CIENCIAMATRIA
Revista Interdisciplinaria de Humanidades, Educación, Ciencia y Tecnología
Año X. Vol. X. N°2. Edición Especial II. 2024
Hecho el depósito de ley: pp201602FA4721
ISSN-L: 2542-3029; ISSN: 2610-802X
Instituto de Investigación y Estudios Avanzados Koinonía. (IIEAK). Santa Ana de Coro. Venezuela

DOI 10.35381/cm.v10i2.1324

Medidas de ciberseguridad aplicadas a los softwares contables en las PYMES de Cuenca, Ecuador

Cybersecurity measures applied to accounting software in SMEs in Cuenca

Paola Verónica Guachún-Orellana
paola.guachun.52@est.ucacue.edu.ec
Universidad Católica de Cuenca, Cuenca, Azuay
Ecuador
https://orcid.org/0009-0006-2239-3230

Rolando Patricio Andrade-Amoroso
randradea@ucacue.edu.ec
Universidad Católica de Cuenca, Cuenca, Azuay
Ecuador
https://orcid.org/0000-0002-6078-3487

Recibido: 20 de diciembre 2023
Revisado: 10 de enero 2024
Aprobado: 01 de abril 2024
Publicado: 15 de abril 2024

CIENCIAMATRIA
Revista Interdisciplinaria de Humanidades, Educación, Ciencia y Tecnología
Año X. Vol. X. N°2. Edición Especial II. 2024
Hecho el depósito de ley: pp201602FA4721
ISSN-L: 2542-3029; ISSN: 2610-802X
Instituto de Investigación y Estudios Avanzados Koinonía. (IIEAK). Santa Ana de Coro. Venezuela

Paola Verónica Guachún-Orellana; Rolando Patricio Andrade-Amoroso

RESUMEN

El estudio aborda la ciberseguridad en PYMES de España, Colombia y Ecuador, enfocándose en la seguridad de los softwares contables. Destaca la falta de conciencia y medidas preventivas ante amenazas cibernéticas. Se empleó una metodología descriptiva con encuestas a contadores en donde se destaca una preferencia por sistemas digitales en empresas pequeñas. Los resultados muestran una preocupante subestimación de la ciberseguridad como inversión estratégica, agravada por la falta de coordinación institucional. Aunque hay conciencia sobre las amenazas, muchas empresas carecen de medidas básicas de protección y recursos asignados para la ciberseguridad. Se observa una correlación entre la elección del sistema contable y la exposición a diferentes riesgos cibernéticos. Las conclusiones resaltan la necesidad de aumentar la conciencia y la preparación en ciberseguridad para proteger los datos financieros, además de impulsar una mejor coordinación entre el sector público y privado para fortalecer la seguridad en los softwares contables en las PYMES.

Descriptores: Protección de datos; derecho a la privacidad; control de la comunicación. (Tesauro UNESCO).

ABSTRACT

The study addresses cybersecurity in SMEs in Spain, Colombia and Ecuador, focusing on the security of accounting software. It highlights the lack of awareness and preventive measures against cyber threats. A descriptive methodology was used with surveys of accountants, highlighting a preference for digital systems in small companies. The results show a worrying underestimation of cyber security as a strategic investment, compounded by a lack of institutional coordination. Although there is awareness of the threats, many companies lack basic protection measures and resources allocated to cybersecurity. A correlation is observed between the choice of accounting system and exposure to different cyber risks. The findings highlight the need to increase cybersecurity awareness and preparedness to protect financial data, as well as to foster better coordination between the public and private sector to strengthen the security of accounting software in SMEs.

Descriptors: Data protection; right to privacy; communication control. (UNESCO Thesaurus).

INTRODUCCIÓN

En la era actual, la tecnología ha elevado la productividad de las organizaciones a niveles sin precedentes. No obstante, junto con sus beneficios, también surgen una serie de desafíos de seguridad que requieren atención y soluciones efectivas. En España, a mediados del año 2017, se detectaron cifras preocupantes relacionadas con la ciberseguridad en las PYMES. El 25% de ellas carecía de programas antivirus, el 50% no actualizaban sus sistemas operativos, el 47% no implementaba contraseñas de acceso para los distintos módulos de sus sistemas informáticos y solo una tercera parte utilizaban copias de seguridad para proteger su información. Las PYMES españolas consideran la ciberseguridad más como un gasto, que como una inversión.

Esto lleva a una falta de análisis adecuado de costos y beneficios, lo que, a su vez, incrementa la confianza de los ciberdelincuentes para perpetrar delitos. En este sentido, se cuestiona la efectividad de la certificación ISO/IEC 27001:2013 (Sistemas de Gestión), porque se basa en documentos, sin ofrecer una justificación adecuada para la aplicación de controles, ni un análisis de la situación real, además se señala que no proporciona un mecanismo eficaz para establecer una relación óptima entre el valor de los activos protegidos y los elementos de defensa implementados por las empresas (Peralta y Aguilar, 2021).

En Colombia, el sector empresarial se enfrenta a ataques cibernéticos debido a la falta de medidas de protección básicas en los equipos informáticos. La ausencia de antivirus y actualizaciones de los sistemas operativos deja a los equipos vulnerables, lo que puede resultar en el acceso no autorizado a los servidores contables de las empresas, esto permite a los atacantes obtener un control total sobre la información sensible de la empresa. En algunas PYMES se han registrado incidentes donde delincuentes cibernéticos han desarrollado programas maliciosos destinados a infiltrarse en las plataformas, con el propósito de sustraer contraseñas, números de cédula, información financiera, entre otros datos sensibles.

Se ha evidenciado que las aplicaciones y programas consumen una gran cantidad de recursos, lo que ocasiona lentitud en las computadoras, problemas de almacenamiento de bases de datos y carencia de mecanismos de protección para el acceso a la información alojada en los servidores (Muñoz et al., 2019). En el año 2022 fue el cuarto país más afectado por ciberataques en Latinoamérica, el pago promedio de rescate por la información fue de 2,04 millones de dólares (Molano, 2023).

Por su parte, Ecuador ha entrado en la vanguardia de sistematizarse y ofrecer a los ciudadanos tramites más ágiles a través de sitios web, esto ha permitido abrir la puerta a los ciberdelitos que son ejecutados por delincuentes y terroristas. En 2018, un ciberataque dirigido al sistema de la Agencia Nacional de Tránsito resultó en beneficio para 15,970 usuarios con licencias de conducir de diversos tipos. Se determinó que usuarios externos identificaron vulnerabilidades en el sistema informático, accedieron a él y perpetraron la acción ilícita, causando pérdidas superiores a un millón de dólares para el Estado.

En abril del 2019, Ecuador recibió más de 40 millones de ataques, la mayoría, a los portales web de entidades públicas, en algunas de ellas viéndose afectada la atención al público, debido a intermitencias, aún no se cuenta con estudios que revelen datos precisos sobre las afectaciones económicas, entre los casos más ocurridos de ciberataques está el hackeo de correos electrónicos, violación de intimidad, apropiación fraudulenta por medios electrónicos. Tras la salida de Julián Assange del consulado ecuatoriano en Londres, se desató una ola de ciberataques dirigidos a importantes entidades gubernamentales ecuatorianas, como la Cancillería, los Ministerios y la Presidencia de la República. Estos ataques, provenientes de diversos países como Gran Bretaña, Estados Unidos y Holanda, expusieron la falta de preparación del país para enfrentar tales amenazas cibernéticas. Aunque existe legislación en materia de ciberseguridad, la falta de coordinación entre las instituciones debilita la implementación efectiva de políticas de seguridad (Cedeño, 2022).

A pesar de la falta de una estrategia de seguridad cibernética a nivel nacional, el país ha logrado grandes avances en cuanto sus capacidades para enfrentar estas amenazas, en gran parte gracias al equipo de respuesta ante incidentes cibernéticos, EcuCERT (Agencia de Regulación y Control de las Telecomunicaciones). En el caso específico de las empresas pequeñas y medianas en la ciudad de Cuenca, el desafío de los ciberataques reside en comprender cómo proteger los datos y sistemas de información mediante la implementación de diversas técnicas de seguridad y el uso de tecnologías de ciberseguridad. Este problema es relevante para las empresas, ya que puede tener un impacto directo en su rentabilidad y sostenibilidad (Zuña Macancela et al., 2019).

En correspondencia con la información que antecede, el presente estudio responderá a la siguiente pregunta de investigación: ¿cuáles son las vulnerabilidades más críticas en los sistemas contables y cómo pueden abordarse para garantizar la ciberseguridad y la integridad de los datos financieros en las empresas PYMES de Cuenca?

En consecuencia, el objetivo del estudio consiste en evaluar las amenazas de ciberseguridad en los sistemas contables y desarrollar estrategias efectivas para proteger la integridad de los datos financieros en las empresas PYMES de Cuenca.

MÉTODO

Para llevar a cabo el estudio sobre las medidas de ciberseguridad aplicadas a los *software*s contables en las PYMES de Cuenca, se desarrolló un método de investigación descriptiva no experimental con una finalidad transversal que buscaba comprender y explicar las prácticas de ciberseguridad en el contexto específico de las PYMES en Cuenca.

La técnica principal utilizada fue la encuesta, con un instrumento específico diseñado en forma de cuestionario que constaba de 30 ítems relacionados con la ciberseguridad y la protección de datos financieros. Este cuestionario se desarrolló considerando las mejores

prácticas y estándares en el campo de la ciberseguridad y fue validado por expertos en el tema.

La unidad de análisis se constituyó por los contadores de las PYMES de Cuenca, ya que son los profesionales responsables de la gestión de la información financiera y, por lo tanto, tienen un papel decisivo en la implementación y mantenimiento de medidas de ciberseguridad.

Para la selección de la muestra, se utilizó un muestreo intencional, donde se identificaron y seleccionaron 42 contadores de PYMES de Cuenca que representaban una variedad de empresas en términos de tamaño, sector y experiencia, se empleó el software JASP para la tabulación y análisis de los datos lo cual permitió obtener la información precisa.

RESULTADOS

Tamaño de la empresa: la mayoría de los contadores encuestados trabajan en empresas pequeñas, con menos de 10 empleados, lo que representa el 52.38% de la muestra. Una proporción menor labora en empresas medianas, de 10 a 50 empleados, con un 30.95%, mientras que un 16.67% indicó trabajar en grandes corporaciones, con más de 50 empleados. Esta distribución refleja una preferencia por entornos laborales más pequeños y medianos, lo que puede impactar en sus responsabilidades y enfoques de trabajo.

Sistemas contables digitales: las empresas han utilizado sistemas contables digitales durante un período prolongado. El 40.48% los usa por más de 5 años, el 35.71% entre 1 y 5 años, y solo el 23.81% los ha adoptado en el último año. Esto sugiere una evolución continua en la gestión contable empresarial hacia lo digital, con una reciente desaceleración atribuible a la saturación del mercado o factores externos como la pandemia.

Tipos de sistemas, incidentes y amenazas: la preferencia de las empresas por sistemas contables locales, representando el 45.24%, se relaciona con una mayor

exposición a incidentes de ciberseguridad, ataques de *malware*, reportados por el 57.14% de estas empresas. Por otro lado, aquellas que optan por *software* híbrido o en la nube, representando el 35.71% y el 19.05%, enfrentan menos incidentes, aunque están expuestas a amenazas como *phishing* y ataques de denegación de servicio (DDoS), con un 21.43% sufriendo ataques de phishing y otro 21.43% siendo víctimas de ataques DDoS. Esto destaca la influencia reveladora de la elección del sistema contable en la vulnerabilidad de una empresa ante las amenazas cibernéticas.

Personal especializado y amenazas de ciberseguridad: los resultados de la encuesta muestran una disponibilidad de personal especializado en ciberseguridad y la percepción de las amenazas de ciberseguridad en las empresas. Por un lado, el 30.95% de las empresas cuentan con un equipo o personal especializado en ciberseguridad, lo que sugiere una respuesta proactiva a las amenazas cibernéticas. Por otro lado, el 69% de los encuestados considera que las amenazas de ciberseguridad representan un riesgo importante para su empresa, lo que indica una conciencia generalizada sobre la importancia de abordar este problema. Esto resalta la necesidad creciente de conciencia y preparación en ciberseguridad dentro de las empresas, y cómo la disponibilidad de personal especializado puede influir en la percepción y gestión de las amenazas cibernéticas.

Confidencialidad de los datos: existe un 50% de los encuestados que consideran que la confidencialidad es alta, mientras que un 40.50% adicional la clasifica como media. Estos datos reflejan el reconocimiento y valoración por parte de varias empresas PYMES sobre la importancia de mantener la confidencialidad de sus datos financieros en sus sistemas contables.

Medidas y protección de datos: los datos sobre medidas de seguridad y protección de datos muestran que el 47.62% de las empresas que utilizan antivirus y *firewall* están preocupadas por el robo de información financiera. Mientras tanto, el 33.33% de aquellas que realizan copias de seguridad regulares se preocupan por la pérdida de datos, al igual

que el 50% de las que implementan políticas de acceso y privilegios. Aunque las empresas están implementando medidas para proteger sus datos financieros, sus preocupaciones varían dependiendo de las medidas específicas que han adoptado (Figura 1).

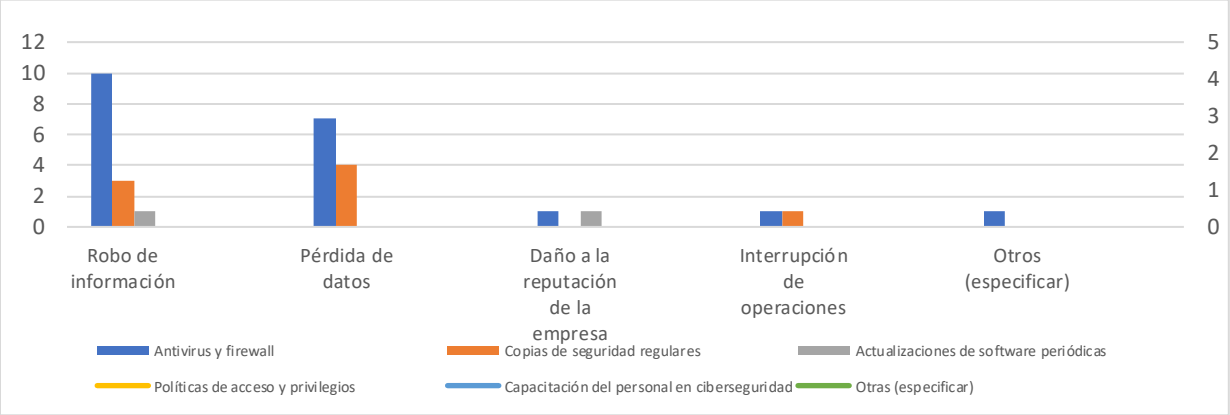

Figura 1. Medidas y protección de ciberseguridad en los sistemas contable.
Elaboración: Los autores.

Ciberseguridad de los proveedores: los resultados de la encuesta revelan que el 33.30% considera que los proveedores de servicios son muy seguros, mientras que el 38.10% los percibe como algo seguros. Sin embargo, un porcentaje considerable, el 14.30%, los califica como poco seguros. Además, otro 14.30% indica no saber o considerar que la pregunta no aplica para ellos. Esto sugiere una diversidad de percepciones sobre la seguridad de los proveedores de servicios en ciberseguridad.

Pruebas y auditorías de seguridad: las prácticas de seguridad, como las pruebas y auditorías, son cada vez más consideradas en las empresas. Mientras que un 23.80% indica llevar a cabo estas pruebas de forma regular, otro grupo relevante, el 26.20%, las realiza ocasionalmente. Además, un 35.70% señala que están considerando hacerlo, lo que propone una tendencia hacia la adopción de estas prácticas de seguridad en el futuro. Sin embargo, un 14.30% afirma no considerar necesario llevar a cabo estas

pruebas. Esto indica una creciente conciencia sobre la importancia de estas prácticas de seguridad.

Políticas y el factor humano: el resumen de los resultados indica que, el 42.90% de empresas implementa políticas sólidas de gestión de contraseñas, como contraseñas complejas y cambios regulares, el 14.30% un porcentaje notable no tiene políticas establecidas en este sentido. Además, el 69% considera que el factor humano, es decir, los empleados, representa un riesgo para la seguridad de la información, mientras que el 26.20% lo considera muy riesgoso. Es importante la concientización sobre la seguridad cibernética y la implementación de políticas adecuadas para mitigar los riesgos asociados con el factor humano.

Herramientas y detección: según los resultados de la encuesta, muestra que el 57.14% utiliza herramientas de monitoreo de red en sus sistemas contables como medida de seguridad. Además, el 9.52% porcentaje emplea herramientas de detección de intrusiones IDS/IPS y el 4.70% sistemas de análisis de comportamiento. Asimismo, se observa que el 9.52 utiliza herramientas de gestión de logs. Por último, un 19.05% de los encuestados indicó utilizar otras herramientas de monitoreo y detección de amenazas no especificadas en la encuesta. Los resultados reflejan una sólida atención a la seguridad en los sistemas contables, en el monitoreo de red y la detección proactiva de amenazas. Se respalda mediante una combinación de herramientas y enfoques para abordar varios aspectos de la seguridad cibernética.

Evaluación y presupuesto: la distribución del presupuesto para medidas de ciberseguridad en sistemas contables varía según la frecuencia de las evaluaciones de riesgos. Un 30.90% lleva a cabo estas evaluaciones trimestralmente, seguido por un 14.30% semestralmente y un 11.90% anualmente. Sin embargo, un considerable 42.90% no realiza evaluaciones periódicas en absoluto. Esta falta de evaluación regular podría estar relacionada con la reducción del presupuesto para ciberseguridad en sistemas contables durante el último año. Los datos muestran que el 66.70% asignó menos de

$1000, el 23.80% entre $1000 y $5000, y solo un pequeño porcentaje, el 7.10%, destinó más de $10000. Esto sugiere una desconexión entre la conciencia de los riesgos y la asignación de recursos para abordarlos, lo que podría dejar a las empresas más vulnerables a amenazas internas en sus sistemas contables (Figura 2).

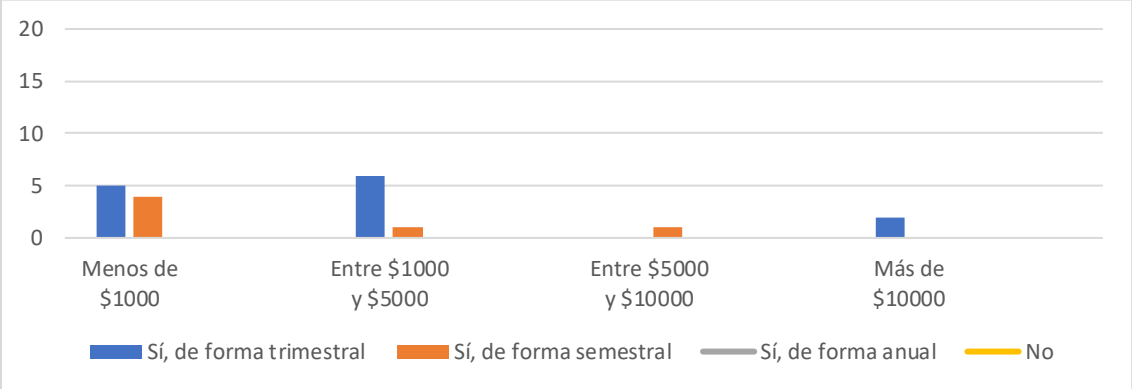

Figura 2. Presupuesto y evaluaciones en los sistemas contables.
Elaboración: Los autores.

Protocolos de seguridad: según los resultados de la encuesta, se observa que el protocolo HTTPS es el más utilizado, con un 35.71% de los encuestados que lo emplea. Le sigue el protocolo de VPN con un 21.43%. Además, que el 2.38% de encuestados utiliza el protocolo TLS 2.38%, mientras que la encriptación de extremo a extremo es utilizada por un 28.57% de los encuestados y el 11.90% de los encuestados mencionó utilizar otros protocolos no especificados en la encuesta. Estos resultados reflejan una preocupación por la seguridad en la comunicación web y la protección integral de los datos, así como una diversidad de enfoques adaptados a las necesidades individuales de cada organización

Copias de seguridad: los resultados de la encuesta muestran que el 35.71% de los encuestados realiza copias de seguridad diariamente, seguido por un 23.81% que lo hace semanalmente y un 26.19% mensualmente. Un 14.29% de los encuestados admitió no realizar copias de seguridad en absoluto. Estos resultados resaltan la importancia de

establecer prácticas regulares de copias de seguridad para proteger la información crítica de la organización.

Evaluación efectiva y estrategias implementadas: los resultados de la encuesta revelan una diferencia en la adopción de medidas para evaluar la efectividad de la ciberseguridad y estrategias implementadas. Mientras que el 38.09% utiliza pruebas de vulnerabilidad, un 35.71% no realiza evaluaciones de efectividad. En cuanto a las estrategias implementadas, el 42.86% opta por capacitaciones periódicas, seguido por un 33.33% que envía correos informativos. Las tácticas menos comunes como simulacros de phishing y carteles informativos son menos empleadas. Estos hallazgos subrayan la necesidad de una mayor atención a la evaluación de la efectividad de las medidas de ciberseguridad y la implementación de estrategias de concientización más variadas y efectivas.

Regulación y cumplimiento normativo: los resultados de la encuesta muestran que un 64.29% indicó que es muy importante, mientras que un 28.57% lo considero algo relevante, solo un pequeño porcentaje expresó que no lo consideraban tan relevante. Esto propone una clara conciencia y valoración de la importancia de cumplir con las regulaciones y normativas en materia de seguridad y protección de datos.

Acceso de los empleados: demuestran que el 45.24% tienen acceso parcial a los sistemas contables, según sus roles específicos dentro de la organización. Además, el 28.57%, indicó que el acceso está limitado solo a ciertas funciones, mientras que un 16.67% tienen acceso temporal para tareas específicas, solo un pequeño porcentaje de los encuestados reportó tener acceso total. Estos hallazgos sugieren una práctica común de restringir el acceso a los sistemas contables según las responsabilidades laborales, lo que contribuye a la seguridad y control de la información financiera dentro de la organización.

Experiencias previas de fuga: revelan que el 40.48% de los contadores encuestados han experimentado fugas de información en sus sistemas contables, mientras que el

59.52% restante no ha tenido tales experiencias. Estos resultados recalcan la realidad de que las fugas de información son un desafío frecuente enfrentado por un segmento de profesionales contables.

Fugas y medidas de protección: existe una clara preocupación por la seguridad de los datos financieros, como lo demuestran medidas como la encriptación de extremo a extremo, utilizada por el 30.95% de los encuestados, y el empleo de redes privadas virtuales, con un 28.57%. También se destaca la verificación de la autenticidad de los destinatarios, con un mismo porcentaje del 28.57%. Para detectar fugas, se emplean diversos enfoques, desde el monitoreo continuo de actividades sospechosas hasta la recepción de reportes de empleados o usuarios. Además, un notable 28.57% emplea métodos no especificados, lo que muestra la diversidad de estrategias adaptadas a las necesidades de cada organización. Estos resultados subrayan la importancia de medidas técnicas y procesos de detección proactivos para mitigar los riesgos asociados con amenazas a la seguridad de los datos financieros (Figura 3).

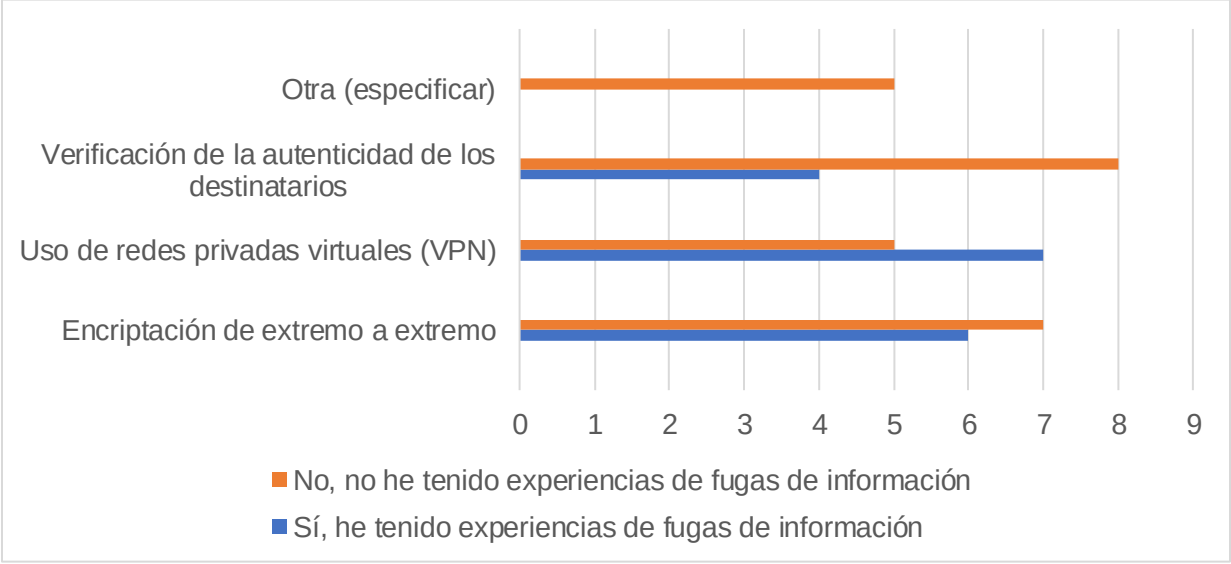

Figura 3. Fugas de información y medidas de seguridad.
Elaboración: Los autores.

Disponibilidad de los datos financieros: el 54.76% indicaron que realizan copias de seguridad en servidores externos, además el 26.19% mencionó tener planes de contingencia y recuperación ante desastres. Esto indica que hay una preocupación por garantizar la disponibilidad de los datos financieros mediante la implementación de medidas como copias de seguridad en servidores externos y planes de contingencia en caso de eventos adversos.

Vulnerabilidad y estrategias: los resultados señalan que los contadores están conscientes de las vulnerabilidades en sus sistemas contables, el 57.14% muestran su preocupación sobre el *software* utilizado, el 21.43% indica que se preocupan por acceso no autorizado por parte de empleados y el 19.05% por la falta de actualizaciones de seguridad. En respuesta, con el 38.09% la estrategia más mencionada para proteger la integridad de los datos financieros es aumentar la inversión en tecnologías de ciberseguridad. Se destaca la importancia de mejorar las políticas, los procedimientos de seguridad, la capacitación del personal, como enfoques complementarios. Esto acentúa la necesidad de una combinación de medidas para garantizar la seguridad de los datos financieros en las empresas PYMES.

Acciones para mitigar las amenazas internas: las medidas más comunes para mitigar amenazas internas en sistemas contables incluyen la restricción de acceso a información sensible, adoptada por el 38.09% de los encuestados. Además, el monitoreo de actividades de usuarios y la implementación de políticas de uso aceptable son prácticas empleadas por el 21.43% de los encuestados. Estos resultados muestran que las empresas están tomando medidas proactivas para proteger sus sistemas contables contra posibles amenazas internas. Estas acciones reflejan un esfuerzo integral por parte de las empresas para proteger sus sistemas contables contra posibles amenazas internas (Figura 4).

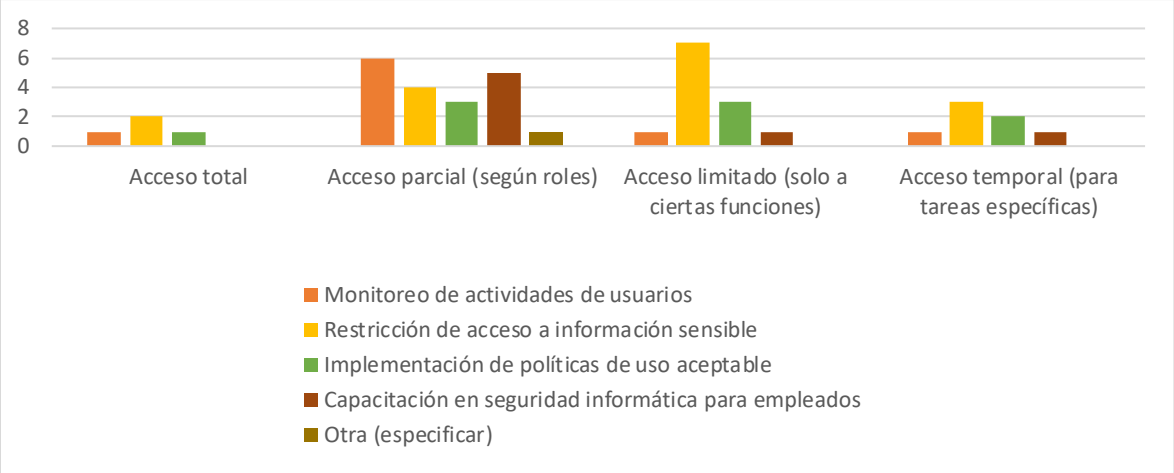

Figura 4. Acceso y mitigación de riesgo, manipulación de datos por los empleados.
Elaboración: Los autores.

DISCUSIÓN

El análisis comparativo entre los resultados del presente estudio y el llevado a cabo en Hermosillo, Sonora, México (Aguilar et al., 2017) revelan varias similitudes y diferencias. En primer lugar, en cuanto a la percepción sobre la calidad y funcionalidad de los sistemas contables, ambos estudios muestran que la mayoría de las empresas encuestadas consideran que cuentan con sistemas adecuados, la diferencia geográfica podría influir en las preferencias y características específicas de los sistemas contables utilizados, así como en las necesidades percibidas por los usuarios.

Una diferencia notable entre los estudios es la preferencia por sistemas sistematizados versus semi-sistematizados. Mientras que el estudio previo proporciona datos sobre esta distinción, el presente estudio no lo hace, lo que podría deberse a diferencias en la infraestructura tecnológica disponible o las prácticas contables comunes en cada región.

En cuanto al impacto de los sistemas de información contable en la toma de decisiones, ambos estudios coinciden en que la mayoría de las empresas perciben que sus sistemas proporcionan información relevante para esta actividad. Sin embargo, el estudio previo indica que el 100% de las empresas encuestadas consideran que su sistema contable

apoya la toma de decisiones, mientras que el presente estudio no ofrece datos específicos sobre esta métrica.

Otra diferencia entre los dos estudios es el nivel de adopción de innovaciones tecnológicas en los sistemas contables. El estudio previo muestra que un porcentaje de empresas utiliza innovaciones tecnológicas con regularidad, el presente estudio no proporciona datos detallados sobre este aspecto. Esta discrepancia podría reflejar diferencias en el nivel de desarrollo tecnológico de las regiones estudiadas o en las estrategias de implementación de tecnología por parte de las empresas encuestadas.

Los resultados del presente estudio, en comparación con el estudio de Zuña et al. (2019), revelan diferencias significativas, según el presente estudio las PYMES han implementado sistemas contables digitales durante un período prolongado, con una preferencia notable por los sistemas locales. Sin embargo, esta preferencia se asocia con una mayor exposición a incidentes de ciberseguridad, como ataques de *malware*. Por otro lado, las empresas que optan por sistemas en la nube enfrentan diferentes amenazas, como *phishing* y ataques *DDoS*. Esto resalta la influencia de la elección del sistema contable en la vulnerabilidad de una empresa ante las amenazas cibernéticas.

En contraste, el segundo estudio se enfoca en la percepción de la importancia de la ciberseguridad en las PYMES de la ciudad de Milagro, Ecuador, se destaca que muchas de estas empresas son vulnerables a los ciberataques debido a la falta de inversión en medidas de seguridad informática y la escasa capacitación del personal en ciberseguridad. Además, se enfatiza la necesidad de un enfoque integral que incluya la actualización de equipos informáticos, la implementación de políticas de seguridad adecuadas y la inversión en tecnologías de ciberseguridad.

Ambos estudios coinciden en la importancia de concientizar a las PYMES sobre los riesgos asociados con la falta de protección cibernética adecuada y la necesidad de invertir en medidas de seguridad. Esto sugiere que la ciberseguridad es un desafío

multidimensional que requiere enfoques variados y adaptados a las necesidades específicas de cada empresa.

Los resultados de esta investigación coinciden en algunos aspectos con los autores Peralta y Aguilar (2021) con respecto a la importancia de afrontar los desafíos de ciberseguridad en un entorno empresarial cada vez más digitalizado, difieren en sus enfoques y énfasis, lo que proporciona una visión más completa del panorama de la ciberseguridad. El presente estudio se centra en aspectos cuantitativos, como la distribución del tamaño de las empresas encuestadas y la adopción de sistemas contables digitales. Destaca la evolución hacia lo digital en la gestión contable empresarial y señala posibles factores que podrían influir en esta tendencia, como la saturación del mercado o la coyuntura económica, incluyendo la pandemia. Proporciona datos concretos sobre la asignación de presupuesto y la frecuencia de las evaluaciones de riesgo, lo que ofrece una perspectiva detallada de la situación actual de la ciberseguridad en las PYMES.

Por otro lado, el segundo estudio se enfoca en aspectos cualitativos, como la percepción de los gerentes sobre la ciberseguridad y la necesidad de cambios en la filosofía empresarial para priorizar la inversión en este ámbito. Destaca la falta de conciencia sobre la importancia de proteger los activos intangibles, como la información financiera, y resalta la necesidad de una mayor concienciación y sensibilización sobre los riesgos cibernéticos. Identifica barreras importantes, como la percepción errónea de la ciberseguridad como un gasto en lugar de una inversión, lo que sugiere la necesidad de una transformación cultural dentro de las organizaciones.

En conjunto, proporcionan un enfoque integral de la ciberseguridad, el primero ofrece una panorámica detallada de la situación actual, mientras que el segundo destaca la importancia de cambios en la mentalidad empresarial para abordar los desafíos de ciberseguridad. Integrar estas perspectivas podría ayudar a desarrollar estrategias más

efectivas para proteger los sistemas contables y los activos digitales de las pequeñas y medianas empresas de Cuenca.

La ciberseguridad en el contexto de las pequeñas y medianas empresas es abordada por diversos estudios. El presente estudio se enfoca en la ciudad de Cuenca, el segundo examina la situación de las PYMES en la ciudad de Guayaquil (Bueno y Haz, 2022). Ambos ofrecen una descripción detallada de los diversos aspectos de la seguridad informática en este ámbito, aunque presentan similitudes, como la alta conciencia sobre la importancia de la ciberseguridad y el interés en implementar medidas correspondientes, también revelan diferencias en la distribución demográfica y los desafíos específicos identificados en cada contexto. Los dos ofrecen información esencial sobre el estado actual de la ciberseguridad en las PYMES, resaltando la imperativa necesidad de reforzar las medidas de seguridad y elevar la conciencia sobre las ciberamenazas.

El primer estudio se centró en la ciudad de Cuenca y analizó la adopción y utilización de sistemas contables digitales en PYMES, así como las medidas de ciberseguridad implementadas. Se encontró que la mayoría de las empresas encuestadas han utilizado sistemas contables digitales durante un período prolongado, con una preferencia por los sistemas locales. Sin embargo, se observó que esta preferencia se asociaba con una mayor exposición a incidentes de ciberseguridad, mientras que las empresas que optaban por sistemas en la nube enfrentaban menos incidentes, pero estaban expuestas a diferentes amenazas como phishing y ataques DDoS (Ribagorda, 2018).

Se evidenció que una parte de las empresas carece de conocimientos básicos sobre ciberseguridad, lo que puede dejarlas vulnerables a posibles explotaciones de seguridad.

Al comparar ambos estudios, se puede destacar que resaltan la necesidad de promover la conciencia sobre la importancia de la ciberseguridad en las PYMES. Ambos estudios señalan que un porcentaje de las empresas carece de conocimientos básicos sobre

ciberseguridad, lo que resalta la importancia de la educación y la capacitación en este campo (Vanegas y Ávila, 2023).

CONCLUSIONES

Los datos indican una clara tendencia hacia la adopción de sistemas contables digitales, aunque con una reciente desaceleración. Esto podría atribuirse a la saturación del mercado o a factores externos como la pandemia. Esta transición también ha expuesto a las empresas a una mayor vulnerabilidad cibernética, en especial a aquellas que optan por sistemas locales en lugar de soluciones en la nube. La elección del sistema contable parece estar correlacionada con la exposición a diferentes tipos de amenazas cibernéticas, lo que destaca la importancia de evaluar las opciones disponibles.

La falta de evaluaciones regulares de riesgos y la asignación limitada de recursos para la ciberseguridad podrían dejar a estas empresas vulnerables a ataques internos y externos, la diversidad de percepciones sobre la seguridad de los proveedores de servicios en ciberseguridad sugiere la necesidad de una mayor transparencia y evaluación de los terceros con los que colaboran las empresas. Mientras que algunas organizaciones están tomando medidas proactivas para proteger sus datos financieros, todavía hay un camino por recorrer en términos de conciencia y preparación en ciberseguridad dentro del sector Pyme en Cuenca, Ecuador.

FINANCIAMIENTO

No monetario.

AGRADECIMIENTO

A la planta docente de la Maestría en Contabilidad y Auditoría de la Universidad Católica de Cuenca.

REFERENCIAS CONSULTADAS

Aguilar, P., Heredia, J., y Leyva, A. (2017). Innovación tecnológica en los sistemas contable de las PYMES [Technological innovation in SME accounting systems]. *Trascender, contabilidad y gestión* (5), 40-51. https://shre.ink/8qgU

Bueno, G., y Haz, L. (2022). Ciberseguridad post covid-19 y su impacto en las PYMES del Ecuador [Post-covid-19 cybersecurity and its impact on Ecuadorian SMEs]. *Pro Sciences: Revista De Producción, Ciencias e Investigación, 6*(46), 103-120. https://doi.org/10.29018/issn.2588-1000vol6iss46

Cedeño, R. (2022). Ciberseguridad y Ciberdefensa: Perspectiva de la situación actual en el Ecuador [Cybersecurity and Cyber Defence: An overview of the current situation in Ecuador]. *Revista Tecnología, Ciencia y Educación Edwards Deming, 6*(1), 50260. https://doi.org/10.37957/rfd.v6i1.88

Molano, D. (2023). Ciberseguridad: Empresas Bajo Ataque [Cybersecurity: Companies Under Attack]. La Republica. https://shre.ink/8Ckg

Muñoz, H., Zapata Cantero, L. G., Requena Vidal, D. M., y Ricardo Villadiego, L. (2019). Riesgos informáticos y alternativas para la seguridad informática en sistemas contables en Colombia [IT risks and alternatives for IT security in Colombian accounting systems]. *Revista Venezolana de Gerencia, 2,*528-541.

Peralta, M., y Aguilar, D. (2021). La Ciberseguridad y su concepción en las PYMES de Cuenca, Ecuador [Cybersecurity and its conception in SMEs in Cuenca, Ecuador]. *Contabilidad y Auditoría, 53*(27), 99-126. https://doi.org/10.56503/Contabilidad_y_Auditoria/Nro.53(27)/2061

Ribagorda, A. (2018). Panorama Actual de la Ciberseguridad [Current Cybersecurity Overview]. *Visión Global*(410), 13-26. https://doi.org/https://shre.ink/8Ckv

Vanegas, M., y Ávila, A. (2023). Análisis de herramientas de ciberseguridad de código abierto para la prevención de ciberataques a pequeñas y medianas empresas de Colombia [Analysis of open source cybersecurity tools for the prevention of cyber-attacks on small and medium-sized enterprises in Colombia]. *Revista CIES, 14*(2), 221-241. https://doi.org/https://shre.ink/8eFc

Zuña, E., Arce, A., Romero, W., y Soledispa, C. (2019). Análisis de la seguridad de la información en las PYMES de la ciudad de Milagro [Analysis of information security in SMEs in the city of Milagro]. *Universidad y Sociedad, 11*(4), 487-492.

Año X. Vol. X. N°2. Edición Especial II. 2024
Hecho el depósito de ley: pp201602FA4721
ISSN-L: 2542-3029; ISSN: 2610-802X
Instituto de Investigación y Estudios Avanzados Koinonía. (IIEAK). Santa Ana de Coro. Venezuela

Zuña-Macancela, E. R., Arce-Ramírez, Á. A., Romero-Berrones, W. J., y Soledispa-Baque, C. J. (2019). Análisis de la seguridad de la información en las PYMES de la ciudad de Milagro [Analysis of the security of the information in the SMES of the city of MILAGRO]. *Revista Universidad y Sociedad*, *11*(4), 487-492.