamanca, G., & Musile Tanzi, P. (2025). Open banking boost and brake: An extended technology acceptance model. *International Journal of Bank Marketing*, 1–28. https://doi.org/10.1108/IJBM-03-2024-0161

Cele, N. N., & Kwenda, S. (2025). Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review. *Journal of Financial Crime*, *32*(1), 31–48. https://doi.org/10.1108/JFC-10-2023-0263

Cele, N. N., & Kwenda, S. (2025b). Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review. *Journal of Financial Crime*, *32*(1), 31–48. https://doi.org/10.1108/JFC-10-2023-0263

Cram, W. A., Wang, T., & Yuan, J. (2023). Cybersecurity Research in Accounting Information Systems: A Review and Framework. *Journal of Emerging Technologies in Accounting*, *20*(1), 15–38. https://doi.org/10.2308/JETA-2020-081

D'Anna, G., Collier, Z. A., & Radford University. (2023). *Cybersecurity for Entrepreneurs*. SAE International. https://doi.org/10.4271/9781468605730

Das, R. (2024). *A Reference Manual for Data Privacy Laws and Cyber Frameworks* (1a ed.). CRC Press. https://doi.org/10.1201/9781003496915

Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., & Costabile, M. F. (2022). Human Factors in Phishing Attacks: A Systematic Literature Review. *ACM Computing Surveys*, *54*(8), 1–35. https://doi.org/10.1145/3469886

Faccia, A., & Petratos, P. (2021). Blockchain, Enterprise Resource Planning (ERP) and Accounting Information Systems (AIS): Research on e-Procurement and System Integration. *Applied Sciences*, *11*(15), 6792. https://doi.org/10.3390/app11156792

Ghadge, A., Weiß, M., Caldwell, N. D., & Wilding, R. (2019). Managing cyber risk in supply chains: A review and research agenda. *Supply Chain Management: An International Journal*, *25*(2), 223–240. https://doi.org/10.1108/SCM-10-2018-0357

Giang, N. P., & Tam, H. T. (2023). Impacts of Blockchain on Accounting in the Business. *Sage Open*, *13*(4), 21582440231222419. https://doi.org/10.1177/21582440231222419

Giordano, P. M. (2017). La concepción de ideología en las perspectivas funcionalistas de Talcott Parsons y Robert Merton. *Reflexión Política*, *19*(37), 136–150.

Jiménez Zavala, J. D., Riera Riera, B. A., Bárcenes Mendoza, P. M., & Alarcón Muñoz, N. E. (2018). La contabilidad y auditoría: Sistemas clave para la gestión eficiente en el sector público y privado. *Contribuciones a la economía*, *16*(3). https://go.exlibris.link/r3XqnQLP

Kavak, H., Padilla, J. J., Vernon-Bido, D., Diallo, S. Y., Gore, R., & Shetty, S. (2021). Simulation for cybersecurity: State of the art and future directions. *Journal of Cybersecurity*, *7*(1), tyab005. https://doi.org/10.1093/cybsec/tyab005

Kissoon, T. (2024). *Optimal Spending on Cybersecurity Measures: DevOps* (1a ed.). CRC Press. https://doi.org/10.1201/9781003404354

Li, S., & Jiang, G. (2025). Security and efficiency improvement of internet financial payment based on blockchain technology. *Discover Computing*, *28*(1), 305. https://doi.org/10.1007/s10791-025-09835-4

Moll, J., & Yigitbasioglu, O. (2019). The role of internet-related technologies in shaping the work of accountants: New directions for accounting research. *The British Accounting Review*, *51*(6), 100833. https://doi.org/10.1016/j.bar.2019.04.002

Monteiro, A., & Cepêda, C. (2021). Accounting Information Systems: Scientific Production and Trends in Research. *Systems*, *9*(3), 67. https://doi.org/10.3390/systems9030067

Nobanee, H., Alodat, A., Bajodah, R., Al-Ali, M., & Al Darmaki, A. (2023). Bibliometric analysis of cybercrime and cybersecurity risks literature. *Journal of Financial Crime, 30*(6), 1736–1754. https://doi.org/10.1108/JFC-11-2022-0287

Parambil, M. M. A., Rustamov, J., Ahmed, S. G., Rustamov, Z., Awad, A. I., Zaki, N., & Alnajjar, F. (2024). Integrating AI-based and conventional cybersecurity measures into online higher education settings: Challenges, opportunities, and prospects. *Computers and Education: Artificial Intelligence*, *7*, 100327. https://doi.org/10.1016/j.caeai.2024.100327

Powell, W. (2025). *The CISO 3.0: A Guide to Next-Generation Cybersecurity Leadership* (1a ed.). CRC Press. https://doi.org/10.1201/9781003510789

Radanliev, P., De Roure, D., Burnap, P., & Santos, O. (2021). Epistemological Equation for Analysing Uncontrollable States in Complex Systems: Quantifying Cyber Risks from the Internet of Things. *The Review of Socionetwork Strategies*, *15*(2), 381–411. https://doi.org/10.1007/s12626-021-00086-5

Ramesh, B., J, C., & Lin, H. (2025). *Cyber Security in Business Analytics* (1a ed.). Chapman and Hall/CRC. https://doi.org/10.1201/9781003540045

Ramos, G. P., Salcedo-Muñoz, V. E., Pacheco Molina, A. M., & Señalin Morales, L. O. (2024). Impacto de la NIC y las NIIF en los estados financieros de las empresas bananeras de la provincia El Oro. *Religación. Revista de Ciencias Sociales y Humanidades*, *9*(40), e2401185. https://doi.org/10.46652/rgn.v9i40.1185

Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., & Almuhaideb, A. M. (2023). A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience. *Sensors*, *23*(16), 7273. https://doi.org/10.3390/s23167273

Singh, T. (2025). *Digital Resilience, Cybersecurity and Supply Chains* (1a ed.). Routledge. https://doi.org/10.4324/9781003604969

Ulven, J. B., & Wangen, G. (2021). A Systematic Review of Cybersecurity Risks in Higher Education. *Future Internet*, *13*(2), 39. https://doi.org/10.3390/fi13020039

Wang, B., Gao, Y., & Wang, W. (2025). Manipulation-Resilient Pricing for Non-Fungible Tokens. *IEEE Internet of Things Journal*, 1–1. https://doi.org/10.1109/JIOT.2025.3647747

Wang, P., Boodraj, M., & Baskerville, R. (2025). Beyond passwords: A review of the hidden risks in two-factor authentication. *Journal of Systems and Information Technology*. https://doi.org/10.1108/JSIT-03-2025-0140

Weigand, H., Blums, I., & Kruijff, J. D. (2020). Shared Ledger Accounting—Implementing the Economic Exchange pattern. *Information Systems*, *90*, 101437. https://doi.org/10.1016/j.is.2019.101437

Zhang, P., & Zhou, M. (2020). Security and Trust in Blockchains: Architecture, Key Technologies, and Open Issues. *IEEE Transactions on Computational Social Systems*, *7*(3), 790–801. https://doi.org/10.1109/TCSS.2020.2990103

Zheng, B., Pan, L., & Liu, S. (2018). Mechanisms for Optimally Scheduling and Pricing Pleasingly Parallel Jobs in Service Clouds. *IEEE Access*, *6*, 73733–73749. https://doi.org/10.1109/ACCESS.2018.2882605

7. Anexos

Anexo 1. Fichaje bibliográfico:

Autores	Año	Idioma	Pregunta (1-2-3)	Resultados principales
Alawida et al.	2025	Inglés	1	El estudio evidencia que las amenazas cibernéticas han evolucionado hacia esquemas más sofisticados, incluyendo fraudes digitales y ataques dirigidos, lo que incrementa significativamente la exposición

				de los sistemas de información contable a vulnerabilidades críticas.
Al-Okaily	2025	Inglés	1	Se demuestra que el nivel de conocimiento en tecnologías de la información influye directamente en el uso adecuado y seguro de los sistemas contables, reduciendo riesgos asociados a errores operativos y fallas humanas.
Badhwar	2021	Inglés	3	Se concluye que la incorporación de inteligencia artificial y criptografía avanzada permite fortalecer los sistemas de ciberseguridad, facilitando la detección temprana de amenazas y la protección de activos digitales.
Boonkrong	2021	Inglés	2	El estudio destaca que los mecanismos de autenticación robusta y control de accesos son esenciales para garantizar la confidencialidad e integridad de la información contable en entornos digitales.
Boss et al.	2022	Inglés	2	Se evidencia que la formación en ciberseguridad dentro del ámbito contable reduce significativamente la vulnerabilidad organizacional, fortaleciendo la prevención de incidentes derivados del factor humano.
Burchi et al.	2025	Inglés	3	Se identifica que el uso de tecnologías digitales y modelos de aceptación tecnológica contribuye a mejorar la eficiencia, seguridad y confiabilidad en la gestión de información financiera.
Cram et al.	2023	Inglés	1	El análisis revela que la ciberseguridad en los sistemas contables requiere marcos estructurados que integren gestión de riesgos, control interno y tecnología para mitigar amenazas emergentes.
Das	2024	Inglés	3	Se concluye que la implementación de marcos regulatorios y normativas internacionales permite fortalecer la gobernanza de la seguridad de la información en las organizaciones.
Desolda et al.	2022	Inglés	1	El estudio demuestra que el factor humano es una de las principales causas de incidentes de seguridad, especialmente en ataques de phishing, donde influyen la falta de capacitación y conciencia digital.
Faccia&Petratos	2021	Inglés	3	Se evidencia que la implementación de blockchain en sistemas contables mejora la transparencia, trazabilidad y seguridad de la información financiera.
Giang&Tam	2023	Inglés	3	Los autores destacan que blockchain reduce significativamente los riesgos de

				manipulación de datos y fortalece la confiabilidad de los registros contables.
GTS Inc. et al.	2023	Inglés	2	El estudio señala que la gestión estratégica de la ciberseguridad permite a las organizaciones anticipar riesgos y mejorar la protección de sus sistemas digitales.
H L et al.	2025	Inglés	2	Se concluye que el uso de analítica de datos y herramientas digitales contribuye a la detección temprana de amenazas y a la toma de decisiones en seguridad.
Kavak et al.	2021	Inglés	3	Se identifica que la simulación en ciberseguridad permite modelar escenarios de riesgo y mejorar la capacidad de respuesta organizacional ante incidentes.
Kissoon	2024	Inglés	2	Se evidencia que la inversión estratégica en ciberseguridad optimiza la protección de los sistemas, reduciendo vulnerabilidades y mejorando la resiliencia organizacional.
Moll&Yigitbasioglu	2019	Inglés	2	El estudio resalta que las auditorías digitales y el uso de tecnologías emergentes fortalecen los controles internos y la transparencia contable.
Monteiro&Cepêda	2021	Inglés	2	Se concluye que la capacitación continua del personal es un elemento clave para reducir riesgos asociados a errores humanos en sistemas contables.
Nobanee et al.	2023	Inglés	1	El análisis bibliométrico evidencia un crecimiento significativo de los delitos cibernéticos, lo que incrementa la necesidad de fortalecer la seguridad digital en organizaciones.
Parambil et al.	2024	Inglés	2	Se demuestra que la integración de inteligencia artificial con medidas tradicionales mejora significativamente la prevención y detección de amenazas.
Powell	2025	Inglés	3	Se destaca que el liderazgo en ciberseguridad es fundamental para integrar estrategias organizacionales que fortalezcan la protección de la información.
Radanliev et al.	2021	Inglés	1	Se concluye que los entornos IoT introducen riesgos complejos e impredecibles que afectan la seguridad de los sistemas contables digitales.
Saeed et al.	2023	Inglés	3	El estudio evidencia que la inteligencia de amenazas permite mejorar la resiliencia organizacional y la capacidad de respuesta ante ciberataques.
Singh	2025	Inglés	3	Se identifica que la resiliencia digital es clave para garantizar la continuidad operativa frente a riesgos cibernéticos.

Ulven&Wangen	2021	Inglés	1	Se demuestra que los entornos digitales presentan múltiples vulnerabilidades que requieren estrategias integrales de seguridad.
Wang et al.	2025	Inglés	1	El estudio evidencia riesgos emergentes relacionados con la manipulación digital y tecnologías descentralizadas.
Wang et al.	2025	Inglés	1	Se concluye que los sistemas de autenticación presentan vulnerabilidades que pueden ser explotadas si no se gestionan adecuadamente.
Weigand et al.	2020	Inglés	2	Se destaca que blockchain mejora la trazabilidad y confiabilidad de los registros contables.
Zhang&Zhou	2020	Inglés	3	Se evidencia que blockchain fortalece la seguridad y confianza en los sistemas de información digital.
Zheng et al.	2018	Inglés	1	Se identifica que los sistemas en la nube presentan riesgos relacionados con acceso no autorizado y pérdida de información.