Revista Multidisciplinaria Perspectivas Investigativas
Multidisciplinary Journal Investigative Perspectives
Vol. 4(Contabilidad y Auditoría), 14-27, 2024
https://doi.org/10.62574/rmpi.v4iContabilidad y Auditoría.154

Auditoría y ciberseguridad en el sector comercial: evaluación de resiliencia ante amenazas digitales

Audit and cyber security in the commercial sector: assessing resilience to digital threats

Karina Alejandra López-Anchala
karina.lopez.83@est.ucacue.edu.ec
Universidad Católica de Cuenca, Cuenca, Azuay, Ecuador
https://orcid.org/0009-0002-3243-0366

Yanice Licenia Ordóñez-Parra
jordonezp@ucacue.edu.ec
Universidad Católica de Cuenca, Cuenca, Azuay, Ecuador
https://orcid.org/0000-0002-5002-2203

RESUMEN

El estudio sobre auditoría y ciberseguridad en empresas comerciales ecuatorianas aborda la creciente importancia de proteger los activos digitales ante amenazas cibernéticas en constante evolución. El objetivo consiste en analizar estrategias para la evaluación y mejora de la resiliencia empresarial en el sector comercial frente a amenazas cibernéticas mediante la Auditoría, identificando las mejores prácticas para su integración efectiva en las estrategias de ciberseguridad. La metodología es descriptiva. Los resultados destacan la importancia del conocimiento técnico del personal en ciberseguridad y el interés en implementar mecanismos de seguridad informática. Sin embargo, se observa una falta de auditorías de seguridad cibernética de manera regular, lo que acentúa la necesidad de una mayor conciencia y acción preventiva en este ámbito. Se resalta la importancia de una colaboración efectiva entre la auditoría interna y la ciberseguridad para fortalecer la postura de seguridad de las empresas.

Descriptores: tecnología adecuada; protección de datos; derecho a la privacidad. (Fuente: Tesauro UNESCO).

ABSTRACT

The study on auditing and cyber security in Ecuadorian commercial enterprises addresses the growing importance of protecting digital assets from evolving cyber threats. The objective is to analyse strategies for assessing and improving business resilience in the commercial sector against cyber threats through auditing, identifying best practices for effective integration into cybersecurity strategies. The methodology is descriptive. The results highlight the importance of staff's technical knowledge of cyber security and interest in implementing cyber security mechanisms. However, there is a lack of regular cyber security audits, which emphasises the need for greater awareness and preventive action in this area. The importance of effective collaboration between internal audit and cyber security to strengthen the security posture of companies is highlighted.

Descriptors: appropriate technology; data protection; right to privacy. (Source: UNESCO Thesaurus).

Recibido: 03/06/2024. Revisado: 08/06/2024. Aprobado: 15/01/2024. Publicado: 17/06/2024.
Sección artículos de investigación

INTRODUCCIÓN

Las empresas, aparte de su tamaño o sector, se ven inmersas en un escenario donde los activos digitales se vuelven cada vez más decisivos y, al mismo tiempo, más vulnerables ante una cantidad de amenazas cibernéticas en constante evolución. El desafío al que se enfrentan las empresas en este panorama es doble: por un lado, la rápida evolución de las tecnologías y las amenazas cibernéticas plantea desafíos para mantenerse al día con las últimas tendencias y vulnerabilidades. Por otro lado, la globalización de los mercados y la interconexión digital implican que las empresas deben considerar las amenazas locales, así como aquellas de alcance internacional que podrían afectar su operatividad (Vega, 2019).

En el ámbito internacional, la creciente interconexión digital entre países y organizaciones resalta la urgencia de abordar las amenazas cibernéticas de manera conjunta y colaborativa. Esta realidad exige adoptar enfoques integrados que promuevan la cooperación entre gobiernos, empresas y entidades internacionales. La colaboración facilita el intercambio de información sobre amenazas emergentes, e impulsa el desarrollo de mejores prácticas y estándares de seguridad cibernética. Además, en un panorama donde los ataques cibernéticos pueden tener repercusiones transnacionales, una respuesta efectiva requiere la coordinación y acción conjunta entre distintos actores para mitigar los impactos y fortalecer la resiliencia frente a estos desafíos digitales (Vega, 2019).

En Ecuador, las empresas enfrentan desafíos de ciberseguridad, desde la escasez de recursos y capacidades técnicas hasta la necesidad de adaptarse a un marco regulatorio en evolución. No obstante, existen oportunidades para fortalecer la resiliencia cibernética mediante la colaboración entre el sector público y privado, el fomento de la investigación y la innovación en seguridad digital, y la promoción de una cultura de ciberseguridad desde los más altos niveles de la organización (Zuñiga-Paredes et al. 2021; Sancho-Hirare, 2017).

En este contexto, la intersección entre la auditoría y la ciberseguridad en el ámbito empresarial para las empresas comerciales representa un campo fértil para la exploración y el desarrollo de estrategias que permitan evaluar y mejorar la resiliencia ante amenazas digitales a nivel internacional, nacional y local. En un mundo donde la seguridad digital se ha convertido en un imperativo estratégico, las empresas que logren adaptarse y fortalecer su postura de ciberseguridad estarán mejor posicionadas para enfrentar los desafíos del futuro digital (Gomero-Cuadra & Sánchez-Calle, 2024).

La auditoría informática se enfoca en la revisión de los controles internos relacionados con el procesamiento electrónico de datos, así como en la verificación de la precisión y validez de la información financiera generada por sistemas informáticos. La implementación de auditorías de manera periódica permite la detección temprana y la subsiguiente corrección de brechas de seguridad, preservando la integridad y confidencialidad de la información. Este enfoque proactivo hacia la gestión de riesgos informáticos contribuye a la fortificación de la postura de seguridad de la organización frente a amenazas emergentes. El uso de herramientas de auditoría asistida por computadora (CAATs) y técnicas de análisis de datos como el análisis de tendencias, el análisis de varianza y el análisis de redes puede mejorar la capacidad de los auditores para detectar fraudes y errores en los sistemas contables (Rodríguez-Labrada et al. 2019).

Es así como la mejora continua en la auditoría informática requiere una combinación equilibrada de tecnología avanzada y profesionales expertos. Los auditores deben aprovechar las herramientas tecnológicas para automatizar tareas rutinarias y centrarse en actividades de mayor valor agregado, como el análisis de riesgos y la interpretación de resultados (Cervera & Goussens, 2024). Dicho proceso conlleva un análisis detallado de la confirmación de múltiples elementos esenciales, vinculados con la tecnología de información (Zeadally et al. 2016). Esto abarca la infraestructura tanto de hardware como de software, la protección de datos junto con su seguridad, los procedimientos para el respaldo, la recuperación de la información.

Los auditores informáticos deben poseer un conocimiento profundo de los sistemas contables, las normativas contables (como GAAP o IFRS) y las regulaciones relacionadas con la privacidad y la protección de datos (como GDPR o HIPAA), además de habilidades técnicas en seguridad informática y análisis de datos (Jeimy & Cano, 2023). Cabe señalar que, la auditoría informática enfrenta desafíos complejos del sector comercial mediante una combinación de estrategias y prácticas enfocadas en la detección, prevención y mitigación de riesgos relacionados con el *phishing*, el *ransomware* y el *malware* (García-Córdoba & Herrero-Pérez, 2020):

Evaluación de la seguridad de la red y sistemas: los auditores informáticos realizan evaluaciones exhaustivas de la infraestructura de TI y los sistemas para identificar vulnerabilidades que podrían ser explotadas por ataques de *phishing, ransomware* o *malware*. Esto implica pruebas de penetración, análisis de vulnerabilidades y evaluaciones de configuración de seguridad.

Concienciación y capacitación del personal: una parte importante de la estrategia de auditoría informática es la educación continua del personal sobre las amenazas de seguridad informática, incluidos el *phishing* y el *ransomware*. Esto implica la realización de programas de concienciación en seguridad, simulacros de phishing y sesiones de capacitación para ayudar a los empleados a reconocer y evitar ataques.

Implementación de controles de seguridad: los auditores trabajan con los equipos de TI para implementar controles de seguridad efectivos, como *firewalls*, sistemas de detección de intrusiones, filtros de correo electrónico y *software* antivirus/*antimalware* actualizado. Estos controles ayudan a prevenir la infiltración de malware y a detectar actividades maliciosas en la red.

Monitorización y detección temprana: se establecen sistemas de monitorización continua para detectar actividades sospechosas, como intentos de phishing, descargas de ransomware o comportamiento anómalo del sistema. Esto permite una respuesta rápida ante posibles incidentes de seguridad y la minimización del impacto.

Respuesta y recuperación ante incidentes: se desarrollan y ponen a prueba planes de respuesta ante incidentes para garantizar una respuesta efectiva en caso de ataques de phishing, ransomware u otras formas de malware. Esto incluye procedimientos para contener la propagación del malware, restaurar sistemas desde copias de seguridad y comunicarse con las partes interesadas de manera oportuna.

Actualización y parcheo de sistemas: se implementa un proceso riguroso para mantener actualizados los sistemas y aplicaciones, así como para aplicar parches de seguridad de manera regular. Esto ayuda a cerrar las brechas de seguridad conocidas y a reducir la superficie de ataque para los actores maliciosos.

En este contexto, la auditoría informática aborda los desafíos del *phishing*, el *ransomware* y el *malware* mediante una combinación de evaluación de riesgos, concienciación del personal, implementación de controles de seguridad, monitorización continua, respuesta a incidentes y mantenimiento de sistemas actualizados. Esto ayuda a las organizaciones a proteger sus activos digitales y a mantener la integridad, confidencialidad y disponibilidad de la información.

Incorporación de la ciberseguridad en los procesos de auditoría: hacia una práctica más resiliente y efectiva

La ciberseguridad se ha convertido en un tema esencial en el ámbito empresarial, en lo que respecta a los procesos de auditoría. Las amenazas cibernéticas representan un problema cada vez más grave y complejo que impacta de forma directa en la efectividad de las prácticas de auditoría. La creciente sofisticación de estas amenazas plantea desafíos para las organizaciones y sus procesos de auditoría, lo que requiere una atención urgente para mejorar la resiliencia y la efectividad de estas prácticas.

Las amenazas cibernéticas abarcan una amplia gama de riesgos, incluyendo *malware, ransomware, phishing*, ataques de denegación de servicio (DDoS) y muchos más. Estas amenazas están en constante evolución, adaptándose a las nuevas tecnologías y tácticas de defensa (Vega, 2019). Además, representan un riesgo característico para la integridad de los datos financieros y operativos de una organización. La infiltración de *malware,* ataques de *ransomware* o *phishing* pueden comprometer la precisión y validez de la información auditada. Estas vulnerabilidades amenazan con socavar la confianza en los datos utilizados en los procesos de auditoría, lo que puede conducir a decisiones erróneas y pérdidas financieras para la empresa.

La detección temprana y la mitigación efectiva de las amenazas cibernéticas son fundamentales para proteger los activos digitales de una organización. Sin embargo, estas tareas pueden resultar difíciles debido a la complejidad y la velocidad con la que evolucionan las amenazas. La rápida evolución de las amenazas cibernéticas requiere que las organizaciones y los auditores mantengan una vigilancia constante y actualicen sus estrategias de ciberseguridad. Esto implica inversiones en capacitación, tecnología y recursos humanos especializados (Vega, 2019).

Por lo mencionado, las amenazas cibernéticas representan un desafío cada vez mayor en la incorporación de la ciberseguridad en los procesos de auditoría. La diversidad y evolución de estas amenazas, su impacto en la integridad de los datos, los desafíos en la detección y mitigación, y la necesidad de actualización constante son aspectos que deben abordarse de manera urgente para mejorar la resiliencia y efectividad de las prácticas de auditoría en un entorno complejo.

En consecuencia, este estudio responde a la siguiente pregunta: ¿cómo puede la Auditoría contribuir a evaluar y mejorar la resiliencia de las empresas comerciales de Quito ante amenazas cibernéticas, y cuáles son las mejores prácticas para la integración efectiva de la Auditoría en estrategias de ciberseguridad?

En consideración el objetivo consiste en analizar estrategias para la evaluación y mejora de la resiliencia empresarial en el sector comercial frente a amenazas cibernéticas mediante la Auditoría, identificando las mejores prácticas para su integración efectiva en las estrategias de ciberseguridad.

MÉTODO

Esta investigación se fundamentó en una metodología descriptiva, lo cual facilitó la captura tanto de la diversidad de opiniones y experiencias de los encuestados como de las tendencias cuantificables y medibles en los datos. Esta aproximación metodológica no solo promovió una comprensión exhaustiva de las actitudes y percepciones asociadas con la implementación en empresas en un momento específico, sino que también permitió explorar integralmente dichos aspectos.

El estudio se centró en empresas comerciales ubicadas en la ciudad de Quito, Ecuador, utilizando un muestreo por conveniencia para seleccionar a 30 contadores públicos autorizados que cumplían con los criterios establecidos. Estos profesionales fueron escogidos para participar en el estudio debido a su experiencia relevante en el ámbito empresarial.

Se empleó como técnica principal una encuesta basada en un cuestionario estructurado compuesto por 25 ítems diseñados para abordar diversas facetas de la auditoría y la ciberseguridad. Esta metodología posibilitó una recolección de datos sistemática y estandarizada.

Posteriormente, los datos recopilados fueron analizados utilizando el software JASP (Just Another Statistics Program), lo que permitió realizar un análisis exhaustivo de los datos y generar conclusiones fundamentadas en evidencia sólida.

RESULTADOS

Se describen los resultados obtenidos de la aplicación del cuestionario:

Frecuencias de auditorías: el análisis de la frecuencia de realización de auditorías de seguridad cibernética en el sector comercial revela una distribución en los hábitos de las empresas. La mayoría (80%) de las empresas encuestadas no llevan a cabo auditorías de seguridad cibernética, lo que sugiere una posible falta de atención o inversión en ciberseguridad. Solo un pequeño porcentaje realiza auditorías anuales (16.67%), mensuales (26.67%), semestrales (13.33%), y trimestrales (6.67%) (ver figura 1). Estos resultados recalcan la necesidad de una mayor conciencia sobre la importancia de la seguridad cibernética y la implementación de medidas preventivas para mitigar los riesgos asociados a los ataques cibernéticos en el entorno empresarial.

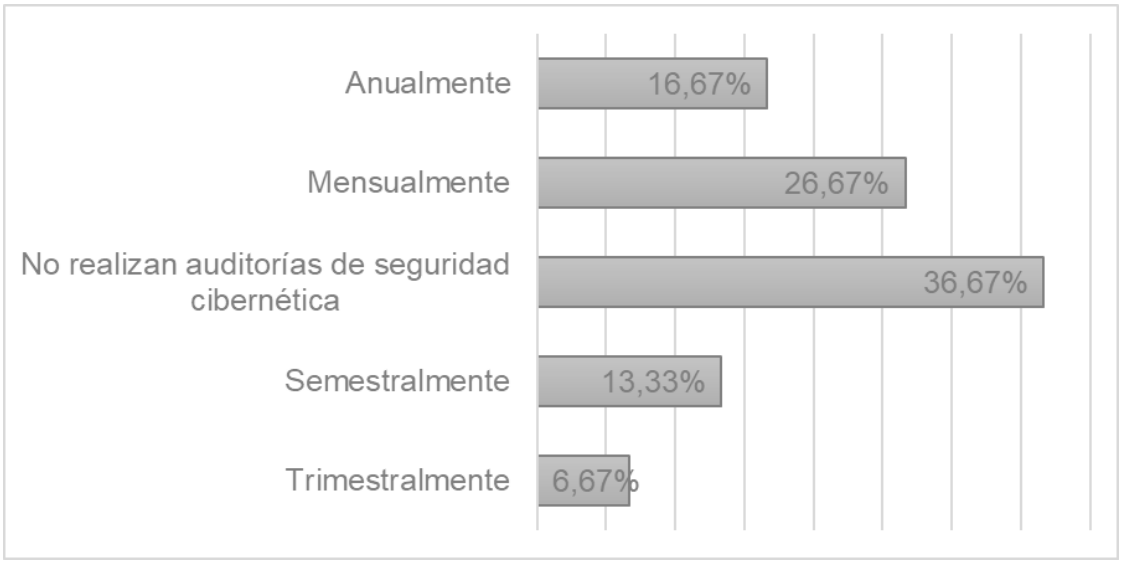

Figura 1
Frecuencias de auditorías
***Nota*.** Los datos fueron tomados de la encuesta aplicada en la provincia de Pichincha, ciudad de Quito, empresas del sector comercial.

Aspectos clave de resiliencia: el análisis de los aspectos considerados más importantes al evaluar la resiliencia de las empresas frente a amenazas cibernéticas en el sector comercial muestra una distribución reveladora en las respuestas. La implementación de medidas de seguridad informática es percibida como el aspecto más relevante por el 36.67% de las empresas encuestadas, seguida de la capacitación del personal en seguridad cibernética (20.00%) y el seguimiento continuo de riesgos y vulnerabilidades (6.67%). Solo un pequeño porcentaje menciona la respuesta rápida y efectiva ante incidentes de seguridad (3.33%) como un aspecto primordial. De acuerdo con los resultados, se requiere un enfoque integral que aborde múltiples aspectos de la ciberseguridad para fortalecer la resiliencia empresarial ante las amenazas cibernéticas.

Áreas críticas de seguridad: el análisis de las áreas consideradas más críticas en términos de seguridad cibernética en el sector comercial revela una clara percepción por parte de las empresas encuestadas. El departamento financiero es identificado como el área más crítica por un amplio porcentaje del 46.67%, seguido por el departamento de Tecnología de la Información (TI) con un 13.33% (ver figura 2). Un menor porcentaje menciona a Recursos Humanos como crítico (10.00%). Sin embargo, un 30.00% considera que todas las áreas son críticas. Estos resultados enfatizan la importancia de una protección robusta en el sector financiero y la necesidad de un enfoque holístico que aborde la seguridad cibernética en todas las áreas de la empresa para garantizar una protección efectiva contra amenazas digitales.

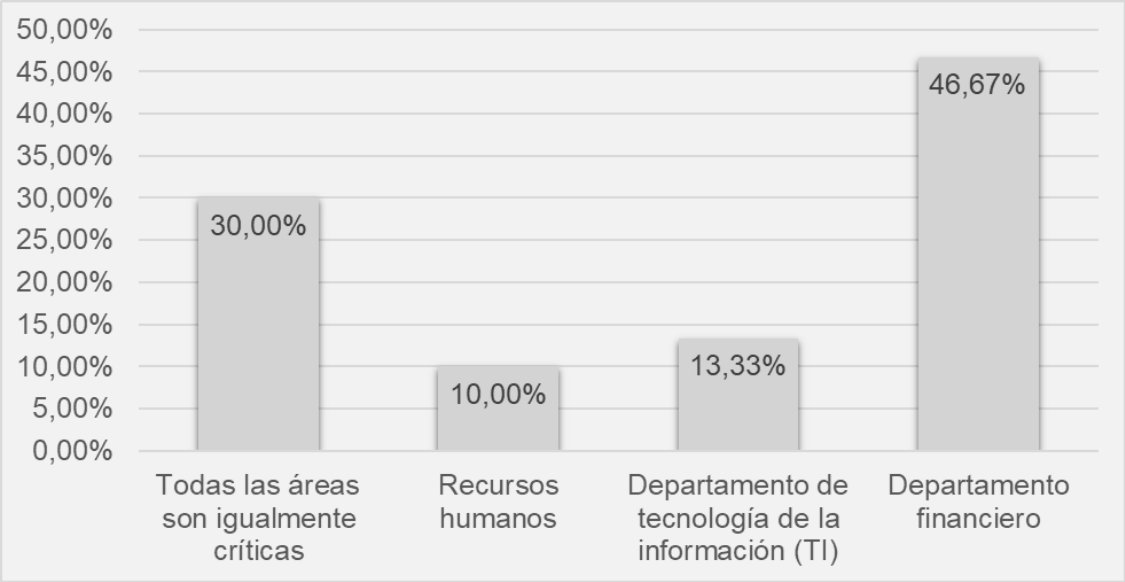

Figura 2
Áreas críticas de seguridad
***Nota*.** Los datos fueron tomados de la encuesta aplicada en la provincia de Pichincha, ciudad de Quito, empresas del sector comercial.

Auditoría y ciberseguridad: un 30.00% de las empresas encuestadas indican que la auditoría está integrada en sus estrategias de ciberseguridad, lo que sugiere un enfoque integral y proactivo hacia la gestión de riesgos digitales. Sin embargo, un 26.67% menciona que la auditoría no está integrada en absoluto, mientras que un 23.33% la considera integrada. Esto indica una brecha en la coordinación entre la auditoría y las estrategias de seguridad cibernética en una parte de las empresas encuestadas. Además, un 10.00% está en proceso de integración, y otro 10.00% no está seguro de su nivel de integración, lo que destaca la necesidad de una mayor claridad y acción en este aspecto para fortalecer la postura de ciberseguridad de las empresas.

Herramientas de auditoría: la opción más común es el uso de auditorías de cumplimiento normativo, seleccionada por el 33.33% de las empresas encuestadas, lo que refleja una atención a los estándares y regulaciones de seguridad. Le sigue el análisis de vulnerabilidades, elegido por el 26.67% de las empresas, lo que indica un enfoque en la identificación de debilidades en los sistemas. Sin embargo, un 16.67% de las empresas indican que no utilizan ninguna herramienta o metodología para las auditorías de seguridad cibernética. Además, un pequeño porcentaje utiliza pruebas de penetración (6.67%), mientras que otro 16.67% utiliza todas las opciones anteriores, lo que indica una estrategia integral de auditoría.

Participación directiva en ciberseguridad: un 30.00% de las empresas indican que la participación del equipo directivo es muy alta, lo que establece un fuerte liderazgo y atención a la ciberseguridad a nivel ejecutivo. Además, otro 30.00% reporta un nivel de participación moderado, lo que indica un interés menos involucramiento directo en comparación con el grupo anterior. Un 20.00% indica un nivel alto de participación, mientras que un 10.00% reporta niveles bajos o muy bajos de participación. Estos resultados resaltan la importancia de la implicación activa del liderazgo en las estrategias de ciberseguridad para promover una cultura de seguridad sólida en toda la organización.

Efectividad de las medidas: el análisis de la efectividad de las medidas de seguridad cibernética en empresas del sector comercial muestra una evaluación diversa. Un 36.67% las considera efectivas, mientras que un 20.00% las califica como muy efectivas. Sin embargo, un 13.33% las ve como poco efectivas, y un 23.33% las percibe como moderada efectiva. Un pequeño porcentaje (6.67%) no está seguro de su eficacia. Estos hallazgos subrayan la

necesidad de una evaluación continua y la implementación de medidas adecuadas para fortalecer la seguridad cibernética empresarial.

Tipos de datos: el análisis de los datos manejados por las empresas comerciales muestra una diversidad de información sensible gestionada. La información financiera y contable es la más común, manejada por el 40.00% de las empresas, destacando la importancia de su protección. Además, un 36.67% maneja todos los tipos de datos mencionados, evidenciando una amplia gama de información sensible. Un 20.00% maneja datos personales de clientes, resaltando la necesidad de proteger la privacidad. Solo un 3.33% maneja secretos comerciales y propiedad intelectual, sugiriendo una menor presencia de datos confidenciales. Estos resultados enfatizan la necesidad de implementar sólidas medidas de seguridad cibernética para proteger la diversidad de datos manejados y garantizar su confidencialidad, integridad y disponibilidad.

Importancia de la formación en ciberseguridad: el análisis de la importancia de la formación en seguridad cibernética en empresas comerciales muestra diversas percepciones. Un 30.00% la considera muy importante, reflejando un fuerte compromiso con la preparación del personal ante las amenazas digitales. Otro 30.00% la califica como fundamental, resaltando su relevancia generalizada en la seguridad empresarial. Sin embargo, un 23.33% la ve como moderada y relevante, sugiriendo la necesidad de más énfasis en este ámbito. Un menor porcentaje (6.67%) la considera poco importante y un 10.00% indica que no se le otorga importancia. Estos resultados subrayan la necesidad de fomentar una cultura de conciencia y capacitación en seguridad cibernética para fortalecer la seguridad digital de las empresas.

Desafíos en resiliencia cibernética: los resultados revelan diversas preocupaciones en el sector comercial. Un 36.67% señala la falta de personal capacitado en seguridad cibernética como el principal desafío, resaltando la necesidad de profesionales cualificados para abordar las complejidades de las amenazas digitales. Además, un 23.33% destaca la falta de apoyo de la alta dirección, determinando la importancia de un liderazgo. Otro 20.00% menciona la complejidad de las amenazas y la escasez de recursos financieros como barreras adicionales para fortalecer la resiliencia cibernética (ver figura 3). Estos hallazgos subrayan la importancia de abordar múltiples aspectos, desde la capacitación del personal hasta el compromiso directivo.

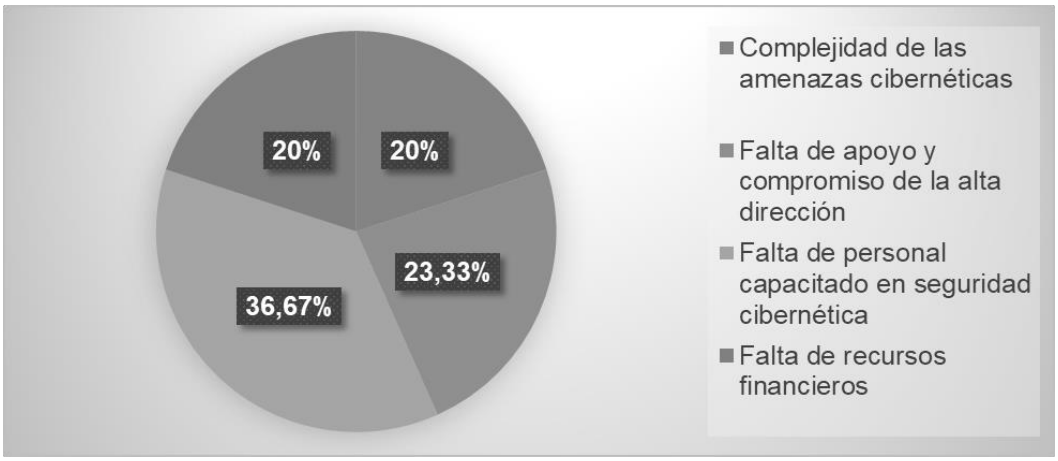

Figura 3
Desafíos en resiliencia cibernética
***Nota*.** Los datos fueron tomados de la encuesta aplicada en la provincia de Pichincha, ciudad de Quito, empresas del sector comercial.

Plan de respuesta a incidentes: el análisis revela una variedad en la disponibilidad y mantenimiento de planes de respuesta a incidentes de seguridad cibernética en empresas del sector comercial. Un 46.67% cuenta con un plan actualizado, indicando una preparación sólida. Sin embargo, un 23.33% tiene un plan desactualizado, sugiriendo la necesidad de mejoras.

Además, un 10.00% está en proceso de implementación, mientras que otro 23.33% aún no tiene planes, señalando oportunidades para fortalecer la preparación ante incidentes cibernéticos. En consecuencia, es necesario tener planes de respuesta actualizados para mitigar posibles impactos en las operaciones empresariales.

Medidas de seguridad efectivas: los datos revelan que las empresas del sector comercial consideran diversas medidas de seguridad cibernética efectivas. Destacan las actualizaciones regulares de software y parches de seguridad, junto con la implementación de autenticación de múltiples factores (MFA), valoradas por el 26.67% y 23.33% respectivas. Además, el uso de firewall y sistemas de detección de intrusiones (IDS) es mencionado por el 16.67% como clave. Aunque la encriptación de datos es menos citada (6.67%), el 26.67% reconoce la efectividad de todas las medidas mencionadas. Estos hallazgos subrayan la importancia de adoptar un enfoque holístico y actualizado en la protección de la infraestructura tecnológica empresarial.

Colaboración interinstitucional: la colaboración entre empresas del sector comercial y otras entidades en temas de ciberseguridad revela una distribución variada. Un 33.33% reporta una colaboración moderada, mientras que un 23.33% indica una alta colaboración y otro 23.33% menciona una baja colaboración. Sin embargo, un 13.33% no está seguro del nivel de colaboración, y un 6.67% declara que no hay colaboración. Estos resultados evidencian que si bien existe cierto grado de cooperación en temas de ciberseguridad, aún hay espacio para mejorar la colaboración interinstitucional, para abordar desafíos y amenazas cibernéticas de manera más efectiva mediante la colaboración entre entidades del sector comercial y otros actores relevantes.

Evaluaciones de riesgos cibernéticos: la realización de evaluaciones periódicas de riesgos cibernéticos y ajustes estratégicos muestra una diversidad de enfoques entre las empresas del sector comercial. Un 26.67% realiza estas evaluaciones, lo que determina un compromiso sólido con la gestión proactiva de riesgos. Además, otro 26.67% lo hace de forma ocasional, mientras que un 20.00% está considerando implementarlo, lo que indica una conciencia creciente sobre la importancia de esta práctica. Sin embargo, un 20.00% no está seguro de si se realizan estas evaluaciones, y un pequeño porcentaje (6.67%) no las considera necesarias. Estos resultados resaltan la necesidad de una evaluación continua de los riesgos cibernéticos y la adopción de estrategias adecuadas para proteger los activos digitales.

Preparación ante ataques avanzados: el 26.67% de las empresas se siente muy preparada para enfrentar los ataques avanzados, mientras que un 23.33% se considera moderadamente preparado. Otro 23.33% se identifica como preparado, un 13.33% se siente poco preparado. Un 13.33% no está seguro de su nivel de preparación. Estos resultados resaltan la necesidad de mejorar las medidas de seguridad para abordar amenazas avanzadas.

Políticas de seguridad cibernética: el 26.67% de las empresas tiene implementadas varias políticas de seguridad cibernética, lo que indica una cobertura integral en aspectos clave de seguridad. Además, el 23.33% cuenta con políticas de gestión de contraseñas y uso aceptable de recursos informáticos. Un 16.67% tiene políticas de acceso remoto, mientras que un 10.00% tiene políticas de gestión de dispositivos móviles. Estos resultados resaltan la importancia de contar con políticas de seguridad cibernética bien definidas para proteger los activos y mitigar los riesgos asociados a las amenazas digitales.

Rol de auditoría interna: el personal de auditoría desempeña diversos roles en la evaluación de la resiliencia empresarial ante amenazas cibernéticas: un 43.33% colabora en esta evaluación y un 23.33% la lidera y mejora. Sin embargo, un 13.33% no está seguro de su rol, mientras que un 6.67% actúa como observador pasivo. Un 13.33% no participa en la evaluación, lo que indica una variedad de niveles de involucramiento del personal de auditoría interna. Es fundamental la colaboración activa de este personal en la evaluación y mejora continua de la resiliencia empresarial frente a amenazas cibernéticas.

Importancia de la documentación de incidentes: la documentación de incidentes de seguridad cibernética y lecciones aprendidas es considerada muy importante por el 33.33% de las empresas encuestadas, lo que resalta el valor que se le atribuye a aprender de los eventos

pasados para mejorar la postura de seguridad. Además, un 23.33% la califica como importante, mientras que un 20.00% la considera moderada e importante. Sin embargo, un 10.00% no le otorga importancia y un 13.33% la percibe como poco importante. Estos resultados indican una variedad de perspectivas respecto a la importancia de documentar incidentes, y acentúan la relevancia de aprender de las experiencias pasadas para fortalecer la seguridad cibernética de la empresa.

Efectividad de la capacitación en ciberseguridad: la evaluación de la efectividad de las actividades de concientización y capacitación en seguridad cibernética muestra una variedad de percepciones entre las empresas encuestadas. Un 33.33% las califica como efectivas, mientras que otro 33.33% las considera muy efectivas, lo que indica un grado de satisfacción con estas iniciativas. Sin embargo, un 20.00% las percibe como poco efectivas, lo que considera áreas de mejora en la calidad o alcance de las actividades de capacitación. Además, un 13.33% las evalúa como moderadamente efectivas. Estos resultados destacan la importancia de continuar evaluando y mejorando las estrategias de capacitación en seguridad cibernética para garantizar una preparación efectiva del personal ante las amenazas digitales.

Estrategias de ciberseguridad: el 33.33% de las empresas señala la resistencia al cambio como el principal obstáculo, sugiriendo retos internos en la adopción de nuevas prácticas. Además, un 33.33% destaca la falta de recursos financieros como una limitación. Otros factores incluyen la falta de comprensión por parte de la dirección ejecutiva (16.67%) y la escasez de experiencia en auditoría de seguridad cibernética (16.67%). Estos hallazgos resaltan la importancia de abordar tanto los desafíos internos como externos para una integración efectiva de la auditoría en las estrategias de ciberseguridad.

Autonomía del equipo de auditoría interna: el 43.33% de las empresas indica una autonomía moderada para el equipo de auditoría interna, lo que propone cierto grado de libertad en la realización de evaluaciones de seguridad cibernética. Sin embargo, un 33.33% reporta una alta autonomía, lo que refleja un nivel de independencia en este proceso. En contraste, un 16.67% señala que el equipo no tiene autonomía, lo que puede indicar limitaciones en la capacidad de acción. Se requiere equilibrar la autonomía con la supervisión adecuada para garantizar una evaluación eficaz de la seguridad cibernética en la empresa.

Pruebas de continuidad: las empresas del sector comercial muestran diferentes enfoques hacia las pruebas de continuidad del negocio en casos de incidentes de seguridad cibernética. Un notable 40.00% realiza estas pruebas en ocasiones, mientras que otro 33.33% lo hace de forma regular, lo que alude un nivel considerable de preparación para mantener la operatividad en situaciones de crisis cibernética. Sin embargo, un 26.67% aún no lleva a cabo estas pruebas o está considerando implementarlas, lo que podría indicar una oportunidad para mejorar la resiliencia empresarial ante incidentes cibernéticos. Estos resultados destacan la importancia de las pruebas de continuidad del negocio para garantizar la capacidad de respuesta y recuperación ante amenazas digitales en el sector comercial.

Colaboración auditoría-ciberseguridad: el nivel de colaboración entre el departamento de Auditoría Interna y el equipo de ciberseguridad en las empresas del sector comercial varía. Un sólido 46.67% describe esta relación como colaborativa, lo que recomienda una estrecha cooperación entre ambos departamentos para abordar los desafíos de seguridad. Además, un 26.67% la califica como muy colaborativa, indicando un alto grado de trabajo en equipo en la gestión de riesgos cibernéticos. Sin embargo, un 16.67% la percibe como poco colaborativa, lo que puede señalar áreas de mejora en la comunicación y coordinación entre los equipos.

Gestión de incidentes: el análisis revela que el 43.33% tiene procedimientos definidos, indicando una sólida preparación. Sin embargo, el 20.00% tiene procedimientos poco claros, sugiriendo una necesidad de mejora. Un 16.67% está en proceso de implementación, mientras que el 20.00% no tiene planes, lo que destaca la oportunidad de fortalecer la preparación ante incidentes cibernéticos. Estos hallazgos muestran la importancia de procedimientos claros para minimizar el impacto de los incidentes de seguridad en las operaciones y la reputación empresarial.

Preparación para cumplimiento normativo: el 53.33% se siente muy preparado para cumplir con regulaciones de seguridad cibernética, esto muestra una sólida base en cumplimiento normativo. Sin embargo, el 20.00% se percibe como poco preparado, lo que indica áreas de mejora en la alineación con las normativas. Es necesario mantener un nivel adecuado de preparación para garantizar el cumplimiento normativo y mitigar posibles riesgos legales y financieros asociados con la seguridad cibernética.

Efectividad de medidas de seguridad: La mayoría de las empresas del sector comercial califican sus medidas de seguridad cibernética como efectivas o muy efectivas, representando el 90% de las respuestas. Este alto porcentaje da una confianza generalizada en la protección de los sistemas y datos. Sin embargo, un pequeño porcentaje (13.33%) la considera moderada efectiva, y otro (10%) se muestra indeciso sobre su efectividad (ver figura 4).

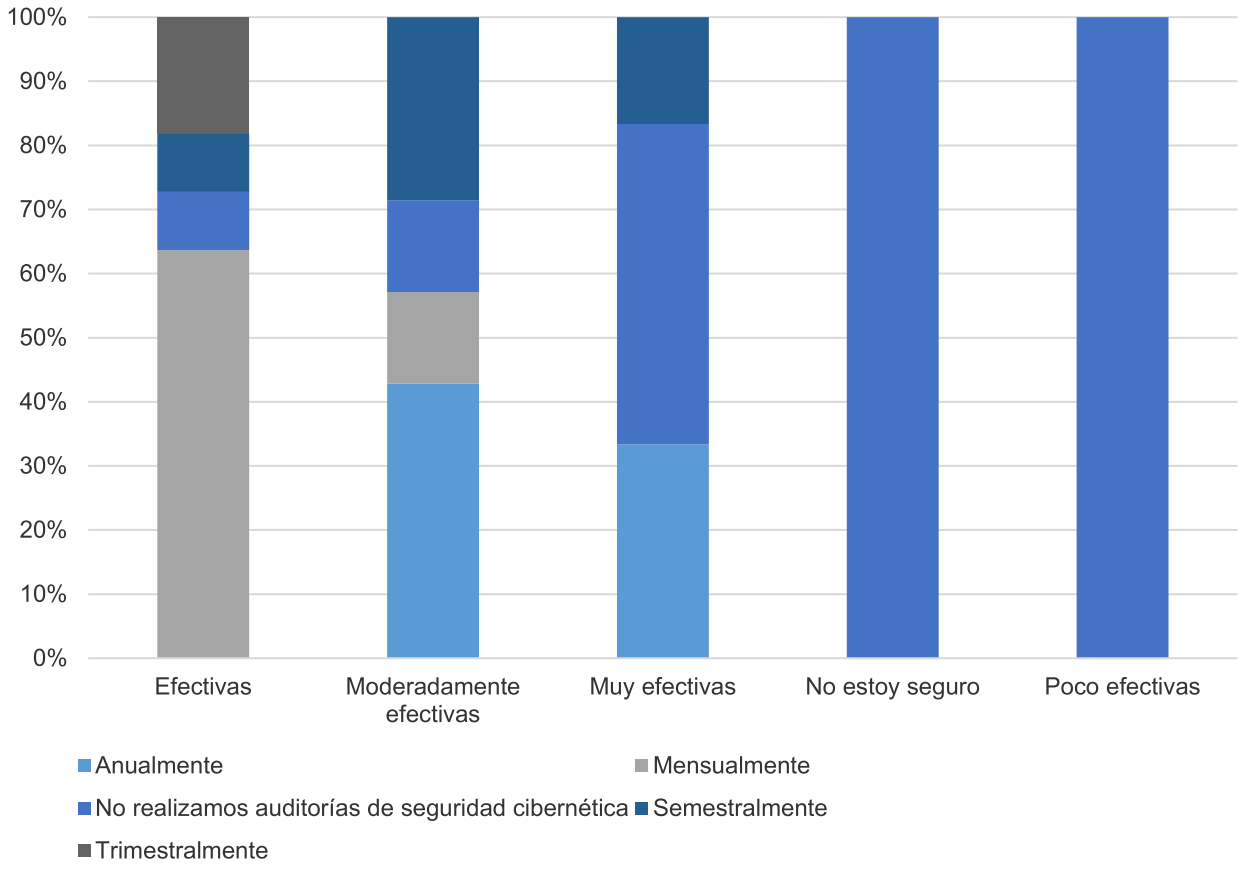

Figura 4
Desafíos en res Efectividad de medidas de seguridad

***Nota*.** Los datos fueron tomados de la encuesta aplicada en la provincia de Pichincha, ciudad de Quito, empresas del sector comercial.

DISCUSIÓN

Al contrastar los resultados obtenidos del presente estudio y de la investigación de llevada a cabo en empresas del sector comercial por (Bueno & Haz, 2022) sobre seguridad cibernética en las pymes ecuatorianas, se destacan dos resultados significativos para su análisis y reflexión.

Primero, la importancia del conocimiento técnico del personal en ciberseguridad se evidencia en ambas investigaciones, las cuales subrayan la creciente conciencia de las pymes sobre la necesidad de capacitación y conocimiento técnico de su personal para mitigar los riesgos

cibernéticos. Es evidente que las empresas reconocen que los empleados son un eslabón fundamental en la cadena de seguridad y que su adecuada capacitación puede reducir la probabilidad de incidentes de seguridad causados por errores humanos o ataques dirigidos.

Segundo, otro resultado relevante es que el 99% de las empresas comerciales muestran interés en implementar mecanismos de ciberseguridad. Esta alta cifra refleja la creciente preocupación de las pymes por proteger sus activos digitales y mantener la integridad, confidencialidad y disponibilidad de la información. El interés en adoptar herramientas y prácticas de seguridad informática y de la información presenta una evolución positiva en la mentalidad empresarial, reconociendo la necesidad de inversiones en ciberseguridad como parte integral de la gestión empresarial moderna (Coronel-Suárez & Quirumbay-Yagual, 2022).

Las implicaciones de estos hallazgos son claras: las pymes ecuatorianas deben priorizar la capacitación en ciberseguridad de su personal como una inversión estratégica para fortalecer sus defensas contra las amenazas cibernéticas. La alta predisposición a implementar mecanismos de seguridad informática refiere una mayor conciencia sobre los riesgos cibernéticos y una disposición activa para abordarlos (Vargas-Borbúa et al. 2017; Zuña-Macancela et al. 2019).

Sin embargo, es concluyente que esta voluntad se traduzca en acciones concretas, como la implementación de políticas de seguridad, el uso de herramientas de protección adecuadas y la colaboración con expertos en ciberseguridad para mitigar los riesgos de manera efectiva. La creación de una guía de buenas prácticas de ciberseguridad, como lo indican los encuestados, podría ser una medida efectiva para estandarizar los procesos de seguridad y mejorar la preparación ante posibles amenazas cibernéticas (Flores-Álava & Mena-Hernández, 2023).

Resultados similares han sido obtenidos por el estudio “Seguridad de la información en instituciones públicas: desafíos y buenas prácticas en el contexto ecuatoriano” (Ávila-Coello, 2024). Ambos estudios revelan que un 80% de las empresas comerciales no realizan auditorías de seguridad cibernética de manera regular, sugiriendo una falta de atención o inversión en la protección de datos. Además, solo un pequeño porcentaje lleva a cabo auditorías anuales (16.67%) o con mayor frecuencia. Esto contrasta con el hallazgo de que el 46.67% de las empresas cuenta con un plan actualizado de respuesta a incidentes, indicando una preparación sólida para manejar posibles ataques cibernéticos.

En el ámbito público, las instituciones ecuatorianas muestran un rendimiento bastante alto en la mayoría de las áreas de gestión de tecnologías de la información, con un 40% realizando pruebas de continuidad de forma ocasional y un 33.33% de forma regular. No obstante, el principal desafío identificado es la transformación digital, con solo un 26.67% de las entidades considerándose preparadas, lo que establece una brecha significativa en la adopción de tecnologías emergentes para fortalecer la ciberseguridad.

Comparando estos resultados, se observa que, mientras las empresas del sector privado tienen una mayor conciencia sobre la importancia de la ciberseguridad y cuentan con planes de respuesta a incidentes más actualizados, las instituciones públicas muestran un desempeño más sólido en términos de evaluación de riesgos y pruebas de continuidad. Sin embargo, ambas enfrentan desafíos en áreas clave, como la falta de personal capacitado, la resistencia al cambio y la necesidad de una mayor colaboración interinstitucional.

Este análisis configura que el sector privado necesita mejorar la frecuencia de sus auditorías y aumentar la conciencia sobre la ciberseguridad. Por su parte, el sector público enfrenta retos en la transformación digital y la adopción de tecnologías emergentes. Ambos sectores podrían beneficiarse de una mayor colaboración y de programas de capacitación más efectivos para fortalecer la protección de datos en Ecuador. La integración de mejores prácticas y un enfoque más proactivo en la gestión de la seguridad cibernética serán cruciales para mejorar la resiliencia y protección de los activos digitales en ambos sectores.

Los resultados del presente estudio en comparación con el estudio de “Gestión del riesgo y la ciberseguridad en el sector financiero popular y solidario del Ecuador (Ojeda-Contreras et al., 2020), revela una dicotomía en cuanto a la adopción de tecnología y la gestión de riesgos en

las entidades financieras, como en el caso de la Cooperativa de Ahorro y Crédito La Merced. Se destaca que el avance y la implementación exitosa de nuevas tecnologías en respuesta a las demandas del mercado, con un respaldo del 87% de los encuestados, adicional se indica una falta de gestión de riesgos y una exposición a la ciberdelincuencia

En ambos estudios se evidencia un alto grado de aceptación y adaptación por parte de las empresas comerciales hacia la implementación de nuevas tecnologías, donde el 81% de ellos informaron haber experimentado ataques maliciosos en sus plataformas digitales el año anterior. Este dato resalta la necesidad de una mayor atención a la ciberseguridad y una mejor educación sobre prácticas seguras en línea para mitigar tales riesgos.

Otra similitud en los resultados de los estudios es la falta de gestión sistemática de riesgos, con el 89% de los empleados, indicando que la gestión de riesgos se realiza de manera empírica y no alineada con los objetivos estratégicos de la institución. Además, el 68% de los consultados opinan que los riesgos no se gestionan de manera efectiva, lo que evidencia una brecha entre la implementación de tecnología y la capacidad para salvaguardar los activos y datos de la cooperativa.

Estos descubrimientos resaltan la imperiosa necesidad de abrazar las nuevas tecnologías como un medio para mantener la competitividad en el panorama financiero contemporáneo. Además, recalcan la importancia crítica de establecer y aplicar prácticas robustas de gestión de riesgos y ciberseguridad. En un entorno donde la tecnología y la ciberseguridad son elementos fundamentales para el éxito empresarial, estos aspectos se vuelven aún más vitales para garantizar la sostenibilidad y el crecimiento en el mercado financiero actual.

CONCLUSIÓN

En el contexto específico de Ecuador, las empresas enfrentan desafíos particulares en materia de ciberseguridad, desde la falta de recursos y capacidades técnicas hasta la adaptación a un marco regulatorio en evolución. Sin embargo, existen oportunidades para fortalecer la resiliencia cibernética a través de la colaboración público-privada, la inversión en investigación e innovación en seguridad digital, y la promoción de una cultura de ciberseguridad en todos los niveles organizacionales. La mayoría de las empresas encuestadas no llevan a cabo auditorías de seguridad cibernética de manera regular, debido a falta de atención o inversión en ciberseguridad. Estos hallazgos resaltan la necesidad de una mayor conciencia sobre la importancia de la seguridad cibernética y la implementación de medidas preventivas para mitigar los riesgos asociados a los ataques cibernéticos en el entorno empresarial.

FINANCIAMIENTO

No monetario

CONFLICTO DE INTERÉS

No existe conflicto de interés con personas o instituciones ligadas a la investigación.

AGRADECIMIENTOS

A la unidad académica de posgrado de la UCACUE.

REFERENCIAS

Ávila-Coello, A. A. (2024). Seguridad de la información en instituciones públicas: desafíos y buenas prácticas en el contexto ecuatoriano [Information Security in Public Institutions: Challenges and Good Practices in the Ecuadorian Context]. *Journal of Economic and Social Science Research*, *4*(2), 140–156. https://doi.org/10.55813/gaea/jessr/v4/n2/96

Bueno, G., & Haz, L. (2022). Ciberseguridad post Covid-19 y su impacto en las pymes del Ecuador [Post-covid-19 cybersecurity and its impact on Ecuador's SMEs]. *Pro*

Sciences: Revista De Producción, Ciencias E Investigación, *6*(46), 103–120. https://doi.org/10.29018/issn.2588-1000vol6iss46.2022pp103-120

Cervera, A., & Goussens, A. (2024). Ciberseguridad y uso de las TIC en el Sector Salud [Cybersecurity and the use of ICTs in the Health Sector]. *Atención primaria, 56*(3). DOI: 10.1016/j.aprim.2023.102854

Coronel-Suárez, I., & Quirumbay-Yagual, D. (2022). Seguridad informática, metodologías, estándares y marco de gestión en un enfoque hacia las aplicaciones web [IT security, methodologies, standards and management framework in a web application approach]. *Revista Científica Y Tecnológica UPSE*, *9*(2), 97-108. https://doi.org/10.26423/rctu.v9i2.672

Flores-Álava, S., & Mena-Hernández, L. (2023). Propuesta de Buenas Prácticas para Mitigar Ciberataques en Usuarios de Entidades Financieras [Proposal for Good Practices to Mitigate Cyber-attacks on Users of Financial Institutions]. *593 Digital Publisher CEIT*, *8*(4), 159-173. https://doi.org/10.33386/593dp.2023.4.1652

García-Córdoba, J, & Herrero-Pérez, L. (2020). La ciberdefensa en los sistemas de información sanitarios militares [Cyberdefense in the military healthcare information systems]. *Sanidad Militar*, *76*(3), 140-142. https://dx.doi.org/10.4321/s1887-85712020000300001

Gomero-Cuadra, Raúl, & Sánchez-Calle, David. (2024). Ciberseguridad en servicios de apoyo al médico ocupacional de la ciudad de Lima. Estudio piloto [Cybersecurity in the support services to occupational physicians in the city of Lima. A pilot study]. *Revista Médica Herediana*, *35*(1), 38-43. https://dx.doi.org/10.20453/rmh.v35i1.5298

Jeimy, J., & Cano, M. (2023). FLEXI - A conceptual model for enterprise cyber resilience. *Procedia Computer Science, 219*, 11-19. https://doi.org/10.1016/j.procs.2023.01.258.

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 [Risk management and cybersecurity in Ecuador's popular and solidarity-based financial sector]. *CIENCIAMATRIA*, *6*(2), 192-219. https://doi.org/10.35381/cm.v6i2.366

Rodríguez-Labrada, Yenis Katia, Cano Inclán, Anisley, & Cuesta Rodríguez, Floriselda. (2019). Estado del arte de la Auditoría de Información [State of the Art of Information Audit]. *E-Ciencias de la Información*, *9*(1), 132-151. https://dx.doi.org/10.15517/eci.v1i1.35409

Sancho-Hirare, Carolina. (2017). Ciberseguridad. Presentación del dossier [Cybersecurity. Presentation of the dossier]. *URVIO Revista Latinoamericana de Estudios de Seguridad*, (20), 8-15. https://doi.org/10.17141/urvio.20.2017.2859

Vargas-Borbúa, Robert, Recalde Herrera, Luis, & P. Reyes Ch., Rolando. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: Modelo ecuatoriano de gobernanza en ciberdefensa [Cyber-defense and cybersecurity, beyond the virtual world: Ecuadorian model of cyber-defense governance]. *URVIO Revista Latinoamericana de Estudios de Seguridad*, (20), 31-45. https://doi.org/10.17141/urvio.20.2017.2571

Vega, E. (2019). *Seguridad de la Información: Principios y Prácticas [Information Security: Principles and Practices].* Alzamora: Editorial Área de Innovación y Desarrollo, S.L. https://doi.org/10.17993/tics.2021.4

Zeadally, S., Isaac, J. T., & Baig, Z. (2016). Security Attacks and Solutions in Electronic Health (E-health) Systems. *Journal of medical systems*, *40*(12), 263. https://doi.org/10.1007/s10916-016-0597-z

Zuña-Macancela, Edgar René, Arce Ramírez, Ángel Alberto, Romero Berrones, Wilson Javier, & Soledispa Baque, César Jorge. (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.

Zuñiga-Paredes, Andrea Raquel, Jalón Arias, Edmundo José, Andrade Olmedo, María Ernestina, & Giler Chango, José Leonardo. (2021). Análisis de seguridad informática en entornos virtuales de la Universidad regional autónoma de los Andes extensión Quevedo en tiempos de covid-19 [Analysis of computer security in virtual environments of the Autonomous regional University of the Andes extension Quevedo in times of covid-19]. *Revista Universidad y Sociedad*, *13*(3), 454-459.