

UNIVERSIDAD CATÓLICA DE CUENCA

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

DIRECCIÓN DE POSGRADOS

Maestría en Contabilidad y Auditoría con mención en Gestión Tributaria

Ciberseguridad y protección de datos contables

INFORME DE INVESTIGACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE MAGISTER EN CONTABILIDAD Y AUDITORÍA MENCIÓN EN GESTIÓN TRIBUTARIA

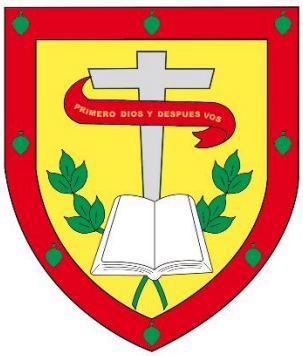
AUTOR: JAVIER JACINTO VÉLIZ NAPA

DIRECTOR: PhD. JUAN DIEGO OCHOA CRESPO

CUENCA - ECUADOR

2026

DIOS, PATRIA, CULTURA Y DESARROLLO



UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE POSGRADOS

Maestría en Contabilidad y Auditoría con mención en Gestión Tributaria

Ciberseguridad y protección de datos contables

INFORME DE INVESTIGACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE MAGISTER EN CONTABILIDAD Y AUDITORÍA MENCIÓN EN GESTIÓN TRIBUTARIA

AUTOR: JAVIER JACINTO VÉLIZ NAPA

DIRECTOR: PhD. JUAN DIEGO OCHOA CRESPO

MANTA - ECUADOR

2026

DIOS, PATRIA, CULTURA Y DESARROLLO

Certificado del Asesor

Se certifica que:

El informe de investigación " Ciberseguridad y protección de datos contables", de autoría del Sr. Javier Jacinto Véliz Napa con número de identidad 1306304542, con nacionalidad ecuatoriana, previo a la obtención del Título de Cuarto Nivel o Posgrado correspondiente a Magíster en Contabilidad y Auditoría Mención en Gestión Tributaria, cumple con la caracterización y estructura (parte protocolaria y parte expositiva) y se sujeta a la normativa pertinente exigida por el Consejo de Educación Superior, CES y la Universidad Católica de Cuenca, en consecuencia se autoriza su presentación para los trámites pertinentes.

Santa Ana de los Ríos de Cuenca

Septiembre de 2026

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
JUAN DIEGO OCHOA CRESPO

Asesor Científico

PhD. Juan Diego Ochoa Crespo

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
JUAN DIEGO OCHOA CRESPO

Asesor Metodológico

PhD. Juan Diego Ochoa Crespo

Declaratoria de Autoría y Responsabilidad

Javier Jacinto Véliz Napa portador(a) de la cédula de ciudadanía Nº **1306304542**. Declaro ser el autor de la obra: "**Ciberseguridad y protección de datos contables"**, sobre la cual me hago responsable sobre las opiniones, versiones e ideas expresadas. Declaro que la misma ha sido elaborada respetando los derechos de propiedad intelectual de terceros y eximo a la Universidad Católica de Cuenca sobre cualquier reclamación que pudiera existir al respecto. Declaro finalmente que mi obra ha sido realizada cumpliendo con todos los requisitos legales, éticos y bioéticos de investigación, que la misma no incumple con la normativa nacional e internacional en el área específica de investigación, sobre la que también me responsabilizo y eximo a la Universidad Católica de Cuenca de toda reclamación al respecto.

Cuenca, **30 de septiembre de 2026**



Validar únicamente en FirmaEC.
Firmado electrónicamente por:
JAVIER JACINTO VELIZ NAPA

F: ……..

Javier Jacinto Véliz Napa

C.I. **1306304542**

Agradecimiento

Agradezco a Dios, por ser la fuente inagotable de fortaleza, sabiduría y fidelidad que renovó mis fuerzas cada día durante este proceso, permitiéndome culminar con éxito esta etapa académica en mi formación profesional.

A mi familia, por su apoyo incondicional, paciencia y palabras de aliento en cada momento de esfuerzo y dedicación, especialmente a mi esposa.

A mis profesores, por compartir sus conocimientos y experiencia a lo largo de la maestría, aportando las herramientas académicas que hicieron posible el desarrollo de esta investigación.

De igual manera agradezco, a mi tutor el Dr. Juan Diego Ochoa, por su guía, disposición y acompañamiento constante durante todo el proceso investigativo, cuyas orientaciones fueron fundamentales para la culminación de esta investigación.

Dedicatoria

A Dios, por ser la fuente de sabiduría y fortaleza que sostuvo cada paso de este proceso, permitiéndome culminar esta etapa con perseverancia y claridad.

"Y si alguno de vosotros tiene falta de sabiduría, pídala a Dios, el cual da a todos abundantemente y sin reproche, y le será dada."

Santiago 1:5

A mi esposa María, por el apoyo incondicional, paciencia y aliento constante durante los momentos de mayor exigencia, siendo el motor que impulsó cada esfuerzo dedicado a esta investigación.

A mi familia y colegas, por acompañarme y creer en la culminación de esta meta académica.

Resumen

La digitalización de las operaciones financieras ha incrementado la susceptibilidad de los registros contables ante vulnerabilidades virtuales, poniendo en riesgo los pilares fundamentales de reserva, exactitud y acceso en los entornos económicos regionales; esta investigación buscó establecer la relación entre las prácticas de ciberseguridad y la protección y fiabilidad de la información contable en empresas comercializadoras de insumos médicos en la provincia de Manabí. Se empleó un diseño cuantitativo correlacional, no experimental y de corte transversal; la recolección de datos se efectuó mediante un cuestionario estructurado aplicado a una muestra de 54 profesionales de las áreas contable y financiera.

El procesamiento mediante estadística paramétrica mostró que la ciberseguridad alcanzó un nivel de madurez moderado (media = 3,009), mientras que la información contable obtuvo una valoración mayor (media = 3,795). El análisis inferencial indicó una correlación positiva de magnitud moderada y significativa ($r = 0,421$; $p = 0,002$), lo cual permitió respaldar la hipótesis planteada. Estos hallazgos sugieren que, si bien existe una alta confianza percibida en los reportes financieros, esta se sustenta sobre una infraestructura digital con brechas de protección que podrían vulnerar la cadena de custodia de los datos. Se concluye que la ciberseguridad se configura como un pilar fundamental del entorno de control interno, siendo indispensable la integración de salvaguardas tecnológicas y organizativas para garantizar que la información contable sea un reflejo fiel, íntegro y verificable de la realidad económica institucional.

Palabras clave: Ciberseguridad, información contable, control interno digital, correlación de Pearson, integridad de datos.

Abstract

The digitalization of financial operations has increased the susceptibility of accounting records to virtual vulnerabilities, jeopardizing the fundamental pillars of confidentiality, accuracy, and accessibility within regional economic environments. This study aimed to establish the relationship between cybersecurity practices and the protection and reliability of accounting information in companies distributing medical supplies in the province of Manabí. A quantitative, non-experimental, cross-sectional correlational design was employed; data collection was carried out using a structured questionnaire administered to a sample of 54 professionals in the accounting and financial fields.

Parametric statistical analysis revealed that cybersecurity reached a moderate level of maturity (mean = 3.009), whereas accounting information received a higher rating (mean = 3.795). Inferential analysis indicated a significant, moderate positive correlation ($r = 0.421$; $p = 0.002$), thereby supporting the proposed hypothesis. These findings suggest that, although there is a high level of perceived confidence in financial reports, this confidence rests on a digital infrastructure with security gaps that could compromise the data chain of custody. It is concluded that cybersecurity constitutes a fundamental pillar of the internal control environment; the integration of technological and organizational safeguards is essential to ensure that accounting information serves as a faithful, integral, and verifiable reflection of the institution's economic reality.

Keywords: Cybersecurity, accounting information, digital internal control, Pearson correlation, data integrity.

Índice de Contenido

Certificado del Asesor ii
Declaratoria de Autoría y Responsabilidad iii
Agradecimiento iv
Dedicatoria v
Resumen vi
Abstract vii
Índice de Contenido viii
Índice de tablas xi
Índice de figuras xii
Capítulo I. Introducción 1
Antecedentes y contextualización 1
Planteamiento del problema 3
Formulación del problema 5
Justificación 6
Objetivos 7
Objetivo General 7
Objetivos Específicos 7
Hipótesis 7
Hipótesis general 8
Hipótesis específicas 8
Capítulo II. Marco Teórico 9
Antecedentes de la investigación 9
Bases teóricas 13
Teoría de la tríada de la seguridad (CIA) 13
Teoría de sistemas de información contable (SIC) 14
Modelo de gobernanza de ciberseguridad (NIST 2.0) 15
Enfoque de resiliencia organizacional y continuidad 16
Marco conceptual 17
Ciberseguridad 17
Protección de datos contables 17
Información contable 18

Sistema de información contable 18
Confidencialidad 19
Integridad de la información 19
Exactitud de los registros contables 20
Disponibilidad de la información 20
Gobernanza y políticas de seguridad 21
Gestión de activos y accesos 21
Autenticación multifactor 22
Seguridad de la infraestructura tecnológica 22
Cifrado de datos 23
Cultura organizacional de ciberseguridad 23
Phishing 24
Resiliencia operativa 24
Plan de continuidad del negocio 25
Recuperación ante desastres 26
Copias de seguridad o respaldos 26
Confiabilidad de los reportes contables 27
Cumplimiento normativo contable y tributario 27
Marco legal 28
Constitución de la República del Ecuador 28
Ley Orgánica de Protección de Datos Personales 29
Código Orgánico Integral Penal 29
Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos 30
Normativa contable y tributaria aplicable 31
Política Pública para la Transformación Digital 31
Desarrollo de hipótesis específicas 32
Capítulo III. Marco metodológico 36
Enfoque y tipo de investigación 36
Diseño de la investigación 36
Población y Muestra 36
Técnicas e instrumentos 37
Validez y confiabilidad 38
Procedimiento 40

Consideraciones éticas 40
Método de análisis de datos 40
Capítulo IV. Resultados y discusión 42
Presentación de resultados 42
Análisis de normalidad 43
Análisis e interpretación 44
Discusión 45
Capítulo V. Conclusiones, recomendaciones y propuesta 50
Conclusiones 50
Recomendaciones 53
Propuesta 54
Plan de fortalecimiento de controles digitales para la protección de registros contables en empresas comercializadoras de insumos médicos de la provincia de Manabí 54
Referencias Bibliográficas 60
Anexos 65
Anexo 1: Matriz de Operacionalización 65
Anexo 2: Encuesta 70

Índice de tablas

Tabla 1. V de Aiken por criterio 39

Tabla 2. Estadísticos descriptivos de los constructos 42

Tabla 3. Prueba de normalidad de Kolmogorov-Smirnov (Lilliefors)..... 44

Tabla 4. Tabla de Correlación de Pearson..... 45

Índice de figuras

Figura 1. Modelo teórico 35

Figura 2. Histograma de la distribución del constructo ciberseguridad 42

Figura 3. Histograma de distribución del constructo información contable 43

Figura 4. Diagrama de dispersión entre ciberseguridad e información contable 45

Capítulo I. Introducción

Antecedentes y contextualización

De acuerdo con el World Economic Forum (2025), la seguridad de la información financiera atraviesa una transformación asociada con la creciente complejidad de las amenazas cibernéticas, las tensiones geopolíticas y el perfeccionamiento de las modalidades empleadas por el crimen organizado digital; mientras las corporaciones de mayor tamaño consolidan mecanismos de defensa más robustos, las organizaciones con recursos limitados enfrentan una mayor exposición ante amenazas automatizadas lo cual amplía las diferencias en materia de resiliencia digital. A ello se suma el uso de inteligencia artificial generativa, tecnología que puede apoyar la detección de intrusiones y, a la vez, facilitar la ejecución de ataques difíciles de reconocer mediante mecanismos defensivos convencionales, lo que impone la necesidad de reestructurar los planes dirigidos a salvaguardar los pilares de reserva, exactitud y acceso permanente de los activos informativos que sustentan la gestión económica institucional.

El estudio desarrollado por Shchyrba et al. (2025) resaltan que en los continentes europeo y asiático la migración de los sistemas contables hacia servicios en la nube ha favorecido la eficiencia operativa, el acceso a la información y la integración de procesos financieros; pese a ello, también ha planteado exigencias jurídicas y técnicas relacionadas con la custodia de los datos, motivo por el cual marcos regulatorios como el Reglamento General de Protección de Datos de la Unión Europea (GDPR) han fortalecido las exigencias sobre transparencia, cifrado y autenticación multifactor en los servicios tecnológicos que procesan información sensible. No obstante, el aumento de las transacciones digitales ha ampliado la exposición de los registros financieros a riesgos como el fraude electrónico, la sustracción de credenciales y el acceso no autorizado, de manera que la adopción de estándares de seguridad se ha convertido en un factor estrechamente vinculado con la confianza depositada en los sistemas que respaldan las operaciones económicas y financieras de las organizaciones.

En América Latina, la expansión tecnológica de las organizaciones ha avanzado con mayor rapidez que el desarrollo de sus capacidades de defensa digital, situación que mantiene expuestos los datos financieros y contables ante diversas amenazas (Gutiérrez, 2025); en este escenario Ramírez et al. (2022) identifican limitaciones en la preparación

técnica y en la existencia de disposiciones que regulen la rendición de cuentas sobre ciberseguridad fuera del sistema financiero tradicional, a lo cual se agrega una producción académica aún limitada sobre la aplicación de la digitalización en los procesos contables, en contraste con la evidencia disponible en Europa y Asia (Gutiérrez, 2025), condición que dificulta la evaluación de las repercusiones financieras derivadas de los incidentes informáticos y limita la información disponible para los grupos de interés respecto de las medidas de protección aplicadas por las empresas (Ramírez et al., 2022).

En Ecuador, la ciberseguridad ha adquirido relevancia institucional ante el aumento de los delitos informáticos que afectan la privacidad y el patrimonio; Mancheno (2024) destacó en su investigación que durante 2023 y 2024 la Fiscalía General del Estado registró un aumento del 68 % en denuncias por acceso no consentido a sistemas y del 40 % en ataques dirigidos contra la integridad de datos financieros. Pese a que el Código Orgánico Integral Penal [COIP] (2014) contempla disposiciones aplicables a estas conductas, la evolución de las tácticas delictivas junto con las dificultades relacionadas con la obtención de evidencia digital pueden limitar la respuesta institucional (Mancheno, 2024), circunstancia que evidencia una disponibilidad limitada de personal especializado, tanto en entidades públicas como privadas, y refuerza la necesidad de fortalecer las capacidades preventivas destinadas a proteger los activos digitales vinculados con la gestión contable y financiera (López & Ordóñez, 2024).

Las pequeñas y medianas empresas ecuatorianas (PYMES) enfrentan desafíos particulares en la protección de datos, debido a que el 80 % de las empresas comerciales analizadas no realiza auditorías de seguridad cibernética con periodicidad definida (López & Ordóñez, 2024), mientras que los estudios efectuados en Cuenca y Guayaquil identificaron una preferencia por sistemas contables locales o de escritorio, atribuida a la percepción de mayor control sobre los registros financieros; esta modalidad pese a transmitir una sensación de seguridad, puede exponer a las organizaciones a ataques de *malware* cuando carecen de actualizaciones y prácticas de mantenimiento adecuadas (Guachún & Andrade, 2024). Las plataformas híbridas y en la nube facilitan el acceso a la información, aunque también enfrentan riesgos asociados con *phishing*, denegación de servicio (DDoS) y sustracción de credenciales, brecha reflejada en que el 66,7 % de las organizaciones examinadas destina menos de mil dólares al año a la seguridad

digital, situación que incrementa la exposición de los registros contables frente a amenazas cibernéticas en este grupo de empresas (Guachún & Andrade, 2024).

Planteamiento del problema

La transformación digital de los sistemas contables ha optimizado la gestión financiera, aunque también ha expuesto a las organizaciones a una creciente complejidad cibernética impulsada por el crimen organizado digital y las tensiones geopolíticas (World Economic Forum, 2025), este fenómeno adquiere mayor relevancia en América Latina, donde la expansión de las infraestructuras tecnológicas ha superado la capacidad de respuesta y la robustez de las salvaguardas digitales en las organizaciones (Ramírez et al., 2022). Según este análisis regional, la vulnerabilidad de los registros contables aumenta debido a que la ciberdefensa no ha evolucionado en la misma proporción que la digitalización de los procesos financieros, a esto se añade la carencia de normativas específicas que regulen la rendición de cuentas fuera del sector financiero tradicional, situación que incrementa la exposición de los registros contables y favorece la omisión de información relacionada con la eficacia de sus mecanismos de protección en los reportes anuales, tal escenario restringe la generación de confianza entre los grupos de interés y limita la valoración de las repercusiones económicas derivadas de posibles brechas de datos (Ramírez et al., 2022).

En Ecuador, las denuncias por acceso no consentido a sistemas registraron un incremento del 68 % y los ataques dirigidos contra la integridad de datos financieros crecieron un 40 % entre 2023 y 2024 (Mancheno, 2024), cifras que reflejan un incremento sostenido de las amenazas dirigidas a la información digital y plantean nuevos desafíos para la protección de los activos contables; aunque el COIP (2014) incorpora disposiciones aplicables a los delitos informáticos, la evolución permanente de las tácticas empleadas por los actores maliciosos, junto con las dificultades para obtener evidencia digital con validez probatoria (Recalde, 2025) restringen la operatividad de respuesta institucional en el entorno nacional.

La problemática se intensifica en las pequeñas y medianas empresas como consecuencia de la escasez de personal técnico especializado y de recursos destinados a la adopción de estándares como la ISO 27001 (Mancheno, 2024); brecha que sostiene una distancia entre la percepción del riesgo y la aplicación efectiva de medidas

preventivas, elevando la exposición de los activos contables frente a amenazas como *ransomware* y *phishing* e incorporando una cultura organizacional en la que la ciberseguridad todavía suele considerarse un gasto prescindible antes que una inversión estratégica, lo cual incrementa la probabilidad de sufrir violaciones de datos y afrontar sanciones regulatorias de elevada incidencia económica (Mancheno, 2024).

Específicamente, en el sector comercial, más del 80 % de los contadores reconoce la existencia de un riesgo real para la integridad de los datos financieros, percepción que contrasta con el nivel de inversión destinado a la protección digital, debido a que cerca de un tercio de las organizaciones asigna menos del 1 % de su presupuesto anual a este propósito (Calle & Andrade, 2024), al tiempo que una proporción considerable de empresas mantiene preferencia por sistemas contables locales de escritorio bajo la premisa de ejercer un mayor control sobre los registros financieros, decisión que incrementa la exposición al *malware* ante la ausencia de actualizaciones críticas (Guachún & Andrade, 2024); a ello se agrega que, aunque las soluciones basadas en la nube ofrecen mayor disponibilidad de la información, permanecen expuestas a ataques de denegación de servicio (DDoS) capaces de interrumpir la continuidad operativa, mientras la ausencia de evaluaciones periódicas en los departamentos financieros dificulta la identificación temprana de vulnerabilidades asociadas con el manejo de los registros contables (Calle & Andrade, 2024), esta realidad justifica el desarrollo de diagnósticos específicos en la provincia de Manabí con el propósito de determinar la eficacia de los protocolos de ciberseguridad aplicados por las empresas comercializadoras de insumos médicos.

Las consecuencias derivadas de una protección insuficiente trascienden la pérdida técnica de datos al propiciar alteraciones fraudulentas capaces de comprometer la confiabilidad de la información contable empresarial y de generar sanciones previstas en la Ley Orgánica de Protección de Datos Personales [LOPDP] (2021), junto con afectaciones a la reputación corporativa de las organizaciones (Mancheno, 2024), a lo cual se agrega la ausencia de planes de respuesta frente a incidentes actualizados, condición que restringe la capacidad institucional para afrontar brechas de seguridad (Calle & Andrade, 2024); en las empresas comercializadoras de insumos médicos de la provincia de Manabí, la integridad de los datos patrimoniales se posiciona como un pilar crítico para la fundamentación de las resoluciones financieras, razón por la cual cualquier afectación a su confiabilidad compromete la estabilidad operativa y

económica de las organizaciones, circunstancia que otorga pertinencia a esta indagación científica, orientada a aportar evidencia empírica que fortalezca la resiliencia organizacional y la transparencia tributaria y financiera.

Formulación del problema

La migración hacia ecosistemas transaccionales electrónicos ha elevado la criticidad de los sistemas de información contable, dejándolos vulnerables a la alteración maliciosa y a las intrusiones ilegales; esta realidad obliga a intensificar las salvaguardas destinadas a sostener la exactitud, el acceso y la veracidad de los balances financieros; en el ámbito nacional, datos procesados por Mancheno (2024) exponen una subida del 68 % en las denuncias por vulneraciones de sistemas, fenómeno que denota una fragilidad constante en el resguardo de activos informativos. Esta situación se agrava debido a que un segmento importante de organizaciones comerciales asigna menos del 1 % de su presupuesto operativo a la ciberdefensa, lo que restringe su solvencia ante ataques automatizados (Calle & Andrade, 2024). Asimismo, la inclinación por arquitecturas contables locales carentes de parches críticos amplifica la susceptibilidad ante el código malicioso (Guachún & Andrade, 2024). A este panorama se suma el vacío normativo sobre la obligatoriedad de reportar la efectividad de los controles digitales, lo que otorga relevancia al examen del nexo entre las estrategias de seguridad y la custodia de los datos patrimoniales dentro de entidades que fundamentan su operatividad en la certidumbre de su información contable.

A partir de las limitaciones técnicas y organizacionales identificadas, sumadas a la relevancia que posee la información contable para la gestión empresarial y la toma de decisiones, la investigación se orienta a responder la siguiente interrogante: ¿Qué relación tienen las prácticas de ciberseguridad en la protección y confiabilidad de la información contable empresarial de las empresas comercializadoras de insumos médicos de la provincia de Manabí?, interrogante que orienta el análisis de la relación existente entre la aplicación de controles de seguridad digital y la protección de la información contable, con el propósito de generar evidencia empírica que contribuya a comprender el comportamiento de ambas variables en el sector objeto de estudio.

Justificación

Este estudio se fundamenta en la necesidad de ampliar el conocimiento sobre la relación entre la ciberseguridad y la información financiera en el ámbito empresarial, línea de investigación que mantiene un desarrollo incipiente en América Latina en contraste con la producción científica generada en Europa y Asia (Gutiérrez, 2025); desde esta perspectiva, el estudio aporta evidencia empírica sobre cómo las prácticas de seguridad digital contribuyen a proteger la información financiera, fortaleciendo los fundamentos de la auditoría informática y aportando elementos para interpretar la teoría de la agencia desde mecanismos de control vinculados con la reducción de la asimetría informativa entre la administración y los grupos de interés (Agudelo Quevedo, 2023; Shafa & Islam, 2025).

Desde un enfoque aplicado, este trabajo busca generar evidencia que permita a las empresas comercializadoras de insumos médicos de la provincia de Manabí disponer de un diagnóstico sustentado en información empírica acerca de las prácticas de ciberseguridad vinculadas con la protección de la información contable (Guachún & Andrade, 2024), aportando criterios que faciliten la identificación de vulnerabilidades asociadas con ataques de *malware*, *phishing* y accesos no autorizados (Calle & Andrade, 2024), junto con elementos que respalden la adopción de estándares internacionales de seguridad como la ISO 27001 los resultados podrán servir de apoyo para la formulación de estrategias institucionales orientadas a fortalecer la ciber resiliencia organizacional, reducir la exposición frente a incidentes informáticos y favorecer procesos de decisión sustentados en información contable confiable (Shafa & Islam, 2025).

La relevancia social del estudio radica en su contribución al fortalecimiento de la protección de la información financiera utilizada por organizaciones vinculadas con la comercialización de insumos médicos, actividad que demanda elevados niveles de confianza por parte de clientes, proveedores, organismos de control y demás grupos de interés; bajo esta premisa, la investigación respalda la consolidación de una cultura enfocada en la protección de la información, la transparencia tributaria y el uso responsable de la información financiera (Ramírez et al., 2022; Shafa & Islam, 2025), guardando correspondencia con las políticas públicas impulsadas en Ecuador para promover la modernización tecnológica del sector productivo (MINTEL, 2025),

aportando evidencia que pueda servir como insumo para nuevas investigaciones y proyectos institucionales encaminados a fortalecer la protección de la información contable en organizaciones expuestas a riesgos cibernéticos (López & Ordóñez, 2024; Mancheno, 2024).

Objetivos

Objetivo general

Determinar la relación entre las prácticas de ciberseguridad y la protección y confiabilidad de la información contable empresarial de las empresas comercializadoras de insumos médicos de la provincia de Manabí.

Objetivos específicos

1. Diagnosticar el estado actual de las medidas técnicas y organizativas de protección digital empleadas en los departamentos financieros de las empresas comercializadoras de insumos médicos para identificar vulnerabilidades asociadas con el manejo de la información contable.
2. Evaluar la relación entre los protocolos de seguridad digital y la integridad y disponibilidad de la información contable empresarial, con el propósito de establecer su asociación con los riesgos de alteración o pérdida de datos sensibles.
3. Correlacionar estadísticamente las dimensiones de la seguridad informática con los factores de protección de datos contables a fin de proponer lineamientos estratégicos que fortalezcan la resiliencia operativa y el cumplimiento normativo.

Hipótesis

Con base en el problema de investigación, los objetivos planteados y el sustento teórico desarrollado, se establecen la hipótesis general y las hipótesis específicas que orientan el análisis estadístico del estudio.

Hipótesis general

H_1: Existe una relación estadísticamente relevante entre las prácticas de ciberseguridad y la información contable de las empresas comercializadoras de insumos médicos de la provincia de Manabí.

Hipótesis específicas

HE_1. La gobernanza y políticas de seguridad se relacionan de forma estadísticamente significativa con la integridad y exactitud de la información contable.

HE_2. La gestión de activos y accesos se relaciona de forma estadísticamente significativa con la confidencialidad tributaria de la información contable.

HE_3. La seguridad de la infraestructura se relaciona de forma estadísticamente significativa con la disponibilidad y el acceso a la información contable.

HE_4. La cultura organizacional en ciberseguridad se relaciona de forma estadísticamente significativa con la confiabilidad de los reportes contables.

HE_5. La resiliencia operativa se relaciona de forma estadísticamente significativa con el cumplimiento normativo contable y tributario.

Capítulo II. Marco teórico

Antecedentes de la investigación

A nivel global, los estudios académicos muestran que la ciberseguridad ha dejado de ser únicamente un mecanismo de defensa tecnológica, convirtiéndose en un elemento esencial dentro de la gestión y gobernanza de los sistemas contables, así como en la garantía de la calidad de los datos que producen. En esta línea, Shafa y Islam (2025) examinaron cómo las prácticas de seguridad digital impactan en los sistemas de información contable y su incidencia en la transparencia financiera, partiendo del reconocimiento de que la transformación digital ha elevado la vulnerabilidad de las organizaciones a riesgos capaces de comprometer la calidad de la información utilizada en los procesos de gestión, auditoría y toma de decisiones; los autores determinaron que la gobernanza de datos, los controles de acceso, el cifrado, las auditorías de seguridad y los mecanismos de respuesta frente a incidentes fortalecen la confiabilidad de los reportes financieros al reducir la probabilidad de errores, alteraciones y vulneraciones de los registros contables, mientras que la integración de estas prácticas contribuye a reforzar la fiabilidad de los informes financieros.

Desde una perspectiva complementaria, Shchyrba et al. (2025) analizaron los desafíos asociados con la utilización de sistemas de contabilidad en la nube durante el período 2020–2024, considerando que la transformación digital de los procesos financieros ha modificado la manera en que las empresas almacenan, procesan y comparten su información contable; los resultados evidenciaron que estas plataformas favorecen la eficiencia operativa, la disponibilidad de los registros y el acceso remoto a los datos financieros, aunque también incrementan la exposición al fraude electrónico, el robo de credenciales y los accesos no autorizados cuando las organizaciones carecen de mecanismos adecuados de protección, razón por la cual los autores proponen integrar cifrado, autenticación multifactor, auditorías periódicas y políticas institucionales de seguridad como elementos orientados a asegurar la protección, la consistencia y el acceso confiable a la información.

La continuidad operativa constituye uno de los pilares de la ciberseguridad, debido a que la interrupción de las plataformas informáticas podría comprometer la disponibilidad de los datos financieros y afectar el desarrollo de los procesos contables;

bajo esta perspectiva, Osundare et al. (2022) estudiaron estrategias dirigidas a fortalecer la continuidad de los servicios financieros mediante infraestructuras tecnológicas resilientes, partiendo de la necesidad de asegurar la disponibilidad de la información ante fallos operativos e incidentes de ciberseguridad que puedan afectar el funcionamiento de los sistemas contables; la investigación demostró que las arquitecturas de centros de datos activo-activo, la redundancia de recursos, la sincronización de la información en tiempo real y el balanceo de carga reducen los períodos de interrupción del servicio, mientras la incorporación de mecanismos de detección de amenazas, segmentación de activos críticos y cifrado de la información incrementa la capacidad institucional para responder y recuperarse ante eventos adversos, evidencia que respalda la incorporación de la resiliencia operativa como una dimensión de la ciberseguridad estrechamente vinculada con la disponibilidad y confiabilidad de la información contable.

La cultura organizacional representa uno de los componentes más influyentes en la consolidación de una estrategia integral de ciberseguridad, debido a que las medidas tecnológicas alcanzan su verdadera eficacia cuando son respaldadas por prácticas institucionales y comportamientos responsables del talento humano; bajo esta perspectiva, Kafi y Akter (2023) estudiaron cómo las prácticas culturales dentro de la organización en materia de seguridad digital impactan en la salvaguarda de los datos financieros y en la confiabilidad de los procesos de auditoría, partiendo del reconocimiento de que la seguridad de los sistemas contables trasciende la incorporación de herramientas tecnológicas y depende, en igual medida, de las prácticas institucionales y del comportamiento del personal responsable del tratamiento de los datos; los autores determinaron que la falta de capacitación, la escasa sensibilización frente a los riesgos digitales y la ausencia de responsabilidades claramente definidas incrementan la probabilidad de errores humanos, filtraciones de información y uso indebido de credenciales, mientras que la formación continua, las campañas de concienciación y la implicación activa de la alta dirección fortalecen la capacidad de las organizaciones para preservar la integridad de los registros financieros y generar evidencia confiable para los procesos de auditoría, planteamiento que sustenta la incorporación de la cultura organizacional como una dimensión de la ciberseguridad vinculada con la protección y confiabilidad de la información contable.

Nyombi et al. (2024) estudiaron los mecanismos destinados a proteger la información tributaria en entornos digitales, centrando su análisis en los controles de acceso y en las estrategias orientadas a preservar la confidencialidad y disponibilidad de los datos financieros frente al incremento de las amenazas cibernéticas; los resultados evidenciaron que la autenticación multifactor, el cifrado de la información y el monitoreo permanente reducen la probabilidad de accesos no autorizados, robo de credenciales y vulneraciones capaces de afectar la continuidad de las operaciones, mientras que la incorporación de planes de recuperación y continuidad fortalece la resiliencia operativa de las entidades mediante el aseguramiento del cumplimiento de sus obligaciones tributarias aun cuando se presenten incidentes de seguridad, evidencia que respalda la relación entre la gestión de activos y accesos, la confidencialidad tributaria y la resiliencia operativa como componentes de la variable ciberseguridad analizada en esta investigación.

En el ámbito ecuatoriano, Calle y Andrade (2024) investigaron la situación de la ciberseguridad en empresas comerciales de la ciudad de Azogues, identificando una marcada discrepancia entre la percepción del riesgo y las acciones implementadas para proteger la información financiera, puesto que el 80 % de los profesionales contables reconocía la existencia de amenazas sobre la integridad de los activos contables y financieros; pese a ello, una proporción considerable de las organizaciones destinaba menos del 1 % de su presupuesto anual al fortalecimiento de la seguridad digital, limitando la implementación de controles preventivos frente a *malware*, *phishing*, intrusiones internas y accesos no autorizados a los sistemas contables. Los autores sostienen que la ausencia de evaluaciones periódicas dificulta la detección temprana de vulnerabilidades y aumenta la probabilidad de incidentes capaces de comprometer la fiabilidad de los datos empleados en los procesos de decisión; esta evidencia permite comprender que la protección de la información contable exige integrar inversión tecnológica, monitoreo continuo, controles internos y una cultura organizacional orientada a la prevención del riesgo, aportando sustento empírico para analizar la ciberseguridad como un factor asociado con la confiabilidad de la información contable en las empresas comercializadoras.

La resiliencia operativa ha adquirido una creciente relevancia en la gestión de la ciberseguridad, debido a que la capacidad de responder y recuperarse frente a incidentes tecnológicos determina la continuidad de los procesos contables y financieros; desde

esta perspectiva, López y Ordóñez (2024) evaluaron la resiliencia empresarial frente a amenazas digitales en el sector comercial de la ciudad de Quito, identificando que el 80 % de las empresas analizadas no efectuaba auditorías periódicas de seguridad, circunstancia que limitaba la detección oportuna de vulnerabilidades en sus sistemas tecnológicos, mientras la ausencia de planes actualizados de respuesta y recuperación reducía la capacidad institucional para restablecer las operaciones después de una brecha de seguridad, especialmente en los departamentos financieros, donde un incidente de *ransomware* o la pérdida de acceso a los sistemas puede comprometer la validez de los registros contables y la continuidad de las actividades empresariales; con base en estos hallazgos, los autores sostienen que la coordinación entre la alta dirección, el área contable y la auditoría informática fortalece la implementación de controles proporcionales a los riesgos existentes, aportando evidencia que respalda la resiliencia operativa como una dimensión de la ciberseguridad estrechamente vinculada con la protección y confiabilidad de la información contable (López & Ordóñez, 2024).

La infraestructura tecnológica utilizada para gestionar la información financiera constituye un elemento determinante en la eficacia de las prácticas de ciberseguridad, debido a que las características de cada plataforma condicionan los mecanismos de protección disponibles y el nivel de exposición frente a amenazas digitales; bajo esta perspectiva, Guachún y Andrade (2024) analizaron el uso de sistemas contables locales y en la nube en empresas ecuatorianas, identificando una marcada preferencia por las soluciones de escritorio al considerarlas una alternativa que proporciona mayor control sobre los datos financieros, percepción que contrasta con la evidencia obtenida por los autores, quienes señalan que la ausencia de actualizaciones críticas, respaldos periódicos y mecanismos de monitoreo incrementa la vulnerabilidad frente a *malware* y pérdidas de información, mientras que las plataformas en la nube favorecen la disponibilidad y el acceso remoto, aunque requieren controles específicos frente al *phishing*, la denegación de servicio y el robo de credenciales; a partir de estos hallazgos, el estudio sostiene que la protección de los sistemas contables depende de la integración entre la infraestructura tecnológica y los controles internos destinados a preservar la integridad, trazabilidad y disponibilidad de los registros digitales, aportando fundamentos que respaldan la dimensión seguridad de la infraestructura (Guachún & Andrade, 2024).

El fortalecimiento de la ciberseguridad exige que las medidas tecnológicas se articulen con el marco jurídico que regula el tratamiento y la protección de la

información, debido a que la eficacia de los controles implementados depende tanto de su solidez técnica como del cumplimiento de las obligaciones legales que rigen la gestión de los datos; bajo esta perspectiva, Enríquez (2025) examinó la adopción de esquemas de seguridad en Ecuador, sosteniendo que las organizaciones deben integrar los estándares técnicos con las disposiciones establecidas en la Ley Orgánica de Protección de Datos Personales [LOPDP] (2021) y el Código Orgánico Integral Penal [COIP] (2014), de manera que la ciberseguridad trascienda la prevención de incidentes para incorporar responsabilidades institucionales vinculadas con la gestión, el resguardo y la seguridad de los datos, fortaleciendo la capacidad de las entidades para reducir riesgos, preservar evidencia digital y responder ante posibles vulneraciones; estos planteamientos adquieren especial relevancia en el sector comercial, donde la información contable y tributaria debe mantenerse íntegra, confidencial y disponible para atender procesos de auditoría, fiscalización y control, aportando fundamentos que respaldan el análisis del cumplimiento normativo como una dimensión vinculada con la ciberseguridad y la protección de la información contable (Enríquez, 2025).

Bases teóricas

Teoría de la tríada de la seguridad (CIA)

La salvaguarda de los activos de información se sustenta en principios que permiten preservar la continuidad de las operaciones frente a amenazas internas y externas, siendo el modelo de la tríada de seguridad –integrada por confidencialidad, integridad y accesibilidad– uno de los marcos conceptuales con mayor aceptación para orientar el diseño de controles destinados a salvaguardar la información en entornos digitales; Guamán (2023) sostiene que estos tres componentes actúan de manera interdependiente, debido a que la pérdida o el debilitamiento de cualquiera de ellos compromete la eficacia del sistema de protección en su conjunto, condición que adquiere especial relevancia en los sistemas de información contable, donde la confidencialidad restringe el acceso a usuarios autorizados, la integridad garantiza que los registros financieros permanezcan libres de alteraciones no autorizadas y la disponibilidad asegura el acceso oportuno a los datos requeridos para respaldar las operaciones, la gestión administrativa y los procesos de decisión, convirtiendo a la tríada confidencialidad, integridad y accesibilidad en la base de las estrategias modernas de ciberseguridad.

La aplicación de este modelo exige complementar los principios conceptuales con controles técnicos y organizacionales diseñados para preservar la fiabilidad de los datos a lo largo de todo su proceso de gestión, razón por la cual la integridad demanda mecanismos de validación que impidan errores materiales, modificaciones no autorizadas o pérdidas de información, mientras la disponibilidad requiere infraestructuras resilientes que permitan mantener operativos los sistemas financieros aun cuando se presenten incidentes tecnológicos; Calle y Andrade (2024) sostienen que la validez de la información contable se fundamenta en la conservación íntegra de los registros desde el momento en que se origina la transacción hasta la emisión de los estados financieros, circunstancia que también requiere garantizar el acceso permanente a plataformas de facturación, declaración tributaria y demás procesos críticos de la organización, de modo que la interacción entre confidencialidad, integridad y disponibilidad constituye una base conceptual para reforzar la protección de las plataformas de información.

Teoría de sistemas de información contable (SIC)

Los sistemas de información contable representan la base tecnológica que posibilita convertir las operaciones económicas en datos financieros relevantes para la administración, el control y la toma de decisiones, razón por la cual su eficacia depende de la integración coordinada entre personas, procesos, recursos tecnológicos junto con procedimientos de supervisión que aseguren la calidad de los datos durante todo su ciclo de procesamiento; Guachún y Andrade (2024) sostienen que estos sistemas conforman una estructura interrelacionada destinada a capturar, procesar, almacenar y comunicar información financiera de manera uniforme, permitiendo que los estados financieros reflejen la realidad económica de las organizaciones mediante registros verificables, oportunos y sustentados documentalmente, condición que fortalece la transparencia de la gestión y facilita los procesos de auditoría, fiscalización y control, convirtiendo al sistema de información contable en un componente esencial para preservar la confiabilidad de la información financiera en entornos empresariales cada vez más digitalizados.

La evolución de los sistemas de información contable ha incorporado mecanismos orientados a fortalecer la seguridad y trazabilidad de los registros digitales, debido a que la automatización de los procesos financieros exige controles capaces de

prevenir alteraciones, detectar accesos no autorizados y garantizar la consistencia de la información procesada; López y Ordóñez (2024) sostienen que el uso del enfoque sistémico en la contabilidad requiere la incorporación de controles de seguridad que validen la integridad de los registros desde el ingreso de las transacciones hasta la generación de los estados financieros, permitiendo a la gerencia disponer de datos actualizados que respalden los procesos de decisión, reducir la incidencia del error humano y mantener un historial verificable de cada operación efectuada, de manera que la interacción entre automatización, control interno y ciberseguridad fortalece la confiabilidad de la información contable y la capacidad institucional para responder a las exigencias de auditoría, supervisión y cumplimiento normativo.

Modelo de gobernanza de ciberseguridad (NIST 2.0)

La gestión de los riesgos cibernéticos requiere modelos que integren la planificación estratégica con la implementación de controles técnicos, razón por la cual el Marco de Ciberseguridad desarrollado por el *National Institute of Standards and Technology* [NIST] (2024) constituye una de las referencias internacionales más utilizadas para orientar la gobernanza de la seguridad de la información; su versión 2.0 incorpora la función *Govern*, mediante la cual la alta dirección asume la responsabilidad de establecer políticas, definir responsabilidades y alinear la gestión de la ciberseguridad con los objetivos institucionales, permitiendo identificar activos críticos, valorar los riesgos que amenazan la continuidad de las operaciones y aplicar salvaguardas proporcionales frente a incidentes como *ransomware*, accesos no autorizados o filtraciones de información, planteamiento que Pacheco y Staino (2025) consideran indispensable para reforzar la articulación entre los departamentos de tecnología y contabilidad, promoviendo que las decisiones relacionadas con la seguridad respondan a una estrategia organizacional integral y no únicamente a requerimientos tecnológicos.

La estructura propuesta por el NIST (2024) estructura la administración de la ciberseguridad a través de funciones dirigidas a gobernar, reconocer, resguardar, detectar, responder y restaurar los activos digitales, permitiendo que las organizaciones desarrollen un proceso continuo de evaluación y mejora frente a amenazas en permanente evolución; este planteamiento refuerza la seguridad de la información financiera mediante la implementación de procedimientos para la custodia de datos, la

detección temprana de incidentes, la recuperación de los servicios críticos y la reducción del impacto operativo derivado de una vulneración de seguridad, facilitando al mismo tiempo el cumplimiento de normas regulatorias vinculadas con la protección de datos personales y la conservación de la evidencia digital, de modo que la gobernanza de la ciberseguridad trasciende la implementación de controles aislados para consolidar un modelo institucional orientado a preservar la reserva, consistencia y accesibilidad de los datos contables.

Enfoque de resiliencia organizacional y continuidad

La resiliencia organizacional constituye un enfoque orientado a incrementar la resiliencia de las instituciones permitiéndoles prever, soportar, actuar y restablecerse ante situaciones que comprometan el desarrollo normal de sus operaciones, razón por la cual ha adquirido una importancia creciente en la gestión de la ciberseguridad como complemento de las estrategias preventivas; Safitra et al. (2023) sostienen que este enfoque trasciende la simple prevención de incidentes al incorporar mecanismos que permiten mantener la continuidad de los procesos críticos, preservar la disponibilidad de la información y restablecer las funciones esenciales después de una vulneración de seguridad, condición que en el ámbito contable resulta imprescindible contar con estrategias de continuidad empresarial, protocolos de restablecimiento frente a contingencias y mecanismos de respaldo que aseguren la conservación de los registros financieros y tributarios, permitiendo que las organizaciones mantengan la integridad de sus operaciones aun cuando enfrenten interrupciones derivadas de incidentes tecnológicos.

La consolidación de un entorno resiliente requiere integrar infraestructura tecnológica, planificación institucional y mecanismos permanentes de recuperación que reduzcan la probabilidad de interrupciones prolongadas, debido a que la continuidad operativa depende tanto de la capacidad para prevenir incidentes como de la rapidez con que los servicios puedan restablecerse cuando estos ocurran; MINTEL (2025) sostiene que la transformación digital de las organizaciones ecuatorianas debe incorporar procesos seguros de digitalización, almacenamiento y recuperación de la información, favoreciendo la utilización de infraestructuras redundantes y servicios de almacenamiento que disminuyan el riesgo asociado a puntos únicos de falla, preserven la disponibilidad de los registros financieros y fortalezcan la capacidad institucional

para atender obligaciones contables, tributarias y de auditoría, de manera que la resiliencia organizacional se consolida como un elemento clave destinado a asegurar la permanencia operativa de los sistemas de información contable en entornos caracterizados por una creciente exposición a riesgos cibernéticos.

Marco conceptual

Ciberseguridad

La ciberseguridad abarca un conjunto de lineamientos, protocolos, mecanismos técnicos y acciones organizacionales dirigidas a resguardar los sistemas de datos frente a peligros que puedan afectar la reserva, consistencia y accesibilidad de la información, razón por la cual su alcance trasciende la implementación de herramientas tecnológicas para incorporar procesos permanentes de gestión del riesgo, gobernanza institucional y mejora continua de los mecanismos de protección; Guamán (2023) la define como un proceso integral orientado a reconocer, analizar y administrar los riesgos que afectan los activos de información, reduciendo la probabilidad de incidentes y las consecuencias derivadas de su materialización, planteamiento que, para efectos de la presente investigación, comprende las acciones implementadas por las empresas comercializadoras de insumos médicos para prevenir accesos no autorizados, alteraciones de los registros contables, pérdida de información, interrupciones operativas y divulgación indebida de datos financieros, incorporando la participación de la alta dirección, la distribución de funciones, la formación continua del personal y la aplicación de controles técnicos, de modo que la ciberseguridad constituye la variable independiente del estudio al representar el conjunto de prácticas cuya relación con la protección y confiabilidad de la información contable será analizada mediante el desarrollo de la investigación.

Protección de datos contables

La salvaguarda de la información contable comprende el conjunto de medidas técnicas, administrativas y organizacionales orientadas a preservar la seguridad de la información financiera durante las etapas de registro, procesamiento, almacenamiento, transmisión y conservación, razón por la cual se convierte en una condición clave para sostener la continuidad operativa; Guachún y Andrade (2024) sostienen que la digitalización de las tareas contables incrementa la eficiencia en la administración

empresarial, aunque también amplía la vulnerabilidad frente a riesgos que pueden afectar la reserva, consistencia y accesibilidad de los registros financieros, circunstancia que exige implementar mecanismos orientados a prevenir accesos no autorizados, alteraciones de la información, pérdidas de datos y divulgaciones indebidas, preservando la evidencia documental necesaria para atender procesos de auditoría, fiscalización y control, de manera que la protección de los datos contables constituye un pilar fundamental para salvaguardar el patrimonio informativo de las entidades y fortalecer la calidad de los datos empleados en la gestión financiera.

Información contable

La información contable se define como un sistema estructurado de datos financieros y económicos que surge del registro, ordenamiento, procesamiento y exposición organizada de las operaciones de una entidad, posibilitando reflejar su posición financiera, resultados económicos y variaciones patrimoniales a través de datos relevantes para la administración, el control y los procesos de decisión; Guachún y Andrade (2024) sostienen que los sistemas de información contable convierten las transacciones económicas en reportes estructurados que respaldan los procesos administrativos, financieros y tributarios de las organizaciones, condición que exige que los datos presenten atributos de exactitud, integridad, oportunidad, verificabilidad y confiabilidad con el fin de atender los requerimientos de los diversos usuarios de la información; aspecto que en la presente investigación, comprende tanto los registros internos como los estados financieros y reportes tributarios generados por las empresas comercializadoras de insumos médicos, constituyendo la variable dependiente del estudio al analizarse su relación con las prácticas de ciberseguridad implementadas por dichas organizaciones.

Sistema de información contable

El sistema contable se configura como una estructura compuesta por individuos, procesos, herramientas tecnológicas, documentación y aplicaciones digitales orientadas a registrar, procesar, almacenar y comunicar la información económica de una organización, permitiendo que las transacciones empresariales se transformen en información financiera útil para la administración, el control interno, el cumplimiento tributario y la elaboración de estados financieros; Guachún y Andrade (2024) sostienen

que estos sistemas operan mediante una estructura interrelacionada de componentes tecnológicos que facilitan el tratamiento uniforme de la información financiera, incorporando módulos destinados a la emisión de facturas, gestión de inventarios, administración de cuentas por cobrar y por pagar, operaciones bancarias, gestión de nómina y obligaciones fiscales, cuya confiabilidad depende de la existencia de mecanismos capaces de preservar la consistencia, accesibilidad y reserva de los registros procesados, de modo que el sistema de información contable constituye el entorno donde convergen las prácticas de ciberseguridad y la calidad de la información generada por las organizaciones.

Confidencialidad

La confidencialidad constituye un pilar fundamental dentro de la seguridad informativa, orientado a garantizar que el acceso, uso y divulgación de los datos se restrinjan exclusivamente a las personas autorizadas conforme a las responsabilidades asignadas por la organización, condición que adquiere especial relevancia en los sistemas de información contable al resguardar registros tributarios, información financiera, cuentas bancarias, costos, márgenes de utilidad y demás datos cuya exposición puede afectar el funcionamiento institucional; Kar y Zolkipli (2021) señalan que este principio busca impedir la divulgación no autorizada de información susceptible de comprometer la privacidad, la competitividad o la seguridad organizacional, finalidad que exige implementar controles de acceso, clasificación de la información, mecanismos robustos de autenticación y restricciones basadas en los perfiles de usuario, permitiendo preservar la reserva de la información financiera, reducir la probabilidad de accesos indebidos y fortalecer la observancia de las disposiciones jurídicas vinculadas con la salvaguarda de la información contable.

Integridad de la información

El principio de integridad de los datos asegura que la información se mantengan completos, exactos, consistentes y protegidos frente a modificaciones no autorizadas durante todas las etapas de su ciclo de uso, condición indispensable para que la información contable represente fielmente las operaciones económicas de una organización y conserve su valor como evidencia para los procesos de gestión, control y auditoría; Calle y Andrade (2024) sostienen que este principio exige preservar la

veracidad de los registros financieros frente a amenazas como el *malware*, las intrusiones y la manipulación deliberada de datos, requiriendo que cualquier modificación realizada sobre la información se encuentre debidamente autorizada, documentada y registrada mediante mecanismos que permitan verificar su trazabilidad, finalidad que, en la presente investigación, comprende la utilización de firmas o certificados digitales, registros de auditoría protegidos y procedimientos periódicos de verificación de la base de datos contable, favoreciendo la transparencia administrativa y reduciendo la probabilidad de errores, fraude o distorsiones que comprometan la fiabilidad de los registros financieros.

Exactitud de los registros contables

La exactitud de los registros contables hace referencia a la correspondencia fiel entre la información incorporada en el sistema contable y las operaciones económicas efectivamente realizadas por la organización, razón por la cual cada transacción debe registrarse utilizando valores, fechas, cuentas contables y documentos de respaldo que reflejen con precisión la realidad financiera de la entidad; López y Ordóñez (2024) sostienen que la implementación de controles preventivos y mecanismos de protección digital contribuye a reducir el riesgo de alteraciones que puedan afectar la validez de la información utilizada para la gestión empresarial, circunstancia que exige aplicar conciliaciones, validaciones automáticas y procedimientos de revisión orientados a detectar duplicidades, omisiones o modificaciones no autorizadas, permitiendo que los estados financieros mantengan niveles adecuados de confiabilidad, verificabilidad y utilidad para la toma de decisiones, contribuyendo a la observancia de los deberes fiscales y a la ejecución de las labores de auditoría.

Disponibilidad de la información

La disponibilidad se reconoce como un fundamento clave dentro de la protección de la información, orientado a garantizar que los sistemas, aplicaciones y datos permanezcan accesibles para los usuarios autorizados cuando las operaciones institucionales así lo requieran, condición que resulta indispensable para asegurar la continuidad de los procesos contables, financieros y tributarios desarrollados mediante plataformas digitales; Kar y Zolkipli (2021) sostienen que este principio permite disponer de la información en forma oportuna, evitando que incidentes tecnológicos

afecten el funcionamiento normal de las organizaciones, mientras Guachún y Andrade (2024) señalan que la digitalización incrementa la eficiencia operativa, aunque también amplía la exposición frente a amenazas capaces de interrumpir el acceso a los sistemas de información, circunstancia que exige implementar respaldos periódicos, mecanismos seguros de acceso remoto, planes de mantenimiento y procedimientos de recuperación orientados a preservar la continuidad de las operaciones, favoreciendo que la información contable permanezca disponible para la gestión administrativa,

Gobernanza y políticas de seguridad

La gobernanza en materia de ciberseguridad abarca las decisiones estratégicas, las funciones asignadas y los instrumentos institucionales mediante los cuales la alta dirección dirige la gestión de los riesgos asociados con los activos de información, permitiendo integrar las políticas de seguridad con los objetivos estratégicos, el control interno y la gestión organizacional; el Marco de Ciberseguridad del NIST (2024) incorpora la función *Govern* como el eje encargado de establecer responsabilidades, definir políticas y supervisar la implementación de los controles orientados a proteger la información institucional, planteamiento que Guamán (2023) complementa al señalar que las políticas de seguridad deben establecer con claridad las funciones, obligaciones y procedimientos aplicables para prevenir el uso inadecuado de los activos digitales y responder frente a incidentes que comprometan la información, razón por la cual esta dimensión comprende la existencia de manuales formalizados, la actualización periódica de las políticas institucionales junto con la implicación de la alta gerencia en la asignación de recursos destinados a fortalecer las prácticas de ciberseguridad como parte de la gestión integral de la organización.

Gestión de activos y accesos

La gestión de activos y accesos comprende el conjunto de procedimientos orientados a identificar, administrar y proteger los activos digitales que sostienen la operatividad de los sistemas informativos institucionales, permitiendo controlar quién puede acceder, consultar, modificar o administrar los activos digitales conforme a las responsabilidades asignadas dentro de la estructura institucional; Pacheco y Staino (2025) sostienen que una administración adecuada de los accesos reduce la superficie de exposición frente a amenazas internas y externas al limitar los privilegios concedidos a

cada usuario, criterio que, en el ámbito contable, exige establecer permisos diferenciados para los módulos financieros, bases de datos, servidores, aplicaciones contables, respaldos y demás recursos tecnológicos, incorporando mecanismos de autenticación, perfiles de acceso y revisiones periódicas de privilegios que restrinjan las acciones a las funciones propias de cada cargo, favoreciendo la protección de los registros financieros y tributarios frente a accesos no autorizados, modificaciones indebidas o extracción de información sensible.

Autenticación multifactor

La autenticación multifactor constituye un mecanismo de control de identidad diseñado para verificar el acceso de los usuarios mediante la combinación de dos o más factores independientes de autenticación, fortaleciendo la protección de los sistemas de información al reducir la probabilidad de que credenciales comprometidas permitan el ingreso no autorizado a los recursos institucionales; Shchyrba et al. (2025) señalan que este procedimiento combina elementos asociados al conocimiento del usuario, la posesión de un dispositivo o la utilización de características biométricas, incrementando los niveles de seguridad frente al robo de credenciales y otras modalidades de acceso ilícito, circunstancia que adquiere especial relevancia en los sistemas de información contable donde se administran módulos relacionados con facturación, nómina, bancos, inventarios y obligaciones tributarias, razón por la cual la presente investigación incorpora la autenticación multifactor como un indicador de la efectividad de las medidas de verificación de identidad aplicadas por las empresas para proteger los datos financieros y contables.

Seguridad de la infraestructura tecnológica

La protección de la infraestructura tecnológica abarca un conjunto de medidas orientadas a salvaguardar los elementos físicos y digitales que sostienen la operatividad de los sistemas de información, garantizando que los recursos tecnológicos utilizados por la organización operen bajo condiciones que reduzcan la probabilidad de incidentes capaces de comprometer la información financiera; Calle y Andrade (2024) sostienen que la protección de la infraestructura exige implementar mecanismos orientados a prevenir, detectar y responder frente a actividades anómalas que afecten los activos digitales, incorporando medidas aplicables a servidores, estaciones de trabajo, redes de

comunicación, bases de datos, dispositivos de almacenamiento, aplicaciones informáticas y servicios en la nube, mediante herramientas perimetrales, sistemas de monitoreo, controles de acceso y mecanismos de cifrado que disminuyan la exposición frente a *malware*, *ransomware*, filtraciones de información y otras amenazas dirigidas contra los sistemas contables, permitiendo preservar la disponibilidad de los datos financieros y asegurar la permanencia de los procesos administrativos, contables y tributarios de la organización.

Cifrado de datos

El cifrado de datos constituye un mecanismo criptográfico orientado a proteger la información mediante su transformación en un formato inteligible únicamente para quienes poseen las credenciales o claves autorizadas para acceder a ella, proporcionando un nivel adicional de protección frente a accesos indebidos, interceptaciones o divulgaciones no autorizadas durante el almacenamiento y la transmisión de la información; Shchyrba et al. (2025) sostienen que esta medida representa una salvaguarda esencial para los sistemas de contabilidad digital debido al incremento de amenazas dirigidas contra la información financiera, criterio que justifica su aplicación sobre bases de datos contables, respaldos electrónicos, comprobantes tributarios, documentos financieros y conexiones remotas utilizadas por las organizaciones, fortaleciendo la confidencialidad de los activos informativos sin sustituir los demás controles de seguridad implementados, razón por la cual el presente estudio incorpora el cifrado como un indicador de la seguridad de la infraestructura tecnológica y de la aptitud organizacional para proteger la información contable frente a riesgos cibernéticos.

Cultura organizacional de ciberseguridad

La cultura de ciberseguridad en el ámbito organizacional comprende el conjunto de conocimientos, valores, conductas y responsabilidades colectivas de los miembros de una organización para promover la utilización responsable de las herramientas digitales y la salvaguarda de los datos institucionales, constituyendo un componente esencial de la gestión del riesgo al incorporar el factor humano como parte de las estrategias destinadas a prevenir incidentes de seguridad; Kafi y Akter (2023) sostienen que la eficacia de la ciberseguridad depende tanto de los controles tecnológicos como de las

conductas adoptadas por quienes utilizan y administran los sistemas de información, criterio que, en el ámbito contable, se refleja en prácticas orientadas a proteger las credenciales de acceso, verificar la legitimidad de las comunicaciones electrónicas, resguardar la información financiera y reportar oportunamente cualquier evento que pueda comprometer los activos digitales, fortaleciendo estas capacidades mediante programas permanentes de capacitación y ejercicios de simulación que incrementen la capacidad del personal para identificar amenazas y responder de forma preventiva, razón por la cual la presente investigación analiza esta dimensión a partir de los procesos de formación y sensibilización desarrollados para proteger la información contable.

Phishing

El *phishing* constituye una modalidad de ingeniería social utilizada para obtener de forma fraudulenta información confidencial mediante comunicaciones o sitios electrónicos diseñados para aparentar legitimidad, aprovechando el comportamiento de los usuarios con el propósito de acceder ilícitamente a credenciales, información financiera o datos institucionales protegidos; Guachún y Andrade (2024) identifican esta amenaza como un riesgo crítico que enfrentan los sistemas contables digitales cuando el personal no dispone de conocimientos suficientes para reconocer intentos de suplantación de identidad, situación que puede facilitar accesos indebidos a plataformas de facturación, cuentas bancarias, declaraciones tributarias y bases de datos relacionadas con clientes, proveedores y demás activos de información, haciendo necesaria la implementación de programas permanentes de concienciación, protocolos para la verificación de comunicaciones electrónicas y procedimientos orientados al reporte inmediato de incidentes, convirtiendo al *phishing* en un riesgo estrechamente vinculado con el factor humano y con el fortalecimiento de la cultura organizacional de ciberseguridad.

Resiliencia operativa

La resiliencia operativa se entiende como la facultad de una organización para prever, soportar, reaccionar, ajustarse y restablecer el funcionamiento de sus procesos críticos frente a incidentes que puedan comprometer la continuidad de sus operaciones, constituyendo un componente esencial de la ciberseguridad al permitir que las funciones

institucionales se mantengan o restablezcan en condiciones aceptables después de una interrupción; López y Ordóñez (2024) sostienen que esta capacidad adquiere especial relevancia frente a amenazas como el *ransomware* y otras vulneraciones que afectan los sistemas de información, criterio que, en el ámbito contable, exige contar con herramientas que posibiliten la recuperación de los registros financieros, restablecer el acceso a las plataformas tecnológicas y garantizar el cumplimiento oportuno de las obligaciones contables y tributarias, finalidad que, según Safitra et al. (2023), requiere integrar infraestructura tecnológica, liderazgo institucional y procesos permanentes de preparación mediante planes de continuidad, respaldos actualizados y pruebas periódicas de recuperación, razón por la cual la presente investigación incorpora la resiliencia operativa como una dimensión de la ciberseguridad asociada con la continuidad empresarial y la salvaguarda de la información contable.

Plan de continuidad del negocio

El plan de continuidad del negocio constituye el instrumento mediante el cual una organización establece los procedimientos destinados a mantener o restablecer sus funciones esenciales cuando ocurren eventos capaces de interrumpir el desarrollo normal de sus operaciones, permitiendo reducir el impacto derivado de fallos tecnológicos, incidentes de ciberseguridad, desastres naturales u otras contingencias que afecten la disponibilidad de los sistemas de información; Pacheco y Staino (2025) sostienen que la continuidad operativa exige identificar los escenarios de riesgo y definir mecanismos orientados a preservar los procesos críticos de la organización, planteamiento que, en el ámbito contable, comprende la recuperación de los datos financieros, la accesibilidad de los sistemas utilizados para la emisión de comprobantes, la ejecución de pagos, la elaboración de reportes tributarios y la conservación de la documentación contable, requiriendo que los procedimientos establecidos sean actualizados, difundidos entre los responsables y sometidos a evaluaciones periódicas para verificar su eficacia, convirtiendo al plan de continuidad del negocio en un indicador de la capacidad institucional para responder y recuperarse ante eventos que afecten la administración de la información contable.

Recuperación ante desastres

La recuperación ante desastres abarca un conjunto de acciones técnicas y administrativas orientadas a restablecer los sistemas de información, la infraestructura tecnológica y los datos afectados por eventos que interrumpan el funcionamiento normal de la organización, teniendo como propósito reducir el tiempo de inactividad y restituir la accesibilidad de los datos esenciales para asegurar la permanencia de las operaciones institucionales; López y Ordóñez (2024) sostienen que la ausencia de planes actualizados limita la capacidad organizacional de reaccionar de manera oportuna frente a incidentes de seguridad, situación que, en el ámbito contable, compromete la recuperación de bases de datos, registros financieros, plataformas de procesamiento y otros medios indispensables para el cumplimiento de las obligaciones administrativas y tributarias, diferenciándose de la continuidad operativa del negocio, ya que esta procura mantener activos los procesos esenciales durante la contingencia, mientras la recuperación ante desastres concentra sus esfuerzos en restablecer los recursos afectados una vez ocurrido el incidente, motivo por el cual la presente investigación considera la existencia de un plan de recuperación para la infraestructura contable como una evidencia de resiliencia operativa.

Copias de seguridad o respaldos

Las copias de seguridad, también denominadas respaldos, corresponden a duplicados de la información que se conservan con el propósito de restaurar los datos cuando estos resultan afectados por pérdidas, fallos técnicos, errores operativos o incidentes de ciberseguridad, constituyendo uno de los mecanismos más importantes para preservar la disponibilidad y continuidad de la información contable frente a eventos que comprometan el funcionamiento de los sistemas; Guachún y Andrade (2024) señalan que la protección de los sistemas contables requiere implementar medidas que garanticen la recuperación de la información ante amenazas capaces de afectar la operación normal de las plataformas tecnológicas, criterio que exige realizar respaldos con una frecuencia acorde con las necesidades de la organización, almacenarlos bajo condiciones seguras y verificar periódicamente su capacidad de restauración, debido a que la sola existencia de copias resulta insuficiente cuando estas se encuentran desactualizadas, deterioradas o expuestas a los mismos riesgos que afectan al sistema principal, razón por la cual esta investigación incorpora los respaldos

como un indicador de la accesibilidad de los datos y de la aptitud institucional para recuperar los registros contables después de un incidente.

Confiabilidad de los reportes contables

La confiabilidad de los reportes contables corresponde al grado en que la información financiera puede considerarse veraz, consistente, verificable y útil para respaldar los procesos de toma de decisiones, auditoría y fiscalización, dependiendo de que los registros que sustentan su elaboración permanezcan completos, exactos, protegidos y elaborados conforme a los principios contables y las disposiciones tributarias aplicables; Shafa y Islam (2025) sostienen que la madurez de las prácticas de ciberseguridad fortalece la transparencia financiera al reducir los riesgos de errores, alteraciones y otras situaciones que pueden comprometer la calidad de los reportes empresariales, planteamiento que, en la presente investigación, se refleja en la evaluación de la consistencia de los saldos, la aplicación de conciliaciones y validaciones, así como en la existencia de controles destinados a prevenir errores durante el registro de las transacciones, razón por la cual la confiabilidad de los reportes se reconoce como una expresión fundamental de la excelencia de la información contable generada por las empresas objeto de estudio.

Cumplimiento normativo contable y tributario

El cumplimiento normativo contable y tributario comprende la observancia de las disposiciones legales, técnicas y administrativas que regulan el registro, conservación, procesamiento y presentación de la información financiera de las organizaciones, garantizando que las actividades contables se desarrollen conforme al marco regulatorio vigente y que los registros generados puedan ser verificados por los organismos competentes; en el contexto ecuatoriano, este cumplimiento implica la aplicación de las Normas Internacionales de Información Financiera (NIIF), las disposiciones emitidas por el Servicio de Rentas Internas (SRI) y las obligaciones relacionadas con la conservación de comprobantes y archivos digitales, incorporando además los deberes establecidos en la Ley Orgánica de Protección de Datos Personales [LOPDP] (2021) respecto al tratamiento y custodia de la información, aspecto que Enríquez (2025) vincula con la necesidad de articular los estándares técnicos de seguridad con el ordenamiento jurídico nacional para fortalecer la protección de los

activos informativos, motivo por el cual esta investigación analiza el cumplimiento normativo como una dimensión de la información contable asociada con la capacidad institucional para mantener procesos seguros, ordenados, trazables y verificables.

Marco legal

El marco legal de la presente investigación se sustenta en las disposiciones del ordenamiento jurídico ecuatoriano que regulan la protección de los datos personales, sancionan las conductas ilícitas cometidas mediante sistemas informáticos y establecen los requisitos aplicables a la validez, conservación, trazabilidad y resguardo de la información contable y tributaria, constituyendo el fundamento normativo que orienta las obligaciones de las empresas comercializadoras de insumos médicos de la provincia de Manabí en el tratamiento de la información financiera administrada mediante plataformas digitales; estas disposiciones reconocen que la seguridad de la información trasciende el ámbito estrictamente tecnológico para convertirse en un componente del control interno, la gestión institucional y la protección de derechos, imponiendo a las organizaciones el deber de adoptar medidas razonables para evitar ingresos ilícitos, alteraciones, pérdidas, divulgaciones improcedentes o interrupciones que comprometan la disponibilidad de los datos, al tiempo que reconocen la validez jurídica de los documentos electrónicos y establecen responsabilidades frente a conductas que afecten la integridad de los sistemas informáticos, razón por la cual el presente marco jurídico proporciona el sustento normativo para examinar la relación entre las estrategias de ciberseguridad y la protección de la información contable.

Constitución de la República del Ecuador

La Constitución de la República del Ecuador (2008) constituye el principal fundamento jurídico para la protección de la información personal y el reconocimiento de los derechos relacionados con el tratamiento de datos en el territorio nacional, estableciendo en el artículo 66, numeral 19, el derecho de toda persona a la protección de sus datos personales y a decidir sobre la recolección, almacenamiento, procesamiento, utilización y difusión de la información que le concierne, salvo las excepciones previstas por la ley; aunque la información contable corresponde principalmente al ámbito organizacional, su gestión incorpora datos personales de trabajadores, clientes, proveedores, representantes legales y demás sujetos vinculados

con la actividad empresarial, circunstancia que obliga a las organizaciones a implementar controles destinados a preservar la confidencialidad, integridad y uso legítimo de los registros físicos y digitales, garantizando que el tratamiento de esta información se realice conforme a los principios constitucionales de privacidad y autodeterminación informativa, motivo por el cual la presente investigación encuentra en este mandato constitucional el fundamento jurídico que respalda la aplicación de prácticas de ciberseguridad orientadas a proteger la información contable y tributaria.

Ley Orgánica de Protección de Datos Personales

La Ley Orgánica de Protección de Datos Personales [LOPDP] (2021) establece el marco jurídico que regula el tratamiento de los datos personales por parte de las entidades públicas y privadas en Ecuador, garantizando el ejercicio del derecho a la protección de la información mediante la definición de principios, obligaciones y mecanismos de control que deben observar las organizaciones responsables de su tratamiento; en el caso de las empresas comercializadoras de insumos médicos, esta normativa adquiere especial relevancia porque los registros contables, tributarios, laborales y comerciales incorporan información que permite identificar a trabajadores, clientes, proveedores, representantes legales y otros titulares de datos personales, circunstancia que exige implementar medidas técnicas y organizativas orientadas a prevenir accesos no autorizados, pérdidas, alteraciones, destrucción o divulgación indebida de la información, mediante controles de acceso, mecanismos de autenticación, cifrado, respaldos y procesos permanentes de capacitación del personal, motivo por el cual la LOPDP (2021) respalda la incorporación de prácticas de ciberseguridad como parte de la gestión contable y administrativa, fortaleciendo la protección de los derechos de los titulares y reduciendo los riesgos legales, operativos y reputacionales para las organizaciones.

Código Orgánico Integral Penal

El Código Orgánico Integral Penal [COIP] (2014) incorpora un conjunto de disposiciones destinadas a prevenir y sancionar las conductas que atentan contra la seguridad de los sistemas de información y comunicación, proporcionando protección jurídica a los activos digitales mediante la tipificación de infracciones relacionadas con el acceso no autorizado, la alteración de la información y la afectación de la integridad

de los sistemas informáticos; dentro de este marco, los artículos 229, 232 y 234 resultan especialmente relevantes para la presente investigación al establecer responsabilidades frente a la revelación ilegal de bases de datos, los ataques contra los sistemas de información y el acceso no consentido a plataformas digitales, situaciones que, en el ámbito contable, pueden materializarse mediante la modificación indebida de registros financieros, la extracción de bases de datos, el acceso ilícito al software contable o la interrupción maliciosa de los servicios tecnológicos, circunstancias que justifican la implementación de controles preventivos y la conservación de evidencias digitales que faciliten la detección, investigación y sanción de estos hechos, razón por la cual el COIP (2014) complementa el marco jurídico de la ciberseguridad al reforzar la protección legal de la información contable y de los sistemas que la soportan.

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos

La Ley de Comercio Electrónico, Firmas y Mensajes de Datos (2002) establece el marco jurídico que reconoce la validez de los documentos electrónicos, los mensajes de datos y las firmas electrónicas utilizados en las actividades comerciales, administrativas y financieras, otorgando seguridad jurídica a las transacciones digitales siempre que se cumplan los requisitos legales relacionados con su autenticidad, integridad y conservación; esta normativa adquiere especial importancia para las empresas comercializadoras de insumos médicos debido a que gran parte de sus operaciones se desarrolla mediante facturas electrónicas, comprobantes de retención, notas de crédito, órdenes de compra, contratos y demás documentos digitales que respaldan los procesos contables y tributarios, incorporando además la firma electrónica como un mecanismo que permite identificar al suscriptor, vincularlo con el contenido del documento y fortalecer los principios de autenticidad, integridad y no repudio, circunstancias que exigen proteger adecuadamente las credenciales, certificados y dispositivos utilizados para su emisión mediante controles propios de la ciberseguridad, motivo por el cual esta ley establece un vínculo directo entre la protección de los sistemas de información y la validez jurídica, probatoria y administrativa de la documentación contable y tributaria.

Normativa contable y tributaria aplicable

La elaboración, conservación y presentación de la información contable debe realizarse conforme al marco normativo vigente en Ecuador, garantizando que los registros financieros reflejen de manera razonable la realidad económica de las organizaciones y puedan ser verificados por los organismos competentes durante los procesos de control y fiscalización; las Normas Internacionales de Información Financiera (NIIF) establecen los criterios aplicables al reconocimiento, medición, presentación y revelación de los hechos económicos, mientras que las disposiciones emitidas por el Servicio de Rentas Internas (SRI) regulan la emisión, transmisión, almacenamiento y conservación de comprobantes electrónicos y demás documentos relacionados con el cumplimiento de las obligaciones tributarias, exigencias que requieren sistemas de información capaces de preservar la integridad, exactitud, disponibilidad y trazabilidad de los registros digitales, capacidades que pueden fortalecerse mediante controles de acceso, mecanismos de validación, respaldos, monitoreo y demás prácticas de ciberseguridad orientadas a proteger la información financiera, razón por la cual la seguridad de los sistemas contables constituye un elemento indispensable para garantizar el cumplimiento oportuno de las obligaciones contables y tributarias de las empresas objeto de estudio.

Política Pública para la Transformación Digital

La Política Pública para la Transformación Digital del Ecuador 2025–2030 promovida por el (MINTEL, 2025), establece los lineamientos estratégicos para impulsar la modernización de los sectores público y privado mediante la incorporación responsable de tecnologías digitales, reconociendo que la seguridad de la información constituye un elemento indispensable para consolidar procesos de transformación que garanticen la confianza, la continuidad operativa y el desarrollo sostenible de las organizaciones; en este contexto, la digitalización de documentos, operaciones y registros contables representa una oportunidad para incrementar la eficiencia administrativa y fortalecer la gestión institucional, aunque también exige la implementación de mecanismos orientados a preservar la confidencialidad, integridad y disponibilidad de la información frente a los riesgos inherentes a los entornos digitales, promoviendo el uso de infraestructuras tecnológicas seguras, procesos confiables para el almacenamiento de datos y capacidades organizacionales que permitan responder

oportunamente ante incidentes que afecten los servicios digitales, motivo por el cual esta política pública respalda el fortalecimiento de las prácticas de ciberseguridad como un componente estratégico del proceso de transformación digital de las empresas comercializadoras de insumos médicos y de la protección de su información contable.

Desarrollo de hipótesis específicas

> **HE_1:** La gobernanza y políticas de seguridad se relacionan de forma estadísticamente significativa con la integridad y exactitud de la información contable.

Shafa y Islam (2025) aportan evidencia que sustenta la hipótesis de que la gobernanza y las políticas de seguridad mantienen una relación estadísticamente significativa con la integridad y exactitud de la información contable, al demostrar que la madurez de la gobernanza de datos y de la ciberseguridad fortalece los sistemas de información contable mediante controles internos que incrementan la transparencia y confiabilidad de los reportes financieros; los autores sostienen que la implementación de políticas formales para la protección de la información, acompañadas de controles de acceso, mecanismos de cifrado, procesos de auditoría y procedimientos estructurados de respuesta ante incidentes, favorece la preservación de la exactitud de los registros contables y reduce la probabilidad de errores o fraudes, afirmación respaldada por un modelo de regresión que explica el 65 % de la variación en la transparencia financiera y evidencia efectos positivos de la gobernanza de la privacidad ($\beta = 0{,}217$), la ciberseguridad ($\beta = 0{,}263$) y la fortaleza de los controles del sistema de información contable como variable mediadora ($\beta = 0{,}303$), resultados que demuestran que una estructura de gobernanza respaldada por políticas institucionales de seguridad contribuye a que la información financiera represente de manera más fiel la realidad económica de las organizaciones, fundamentando así la aceptación de la hipótesis específica planteada (Shafa & Islam, 2025).

> **HE_2:** La gestión de activos y accesos se relaciona de forma estadísticamente significativa con la confidencialidad tributaria de la información contable.

Nurwanah (2024) aporta evidencia que sustenta la hipótesis de que la gestión de activos y accesos mantiene una relación estadísticamente significativa con la confidencialidad tributaria de la información contable, al sostener que la protección

efectiva de los sistemas depende de mecanismos capaces de restringir el acceso exclusivamente a usuarios autorizados y resguardar los activos digitales mediante controles de autenticación multifactor, cifrado y políticas de acceso basadas en roles, prácticas que reducen el riesgo de divulgación o alteración indebida de registros financieros sensibles; esta interpretación es consistente con los hallazgos de Nyombi et al. (2024), quienes señalan que la aplicación de protocolos estandarizados en la gestión de la información tributaria fortalece la protección de los datos del contribuyente frente a amenazas como el *phishing* y el *ransomware*, favoreciendo simultáneamente el cumplimiento de los marcos regulatorios relacionados con la privacidad de la información, mientras el monitoreo continuo de las transacciones permite identificar oportunamente comportamientos anómalos y disminuir la probabilidad de intrusiones que comprometan la confidencialidad de los datos, razón por la cual la adecuada gestión de activos y accesos constituye un elemento determinante para preservar el carácter reservado de la información contable y fundamenta la aceptación de la hipótesis específica planteada (Nurwanah, 2024; Nyombi et al., 2024).

> **HE_3:** La seguridad de la infraestructura se relaciona de forma estadísticamente significativa con la disponibilidad y el acceso a la información contable.

Osundare et al. (2022) aportan evidencia que sustenta la hipótesis de que la seguridad de la infraestructura mantiene una relación estadísticamente significativa con la disponibilidad y el acceso a la información contable, al demostrar que la implementación de arquitecturas de centros de datos activo-activo fortalece la continuidad operativa mediante mecanismos de redundancia, balanceo de carga y sincronización de la información en tiempo real, capacidades que permiten mantener los servicios financieros disponibles incluso durante fallos parciales o actividades de mantenimiento sin afectar el funcionamiento de los sistemas; los autores sostienen además que una infraestructura tecnológica robusta debe integrar mecanismos de cifrado de extremo a extremo, sistemas inteligentes para la detección temprana de amenazas y modelos de gestión apoyados en redes definidas por software y computación en la nube, tecnologías que incrementan la resiliencia de la plataforma tecnológica, reducen la probabilidad de interrupciones ocasionadas por ataques cibernéticos y garantizan el acceso permanente a los registros financieros necesarios para la gestión empresarial, razón por la cual la protección de la infraestructura

tecnológica constituye un factor determinante para preservar la disponibilidad de la información contable y fundamenta la aceptación de la hipótesis específica planteada (Osundare et al., 2022).

> **HE_4:** La cultura organizacional en ciberseguridad se relaciona de forma estadísticamente significativa con la confiabilidad de los reportes contables.

Kafi y Akter (2023) aportan evidencia que sustenta la hipótesis de que la cultura organizacional en ciberseguridad mantiene una relación estadísticamente significativa con la confiabilidad de los reportes contables, al demostrar que la protección de la información financiera depende no solo de la implementación de controles tecnológicos, sino también del desarrollo de una cultura institucional orientada a la seguridad, en la que la capacitación permanente, la concienciación del personal y la responsabilidad compartida fortalecen la capacidad de la organización para prevenir errores humanos y reducir la incidencia de amenazas como el *phishing* o las filtraciones de información; los autores sostienen además que la alineación con marcos internacionales como NIST favorece la adopción de buenas prácticas que preservan la integridad de los datos desde el registro de las transacciones hasta la elaboración de los estados financieros, facilitando la obtención de evidencia digital confiable para los procesos de auditoría y fortaleciendo la transparencia de la información contable, razón por la cual el fortalecimiento de la cultura organizacional en ciberseguridad constituye un factor determinante para incrementar la confiabilidad de los reportes financieros y fundamenta la aceptación de la hipótesis específica planteada (Kafi & Akter, 2023).

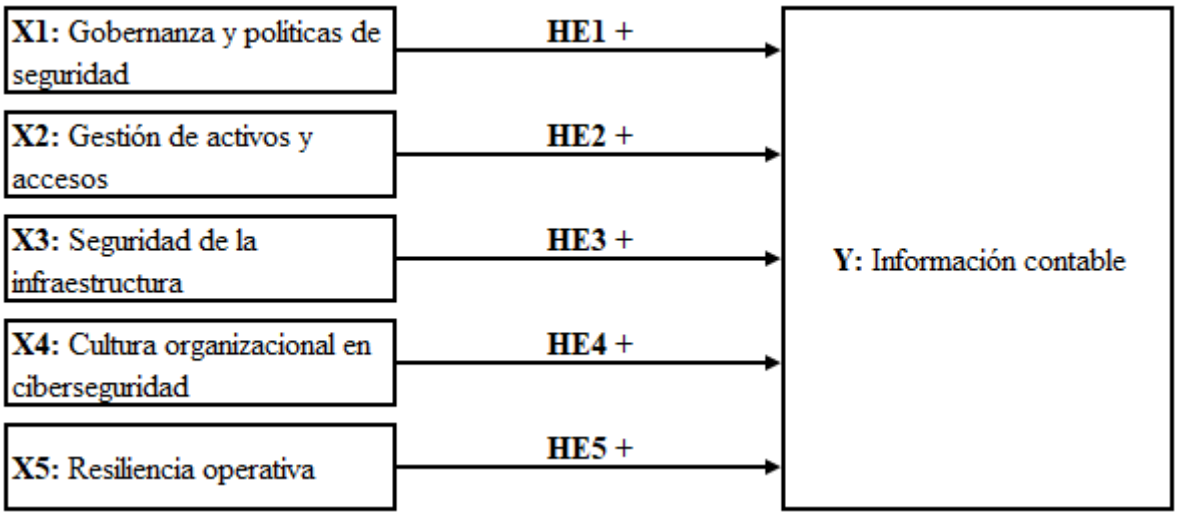
> **HE_5:** La resiliencia operativa se relaciona de forma estadísticamente significativa con el cumplimiento normativo contable y tributario.

Nyombi et al. (2024) aportan evidencia que sustenta la hipótesis de que la resiliencia operativa mantiene una relación estadísticamente significativa con el cumplimiento normativo contable y tributario, al demostrar que las organizaciones que implementan protocolos integrales de ciberseguridad, planes formales de respuesta a incidentes y mecanismos permanentes de monitoreo fortalecen su capacidad para mantener la continuidad de las operaciones frente a eventos que comprometen los sistemas de información, condición que favorece la protección de la confidencialidad, integridad y disponibilidad de los datos utilizados para atender las obligaciones contables y tributarias; en esta misma línea, Safitra et al. (2023) sostienen que la resiliencia operativa requiere integrar capacidades tecnológicas con liderazgo

organizacional y procesos de recuperación previamente planificados, mientras que Shchyrba et al. (2025) destacan que la incorporación de controles como el cifrado de la información y la autenticación multifactor incrementa la capacidad institucional para prevenir accesos no autorizados y preservar la continuidad de los servicios digitales, planteamientos que resultan consistentes con la Política Pública para la Transformación Digital del Ecuador, la cual promueve el fortalecimiento de infraestructuras tecnológicas seguras como condición para una gestión pública y empresarial confiable (MINTEL, 2025), razón por la cual la resiliencia operativa constituye un elemento determinante para asegurar el cumplimiento de las obligaciones contables y tributarias en entornos digitales y fundamenta la aceptación de la hipótesis específica planteada (Nyombi et al., 2024; Safitra et al., 2023; Shchyrba et al., 2025; MINTEL, 2025).
En consecuencia, la Figura 1 muestra el modelo teórico de la presente investigación.

Figura 1.

Modelo teórico.



Capítulo III. Marco metodológico

Enfoque y tipo de investigación

La presente investigación se desarrolló bajo el paradigma positivista, el cual parte de que los fenómenos pueden observarse, medirse y analizarse objetivamente mediante procedimientos empíricos y técnicas estadísticas, permitiendo examinar la relación existente entre las prácticas de ciberseguridad y la información contable en las empresas comercializadoras de insumos médicos de la provincia de Manabí; en concordancia con este paradigma, se adoptó un enfoque cuantitativo, debido a que posibilita recolectar información mediante un instrumento estandarizado, cuantificar las variables de estudio y analizar estadísticamente el grado de asociación entre ellas, mientras que el estudio se clasificó como correlacional porque su propósito consistió en determinar la relación existente entre la ciberseguridad y la protección y confiabilidad de la información contable, sin pretender establecer relaciones de causalidad, proporcionando evidencia objetiva para contrastar las hipótesis planteadas (Medina Romero, 2025).

Diseño de la investigación

La investigación se desarrolló bajo un diseño no experimental, debido a que las variables de estudio fueron observadas tal como se presentan en su contexto natural, sin que el investigador interviniera o manipulara deliberadamente las prácticas de ciberseguridad ni las características de la información contable de las empresas comercializadoras de insumos médicos de la provincia de Manabí; asimismo, el estudio adoptó un diseño transversal, puesto que la recolección de los datos se efectuó en un único momento del tiempo, permitiendo obtener un diagnóstico de la relación existente entre ambas variables en las condiciones reales en que se desarrollan las actividades contables y administrativas de las organizaciones, proporcionando información pertinente para el cumplimiento de los objetivos y la contrastación de las hipótesis planteadas (Medina Romero, 2025).

Población y muestra

El universo de estudio estuvo constituido por 62 empresas comercializadoras de insumos médicos registradas en la provincia de Manabí, según datos oficiales del

Servicio de Rentas Internas [SRI] (2025). Para determinar la muestra representativa se aplicó un muestreo probabilístico aleatorio simple con un nivel de confianza del 95% y un margen de error del 5%, lo cual garantizó que los resultados obtenidos pudieran generalizarse al total de la población estudiada.

El cálculo muestral arrojó un tamaño de 54 empresas, cuyos profesionales de las áreas contables y financieras participaron en el proceso de recolección de datos; estos profesionales desempeñan funciones relacionadas con el registro, procesamiento y custodia de la información contable, además de utilizar los sistemas informáticos que soportan dichos procesos. La selección aleatoria de las unidades muestrales eliminó sesgos en la conformación del grupo de estudio, permitiendo que cada organización del universo tuviera la misma probabilidad de ser incluida, este procedimiento fortaleció la representatividad de la muestra y garantizó que las conclusiones reflejaran la realidad del sector comercial de insumos médicos en la provincia de Manabí.

Técnicas e instrumentos

La técnica de la encuesta se utilizó como fuente de recolección de información, la cual permitió capturar datos cuantitativos y cualitativos de manera sistemática y rigurosa en la muestra seleccionada; el instrumento empleado consistió en un cuestionario estructurado que incluía preguntas cerradas evaluadas mediante una escala de Likert, diseñadas para cuantificar el nivel de implementación de los protocolos de seguridad y la percepción de integridad contable. Complementariamente, el estudio se apoyó en el método analítico-sintético para descomponer las dimensiones de ciberseguridad y el método histórico-lógico para comprender la evolución de las medidas de protección digital en respuesta a incidentes de seguridad previos; estos métodos y técnicas permitieron que la recolección de datos fuese pertinente y estuviera alineada con los objetivos de diagnosticar vulnerabilidades críticas en el manejo de registros sensibles.

La operacionalización de las variables se presenta en la Matriz de Operacionalización (véase Anexo 1), donde se detallan las dimensiones, indicadores e ítems considerados en el cuestionario aplicado; asimismo, el cuestionario estructurado con los 35 ítems utilizados en la investigación se incluye en el Anexo 2, lo que permite consultar íntegramente las preguntas aplicadas a la muestra seleccionada.

Validez y confiabilidad

Con el propósito de garantizar la calidad metodológica del instrumento, el cuestionario fue sometido previamente a un proceso de validación mediante juicio de expertos antes de su aplicación a la población objeto de estudio; esta etapa tuvo como finalidad determinar el grado de correspondencia entre los ítems formulados y los constructos definidos en la investigación, considerando los criterios de claridad, pertinencia y relevancia. La evaluación permitió verificar que las preguntas presentaran una formulación comprensible, fueran coherentes con los objetivos de medición y resultaran relevantes para la evaluación de las variables y dimensiones contempladas en el instrumento.

La valoración del cuestionario se llevó a cabo a través de una matriz diseñada específicamente para este fin; cada experto calificó los 35 ítems utilizando una escala ordinal de cuatro niveles, donde 1 representaba “No adecuado”, 2 “Poco adecuado”, 3 “Adecuado” y 4 “Muy adecuado”. Con base en las puntuaciones obtenidas, se calculó el coeficiente V de Aiken para cada ítem. Este estadístico cuantifica el nivel de concordancia entre los expertos respecto a la pertinencia del contenido de los ítems, siendo su valor máximo 1 (acuerdo total) y mínimo 0 (ausencia de acuerdo). La fórmula utilizada fue:

$$V = \Sigma(r - l_0) / [n(c - 1)]$$

Donde:

r = puntuación asignada por cada experto;

l_0 = puntuación mínima de la escala, correspondiente a 1;

n = número de expertos, correspondiente a 5;

c = número de categorías de respuesta, correspondiente a 4.

Los resultados obtenidos en la Tabla 1 evidenciaron un alto nivel de validez de contenido del instrumento. Los valores del coeficiente V de Aiken para las 105 evaluaciones realizadas oscilaron entre 0,800 y 1,000, mientras que el valor promedio global alcanzó V = 0,938; por criterio, se obtuvo un valor promedio de V = 0,947 para

claridad, V = 0,928 para pertinencia y V = 0,939 para relevancia. Estos resultados indican que los expertos consideraron que los ítems presentan una formulación adecuada, guardan correspondencia con los aspectos que se pretende medir y poseen relevancia suficiente para los propósitos de la investigación.

De las 105 valoraciones ítem-criterio, 85 (81,0 %) alcanzaron valores de V de Aiken iguales o superiores a 0,90, mientras que las restantes 20 (19,0 %) se ubicaron entre 0,80 y 0,89. No se registraron valores inferiores a 0,80. En consecuencia, ninguno de los 35 ítems requirió eliminación, por lo que todos fueron considerados aptos para continuar con el proceso de aplicación del instrumento. La evidencia obtenida mediante el juicio de expertos permite, por tanto, sostener que el cuestionario presenta un nivel de validez de contenido muy alto, constituyéndose en una base metodológica adecuada para su aplicación en la investigación.

Tabla 1.

V de Aiken por criterio

Criterio	**V de Aiken**	**Media**	**Interpretación**
Claridad	0.947	3.84	Muy alta
Pertinencia	0.928	3.78	Muy alta
Relevancia	0.939	3.82	Muy alta
Global	0.938	3.81	Muy alta

Nota: Criterios de validez de contenido obtenidos a partir de la valoración de los expertos.

En cuanto a la confiabilidad, debe precisarse que esta será determinada posteriormente a partir de las respuestas obtenidas de los participantes de la investigación, debido a que el juicio de expertos constituye fundamentalmente una fuente de evidencia para establecer la validez de contenido y no sustituye la evaluación de la consistencia interna del instrumento en la muestra de estudio. En consecuencia, la confiabilidad definitiva será evaluada mediante los estadísticos correspondientes una vez obtenida la base de datos de la aplicación del cuestionario.

Procedimiento

El desarrollo de la investigación se llevó a cabo mediante una secuencia de actividades orientadas al cumplimiento de los objetivos planteados; en una primera etapa se realizó la revisión y análisis de la literatura científica y de la normativa relacionada con la ciberseguridad y la información contable, lo que permitió fundamentar teóricamente el estudio y estructurar el instrumento de recolección de datos; posteriormente, se efectuó la validación del cuestionario mediante juicio de expertos y su aplicación a los profesionales de las áreas contables y financieras de las empresas comercializadoras de insumos médicos de la provincia de Manabí, procurando que el proceso de levantamiento de la información no interfiriera con el desarrollo normal de las actividades organizacionales; finalmente, los datos obtenidos fueron codificados, organizados y procesados mediante técnicas de análisis estadístico, permitiendo contrastar las hipótesis de investigación e interpretar los resultados en función de los objetivos propuestos.

Consideraciones éticas

La investigación se desarrolló conforme a los principios éticos de respeto por las personas, confidencialidad, integridad científica y responsabilidad en el manejo de la información; la participación de los profesionales de las áreas contables y financieras fue voluntaria, previa aceptación de su colaboración, garantizándose el anonimato de los participantes y la confidencialidad de la información proporcionada, la cual fue utilizada exclusivamente con fines académicos y de investigación; asimismo, los datos obtenidos fueron procesados de manera objetiva, sin alteraciones ni manipulaciones, asegurando que los resultados y conclusiones se fundamentaran únicamente en la evidencia recolectada; adicionalmente, el tratamiento de la información se realizó en concordancia con las disposiciones de la Ley Orgánica de Protección de Datos Personales (2021), respetando los principios de licitud, confidencialidad y protección de los datos personales durante todas las etapas del estudio.

Método de análisis de datos

Para el procesamiento y análisis de la información se utilizó el software RStudio, mediante el cual se organizaron, codificaron y analizaron los datos obtenidos a partir de los cuestionarios aplicados; inicialmente, se efectuó un análisis descriptivo utilizando

medidas de tendencia central y de dispersión con el propósito de caracterizar el comportamiento de las variables de estudio, posteriormente se verificó el supuesto de normalidad mediante la prueba de Kolmogorov-Smirnov con corrección de *Lilliefors*, a fin de determinar la técnica estadística más adecuada para la contrastación de las hipótesis y, una vez comprobado el cumplimiento de dicho supuesto, se aplicó el coeficiente de correlación de Pearson para establecer el grado de asociación entre la ciberseguridad y la información contable, considerando un nivel de significancia de $\alpha = 0,05$, procedimiento que permitió realizar un análisis objetivo y consistente con el enfoque cuantitativo y el diseño correlacional de la investigación.

Capítulo IV. Resultados y discusión

Presentación de resultados

La descripción estadística de las variables permite identificar diferencias en el comportamiento de la ciberseguridad y de la información contable dentro de las empresas comercializadoras de insumos médicos de la provincia de Manabí; los resultados que se observan en la Tabla 2 muestran que la variable Ciberseguridad alcanzó una media de 3,009 y una desviación estándar de 0,951, evidenciando un nivel moderado de implementación acompañado de una variabilidad relativamente elevada entre las respuestas, mientras que la variable Información contable registró una media de 3,795 y una desviación estándar de 0,655, reflejando una valoración más alta y una mayor homogeneidad en la percepción de los participantes respecto de la calidad de la información generada, resultados que permiten caracterizar el comportamiento inicial de ambas variables y constituyen la base para los análisis inferenciales desarrollados posteriormente.

Tabla 2.

Estadísticos descriptivos de los constructos.

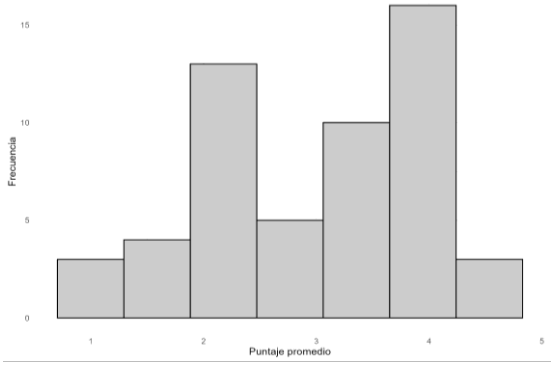
Constructo	Media	Mediana	Desv.	Mínimo	Maximo	Asimetría	Curtosis
Ciberseguridad	3.009	3.133	0.951	1.000	4.533	-0.349	-0.840
Información contable	3.795	3.867	0.655	2.267	5.000	-0.287	-0.629

Nota. Elaboración propia a partir del análisis realizado en RStudio.

La Figura 2 presenta la distribución de los puntajes correspondientes al constructo Ciberseguridad, observándose una dispersión apreciable de las respuestas a lo largo de la escala de medición; el histograma muestra una distribución de frecuencias consistente con la variabilidad identificada en los estadísticos descriptivos, reflejando diferencias en la percepción de los participantes respecto al nivel de implementación de las prácticas de ciberseguridad en las empresas analizadas.

Figura 2.

Histograma de la distribución del constructo ciberseguridad.

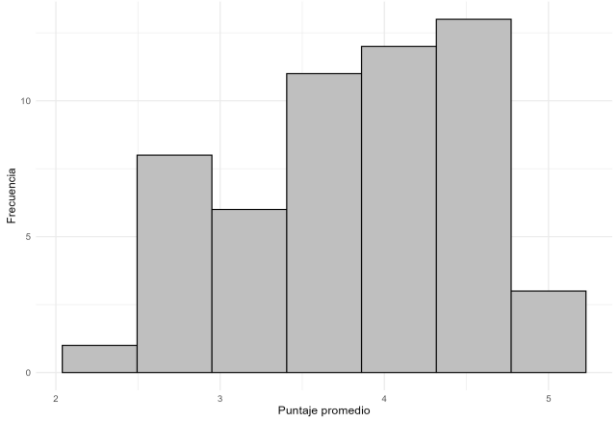


Nota. Distribución de los puntajes promedio del constructo ciberseguridad en una escala Likert de 1 a 5. Elaboración propia a partir del análisis realizado en RStudio.

La Figura 3 muestra la distribución de los puntajes del constructo Información contable, apreciándose una mayor concentración de las respuestas en los niveles superiores de la escala; el histograma evidencia una menor dispersión en comparación con el constructo Ciberseguridad, comportamiento que resulta consistente con los estadísticos descriptivos obtenidos para esta variable y refleja una mayor homogeneidad en las respuestas de los participantes.

Figura 3.

Histograma de distribución del constructo información contable.



Nota. Distribución de los puntajes promedio del constructo información contable en una escala Likert de 1 a 5. Elaboración propia a partir del análisis realizado en RStudio.

Análisis de normalidad

Con el propósito de determinar la prueba estadística adecuada para la contrastación de las hipótesis, se evaluó la distribución de los datos mediante la prueba de Kolmogorov-Smirnov con corrección de *Lilliefors*; los resultados presentados en la Tabla 3 muestran valores de significancia de p=0,087 para la variable Ciberseguridad y p=0,316 para la variable Información contable, ambos superiores al nivel de

significancia establecido (α = 0,05), por lo que no se rechazó la hipótesis de normalidad y se concluyó que los datos presentan una distribución compatible con la normalidad, condición que justificó la utilización de pruebas estadísticas paramétricas para el análisis de la relación entre las variables.

Tabla 3.

Prueba de normalidad de Kolmogorov-Smirnov (Lilliefors).

Constructo	Estadístico	p_value	Distribución normal	Decisión
Ciberseguridad	0.112	0.087	Sí	No se rechaza la hipótesis de normalidad.
Información contable	0.091	0.316	Sí	No se rechaza la hipótesis de normalidad.

Nota. Se aplicó la prueba de Kolmogorov-Smirnov con corrección de Lilliefors debido a que el tamaño de la muestra (n = 54) fue superior a 50 observaciones. Elaboración propia a partir del análisis realizado en RStudio.

Análisis e interpretación

La Tabla 4 presenta los resultados del análisis de correlación realizado para contrastar la hipótesis general de la investigación; el coeficiente de correlación de Pearson obtenido fue de r = 0,421, valor que evidencia una asociación positiva de magnitud moderada entre la ciberseguridad y la información contable en las empresas comercializadoras de insumos médicos de la provincia de Manabí, mientras que el nivel de significancia (p = 0,002) fue inferior al nivel establecido (α = 0,05), resultado que permitió rechazar la hipótesis nula y aceptar la hipótesis general de investigación, concluyendo que existe una relación estadísticamente significativa entre ambas variables dentro de la muestra analizada.

Dado que la investigación corresponde a un diseño correlacional, no experimental y de corte transversal, los resultados evidencian únicamente la existencia de una asociación estadísticamente significativa, sin que ello implique una relación de causalidad entre las variables; adicionalmente, el intervalo de confianza del 95 %, comprendido entre 0,173 y 0,619, respalda la estabilidad de la estimación obtenida y confirma que la relación identificada mantiene una magnitud moderada, por lo que la

información contable puede estar influenciada, además, por otros factores organizacionales que no forman parte del presente estudio.

Tabla 4.

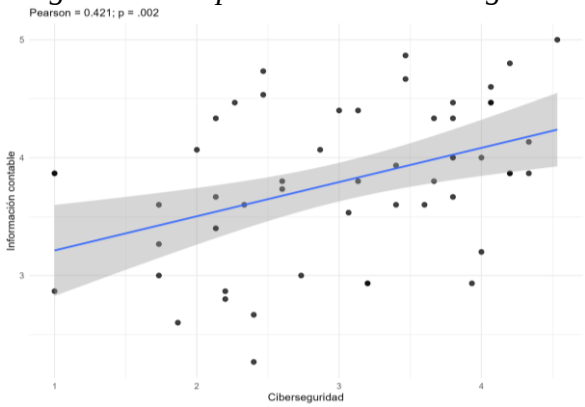
Tabla de Correlación de Pearson.

Variables	Método	Coeficiente (rho)	p_value
Ciberseguridad - Información contable	Pearson	0.421	0.002

Nota. Se aplicó el coeficiente de correlación de Pearson con un nivel de confianza del 95%. Elaboración propia a partir del análisis realizado en RStudio.

Figura 4.

Diagrama de dispersión entre ciberseguridad e información contable.



Nota. Representación de la observación de la muestra y línea de tendencia de la relación lineal entre los puntajes promedio de ciberseguridad e información contable. Elaboración propia a partir de los resultados de la encuesta.

Discusión

La presente investigación tuvo como propósito determinar la relación entre las prácticas de ciberseguridad y la protección y confiabilidad de la información contable en las empresas comercializadoras de insumos médicos de la provincia de Manabí; los resultados evidenciaron una relación positiva, moderada y estadísticamente significativa entre ambas variables (r = .421; p = .002), por lo que se aceptó la hipótesis general de investigación. Este hallazgo indica que, dentro de la muestra analizada, las empresas que reportan mejores prácticas de ciberseguridad tienden también a presentar mayores niveles percibidos de protección, integridad y confiabilidad de su información contable; sin embargo, debido al diseño correlacional, no experimental y de corte transversal, estos resultados deben interpretarse como una asociación estadísticamente significativa y no como evidencia de una relación causal.

En el contexto de las empresas comercializadoras de insumos médicos de la provincia de Manabí, los resultados permiten comprender que la confiabilidad de la información contable no depende únicamente del cumplimiento de procedimientos contables y tributarios, sino también de la existencia de controles tecnológicos y organizacionales que contribuyen a proteger los registros financieros. Entre estos controles destacan la gestión de accesos, la protección de credenciales, los mecanismos de respaldo, la disponibilidad de los sistemas y la capacitación del personal; en consecuencia, la ciberseguridad debe entenderse como un componente complementario del sistema de control interno que fortalece el procesamiento, almacenamiento y conservación de la información financiera coincidiendo esta interpretación con el planteamiento de Guamán (2023), quien sostiene que la gestión de riesgos debe integrar medidas destinadas a preservar la confidencialidad, integridad y disponibilidad de la información institucional.

La relación observada puede explicarse porque los controles de seguridad favorecen la trazabilidad de las operaciones y delimitan las responsabilidades de los usuarios que interactúan con los sistemas contables; la utilización de cuentas individuales, permisos basados en funciones, autenticación segura y registros de auditoría contribuye a reducir el riesgo de accesos indebidos y modificaciones no autorizadas. Asimismo, las copias de seguridad, la actualización de los sistemas y los procedimientos de recuperación favorecen la continuidad operativa frente a fallos técnicos o incidentes de ciberseguridad; no obstante, la magnitud moderada de la correlación indica que la confiabilidad de la información contable también puede estar asociada con otros factores organizacionales, como la calidad del control interno, la adecuada segregación de funciones, la capacitación profesional, la supervisión administrativa y el cumplimiento de la normativa contable y tributaria por lo que no resulta metodológicamente adecuado atribuir la calidad de la información financiera únicamente al nivel de ciberseguridad percibido por los participantes.

Los resultados obtenidos son consistentes con la evidencia reportada por Shafa y Islam (2025), quienes identificaron que la madurez de la gobernanza de datos y de la ciberseguridad fortalece los controles internos de los sistemas de información contable y favorece la transparencia de los reportes financieros; de manera similar, Nurwanah (2024) señala que la gestión estratégica de la ciberseguridad, mediante controles de acceso y protección de activos digitales, contribuye a preservar la confidencialidad de la

información financiera y tributaria. Asimismo, Kafi y Akter (2023) destacan que la protección de la información no depende exclusivamente de herramientas tecnológicas, sino también de una cultura organizacional basada en la capacitación continua, la concienciación del personal y la adopción de buenas prácticas de seguridad; en conjunto, estos antecedentes respaldan la interpretación de que la ciberseguridad constituye un proceso integral en el que convergen factores tecnológicos, organizacionales y humanos.

También se identifican coincidencias con investigaciones desarrolladas en Ecuador. Calle y Andrade (2024) evidenciaron que las empresas comerciales enfrentan riesgos relacionados con *malware*, accesos no autorizados y deficiencias en la evaluación periódica de la seguridad informática, situaciones que pueden afectar la integridad de la información utilizada para la toma de decisiones; de igual forma, López y Ordóñez (2024) identificaron limitaciones en los planes de respuesta a incidentes y en las auditorías de seguridad implementadas por organizaciones comerciales; no obstante, el presente estudio difiere de estos trabajos porque no evaluó la ocurrencia de incidentes específicos ni la eficacia técnica de controles particulares, sino la percepción de los profesionales responsables del manejo de la información contable. Además, mientras las investigaciones previas enfatizan las vulnerabilidades existentes, los resultados obtenidos muestran que la información contable fue valorada favorablemente aun cuando las prácticas de ciberseguridad alcanzaron únicamente un nivel moderado, lo que sugiere que la confiabilidad percibida también puede estar influenciada por procedimientos administrativos y contables consolidados dentro de las organizaciones.

Los resultados descriptivos complementan esta interpretación en donde la variable información contable presentó una media superior y una menor dispersión respecto a la ciberseguridad, lo que evidencia una percepción más homogénea sobre la calidad de los registros financieros; en contraste, la mayor variabilidad observada en la ciberseguridad refleja diferencias entre las empresas en aspectos como la formalización de políticas, el control de accesos, la protección de la infraestructura tecnológica, la capacitación del personal y las estrategias de continuidad operativa. Esta situación pone de manifiesto la existencia de distintos niveles de madurez en la gestión de la seguridad digital dentro del sector analizado. En este sentido, el enfoque de gestión de la exposición propuesto por Pacheco y Staino (2025) resulta pertinente al destacar la

necesidad de identificar y reducir vulnerabilidades antes de que comprometan los activos informativos de la organización.

Desde el punto de vista teórico, la investigación aporta evidencia empírica sobre la relación entre la ciberseguridad y la información contable en empresas comercializadoras de insumos médicos de la provincia de Manabí, un contexto poco abordado por la literatura nacional; los resultados respaldan los postulados de la teoría de los sistemas de información contable y del Marco de Ciberseguridad del NIST (2024), al mostrar que la gobernanza, la protección, la detección, la respuesta y la recuperación constituyen elementos relacionados con la preservación de la información financiera, los hallazgos son coherentes con la teoría de la agencia al sugerir que el fortalecimiento de los controles digitales contribuye a reducir riesgos asociados con el acceso, la modificación o la divulgación indebida de información relevante para la toma de decisiones; no obstante, estas interpretaciones deben entenderse como consistentes con el marco teórico utilizado y no como demostraciones de relaciones causales.

Desde una perspectiva práctica, los resultados sugieren que las empresas participantes deberían fortalecer progresivamente sus controles de ciberseguridad en coordinación con sus procesos contables y tributarios; entre las acciones recomendadas se encuentran la formalización de políticas de seguridad, la revisión periódica de los permisos de acceso, la implementación de autenticación multifactor cuando resulte técnicamente viable, la realización de respaldos periódicos y la capacitación continua del personal sobre protección de información y prevención de amenazas digitales. Estas acciones requieren el compromiso de la alta dirección y la coordinación entre las áreas administrativas, contables y tecnológicas, ya que la ciberseguridad constituye una responsabilidad institucional y no exclusivamente informática; esta recomendación es consistente con los lineamientos de la Política Pública para la Transformación Digital del Ecuador (MINTEL, 2025), que promueve el fortalecimiento de infraestructuras digitales seguras como parte del proceso de modernización organizacional.

Los resultados deben interpretarse considerando las limitaciones del estudio; como la muestra estuvo conformada por 54 participantes seleccionados mediante un muestreo no probabilístico por conveniencia, lo que limita la generalización de los hallazgos a otros sectores económicos o regiones del país; además, el diseño transversal únicamente permitió analizar la relación entre las variables en un momento específico,

sin evaluar su evolución en el tiempo; el instrumento recopiló percepciones de los participantes, las cuales pueden estar influenciadas por sus experiencias y conocimientos sobre las prácticas de seguridad existentes en sus organizaciones. En futuras investigaciones sería conveniente ampliar el tamaño de la muestra, incorporar diferentes sectores productivos, utilizar diseños longitudinales y complementar los cuestionarios con auditorías documentales, evaluación técnica de controles y análisis de incidentes reales de ciberseguridad.

En síntesis, la investigación demuestra la existencia de una relación positiva y estadísticamente significativa entre la ciberseguridad y la información contable en las empresas comercializadoras de insumos médicos de la provincia de Manabí; aunque los resultados no permiten establecer una relación de causa y efecto, sí respaldan la importancia de integrar controles tecnológicos, organizacionales y humanos como parte del sistema de control interno orientado a proteger la información financiera; en consecuencia, la principal contribución del estudio consiste en aportar evidencia empírica que respalda la incorporación de la ciberseguridad como un componente relevante para fortalecer la protección, confiabilidad y continuidad de los procesos contables dentro del entorno empresarial.

Capítulo V. Conclusiones, recomendaciones y propuesta

Conclusiones

La presente investigación cumplió el objetivo general de determinar la relación entre las prácticas de ciberseguridad y la protección y confiabilidad de la información contable en las empresas comercializadoras de insumos médicos de la provincia de Manabí; los resultados obtenidos permitieron establecer la existencia de una relación positiva, moderada y estadísticamente significativa entre ambas variables, razón por la cual se aceptó la hipótesis general de investigación; en consecuencia, las empresas cuyos profesionales perciben un mayor nivel de implementación de prácticas de ciberseguridad también tienden a percibir mejores condiciones de protección, integridad, disponibilidad, confidencialidad y confiabilidad de la información contable; sin embargo, esta conclusión debe interpretarse dentro de los límites propios de un estudio cuantitativo de alcance correlacional, diseño no experimental y corte transversal, por lo que la evidencia obtenida permite afirmar la existencia de una asociación significativa entre las variables, mas no una relación de causa y efecto.

Desde el punto de vista metodológico, la investigación se desarrolló mediante un enfoque cuantitativo que permitió medir objetivamente las variables objeto de estudio y analizar su comportamiento a través de procedimientos estadísticos; la información fue recopilada mediante un cuestionario estructurado con escala de Likert aplicado a 54 profesionales de las áreas contables y financieras de empresas comercializadoras de insumos médicos de la provincia de Manabí, mientras que la comprobación de la normalidad mediante la prueba de Kolmogorov-Smirnov con corrección de *Lilliefors* justificó la utilización del coeficiente de correlación de Pearson para contrastar la hipótesis general. El resultado obtenido ($r = 0.421$; $p = 0.002$) evidenció una relación positiva de magnitud moderada entre la ciberseguridad y la información contable, proporcionando evidencia estadística suficiente para sustentar las conclusiones del estudio y garantizar la consistencia del análisis inferencial realizado.

El principal hallazgo científico demuestra que la ciberseguridad constituye un componente relevante del entorno de control que respalda la gestión de la información contable dentro de las organizaciones analizadas, puesto que la protección de los registros financieros no depende exclusivamente de la correcta aplicación de

procedimientos contables y tributarios, sino también de las condiciones tecnológicas y organizacionales bajo las cuales la información es registrada, procesada, almacenada y consultada. En este sentido, la existencia de políticas de seguridad, mecanismos adecuados de control de accesos, protección de credenciales, actualización de la infraestructura tecnológica, realización de copias de seguridad y capacitación permanente del personal representan prácticas que favorecen un manejo más seguro de la información financiera; no obstante, la magnitud moderada de la correlación también evidencia que la confiabilidad de la información contable está asociada con otros factores institucionales, entre ellos la calidad del control interno, la segregación de funciones, la supervisión administrativa, la competencia técnica del personal y el cumplimiento de la normativa contable y tributaria.

El análisis descriptivo permitió identificar que la información contable presentó una valoración más favorable y homogénea que la variable ciberseguridad, mientras que esta última mostró un nivel moderado y una mayor variabilidad entre las empresas participantes; este comportamiento sugiere que las organizaciones conceden especial importancia al registro de las operaciones financieras y al cumplimiento de sus obligaciones contables y tributarias; sin embargo, todavía existen diferencias importantes en el grado de desarrollo de los controles digitales que respaldan dichos procesos. En consecuencia, una percepción favorable sobre la calidad de la información contable no debe interpretarse como evidencia de ausencia de riesgos tecnológicos, sino como un indicio de que aún existen oportunidades para fortalecer aspectos relacionados con la gobernanza de la seguridad, la gestión de accesos, la protección de la infraestructura tecnológica, la cultura organizacional y la resiliencia operativa, dimensiones que fueron consideradas dentro del modelo teórico desarrollado en esta investigación.

El estudio aporta evidencia empírica sobre la relación existente entre la ciberseguridad y la información contable en un contexto empresarial específico de la provincia de Manabí, contribuyendo a ampliar el conocimiento disponible sobre esta temática en el ámbito nacional; los resultados obtenidos son consistentes con los planteamientos de Shafa y Islam (2025), quienes sostienen que la madurez de la ciberseguridad y de los controles de los sistemas de información contable favorece la transparencia y confiabilidad de los reportes financieros; asimismo, guardan concordancia con el enfoque propuesto por el (NIST, 2024), el cual reconoce la

gobernanza, la protección, la detección, la respuesta y la recuperación como funciones esenciales para preservar los activos de información; desde esta perspectiva, la investigación fortalece la integración entre la gestión contable y la gestión de riesgos digitales, ofreciendo evidencia útil para futuras investigaciones desarrolladas en organizaciones comerciales ecuatorianas.

En el ámbito organizacional, los resultados permiten concluir que la ciberseguridad debe asumirse como una responsabilidad institucional compartida entre la alta dirección, el personal contable y las áreas responsables de la tecnología de la información, ya que la protección de los registros financieros requiere tanto controles técnicos como procedimientos administrativos claramente definidos; en consecuencia, las empresas deberían fortalecer progresivamente sus políticas de seguridad, revisar periódicamente los privilegios de acceso, implementar mecanismos de autenticación reforzada cuando resulte técnicamente viable, mantener programas sistemáticos de copias de seguridad y desarrollar procesos continuos de capacitación orientados a la prevención del *phishing*, la protección de credenciales y el manejo seguro de la información financiera. Estas acciones pueden contribuir al fortalecimiento del control interno digital y favorecer la conservación de evidencia contable útil para fines administrativos, tributarios y de auditoría, en concordancia con las orientaciones nacionales sobre transformación digital impulsadas por el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL, 2025).

Las conclusiones alcanzadas deben interpretarse considerando las limitaciones metodológicas propias del estudio; en primer lugar, la muestra estuvo conformada por 54 profesionales seleccionados mediante un muestreo no probabilístico por conveniencia, circunstancia que limita la posibilidad de generalizar los resultados hacia otras empresas, sectores económicos o provincias del país; adicionalmente, el diseño transversal permitió analizar las variables en un único momento, sin evaluar su evolución a lo largo del tiempo ni los posibles efectos derivados de la implementación de nuevos controles de ciberseguridad. Del mismo modo, la información obtenida provino de las percepciones de los participantes mediante un cuestionario estructurado, por lo que no se incorporaron auditorías técnicas, pruebas de vulnerabilidad, análisis de incidentes reales o revisión documental de políticas institucionales que complementaran la evaluación de los controles implementados.

Finalmente, se recomienda que futuras investigaciones amplíen la cobertura geográfica y sectorial mediante muestras probabilísticas, incorporen diseños longitudinales que permitan evaluar la evolución de las prácticas de ciberseguridad y complementen la información obtenida mediante encuestas con auditorías de sistemas, análisis de vulnerabilidades, revisión documental y evaluación objetiva de los controles tecnológicos implementados por las organizaciones; asimismo, resultaría pertinente analizar el efecto de variables como el control interno, la cultura organizacional, la capacitación del personal, el cumplimiento normativo y la adopción de sistemas contables en la nube sobre la calidad de la información financiera. En síntesis, la investigación demuestra que la ciberseguridad mantiene una relación positiva y estadísticamente significativa con la protección y confiabilidad de la información contable en las empresas comercializadoras de insumos médicos de la provincia de Manabí, lo que respalda su incorporación como un componente estratégico del sistema de control interno y de la gestión administrativa, contable y tributaria de las organizaciones, contribuyendo así al fortalecimiento de la confianza en la información financiera y al desarrollo de procesos empresariales más seguros y sostenibles.

Recomendaciones

En función de los resultados obtenidos y las conclusiones del estudio, se recomienda a la alta dirección y a los responsables financieros de las comercializadoras de insumos médicos de Manabí fortalecer sus políticas de gobernanza digital; de manera fundamental en las empresas que aún no cuentan con manuales de seguridad formalizados procedan con su elaboración y socialización periódica entre el personal contable; la asignación de recursos debe priorizar controles básicos pero efectivos, tales como la implementación obligatoria de la autenticación de doble factor (MFA) para el acceso a sistemas contables y la delimitación estricta de permisos según los roles y responsabilidades de cada usuario en el área financiera.

Asimismo, se sugiere integrar la capacitación en ciberseguridad dentro de los programas de formación continua para el personal administrativo y contable; dado que el factor humano es un componente crítico en la protección de datos, estas capacitaciones deben enfocarse en la detección de amenazas comunes, como el *phishing*, y en el manejo seguro de credenciales de acceso; de igual manera, es recomendable que las organizaciones establezcan planes básicos de continuidad del negocio y realicen respaldos periódicos de la información contable en ubicaciones

seguras, asegurando así que los registros financieros permanezcan disponibles y protegidos frente a fallos técnicos o incidentes de seguridad inesperados.

Desde la perspectiva académica y científica, se recomienda a futuros investigadores ampliar el tamaño de la muestra e incluir empresas de otros sectores comerciales de la provincia de Manabí para realizar análisis comparativos; también resultaría valioso desarrollar estudios con un enfoque cualitativo que exploren las barreras organizacionales y financieras que limitan la inversión en ciberseguridad dentro de las PYMES. Finalmente, se propone realizar investigaciones que analicen la relación entre la ciberseguridad y otras variables del control interno contable, con el fin de obtener una visión más integral de los factores que determinan la confiabilidad de la información financiera en el entorno digital ecuatoriano.

Propuesta

Plan de fortalecimiento de controles digitales para la protección de registros contables en empresas comercializadoras de insumos médicos de la provincia de Manabí

Justificación

El diagnóstico realizado evidencia que, aunque existe una alta confianza en la información contable, esta reposa sobre infraestructuras digitales con brechas críticas de inversión (66,7 % invierte menos de $1000 anuales) y una alarmante falta de auditorías periódicas (80 %). Por tanto, es imperativo transitar de un enfoque de protección reactiva a uno de ciberdefensa activa y gestión de la exposición.

La propuesta responde a las dimensiones consideradas en la operacionalización de la variable ciberseguridad: gobernanza y políticas, gestión de activos y accesos, seguridad de la infraestructura, cultura organizacional y resiliencia operativa; su finalidad no es sustituir los procedimientos contables ni implementar soluciones tecnológicas complejas que excedan las posibilidades de las empresas participantes. Por el contrario, busca establecer acciones prácticas, comprensibles y aplicables por la alta dirección, el personal contable y los responsables de los sistemas informáticos; la implementación gradual de estos controles puede contribuir a reducir vulnerabilidades relacionadas con accesos no autorizados, pérdida de información, alteración de registros y suspensión de actividades contables. De esta manera, se procura complementar el

control interno contable mediante medidas básicas de seguridad digital ajustadas a la realidad organizacional de las comercializadoras de insumos médicos de Manabí.

Objetivo

Fortalecer los controles digitales relacionados con la protección de los registros contables en las empresas comercializadoras de insumos médicos de la provincia de Manabí, mediante acciones de gobernanza, control de accesos, protección de infraestructura, capacitación del personal y continuidad operativa.

Beneficiarios

Los beneficiarios directos de la propuesta son los profesionales que intervienen en los procesos contables, financieros, tributarios y administrativos de las empresas comercializadoras de insumos médicos de la provincia de Manabí; también se incluyen los responsables de tecnología o las personas encargadas de administrar los sistemas contables, debido a que participan en la configuración de accesos, respaldos y mecanismos de protección de la información. Como beneficiarios indirectos se encuentran los gerentes, propietarios, proveedores, clientes, organismos de control y demás grupos de interés que requieren información contable o tributaria confiable; el fortalecimiento de los controles digitales puede favorecer la conservación, disponibilidad y trazabilidad de los registros utilizados en la gestión empresarial. Asimismo, contribuye a que las organizaciones dispongan de mejores condiciones para responder ante situaciones que afecten sus sistemas de información.

Estructura de la propuesta

La propuesta se organiza en cinco componentes interrelacionados; cada componente se vincula con una dimensión de la variable ciberseguridad evaluada en la investigación y plantea actividades de aplicación gradual, las acciones propuestas pueden ser adaptadas de acuerdo con el tamaño, los recursos disponibles y el nivel de digitalización de cada empresa. La responsabilidad de su ejecución debe recaer en la alta dirección, en coordinación con el área contable y con la persona responsable de los sistemas tecnológicos; la revisión periódica de las medidas permitirá identificar avances, dificultades y necesidades de ajuste; de esta manera, la propuesta se concibe

como una guía práctica para mejorar progresivamente la protección de los registros contables.

Componente 1. Gobernanza y políticas de seguridad

El primer componente consiste en establecer lineamientos internos que orienten el uso seguro de la información contable y tributaria; cada empresa debería contar con un documento sencillo que defina responsabilidades, normas de acceso, uso adecuado de contraseñas, manejo de archivos financieros, realización de respaldos y procedimiento de reporte de incidentes. Este documento debe ser aprobado por la gerencia y socializado con todo el personal que tenga contacto con registros contables o sistemas financieros, la política debe evitar términos excesivamente técnicos y emplear instrucciones claras, de modo que pueda ser comprendida y aplicada por los usuarios contables y administrativos. También es recomendable revisar el documento al menos una vez por año o cuando la empresa incorpore nuevos sistemas, procesos o modalidades de trabajo; la formalización de estas directrices facilita que la protección de la información sea asumida como una responsabilidad organizacional y no exclusivamente tecnológica.

Componente 2. Gestión de activos y accesos

El segundo componente se orienta a controlar quién puede ingresar a los sistemas contables y qué acciones puede realizar dentro de ellos; cada trabajador debe disponer de un usuario individual, evitando el uso compartido de claves de acceso, ya que esta práctica dificulta identificar responsabilidades ante errores, modificaciones o incidentes. Los permisos deben asignarse según las funciones de cada puesto; por ejemplo, el personal encargado de registrar transacciones no necesariamente debe contar con autorización para modificar configuraciones, eliminar información o aprobar procesos sensibles; cuando el sistema contable o financiero lo permita, se recomienda activar la autenticación de doble factor para reforzar la verificación de identidad. Además, los accesos deben revisarse de forma periódica, especialmente cuando un trabajador cambia de cargo, se ausenta temporalmente o finaliza su relación laboral, estas medidas fortalecen la trazabilidad de las operaciones y reducen el riesgo de accesos no autorizados a la información contable.

Componente 3. Seguridad de la infraestructura tecnológica

El tercer componente se relaciona con la protección básica de los equipos, programas, redes y medios de almacenamiento utilizados para procesar la información contable; las empresas deben procurar que los equipos destinados a actividades financieras cuenten con actualizaciones vigentes de sus sistemas operativos y programas, así como con herramientas de protección contra software malicioso. También se recomienda mantener separados, cuando sea posible, los accesos administrativos de los accesos utilizados para las tareas contables diarias; la red de la empresa debe contar con contraseñas seguras y evitar conexiones no autorizadas que puedan exponer los equipos donde se almacenan documentos financieros o tributarios; en el caso de archivos que contengan información sensible, se deben aplicar mecanismos de protección disponibles en las herramientas utilizadas por la organización. Estas acciones no eliminan completamente los riesgos digitales, pero contribuyen a mejorar las condiciones de seguridad de la infraestructura que sustenta los procesos contables.

Componente 4. Cultura organizacional de ciberseguridad

El cuarto componente busca fortalecer los conocimientos y hábitos del personal, considerando que muchas situaciones de riesgo se producen por errores involuntarios en el uso de correos electrónicos, contraseñas, archivos adjuntos o dispositivos externos; se propone realizar capacitaciones periódicas y breves dirigidas al personal contable, financiero y administrativo. Los contenidos deben abordar temas prácticos, tales como la creación de contraseñas seguras, la identificación de mensajes fraudulentos, el cuidado de documentos financieros, el uso responsable de dispositivos y la importancia de reportar oportunamente cualquier situación inusual; las capacitaciones pueden complementarse con recordatorios internos, guías sencillas y ejercicios de verificación de conocimientos. Es importante que estas actividades no se enfoquen en sancionar al personal, sino en promover una cultura preventiva y de corresponsabilidad; la participación de la alta dirección resulta esencial para demostrar que la protección de los datos contables constituye una prioridad institucional.

Componente 5. Resiliencia operativa y continuidad de la información contable

El quinto componente se orienta a preservar la disponibilidad de la información contable ante fallos técnicos, errores humanos, pérdida de equipos o incidentes de seguridad; se recomienda establecer un procedimiento básico de respaldo que defina qué información debe copiarse, con qué frecuencia, quién es responsable de verificar el proceso y dónde se almacenarán las copias de seguridad. Los respaldos deben mantenerse en una ubicación distinta al equipo principal o mediante un servicio de almacenamiento seguro que permita recuperar la información si ocurre un incidente; asimismo, cada empresa debe definir un procedimiento de respuesta que indique las acciones iniciales frente a situaciones como pérdida de acceso al sistema, eliminación accidental de archivos, infección por software malicioso o sospecha de ingreso no autorizado; el procedimiento debe incluir la comunicación inmediata a los responsables, la preservación de evidencias y la recuperación de la información mediante los respaldos disponibles. La realización de pruebas periódicas permitirá verificar que las copias de seguridad puedan ser utilizadas efectivamente cuando se requieran.

Plan de implementación

La aplicación de la propuesta puede desarrollarse durante un período inicial de seis meses, mediante actividades secuenciales que permitan a las empresas avanzar de forma ordenada; la duración puede ajustarse según la disponibilidad de recursos, el tamaño de la organización y el estado actual de sus controles digitales; durante todo el proceso, la gerencia debe supervisar el cumplimiento de las actividades y procurar la participación del personal contable y de los responsables tecnológicos. El seguimiento debe documentarse mediante registros sencillos que demuestren las acciones ejecutadas; al finalizar el período inicial, se recomienda realizar una evaluación interna para identificar los controles implementados, las dificultades encontradas y las acciones pendientes. Esta evaluación permitirá mantener la propuesta como un proceso de mejora continua.

Indicadores de seguimiento

Para verificar el avance de la propuesta, cada empresa puede utilizar indicadores sencillos que permitan medir el cumplimiento de las actividades programadas; estos indicadores no buscan evaluar técnicamente la totalidad de la ciberseguridad organizacional, sino facilitar el control de las acciones básicas planteadas. La revisión

puede realizarse mensualmente durante la fase de implementación y, posteriormente, de forma trimestral o semestral; los resultados deben ser conocidos por la gerencia y por los responsables de las áreas involucradas, el uso de evidencias documentales permitirá demostrar la continuidad de los controles y respaldar la adopción de decisiones de mejora.

Referencias bibliográficas

Agudelo Quevedo, K. L. (2023). Efectos de incorporar el enfoque de contabilidad tridimensional para el reconocimiento y contabilización de los costos ambientales en las organizaciones tradicionales. https://hdl.handle.net/20.500.14625/38325 La - Spanish

Amos Nyombi, Wycliff Nagalila, Babrah Happy, Mark Sekinobe, & Jimmy Ampe. (2024). Enhancing cybersecurity protocols in tax accounting practices: Strategies for protecting taxpayer information. World Journal of Advanced Research and Reviews, 23(3), 1788-1798. https://doi.org/10.30574/wjarr.2024.23.3.2838

Código Orgánico Integral Penal, Registro Oficial Suplemento 180 Oficio No. SAN (2014).

Constitución de la República del Ecuador, Registro Oficial 449 (2008). https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/02/Constitucion-de-la-Republica-del-Ecuador_act_ene-2021.pdf

Enríquez Guerrón, J. A. (2025). Esquema de seguridad de la información para comunidades indígenas en las zonas rurales de Otavalo: Alineación con las normas ISO 27002, el Código Orgánico Integral Penal (COIP) y la Ley Orgánica de Protección de Datos Personales (LOPDP) en Ecuador [Tesis de maestría]. Universidad Tecnológica Israel.

Guachún-Orellana, P. V., & Andrade-Amoroso, R. P. (2024). Medidas de ciberseguridad aplicadas a los softwares contables en las PYMES de Cuenca, Ecuador. CIENCIAMATRIA, 10(2), 168-187. https://doi.org/10.35381/cm.v10i2.1324

Gutiérrez-Navarro, C. F. (2025). Transformación Digital en la Contabilidad y Prácticas Empresariales. Revista Docentes 2.0, 18(2), 287-302. https://doi.org/10.37843/rted.v18i2.719

José Manuel Guamán Guamán. (2023). Análisis de riesgos y amenazas de ciberseguridad en el estado ecuatoriano, utilizando la metodología Magerit [Trabajo de titulación (Ingeniería en Sistemas de Información), Universidad Católica de Cuenca]. https://dspace.ucacue.edu.ec/handle/ucacue/16301

Kafi, M. A., & Akter, N. (2023). Securing Financial Information in the Digital Realm: Case Studies in Cybersecurity for Accounting Data Protection. American Journal of Trade and Policy, 10(1), 15-26. https://doi.org/10.18034/ajtp.v10i1.659

Kar Yee, C., & Zolkipli, M. F. (2021). Review on Confidentiality, Integrity and Availability in Information Security. Journal of ICT in Education, 8(2), 34-42. https://doi.org/10.37134/jictie.vol8.2.4.2021

Ley de Comercio Electrónico, Firmas y Mensajes de Datos, Ley 67 Registro Oficial Suplemento 557 (2002).

Ley Orgánica de Protección de Datos Personales, Registro Oficial Quinto Suplemento N° 459 1 (2021). https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Ley-Organica-de-Datos-Personales.pdf

López-Anchala, K. A., & Ordóñez-Parra, Y. L. (2024). 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]. Revista Multidisciplinaria Perspectivas Investigativas, 4(especial), 14-27. https://doi.org/10.62574/rmpi.v4iespecial.154

Mancheno Román, C. A. (2024). Impacto de las regulaciones de seguridad de la información en PYMEs en Ecuador [Tesis de doctorado]. Universidad Católica de Santiago de Guayaquil.

Medina Romero, M. Á. (2025). Metodología Integral de la Investigación Científica: Fundamentos, Estrategias y Aplicaciones Digitales. Editorial Investigativa Latinoamericana. https://doi.org/10.62131/978-9942-573-13-1

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2025). Instrumento de Política Pública para la Transformación Digital del Ecuador 2025-2030. Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL). https://shre.ink/5afQ

Mónica Elizabeth Calle-Tenesaca & Rolando Patricio Andrade-Amoroso. (2024, agosto). Ciberseguridad en contabilidad: Protegiendo la integridad de los datos financieros en empresas comerciales. Revista Metropolitana de Ciencias Aplicadas, 7(S2), 87-98. https://doi.org/10.62452/bdc3pg66

National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29; p. NIST CSWP 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

Nurwanah, A. (2024). Cybersecurity in Accounting Information Systems: Challenges and Solutions. Advances in Applied Accounting Research, 2(3), 157-168. https://doi.org/10.60079/aaar.v2i3.336

Olajide Soji Osundare, Chidiebere Somadina Ike, Ololade Gilbert Fakeyede, & Adebimpe Bolatito Ige. (2022). Active/Active data center strategies for financial services: Balancing high availability with security. Computer Science & IT Research Journal, 3(3), 92-114. https://doi.org/10.51594/csitrj.v3i3.1494

Pacheco, F., & Staino, D. (2025). Gestión de la exposición en ciberseguridad. SADIO Electronic Journal of Informatics and Operations Research, 24(1), e071. https://doi.org/10.24215/15146774e071

Ramírez, M., Rodríguez Ariza, L., Gómez Miranda, M. E., & Vartika. (2022). The Disclosures of Information on Cybersecurity in Listed Companies in Latin America—Proposal for a Cybersecurity Disclosure Index. Sustainability, 14(3), 1390. https://doi.org/10.3390/su14031390

Recalde, D. (2025). Critical legal analysis of identity theft by electronic means as an independent criminal offense in the Organic Integral Penal Code. Centro Sur, 9(1), 15-28. https://doi.org/10.37955/cs.v9i1.374

Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. Sustainability, 15(18), 13369. https://doi.org/10.3390/su151813369

Servicio de Rentas Internas SRI. (2025). Catastro de Contribuyentes de la Provincia de Manabí [Dataset]. https://descargas.sri.gob.ec/download/datosAbiertos/SRI_RUC_Manabi.zip

Shafa, H., & Islam, A. (2025). IMPACT OF DATA PRIVACY AND CYBERSECURITY IN ACCOUNTING INFORMATION SYSTEMS ON FINANCIAL TRANSPARENCY. International Journal of Scientific Interdisciplinary Research, 06(01), 254-292. https://doi.org/10.63125/xs0xt970

Shchyrba, I., Lagovska, O., Demianyshyna, O., Myronchuk, Z., & Shebeshten, E. (2025). Challenges of Cloud Accounting Systems Landscape within the Context of Cybersecurity Paradigm. Management (Montevideo), 3, 252. https://doi.org/10.62486/agma2025252

World Economic Forum (with Accenture). (2025). Global Cybersecurity Outlook 2025 (Insight Report). World Economic Forum. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

Anexos

Anexo 1: Matriz de operacionalización

Variable	Dimensiones	Indicadores	Ítems
Independiente: Ciberseguridad	**Gobernanza y políticas**	Grado de formalización de normativas internas de seguridad.	La empresa cuenta con un manual formalizado de políticas de seguridad de la información. Las políticas de seguridad de la información se revisan y actualizan periódicamente. La alta dirección muestra un compromiso visible en la asignación de recursos e implementación de ciberseguridad.
	Gestión de activos y accesos	Eficacia de los controles de identidad y privilegios.	Se exige autenticación de doble factor (MFA) para acceder a los sistemas contables y financieros. Los accesos a los módulos contables están rigurosamente delimitados según el rol de cada usuario. Se evalúan y ajustan periódicamente los permisos de acceso concedidos al personal.

Seguridad de la infraestructura	Nivel de robustez de las defensas perimetrales y de red.	La red corporativa está protegida por herramientas perimetrales avanzadas (firewalls, filtros de red). Se dispone de herramientas para la detección y monitoreo de accesos o actividades no autorizadas. La información contable se mantiene cifrada tanto en almacenamiento como durante su transmisión.
Cultura organizacional	Frecuencia y efectividad de los programas de concienciación.	El personal que maneja información contable recibe capacitación periódica en ciberseguridad. Se realizan pruebas o simulacros (como simulación de phishing) para medir la alerta del personal. Existe un programa continuo de sensibilización sobre riesgos y buenas prácticas informáticas.
Resiliencia operativa	Capacidad de respuesta y	La empresa posee un plan formal de continuidad del negocio

		recuperación ante desastres.	ante incidentes tecnológicos. Se cuenta con un plan de recuperación ante desastres aplicable a la infraestructura contable. Se ejecutan pruebas periódicas para verificar la efectividad de los planes de contingencia.
	Integridad y exactitud	Consistencia de los saldos y registros frente a alteraciones.	Se utilizan mecanismos digitales (como firmas o certificados) que aseguran la inalterabilidad de los registros contables. El sistema conserva registros de auditoría (logs) protegidos contra modificaciones no autorizadas. Se efectúan verificaciones periódicas para confirmar que la base de datos contable no ha sido alterada.
Dependiente: Información contable	**Confidencialidad tributaria**	Protección de datos sensibles frente a terceros no autorizados.	La información de índole tributaria y financiera está estrictamente restringida al personal autorizado. Las prácticas de manejo de datos se alinean con

		las exigencias de la Ley Orgánica de Protección de Datos Personales [LOPDP] (2021). La información contable se clasifica internamente según su nivel de confidencialidad y sensibilidad.
Disponibilidad y acceso	Continuidad del servicio de los sistemas de información financiera.	Los sistemas contables están operativos y accesibles de manera continua cuando la operación lo requiere. El acceso remoto al sistema contable se realiza mediante canales seguros (VPN o conexiones cifradas). Se generan copias de seguridad (respaldos) de los datos contables con la frecuencia necesaria para evitar pérdidas.
Confiabilidad de reportes	Grado de veracidad de los estados financieros para auditoría.	Las conciliaciones y validaciones del sistema garantizan saldos precisos y sin inconsistencias. Los estados financieros generados por el sistema reflejan consistencia y

		coherencia entre sus periodos. El sistema aplica validaciones automáticas que previenen errores en el registro de transacciones.
Cumplimiento normativo	Alineación con estándares contables y exigencias del SRI.	La estructura del software contable permite emitir información bajo la normativa NIIF vigente. El sistema genera los reportes tributarios y anexos cumpliendo estrictamente con los formatos requeridos por el SRI. Se garantiza el almacenamiento digital seguro de los comprobantes y archivos contables durante el tiempo exigido por la ley.

Nota. Indicadores medibles para evaluar cómo los controles técnicos y organizativos garantizan la integridad y fiabilidad de los registros financieros.

Anexo 2: Encuesta

MAESTRÍA EN CONTABILIDAD Y AUDITORÍA MENCIÓN GESTIÓN TRIBUTARIA

CUESTIONARIO SOBRE CIBERSEGURIDAD Y INFORMACIÓN CONTABLE

Objetivo del estudio

Determinar la relación entre las prácticas de ciberseguridad y la información contable de las empresas comercializadoras de insumos médicos de la provincia de Manabí, con el fin de generar recomendaciones que fortalezcan la seguridad digital y la calidad de la información financiera.

Estimado(a) profesional contable:

Reciba un cordial saludo. El presente cuestionario forma parte de un proyecto de investigación de maestría en Contabilidad y Auditoría. Su experiencia y conocimiento del área contable de su empresa son muy valiosos para este estudio, por lo que le solicitamos responder con la mayor sinceridad posible.

Indicaciones para responder

- El cuestionario tiene una duración aproximada de 10 a 15 minutos.
- No existen respuestas correctas o incorrectas; responda según su experiencia real en la empresa.
- Marque con una (X) dentro del casillero (☐) que mejor represente su respuesta.
- Responda todas las preguntas; si tiene dudas sobre algún término, elija la opción que más se acerque a su percepción.
- La información recopilada es de uso exclusivamente académico y su tratamiento será confidencial y anónimo.

Agradecemos de antemano su valioso tiempo y su honesta colaboración.

Sección I. Datos demográficos

Marque la opción que corresponda a su situación actual.

1. Rango de edad
☐ Menos de 25 años ☐ 25 a 35 años ☐ 36 a 45 años ☐ 46 a 55 años ☐ Más de 55 años
2. Cargo o puesto que desempeña en la empresa
☐ Contador(a) general ☐ Auxiliar contable ☐ Analista financiero(a) ☐ Jefe(a) financiero(a) / Gerente contable ☐ Otro
3. Años de experiencia en el área contable
☐ Menos de 1 año ☐ 1 a 5 años ☐ 6 a 10 años ☐ 11 a 15 años ☐ Más de 15 años
4. Tamaño de la empresa donde labora (número de empleados)
☐ 1 a 9 (microempresa) ☐ 10 a 49 (pequeña) ☐ 50 a 199 (mediana) ☐ 200 o más (grande)
5. ¿Cómo calificaría su nivel de conocimiento en el uso de herramientas informáticas y sistemas contables digitales?
☐ Básico ☐ Medio ☐ Avanzado

Sección II. Prácticas de ciberseguridad

Indique su grado de acuerdo con las siguientes afirmaciones sobre la ciberseguridad en su empresa, según la siguiente escala:

1 = Totalmente en desacuerdo 2 = En desacuerdo 3 = Ni de acuerdo ni en desacuerdo
4 = De acuerdo 5 = Totalmente de acuerdo

Gobernanza y políticas de seguridad

Ítem	1 Totalmente en desacuerdo	2 En desacuerdo	3 Ni de acuerdo ni en desacuerdo	4 De acuerdo	5 Totalmente de acuerdo
6. La empresa cuenta con un manual formalizado de políticas de seguridad de la información.	☐	☐	☐	☐	☐
7. Las políticas de seguridad de la información se revisan y actualizan periódicamente.	☐	☐	☐	☐	☐
8. La gerencia muestra un compromiso visible destinando recursos para la ciberseguridad.	☐	☐	☐	☐	☐

Gestión de activos y accesos

Ítem	1 Totalmente en desacuerdo	2 En desacuerdo	3 Ni de acuerdo ni en desacuerdo	4 De acuerdo	5 Totalmente de acuerdo
9. Se exige verificación en dos pasos (doble factor) para acceder a los sistemas contables y financieros.	☐	☐	☐	☐	☐
10. Los accesos a los módulos contables están claramente delimitados según el cargo de cada usuario.	☐	☐	☐	☐	☐
11. Se revisan y ajustan periódicamente los permisos de acceso concedidos al personal.	☐	☐	☐	☐	☐

Seguridad de la infraestructura

Ítem	1 Totalmente en desacuerdo	2 En desacuerdo	3 Ni de acuerdo ni en desacuerdo	4 De acuerdo	5 Totalmente de acuerdo
12. La red de la empresa está protegida por herramientas avanzadas de seguridad (antivirus, filtros, cortafuegos).	☐	☐	☐	☐	☐
13. Se dispone de herramientas para detectar y monitorear accesos o actividades no autorizadas.	☐	☐	☐	☐	☐
14. La información contable se mantiene protegida (cifrada) tanto al almacenarse como al enviarse.	☐	☐	☐	☐	☐

Cultura organizacional en ciberseguridad

Ítem	1 Totalmente en desacuerdo	2 En desacuerdo	3 Ni de acuerdo ni en desacuerdo	4 De acuerdo	5 Totalmente de acuerdo
15. El personal que maneja información contable recibe capacitación periódica en ciberseguridad.	☐	☐	☐	☐	☐
16. Se realizan simulacros (por ejemplo, de correos falsos o *phishing*) para medir la alerta del personal.	☐	☐	☐	☐	☐
17. Existe un programa continuo de sensibilización sobre riesgos y buenas prácticas informáticas.	☐	☐	☐	☐	☐

Resiliencia operativa

Ítem	1 Totalmente en desacuerdo	2 En desacuerdo	3 Ni de acuerdo ni en desacuerdo	4 De acuerdo	5 Totalmente de acuerdo
18. La empresa posee un plan formal de continuidad del negocio ante incidentes tecnológicos.	☐	☐	☐	☐	☐

19. Se cuenta con un plan de recuperación ante desastres aplicable a la infraestructura contable.	☐	☐	☐	☐	☐
20. Se ejecutan pruebas periódicas para verificar la efectividad de los planes de contingencia.	☐	☐	☐	☐	☐

Sección III. Información contable

Indique con qué frecuencia se presentan las siguientes situaciones en su empresa, según la siguiente escala:

1 = Nunca 2 = Casi nunca 3 = A veces 4 = Casi siempre 5 = Siempre

Integridad y exactitud

Ítem	1 Nunca	2 Casi nunca	3 A veces	4 Casi siempre	5 Siempre
21. Se utilizan mecanismos digitales (como firmas o certificados) que aseguran que los registros contables no se puedan alterar.	☐	☐	☐	☐	☐
22. El sistema conserva un registro de auditoría (historial de cambios) protegido contra modificaciones no autorizadas.	☐	☐	☐	☐	☐
23. Se realizan verificaciones periódicas para confirmar que la base de datos contable no ha sido alterada.	☐	☐	☐	☐	☐

Confidencialidad tributaria

Ítem	1 Nunca	2 Casi nunca	3 A veces	4 Casi siempre	5 Siempre
24. La información tributaria y financiera está estrictamente restringida al personal autorizado.	☐	☐	☐	☐	☐
25. Las prácticas de manejo de datos se alinean con las exigencias de la Ley Orgánica de Protección de Datos Personales (LOPDP).	☐	☐	☐	☐	☐
26. La información contable se clasifica internamente según su nivel de confidencialidad.	☐	☐	☐	☐	☐

Disponibilidad y acceso

Ítem	1 Nunca	2 Casi nunca	3 A veces	4 Casi siempre	5 Siempre
27. Los sistemas contables están operativos y accesibles de manera continua cuando se los necesita.	☐	☐	☐	☐	☐
28. El acceso remoto al sistema contable se realiza mediante canales seguros (VPN o conexiones cifradas).	☐	☐	☐	☐	☐
29. Se generan copias de seguridad (respaldos) de los datos contables con la frecuencia necesaria para evitar pérdidas.	☐	☐	☐	☐	☐

Confiabilidad de reportes

Ítem	1 Nunca	2 Casi nunca	3 A veces	4 Casi siempre	5 Siempre
30. Las conciliaciones y validaciones del sistema garantizan saldos precisos y sin inconsistencias.	☐	☐	☐	☐	☐
31. Los estados financieros generados por el sistema reflejan consistencia entre sus periodos.	☐	☐	☐	☐	☐
32. El sistema aplica validaciones automáticas que previenen errores en el registro de transacciones.	☐	☐	☐	☐	☐

Cumplimiento normativo

Ítem	1 Nunca	2 Casi nunca	3 A veces	4 Casi siempre	5 Siempre
33. La estructura del software contable permite emitir información bajo la normativa NIIF vigente.	☐	☐	☐	☐	☐
34. El sistema genera los reportes tributarios y anexos cumpliendo con los formatos requeridos por el SRI.	☐	☐	☐	☐	☐
35. Se garantiza el almacenamiento digital seguro de los comprobantes y archivos	☐	☐	☐	☐	☐

contables durante el tiempo exigido por la ley.					

Muchas gracias por su tiempo y por su valiosa colaboración con esta investigación. Sus respuestas contribuirán directamente al fortalecimiento de la ciberseguridad y la confiabilidad de la información contable en el sector.