Ciencia y Educación
(L-ISSN: 2790-8402 E-ISSN: 2707-3378)
Vol. 7 No. 4.1
Edición Especial IV 2026

EVALUACIÓN DE BRECHAS Y MADUREZ EN CIBERSEGURIDAD EN PYMES TECNOLÓGICAS DE LOJA PARA EL FORTALECIMIENTO DE SU RESILIENCIA DIGITAL

GAP AND MATURITY ASSESSMENT IN CYBERSECURITY IN TECHNOLOGY SMEs IN LOJA TO STRENGTHEN THEIR DIGITAL RESILIENCE

Autores: [1]Freddy David Espinoza Quezada, [2]Daniel Iván Quirumbay Yagual.
[1]ORCID ID: https://orcid.org/0009-0008-3506-6612
[2]ORCID ID: https://orcid.org/0000-0002-6513-3520
[1]E-mail de contacto: freddy.espinozaquezada9703@upse.edu.ec
[2]E-mail de contacto: dquirumbay@upse.edu.ec
Afiliación: [1*2*]Universidad Estatal Península de Santa Elena, (Ecuador).
Artículo recibido: 22 de Abril del 2026
Artículo revisado: 24 de Abril del 2026
Artículo aprobado: 26 de Abril del 2026
[1]Ingeniero en Electrónica y Telecomunicaciones, egresado de la Universidad Técnica Particular de Loja, (Ecuador), con 10 años de experiencia en el ámbito de las telecomunicaciones, redes, infraestructura, seguridad electrónica y domótica. Magíster en Telecomunicaciones en la Universidad del Azuay, (Ecuador). Maestrante de la Maestría en Ciberseguridad en la Universidad Estatal Península de Santa Elena, (Ecuador). Actualmente, se desempeña como Ingeniero de Diseño y Soporte Técnico en la Empresa Segcomp, (Ecuador).
[2]Licenciado en Sistemas de Información, egresado de la Escuela Superior Politécnica del Litoral, (Ecuador). Magíster en Seguridad Informática Aplicada, egresado de la Escuela Superior Politécnica del Litoral, (Ecuador). Actualmente cursa el Doctorado en Tecnologías de la Información y las Comunicaciones en la Universidade da Coruña, (España).

Resumen

La transformación digital ha impulsado el crecimiento de las pequeñas y medianas empresas (PYMES) del sector tecnológico; sin embargo, este proceso no siempre ha estado acompañado por una gestión estructurada de la ciberseguridad, lo que incrementa la exposición a riesgos digitales y compromete la continuidad operativa. En este contexto, el estudio tuvo como objetivo evaluar el nivel de madurez en ciberseguridad de las PYMES tecnológicas de la ciudad de Loja e identificar las brechas organizacionales que inciden en su resiliencia digital. La investigación adoptó un enfoque cuantitativo, con diseño no experimental y transversal, aplicando una encuesta estructurada a 20 PyMEs mediante una escala Likert de cinco puntos para analizar cinco dimensiones: recursos, gobernanza y responsabilidades, cultura organizacional, capacidades técnicas y políticas de seguridad; el instrumento evidenció alta consistencia interna ($\alpha = 0{,}92$). Los resultados muestran un nivel medio de madurez en ciberseguridad, con una media global de 2,65 sobre 5 y valores entre 1,0 y 4,9; las capacidades técnicas alcanzaron el mayor nivel relativo ($\approx$ 2,8), mientras que la cultura organizacional y las políticas de seguridad registraron los puntajes más bajos ($\approx$ 2,5), evidenciando un enfoque predominantemente reactivo. En conclusión, la evaluación de la madurez en ciberseguridad se consolida como un instrumento estratégico para diagnosticar brechas estructurales y orientar decisiones progresivas que fortalezcan de manera sostenible la resiliencia digital empresarial, en coherencia con el marco normativo ecuatoriano y los estándares internacionales de referencia.
Palabras clave: Ciberseguridad, Políticas de seguridad, Resiliencia digital, Transformación digital, Brechas en ciberseguridad.

Abstract

Digital transformation has driven the growth of small and medium-sized enterprises (SMES) in the technology sector; however, this process has not always been accompanied by structured cybersecurity management, increasing exposure to digital risks and compromising operational continuity. In this context, the study aimed to evaluate the cybersecurity maturity level of technology SMES in the city of Loja and identify organizational gaps that affect their digital resilience. The research adopted a quantitative approach, with a non-

experimental, cross-sectional design, applying a structured survey to 20 SMEs using a five-point Likert scale to analyze five dimensions: resources, governance and responsibilities, organizational culture, technical capabilities, and security policies. The instrument demonstrated high internal consistency (α = 0.92). The results show a medium level of cybersecurity maturity, with an overall mean of 2.65 out of 5 and values between 1.0 and 4.9. Technical capabilities reached the highest relative level (≈ 2.8), while organizational culture and security policies registered the lowest scores (≈ 2.5), demonstrating a predominantly reactive approach. In conclusion, the cybersecurity maturity assessment is consolidated as a strategic tool for diagnosing structural gaps and guiding progressive decisions that sustainably strengthen corporate digital resilience, in accordance with the Ecuadorian regulatory framework and international benchmark standards.

Keywords: Cybersecurity, Security policies, Digital resilience, Digital transformation, Cybersecurity gaps.

Sumário

A transformação digital impulsionou o crescimento das pequenas e médias empresas (PMES) do setor tecnológico; contudo, esse processo nem sempre foi acompanhado por uma gestão estruturada de cibersegurança, aumentando a exposição a riscos digitais e comprometendo a continuidade operacional. Nesse contexto, o estudo teve como objetivo avaliar o nível de maturidade em cibersegurança de PMEs do setor tecnológico na cidade de Loja e identificar lacunas organizacionais que afetam sua resiliência digital. A pesquisa adotou uma abordagem quantitativa, com delineamento transversal não experimental, aplicando um questionário estruturado a 20 PMEs, utilizando uma escala Likert de cinco pontos para analisar cinco dimensões: recursos, governança e responsabilidades, cultura organizacional, capacidades técnicas e políticas de segurança. O instrumento demonstrou alta consistência interna (α = 0,92). Os resultados apontam um nível médio de maturidade em cibersegurança, com média geral de 2,65 em 5 e valores entre 1,0 e 4,9. As capacidades técnicas atingiram o nível relativo mais alto (≈ 2,8), enquanto a cultura organizacional e as políticas de segurança registraram as pontuações mais baixas (≈ 2,5), demonstrando uma abordagem predominantemente reativa. Em conclusão, a avaliação da maturidade em cibersegurança se consolida como uma ferramenta estratégica para diagnosticar lacunas estruturais e orientar decisões progressivas que fortaleçam de forma sustentável a resiliência digital corporativa, em conformidade com o marco regulatório equatoriano e os padrões internacionais de referência.

Palavras-chave: Cibersegurança, Políticas de segurança, Resiliência digital, Transformação digital, Lacunas em cibersegurança.

Introducción

La transformación digital ha reconfigurado las operaciones de las pequeñas y medianas empresas (PYMES) a nivel global, generando oportunidades de innovación y competitividad, pero también incrementando su exposición a amenazas cibernéticas. En este contexto, la ciberseguridad se ha consolidado como un desafío estratégico para la sostenibilidad organizacional, dado que los ciberataques representan uno de los principales riesgos globales por su impacto económico, operativo y reputacional (Aguilar, 2021). Esta preocupación se refleja en el ámbito internacional, donde más de 106 países han desarrollado políticas de ciberseguridad (Organization of American States, 2025). Sin embargo, en América Latina esta problemática se intensifica, ya que solo el 42 % de las PYMES ha implementado políticas formales de seguridad, evidenciando una alta vulnerabilidad asociada a limitaciones de recursos y capacitación (Zambrano et al., 2024; Luján et al., 2023). En el contexto ecuatoriano, si bien

las Pymes han mostrado avances en la adopción de tecnologías digitales con el objetivo de fortalecer su competitividad, la ciberseguridad aún no se ha consolidado como una prioridad estratégica dentro de sus procesos de gestión.

Evidencia empírica reciente indica que una proporción significativa de estas organizaciones opera con niveles básicos de digitalización y con mecanismos de protección incipientes, dado que aproximadamente el 65 % de las empresas dispone únicamente de tecnología mínima y prácticas limitadas en materia de ciberseguridad (Armijos et al., 2024). Esta situación se ve agravada por la persistencia de brechas estructurales en la aplicación de los marcos normativos vigentes, donde el nivel de cumplimiento regulatorio en seguridad digital apenas alcanza el 31 % en el segmento de las PYMES. A ello se suman las limitaciones en la efectividad de las políticas públicas orientadas a fortalecer la seguridad cibernética en el entorno empresarial, lo que contribuye a mantener una gestión fragmentada y reactiva de los riesgos digitales (Vasco et al., 2025; Pozo, 2022).

En la ciudad de Loja, las PYMES tecnológicas desempeñan un papel relevante en el desarrollo de la economía local. De acuerdo con datos del Instituto Nacional de Estadística y Censos, existen aproximadamente 56 empresas del sector tecnológico en la provincia (Instituto Nacional de Estadística y Censos INEC, 2024). Sin embargo, investigaciones previas evidencian que estas organizaciones presentan en su mayoría, niveles bajos o intermedios de madurez en ciberseguridad, con brechas en el ámbito organizativo, normativo y cultural de la gestión de riesgos digitales (Vera, 2020; Zuñiga et al., 2020). En este sentido, las brechas identificadas en el contexto local se alinean con tendencias más amplias, donde la limitada madurez en ciberseguridad incrementa la vulnerabilidad de las Pymes. Esta situación resulta particularmente crítica considerando que el 57 % de las PYMES reconoce que un ciberataque puede comprometer significativamente su continuidad operativa (European Union Agency for Cybersecurity, 2021).

Desde esta perspectiva, el presente estudio se justifica en la necesidad de evaluar la madurez en ciberseguridad de las PYMES tecnológicas de Loja, identificando brechas estructurales y áreas prioritarias de mejora. Para ello, se adopta un enfoque cuantitativo y descriptivo mediante la aplicación de una encuesta a 20 empresas del sector. El instrumento analiza cinco dimensiones fundamentales: cultura organizacional, gobernanza y responsabilidades, capacitación del personal, infraestructura tecnológica y políticas de seguridad. Este estudio enfatiza la importancia de fortalecer la resiliencia digital de las PYMES de la ciudad de Loja mediante una gestión eficiente de los recursos, la formación continua del talento humano y la implementación de políticas de seguridad alineadas con marcos regulatorios nacionales e internacionales, como el NIST Cybersecurity Framework y el Cybersecurity Capability Maturity Model (C2M2).

Estos referentes contribuyen a mejorar la gestión de los riesgos digitales y a promover la sostenibilidad organizacional en entornos altamente competitivos y vulnerables (National Institute of Standards and Technology, 2018; U.S. Department of Energy, 2022). En este sentido, la ciberseguridad debe abordarse no solo como un desafío técnico, sino como un pilar estratégico de la transformación digital, indispensable para garantizar la continuidad operativa y la competitividad de las PYMES.

En este contexto, a pesar de las referencias bibliográficas acerca de seguridad corporativa existe un vacío en la medición cuantitativa de la madurez en ciberseguridad específicamente, en las PyMEs de la ciudad de Loja, donde los recursos son limitados y en un entorno donde aún no se han desarrollado análisis estructurados sobre esta problemática.

A partir de una metodología clara y sistemática, alineada con la normativa ecuatoriana vigente y con marcos internacionales, en este trabajo se identifica las brechas tanto organizacionales como técnicas. De esta forma, los resultados no solo aportan evidencia empírica para el ámbito académico, sino que también pueden servir como referencia práctica para que las empresas fortalezcan su gestión de la seguridad de la información y orienten decisiones estratégicas encaminadas al desarrollo progresivo y sostenible de su resiliencia digital. En los últimos años, la transformación digital se ha convertido en un componente clave para las pequeñas y medianas empresas (PyMEs), ya que les permite fortalecer su competitividad, impulsar la innovación y optimizar sus procesos internos. Sin embargo, en muchos escenarios dicho avance tecnológico se desarrolla de forma gradual y sin una planificación integral con limitaciones en la adopción de medidas adecuadas de ciberseguridad, especialmente en organizaciones con recursos humanos y financieros reducidos.

Dentro del ámbito latinoamericano, donde persisten bajos niveles de madurez digital y debilidades en la gestión organizacional, esta situación incrementa la exposición de las PyMEs a amenazas frecuentes como el phishing, el ransomware y las técnicas de ingeniería social. (Zambrano et al., 2024; Porrúa, 2025). En las pequeñas y medianas empresas, la adopción de herramientas digitales crece de forma relevante en comparación a la implementación de prácticas formales y técnicas para la protección de la información, tal como lo evidencian diversas investigaciones realizadas a nivel regional. A su vez, esta brecha da lugar a una mayor superficie de ataque y, en consecuencia, un crecimiento significativo del riesgo de incidentes cibernéticos (Luján et al., 2023); León et al., 2022). En este contexto, la ciberseguridad se configura como un pilar indispensable de la transformación digital, ya que su ausencia compromete principios fundamentales como la confidencialidad, la integridad, la disponibilidad y el no repudio de los datos.

La gestión de la ciberseguridad en las pequeñas y medianas empresas (PYMES) en Ecuador aún no se ha consolidado como un eje estratégico prioritario. Según señalan (Peralta y Aguilar, 2021), estas organizaciones suelen enfocar sus esfuerzos en la reducción de costos y en la mejora de la eficiencia operativa, lo que restringe la asignación de recursos destinados a la protección de los sistemas de información. En consecuencia, se evidencia una brecha relevante entre el nivel de digitalización alcanzado y las capacidades institucionales para gestionar de manera adecuada los riesgos cibernéticos. A ello se suma la limitada disponibilidad de profesionales especializados, la ausencia de estructuras organizativas orientadas a la seguridad y el uso intensivo de tecnologías, factores que incrementan la vulnerabilidad de las PyMEs frente a las amenazas digitales (Ramos, 2023).

En la ciudad de Loja, esta problemática adquiere características particulares. Según datos del (Instituto Nacional de Estadística y Censos INEC, 2024), en la provincia se registran 53 empresas pequeñas, 2 medianas de tipo A y 1 mediana de tipo B dedicadas al sector

tecnológico. La adopción de la transformación digital representa para estas organizaciones una oportunidad para optimizar sus procesos y fomentar la innovación; sin embargo, el ient3limitado énfasis en ciberseguridad dentro de las empresas, la escasa articulación con marcos normativos nacionales e internacionales, la falta de políticas formalizadas y la insuficiente asignación de recursos económicos dificultan la construcción de entornos digitales resilientes. En este contexto, se configura un escenario de alta vulnerabilidad que hace necesaria una evaluación sistemática de los niveles de madurez y de las brechas existentes en materia de ciberseguridad.

En ciberseguridad, las brechas son las diferencias que surgen entre las actividades que realizan para asegurar la información y las guías que han sido definidas por normativas y estándares establecidos. Estas deficiencias en las pequeñas y medianas empresas, afectan la gestión del riesgo digital y se originan como resultado de la interacción entre factores económicos, organizativos, tecnológicos y humanos. Uno de los factores más relevantes es la escasa asignación de recursos económicos para la seguridad de la información, debido a que se ve como un gasto en lugar de una inversión estratégica (Bustillos y Rojas, 2022). Por lo cual, dicha restricción limita la implementación de auditorías especializadas, controles técnicos avanzados y planes formales para responder a incidentes.

A ello se suma la falta de procedimientos de seguridad y políticas internas documentadas, algo común en las PyMEs de Ecuador, aunque su dependencia de los sistemas de información ha ido en aumento (Vera, 2020). Además, la escasez de formación y concienciación en ciberseguridad vuelve el factor humano un elemento esencial de vulnerabilidad; esto hace más efectivos los ataques basados en phishing e ingeniería social (Maldonado, 2022; Villarreal, 2024). Estas brechas muestran una falta de conexión entre la adopción tecnológica y la madurez en ciberseguridad, lo que subraya la importancia de analizarlas sistemáticamente como fundamento para robustecer la resiliencia digital.

La madurez en la ciberseguridad organizacional hace referencia a la medida en que una compañía incorpora de manera sistemática procesos, políticas, controles técnicos y cultura de seguridad a su gestión. Por lo tanto, las acciones de seguridad tienden a ser reactivas y fragmentadas en niveles bajos de madurez, mientras que en aquellos más altos se distinguen por la gobernanza, la planificación y la mejora continua. El nivel de madurez organizacional y digital guarda una relación directa con el grado de madurez en ciberseguridad en las PyMEs de Ecuador. Por ende, la incorporación de tecnologías sin una evaluación estructurada de riesgos, limita la capacidad para prevenir, detectar y responder a incidentes (Armijos et al., 2024). Además Villarreal (2024) afirma que la ausencia de una capacitación del personal humano obstaculiza la creación de una cultura organizacional enfocada en la seguridad.

Desde el punto de vista de la ciberseguridad organizacional, la conformidad con estándares internacionales establece criterios que sirven para medir la capacidad institucional con respecto a la administración de la seguridad de la información. Este método se basa en la gestión de riesgos, la determinación de responsabilidades y la formalización de procedimientos de control y mejora, lo cual posibilita el análisis estructurado del estado de la ciberseguridad en las organizaciones (International Organization for Standardization;

International Electrotechnical Commission, 2022). No obstante Choez y Mora (2025), mencionan que la implementación de este estándar en las PyMEs está limitada por restricciones de recursos y habilidades técnicas. Desde esta perspectiva, marcos complementarios como el NIST Cybersecurity Framework y el Cybersecurity Capability Maturity Model (C2M2) hacen posible la evaluación gradual de las capacidades técnicas y organizacionales, lo cual posibilita detectar brechas entre el nivel esperado de madurez y la situación actual.

En consecuencia, la evaluación del grado de madurez se establece como una herramienta diagnóstica para guiar en la toma de decisiones estratégicas en el manejo de la ciberseguridad. Se define la resiliencia digital como la habilidad de una organización para prevenir, identificar, reaccionar y reponerse ante incidentes de ciberseguridad, asegurando la continuidad de las operaciones. En las pequeñas y medianas empresas, esta habilidad se basa en la coordinación entre los controles técnicos, los procedimientos organizativos y la capacitación del talento humano. Así mismo, la resiliencia digital se establece como un elemento transversal en el manejo de la seguridad de la información y no como una medida tecnológica aislada. Según Orellana (2020) y López y Ordóñez (2024) la falta de roles definidos, planes formales de respuesta y mecanismos de comunicación interna intensifican el impacto de los incidentes cibernéticos en las PYMES de Ecuador.

Por lo tanto, la falta de estructuras organizativas enfocadas en la seguridad, limita la capacidad de prevención y recuperación ante situaciones adversas. Por otro lado, la capacitación sistemática y la concienciación en seguridad mejoran las prácticas de protección de la información y disminuyen el número de fallos operativos, como indica (Maldonado 2022). En el ámbito normativo, el marco jurídico ecuatoriano refuerza la implementación de estrategias en materia de ciberseguridad. En este sentido, la protección de los datos personales es un objetivo esencial del manejo de la información, según lo indica el artículo 1 de la Ley Orgánica de Protección de Datos Personales. Dicha ley, se rige por principios como la confidencialidad, la seguridad y la responsabilidad proactiva (art. 10).

Por lo tanto, la normativa requiere que se implementen medidas organizativas y técnicas basadas en procedimientos de gestión y análisis del riesgo (arts. 37, 40 y 41), además, de incluir la seguridad desde el diseño y por defecto en los procesos digitales (art. 39). Por lo tanto, dicho marco facilita el fortalecimiento de la resiliencia digital de las PYMES (Ley orgánica de protección de datos personales, 2021). En este mismo contexto, el Reglamento General de la Ley Orgánica de Protección de Datos Personales, operacionaliza dichas disposiciones y define las pautas para su implementación. Por ende, las entidades tienen que incorporar acciones técnicas y organizativas que se alineen con la naturaleza del tratamiento, los riesgos relacionados y el estado de la técnica, según este reglamento (arts. 33 y 34).

Del mismo modo, fomenta la ejecución de evaluaciones de impacto como método preventivo (arts. 29 y 30) y establece el procedimiento para notificar las violaciones a la seguridad que supongan un peligro para los derechos de los titulares (arts. 24, 26 y 28). En consecuencia, el reglamento se establece como una guía práctica para manejar la resiliencia digital en las pequeñas y medianas empresas (Presidencia de la República del Ecuador, 2023). Por otro lado, el Código Orgánico

Integral Penal (COIP) considera la ciberseguridad desde un enfoque sancionatorio al penalizar comportamientos como el acceso no autorizado a sistemas informáticos, la divulgación inapropiada de bases de datos y el daño informático en el entorno digital, entre otros. Por lo tanto, a diferencia del enfoque preventivo y organizativo que buscan las leyes de protección de datos, el COIP adopta un método reactivo, interviniendo después de que las deficiencias en la gestión de la seguridad de la información se hayan convertido en un delito.

Así mismo en el ámbito de las pequeñas y medianas empresas, donde las limitaciones técnicas y organizativas a menudo dan lugar a brechas en la madurez de la ciberseguridad, este marco legal se vuelve crítico para demostrar que una gestión insuficiente de la seguridad de la información afecta negativamente la continuidad operativa y la resiliencia digital, lo cual puede ocasionar problemas legales (Asamblea Nacional del Ecuador, 2014). Así mismo, la Ley de Comercio electrónico, firmas electrónicas y mensajes de datos establece reglas con el objetivo de asegurar la disponibilidad, integridad, confidencialidad y autenticidad de los datos en el contexto de las transacciones digitales. Dicha normativa, a través de los artículos 5, 7, 8, 9, 10 y 15, enfatiza la responsabilidad de establecer controles de seguridad en la administración de transacciones digitales y en la protección de la información personal.

Por lo tanto, estas pautas ayudan a disminuir las disparidades en términos de madurez en ciberseguridad en las pequeñas y medianas empresas (PYMES) (Ley de comercio electrónico, firmas electrónicas y mensajes de datos, 2002). En Ecuador, la Ley Orgánica de Telecomunicaciones aporta aspectos significativos para el diagnóstico de la resiliencia digital. Por consiguiente, aunque esta normativa no regula directamente la gestión interna de la ciberseguridad organizacional, sí define ciertos objetivos en los artículos 22 y 24, los cuales establecen que se debe proteger la integridad y disponibilidad de las redes. Además, el artículo 3, por su parte, señala que los servicios de telecomunicaciones deben ser continuos y de buena calidad.

En consecuencia, la estabilidad de las telecomunicaciones se presenta como un elemento que permite la resiliencia digital en las pequeñas y medianas empresas (PYMES), debido que, gracias a la conectividad, esta mantiene el funcionamiento de los sistemas de información y los servicios digitales (Ley orgánica de telecomunicaciones, 2015). A pesar de que el esquema gubernamental de seguridad de la información (EGSI) está dirigido, en su mayoría, a las entidades públicas, sus directrices técnicas son un referente útil para examinar la ciberseguridad en las empresas privadas, especialmente en las pequeñas y medianas empresas tecnológicas. Por consiguiente, el EGSI fomenta, en su marco normativo, la gestión e identificación de riesgos, la protección y clasificación de los activos de la información, la asignación de roles y sus responsabilidades y, así como el manejo de incidentes y la continuidad de los servicios digitales.

Como resultado, a pesar de que no se considera un modelo de madurez formal ni un estándar que pueda ser certificado, sus lineamientos son relevantes para robustecer gradualmente la resiliencia digital en el entorno ecuatoriano (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2024). De manera similar la ISO/IEC 27001:2022, define un esquema internacional para manejar la seguridad de la información la cual se

fundamenta en la mejora continua y en la gestión de riesgos. No obstante, la norma fomenta la asignación de roles y responsabilidades (controles 5.1 y 5.2), el manejo sistemático de incidentes (control 5.24), la concienciación del personal (control 6.3) y la definición de políticas de seguridad. Por lo tanto, dichos controles posibilitan la detección de brechas y la priorización de acciones factibles en las pequeñas y medianas empresas sin necesidad de procedimientos formales de certificación (International Organization for Standardization; International Electrotechnical Commission, 2022).

Desde otra perspectiva, el marco COBIT ofrece directrices para promover la alineación de los objetivos del negocio con la gestión de la seguridad de la información. Asimismo, (ISACA, 2019) afirma que tales directrices ayudan a definir roles, responsabilidades, supervisión del desempeño organizacional y gestión de riesgos en PYMES con recursos limitados. Por lo tanto, este modelo complementa y fortalece los enfoques técnicos y regulatorios al enfatizar la integración dentro del sistema de gobierno y gestión organizacional y mejorar progresivamente el nivel de madurez de la ciberseguridad. Además, esto no reemplaza los controles establecidos por normas como ISO/IEC 27001, sino que actúa como un elemento integrador que potencia su aplicación.

Asimismo, el Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST CSF) organiza la gestión de la ciberseguridad en cinco funciones, las cuales son la identificación, protección, detección, respuesta y recuperación. Además, según el (National Institute of Standards and Technology, 2018), este método hace más fácil la conversión de los principios normativos en acciones específicas, lo cual es relevante para las pequeñas y medianas empresas debido a que posibilita una adopción acorde con sus capacidades organizacionales. Sin embargo, el NIST CSF ayuda a robustecer la resiliencia digital y funciona como un marco que complementa a la ISO/IEC 27001. Por ende, no reemplaza su enfoque de gestión, sino que lo potencia en términos de aplicación práctica y de desarrollo del nivel de madurez en ciberseguridad.

Por el contrario, el Cybersecurity Capability Maturity Model está enfocado en la medición del nivel de madurez de las capacidades de ciberseguridad a nivel organizacional. Además, el C2M2 posibilita la evaluación del desarrollo de las capacidades descritas por el NIST a través de niveles de madurez establecidos. Así mismo, este modelo permite detectar brechas y priorizar las acciones de mejora, lo que fomenta un fortalecimiento progresivo de la resiliencia digital en línea con las capacidades organizacionales de las PYMES (U.S. Department of Energy, 2022). En síntesis, la información analizada evidencia que la ciberseguridad en las PyMEs tecnológicas demanda no solo controles técnicos, sino también de prácticas organizativas y del cumplimiento de normativas.

Materiales y Métodos

La presente investigación tiene como finalidad evaluar el nivel de madurez en ciberseguridad de las pequeñas y medianas empresas (PYMES) del sector tecnológico de la ciudad de Loja, aportando un diagnóstico estructurado que permita comprender sus brechas organizacionales y técnicas, y orientar acciones progresivas de mejora basadas en la evidencia empírica obtenida. La investigación se desarrolla bajo un enfoque cuantitativo, con un alcance analítico–descriptivo, orientado a la

medición objetiva de variables asociadas con la gestión de la ciberseguridad. De este modo, el diseño metodológico se define como no experimental y transversal, dado que las variables se observan en su contexto natural y, en consecuencia, la recolección de los datos se efectúa en un único momento del tiempo. La población de estudio está conformada por las PyMEs del sector tecnológico de la ciudad de Loja.

La muestra está integrada por 20 PyMEs tecnológicas, seleccionadas mediante muestreo no probabilístico por conveniencia, considerando criterios de accesibilidad, disposición a participar y pertenencia al sector. Esta selección resulta adecuada para un estudio de carácter diagnóstico y analítico, considerando las limitaciones de acceso a información sensible vinculada con la ciberseguridad. La técnica de recolección de datos utilizada es la encuesta estructurada, aplicada al personal que se desempeñe en las pymes participantes. El instrumento corresponde a un cuestionario estructurado, implementado mediante un formulario digital en Google Forms. El cuestionario emplea una escala tipo Likert de cinco niveles, que permite evaluar dimensiones relacionadas con la falta de recursos financieros, la escasez de personal especializado, la limitada cultura organizacional, la infraestructura y las políticas formales.

Los datos obtenidos se organizan y analizan mediante estadística descriptiva, utilizando herramientas informáticas como Microsoft Excel, a través del cálculo de medias, medianas, desviaciones estándar, el mínimo y máximo con el propósito de identificar los niveles de madurez en ciberseguridad y las brechas existentes. Asimismo, previo al análisis de los datos, se evaluó la confiabilidad del instrumento mediante el coeficiente Alfa de Cronbach, obteniéndose un valor de $\alpha = 0,92$, lo que evidencia una muy alta consistencia interna del cuestionario aplicado y respalda la fiabilidad de los datos recopilados para el estudio. A partir del análisis descriptivo realizado, los resultados permiten identificar con mayor precisión las brechas organizacionales y técnicas presentes en las PYMES tecnológicas de la ciudad de Loja.

Estos hallazgos evidencian diferencias en el nivel de madurez entre dimensiones, lo que aporta una visión estructurada del estado actual de la gestión de la ciberseguridad en el sector. Con base en la evidencia obtenida, se plantean orientaciones generales encaminadas al fortalecimiento progresivo de la resiliencia digital, sin que ello implique la implementación directa de acciones estratégicas dentro del presente estudio. El nivel de madurez en ciberseguridad se evaluó en cinco dimensiones organizacionales como recursos, gobernanza y responsabilidades, cultura organizacional, capacidades técnicas y políticas de seguridad. Por lo cual, cada factor se analizó por medio de dos preguntas y su valoración se realizó a través de la escala Likert de cinco puntos. Así mismo, con base a los datos obtenidos en la encuesta, se realizó un promedio de los ítems con cada dimensión por PyME y, a su vez, se estableció un índice de madurez global, calculado como el promedio de las cinco dimensiones.

Con el propósito de otorgar mayor precisión interpretativa al índice construido, se establecieron tres niveles de madurez en función de los valores obtenidos: bajo (1,0–2,0), correspondiente a prácticas incipientes y predominantemente reactivas; medio (2,1–3,0), asociado a procesos parcialmente definidos y en desarrollo; y avanzado (>3,0), caracterizado por una gestión formalizada y orientada a la mejora

continua. Esta clasificación mantiene coherencia con la lógica de niveles utilizada en modelos de madurez en ciberseguridad, donde el avance organizacional se entiende como un proceso progresivo.

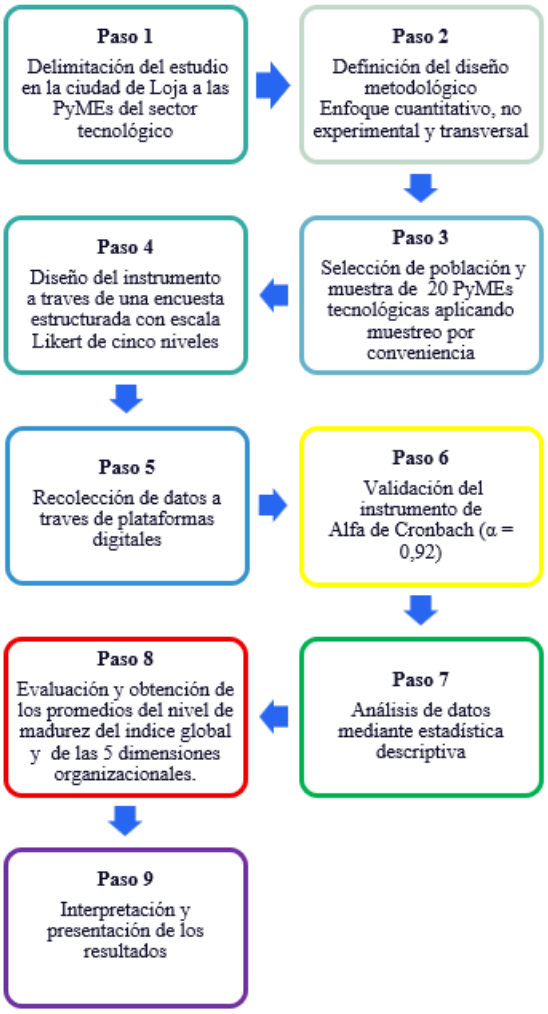

Figura 1. *Diagrama de proceso metodológico de la investigación*

Fuente: Elaboración propia

Resultados y Discusión

Investigaciones previas desarrolladas en contextos empresariales similares han identificado patrones comparables en la gestión de la ciberseguridad en PYMES ecuatorianas. En particular, el estudio realizado por (Zuñiga et al., 2020) en la ciudad de Quevedo, con una muestra de 30 PYMES, evidenció que solo una proporción reducida de empresas había formalizado mecanismos y políticas de seguridad, mientras que el 43 % del personal desconocía su cumplimiento. Asimismo, más del 50 % de las organizaciones disponía de infraestructura tecnológica básica sin respaldo normativo en la gestión de la información. Bajo este referente empírico, los resultados que se presentan a continuación permiten contrastar dicha realidad con la situación de las PyMEs tecnológicas de ciudad de Loja, a partir del análisis descriptivo del nivel de madurez en ciberseguridad. El presente estudio tuvo como objetivo evaluar el nivel de madurez en ciberseguridad de las PyMEs tecnológicas de Loja mediante el análisis de los datos obtenidos a través de una encuesta aplicada a las organizaciones participantes. La Tabla 1 presenta los estadísticos descriptivos del nivel de madurez global.

Tabla 1 *Estadísticos descriptivos del nivel de madurez global en ciberseguridad de las PyMEs Tecnológicas*

Estadístico	Valor
Media	2,65
Mediana	2,75
Desviación estándar	1,00
Mínimo	1,00
Máximo	4,90

Fuente: Elaboración propia.

Los resultados muestran que el nivel de madurez global en ciberseguridad se sitúa en un rango medio. La media obtenida (2,65) evidencia la presencia de prácticas de ciberseguridad parcialmente definidas y en desarrollo dentro de las organizaciones evaluadas. La mediana (2,75) confirma un comportamiento cercano al promedio, mientras que la desviación estándar (1,00) indica una heterogeneidad relevante entre las PyMEs analizadas. Los valores mínimos (1,00) y

máximo (4,90) revelan la coexistencia de empresas con niveles críticamente bajos junto a otras con avances parciales. En términos estructurales, el promedio global de 2,65 indica que la mayoría de las PyMEs evaluadas se sitúan en un nivel medio de madurez, con procesos parcialmente definidos y en desarrollo. Si bien cuentan con controles técnicos, estos aún no se integran de manera consistente dentro de una gobernanza formal ni se respaldan mediante políticas claramente institucionalizadas. En consecuencia, la gestión de la ciberseguridad se mantiene en una fase de consolidación, con predominio de acciones correctivas sobre estrategias preventivas sistemáticas.

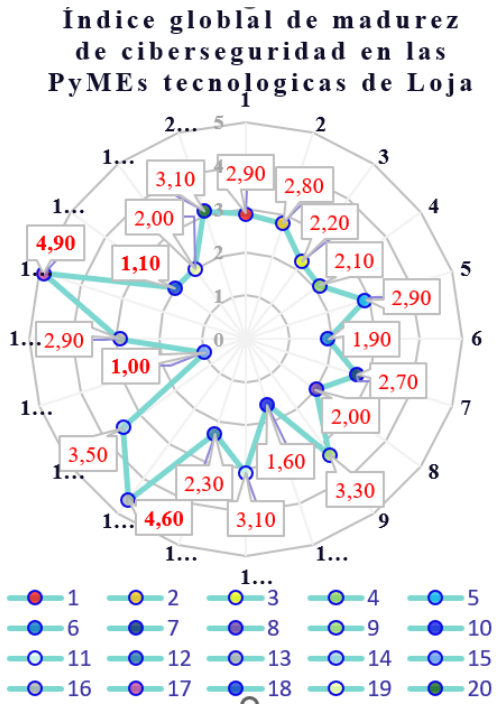

Figura 2. *Índice global de madurez de ciberseguridad en las PYMES tecnológicas de Loja*

Fuente: Elaboración propia

La Figura 2 presenta la distribución del índice de madurez global por empresa. Se observa que la mayoría de las organizaciones se concentra en niveles bajos y medios, con puntuaciones entre 2,00 y 3,10. Algunas PyMEs alcanzan valores superiores cercanos a 4,60 y 4,90, mientras que los valores más bajos, alrededor de 1,00 y 1,10, reflejan escenarios de alta vulnerabilidad. En conjunto, la dispersión observada confirma diferencias significativas en el nivel de madurez del sector. Por su parte, la Figura 3 y la Tabla 2 muestran el nivel promedio de madurez de las dimensiones organizacionales evaluadas. Las capacidades técnicas y la gobernanza presentan los valores más altos, con promedios cercanos a 2,80, aunque permanecen en niveles intermedios. En contraste, la cultura organizacional y las políticas de seguridad registran los valores más bajos, alrededor de 2,50, mientras que la dimensión de recursos con 2,60.

Figura 3. *Nivel de madurez de las dimensiones organizacionales de las Pymes Tecnológicas de Loja*

Fuente: Elaboración propia

Adicionalmente, la dispersión observada en todas las dimensiones evidencia diferencias relevantes entre las PYMES, reflejando la coexistencia de prácticas incipientes y otras más estructuradas dentro de cada factor analizado.

Tabla 2. *Estadísticos descriptivos del nivel de madurez en ciberseguridad de las dimensiones organizacionales de las PyMEs Tecnológicas*

Estadístico	Cultura	Gobernanza	Recursos	Técnica	Políticas
Media	2,55	2,78	2,58	2,78	2,55
Mediana	2,00	3,00	3,00	3,00	2,00
Desviación Estándar	1,38	1,25	1,33	1,33	1,28
Mínimo	1,00	1,00	1,00	1,00	1,00
Máximo	5,00	5,00	5,00	5,00	5,00

Fuente: Elaboración propia

En conjunto, los resultados evidencian que el nivel medio de madurez en ciberseguridad, observado en las PyMEs tecnológicas de Loja se desarrolla en un contexto donde la adopción tecnológica no ha estado acompañada por una consolidación equivalente de estructuras organizacionales y normativas. Aunque se identifican avances en el ámbito técnico, estos no se articulan de manera sistemática con políticas formalizadas, una asignación clara de responsabilidades ni con una cultura organizacional orientada a la gestión del riesgo. En este escenario, la ciberseguridad tiende a gestionarse de manera predominantemente reactiva, lo que explica la variabilidad observada entre organizaciones y la persistencia de brechas en dimensiones como la cultura y las políticas de seguridad. El análisis comparativo entre dimensiones permite observar que las empresas con mayores puntajes en gobernanza y responsabilidades suelen presentar niveles superiores en el índice global de madurez.

En contraste, los valores más bajos registrados en cultura organizacional y políticas de seguridad evidencian que estos factores actúan como limitantes estructurales del desarrollo integral de la ciberseguridad. Este comportamiento sugiere que el fortalecimiento técnico, aunque necesario, no garantiza por sí solo una madurez organizacional equivalente, sino que requiere articulación coherente con componentes normativos, culturales y de gestión interna. Los resultados confirman que las PYMES tecnológicas de la ciudad de Loja presentan un nivel medio de madurez en ciberseguridad. El promedio global de 2,65 sobre 5 refleja que, si bien existen prácticas básicas de protección, estas aún no se integran plenamente en una gestión formal y estructurada del riesgo. Este hallazgo amplía la evidencia disponible en el contexto ecuatoriano, ya que demuestra que la madurez en ciberseguridad no depende únicamente de la infraestructura tecnológica, sino también de la capacidad organizacional para definir políticas, asignar responsabilidades y consolidar procesos de seguridad de forma coherente. El mayor puntaje en la dimensión técnica (≈ 2,78) sugiere que las empresas han priorizado la implementación de controles operativos para proteger su infraestructura digital.

No obstante, los valores más bajos en cultura organizacional y políticas de seguridad (≈ 2,55) evidencian que dichos controles carecen de lineamientos formales y de una estructura interna que garantice su sostenibilidad. En consecuencia, la seguridad se gestiona de manera predominantemente reactiva, como respuesta a incidentes, y no como parte de una estrategia preventiva consolidada. Este comportamiento evidencia que la incorporación de herramientas tecnológicas, aunque necesaria,

resulta insuficiente si no se integra dentro de una estructura organizacional que defina responsabilidades, formalice procesos y gestione el riesgo de manera sistemática. La brecha identificada responde a factores estructurales propios del entorno organizacional de las PyMEs locales. La limitada disponibilidad de recursos, la escasez de personal especializado y la prioridad otorgada a objetivos operativos inmediatos dificultan la adopción integral de marcos como ISO/IEC 27001 o el NIST Cybersecurity Framework.

Asimismo, aunque Ecuador cuenta con un marco regulatorio en materia de protección de datos y seguridad digital, su existencia no garantiza por sí sola un mayor nivel de madurez si no se aplica de manera efectiva dentro de cada organización. En este contexto, resulta pertinente promover enfoques de madurez progresiva, como el Cybersecurity Capability Maturity Model (C2M2), que permiten estructurar mejoras continuas acordes con las capacidades reales de las PyMEs y avanzar gradualmente hacia niveles superiores de gestión. Estos resultados guardan coherencia con investigaciones desarrolladas en PyMEs latinoamericanas, donde se ha evidenciado que el crecimiento en la adopción tecnológica no siempre se acompaña de una consolidación organizacional equivalente en materia de ciberseguridad.

Estudios realizados en Ecuador y en otros países de la región describen escenarios similares, caracterizados por avances operativos en infraestructura digital, pero con debilidades en gobernanza, formalización de políticas y cultura de seguridad. Esta coincidencia permite interpretar que la situación identificada en las PYMES tecnológicas de Loja no constituye un caso aislado, sino que responde a una tendencia regional asociada a limitaciones estructurales y a procesos de madurez aún en desarrollo. La variabilidad observada entre empresas, reflejada en una desviación estándar de 1,00, confirma que el nivel de madurez está estrechamente vinculado a decisiones internas relacionadas con la gobernanza y la formalización de procesos. Esto evidencia que el avance en ciberseguridad requiere coherencia entre tecnología, organización y responsabilidad institucional, y no únicamente inversión en infraestructura digital.

Desde una perspectiva práctica, los resultados sugieren que las PyMEs tecnológicas deberían enfocarse en la formalización progresiva de políticas de seguridad, la definición clara de roles y responsabilidades, y la realización periódica de análisis de riesgos. La adopción gradual de estándares internacionales puede servir como guía para fortalecer la estructura interna sin necesidad de asumir procesos de certificación inmediatos. De igual forma, las entidades de control y los organismos de apoyo empresarial pueden desempeñar un papel clave mediante programas de capacitación y acompañamiento técnico adaptados a la realidad del sector.

En síntesis, el principal desafío identificado no radica en la disponibilidad de herramientas tecnológicas, sino en la limitada articulación organizacional que impide gestionar la seguridad de manera integral y sostenida. La evidencia obtenida permite interpretar la madurez en ciberseguridad como un proceso progresivo que exige coherencia estructural entre gobernanza, cultura organizacional, gestión sistemática del riesgo y cumplimiento normativo, elementos que constituyen la base para el fortalecimiento sostenible de la resiliencia digital empresarial. Aunque el análisis ofrece una visión diagnóstica clara sobre el nivel de madurez en ciberseguridad de

las PYMES tecnológicas de Loja y evidencia una brecha entre capacidades técnicas y estructura organizacional, futuras investigaciones podrían profundizar en la aplicación efectiva del marco regulatorio ecuatoriano y de las buenas prácticas de ciberseguridad, tanto en la región como a nivel nacional. Evaluar estos procesos en un período determinado permitiría analizar la evolución de la madurez organizacional y el impacto concreto de articular la normativa nacional con estándares internacionales. Este enfoque contribuiría a determinar en qué medida una aplicación estructurada y sostenida en el tiempo fortalece realmente la resiliencia digital empresarial en el contexto de las pequeñas y medianas empresas tecnológicas.

Conclusiones

La presente investigación permitió evaluar de manera sistemática el nivel de madurez en ciberseguridad de las PyMEs tecnológicas de la ciudad de Loja, evidenciando que, en términos generales, estas organizaciones se sitúan en un nivel medio de madurez en ciberseguridad. Este hallazgo se sustenta en un índice global promedio de 2,65 sobre 5, con valores que oscilan entre 1,0 y 4,9, lo que pone de manifiesto la existencia de brechas estructurales que reflejan limitaciones en la capacidad institucional para gestionar de forma integral los riesgos asociados a la transformación digital. En este contexto, dichas condiciones se observan en un escenario donde la resiliencia digital y la continuidad operativa aún requieren fortalecimiento progresivo.

El análisis por dimensiones mostró que, si bien las PyMEs presentan un mayor desarrollo relativo en capacidades técnicas básicas, este avance no se traduce en una gestión integral de la ciberseguridad. En particular, las capacidades técnicas alcanzaron el promedio más alto (≈ 2,78), mientras que componentes organizacionales clave, como la cultura organizacional y las políticas de seguridad, registraron los valores más bajos (≈ 2,55). Estos hallazgos evidencian que la ciberseguridad continúa abordándose de manera fragmentada y predominantemente reactiva, lo que incrementa la exposición a incidentes y dificulta la consolidación de prácticas sostenibles de seguridad de la información.

La principal contribución científica de este estudio radica en la construcción y aplicación de un índice integrado de madurez en ciberseguridad adaptado al contexto normativo ecuatoriano, que permite evaluar de manera simultánea dimensiones técnicas, organizacionales y regulatorias en PyMEs tecnológicas locales. A diferencia de enfoques centrados exclusivamente en la infraestructura tecnológica, la investigación demuestra empíricamente que la brecha identificada se explica principalmente por factores asociados a la gobernanza y la formalización interna de procesos.

De esta manera, el trabajo fortalece el análisis académico en el contexto ecuatoriano al vincular el marco regulatorio nacional con modelos internacionales de madurez, proporcionando una base metodológica y estratégica para el diseño de acciones progresivas orientadas al fortalecimiento sostenible de la resiliencia digital empresarial. Asimismo, las diferencias observadas entre los niveles de madurez evidencian una marcada heterogeneidad en el sector tecnológico local, reflejada en una desviación estándar de 1,00. Este comportamiento confirma la coexistencia de PyMEs con niveles críticamente bajos junto a otras con avances parciales, lo que refuerza la necesidad de adoptar enfoques progresivos y flexibles ajustados a la realidad operativa de

cada organización y a sus limitaciones económicas, técnicas y organizativas. Desde la perspectiva normativa, los niveles de madurez identificados representan un desafío frente a las exigencias del marco regulatorio ecuatoriano y a los lineamientos promovidos por estándares internacionales como ISO/IEC 27001, el NIST Cybersecurity Framework y COBIT. El hecho de que todas las dimensiones evaluadas presenten valores promedio inferiores a 3, en una escala de 5, evidencia que una proporción significativa de las PyMEs aún no cuenta con medidas técnicas y organizativas consolidadas, lo que incrementa los riesgos operativos y legales asociados a una gestión insuficiente de la seguridad de la información.

El fortalecimiento de la resiliencia digital en las PyMEs tecnológicas de la ciudad de Loja requiere avanzar hacia una gestión integral de la ciberseguridad que articule de manera coherente las capacidades técnicas con los componentes organizacionales, culturales y normativos. En este sentido, la identificación de brechas y la evaluación del nivel de madurez constituyen un punto de partida estratégico para el diseño de acciones progresivas, alineadas con modelos como el Cybersecurity Capability Maturity Model (C2M2) y coherentes con el marco legal vigente, contribuyendo a una transformación digital segura, responsable y sostenible.

Referencias Bibliográficas

Aguilar, J. (2021). Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior. Estudios Internacionales, 169–197. https://doi.org/10.5354/0719-3769.2021.57067

Armijos, V., Espinoza, M., & Rodríguez, G. (2024). Nivel de madurez digital en micro, pequeñas y medianas empresas del sur de Ecuador: Estrategias para el fortalecimiento. Memorias de la Conferencia Iberoamericana de Complejidad, Informática y Cibernética, 269–275. https://doi.org/10.54808/CICIC2024.01.269

Asamblea Nacional del Ecuador. (2014). Código Orgánico Integral Penal. Registro Oficial Suplemento No. 180.

Asamblea Nacional del Ecuador. (2015). Ley orgánica de telecomunicaciones. Registro Oficial Suplemento No. 439.

Asamblea Nacional del Ecuador. (2021). Ley orgánica de protección de datos personales. Registro Oficial Suplemento No. 459.

Bustillos, O., & Rojas, J. (2022). Protocolo básico de ciberseguridad para pymes. Interfases, (16), 168–186. https://doi.org/10.26439/interfases2022.n016.6021

Choez, C., & Mora, A. (2025). La ciberseguridad como prioridad empresarial dentro de marcos regulatorios y normativos internacionales. Revista Científica Ciencia y Método, 3. https://doi.org/10.55813/gaea/rcym/v3/n3/38

Congreso Nacional del Ecuador. (2002). Ley de comercio electrónico, firmas electrónicas y mensajes de datos. Registro Oficial Suplemento No. 557.

European Union Agency for Cybersecurity. (2021). Cybersecurity for SMEs: Challenges and recommendations. https://doi.org/10.2824/770352

Instituto Nacional de Estadística y Censos. (2024). Registro Estadístico de Empresas (REEM). https://app.powerbi.com/view?r=eyJrIjoiYmVjNTZkYWMtMjBmMC00YzJkLWE1ZTctNjFjMTk3Y2VhZDQ5IiwidCI6ImYxNThhMmU4LWNhZWMtNDQwNi1iMGFiLWY1ZTI1OWJkYTExMiJ9

International Organization for Standardization & International Electrotechnical Commission. (2022). ISO/IEC 27001: Information security management systems — Requirements. https://www.iso.org/standard/82875.html

ISACA. (2019). COBIT 2019 framework: Introduction and methodology. https://www.isaca.org/resources/cobit

León, E., Tesillo, C., Escobar, Y., & Godoy, L. (2022). Revisión de los avances y cambios en ciberseguridad en el Perú, para una transformación digital. Revista Innovación y Software. https://doi.org/10.48168/innosoft.s9.a62

López, K., & Ordóñez, Y. (2024). Auditoría y ciberseguridad en el sector comercial: evaluación de resiliencia ante amenazas digitales. Revista Multidisciplinaria de Investigación, 4, 14–27. https://doi.org/10.62574/rmpi.v4iespecial.154

Luján, L., Centurión, M., Maciel, M., Gheringhelli, L., & Mareco, G. (2023). Transformación digital de las PYMES en Paraguay: retos y oportunidades. Ciencia Latina Revista Científica Multidisciplinar, 7(5), 8294–8309. https://doi.org/10.37811/cl_rcm.v7i5.8411

Maldonado, V. (2022). El rol del talento humano en la transformación digital de las empresas ecuatorianas. Revista Científica Zambos, 1(2), 34–50. https://doi.org/10.69484/rcz/v1/n2/26

Porrúa, M. (2025). Digital transformation and cybersecurity in Latin America and the Caribbean. http://dx.doi.org/10.18235/0013872

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2024). Esquema Gubernamental de Seguridad de la Información (EGSI). Registro Oficial No. 509.

National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity. http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Orellana, F. (2020). Cybersecurity incident response capabilities in the Ecuadorian small business sector [Tesis]. https://www.proquest.com/openview/05929b02aa9fe10cbad74c6880aaa513

Peralta, M., & Aguilar, D. (2021). La ciberseguridad y su concepción en las PYMES de Cuenca, Ecuador. http://ojs.econ.uba.ar/index.php/Contyaudit/article/view/2061/2797

Pozo, L. (2022). Ciberseguridad y ciberdefensa como ejes estratégicos de la seguridad nacional en el Ecuador [Tesis]. http://repositorio.iaen.edu.ec/handle/24000/6103

Presidencia de la República del Ecuador. (2023). Reglamento a la Ley orgánica de protección de datos personales. Registro Oficial No. 435.

Ramos, F. (2023). Seguridad cibernética en empresas ecuatorianas: prácticas y retos actuales. Revista Científica Zambos, 2(3), 16–28. https://doi.org/10.69484/rcz/v2/n3/47

U.S. Department of Energy. (2022). Cybersecurity capability maturity model (C2M2). https://www.energy.gov/sites/default/files/2022-06/C2M2%20Version%202.1.pdf

Vasco, J., Ruiz, G., Macas, B., & León, V. (2025). Ciberseguridad y protección de datos personales: desafíos y perspectivas. GADE: Revista Científica, 5(1), 675–688. https://doi.org/10.63549/rg.v5i1.642

Vera, J. (2020). Sistema digital y la gestión turística hotelera en la ciudad de Quevedo [Proyecto de investigación]. http://dspace.utb.edu.ec/handle/49000/7925

Villarreal, G. (2024). Transformación de las PYMES ecuatorianas a través de la educación tecnológica. Sapiens International Multidisciplinary Journal, 1(3), 185–197. https://doi.org/10.71068/7t08j334

Zambrano, A., Meza, Y., Villavicencio, C., & Rodríguez, A. (2024). Ciberataques en América Latina: desafíos de la era digital. Revista Compromiso Social. https://doi.org/10.5377/recoso.v1i13.19295

Zuñiga, A., Serrano, I., & Molina, L. (2020). Seguridad informática en las PyMES de la ciudad de Quevedo. Journal of Business and Entrepreneurial Studies, 4, 232–241. https://doi.org/10.37956/jbes.v4i2.97

Declaraciones éticas y editoriales del artículo
Contribución de los autores (Taxonomía CRediT) Freddy David Espinoza Quezada: conceptualización de la investigación, diseño metodológico, desarrollo del proceso investigativo, análisis formal de los datos, redacción del borrador original del manuscrito, revisión crítica del contenido científico y supervisión general del estudio. Iván Daniel Quirumba Yagual: curación y organización de los datos, participación en la recolección de información, validación de los resultados obtenidos y elaboración de representaciones gráficas y visualización de los datos.
Declaración de conflicto de intereses Los autores declaran que no existe conflicto de intereses en relación con la investigación presentada, la autoría del manuscrito ni la publicación del presente artículo.
Declaración de financiamiento La presente investigación no recibió financiamiento específico de agencias públicas, comerciales o de organizaciones sin fines de lucro. En caso de existir financiamiento institucional o externo, este deberá ser declarado explícitamente por los autores en esta sección.
Declaración del editor El editor responsable certifica que el proceso editorial del presente artículo se desarrolló conforme a los principios de integridad científica, transparencia y buenas prácticas editoriales. El manuscrito fue sometido a un proceso de evaluación mediante revisión por pares doble ciego, garantizando la confidencialidad de la identidad de los autores y revisores durante todo el proceso de dictamen académico. Asimismo, el editor declara que el artículo cumple con los criterios científicos, metodológicos y éticos establecidos por la revista.
Declaración de los revisores Los revisores externos que participaron en la evaluación del presente manuscrito declaran haber realizado el proceso de revisión de manera objetiva, independiente y confidencial. Asimismo, manifiestan que no mantienen conflictos de interés con los autores ni con la investigación evaluada, y que sus observaciones y recomendaciones se fundamentan exclusivamente en criterios científicos, metodológicos y académicos.
Declaración ética de la investigación Los autores declaran que la investigación se desarrolló respetando los principios éticos de la investigación científica, garantizando la confidencialidad de los datos y el respeto a los participantes del estudio. En los casos en que la investigación involucre seres humanos, los procedimientos deben ajustarse a los principios éticos establecidos en la Declaración de Helsinki y a las normativas institucionales correspondientes.
Declaración sobre el uso de inteligencia artificial Los autores declaran que el uso de herramientas de inteligencia artificial, en caso de haberse utilizado durante el proceso de investigación o redacción del manuscrito, se realizó únicamente como apoyo técnico para mejorar la claridad del lenguaje o el análisis de información, manteniendo siempre la responsabilidad intelectual sobre el contenido del artículo. Las herramientas de inteligencia artificial no fueron utilizadas como autoras del manuscrito ni sustituyen la responsabilidad académica de los investigadores.
Disponibilidad de datos Los datos que respaldan los resultados de esta investigación estarán disponibles previa solicitud razonable al autor de correspondencia, respetando las normas éticas y de confidencialidad establecidas por la investigación.