08

SEGURIDAD Y REGULACIONES

DE PRIVACIDAD EN LA CONTABILIDAD DIGITAL PARA PROTEGER DATOS FINANCIEROS SENSIBLES

ISSN: 2631-2662

Fecha de presentación: enero, 2025 **Fecha de aceptación:** marzo, 2025 **Fecha de publicación:** abril, 2025

SEGURIDAD Y REGULACIONES

DE PRIVACIDAD EN LA CONTABILIDAD DIGITAL PARA PROTEGER DATOS FINANCIEROS SENSIBLES

SECURITY AND PRIVACY REGULATIONS IN DIGITAL ACCOUNTING TO PROTECT SENSITIVE FINANCIAL DATA

María Isabel Cargua-García[1]
E-mail: maria.cargua.05@est.ucacue.edu.ec
ORCID: https://orcid.org/0009-0001-6210-1793
Mireya Magdalena Torres-Palacios[1]
E-mail: mireya.torres@ucacue.edu.ec
ORCID: https://orcid.org/0000-0002-7724-3313
[1]Universidad Católica de Cuenca. Ecuador.

Cita sugerida (APA, séptima edición)

Cargua-García, M. I., & Torres-Palacios, M. M. (2025). Seguridad y regulaciones de privacidad en la contabilidad digital para proteger datos financieros sensibles. *Revista Metropolitana de Ciencias Aplicadas*, 8(2), 74-84.

RESUMEN

La contabilidad digital representa una valiosa herramienta para la modernización de las organizaciones financieras, optimizando procesos, mejorando la precisión en los informes y facilitando la toma de decisiones. El objetivo de la presente investigación es establecer un marco integral de contabilidad digital que garantice la seguridad y privacidad de los datos financieros en las cooperativas de ahorro y crédito en la provincia de Pichincha, Ecuador. La investigación es de tipo no experimental y sigue un diseño mixto, por medio del cual se evaluó el nivel de conocimiento sobre prácticas de ciberseguridad, grado de automatización de los procesos contables y la capacitación del personal. Los resultados indican avances en la automatización. Sin embargo, evidencian falencias en la implementación de medidas de seguridad como autenticación avanzada y cifrado. Se propone un marco integral que incluye políticas claras, tecnologías avanzadas y capacitación continua. Se concluye que es necesario fortalecer las capacidades técnicas del sector para afrontar los desafíos en este ámbito.

Palabras clave:

Contabilidad, seguridad, privacidad, datos, automatización.

ABSTRACT

Digital accounting represents a valuable tool for the modernization of financial organizations, optimizing processes, improving reporting accuracy and facilitating decision making. The objective of this research is to establish a comprehensive digital accounting framework that ensures the security and privacy of financial data in credit unions in the province of Pichincha, Ecuador. The research is non-experimental and follows a mixed design, through which the level of knowledge about cybersecurity practices, degree of automation of accounting processes, and staff training were evaluated. The results indicate progress in automation; however, they show weaknesses in the implementation of security measures such as advanced authentication and encryption. A comprehensive framework is proposed that includes clear policies, advanced technologies and continuous training. The conclusions highlight the need to strengthen the technical capabilities of the sector to meet the challenges in this area.

Keywords:

Accounting, security, privacy, data, automation.

INTRODUCCIÓN

A lo largo de la historia, la protección de los datos financieros sensibles ha evolucionado en respuesta a los avances tecnológicos y los riesgos asociados. No obstante, con el advenimiento de la contabilidad digital, los riesgos se han multiplicado y agravado debido a la dependencia de sistemas en línea. En consecuencia, las violaciones en este terreno son preocupantes debido a los ataques cibernéticos y accesos indebidos (Cortes, 2023).

A nivel global, de manera específica en Europa, la protección de datos financieros en la contabilidad digital se sustenta en un marco regulatorio robusto, liderado por el Reglamento General de Protección de Datos (RGPD) y la PSD2 (***Payment Services Directive***), que establecen normas estrictas para el manejo de datos personales y la seguridad de transacciones electrónicas. A pesar de este marco, las instituciones financieras enfrentan amenazas como ciberataques, fraude en línea y brechas de datos, que pueden comprometer la seguridad y privacidad de la información financiera crítica. Asimismo, el cumplimiento de regulaciones cada vez más exigentes añade un desafío legal y de cumplimiento, con el riesgo de sanciones severas y daños a la reputación en caso de incumplimiento (Li, 2024).

De manera similar, en América Latina, la protección de datos financieros en la contabilidad digital se aborda mediante regulaciones en desarrollo, inversiones en ciberseguridad y alfabetización digital, buscando alinearse con normativas globales como el RGPD. Asimismo, se invierte en tecnologías avanzadas como redes seguras y criptografía y se educa a empleados y clientes en prácticas seguras para minimizar riesgos. A pesar de ello, como se ha mencionado, las instituciones enfrentan distintas amenazas que pueden resultar en riesgos legales y reputacionales. Por otro lado, la integración de ***fintechs*** (empresas que utilizan la tecnología para ofrecer servicios financieros) añade complejidad y riesgos en la interoperabilidad y seguridad de nuevas plataformas (Viera et al., 2023).

En particular, México, Brasil, Colombia, Perú y Chile son los cinco países que enfrentan un mayor número de ciberamenazas en Iberoamérica, según un reciente informe de ***Etek International***. De hecho, este estudio resalta que el 63 % de los delitos motivados por razones financieras son los más comunes en la región. En promedio, se registra un ataque cada 45 segundos, con un costo medio de 231.000 euros. Es importante destacar que, de acuerdo con este informe, el sector financiero se encuentra entre los más afectados y que, al igual que en otras partes del mundo, se confirma un aumento en la peligrosidad, sofisticación y tasa de éxito de estas ciberamenazas.

En concordancia con lo anterior, de acuerdo con el más reciente informe de Kaspersky 2023, la incidencia de phishing en Latinoamérica ha aumentado seis veces. En este sentido, Ecuador se sitúa entre los países con mayor número de ataques de phishing, ocupando el quinto lugar en el ranking. Asimismo, otro tipo de ataque que ha experimentado un notable incremento en 2023 son los troyanos bancarios, con un aumento del 50 % (Cirion Technologies, 2024).

En el caso específico de Ecuador, la adopción de servicios financieros digitales por las cooperativas de ahorro y crédito (COAC) implica ciertos desafíos en cuanto a ciberseguridad y protección de datos. En este punto, es importante mencionar que las COAC son instituciones democráticas y sin fines de lucro, constituidas por asociaciones voluntarias de personas que se organizan para satisfacer sus necesidades económicas, sociales y culturales a través de la propiedad común. Estas cooperativas actúan como intermediarios financieros, movilizando los ahorros de sus socios para ofrecer créditos accesibles y productos financieros adaptados a diversas circunstancias socioeconómicas (Luque & Peñaherrera, 2021).

Las COAC en Ecuador surgieron para atender a la población de bajos ingresos, excluida a lo largo de los años por la banca tradicional, enfocándose en un inicio en grupos productivos y pequeñas comunidades. Su objetivo principal es el desarrollo social, buscando un equilibrio entre beneficios sociales y sostenibilidad económica, priorizando la rentabilidad financiera para lograr la social. Pese a lo indicado, en las últimas décadas, la liberalización financiera y la innovación tecnológica han representado para estas organizaciones importantes desafíos. Por lo tanto, las COAC enfrentan la necesidad de competir en un entorno de alta inversión y adoptar tecnologías para agregar valor a sus servicios, a menudo replicando los mecanismos de la banca tradicional (Hinostroza et al., 2023).

Como se ha mencionado, las COAC enfrentan desafíos frente a la digitalización, como la vulnerabilidad ante ciberataques (phishing y ransomware) y demás riesgos que plantea la recopilación de datos personales y financieros con respecto a la seguridad y privacidad de estos. Estas amenazas requieren de políticas de protección de datos estrictas para evitar filtraciones (Minango & Vásconez, 2024).

Ante esta situación, para salvaguardar los datos financieros sensibles de las COAC en la provincia de Pichincha, Ecuador, es imperativo implementar estrategias de control robustas. En particular, un sistema de monitoreo de operaciones capaz de detectar actividades fraudulentas o sospechosas, mediante el análisis de transacciones y comportamientos atípicos, sería de gran utilidad para estas cooperativas. Este panorama plantea el siguiente problema: ¿Cómo garantizar la seguridad de los datos financieros sensibles en el marco de la contabilidad digital en cooperativas de ahorro y crédito en la provincia de Pichincha, Ecuador?

En consecuencia, el objetivo de esta investigación es establecer un marco integral de contabilidad digital que garantice la seguridad y privacidad de los datos financieros en las cooperativas de ahorro y crédito en la provincia de Pichincha, Ecuador, mediante la implementación de sistemas avanzados de monitoreo de transacciones, autenticación multifactorial, uso de tecnologías de aprendizaje automático para la detección de fraudes y capacitación en ciberseguridad para empleados y socios.

La contabilidad tradicional, caracterizada por procesos manuales, registros en papel y una limitada capacidad de análisis, ha experimentado una transformación profunda en la era digital. En efecto, la adopción de tecnologías avanzadas ha dado lugar a la contabilidad digital, la cual se define como el uso de tecnologías digitales para automatizar, optimizar y transformar los procesos contables y financieros de una organización. De esta manera, este nuevo modo de contabilidad redefine la gestión y el reporte de la información financiera (Ojeda et al., 2020).

Resulta evidente que la contabilidad digital ofrece numerosos beneficios, destacando la reducción de costos operativos. Por ejemplo, la automatización de procesos disminuye la necesidad de personal para tareas manuales y reduce el consumo de suministros. De manera adicional, el acceso a información financiera precisa y en tiempo real mejora la toma de decisiones, permitiendo a los gerentes analizar datos actualizados para identificar tendencias y planificar estrategias. Asimismo, la agilidad en procesos como la facturación y la gestión de pagos facilita una respuesta rápida a los cambios del mercado y la automatización de cálculos y registros reduce de manera notable los errores humanos (Stender et al., 2025).

Para su buen desempeño, la contabilidad digital se apoya en diversas herramientas tecnológicas, tales como ***softwares*** contables que permiten la automatización de tareas como la facturación, la gestión de pagos y la elaboración de informes financieros, o los sistemas ERP (***Enterprise Resource Planning***) que integran los procesos contables con otras áreas de la empresa, como la gestión de inventarios o la gestión de recursos humanos. Se suman los sistemas de automatización que utilizan la inteligencia artificial (IA) y el aprendizaje automático para automatizar tareas repetitivas y mejorar la precisión de los datos. Otras herramientas como el análisis de datos permiten obtener información valiosa a partir de los datos financieros, facilitando la toma de decisiones estratégicas;y, la contabilidad en la nube permite el acceso a la información financiera desde cualquier lugar y en cualquier momento, lo que mejora la colaboración y la flexibilidad (Acosta et al., 2024).

En cuanto a las tendencias asociadas con la implementación de la tecnología en los procesos contables, se tiene que el ***Big Data***, la IA y el ***Blockchain*** están transformando la contabilidad al permitir el análisis de grandes volúmenes de datos para detectar patrones y fraudes, automatizar tareas repetitivas y mejorar la toma de decisiones estratégicas. La IA, con sus algoritmos, analiza datos financieros para identificar anomalías y predecir tendencias, liberando a los contadores para tareas más estratégicas. ***Blockchain***, por su parte, crea registros contables inmutables y transparentes, mejorando la seguridad, reduciendo los costos de auditoría y facilitando la creación de contratos inteligentes (González et al., 2024).

A pesar de las bondades, estas tecnologías, también, plantean desafíos en términos de implementación, seguridad de la información, privacidad de los datos y cumplimiento normativo. La implementación de la contabilidad digital implica un cambio cultural en la organización, por lo que se debe realizar una adecuada gestión del cambio. La capacitación del personal es esencial para asegurar que los empleados tengan las habilidades necesarias para utilizar las nuevas tecnologías. De manera adicional, es importante fomentar una cultura organizacional que promueva la adopción de la tecnología y la innovación. Esta gestión del cambio debe ser un proceso continuo que acompañe a la organización en su evolución hacia la contabilidad digital (Millán, 2023).

Por otro lado, la digitalización aumenta la exposición a ataques cibernéticos y fugas de información, lo que requiere implementar medidas de seguridad robustas y considerar los riesgos asociados a la dependencia de tecnologías. La contabilidad digital depende de sistemas informáticos y conexiones a internet, lo que puede generar interrupciones en caso de fallas técnicas o cortes de energía (Ojeda et al., 2020).

En este sentido, un marco integral de contabilidad digital es indispensable para que las instituciones aprovechen la transformación digital mientras mitigan los riesgos asociados. Este marco debe incluir componentes relevantes como la seguridad de la información, la privacidad de los datos, el cumplimiento normativo, la automatización de procesos, el análisis de datos, la capacitación del personal y la implementación de sistemas de monitoreo y auditoría. Al integrar estos elementos, se garantiza la confidencialidad, integridad y disponibilidad de los datos financieros, se protege la información personal de clientes y empleados, se automatizan tareas repetitivas para mejorar la eficiencia y se asegura el cumplimiento de las leyes y regulaciones aplicables (Ojeda et al., 2020).

En cuanto a la normatividad y regulaciones, la contabilidad digital está sujeta a diversas leyes fiscales y de privacidad de datos que varían según la jurisdicción, regulando la presentación electrónica de declaraciones de impuestos, la facturación electrónica y la conservación de registros digitales. Las leyes de privacidad de datos, como el RGPD en la Unión Europea o la Ley Orgánica de Protección de Datos Personales en Ecuador, establecen los requisitos para la recopilación, almacenamiento y procesamiento de datos personales en sistemas contables digitales.

Por otro lado, las Normas Internacionales de Información Financiera (NIIF) establecen los principios para el reconocimiento, medición, presentación y revelación de transacciones financieras realizadas a través de plataformas digitales y sistemas automatizados (Sullivan, 2020). De igual forma, las NIIF abordan aspectos como la valoración de activos intangibles generados por la tecnología y la presentación de información sobre riesgos cibernéticos.

La seguridad de los datos financieros es un pilar en el sector financiero, dada la naturaleza sensible de la información manejada. La integridad y confidencialidad de estos datos es muy importante, pues las brechas de seguridad pueden desencadenar pérdidas económicas masivas, daños reputacionales y la erosión de la confianza del cliente. En un mundo cada vez más digitalizado, la dependencia de sistemas en línea incrementa la vulnerabilidad a ciberataques sofisticados, y la globalización financiera exige estándares de seguridad uniformes para proteger los datos en transacciones transfronterizas. Estos ciberataques han evolucionado abriendo nuevas vías para el fraude, como el robo de identidad en línea y el acceso no autorizado a cuentas bancarias, donde los ciberdelincuentes emplean técnicas cada vez más complejas para eludir las medidas de seguridad (Li, 2024).

Las tecnologías y herramientas empleadas para la seguridad de los datos financieros abarcan la ciberseguridad, con ***firewalls***, sistemas de detección y prevención de intrusiones, cifrado de datos y autenticación multifactorial; la seguridad de datos, con gestión de bases de datos seguras, anonimización y seudonimización de datos y tecnologías de enmascaramiento de datos; y tecnologías emergentes como la IA, el aprendizaje automático, ***Blockchain*** y la computación en la nube segura (González et al., 2024). En el sector financiero, la seguridad se extiende a la banca digital, con protección de aplicaciones móviles y banca en línea, seguridad en pagos electrónicos y cumplimiento con regulaciones como PSD2 (Viera et al., 2023).

Bajo esta perspectiva, las mejores prácticas y estrategias para la seguridad de los datos financieros incluyen la gobernanza de la seguridad de la información mediante procedimientos claros, roles y responsabilidades definidos, auditorías periódicas a través de la capacitación del personal y la colaboración y compartición de información, con participación en foros, compartición de inteligencia sobre amenazas y capacitación en ciberseguridad para empleados y socios (Muñoz et al., 2019)donde se ve afectada la información y las alternativas que setoman para contrarrestar, disminuir y controlar estos tipos de situaciones, tomando como base las buenas prácticas en la aplicación de la seguridad informática en los sistemas contables. Además, se llevó a cabo una comparación de los países como España y Colombia de las medidas tomadas para capacitar, prevenir y controlar aquellos delitos informáticos que se den dentro de una organización en el ejercicio de sus procesos contables a través de sistemas digitales o computarizados (bases de datos.

La privacidad de los datos financieros ha cobrado gran relevancia en la era digital, diferenciándose de la seguridad en su enfoque: mientras la seguridad protege los datos del acceso no autorizado, la privacidad salvaguarda el derecho individual a controlar la recopilación, uso y compartición de su información financiera. Este derecho, ligado a principios como la libertad y la autonomía, fortalece la confianza en las instituciones financieras (Cristancho, 2023).

La privacidad financiera empodera a las personas para tomar decisiones informadas, previniendo la discriminación y el uso indebido de datos. A nivel social, resguarda contra la vigilancia masiva y el perfilamiento discriminatorio y a nivel económico, impulsa la innovación y la competencia al asegurar el acceso equitativo a la información. La ausencia de privacidad puede derivar en exclusión financiera y erosión de la confianza institucional, mientras que su protección robusta fomenta la inclusión, la innovación y la economía digital (Banco Mundial, 2022).

La IA y ***Blockchain*** son valiosas herramientas para proteger la privacidad en la era digital, al igual que las Tecnologías de Mejora de la Privacidad (PETs) como la criptografía homomórfica y la privacidad diferencial, las cuales permiten un uso responsable de los datos. Sin embargo, la IA aunque ofrece beneficios en la detección de anomalías, requiere marcos éticos y técnicas como el aprendizaje federado para mitigar riesgos de vigilancia. Por su parte, si bien el ***Blockchain*** mejora la privacidad mediante anonimización y gestión de identidad, enfrenta desafíos como la inmutabilidad y la trazabilidad, que requieren soluciones específicas como transacciones confidenciales (Cristancho, 2023).

En cuanto a la normativa sobre la privacidad de los datos financieros, en Ecuador, la Ley Orgánica de Protección de Datos Personales (LOPD), promulgada en 2021, ha fortalecido el marco legal de privacidad, alineándose con estándares internacionales como el RGPD. La LOPD reconoce derechos y establece obligaciones para los responsables del tratamiento de datos, supervisados por la Superintendencia de Protección de Datos Personales (Corporación Nacional de Finanzas Populares y Solidarias, 2021).

Por último, un importante aspecto a abordar con respecto a la privacidad de datos financieros es su gestión, la cual debe ser un proceso continuo que implique la implementación de políticas, procedimientos y controles, incluyendo la evaluación de riesgos, la capacitación del personal y la comunicación transparente con los titulares de datos. Bajo esta línea, las organizaciones deben adoptar un enfoque de privacidad por diseño y realizar evaluaciones de impacto de privacidad, reconociendo que la protección

de la privacidad es tanto un requisito legal como un factor de confianza y reputación.

MATERIALES Y MÉTODOS

El estudio no experimental busca comprender las relaciones entre variables a través de la observación y el análisis, sin ejercer control directo sobre ellas. Por otro lado, el estudio transversal se caracteriza por la recolección de datos en un único momento (Hernández et al., 2010). La presente investigación es del tipo no experimental-transversal, puesto que se analizaron las variables tal como se presentaban en su condición original, sin intervenir en los sistemas existentes de las cooperativas de ahorro y crédito y la recopilación de datos se hizo en un único momento.

Por otro lado, el diseño mixto implica la recolección, análisis e integración de datos, generando inferencias tanto cuantitativas como cualitativas, proporcionando una perspectiva más amplia y profunda y una mejor exploración y explotación de los datos (Hernández et al., 2010). Esta investigación adoptó un diseño mixto, combinando métodos cuantitativos y cualitativos para un análisis más completo. El enfoque cuantitativo se implementó a través de encuestas y el enfoque cualitativo, mediante la revisión documental. La integración de ambos métodos fortaleció la validez de los resultados al permitir la triangulación de datos.

En este marco metodológico, el alcance descriptivo y explicativo desempeñaron roles clave. El alcance descriptivo se enfocó en especificar las propiedades y características de los fenómenos bajo estudio, como el nivel de conocimiento sobre contabilidad financiera y la seguridad de los datos entre los trabajadores de las cooperativas. Este enfoque permitió recopilar información precisa sobre conceptos y variables, sin entrar en la causalidad entre ellos. Por su parte, el alcance explicativo se orientó a proporcionar una comprensión más profunda de los fenómenos, explorando las causas y factores que influencian el desarrollo de las prácticas de contabilidad digital en las cooperativas de ahorro y crédito de la provincia de Pichincha. Así, la combinación de ambos alcances, junto con el diseño mixto, facilitó un análisis integral y multifacético del fenómeno estudiado.

En esta investigación se empleó el método inductivo-deductivo al analizar los datos de las encuestas para derivar conclusiones sobre las necesidades de las cooperativas. Mientras que el método analítico-sintético se aplicó al descomponer la contabilidad digital en sus componentes (seguridad, privacidad, conocimiento técnico) para luego integrarlos en un marco integral. Por otro lado, el método sistémico se implementó al considerar las cooperativas como sistemas complejos, donde la contabilidad digital interactúa con otros factores organizacionales y legales, buscando un marco integral para la protección de datos financieros (Hernández et al., 2010).

Se aplicó una encuesta compuesta por un cuestionario de 20 ítems, previamente validado por expertos, enfocado en la seguridad y las regulaciones de privacidad en la contabilidad digital. Además, se realizó una revisión exhaustiva de la literatura disponible, que incluyó artículos científicos, tesis y portales oficiales, para obtener una comprensión más profunda sobre la contabilidad digital y las medidas de seguridad y privacidad de los datos financieros. Esta combinación de métodos permitió contar con una base sólida de información tanto empírica como teórica, relevante para el objetivo del estudio.

La unidad de análisis en esta investigación estuvo conformada por las cooperativas de ahorro y crédito ubicadas en la provincia de Pichincha, que suman un total de 47, según el Banco Central del Ecuador (2014). De estas, se seleccionaron 25 cooperativas mediante un muestreo intencional.

RESULTADOS Y DISCUSIÓN

Automatización de procesos contables: el análisis de la muestra indica que en su gran mayoría las cooperativas tienen procesos contables automatizados de manera parcial, mientras que el otro porcentaje los tienen automatizados en su totalidad. Esto permite verificar un alto nivel de adopción de tecnología, y prudencia en el manejo y protección de información financiera.

Sistemas de contabilidad digital utilizados: se puede evidenciar que un gran porcentaje de instituciones utiliza sistemas ERP integrados, destacando su capacidad para centralizar y automatizar procesos, mejorar la trazabilidad y garantizar el cumplimiento normativo, mientras que un porcentaje menor recurre a soluciones personalizadas, adaptadas a necesidades específicas, lo que les permite mayor flexibilidad en ciertos aspectos, aunque con mayores costos y complejidad técnica, y un 8 % aún utiliza software básico, lo que podría limitar su capacidad de respuesta ante las demandas regulatorias y la creciente competencia.

Capacitación en herramientas digitales: la mayoría del personal tiene un nivel de capacitación medio, lo que indica que están familiarizadas con las herramientas digitales necesarias para desempeñar sus funciones. Un 28 % alcanza un nivel alto de capacitación, lo que demuestra que existe un grupo especializado que lidera la adopción de nuevas tecnologías en la organización. Sin embargo, un pequeño grupo se encuentra con niveles bajos o muy bajos de capacitación, lo que representa que podrían enfrentar dificultades al trabajar con herramientas digitales.

Frecuencia de capacitaciones digitales: una gran parte de COAC organiza capacitaciones al menos dos veces al año, lo que asegura que sus empleados se mantengan actualizados con las herramientas digitales necesarias para desempeñar sus funciones de manera eficiente. Tan solo el 12 % de las cooperativas realiza capacitaciones

muy frecuentes, lo que demuestra un enfoque proactivo hacia el aprendizaje y la adaptación a nuevas tecnologías.

Impacto de herramientas digitales en la reducción de errores: según los datos presentados, el 52 % de los encuestados reportó una reducción considerable de errores humanos, mientras que un 40 % observó una reducción parcial. Esto refleja que el uso de herramientas digitales mitiga riesgos asociados a la intervención manual y optimiza los procesos operativos.

Calidad de la infraestructura tecnológica: los datos de la encuesta reflejan una tendencia positiva e incrementable en las cooperativas en cuanto a su infraestructura, lo que indica que, cuentan con lo necesario para operar permitiendo una satisfacción general en la prestación de sus servicios, lo que refleja que estas cooperativas están mejor posicionadas para enfrentar los retos tecnológicos y aprovechar nuevas oportunidades. Sin embargo, un pequeño porcentaje evalúa como deficiente o muy deficiente, lo que representa una preocupación, ya que una infraestructura inadecuada puede limitar la eficiencia operativa y la adopción de nuevas tecnologías.

Medidas de autenticación para datos financieros: la mayoría de los encuestados utiliza autenticación multifactor (MFA), una estrategia robusta que combina múltiples métodos de verificación para dificultar accesos no autorizados. Sin embargo, el 44 % todavía depende de contraseñas básicas, lo que representa un riesgo relevante ante ataques comunes. Por otro lado, solo el 4 % emplea biometría, una tecnología que ofrece altos niveles de seguridad y comodidad. No obstante, su adopción es limitada debido a costos iniciales y barreras tecnológicas. En la tabla 1 se presentan las frecuencias de medidas de autenticación.

Tabla 1. Frecuencias de medidas de autenticación.

Medidas de autenticación	Frecuencia	Porcentaje
a) Contraseñas básicas	11	44
b) Autenticación multifactorial (MFA)	13	52
c) Biometría	1	4
Total	25	100

Cifrado de datos financieros: la mayoría de las cooperativas cuenta con datos cifrados, lo que indica que, aunque se ha tomado una medida importante para proteger la información, la implementación del cifrado no es total, lo que podría dejar algunos datos expuestos a riesgos. Por otro lado, el 28 % de las cooperativas cifra la totalidad de sus datos, lo que refleja un nivel más alto de seguridad y protección ante posibles ciberataques o accesos no autorizados.

Actualización de sistemas de seguridad: los resultados muestran distintos niveles de compromiso en la gestión de actualizaciones de seguridad dentro de las cooperativas. Se identifican prácticas enfocadas en la actualización continua de los sistemas, lo que indica una estrategia sostenida para minimizar vulnerabilidades. Otra parte de las cooperativas implementa parches con mayor frecuencia, lo que apunta a un enfoque aún más dinámico y preventivo en la protección de la información. Estas diferencias en la periodicidad de las actualizaciones reflejan distintos niveles de madurez en la gestión de ciberseguridad y el grado de prioridad que otorgan a la protección de sus sistemas contables.

Auditorías internas: podemos observar que algunas COAC optan por auditorías con una periodicidad corta, lo que indica un seguimiento detallado y constante de sus operaciones. Otras implementan revisiones con intervalos más amplios, manteniendo un control periódico, aunque con menor frecuencia. Un grupo reducido no lleva a cabo auditorías internas, lo que contrasta con la tendencia general de priorizar el cumplimiento y la rendición de cuentas. Estas diferencias reflejan distintos niveles de rigurosidad en la aplicación de controles internos y en la supervisión de las políticas de privacidad. **Monitoreo en tiempo real**: el 52 % realiza un monitoreo parcial con herramientas limitadas, mientras que el 28 % usa herramientas avanzadas para una mayor seguridad. Sin embargo, el 20 % no realiza monitoreo, lo que representa un notable riesgo. Para mejorar la protección de los datos, es importante que las cooperativas fortalezcan sus sistemas de monitoreo, implementando herramientas más robustas y garantizando una vigilancia constante.

Preparación ante ciberataques: el 40 % considera que su preparación es moderada, lo que pone de manifiesto un enfoque intermedio en la adopción de medidas de ciberseguridad. Un 32 % la califica como alta, lo que refleja un esfuerzo sólido para protegerse contra amenazas cibernéticas. Sin embargo, el 28 % tiene niveles de preparación bajos o muy bajos, lo que indica que aún existen cooperativas con vulnerabilidades en sus estrategias de seguridad.

Políticas de privacidad documentadas: el 60 % de las cooperativas tiene políticas de privacidad parcial documentadas, mientras que el 32 % las tiene documentadas en su totalidad**,** lo que refleja avances en la formalización de estas políticas. A pesar de ello, aún queda trabajo por hacer, ya que una mayor formalización y documentación integral de las políticas de privacidad ayudará a garantizar la protección adecuada de los datos y cumplir con las regulaciones.

Acuerdos de confidencialidad: de acuerdo con la encuesta, el 48 % de las organizaciones siempre firma acuerdos de confidencialidad, asegurando que tanto empleados como terceros se comprometan a proteger la información. A diferencia del otro 40% que lo hace de manera ocasional, lo que podría generar brechas en la seguridad, ya que no todos los involucrados están

comprometidos. Por último, un 12 % de las organizaciones no utiliza esta práctica, lo que representa un riesgo representativo en términos de seguridad de la información.

Eficacia de las medidas de protección: el 64 % de los encuestados considera que sus medidas de protección en cierto grado son eficaces, mientras que el 20 % las califica como muy eficaces, lo que indica que, en general, estas estrategias cumplen su propósito de mitigar riesgos. El 16 % evalúa estas medidas como ineficaces o muy ineficaces, lo que refleja la existencia de brechas en su implementación o actualización frente a amenazas emergentes.

Frecuencia de auditorías de privacidad y regulación de datos: el 48 % realiza auditorías de forma semestral y el 32 % las lleva a cabo una vez al año, lo que refleja un enfoque regular en la protección de la privacidad. Solo el 12 % no realiza auditorías, lo que indica que la mayoría de las cooperativas está tomando medidas para asegurar la privacidad y el cumplimiento de las regulaciones. En la figura 1 se representa la frecuencia de auditorías.

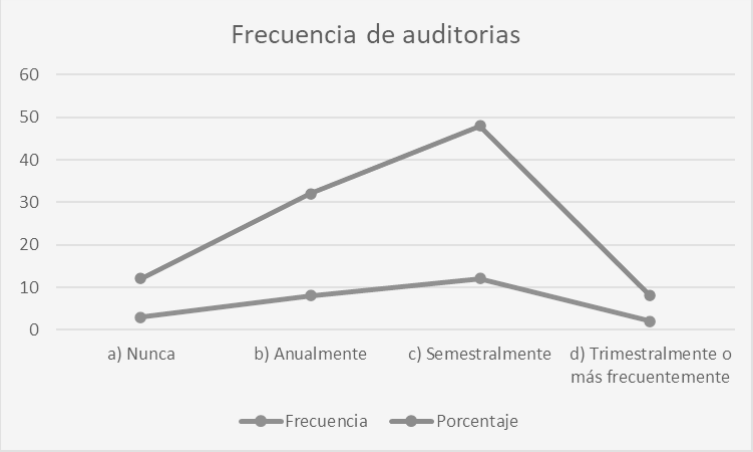

Figura 1. Frecuencia de auditorías.

La figura 1 muestra la frecuencia de auditorías de privacidad en las cooperativas, reflejando un enfoque regular y comprometido con la protección de la privacidad y el cumplimiento de las regulaciones.

Efectividad en detección temprana de violaciones a los sistemas de seguridad: el 52 % considera que la detección es efectiva, mientras que el 28 % la califica como muy efectiva, lo que indica una mejora en los mecanismos de respuesta ante incidentes. Estos resultados reflejan un progreso importante en la capacidad para identificar y abordar violaciones de seguridad a tiempo, aunque aún se pueden realizar mejoras en algunas áreas.

Desarrollo de un marco integral de contabilidad digital para la protección de datos financieros en las COAC de Pichincha, Ecuador

En la tabla 2 se presentan un conjunto de medidas para implementar un marco de contabilidad digital centradas en la protección de datos financieros mediante políticas de seguridad, cifrado, control de acceso y cumplimiento normativo.

Tabla 2. Marco integral de contabilidad digital para la protección de datos financieros.

Estrategia	Descripción	Adopción	Responsable(s)
Definición de políticas de seguridad y privacidad	Establecer políticas claras sobre cómo manejar, proteger y almacenar datos financieros y personales, alineadas con las normativas locales e internacionales.	Análisis de normativas, redacción de políticas, aprobación por la dirección. Difusión a empleados, publicación en intranet.	Comité de Seguridad de la Información / Gerente de TI
Implementación de medidas de cifrado de datos	Implementar sistemas de cifrado para proteger los datos en tránsito y almacenados.	Selección de algoritmos de cifrado, adquisición de software/hardware. Cifrado de bases de datos, comunicaciones, copias de seguridad.	Equipo de Tecnología / Proveedor de Servicios de TI
Control de acceso y autenticación	Realizar control de acceso basado en roles y autenticación de múltiples factores (MFA) para proteger el acceso a los sistemas contables.	Definición de roles, configuración de MFA. Asignación de permisos, activación de MFA para usuarios.	Administrador de Sistemas / Departamento de Seguridad

Capacitación del personal en seguridad de la información	Capacitar a todos los empleados sobre el manejo seguro de los datos financieros y mejores prácticas de ciberseguridad.	Diseño de programa, selección de materiales. Sesiones presenciales, cursos online, simulacros de phishing.	Recursos Humanos / Coordinador de Capacitación
Evaluación y gestión de riesgos	Realizar análisis de riesgos periódicos para identificar vulnerabilidades en los sistemas y procesos de contabilidad digital.	Definición de metodología, cronograma. Análisis de vulnerabilidades, evaluación de controles, elaboración de informes.	Gerente de Riesgos / Auditor Interno
Auditorías internas y externas	Realizar auditorías regulares para verificar la implementación de las políticas de seguridad y el cumplimiento normativo.	Definición de alcance, selección de auditores. Revisión de registros, entrevistas, pruebas de seguridad, elaboración de informes.	Auditor Interno / Auditor Externo
Creación de un plan de contingencia y recuperación ante desastres	Establecer procedimientos para restaurar los datos financieros en caso de incidentes o fallos en el sistema.	Identificación de escenarios, definición de procedimientos. Pruebas de recuperación, almacenamiento de copias de seguridad, comunicación con stakeholders.	Equipo de Continuidad del Negocio / Gerente de TI
Supervisión continua y monitoreo de sistemas	Implementar herramientas de monitoreo para detectar cualquier intento de intrusión o brechas de seguridad en tiempo real.	Selección de herramientas, configuración de alertas. Monitoreo de tráfico, registro de eventos.	Administrador de Redes / Proveedor de Servicios de TI
Cumplimiento normativo y regulatorio	Asegurarse de que todos los procesos de contabilidad digital cumplan con las leyes nacionales (Ley Orgánica de Protección de Datos Personales) y normativas internacionales aplicables.	Revisión de normativas, elaboración de planes de acción. Adaptación de procesos, seguimiento de cambios legales.	Director General / Asesor Legal
Transparencia con los socios y comunicación de medidas de seguridad	Informar a los socios sobre las políticas de seguridad y cómo se protegerán sus datos personales y financieros.	Elaboración de comunicados, diseño de canales de comunicación. Publicación en web, envío de correos, reuniones informativas.	Gerente de Comunicaciones / Director General
Revisión continua de políticas y tecnologías	Actualizar y mejorar las políticas de seguridad y las tecnologías utilizadas, con base en los cambios tecnológicos y regulatorios.	Monitoreo de tendencias, evaluación de nuevas tecnologías. Implementación: Actualización de políticas, adquisición de software/hardware, capacitación.	Comité de Seguridad de la Información / Gerente de TI
Evaluación de proveedores externos y servicios en la nube	Asegurarse de que los proveedores de servicios tecnológicos (software contable, almacenamiento en la nube, etc.) cumplan con estándares de seguridad y privacidad.	Elaboración de cuestionarios, revisión de contratos. Auditorías a proveedores, cláusulas de seguridad en contratos.	Gerente de TI / Departamento de Compras

Para aplicar el marco integral de contabilidad digital en las COAC, se requiere el compromiso de la alta dirección, infraestructura tecnológica adecuada, personal capacitado, políticas claras de seguridad, evaluación de riesgos y cumplimiento normativo, así como un plan de contingencia y monitoreo continuo.

CONCLUSIONES

La protección de datos financieros es decisiva ante las crecientes amenazas cibernéticas y avances tecnológicos. En América Latina, el sector financiero enfrenta vulnerabilidades debido a limitaciones tecnológicas y falta de especialización en ciberseguridad. En Ecuador, las COAC necesitan adoptar medidas como monitoreo de transacciones, autenticación avanzada y herramientas de aprendizaje automático, junto con capacitación y cumplimiento normativo. Estas acciones fortalecerán la seguridad de los datos y promoverán la confianza y estabilidad en el sector financiero local.

La contabilidad digital es determinante para la modernización empresarial, mejorando la eficiencia, precisión en los informes financieros y el análisis estratégico. Su adopción en Ecuador aumenta la protección de datos sensibles, aunque enfrenta desafíos como la falta de formación técnica y resistencia al cambio. Superados estos obstáculos, continuará impulsando la productividad, la toma de decisiones informadas y la competitividad en un entorno económico dinámico.

La seguridad de los datos financieros es esencial para proteger la información confidencial de los usuarios en el sistema cooperativo. Medidas como el acceso autorizado, el cifrado avanzado y la detección de amenazas juegan un papel decisivo en prevenir fraudes e intrusiones. El cifrado garantiza la protección de los datos durante su transmisión, dificultando su interceptación. En conjunto, las herramientas de detección permiten identificar amenazas de forma

proactiva, aumentando la confianza de los usuarios. Estas prácticas fortalecen la seguridad en los canales digitales, promoviendo una mayor inclusión financiera y estabilidad en el sistema. En conjunto, son determinantes para asegurar la integridad del entorno digital cooperativo.

La privacidad de los datos financieros es esencial para proteger la información sensible y garantizar la autonomía de los usuarios en el ámbito financiero. Normativas y sistemas de gestión de seguridad, junto con estrategias como autenticación multifactorial y análisis predictivo, son vitales para proteger los datos en cooperativas de ahorro y crédito en Pichincha, Ecuador. Sin embargo, desafíos como la resistencia al cambio, la falta de capacidades técnicas y problemas de infraestructura requieren investigaciones adicionales para fortalecer la ciberseguridad y avanzar en la transformación digital del sector.

Los resultados indican que las cooperativas de Pichincha han avanzado en la automatización de procesos contables, aunque aún falta completar la automatización total. En cuanto a seguridad, a pesar de la implementación de medidas avanzadas de autenticación y cifrado, la mayoría sigue utilizando métodos básicos, lo que presenta riesgos. La capacitación del personal es adecuada, no obstante, algunos empleados necesitan más formación. Incluso, aunque se realizan auditorías y monitoreos, la preparación ante ciberataques es moderada, lo que resalta la necesidad de mejorar las estrategias de ciberseguridad y protección de datos.

El marco integral de contabilidad digital propuesto para las cooperativas de ahorro y crédito de Pichincha busca garantizar la seguridad y privacidad de los datos financieros mediante políticas claras, tecnologías avanzadas como cifrado y autenticación multifactorial, y capacitación continua del personal. Se implementarán auditorías regulares, gestión de riesgos y monitoreo constante para asegurar el cumplimiento normativo y detectar brechas de seguridad. La colaboración con proveedores seguros refuerza la protección de los sistemas, fomentando confianza entre los socios y promoviendo una cultura de ciberseguridad en la organización.

REFERENCIAS BIBLIOGRÁFICAS

Acosta, W., Gamarra, M., & Villalba, A. (2024). Adaptación de los contadores a la evolución de las herramientas contables en la era digital. *Ciencia Latina Revista Científica Multidisciplinar*, *8*(3), 5331–5350. https://doi.org/https://doi.org/10.37811/cl_rcm.v8i3.11740

Banco Central del Ecuador. (2014). *Cooperativas de ahorro y crédito calificadas al sistema nacional de pagos por segmentos*. https://contenido.bce.fin.ec/documentos/ServiciosBCentral/COACS/Coacsaprobadasxregionact.pdf

Banco Mundial. (2022). *Inclusión financiera*. https://www.bancomundial.org/es/topic/financialinclusion/overview

Cirion Technologies. (2024). *Ciberseguridad financiera: Protegiendo el futuro de la banca ecuatoriana*. https://press.ciriontechnologies.com/2024/05/15/ciberseguridad-financiera-protegiendo-futuro-banca-ecuatoriana/

Corporación Nacional de Finanzas Populares y Solidarias. (2021). *Ley Orgánica de Protección de Datos Personales*. https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Cortes, M. (2023). *Importancia de la seguridad informática en los softwares contables y su impacto en la gestión contable y financiera*. (Proyecto Investigativo). Universidad de La Salle.

Cristancho, A. (2023). *La privacidad y seguridad de los datos en la era digital: retos y soluciones*. Fundación FEPROPAZ. https://fepropaz.com/privacidad-y-seguridad-de-datos/

González, S., Chamorro, J., & Rivera, C. (2024). Impacto de la inteligencia artificial en los procesos contables mediante revisión de tendencias y desafíos. *Multidisciplinary Collaborative Journal*, *2*(2), 45–56. https://doi.org/https://doi.org/10.70881/mcj/v2/n2/35

Hernández, R., Fernández, C., & Baptista, M. (2010). *Metodología de la investigación*. McGraw-Hill.

Hinostroza, G., Hermida, L., & Salazar, S. (2023). Desviación de la naturaleza social de las cooperativas de ahorro y crédito ubicadas en el segmento 1 del cantón Portoviejo. *Cofin Habana*, *17*(2). http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2073-60612023000200015

Li, K. (2024). *España y la Unión Europea: Estudio comparativo sobre transparencia y buena gobernanza*. (Tesis de maestría). Universitat Autónoma de Barcelona.

Luque, A., & Peñaherrera, J. (2021). Cooperativas de ahorro y crédito en Ecuador: el desafío de ser cooperativas. *REVESCO Revista de Estudios Cooperativos*, *138*, 1–17. https://doi.org/10.5209/REVE.73870

Millán, L. (2023). *Gestión del cambio en la implementación de nuevas tecnologías*. OpenWebinars. https://openwebinars.net/blog/gestion-del-cambio-en-la-implementacion-de-nuevas-tecnologias/

Minango, E., & Vásconez, L. (2024). Análisis comparativo de cartera de créditos en cooperativas de ahorro y crédito: riesgos y desafíos. *Cienciamatria*, *10*(1), 181–206. https://doi.org/10.35381/cm.v10i1.1217

Muñoz, H., Zapata, L., Requena, D., & Ricardo, L. (2019). Riesgos informáticos y alternativas para la seguridad informática en sistemas contables en Colombia. *Revista Venezolana de Gerencia RVG*, *24*(2), 528–541. https://doi.org/10.37960/revista.v24i2.31508

Ojeda, F., Moreno, V., & Torres, M. (2020). Gestión del riesgo y la ciberseguridad en el sector financiero popular y solidario del Ecuador. ***Cienciamatria***, ***6***(2), 192–219. https://doi.org/10.35381/cm.v6i2.366

Stender, S., Lagovska, O., Roshko, N., Soloshchak, A., & Lemishovska, O. (2025). Enhancing Business Competitiveness through Accounting Digitalization Mejora de la competitividad empresarial mediante la digitalización de la contabilidad. ***Salud, Ciencia y Tecnología***, ***4***(693). https://doi.org/10.56294/saludcyt2025693

Sullivan, G. (2020). ***Uso de las NIIF en la tributación de la economía digital***. Asociación Interamericana de Contabilidad. https://contadores-aic.org/uso-de-las-niif-en-la-tributacion-de-la-economia-digital/

Viera, L., Márquez, H., León, S., & De La Cruz, N. (2023). Utilización de canales digitales de las entidades bancarias del sector público privado. Estudio de revisión. ***Revista de Climatología***, ***23***, 1184–1201. https://doi.org/10.59427/rcli/2023/v23cs.1184-1201