09

CIBERSEGURIDAD

EN CONTABILIDAD: PROTEGIENDO LA INTEGRIDAD DE LOS DATOS FINANCIEROS EN EMPRESAS COMERCIALES

ISSN: 2631-2662

Fecha de presentación: mayo, 2024 **Fecha de aceptación:** junio, 2024 **Fecha de publicación:** agosto, 2024

CIBERSEGURIDAD

EN CONTABILIDAD: PROTEGIENDO LA INTEGRIDAD DE LOS DATOS FINANCIEROS EN EMPRESAS COMERCIALES

CYBERSECURITY IN ACCOUNTING: PROTECTING THE INTEGRITY OF FINANCIAL DATA IN COMMERCIAL ENTERPRISES

Mónica Elizabeth Calle-Tenesaca[1]
E-mail: mecallet02@est.ucacue.edu.ec
ORCID: https://orcid.org/0009-0009-7816-8472
Rolando Patricio Andrade-Amoroso[1]
E-mail: randradea@ucacue.edu.ec
ORCID: https://orcid.org/0000-0002-6078-3487
[1]Universidad Católica de Cuenca. Ecuador.

Cita sugerida (APA, séptima edición)

Calle-Tenesaca, M. E., & Andrade-Amoroso, R. P. (2024). Ciberseguridad en contabilidad: protegiendo la integridad de los datos financieros en empresas comerciales. *Revista Metropolitana de Ciencias Aplicadas*, 7(S2), 87-98.

RESUMEN

El estudio analizó la ciberseguridad en empresas de comercialización en Azogues, Ecuador, evaluando la exposición a riesgos cibernéticos, medidas de mitigación y preparación ante amenazas. Se encuestó a contadores sobre interrupciones en operaciones, tipo de amenazas y políticas de seguridad. Los resultados muestran que el comercio al por menor es predominante y que la mayoría de las empresas han considerado contratar servicios externos de ciberseguridad. Las amenazas más comunes incluyen intrusiones internas y malware. Aunque la mayoría realiza actualizaciones de software y capacita al personal en seguridad informática, aún existe preocupación por la preparación ante amenazas cibernéticas y una asignación limitada de presupuesto para ciberseguridad. Se destacan debilidades en la implementación de controles internos y la necesidad de una mayor inversión en tecnología de seguridad. En conclusión, se necesita mejorar la conciencia y la capacitación en ciberseguridad, así como aumentar la inversión para fortalecer las defensas cibernéticas y mitigar los riesgos de seguridad.

Palabras clave:

Tecnología, seguridad, comercialización, contabilidad.

ABSTRACT

The study analyzed cybersecurity in trading companies in Azogues, Ecuador, assessing cyber risk exposure, mitigation measures, and threat preparedness. Accountants were surveyed about disruptions in operations, type of threats, and security policies. The results show that retail is predominant and that most companies have considered outsourcing cybersecurity services. The most common threats include insider intrusions and malware. Although most perform software upgrades and train staff in IT security, there are still concerns about cyber threat preparedness and limited budget allocation for cybersecurity. Weaknesses in the implementation of internal controls and the need for greater investment in security technology are highlighted. In conclusion, there is a need for improved cybersecurity awareness and training, as well as increased investment to strengthen cyber defenses and mitigate security risks.

Keywords:

Technology, safety, marketing, accounting.

INTRODUCCIÓN

La ciberseguridad tiene su origen en 1987 en la Universidad de Delaware en los Estados Unidos donde se provocó el primer suceso relacionado con la seguridad de la red Internet, ocasionando un colapso en varios sistemas, considerado uno de los primeros incidentes graves de seguridad en la historia de Internet. En este contexto, tras la rápida evolución de la tecnología de la información y la digitalización de los procesos contables, se incrementa la exposición a riesgos cibernéticos, como fraudes, robos de información confidencial y manipulación de datos. Por lo tanto, se vuelve exigente proteger e implementar medidas de seguridad para salvaguardar la integridad, confidencialidad y disponibilidad de la información contable (Muñoz et al., 2019).

La ciberseguridad en los sistemas contables surge como respuesta a la rápida evolución de la tecnología de la información y la digitalización de los procesos contables. Conforme las empresas adoptan sistemas informáticos, se incrementa la exposición a riesgos cibernéticos, por lo tanto, se vuelve imperativo proteger e implementar medidas de seguridad para salvaguardar la integridad, confidencialidad y disponibilidad de la información contable. Tanto las empresas como los profesionales de la contabilidad deben establecer políticas de seguridad, controles internos y adoptar tecnologías de protección para mitigar los riesgos cibernéticos y así fortalecer la confidencialidad de la información financiera (Izaguirre & León, 2018).

En este sentido, la protección de los datos contables se convierte en una prioridad ineludible, ya que la seguridad cibernética se constituye como el escudo necesario contra amenazas que podrían comprometer la integridad y confidencialidad de la información financiera.

Con base en la información previamente expuesta, este estudio se enfocará en responder a la siguiente pregunta científica: ¿Cuáles son las vulnerabilidades más críticas en los sistemas contables y cómo pueden abordarse para asegurar la ciberseguridad y la integridad de los datos financieros en las empresas comerciales de la ciudad de Azogues, Ecuador? En este sentido, el objetivo principal radica en evaluar las amenazas de ciberseguridad presentes en los sistemas contables de las empresas comerciales de la ciudad de Azogues y proponer estrategias efectivas para proteger la integridad de los datos financieros.

En la actualidad, los inversionistas muestran un marcado interés en comprender con precisión el riesgo financiero y tomar decisiones informadas sobre la adquisición, retención o venta de sus inversiones. Para alcanzar este propósito, es indispensable que tengan acceso a estados financieros elaborados conforme a las Normas Internacionales de Información Financiera (NIIF). Estos estados financieros no solo ofrecen información relevante a los usuarios, sino que también les capacitan para realizar decisiones económicas fundamentadas. Los estados financieros representan el principal medio de comunicación de información financiera hacia agentes externos a la organización (Rodríguez, 2018).

La información financiera desempeña un papel esencial en el ámbito empresarial y financiero, siendo utilizada en todas las facetas de la actividad económica a nivel mundial desde hace varias décadas. La adopción de las NIIF es uno de los elementos más destacados en este contexto, ya que garantiza la comparabilidad, transparencia y calidad de los datos financieros, estableciendo principios contables uniformes que permiten a las empresas informar de manera consistente y comprensible. Diversos países alrededor del mundo han adoptado las NIIF o están en proceso de convergencia hacia estos estándares contables internacionales, entre ellos la Unión Europea, Estados Unidos, Canadá, Australia, Reino Unido y Brasil (Encalada et al., 2018).

En Latinoamérica, la mayoría de las empresas están elaborando sus reportes financieros bajo las NIIF, lo que ha tenido un impacto significativo. Por ejemplo, en Chile y Colombia, esta transición ha generado efectos positivos en la calidad de la información financiera para las empresas, observándose un incremento en la transparencia, una reducción en el costo de capital y mejoras en la liquidez empresarial, lo que ha resultado en una mejora general en la calidad de los resultados financieros (Contreras et al., 2019).

En la misma línea de investigación, Brasil ha implementado las NIIF desde el 2009, iniciando una tendencia seguida por otros países latinoamericanos como Argentina, Chile y México, destacándose como pioneros en la región al presentar sus estados financieros conforme a las NIIF. Por otro lado, Europa adoptó estas normas en 2005 y ha abordado los procesos, consecuencias, dificultades y resultados vinculados a dicha adopción en relación con los indicadores financieros (Celi et al., 2018).

Contrariamente, en algunos países de Latinoamérica como Bolivia, Cuba, Puerto Rico y México, no se requiere ni permite el uso de las NIIF; en su lugar, se aplica la normativa local. Sin embargo, es importante destacar que la adopción de las NIIF no es obligatoria en todos los países donde se han implementado. Por ejemplo, en Uruguay y Colombia, aunque están permitidas, su adopción plena depende de la necesidad de la empresa y el cumplimiento de ciertos requisitos (Chávez, 2020).

La implementación de las NIIF en Ecuador ha generado cambios significativos en las empresas, especialmente en las PYMES. Desde 2012, las PYMES ecuatorianas están obligadas a preparar sus estados financieros de acuerdo con las NIIF. Los requisitos de reconocimiento, medición y presentación establecidos por estas normas han motivado a las entidades ecuatorianas a ajustarse a estos estándares para mejorar la calidad de su información

contable. La transición a las NIIF implica capacitación, implementación y evaluación de impactos, asegurando así una adecuada adopción de las normas internacionales (Encalada et al., 2018).

En este contexto, la Federación de Colegios de Contadores Públicos del Ecuador comunicó en agosto de 2006, con publicación oficial el 4 de septiembre del mismo año, que las sociedades que realicen oferta pública de valores según los términos de la Ley de Mercado de Capitales están obligadas a preparar y presentar sus estados financieros de acuerdo con las NIIF y las Normas Internacionales de Contabilidad (NIC). Estas normativas buscan uniformizar la información en los estados financieros y promover la transparencia contable en Ecuador (Cando et al., 2019).

Durante varios años en Ecuador, se han aplicado los Principios Contables Generalmente Aceptados (PCGA) de acuerdo con las Normas Ecuatorianas de Contabilidad (NEC). Sin embargo, debido a la influencia de la globalización y la adopción a nivel mundial, el gobierno ecuatoriano, a través de la Superintendencia de Compañías (SIC), emitió la resolución 08.G.D. DSC.010 el 20 de noviembre de 2008. Esta resolución establece un cronograma para la implementación de las NIIF en las empresas ecuatorianas. Esta adopción implica cambios en los estados financieros, los cuales tienen un impacto notable en los ratios financieros (Celi et al., 2018).

La importancia de la información financiera radica en su capacidad para influir en las decisiones de los usuarios al proporcionar datos específicos y oportunos para evaluar la situación financiera y el rendimiento de una entidad. La información financiera relevante es aquella que puede afectar las decisiones económicas al ayudar a predecir eventos futuros, confirmar o corregir expectativas pasadas, o confirmar la exactitud de evaluaciones anteriores. La relevancia se ve reforzada cuando la información cumple con criterios como ser oportuna, confiable, comprensible y comparable. La adopción de normas internacionales, como las NIIF para las Pymes, mejora la relevancia al proporcionar un marco común y consistente. Para las pequeñas y medianas empresas, la relevancia financiera es crítica para atraer inversores, obtener financiamiento, tomar decisiones estratégicas y cumplir con requisitos regulatorios. Presentar información financiera transparente y fundamental mejora la credibilidad y confianza entre los usuarios (Encalada et al., 2018).

La aplicación de las NIIF ha suscitado debates en la comunidad contable respecto a la interpretación y discusión de los conceptos de reglas y principios desde una perspectiva legal. Se destaca la importancia de la consistencia y coherencia en las normas contables, donde la consistencia asegura que las normas no se contradigan entre sí, mientras que la coherencia se refiere a la relación entre principios y reglas. Actualmente, los iuspositivistas dan prioridad a las reglas en la discusión jurídica, mientras que los iusnaturalistas reconocen que las reglas implícitamente contienen principios y les otorgan prioridad en casos donde las reglas no resuelvan un problema o estén en conflicto. Por lo tanto, una estructura jurídica basada en reglas privilegia estas en casos de conflicto, mientras que en una estructura basada en principios, estos prevalecerán sobre las reglas (Agreda et al., 2022).

Es fundamental seguir los principios contables y regulaciones al preparar información financiera para asegurar transparencia. Sin embargo, en Ecuador, la consistencia en su aplicación puede variar debido a factores como la adopción de las NIIF y la supervisión de entidades reguladoras como la Superintendencia de Compañías, Valores y Seguros. La introducción de las NIIF ha implicado ajustes importantes en las políticas contables y en la presentación de estados financieros, lo cual puede influir en el grado de cumplimiento de los principios contables y normativas. Además, la supervisión de entidades reguladoras como la Superintendencia de Compañías, Valores y Seguros se encarga de asegurar que se cumplan las regulaciones contables en Ecuador.

Las políticas contables se refieren a los principios, bases, acuerdos, reglas y procedimientos específicos que una entidad adopta para elaborar y presentar sus estados financieros. Un análisis efectuado sobre 141 empresas listadas en la bolsa de México entre los años 2000 y 2013 revela que los ajustes en las regulaciones contables mejoran la importancia evaluativa de la información financiera. Durante este estudio, se evaluaron variables como utilidad antes de impuestos e intereses, patrimonio, rotación de activos, rotación de deuda y tamaño de la empresa. Se destaca que la información conforme a las NIIF es más fiable tanto para inversionistas nacionales como extranjeros. Además, se observa un mayor control por parte de los administradores en cuanto a la manipulación de la información (Ayabaca & Aguirre, 2018).

En relación con los informes financieros, estos documentos organizan y detallan la información financiera de una empresa durante un período específico, incluyendo estados financieros básicos como el balance general, el estado de resultados, el estado de flujo de efectivo y el estado de cambios en el patrimonio neto. Estos estados revelan datos sobre los activos, pasivos, ingresos, gastos, flujos de efectivo y cambios en el patrimonio de la empresa. Es esencial que el lenguaje empleado en estos informes sea claro y comprensible para los usuarios, fomentando así la claridad, la coherencia, la adaptación al público objetivo, la transparencia y la veracidad en la presentación de la información. Estas prácticas son fundamentales para facilitar una comunicación efectiva y promover una toma de decisiones informada en el ámbito empresarial (Carranza, 2019).

La evaluación integral de ciberseguridad constituye un proceso minucioso y exhaustivo diseñado para analizar y evaluar todos los elementos vinculados con la seguridad informática de una entidad. Este análisis aborda diversas

dimensiones, que incluyen aspectos técnicos, humanos, organizativos y legales, con el objetivo de identificar posibles vulnerabilidades, riesgos y amenazas que puedan afectar la seguridad de la información y los activos digitales de la organización. Al llevar a cabo esta evaluación integral, se pueden ejecutar diversas actividades, como el análisis de la infraestructura tecnológica, que permite evaluar sistemas, redes, aplicaciones y dispositivos en busca de posibles fallos de seguridad y vulnerabilidades. Asimismo, se incluye la evaluación de políticas y procedimientos para asegurar su actualización y eficacia. Además, la evaluación de conciencia y capacitación garantiza que los empleados cuenten con un amplio conocimiento en ciberseguridad, capacitándolos para identificar y responder a posibles amenazas.

En este sentido, los activos digitales comprenden elementos de valor que una organización o individuo posee en formato digital, como información confidencial, datos personales, propiedad intelectual, software, bases de datos, documentos electrónicos y contraseñas, entre otros recursos digitales esenciales para el desarrollo de las operaciones de una entidad. La protección de estos activos digitales se vuelve imperativa para preservar la seguridad de la información y prevenir posibles ciberataques que puedan comprometer la integridad, confidencialidad y disponibilidad de dichos recursos. La gestión eficaz de los activos digitales implica la aplicación de medidas de seguridad, políticas de acceso, respaldo de datos, cifrado y otras prácticas diseñadas para mitigar riesgos y garantizar la continuidad ininterrumpida de las operaciones (Izaguirre & León, 2018).

Los activos digitales son esenciales para el funcionamiento de una organización, abarcan datos, sistemas de información, infraestructura tecnológica, software, propiedad intelectual y la reputación online. La protección efectiva de estos elementos, mediante medidas de ciberseguridad, políticas de acceso y uso, copias de seguridad y cifrado de datos, resulta esencial para garantizar la seguridad de la información, asegurar la continuidad del negocio y preservar la reputación de la organización en el entorno digital (Caamaño & Gil, 2020).

La gestión de riesgos implica un proceso continuo de identificación, evaluación y respuesta ante posibles amenazas. Para abordar estos riesgos de manera efectiva, las organizaciones necesitan comprender tanto la probabilidad de ocurrencia de un evento como su posible impacto. El contexto empresarial desempeña un papel crucial en las decisiones sobre riesgos; por ejemplo, una pequeña empresa puede ser más tolerante al riesgo que una empresa grande y consolidada. Conscientes de que la exposición a un riesgo puede generar pérdidas financieras, resulta esencial estimar su impacto mediante la implementación de controles (Ortega, 2021).

La gestión de riesgos de ciberseguridad es un proceso que busca identificar, evaluar y mitigar los riesgos vinculados a la seguridad de la información y la tecnología en una organización. Esto implica la aplicación de medidas preventivas y correctivas para resguardar los activos de información contra posibles amenazas cibernéticas. Las actividades clave en este proceso incluyen la identificación de riesgos, catalogando posibles amenazas como malware, phishing o robo de datos. Luego, se evalúa la probabilidad de ocurrencia y el impacto potencial en la organización. Después de identificar y evaluar los riesgos, se implementan medidas de mitigación, como controles de seguridad y políticas internas. El monitoreo constante y la revisión periódica de las medidas de seguridad son esenciales para adaptarse a las nuevas amenazas cibernéticas. En un mundo digital y conectado, la gestión de riesgos de ciberseguridad resulta fundamental para salvaguardar la información sensible y garantizar la continuidad operativa de la organización (Caamaño & Gil, 2020).

Los sistemas contables desempeñan un papel crucial en la gestión de la información financiera y contable. Sin embargo, están expuestos a una variedad de riesgos que pueden comprometer la integridad, confidencialidad y disponibilidad de los datos. Uno de estos riesgos es el acceso no autorizado, donde personas ajenas pueden ingresar a los sistemas contables y manipular la información financiera de la empresa, lo que podría resultar en fraudes o alteraciones de los registros contables. El delito de phishing también representa una amenaza, ya que los perpetradores se infiltran mediante correos electrónicos con el objetivo de obtener información confidencial de las empresas. Además, la fuga de información, que implica la divulgación de datos sensibles a terceros no autorizados, y la falta de actualizaciones de seguridad en los sistemas contables, pueden dejarlos vulnerables a ataques cibernéticos. Para mitigar estos riesgos, es fundamental implementar medidas de seguridad robustas, como el cifrado de datos, capacitación en ciberseguridad para el personal y copias de seguridad regulares (Ojeda et al., 2020).

Los controles de seguridad constituyen medidas o acciones destinadas a salvaguardar los activos de información de una organización ante posibles amenazas y riesgos. Estos controles se rigen por estándares y marcos de referencia, como la norma ISO 27001, que ofrece un enfoque sistemático para establecer, implementar, mantener y mejorar un sistema de gestión de la seguridad de la información. Asimismo, la norma ISO 27002 proporciona un conjunto de controles y buenas prácticas específicas para la seguridad de la información en una organización (Muñoz et al., 2019).

En el contexto ecuatoriano, la falta de coordinación y políticas definidas en materia de ciberseguridad ha generado un entorno poco sistemático. Esta carencia se refleja en la ausencia de un plan de acciones unificado para todas las entidades del país. Además, la falta de previsión

por parte del gobierno en este ámbito ha dejado abierta la posibilidad de que la gestión tecnológica de la infraestructura e información nacional se vea vulnerable ante amenazas externas. Esta situación recalca la urgencia de rediseñar la organización de la política de ciberdefensa en todos sus niveles. Para lograr esto, se necesitarán acciones coordinadas a nivel gubernamental, junto con la implementación de políticas claras y la promulgación de legislación adecuada. Solo así se podrá proteger de manera eficaz la infraestructura digital y la información del país (Vargas et al., 2017).

En cuanto a la legislación ecuatoriana, la sección tercera del Código Orgánico Integral Penal aborda los delitos contra la seguridad de los activos de los sistemas de información y comunicación. Por ejemplo, el artículo 229 establece que revelar ilegalmente la base de datos con el propósito de violar el secreto, intimidad y privacidad de las personas, conlleva una pena de uno a tres años de prisión. El artículo 230 sanciona la interceptación ilegal de datos con tres a cinco años de prisión, incluyendo diversas acciones como la interceptación, escucha, desviación o copia de información sin autorización. El artículo 232 castiga los ataques a la integridad de sistemas informáticos con tres a cinco años de prisión, cubriendo acciones como la destrucción o alteración de datos informáticos. Por último, el artículo 234 penaliza el acceso no consentido a sistemas informáticos con tres a cinco años de prisión, incluyendo la explotación ilegítima de dicho acceso y la modificación de portales web sin autorización (Ecuador. Asamblea Nacional, 2021).

MATERIALES Y MÉTODOS

Se llevó a cabo un estudio utilizando un enfoque cuali-cuantitativo dentro de un marco de investigación no experimental. Este estudio adoptó un alcance descriptivo-explicativo con una finalidad transversal, realizado en un solo momento del tiempo.

Los métodos empleados para esta investigación incluyeron el método histórico-lógico, que permitió examinar la evolución histórica de la ciberseguridad en el ámbito contable, identificando patrones y tendencias que ayudaron a contextualizar los desafíos actuales en este campo. Al comprender la evolución de la ciberseguridad en el contexto contable a lo largo del tiempo, se estableció una base sólida para analizar y abordar los problemas actuales. Por otro lado, el método inductivo-deductivo se utilizó para derivar conclusiones generales a partir de la recopilación de datos sobre incidentes de seguridad y prácticas de protección de datos en empresas comerciales, lo que permitió formular teorías sobre cómo mejorar la ciberseguridad en este ámbito. Finalmente, el método comparativo permitió contrastar diferentes enfoques, estrategias y prácticas de ciberseguridad utilizadas en diversas empresas comerciales, identificando las mejores prácticas y lecciones aprendidas que podrían aplicarse para mejorar la protección de la integridad de los datos financieros en el contexto contable.

La técnica principal empleada fue la encuesta, compuesta por 22 ítems relacionados con la ciberseguridad en contabilidad y la información financiera. Este instrumento se aplicó en forma de cuestionario, diseñado específicamente para este estudio.

La unidad de análisis estuvo conformada por empresas de comercialización ubicadas en la ciudad de Azogues. El muestreo se realizó por conveniencia, seleccionando un total de 33 empresas representadas por sus contadores que cumplían con los criterios establecidos para participar en la investigación.

Para el análisis estadístico de los datos recopilados a través de la encuesta, se empleó el software JASP. Esta herramienta proporcionó una plataforma eficiente y confiable para realizar análisis estadísticos avanzados, facilitando la interpretación de los resultados y la generación de conclusiones específicas. El uso de JASP permitió realizar análisis descriptivos, inferenciales y exploratorios, contribuyendo así al rigor y la validez de los hallazgos de la investigación.

RESULTADOS Y DISCUSIÓN

Sector económico: los resultados revelan que la mayoría de las empresas de comercialización encuestadas en la ciudad de Azogues se enfocan en el sector del comercio al por menor, lo que representa el 51.52%. Por otro lado, el comercio al por mayor muestra una presencia abrumadora, con 16 respuestas, equivalente al 48.48%.

Interrupción en las operaciones: entre los encuestados, un 48.50% indica que sus empresas nunca han experimentado una interrupción en las operaciones comerciales debido a un incidente de seguridad cibernética en los sistemas contables. Sin embargo, un porcentaje 18.20% reporta haber experimentado interrupciones tanto en varias ocasiones y el 21.20% de manera esporádica. Además, un 12.12% de los encuestados no están seguros si su empresa ha experimentado tales interrupciones.

Servicios externos, amenazas y vulnerabilidades de ciberseguridad: se observa en los resultados que la mayoría de las empresas que han identificado menos de 5 amenazas y vulnerabilidades han considerado la posibilidad de contratar servicios externos de ciberseguridad, mientras que un número similar de empresas en esta categoría no lo han considerado. Por otro lado, la mayoría de las empresas que han identificado entre 2 y 5 sistemas con amenazas y vulnerabilidades también han considerado esta posibilidad. Además, la única empresa que identificó más de 10 amenazas y vulnerabilidades no ha considerado la posibilidad de contratar servicios externos de ciberseguridad**.**

Tipo de amenazas: Durante los últimos 12 meses, se han experimentado varias amenazas de ciberseguridad en

los sistemas contables de las empresas encuestadas. Entre las más comunes se encuentran las intrusiones internas, reportadas por el 33.33% de los encuestados, seguidas por el ***malware***, con un 27.27%. También se destacan los ataques de denegación de servicio (DDoS), que representan el 15.15% de las respuestas. El ***phishing*** también ha sido una amenaza reveladora, reportada por el 18.18% de los encuestados. Además, un pequeño porcentaje de encuestados mencionó otras amenazas no especificadas.

Afección de la integridad de los datos financieros: Los datos revelan que la mayoría de los encuestados, un 57.58%, califican la probabilidad de que las amenazas afecten la integridad de los datos financieros de manera moderada. Esto sugiere una percepción de riesgo significativa, pero no inmediata, en cuanto a la seguridad de los datos financieros. Además, un porcentaje considerable de encuestados, el 24.24%, considera que la probabilidad de impacto es alta, lo que refleja una preocupación sustancial por la seguridad de los datos financieros frente a estas amenazas. Por otro lado, un pequeño grupo, el 18.18% (ver tabla 1), califica la probabilidad como baja.

Tabla 1. Afecciones según las amenazas de ciberseguridad.

¿Cómo calificaría la probabilidad de que estas amenazas afecten la integridad de los datos financieros?		Frecuencia		Porcentaje		Porcentaje Válido		Porcentaje Acumulado	
a) Baja		6		18.182		18.182		18.182	
b) Moderada		19		57.576		57.576		75.758	
c) Alta		8		24.242		24.242		100.000	
Total		33		100.000					

Sistemas de gestión financiera y contable: el 72.73% de encuestados utiliza un único sistema de gestión financiera y contable. Esto propone una tendencia hacia la consolidación de las funciones contables y financieras en un único sistema integrado. Sin embargo, un porcentaje característico de las empresas 21.21% utiliza entre 2 y 5 sistemas diferentes para estas funciones, lo que puede indicar una mayor complejidad en la estructura de gestión financiera y contable. Además, un pequeño número de empresas (6.06%) utiliza más de 5 sistemas, lo que podría implicar una fragmentación característica en la gestión de datos financieros y contables.

Medidas de mitigación: los resultados revelan que las empresas han implementado una variedad de medidas de mitigación para reducir los riesgos de ciberseguridad. La más común es la realización de actualizaciones regulares de software, con un porcentaje del 54.55%. Esto indica una atención específica a mantener los sistemas actualizados para abordar vulnerabilidades conocidas. Además, el 6.06% siendo un pequeño porcentaje de empresas ha implementado ***firewalls*** y sistemas de detección de intrusiones y han efectuado controles de seguridad 12.12% d. Por otro lado, la capacitación del personal en seguridad informática también ha sido una medida destacada, con un 21.21% de las respuestas.

Políticas y procedimientos: la investigación muestra una variedad de respuestas en cuanto a la implementación y claridad de las políticas y procedimientos específicos para proteger la integridad de los datos financieros en los sistemas contables de las empresas encuestadas. El 30.30% de los encuestados afirmaron contar con políticas y procedimientos bien definidos, mientras que un 18.18% mencionó tener políticas y procedimientos, pero estos no están definidos ni implementados de forma clara. Además, un 15.15% de los encuestados indicaron que sus empresas no cuentan con políticas ni procedimientos específicos en absoluto. Por otro lado, un número considerable de encuestados, el 18.18%, expresó incertidumbre sobre este aspecto.

Políticas de acceso y autenticación: las políticas de acceso y autenticación aplicadas a los sistemas contables de las empresas encuestadas se centran en el uso de contraseñas fuertes y el cambio regular, con un 54.55% de las respuestas. Esto indica una práctica común de seguridad para proteger el acceso a los sistemas contables. Además, un porcentaje específico de empresas con el 27.27% emplea la restricción de acceso basada en roles, lo que sugiere una gestión más granular de los permisos de acceso según las funciones y responsabilidades de los usuarios. Además, un 18.18% de las empresas aplican autenticación de dos factores, lo que agrega una capa adicional de seguridad para verificar la identidad de los usuarios.

Auditorías de cumplimiento en materia de seguridad: los datos reflejan que el 27.27% de las empresas ha llevado a cabo de forma regular auditorías de cumplimiento en materia de seguridad de la información, lo que propone un compromiso continuo con la evaluación y mejora de los estándares de seguridad de la información. Además, un 18.18% lleva a cabo estas auditorías de forma ocasional, lo que indica una atención periódica menos frecuente a este aspecto. Sin embargo, un número considerable de empresas, el 54.55% aún no ha realizado auditorías.

Nivel de vulnerabilidad: según los resultados, el nivel de vulnerabilidad de los sistemas contables de la empresa en relación con posibles amenazas cibernéticas muestra una distribución específica. Un 12.12% de los encuestados califica los sistemas como muy vulnerables, mientras que el 30.30% los considera moderadamente vulnerables. Por otro lado, un 36.36% los percibe como poco vulnerables. Es notable que un 21.21% de los encuestados indican no estar seguros de la vulnerabilidad de los sistemas contables.

Formación en seguridad informática: según los encuestados, un 69.70%, indican que menos del 25% de los empleados de la empresa recibe formación en seguridad de la información. Además, un 21.21% señala que entre el 25% y el 50% de los empleados recibe esta formación, mientras que solo un 9.09% afirma que más del 50% (ver tabla 2) de los empleados recibe este tipo de formación.

Tabla 2. Formación en seguridad informática.

¿Qué porcentaje de empleados de la empresa recibe formación en seguridad de la información?	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
a) Menos del 25%	23	69.697	69.697	69.697
b) Entre 25% y 50%	7	21.212	21.212	90.909
c) Más del 50%	3	9.091	9.091	100.000
Total	33	100.000		

Medidas de mitigación: tras la indagación, los resultados exteriorizan una variedad de medidas de mitigación implementadas en las empresas encuestadas para reducir los riesgos de ciberseguridad. El 48.48% de los encuestados indicaron haber implementado antivirus, lo que sugiere que esta es una medida de seguridad adoptada. Además, un 24.24% mencionó realizar actualizaciones regulares de software, lo que es concluyente para mantener los sistemas protegidos contra vulnerabilidades conocidas. La capacitación en seguridad para empleados también se mencionó, aunque en menor medida, con un 9.09% de los encuestados. Además, hubo menciones de otras medidas de mitigación no especificadas, lo que indica una diversidad en los enfoques utilizados por las empresas. Sin embargo, es notable que solo un 12.12% mencionó el uso de firewall como medida de mitigación.

Amenazas de ciberseguridad en los datos financieros: En cuanto al impacto de las amenazas de ciberseguridad en la integridad de los datos financieros de la organización, se observa que el 6.06% de los encuestados reportaron un impacto muy alto, mientras que otro 6.06% indicaron un impacto alto. Por otro lado, el 48.48% de los encuestados señalaron un impacto moderado, y el 33.33% reportaron un impacto bajo. Solo el 6.06% (ver figura 1) afirmaron que no han experimentado ningún impacto.

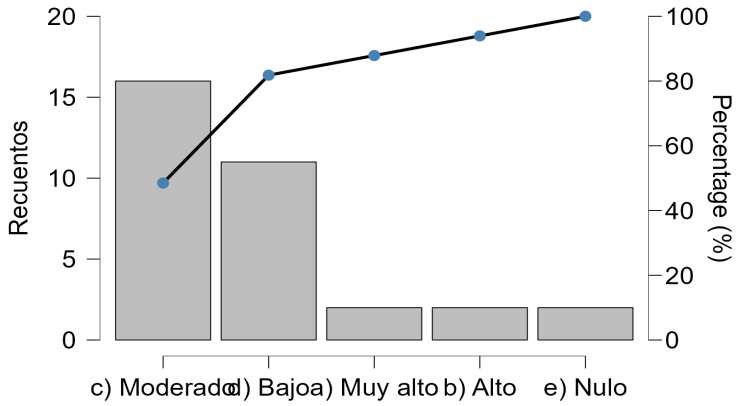

Figura 1. Amenazas de ciberseguridad en los datos financieros.

Evaluaciones de seguridad cibernética: existe una variedad de prácticas en cuanto a la frecuencia de las evaluaciones de seguridad cibernética en los sistemas contables de las empresas. Un 27.27% de los encuestados indicaron que se realizan evaluaciones periódicas, al menos una vez al año, mientras que un 45.45% señalaron que estas evaluaciones ocurren de forma ocasional, cada varios años. Por otro lado, un 15.15% de los encuestados manifestaron no estar seguros de la frecuencia de estas evaluaciones, y un 12.12% (ver tabla 3) indicaron que en su empresa no se realizan evaluaciones de seguridad cibernética en absoluto.

Tabla 3. Evolución de seguridad cibernética.

¿Con qué frecuencia se realizan evaluaciones de seguridad cibernética en los sistemas contables de la empresa donde labora?	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
d) No estoy seguro	5	15.152	15.152	15.152
a) Regular (al menos una vez al año)	9	27.273	27.273	42.424
b) Ocasional (cada varios años)	15	45.455	45.455	87.879
c) No se realizan evaluaciones de seguridad cibernética	4	12.121	12.121	100.000
Total	33	100.000		

Mejoras para fortalecer la ciberseguridad: la encuesta revela varias sugerencias para fortalecer la ciberseguridad en los sistemas contables. El 45.45%, indicaron que una mayor inversión en tecnología de seguridad sería una mejora necesaria. Además, el 21.21% sugirió implementar políticas de seguridad más estrictas. Otras sugerencias incluyen mejorar la capacitación en seguridad para empleados, con un 12.12% de los encuestados respaldando esta idea. Solo un pequeño porcentaje mencionó otras mejoras específicas o no proporcionaron una respuesta clara.

Presupuesto anual destinado para la ciberseguridad: los resultados muestran una distribución diversa en cuanto al porcentaje del presupuesto anual destinado a actividades relacionadas con la ciberseguridad de los sistemas contables. Un tercio de los encuestados que representan el 33.33% indicaron que destinan menos del 1% de su presupuesto a este fin, mientras que otro tercio el 36.36% asigna entre el 1% y el 5%. Solo un pequeño porcentaje, el 12.12% dedica entre el 5% y el 10% de su presupuesto, y el 6.06% de encuestados no están seguros sobre este aspecto. Además, un 6.06% mencionó que no se destina un presupuesto específico a ciberseguridad, y otro 6.06% destinan más del 10% de su presupuesto para estas actividades.

Preparación de la organización frente a las amenazas: los resultados indican que hay una preocupante tendencia entre los encuestados respecto a la preparación de sus organizaciones para hacer frente a amenazas cibernéticas. El 54.55% considera que su organización está poco preparada, mientras que otro 27.27% la califica como preparada. Sin embargo, solo el 9.09% la percibe como muy preparada, y el mismo porcentaje, 9.09%, la considera nada preparada.

Pérdidas financieras: el 51.52% de los encuestados informaron que sus empresas no han experimentado pérdidas financieras, mientras que el 15.15% mencionó haber experimentado pérdidas menores y un 6.06% reportó pérdidas representativas. Sin embargo, es importante destacar que un 12.12% de los encuestados expresaron incertidumbre sobre este tema, lo que sugiere una falta de claridad o en cuanto a los impactos financieros de los incidentes de seguridad cibernética**.**

Copias de seguridad: los resultados muestran que un 36.36% de los encuestados indicaron que realizan copias de seguridad todos los días, mientras que otro 30.30% lo hace semanal. Además, un 15.15% realiza copias de seguridad cada mes y otro 15.15% de manera ocasional, cada varios meses. Sin embargo, es preocupante observar que un pequeño porcentaje, el 3.03%, indicó que no se realizan copias de seguridad en absoluto.

Medidas para implementar: un considerable porcentaje, el 36.36% de los encuestados señalaron, la falta de conciencia y comprensión sobre ciberseguridad por parte del personal es percibida como el principal desafío para implementar medidas en los sistemas contables de las empresas encuestadas, seguido por la falta de recursos financieros para invertir en tecnología y capacitación en ciberseguridad, con un 21.21%. Otros desafíos mencionados incluyen la complejidad y diversidad de las amenazas cibernéticas, que representan el 15.15% de las respuestas.

En este estudio, se lleva a cabo un análisis exhaustivo de los riesgos cibernéticos en las empresas de comercialización en la ciudad de Azogues, proporcionando una panorámica amplia de las amenazas que enfrentan estas empresas en su conjunto. Por otro lado, el estudio realizado por Poma & Huamán (2023), se enfoca en una evaluación más específica dentro de una empresa particular, en este caso, Jama-Café Restaurant. En este estudio se exploran las percepciones de los trabajadores sobre los problemas de ciberseguridad y las estrategias para mitigarlos.

Al comparar los resultados de ambos estudios, se observa que las amenazas cibernéticas identificadas, como los troyanos, virus y otras formas de malware, son mencionadas tanto en el contexto global de las empresas de comercialización como en el ámbito interno de la empresa Jama-Café Restaurant. Esto resalta la necesidad de implementar medidas de protección adecuadas en todos los niveles, desde el ámbito más amplio de la industria hasta el entorno específico de cada organización.

Además, ambos estudios subrayan la importancia de la conciencia y la capacitación en ciberseguridad. Mientras que el primer estudio destaca la necesidad de implementar estrategias de prevención en todas las empresas de comercialización, el segundo estudio muestra cómo la capacitación y la adopción de buenas prácticas por parte del personal pueden contribuir de manera significativa a mitigar los riesgos dentro de una empresa específica como Jama-Café Restaurant.

En paralelo, el presente estudio se enfoca en identificar amenazas y describir factores de riesgo comunes en las empresas comerciales de la ciudad de Azogues, mientras que el estudio de Peña et al. (2023), aborda la aplicación de la ley y la percepción de los especialistas sobre el marco legal existente en Ecuador. Nuestro estudio proporciona una visión detallada de las amenazas de ciberseguridad, identificando los tipos de ataques más comunes en el panorama actual. Esto establece una base sólida para comprender las diversas formas en que los sistemas informáticos pueden ser comprometidos y los posibles impactos que estos ataques pueden tener en la integridad y disponibilidad de los datos en los sistemas contables. Además, resalta la importancia de implementar soluciones de detección y prevención de ataques para mitigar estos riesgos.

Por otro lado, el estudio legal ofrece una perspectiva más regulatoria sobre la ciberseguridad, centrándose en la aplicación de la ley y el análisis del marco legal existente en Ecuador. Se destaca la preocupación por la confidencialidad de la información y la protección de la privacidad individual, pero también se señala la necesidad de una legislación más amplia que aborde aspectos como la integridad y disponibilidad de la información, así como la protección de sistemas y redes (Peña et al., 2023). Además, se discuten los desafíos específicos que enfrentan los profesionales del derecho al juzgar delitos de ciberseguridad, incluida la falta de evidencia física y la rápida evolución de las amenazas cibernéticas.

Al comparar ambos estudios, se evidencia una intersección entre los aspectos técnicos y legales de la ciberseguridad. Ambos coinciden en la necesidad de conciencia, capacitación especializada y colaboración internacional para abordar las amenazas cibernéticas, especialmente en países en desarrollo como Ecuador. Esta convergencia destaca la importancia de abordar la ciberseguridad desde una perspectiva integral que combine tanto aspectos técnicos como legales para garantizar la protección efectiva de los sistemas de información y la integridad de los datos en el entorno empresarial actual.

En el presente estudio enfocado en las empresas de comercialización en Azogues, se observa una preocupación generalizada por las amenazas cibernéticas, especialmente en lo que respecta a la interrupción de operaciones, la integridad de los datos financieros y la vulnerabilidad de los sistemas contables. Aunque la mayoría de las empresas encuestadas han implementado medidas de mitigación, como actualizaciones de software y políticas de acceso, aún persiste una percepción de vulnerabilidad y una falta de preparación para enfrentar estas amenazas.

Por otro lado, el estudio realizado en la Cooperativa de Ahorro y Crédito la Merced (Ojeda et al., 2020) revela una mayor conciencia sobre los riesgos cibernéticos entre los encuestados, particularmente en relación con delitos informáticos como el ***phishing*** y el ***malware***. Aunque la implementación de nuevas tecnologías se percibe como beneficiosa en términos de eficiencia y respuesta a las demandas del mercado, también se reconoce la necesidad de mejorar la gestión de riesgos en el contexto de la banca digital.

Una de las principales diferencias entre ambos estudios radica en la percepción de la preparación y la gestión de riesgos. Mientras que en las empresas de comercialización en Azogues existe una preocupación generalizada y una percepción de vulnerabilidad, en la Cooperativa de Ahorro y Crédito la Merced se observa una mayor conciencia sobre los riesgos cibernéticos. En términos de medidas de mitigación, ambos estudios coinciden en la importancia de implementar políticas de seguridad, realizar actualizaciones de software y capacitar al personal en seguridad informática. Sin embargo, mientras que en las empresas de comercialización se destaca la necesidad de políticas y procedimientos más claros, en la cooperativa se enfatiza la importancia de una cultura de riesgo y una gestión más técnica de los riesgos cibernéticos.

CONCLUSIONES

Se ha observado un aumento en la exposición a riesgos cibernéticos debido a la rápida evolución de la tecnología de la información y la digitalización de los procesos contables. Este fenómeno marca la importancia de implementar medidas de seguridad robustas para proteger la integridad, confidencialidad y disponibilidad de la información contable.

Existe una preocupación significativa sobre la preparación de las organizaciones para hacer frente a las amenazas cibernéticas, con el 54.55% de los encuestados considerando que sus organizaciones están poco preparadas para enfrentar estas amenazas. Este dato revela una necesidad urgente de mejorar la preparación y la respuesta ante incidentes cibernéticos.

A pesar de la creciente amenaza de ataques cibernéticos, una proporción considerable de empresas destina una parte limitada de su presupuesto anual a actividades relacionadas con la ciberseguridad. Por ejemplo, el 33.33% asigna menos del 1% de su presupuesto para este fin. Esto subraya la necesidad de una mayor inversión en tecnología y recursos para fortalecer las defensas cibernéticas y mitigar los riesgos de seguridad.

Si bien la mayoría de las empresas realizan copias de seguridad de los datos financieros almacenados en los sistemas contables con cierta frecuencia, todavía existe un pequeño porcentaje (3.03%) que no realiza copias de seguridad en absoluto. Además, aunque algunas medidas de mitigación, como las actualizaciones regulares de software y la capacitación del personal en seguridad informática, son comunes, otras, como la implementación de firewalls, son menos utilizadas. Esto indica la necesidad de una adopción más amplia de prácticas de ciberseguridad fundamentales para proteger los activos de información de las empresas.

Las vulnerabilidades más críticas en los sistemas contables de las empresas comerciales de Azogues, Ecuador, incluyen el acceso no autorizado, phishing y malware, fuga de información y falta de actualizaciones de seguridad. Para abordar estas amenazas y asegurar la ciberseguridad y la integridad de los datos financieros, es fundamental implementar autenticación multifactor, contraseñas robustas y controles de acceso basados en roles. Además, capacitar al personal en ciberseguridad, utilizar filtros avanzados de correo electrónico, software antivirus actualizado, cifrado de datos y políticas estrictas de privacidad. También es crucial realizar actualizaciones regulares de software y aplicar parches de seguridad inmediatamente para corregir fallas y prevenir ataques cibernéticos.

REFERENCIAS BIBLIOGRÁFICAS

Agreda, E., Rincón, C., & Molina, F. (2022). El debate de los principios y reglas en la normatividad contable internacional. ***Entramado***, 18(2). https://doi.org/10.18041/1900-3803/entramado.2.7890

Ayabaca Mogrovejo, O. F., & Aguirre Maxi, J. C. (2018). Estudio de la adopción de las normas internacionales de información financiera en el sector industrial y comercial de Cuenca, sus principales ajustes y políticas contables. ***Revista Economía Y Política***, ***2***(28), 9–19. https://doi.org/10.25097/rep.n28.2018.01

Caamaño, E., & Gil, R. (2020). Prevención de riesgos por ciberseguridad desde la auditoria. ***NOVUM, Revista de Ciencias Sociales Aplicadas***, 1(10), 61-80. https://revistas.unal.edu.co/index.php/novum/article/view/84210/73653

Cando, J., Cunuhay, L., Tualombo, M., & Toaquiza, S. (2019). Impactos de las NIC y las NIIF en los estados financieros. ***Ciencias economicas y empresariales***, 9(40), 329-339. https://doi.org/10.23857/fipcaec.v5i14.175

Carranza, M. (2019). La norma internacional de contabilidad 16 y su efecto en los estados financieros de las empresas agroindustriales. ***Revista ciencia y tecnología, 15***(3), 85-95. https://revistas.unitru.edu.pe/index.php/PGM/article/view/2524

Celi, M., Villegas, F., Gaibor, F., & Robles, M. (2018). Expectativas y realidades sobre la implementación de las NIIF en las empresas comerciales más grandes de Ecuador. ***Espacios, 39***(06). https://www.revistaespacios.com/a18v39n06/a18v39n06p01.pdf

Chávez, A. (2020). A 10 años de publicación de las NIIF para Pymes. Su adopción en la actividad hotelera en Latinoamérica. ***Espacios, 41***(19), 166-178. https://www.revistaespacios.com/a20v41n19/a20v41n19p12.pdf

Contreras, H., Carrasco, G., & Altamirano, F. (2019). Aplicación de las NIIF en Colombia y Chile: un análisis exhaustivo sobre la calidad de la información financiera. ***Contabilidad, auditoría y gestión empresarial, 17***, 1-14. https://doi.org/10.35928/cr.vol17.2019.75

Ecuador. Asamblea Nacional. (2021). Código Orgánico Integral Penal. https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

Encalada, V., Encarnación, O., & Ruíz, S. (2018). Norma internacional de información financiera: diseño e implementación en las pequeñas y medianas empresas. ***Revista Internacional de Investigación e Innovación Tecnológica, 6***(35). https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2007-97532018000500001

Izaguirre Olmedo, J., & León Gavilánez, F. (2018). Análisis de los ciberataques realizados en América Latina. ***INNOVA Research Journal***, ***3***(9), 172–181. https://doi.org/10.33890/innova.v3.n9.2018.837

Muñoz Hernández, H., Zapata Cantero, L. G., Requena Vidal, D. M., & Ricardo Villadiego, L. (2020). Riesgos informáticos y alternativas para la seguridad informática en sistemas contables en Colombia. ***Revista Venezolana De Gerencia***, ***24***(2), 528-541. https://doi.org/10.37960/revista.v24i2.31508

Ojeda-Contreras, F., Moreno-Narváez, V., & Torres-Palacios, 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

Ortega, J. (2021). ***Ciberseguridad manual práctico.*** Ediciones Paraninfo, SA.

Peña Guano, S., Castillo Cruz, E., & Peña Guano, P. (2023). Elementos de ciberseguridad en los países en desarrollo y su impacto en la seguridad nacional: una encuesta sobre el derecho informático en Ecuador. ***Serie Científica De La Universidad De Las Ciencias Informáticas***, ***16***(12), 1-18. https://publicaciones.uci.cu/index.php/serie/article/view/1495

Poma Vargas, A. E., & Huamán Gonzales, C. L. (2023). Ciberseguridad y calidad de vida digital en una empresa de Trujillo. ***YACHAQ***, ***6***(2), 91–123. https://doi.org/10.46363/yachaq.v6i2.4

Rodríguez, J. (2018). Elementos clave para definir el concepto de utilidad en la información financiera. ***Actualidad Contable Faces, 21***(36), 136-150. https://www.redalyc.org/journal/257/25754826007/html/

Vargas Borbúa, R., Reyes Chicango, R. P., & Recalde Herrera, L. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa. ***URVIO. Revista Latinoamericana De Estudios De Seguridad***, (20), 31–45. https://doi.org/10.17141/urvio.20.2017.2571