PRÁCTICAS DE SEGURIDAD DE LA INFORMACIÓN EN MIPYMES DE VILLAVICENCIO: UN ESTUDIO DE CASO MÚLTIPLE PARA LA IDENTIFICACIÓN DE OPORTUNIDADES DE MEJORA DESDE LOS MARCOS COSO-ERM Y COBIT 2019

JEIDY TATIANA GARZÓN GARZÓN
YOLANDA AROCA GARCIA

UNIVERSIDAD SANTO TOMÁS
FACULTAD DE CONTADURÍA PÚBLICA
VILLAVICENCIO
2026

Prácticas de seguridad de la información en mipymes de Villavicencio: un estudio de caso múltiple para la identificación de oportunidades de mejora desde los marcos coso-erm y cobit 2019

JEIDY TATIANA GARZÓN GARZÓN
YOLANDA AROCA GARCIA

Trabajo de grado presentado como requisito para optar al título de Contador Público

Director
Mg. JOSÉ JOAQUÍN FLÓREZ BAQUERO
Magíster en Controlling
Magíster en Innovación
Magíster en Sistemas Integrados de Gestión de la Calidad

UNIVERSIDAD SANTO TOMÁS
FACULTAD DE CONTADURÍA PÚBLICA
VILLAVICENCIO
2026

Autoridades Académicas

P. Álvaro José ARANGO RESTREPO, O.P.
Rector General

P. Adrián Mauricio GARCÍA PEÑARANDA, O.P.
Vicerrector Académico General

P. Luis Antonio ALFONSO VARGAS, O.P.
Rector Seccional Villavicencio

P. Juan Francisco CORREA HIGUERA, O.P.
Vicerrector Académico Seccional Villavicencio

Mg. Julieth Andrea SIERRA TOBÓN
Secretaria General Seccional Villavicencio

Mg. José Joaquín FLÓREZ BAQUERO
Decano Facultad de Contaduría Pública

Agradecimientos

Este proceso representó para nosotras aprendizaje, dedicación y crecimiento tanto académico como personal. Cada etapa desarrollada permitió fortalecer nuestros conocimientos y reafirmar la importancia del compromiso y la constancia para alcanzar las metas propuestas.

Por esta razón, queremos agradecer principalmente a Dios, por acompañarnos y darnos la sabiduría, la fortaleza y la motivación necesarias para culminar satisfactoriamente este proyecto.

A nuestras familias y seres queridos, por su apoyo incondicional, comprensión y confianza durante todo este proceso, siendo una fuente permanente de motivación en los momentos de mayor exigencia. A los docentes y a todas las personas que contribuyeron con sus conocimientos, orientaciones y aportes, los cuales fueron fundamentales para el desarrollo de esta investigación.

Al mismo tiempo, reconocemos el esfuerzo, la responsabilidad y el trabajo en equipo que nos permitió superar los desafíos presentados y convertir esta experiencia en un logro significativo para nuestra formación profesional

Contenido

Pág.

Resumen 14
Abstract 15
Introducción 16
1. Planteamiento del problema 17
1.1 Descripción del problema 17
1.2 Pregunta de investigación 18
1.2.1 Subpregunta de investigación 18
2. Objetivos de la investigación 19
2.1 Objetivo general 19
2.2 Objetivos específicos 19
3. Justificación 20
4. Alcance del proyecto 22
5. Antecedentes 23
5.1 Contexto internacional y latinoamericano 23
5.2 Contexto nacional (Colombia) 24
6. Marco referencial 25
6.1 Marco Teórico 25
6.1.1 Concepto del riesgo 25
6.1.2 Riesgo tecnológico 25
6.1.3 Riesgo cibernético en MiPymes: 26
6.1.4 Gestión del riesgo COSO-ERM 26
6.1.5 Gobernanza TI-COBIT 2019 27
6.1.6 Control interno 27
6.1.7 Continuidad del negocio: 28
6.2 Marco conceptual 28
6.3 Marco Legal 29
6.3.1 Normativa de protección de datos 29

6.3.2 Normativa contable y tributaria 29
6.3.3 Normativa de ciberseguridad 30
6.3.4 Normativa internacional 30
6.4 Marco institucional 30
7. Metodología 32
7.1 Enfoque de la investigación 32
7.2 Tipo de investigación 33
7.3 Población y muestra 34
7.4 Técnicas e Instrumentos 35
7.5 Variables del estudio 36
7.6 Análisis de datos 37
7.7 Consideraciones éticas 40
8. Resultados 42
8.1 Identificación de prácticas y condiciones: 43
8.2 Efectos de las prácticas de seguridad en la operatividad y confiabilidad 44
8.3 Análisis desde el modelo COSO-ERM 46
8.4 Nivel de capacidad tecnológica 47
Conclusiones 53
Recomendaciones 55
Recomendaciones asociadas al Objetivo Específico 1 55
Recomendaciones asociadas al Objetivo Específico 2 56
Recomendaciones asociadas al Objetivo Específico 3 (COSO-ERM) 57
Recomendaciones asociadas al Objetivo Específico 4 (COBIT 2019) 59
Bibliografía 61
Anexos 63

Lista de Tablas

Pág.

Tabla 1 Marco conceptual 28
Tabla 2 Entidades regulatorias..... 30
Tabla 3 Variable independiente: Riesgo Cibernético 36
Tabla 4 Variable dependiente: Confiabilidad de la información contable y operatividad 37
Tabla 5 Variable interviniente: Control interno (COSO) 37
Tabla 6 Variable interviniente: Gestión tecnológica (COBIT)..... 37
Tabla 7 Proceso de codificación y categorización..... 39
Tabla 8 Códigos de identificación 43
Tabla 9 Resultados cuantitativos 44
Tabla 10 Lineamientos COSO-ERM..... 47
Tabla 11 Asignaciones de nivel..... 51
Tabla 12 Hallazgos 51
Tabla 13 Recomendaciones para el componente del modelo COSO-ERM 59
Tabla 14 Avance esperado en los dominios de COBIT 2019 evaluados..... 60
Tabla 15 Consolidación de respuestas por participante..... 67
Tabla 16 Respuestas del cuestionario de control..... 67
Tabla 17 Frecuencias y porcentajes por hallazgo 69
Tabla 18 Análisis comparativo por empresa 69

Lista de Figuras

Pág.

Figura 1 Representación gráfica del enfoque cualitativo y cuantitativo..... 33
Figura 2 Representación gráfica métodos aplicado 34
Figura 3 Niveles de capacidad (0 a 5)..... 51

Lista de Anexos

Pág.

Anexo A. Guía de entrevista semiestructurada..... 63
Anexo B. Cuestionario de control 65
Anexo C. Consolidado de resultados del cuestionario de control 67

Resumen

La creciente digitalización de los procesos contables y administrativos ha llevado a que las MiPymes colombianas dependan cada vez más de herramientas tecnológicas para gestionar información financiera. Sin embargo, en muchos casos esta adopción tecnológica no ha sido acompañada por mecanismos formales de control interno y seguridad de la información, aumentando la exposición a riesgos cibernéticos que pueden afectar la operatividad y la confiabilidad de los registros contables. Con esto, se evaluaron prácticas en 2 pymes de Villavicencio mediante los modelos COSO-ERM y COBIT 2019. Con base en un alcance cualitativo y descriptivo-analítico, con un estudio de casos múltiples como estrategia metodológica. Los datos se recopilaron mediante entrevistas semiestructuradas y encuestas al personal vinculado a los procesos contables y tecnológicos en las organizaciones participantes. Los resultados evidenciaron que ambas empresas cuentan con procesos contables digitalizados, usuarios individuales y mecanismos de respaldo automático de información.

No obstante, se identificaron debilidades relacionadas con la ausencia de políticas formales de seguridad, controles poco estructurados, uso de aplicaciones de mensajería para compartir información financiera y limitada gestión preventiva frente a riesgos tecnológicos. Asimismo, se observó dependencia del conocimiento empírico del personal y escasa supervisión sobre algunos procesos tecnológicos. Desde el enfoque COSO-ERM se identificaron deficiencias en evaluación de riesgos, supervisión y formalización de controles internos. Por su parte, COBIT 2019 permitió evidenciar niveles básicos e intermedios de capacidad tecnológica, especialmente en aspectos relacionados con seguridad de la información y continuidad operativa. En conclusión, las vulnerabilidades fundamentales no solo tienen naturaleza tecnológica, sino que también se sustentan en bases organizativas intrínsecas. La informalidad en el proceso operativo, la insuficiencia en la documentación y una cultura de gestión de riesgos de bajo nivel plantean serias amenazas a la integridad y la confiabilidad de la información contable.

Palabras clave: riesgo cibernético, control interno, seguridad de la información, COSO-ERM, COBIT 2019, información contable.

Abstract

The increasing digitalization of accounting and administrative processes has led Colombian SMEs to rely increasingly on technological tools to manage financial information. However, in many cases, this technological adoption has not been accompanied by formal internal control and information security mechanisms, increasing exposure to cyber risks that may affect operational performance and the reliability of accounting records. In this context, practices implemented in two SMEs located in Villavicencio were evaluated through the COSO-ERM and COBIT 2019 frameworks. This research was developed under a qualitative and descriptive-analytical approach, using a multiple case study as the methodological strategy. Data was collected through semi-structured interviews and surveys conducted with personnel involved in accounting and technological processes within the participating organizations. The results showed that both companies have digitalized accounting processes, individual user access, and automatic information backup mechanisms.

However, weaknesses were identified regarding the absence of formal security policies, poorly structured controls, the use of messaging applications to share financial information, and limited preventive management of technological risks. Likewise, dependence on employees empirical knowledge and limited supervision of certain technological processes were observed. From the COSO-ERM perspective, deficiencies were identified in risk assessment, monitoring, and the formalization of internal controls. In turn, COBIT 2019 revealed basic and intermediate levels of technological capability, especially in aspects related to information security and operational continuity. In conclusion, the identified vulnerabilities are not only technological in nature but are also supported by intrinsic organizational weaknesses. Informality in operational processes, insufficient documentation, and a low-level risk management culture pose significant threats to the integrity and reliability of accounting information.

Keywords: cyber risk, internal control, information security, COSO-ERM, COBIT 2019, accounting information.

Introducción

Los procesos administrativos y contables han transformado la manera en que las MiPymes desarrollan sus actividades operativas y manejan la información financiera. Actualmente, muchas organizaciones utilizan herramientas como software en la nube, plataformas digitales, almacenamiento electrónico y aplicaciones de mensajería para llevar a cabo registros financieros, compartir documentos y cumplir con sus responsabilidades tributarias. Estos han generado nuevos desafíos en materia de seguridad de los datos y continuidad de las actividades.

En numerosas MiPymes, la adopción tecnológica ocurre sin el respaldo de políticas claras de seguridad, controles internos sólidos ni sistemas adecuados de gestión TI. Como consecuencia, se generan condiciones de escasa protección de la información, ausencia de respaldos digitales y uso inapropiado de herramientas de comunicación, lo que afecta directamente la integridad, disponibilidad y confiabilidad de los datos financieros.

En este contexto, modelos como COSO-ERM y COBIT 2019 ofrecen estructuras analíticas que permiten evaluar la efectividad de los controles organizacionales y el nivel de madurez en la gestión tecnológica. El propósito de esta investigación es analizar las prácticas de seguridad de la información y las condiciones de exposición al riesgo cibernético en las áreas contables de dos MiPymes de Villavicencio, pertenecientes a diferentes sectores económicos, mediante un enfoque cualitativo-descriptivo con apoyo de cuestionarios estructurados.

El documento se organiza en los siguientes apartados: planteamiento del problema y objetivos, justificación y alcance, antecedentes, marco referencial (teórico, conceptual, legal e institucional), metodología, resultados, conclusiones y recomendaciones.

1. Planteamiento del problema

1.1 Descripción del problema

En el contexto actual, la creciente digitalización de los procesos contables y financieros ha incrementado el uso de tecnologías de la información en las organizaciones, mejorando la eficiencia operativa, el acceso a la información y la automatización de tareas. Sin embargo, este proceso también ha incrementado la exposición a riesgos cibernéticos, generando nuevos desafíos en la seguridad de la información y la gestión de riesgos en entornos digitales (Comisión de Regulación de Comunicaciones, 2025; Hoong & Rezania, 2024).

En el ecosistema empresarial colombiano, las MiPymes representan más del 90% del tejido productivo nacional, pero operan frecuentemente con recursos limitados, estructuras organizacionales reducidas y escasa formalización de sus procesos internos. Cuando estas empresas incorporan herramientas digitales para la gestión contable software en la nube, servidores compartidos, facturación electrónica, lo hacen en un contexto donde los controles de seguridad suelen rezagarse respecto a la velocidad de la adopción tecnológica. Esta condición genera una brecha operativa que ha sido documentada en el contexto colombiano por investigadores como Sarmiento Suárez et al. (2024) y Gordillo (2024), y que se profundiza en regiones como el Meta, donde la oferta de servicios especializados en ciberseguridad y auditoria TI es aún incipiente (Gómez Guevara, 2025; Chidukwani et al., 2026).

Desde una perspectiva contable, el riesgo cibernético trasciende el ámbito tecnológico, ya que afecta directamente la confiabilidad de la información financiera. La ocurrencia de incidentes como accesos no autorizados, pérdida de datos o fallas en los sistemas puede generar errores en los registros contables, inconsistencias en los estados financieros, interrupciones operativas y posibles incumplimientos normativos (Rey, 2024; El Ferjani El Ferjani et al., 2025).

Aunque existen marcos internacionales como **COSO-ERM** y **COBIT 2019**, pensados para guiar el control interno y la gobernanza tecnológica, en las MiPymes su adopción no suele ser amplia. Muchas veces, el control interno no toma en cuenta de manera suficiente los riesgos tecnológicos, y la gestión de la tecnología no siempre se alinea con los objetivos contables y financieros.

El problema principal de la investigación es la ausencia de integración entre el control interno y la gestión tecnológica, lo que complica una gestión estructurada de los riesgos cibernéticos y tiene un impacto negativo en aspectos fundamentales, como la operatividad y confiabilidad de los datos contables en las MiPymes de Villavicencio. Debido a sus características organizacionales y tecnológicas, esta desconexión puede aumentar la vulnerabilidad y muestra la importancia de analizar cómo se están gestionando estos riesgos en la práctica.

1.2 Pregunta de investigación

¿Cómo inciden las prácticas de seguridad de la información y los mecanismos de control interno y gestión tecnológica en la operatividad y confiabilidad de la información contable de las MiPymes de Villavicencio?

1.2.1 Subpregunta de investigación

¿Qué debilidades en control interno y gestión tecnológica pueden incrementar la exposición al riesgo cibernético en las MiPymes analizadas?

2. Objetivos de la investigación

2.1 Objetivo general

Analizar las prácticas de seguridad de la información y las condiciones de exposición al riesgo cibernético que inciden en la operatividad y confiabilidad de la información contable en las MiPymes de Villavicencio, a partir de la evaluación del control interno y la madurez de la gestión tecnológica desde los marcos COSO-ERM y COBIT 2019.

2.2 Objetivos específicos

1. Identificar las prácticas de seguridad de la información y los factores de exposición al riesgo cibernético presentes en las MiPymes objeto de estudio en Villavicencio.
2. Analizar los efectos de las prácticas de seguridad de la información y de la exposición al riesgo cibernético en la operatividad y en la confiabilidad de la información contable de las empresas analizadas, en relación con el control interno y la gestión tecnológica.
3. Evaluar las prácticas de gestión del riesgo cibernético dentro del sistema de control interno de las MiPymes objeto de estudio, con base en los lineamientos del modelo COSO-ERM.
4. Determinar el nivel de madurez de las prácticas de gestión de tecnologías de la información en las empresas objeto de estudio, a partir de criterios establecidos en COBIT 2019.

3. Justificación

El contador público en ejercicio profesional no solo debe garantizar la exactitud de los registros, sino también la integridad y disponibilidad de la información que soporta esos registros. En un entorno donde las MiPymes colombianas operan sus procesos contables a través de plataformas digitales, servidores locales y aplicaciones móviles, la seguridad de la información deja de ser un simple asunto tecnológico para convertirse en un pilar esencial del control interno y la confianza empresarial. Cuando esa seguridad se vulnera, no solo se pierden datos: se ponen en riesgo obligaciones fiscales, se dificulta reconstruir la historia de las operaciones y, sobre todo, se debilita la confianza de quienes dependen de la información financiera para tomar decisiones (Gómez Guevara, 2025; Sarmiento Suárez et al., 2024).

Desde la perspectiva contable, esta circunstancia es particularmente relevante, puesto que las debilidades en términos de seguridad de la información pueden poner en riesgo la integridad, confiabilidad y disponibilidad de los registros financieros, generando posibles errores operativos, pérdida de datos y problemas para cumplir con obligaciones fiscales y administrativas (Rey, 2024; Chávez Buitrago, 2024). Esta problemática se vuelve más crítica en situaciones donde los procesos contables dependen cada vez más de plataformas digitales y de sistemas electrónicos de almacenamiento.

A nivel académico, la investigación busca aportar al análisis de las prácticas de seguridad de la información desde una perspectiva contable y organizacional, integrando elementos de control interno y gestión tecnológica mediante referentes como COSO-ERM (Committee of Sponsoring Organizations of the Treadway Commission, 2017) y COBIT 2019 (Information Systems Audit and Control Association, 2019). Este enfoque permite observar la interacción entre tecnología, control y confianza en la información, brindando una visión más cercana y comprensible de los desafíos que enfrentan las pequeñas y medianas empresas en su día a día.

En la práctica, este estudio busca detectar áreas en las que las MiPymes pueden mejorar, ya sea en el control interno, el acceso a sistemas, la continuidad de sus operaciones o la gestión de la información contable digitalizada. Los hallazgos no solo proporcionaran un punto de partida para fortalecer la seguridad, sino que también servirán como guía para tomar decisiones cuando las compañías se enfrenten a riesgos tecnológicos.

Desde el punto de vista metodológico, la investigación se basa en un estudio de caso múltiple, empleando entrevistas y cuestionarios como herramientas principales. Esto permite observar y analizar cómo las organizaciones realmente llevan a cabo sus prácticas, entendiendo mejor los retos que enfrentan las MiPymes al digitalizar sus procesos contables.

4. Alcance del proyecto

Esta investigación tiene un enfoque analítico y descriptivo, cuyo propósito es examinar la gestión tecnológica, el control interno y las prácticas de seguridad de la información en los sectores contables de las MiPymes que son objeto de investigación.

El estudio se desarrolla mediante un análisis contextualizado de dos MiPymes ubicadas en la ciudad de Villavicencio, pertenecientes a sectores económicos distintos, con el propósito de identificar condiciones organizacionales relacionadas con la exposición al riesgo cibernético y como este podría afectar la operatividad y confiabilidad de la información contable.

La investigación se limita al análisis de prácticas, percepciones y mecanismos de control que están presentes en las organizaciones participantes, utilizando como referentes para la evaluación los marcos COSO-ERM y COBIT 2019.

Asimismo, el estudio no contempla auditorías técnicas de sistemas, pruebas especializadas de ciberseguridad ni mediciones cuantitativas de incidentes tecnológicos. Por lo tanto, los resultados obtenidos corresponden exclusivamente al contexto de las empresas analizadas y no buscan ser generalizables a la totalidad de las MiPymes.

5. Antecedentes

Los antecedentes de la presente investigación se estructuran en una progresión que abarca los ámbitos internacional, latinoamericano y nacional, con el propósito de evidenciar la evolución del conocimiento en torno al riesgo cibernético y su incidencia en la confiabilidad de la información contable en las micro, pequeñas y medianas empresas (MiPymes). Esta permite identificar no solo los avances teóricos y metodológicos, sino también las limitaciones existentes en la integración entre ciberseguridad, control interno y gestión tecnológica en contextos empresariales reales.

5.1 Contexto internacional y latinoamericano

A nivel internacional, la gestión del riesgo cibernético en MiPymes ha evolucionado hacia enfoques integrales que incorporan control interno, gobernanza y toma de decisiones estratégicas. Investigaciones recientes evidencian una brecha persistente entre la percepción de seguridad de las organizaciones y la realidad de sus operaciones, lo que amplía su vulnerabilidad frente a amenazas digitales (Chidukwani et al., 2026). Hoong y Rezania (2024) señalan que la adopción de prácticas de ciberseguridad en MiPymes depende de factores culturales y estructurales que dificultan la alineación entre gestión tecnológica y objetivos empresariales, mientras que Hoong et al. (2024) identifican que los directivos frecuentemente carecen de claridad para implementar estas estrategias en entornos reales.

En el contexto latinoamericano, Suescum Coelho et al. (2025) destacan que la escasa de articulación entre los procesos financieros y la gestión del riesgo incrementa la vulnerabilidad organizacional, especialmente en entornos con debilidades institucionales. El Ferjani El Ferjani et al. (2025) evidencian que las MiPymes de la región presentan dificultades estructurales para implementar medidas de protección adecuadas, manteniendo una gestión del riesgo cibernético predominantemente reactiva que compromete la confiabilidad de la información utilizada para la toma de decisiones.

5.2 Contexto nacional (Colombia)

En Colombia, Gómez Guevara (2025) señala que muchas MiPymes carecen de políticas de seguridad definidas y controles básicos de protección, aumentando la vulnerabilidad de la información contable en medios digitales. Sarmiento Suárez et al. (2024) documentan que la digitalización ha avanzado más rápido que la implementación de controles, generando brechas que afectan la confiabilidad de la información. Rey (2024) evidencia que los riesgos asociados a la información contable son también regulatorios cuando no existen estructuras sólidas de control interno, tendencia que la Comisión de Regulación de Comunicaciones (2025) confirma al señalar la necesidad de fortalecer la ciberseguridad en sectores empresariales con menor madurez tecnológica.

En síntesis, aunque existen avances importantes en el estudio del riesgo cibernético a nivel internacional y nacional, persiste un vacío investigativo en el análisis conjunto del riesgo cibernético, el control interno y el nivel de madurez tecnológica en contextos regionales como Villavicencio, que esta investigación busca abordar.

6. Marco referencial

6.1 Marco Teórico

6.1.1 Concepto del riesgo

Las organizaciones desarrollan sus actividades en entornos cambiantes donde factores internos y externos como errores humanos, fallas tecnológicas, decisiones operativas inadecuadas o cambios económicos pueden generar incertidumbre y afectar el cumplimiento de sus objetivos (COSO, 2017). El riesgo se entiende como la posibilidad de que ciertos eventos produzcan efectos negativos sobre la operación, la estabilidad o los resultados de una organización.

Según COSO (2017), el riesgo no solo depende de la probabilidad de que un evento ocurra, sino también del impacto que este pueda generar. Por ello, las empresas requieren mecanismos para identificar, evaluar y responder oportunamente a situaciones que puedan afectar sus objetivos estratégicos y operativos. En el área contable, esta gestión adquiere especial relevancia dado el uso intensivo de herramientas digitales para registrar, almacenar y procesar información financiera: la ausencia de controles adecuados sobre el acceso, las copias de seguridad o el manejo de datos puede generar pérdidas de información, alteraciones en los registros y dificultades en los reportes financieros (Rey, 2024).

6.1.2 Riesgo tecnológico

Desde una perspectiva organizacional, el riesgo tecnológico se manifiesta cuando las interrupciones o deficiencias en la gestión de los sistemas de información comprometen la continuidad operativa de las empresas. En contextos donde los procesos contables dependen de software financiero, servicios en la nube y plataformas digitales, la exposición a fallos operativos y problemas de seguridad se intensifica (Hoong & Rezania, 2024). En el área contable, esta vulnerabilidad es especialmente crítica dado que actividades como la facturación electrónica, el registro de transacciones y el almacenamiento de información financiera operan íntegramente en entornos digitales, cuya interrupción puede afectar directamente la calidad y confiabilidad de los datos (Sarmiento Suárez et al., 2024).

6.1.3 Riesgo cibernético en MiPymes:

El riesgo cibernético comprende amenazas digitales, accesos indebidos, fraudes electrónicos, pérdida de información, ataques informáticos que pueden afectar la seguridad de la información financiera y operativa (El Ferjani El Ferjani et al., 2025). A diferencia de otros riesgos tecnológicos, también proviene de prácticas inadecuadas de los propios usuarios (contraseñas débiles, apertura de enlaces fraudulentos, ausencia de protocolos), lo que incrementa la complejidad de su gestión (Chidukwani et al., 2026). Este tipo de riesgo puede generar inconsistencias en los estados financieros, incumplimientos normativos y afectaciones en la toma de decisiones (Rey, 2024).

Las MiPymes presentan mayor vulnerabilidad frente a estos riesgos debido a limitaciones económicas, tecnológicas y de personal especializado. La adopción de facturación electrónica, pagos digitales y almacenamiento en la nube ha mejorado algunos procesos, pero la ausencia de controles adecuados puede afectar la integridad y disponibilidad de la información financiera (Gómez Guevara, 2025; Sarmiento Suárez et al., 2024). Frente a este escenario, las MiPymes requieren fortalecer prácticas de control interno, respaldo de información y gestión de riesgos tecnológicos, especialmente en organizaciones con baja madurez digital (Rey, 2024).

6.1.4 Gestión del riesgo COSO-ERM

El COSO-ERM (Enterprise Risk Management), publicado por el Committee of Sponsoring Organizations of the Treadway Commission en su versión de 2017, ofrece una estructura analítica para valorar no solo si existen controles, sino si estos son efectivos en la gestión de los riesgos que la organización enfrenta. El modelo plantea que la gestión del riesgo debe incorporarse a los procesos estratégicos y operativos, apoyándose en cinco componentes interrelacionados: gobierno y cultura, estrategia y establecimiento de objetivos, desempeño, revisión y mejora, e información, comunicación y reporte (COSO, 2017).

En esta investigación, COSO-ERM sirve como base para analizar la forma en que las MiPymes gestionan los riesgos asociados a sus procesos tecnológicos e información contable, permitiendo identificar debilidades en supervisión, evaluación de riesgos y formalización de controles. Su aplicación resulta relevante en entornos digitales porque incorpora el riesgo cibernético dentro de la gestión empresarial no como un problema tecnológico aislado,

incentivando medidas preventivas orientadas a resguardar la información financiera y mejorar la continuidad operativa (COSO, 2017).

6.1.5 Gobernanza TI-COBIT 2019

COBIT 2019, desarrollado por ISACA, es un marco de gobernanza y gestión de TI que ayuda a las organizaciones a establecer mecanismos de control, supervisión y administración sobre sus procesos tecnológicos. Su versión 2019 incorpora factores de diseño que facilitan la adaptación del modelo a las características y nivel de riesgo de cada organización, lo cual es especialmente útil en el contexto de las MiPymes (ISACA, 2019). A través de sus dominios APO (Alinear, Planificar y Organizar), DSS (Entregar, Servicio y Soporte) y EDM (Evaluar, Dirigir y Monitorear) (ISACA, 2019), permite identificar áreas de mejora en seguridad de la información, gestión de accesos, continuidad operativa y supervisión de sistemas contables.

El enfoque de COBIT 2019 complementa COSO-ERM: mientras COSO se orienta a la gestión integral de riesgos organizacionales, COBIT profundiza en la administración y control de la tecnología. Juntos conforman el referente analítico central de esta investigación para evaluar tanto la estructura de control interno como el nivel de capacidad en la gestión tecnológica de las MiPymes estudiadas.

6.1.6 Control interno

Conforme a COSO (2017) el control interno constituye un instrumento que apoya el funcionamiento estructurado y confiable de la organización, más allá de un conjunto de procedimientos administrativos. De acuerdo con, abarca el diseño e implementación de políticas, actividades y procesos orientados a brindar seguridad razonable en el alcance de metas operativas, financieras y de cumplimiento. En el ámbito contable cobra especial importancia porque muchas decisiones estratégicas se fundamentan en la exactitud y confiabilidad de la información financiera: controles sólidos sobre registros, autorizaciones, soportes documentales e informes ayudan a minimizar errores, prevenir fraudes y fortalecer la transparencia (Rey, 2024).

Con el crecimiento del uso de tecnologías digitales, los controles internos se han adaptado a nuevos riesgos: administración de accesos, respaldos de información, protección de bases de datos y supervisión de sistemas contables. El control interno actúa así como elemento articulador

entre la gestión integral del riesgo propuesta por COSO-ERM y la gobernanza tecnológica de COBIT 2019 (ISACA, 2019).

6.1.7 Continuidad del negocio:

Según Hoong & Rezania (2024) muchas actividades empresariales dependen del funcionamiento permanente de sistemas informáticos, plataformas en la nube y servicios digitales, por lo que cualquier interrupción tecnológica puede afectar directamente la capacidad de la empresa para mantener sus operaciones. Incidentes como fallas en los sistemas, accesos no autorizados, ataques informáticos o pérdida de información pueden interrumpir procesos críticos como la facturación electrónica, el registro de operaciones contables y la elaboración de reportes financieros.

Esta situación es especialmente crítica en las MiPymes, donde la respuesta ante incidentes suele basarse en experiencia práctica o conocimientos informales del personal, en lugar de procedimientos establecidos, lo que incrementa su vulnerabilidad ante la interrupción operativa (Chidukwani et al., 2026; Gómez Guevara, 2025). Los marcos COSO-ERM y COBIT 2019 ofrecen herramientas para mejorar la prevención de riesgos y mantener la operación ininterrumpida en entornos digitalizados.

6.2 Marco conceptual

Los siguientes conceptos se emplean en la investigación con las definiciones operativas que se indican. Su desarrollo teórico completo se encuentra en el Marco Teórico.

Tabla 1 *Marco conceptual*

Concepto	Definición operativa en esta investigación
Riesgo cibernético	Posibilidad de que amenazas o vulnerabilidades digitales (phishing, accesos no autorizados, pérdida de datos, malware) afecten la confidencialidad, integridad y disponibilidad de la información contable de las MiPymes (Chidukwani et al., 2026; Hoong & Rezania, 2024).
Información contable	Conjunto de registros financieros digitalizados que soportan la toma de decisiones empresariales. Su confiabilidad depende tanto del cumplimiento de normas contables como de controles que protejan los datos en entornos tecnológicos (Rey, 2024).

Concepto	Definición operativa en esta investigación
Control interno	Políticas y procedimientos orientados a reducir riesgos y fortalecer el cumplimiento de objetivos organizacionales, incluyendo administración de accesos, protección de datos, supervisión de sistemas y respaldo de información (COSO, 2017).
Transformación digital	Integración de TI en procesos organizacionales (facturación electrónica, sistemas contables, almacenamiento en la nube) que mejora la eficiencia operativa, pero genera nuevos desafíos de seguridad para organizaciones sin mecanismos suficientes de control (Sarmiento Suárez et al., 2024).
Madurez tecnológica	Nivel de capacidad de una organización para gestionar, controlar y supervisar sus procesos tecnológicos de manera formal y documentada, evaluado mediante los dominios de COBIT 2019 (ISACA, 2019).

6.3 Marco Legal

6.3.1 Normativa de protección de datos

La Ley 1581 de 2012 establece en Colombia las obligaciones para la recolección, almacenamiento, uso y tratamiento de datos personales. Para las MiPymes que gestionan información de clientes, proveedores y empleados mediante software contable, facturación electrónica o servicios en la nube, esta normativa implica la necesidad de controles internos que prevengan accesos no autorizados y pérdida de datos. Desde los marcos COSO-ERM y COBIT 2019, el cumplimiento de esta norma requiere actividades de control de accesos (APO13, DSS05) y evaluación de riesgos asociados a la gestión de datos personales. Ley 1581 (2012).

6.3.2 Normativa contable y tributaria

El Estatuto Tributario y la normativa de la DIAN exigen a las empresas conservar registros contables exactos, verificables y legalmente constituidos. La implementación de factura electrónica obligatoria (Resoluciones DIAN 000042/2020 y 000165/2023) ha incrementado la dependencia de sistemas digitales para cumplir obligaciones fiscales. Los riesgos cibernéticos representan una amenaza directa para este cumplimiento: fallas tecnológicas, accesos no autorizados o pérdida de información pueden generar inconsistencias contables, retrasos en reportes tributarios y sanciones. Esto refuerza la necesidad de controles internos y gobierno TI alineados con COSO-ERM y COBIT 2019 DIAN (2020, 2023); Decreto 624 (1989).

6.3.3 Normativa de ciberseguridad

La Política Nacional de Seguridad Digital (PNSD), promovida por el MinTIC, establece lineamientos para que las organizaciones prevengan, detecten y respondan a incidentes que vulneren activos de información. El Ministerio ha impulsado programas específicos para MiPymes, reconociendo que estas entidades enfrentan limitaciones de infraestructura y mecanismos de seguridad. Estos lineamientos coinciden con los requisitos de COSO-ERM (gobierno y cultura, supervisión) y COBIT 2019 (EDM01, APO13) al señalar la necesidad de integrar gestión del riesgo, control interno y gobernanza tecnológica.

6.3.4 Normativa internacional

Las NIIF para PYMES (IASB) establecen que la información financiera debe ser relevante, confiable y libre de errores materiales; en entornos digitalizados, esto requiere controles de seguridad que protejan la integridad de los datos. La norma ISO/IEC 27001:2022 provee un marco de referencia para implementar sistemas de gestión de seguridad de la información, permitiendo establecer controles para proteger la confidencialidad, integridad y disponibilidad de los datos ante amenazas cibernéticas. Ambos estándares coinciden con la necesidad de fortalecer el control interno, la gestión del riesgo y la gobernanza tecnológica en las MiPymes.

6.4 Marco institucional

Las siguientes entidades enmarcan el contexto institucional de la investigación.

Tabla 2 *Entidades regulatorias*

Entidad / Organismo	Relevancia para la investigación
DIAN (Dirección de Impuestos y Aduanas Nacionales)	Supervisa los procesos de registro contable y tributario. Los riesgos cibernéticos amenazan directamente el cumplimiento de las obligaciones digitales (factura electrónica), pudiendo generar inconsistencias contables y sanciones por retrasos en reportes.
Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)	Formula la Política Nacional de Seguridad Digital y promueve programas de ciberseguridad para MiPymes. Sus lineamientos sobre cultura de prevención y gestión del riesgo son coherentes con los marcos COSO-ERM y COBIT 2019 aplicados en este estudio.

Entidad / Organismo	Relevancia para la investigación
Cámara de Comercio de Villavicencio	Fuente de información sobre el tejido empresarial local de MiPymes. Facilita el contexto sobre la adopción tecnológica en el ecosistema empresarial regional objeto de estudio.
Junta Central de Contadores (JCC)	Regula el ejercicio profesional de la contaduría. Su marco ético y normativo vincula al contador con la responsabilidad de velar por el manejo adecuado de la información financiera, incluyendo su seguridad en entornos digitales.
Consejo Técnico de la Contaduría Pública (CTCP)	Orienta la estandarización técnica contable en Colombia. Sus lineamientos sobre calidad, transparencia y comparabilidad de la información financiera adquieren mayor relevancia en entornos electrónicos dependientes de sistemas tecnológicos.
COSO (Committee of Sponsoring Organizations)	Organismo internacional que desarrolló el modelo COSO-ERM utilizado en esta investigación como referente para evaluar el control interno y la gestión de riesgos cibernéticos.
ISACA (Information Systems Audit and Control Association)	Asociación profesional internacional que desarrolló COBIT 2019, marco utilizado en esta investigación para evaluar la madurez en la gestión de TI.

7. Metodología

El desarrollo de la presente investigación se fundamenta en una estructura metodológica diseñada para comprender la complejidad del riesgo cibernético y su incidencia en los procesos contables de las organizaciones. A continuación, se detallan los criterios y procedimientos técnicos que guiaron el desarrollo del estudio.

7.1 Enfoque de la investigación

La presente investigación se desarrolló bajo un enfoque mixto predominantemente cualitativo con apoyo descriptivo cuantitativo, orientado a comprender la incidencia del riesgo cibernético en la operatividad y en la confiabilidad de la información contable en las MiPymes. La parte cualitativa permitió comprender las prácticas, percepciones y dinámicas organizacionales relacionadas con el control interno y la gestión tecnológica, a través de la aplicación de entrevistas semiestructuradas. Este enfoque permitió lograr una interpretación profunda del fenómeno en su contexto real, especialmente en organizaciones con limitaciones estructurales y tecnológicas como las MiPymes.

Asimismo, para el componente cuantitativo se utilizó la aplicación de cuestionarios estructurados, los cuales se analizaron a través de estadísticas descriptivas básicas, con el uso de frecuencias y porcentajes. Esto permitió reconocer las tendencias relativas a la exposición a riesgos cibernéticos, el uso de tecnologías digitales y el nivel de implementación de los controles internos. La integración de ambos componentes permitió contrastar los hallazgos obtenidos en las entrevistas con la información cuantitativa recopilada, fortaleciendo la interpretación de los resultados y la comprensión integral del fenómeno estudiado (Barreto Ascona & Lezcano Mencia, 2023).

Figura 1 *Representación gráfica del enfoque cualitativo y cuantitativo*

7.2 Tipo de investigación

El alcance de la investigación fue descriptivo-analítico, ya que pretendió caracterizar las prácticas organizacionales relacionadas con el riesgo cibernético, el control interno y la gestión tecnológica de las MiPymes estudiadas, y analizar su incidencia en la confiabilidad de la información contable y la operatividad empresarial. El alcance descriptivo facilitó la identificación de las condiciones, dinámicas y mecanismos empleados por las organizaciones para afrontar los riesgos tecnológicos y cibernéticos, todo ello sin intervenir en el entorno de estudio. Por su parte, el componente analítico facilitó la interpretación de las relaciones entre los riesgos identificados, los controles implementados y los efectos observados sobre los procesos contables.

En cuanto al diseño, la investigación se desarrolló mediante un estudio de caso múltiple. Este diseño permitió realizar un análisis comparativo entre dos organizaciones con características

similares en cuanto al uso de tecnologías digitales en procesos contables, pero con diferencias en sus prácticas de control y gestión tecnológica. La selección de dos casos se fundamentó en la metodología de estudio de caso múltiple, la cual permite analizar fenómenos organizacionales dentro de contextos reales mediante la comparación de prácticas, dinámicas y patrones entre diferentes unidades de análisis (Alonso, 2023).

Conforme a esta metodología, la lógica del estudio de caso múltiple no busca representatividad estadística sino profundidad interpretativa y replicación analítica: cada caso sirve para confirmar o contrastar los hallazgos del otro, lo que fortalece la validez interna de las conclusiones. La selección respondió a criterios de accesibilidad, pertinencia temática y contraste sectorial, garantizando que la comparación entre casos aportara información relevante sobre el fenómeno estudiado sin pretender generalización estadística al conjunto de MiPymes de Villavicencio.

Figura 2 *Representación gráfica métodos aplicado*

7.3 Población y muestra

La población de la investigación estuvo conformada por las micro, pequeñas y medianas empresas (MiPymes) ubicadas en la ciudad de Villavicencio, Meta, que utilizan tecnologías de la información en sus procesos operativos y contables.

La muestra estuvo integrada por dos empresas seleccionadas mediante un muestreo no probabilístico, intencional y por conveniencia, considerando criterios como accesibilidad a la

información, disposición para participar y uso de herramientas tecnológicas en procesos contables, incluyendo facturación electrónica, pagos digitales y almacenamiento en la nube.

La selección de dos casos se fundamentó en la metodología de estudio de caso múltiple, la cual permite analizar fenómenos organizacionales dentro de contextos reales mediante la comparación de prácticas, dinámicas y patrones entre diferentes unidades de análisis (Alonso, 2023). Conforme a esta metodología, la lógica del estudio de caso múltiple no busca representatividad estadística sino profundidad interpretativa: cada caso sirve para confirmar o contrastar los hallazgos del otro, lo que fortalece la validez analítica de las conclusiones. El propósito no fue generalizar los resultados, sino obtener una comprensión profunda del fenómeno estudiado en su contexto rea.

7.4 Técnicas e Instrumentos

Para el desarrollo de la presente investigación, se emplearon técnicas de recolección de información de carácter cualitativo y cuantitativo, en coherencia con el enfoque predominantemente cualitativo del estudio.

En la parte cualitativa, se emplearon entrevistas semiestructuradas (Ver anexo A) compuestas por preguntas abiertas que facilita la recopilación de datos, derivando la mayor cantidad posible de información directa por parte de los participantes orientados a la adaptación sobre sus experiencias, percepciones y prácticas que sustentan la gestión del riesgo cibernético en las PYMES. La guía de entrevista fue diseñada con base en los hallazgos preliminares de la investigación, incorporando preguntas previamente definidas y permitiendo flexibilidad para profundizar en aspectos relevantes identificados durante el desarrollo de las entrevistas.

Para el componente cuantitativo de esta investigación, se utilizó el cuestionario (Ver anexo B) como método de recopilación de datos con el fin de recopilar datos estructurados sobre la frecuencia con la que las PYMES están expuestas a distintos riesgos cibernéticos, qué tan bien han implementado controles internos y cómo gestionan la información tecnológica. El cuestionario contiene preguntas cerradas, lo que facilitará cuantificar los datos y realizar estadísticas básicas sobre las respuestas.

Cada instrumento se estructura en torno a categorías específicas de análisis (para describir las condiciones de exposición, analizar el posible impacto en las operaciones, evaluar la necesidad de la información contable y la revisión del control interno y profundizar en la tecnología). Estos

métodos permitieron abordar el fenómeno de estudio de manera holística y en línea con los objetivos establecidos.

Cabe precisar que los indicadores asociados a la variable dependiente específicamente los relacionados con exactitud, integridad y oportunidad de la información contable fueron medidos exclusivamente mediante entrevista semiestructurada, dado el carácter perceptual y exploratorio de estos fenómenos en el contexto de las organizaciones estudiadas. Esta decisión es coherente con el enfoque predominantemente cualitativo de la investigación y con la naturaleza de las MiPymes como unidades de análisis donde los efectos sobre la confiabilidad contable se manifiestan principalmente a través de experiencias y percepciones del personal vinculado al área financiera (Barreto Ascona & Lezcano Mencia, 2023). Los indicadores de las variables intervinientes, en cambio, fueron abordados mediante técnica mixta, combinando entrevista y cuestionario para fortalecer la triangulación de los hallazgos.

7.5 Variables del estudio

A continuación, se presentan las variables del estudio:

- **Variable independiente:** Riesgo cibernético
- **Variable dependiente:** Confiabilidad de la información contable y operatividad
- **Variables intervinientes:** Control interno (COSO) y gestión tecnológica (COBIT)

Tabla 3 *Variable independiente: Riesgo Cibernético*

Dimensión	Indicador	Definición Operativa	Técnica	Instrumento
Exposición al riesgo	Uso de servicios en la nube	Frecuencia de uso de plataformas digitales en procesos contables	Cuantitativa	Cuestionario
	Uso de facturación electrónica	Nivel de dependencia de sistemas digitales	Cuantitativa	Cuestionario
	Acceso a sistemas digitales	Nivel de uso de internet y software contable	Cuantitativa	Cuestionario
Vulnerabilidades	Seguridad de accesos	Uso de contraseñas seguras, roles y autenticación	Mixta	Cuestionario / Entrevista
	Actualización de sistemas	Frecuencia de actualización de software	Cuantitativa	Cuestionario
Incidentes	Frecuencia de incidentes	Número de eventos de seguridad reportados	Cuantitativa	Cuestionario
		Descripción de eventos de ciberataques	Cualitativa	Entrevista

Tabla 4 *Variable dependiente: Confiabilidad de la información contable y operatividad*

Dimensión	Indicador	Definición Operativa	Técnica	Instrumento
Exactitud	Errores contables	Frecuencia de inconsistencias en registros	Cualitativa	Entrevista
Integridad	Alteración o pérdida de datos	Información incompleta o modificada	Cualitativa	Entrevista
Oportunidad	Tiempo de reportes	Tiempo de generación de informes contables	Cualitativa	Entrevista
Continuidad operativa	Interrupciones	Frecuencia de interrupciones en procesos contables	Cualitativa	Entrevista
	Continuidad del servicio	Capacidad de la empresa para seguir operando	Cualitativa	Entrevista
	Retrasos en procesos	Demoras en registros o reportes contables	Cualitativa	Entrevista
	Pérdida de información	Casos de información no disponible	Cualitativa	Entrevista

Tabla 5 *Variable interviniente: Control interno (COSO)*

Dimensión	Indicador	Definición Operativa	Técnica	Instrumento
Ambiente de control	Existencia de políticas de control	Presencia de normas internas de control	Mixta	Entrevista / Cuestionario
Evaluación de riesgos	Identificación de riesgos	Reconocimiento de riesgos cibernéticos	Mixta	Entrevista / Cuestionario
Actividades de control	Controles implementados	Procedimientos de control en procesos	Mixta	Entrevista / Cuestionario
Supervisión	Monitoreo y supervisión	Seguimiento a controles	Mixta	Entrevista / Cuestionario

Tabla 6 *Variable interviniente: Gestión tecnológica (COBIT)*

Dimensión	Indicador	Definición Operativa	Técnica	Instrumento
Uso de TI	Herramientas tecnológicas	Software contable utilizado	Cuantitativa	Cuestionario
Seguridad de la información	Control de accesos	Uso de contraseñas y permisos	Mixta	Entrevista / Cuestionario
Respaldo de información	Copias de seguridad	Existencia y frecuencia de copias de seguridad	Mixta	Entrevista / Cuestionario
Gestión de incidentes	Respuesta a fallos	Acciones ante incidentes tecnológicos	Cualitativa	Entrevista

7.6 Análisis de datos

El análisis de la información se desarrolló mediante un enfoque predominantemente cualitativo con apoyo descriptivo cuantitativo, en el cual se integraron técnicas cualitativas y

cuantitativas, con el propósito de interpretar los riesgos cibernéticos y su incidencia en la información contable de las MiPymes objeto de estudio. Para ello, se empleó el modelo COSO como referente para evaluar la estructura y efectividad del control interno frente a los riesgos cibernéticos, mientras que COBIT 2019 se utilizó como marco de referencia para analizar la gestión y el gobierno de las tecnologías de la información dentro de las organizaciones.

Una vez obtenida la información a través de la entrevista semiestructurada (ver Anexo A), esta fue analizada mediante un proceso sistemático de análisis temático, desarrollado en las siguientes etapas:

- **Análisis y organización de la información:** A partir de las respuestas proporcionadas por los participantes, se elaboró un análisis interpretativo que incluyó fragmentos relevantes de sus respuestas, con el propósito de contextualizar y sustentar los hallazgos identificados.
- **Codificación abierta:** Los códigos utilizados (TEC, VUL, INT, PER, EXA, POL, RIE, RES, GIN), se derivan de la operacionalización de variables definidas en el diseño metodológico, lo que garantiza coherencia entre los objetivos de investigación, las categorías de análisis y los instrumentos de recolección de información. Cada código fue asignado a fragmentos específicos de las entrevistas, permitiendo clasificar la información según su contenido y facilitar la identificación de patrones, recurrencias y relaciones entre las prácticas organizacionales descritas por los participantes.
- **Categorización**: Los códigos obtenidos fueron agrupados en categorías y subcategorías previamente definidos, tales como: exposición al riesgo cibernético, impacto en la operatividad, confiabilidad de la información contable, control interno y gestión tecnológica.

Con el fin de fortalecer la coherencia metodológica, las categorías de análisis se articularon con los marcos de referencia COSO y COBIT 2019. De este modo, las categorías relacionadas con control interno (políticas y controles, evaluación de riesgos y supervisión) fueron analizadas a partir de los componentes del modelo COSO, permitiendo evaluar la estructura, formalización y efectividad de los controles en los procesos contables.

Por su parte, las categorías asociadas a la gestión tecnológica (seguridad de la información, respaldo de datos y gestión de incidentes) fueron interpretadas con base en COBIT 2019, lo que

permitió analizar el nivel de capacidad en la gestión de tecnologías de la información y su relación con la seguridad de la información contable.

Adicionalmente, las categorías de exposición al riesgo cibernético, impacto en la operatividad y confiabilidad de la información contable se utilizaron como ejes integradores del análisis, permitiendo relacionar los riesgos identificados con sus efectos en los procesos contables y la respuesta organizacional desde el control interno y la gestión tecnológica.

- **Análisis e interpretación**: Se interpretaron los hallazgos cualitativos estableciendo relaciones entre las categorías y los marcos teóricos mencionados, permitiendo comprender la forma en que las organizaciones gestionan los riesgos cibernéticos en sus procesos contables.

Por otra parte, en el componente cuantitativo, la información obtenida a través del cuestionario (ver Anexo B) fue analizada mediante estadística descriptiva, utilizando herramientas como tablas de frecuencias y porcentajes. Este análisis permitió identificar el nivel de implementación de prácticas, la frecuencia de controles y posibles brechas en la gestión del riesgo cibernético. Los resultados fueron interpretados a la luz de COBIT 2019, especialmente en lo relacionado con la gestión de riesgos y la seguridad de la información.

Posteriormente, se llevó a cabo una triangulación de la información, comparando los hallazgos obtenidos en las entrevistas con los resultados del cuestionario, con el fin de validar la consistencia de los datos, fortalecer la confiabilidad de los hallazgos y obtener una comprensión integral de las MiPymes estudiadas.

Finalmente, los resultados fueron interpretados de manera articulada, permitiendo contrastar las prácticas organizacionales identificadas con los referentes teóricos, con el fin de evidenciar niveles de cumplimiento y detectar brechas. Con ello, se formularon recomendaciones orientadas al fortalecimiento de la seguridad de la información contable en las MiPymes analizadas. El proceso de codificación y categorización se apoyó en herramientas ofimáticas como Microsoft Excel, lo que permitió organizar, clasificar y analizar la información de manera sistemática.

Tabla 7 *Proceso de codificación y categorización*

Fragmento de la entrevista	Código	Categoría	Interpretación
“Usamos un software contable en la nube, pero no sabemos	TEC	Uso de tecnologías	Exposición al riesgo cibernético	Existe uso de herramientas digitales sin control claro de

Fragmento de la entrevista	Código	Categoría	Interpretación
bien quién más puede acceder.”			accesos, lo que incrementa la vulnerabilidad.
“Las contraseñas las manejan varias personas y no se cambian con frecuencia.”	VUL	Vulnerabilidades	Exposición al riesgo cibernético	Se evidencia debilidad en controles de acceso, aumentando el riesgo de uso indebido de la información.
“Una vez el sistema se cayó y no pudimos facturar en todo el día.”	INT	Interrupciones	Impacto en la operatividad	Los fallos tecnológicos afectan directamente la continuidad de los procesos operativos.
“Se nos perdió información contable y tocó reconstruirla manualmente.”	PER	Pérdida de información	Impacto en la operatividad	La ausencia de respaldos adecuados afecta la disponibilidad y confiabilidad de la información.
“A veces los informes salen con errores porque el sistema falla.”	EXA	Exactitud	Confiabilidad de la información contable	Los riesgos tecnológicos impactan la precisión de los registros contables.
“No tenemos políticas claras de seguridad, todo se maneja de forma informal.”	POL	Políticas y controles	Control interno (COSO)	La ausencia de lineamientos formales debilita el sistema de control interno.
“No evaluamos riesgos tecnológicos, eso casi no se tiene en cuenta.”	RIE	Evaluación de riesgos	Control interno (COSO)	No existe una gestión estructurada del riesgo cibernético dentro de la organización.
“Sí hacemos copias de seguridad, pero solo cuando nos acordamos.”	RES	Respaldo de información	Gestión tecnológica (COBIT)	La gestión de backups es informal, lo que incrementa el riesgo de pérdida de datos.
“Cuando pasa algo, simplemente tratamos de solucionarlo en el momento.”	GIN	Gestión de incidentes	Gestión tecnológica (COBIT)	No existen protocolos definidos para la respuesta ante incidentes.

7.7 Consideraciones éticas

El desarrollo de la presente investigación se llevó a cabo bajo principios éticos que garanticen el respeto, la confidencialidad y la integridad de la información suministrada por las MiPymes participantes. Las disposiciones iniciales implicaron obtener el consentimiento de las organizaciones objeto de estudio después de que se divulgaran los objetivos de la investigación. En este sentido, se solicitó el consentimiento de participación con libertad de colaboración, sin imposición.

Además, se garantizó que los resultados fueran confidenciales, de modo que no se filtraran datos sensibles sobre contabilidad, tecnología o administración. Esta manera permite que los datos sean puramente académicos, sin identificar las organizaciones específicas que participaron en la

encuesta y presentando únicamente resultados a nivel general. Asimismo, la integridad de los datos obtuvo protección, asegurando que no se someterán a modificaciones ni a manipulaciones durante el análisis. Los datos se mantienen protegidos y su acceso está restringido exclusivamente a los investigadores responsables del estudio.

Alternativamente, se realizó un trabajo de manera responsable y transparente al interpretar los resultados sin introducir sesgos ni otras distorsiones que pudieran poner en riesgo la integridad de las conclusiones. Los resultados se informaron de forma objetiva, reflejando la realidad de las presentaciones observadas y percibidas en las organizaciones del estudio. Por último, la investigación se llevó a cabo de acuerdo con los principios de ética profesional y académica, utilizando fuentes de información correctamente, sin ningún tipo de plagio

8. Resultados

El presente estudio de caso múltiple se desarrolló en dos MiPymes ubicadas en Villavicencio, las cuales pertenecen a sectores económicos diferentes y utilizan herramientas tecnológicas para el desarrollo de sus procesos administrativos y contables. Con el propósito de garantizar la confidencialidad de la información y el anonimato de las organizaciones participantes, estas serán identificadas como Empresa A y Empresa B.

La Empresa A pertenece al sector de servicios relacionados con procedimientos estéticos y de belleza. Sus procesos contables y administrativos se apoyan en un software contable en la nube, además del uso de servidores y carpetas digitales para el almacenamiento y gestión documental de la información financiera. El área contable está conformada principalmente por un auxiliar contable, tesorero, auxiliar de recursos humanos y un contador con el cargo de (coordinador financiero), y cuenta con apoyo de un ingeniero de sistemas que brinda soporte técnico de manera remota y presencial cuando es requerido.

Por otra parte, la Empresa B pertenece al sector agroindustrial, específicamente al cultivo de palma de aceite. La organización también utiliza herramientas digitales para el manejo de la información contable, incluyendo software contable en la nube, almacenamiento en servidor y carpetas digitales. Su estructura contable es similar a la de la Empresa A, contando con un auxiliar contable, tesorero, auxiliar de recursos humanos y un contador con el cargo de (coordinador financiero). Adicionalmente, dispone de personal de apoyo tecnológico y profesional relacionado con las actividades operativas del sector agrícola.

Aunque ambas empresas presentan características similares en cuanto al uso de tecnologías de información y digitalización de procesos contables, durante la recolección de información se identificaron diferencias en el nivel de organización y gestión de los procesos administrativos y tecnológicos. En la Empresa A en este sentido una mayor estructuración en el manejo de la información y en los controles asociados al sistema contable. En contraste, la Empresa B presenta oportunidades de mejora relacionadas con la organización de la información, el seguimiento de procesos administrativos y el control de algunas actividades financieras y operativas.

La información analizada en esta investigación fue obtenida mediante la aplicación del cuestionario y entrevista semiestructurada realizadas al personal vinculado con el área contable y

financiera de cada organización. Se emplearon códigos de identificación según la empresa y el cargo desempeñado, tal como se presenta a continuación:

Tabla 8 *Códigos de identificación*

Código	Empresa	Cargo
E1-AF	Empresa A	Auxiliar financiero
E1-C	Empresa A	Contador
E2-AF	Empresa B	Auxiliar financiero
E2-C	Empresa B	Contador

8.1 Identificación de prácticas y condiciones:

Ambas organizaciones utilizan software contable en la nube, servidores y almacenamiento digital como parte de sus procesos operativos, evidenciando un nivel básico de digitalización de la información financiera y administrativa. Los sistemas permiten identificar usuarios, fechas y modificaciones realizadas dentro de la plataforma, lo que facilita la trazabilidad de los registros contables.

Sin embargo, en ambas empresas se identificaron debilidades relacionadas con la gestión formal de accesos, ya que la revisión y eliminación de usuarios se realiza de manera ocasional y sin procedimientos documentados. De igual forma, aunque cuentan con copias de seguridad automáticas, no existen controles periódicos para validar la recuperación de la información respaldada.

También se observó el uso frecuente de WhatsApp para compartir soportes financieros y autorizaciones, práctica que representa un riesgo en términos de seguridad y control documental. Asimismo, las capacitaciones en seguridad de la información se realizan de forma ocasional y no bajo programas estructurados.

A nivel comparativo, la Empresa A presenta una mayor organización tecnológica y controles operativos más definidos, mientras que la Empresa B evidencia una gestión más informal y dependiente de la comunicación verbal, especialmente en procesos financieros y presupuestales.

Estos resultados cuantitativos permitieron complementar los hallazgos obtenidos en las entrevistas semiestructuradas y fortalecer la interpretación integral del fenómeno analizado.

Tabla 9 *Resultados cuantitativos*

Categoría evaluada	Empresa A	Empresa B	Hallazgo comparativo
Software contable	SIIGO nube Pro	SIIGO nube básico	Diferencia en capacidad tecnológica
Gestión de accesos	Mayor control operativo	Control más informal	Diferencia en supervisión
Eliminación de usuarios	Ocasionalmente tardía	Ocasionalmente tardía	Debilidad compartida
Copias de seguridad	Automáticos	Automáticos	Sin validación de recuperación
Uso de WhatsApp	Frecuente	Frecuente	Riesgo compartido
Capacitación	Ocasional	Ocasional	Baja formalización
Soporte TI	Más estructurado	Más reactivo	Diferencia de madurez

El análisis comparativo permitió identificar que ambas empresas comparten debilidades relacionadas con formalización de controles, gestión documental y capacitación en seguridad de la información. Sin embargo, la Empresa A evidencia una estructura tecnológica relativamente más organizada, mientras que la Empresa B presenta mayor dependencia de procesos verbales y controles reactivos, situación que incrementa la exposición a riesgos operativos y limita la trazabilidad de la información financiera.

Con el fin de fortalecer la validez de los hallazgos y las respuestas por participante, junto con las frecuencias absolutas y porcentuales calculadas para cada hallazgo, se encuentra disponible en el Anexo C (Tablas C.1, C.2 y C.3), donde se presenta la evidencia estructurada del cuestionario que sustenta los análisis descritos en este capítulo.

8.2 Efectos de las prácticas de seguridad en la operatividad y confiabilidad

Uno de los principales aspectos identificados corresponde al manejo informal de procesos relacionados con autorizaciones, solicitudes de pagos y comunicación de información financiera mediante aplicaciones de mensajería instantánea como WhatsApp. Desde una perspectiva contable, esta práctica compromete directamente el principio de trazabilidad documental, dado que la información que soporta los registros financieros queda dispersa en conversaciones y dispositivos personales sin control institucional. Cuando los canales de comunicación financiera no son trazables ni verificables, se incrementa el riesgo de error en los estados financieros y se dificulta la reconstrucción de operaciones ante requerimientos de auditoría o fiscalización (Rey, 2024). Adicionalmente, la ausencia de un canal institucional impide verificar la integridad de las

autorizaciones, lo que en términos del modelo COSO-ERM representa una debilidad directa en el componente de Información, Comunicación y Reporte, cuya función es garantizar que la información relevante fluya de manera oportuna, exacta y a través de medios seguros (COSO, 2017).

La ausencia de procedimientos documentados para la revisión periódica de accesos y permisos dentro de los sistemas contables genera riesgos asociados a accesos innecesarios o a la permanencia de usuarios activos más allá del tiempo requerido. Aunque las empresas mantienen usuarios individuales con trazabilidad dentro del software, la falta de controles formales aumenta la dependencia de la supervisión manual y del criterio individual del personal disponible. Esta situación es coherente con lo señalado por Gómez Guevara (2025), quien identifica la ausencia de procedimientos de gestión de accesos como una de las principales brechas de seguridad en MiPymes colombianas, y confirma el nivel 1 (Inicial) asignado en el dominio DSS05 de COBIT 2019 para ambas organizaciones (ISACA, 2019).

En cuanto al respaldo de la información, se identificó que ambas organizaciones realizan copias de seguridad automáticas tanto en la nube como en servidores internos; sin embargo, ninguna ha efectuado pruebas periódicas de recuperación ni cuenta con procedimientos documentados de continuidad operativa. Esta condición es especialmente crítica desde el marco del control interno, dado que la existencia de un respaldo no verificado equivale, en términos operativos, a la ausencia de respaldo: si el procedimiento de recuperación falla ante un incidente real, los registros contables pueden resultar irrecuperables, comprometiendo tanto la continuidad de las obligaciones tributarias ante la DIAN como la integridad de la información financiera utilizada para la toma de decisiones (Rey, 2024; Sarmiento Suárez et al., 2024).

La dependencia del conocimiento empírico del personal evidencia limitaciones en la formalización organizacional para resolver incidentes relacionados con los sistemas contables. En ambas empresas, gran parte de las soluciones ante errores o situaciones inusuales dependen directamente del ingeniero de sistemas o de la experiencia acumulada por los trabajadores del área contable. Esta dependencia puede afectar la continuidad operativa en situaciones donde no exista disponibilidad inmediata del personal clave, y representa, desde COSO-ERM, una debilidad en el componente de Supervisión y Mejora, al no existir mecanismos institucionales que garanticen la respuesta organizacional con independencia del individuo disponible (COSO, 2017; Chidukwani et al., 2026).

La inexistencia de políticas formales de seguridad implica que, aunque el personal manifiesta tener conocimientos básicos sobre riesgos tecnológicos como correos fraudulentos o accesos sospechosos, las medidas preventivas implementadas se basan en recomendaciones generales y prácticas informales. Esta condición incrementa la exposición al riesgo cibernético, especialmente ante amenazas de phishing, robo de credenciales o manejo inadecuado de información financiera (Chidukwani et al., 2026; El Ferjani El Ferjani et al., 2025). En términos del modelo COSO-ERM, la ausencia de políticas representa una debilidad estructural en el componente de Gobierno y Cultura: sin lineamientos formalizados no es posible construir una cultura organizacional orientada a la prevención del riesgo, condición que COSO (2017) identifica como requisito base para la efectividad de cualquier sistema de control interno.

En términos generales, las situaciones identificadas muestran que las principales vulnerabilidades no se originan únicamente en la tecnología utilizada, sino también en factores organizacionales relacionados con informalidad operativa, ausencia de documentación y limitada cultura de gestión del riesgo. Estas condiciones afectan la confiabilidad, integridad y continuidad de la información contable, generando exposición frente a riesgos que, de materializarse, comprometerían tanto la toma de decisiones interna como el cumplimiento de obligaciones externas (Gómez Guevara, 2025; Sarmiento Suárez et al., 2024; Rey, 2024).

8.3 Análisis desde el modelo COSO-ERM

El análisis de los hallazgos se realizó tomando como referencia los componentes del modelo COSO-ERM, con el fin de evaluar la forma en que las MiPymes gestionan los riesgos cibernéticos relacionados con sus procesos contables y tecnológicos.

En el componente de gobierno y cultura, ambas empresas presentan debilidades en la formalización de políticas de seguridad y capacitación en ciberseguridad. No obstante, la Empresa A evidencia una mayor organización y supervisión sobre el manejo de la información, mientras que la Empresa B mantiene procesos más informales y dependientes de la comunicación verbal y herramientas como WhatsApp.

Respecto a estrategia y establecimiento de objetivos, se identificó que ninguna de las organizaciones incorpora formalmente el riesgo cibernético dentro de su planeación o evaluación

organizacional. Las decisiones relacionadas con seguridad tecnológica se realizan principalmente de manera reactiva y no preventiva.

En relación con el componente de desempeño, ambas empresas presentan vulnerabilidades asociadas al control de accesos, eliminación tardía de usuarios y ausencia de validación periódica de copias de seguridad. Estas condiciones incrementan el riesgo de pérdida de información y afectaciones en la confiabilidad de los registros contables.

En cuanto a revisión y mejora, no se evidenciaron procesos formales de monitoreo o auditoría tecnológica. Aunque ambas organizaciones cuentan con soporte técnico, este se orienta principalmente a resolver fallas operativas y no a la prevención de riesgos cibernéticos.

Finalmente, en el componente de información, comunicación y reporte, se identificó el uso frecuente de medios no institucionales para compartir información financiera, lo que limita la trazabilidad y seguridad de los datos contables.

En términos generales, ambas empresas presentan un nivel parcial de cumplimiento de los lineamientos COSO-ERM. Sin embargo, la Empresa A muestra una gestión relativamente más estructurada frente a la Empresa B, la cual evidencia mayores debilidades en supervisión, control interno y formalización de procesos tecnológicos.

Tabla 10 *Lineamientos COSO-ERM*

Componente COSO-ERM	Empresa A	Empresa B	Nivel identificado
Ambiente de control	Controles básicos parcialmente definidos	Controles mayormente informales	Bajo
Evaluación de riesgos	Reconocimiento básico de amenazas	Gestión reactiva	Bajo
Actividades de control	Trazabilidad y accesos individuales	Dependencia Informal	Medio-bajo
Información y comunicación	Uso frecuente de WhatsApp	Alta informalidad operativa	Bajo
Supervisión	Validaciones ocasionales	Supervisión reactiva	Bajo

8.4 Nivel de capacidad tecnológica

El análisis realizado evidencia que ambas organizaciones han incorporado herramientas tecnológicas para apoyar los procesos contables y financieros, especialmente mediante software

contable en la nube, almacenamiento digital y soporte técnico básico. No obstante, los resultados muestran niveles de capacidad limitados desde el enfoque COBIT 2019, debido a la baja formalización de procedimientos, la dependencia de controles manuales y la gestión reactiva de los riesgos tecnológicos.

En términos comparativos, la Empresa A presenta un mayor nivel de organización tecnológica y acompañamiento operativo, reflejado en mejores prácticas de control y soporte TI. Por su parte, la Empresa B mantiene procesos más informales y dependientes del conocimiento del personal, especialmente en actividades relacionadas con supervisión, control operativo y gestión de incidentes.

Los hallazgos también fueron interpretados tomando como referencia algunos objetivos de gestión establecidos en COBIT 2019. En relación con el objetivo **APO12 – Managed Risk**, cuyas actividades clave según COBIT 2019 incluyen recopilar datos sobre riesgos TI, mantener un perfil de riesgo actualizado y comunicar el estado del riesgo a los responsables de la organización (ISACA, 2019). En ambas empresas analizadas, ninguna de estas actividades se ejecuta formalmente. El cuestionario reveló que cuando algo falla en los sistemas "nunca se documenta lo ocurrido" (pregunta 20: opción Nunca), lo que impide construir el historial de incidentes necesario para alimentar un perfil de riesgo. La Empresa A recibió un correo sospechoso de posible phishing, pero la respuesta fue ignorarlo sin documentarlo ni reportarlo formalmente al área de sistemas. Este patrón reactivo, sin evaluación previa de amenazas ni registro por lo que corresponde a nivel 1 (Inicial) en APO12 para ambas organizaciones (ISACA, 2019).

Asimismo, respecto al objetivo **DSS05 – Managed Security Services**, las actividades definidas por COBIT 2019 para este objetivo incluyen gestionar la seguridad de accesos, proteger la información en los puntos de acceso monitorear la infraestructura para detectar eventos de seguridad (ISACA, 2019). Los resultados del cuestionario permitieron evaluar cada una de estas actividades con evidencia directa. En gestión de accesos: los usuarios de empleados retirados "quedan activos por un tiempo mientras se organiza" (pregunta 1, opción c), y los accesos se comparten "frecuentemente" entre compañeros cuando se necesita (pregunta 2, opción d). En protección de los puntos de acceso: el personal comparte información confidencial por WhatsApp personal, correo externo o memorias USB "frecuentemente" (pregunta 23). En detección de incidentes: ante un fallo en los controles, la detección ocurriría "cuando ya hubiera un problema visible" (pregunta 16, opción c). La Empresa A, con revisión informal mensual de accesos, alcanza

nivel 2 (Repetible) en DSS05. La Empresa B, sin estas prácticas consistentes, se ubica en nivel 1 (Inicial) (ISACA, 2019).

a) APO13 – Managed Security (Gestión de Seguridad)

El objetivo APO13 de COBIT 2019 establece que las organizaciones deben definir, operar y monitorear un sistema de gestión de seguridad de la información que proteja los activos de datos frente a amenazas internas y externas (ISACA, 2019). Las actividades clave que define este objetivo incluyen: establecer una política de seguridad documentada, asignar responsabilidades formales sobre la protección de la información, y realizar revisiones periódicas de la efectividad de los controles implementados. Los hallazgos del presente estudio indican que ninguna de las dos empresas cumple con estas actividades de manera formal. La Empresa A no cuenta con una política escrita de seguridad, aunque su participante E1-AF reconoció explícitamente que "sólo el personal del área correspondiente debería tener acceso a información sensible", lo que refleja conciencia de la necesidad sin formalización.

La Empresa B, con solo seis empleados, opera sin ninguna estructura de responsabilidades sobre seguridad: el participante E2-AF indicó que, ante una duda de seguridad, la acción sería simplemente "preguntar al ingeniero de sistemas". Esta dependencia de una persona no vinculada formalmente a un rol de seguridad confirma la ausencia de un sistema de gestión de seguridad. Conforme a los criterios de COBIT 2019, ambas organizaciones se ubican en nivel 0 (Inexistente) para APO13, dado que no existe una política de seguridad documentada, roles formalmente asignados ni procesos de revisión periódica de controles (ISACA, 2019).

b) EDM01 – Governed IT Framework (Marco de Gobierno TI)

El objetivo EDM01 de COBIT 2019 corresponde al dominio de gobierno y establece que la alta dirección debe definir y mantener un marco de gobierno que oriente cómo se utilizan, gestionan y controlan las tecnologías de la información dentro de la organización (ISACA, 2019). Sus actividades principales incluyen: establecer principios y políticas para el uso de TI, asignar responsabilidades de gobierno y asegurar la alineación entre la estrategia tecnológica y los objetivos del negocio. En el contexto de las empresas analizadas, este objetivo resulta especialmente significativo porque su ausencia no es solo un vacío técnico, sino un vacío de dirección estratégica.

En la Empresa A, las decisiones tecnológicas son tomadas por el ingeniero de sistemas en respuesta a solicitudes operativas canalizadas informalmente por WhatsApp, sin que exista un

marco de políticas ni criterios institucionales que guíen esas decisiones. En la Empresa B, la gestión tecnológica depende únicamente de la disponibilidad del soporte externo, sin ningún nivel de supervisión directiva. El cuestionario confirmó que en ambas empresas los procesos contables con componente tecnológico se documentan en "manuales o procedimientos escritos" según la pregunta 15, pero esta documentación no abarca los procesos de seguridad ni el gobierno de TI. En términos del modelo de capacidad de COBIT 2019, ambas organizaciones se ubican en nivel 0 (Inexistente) para EDM01, ya que no existe ningún marco de gobierno TI reconocido, documentado ni comunicado a la organización (ISACA, 2019).

c) DSS04 – Managed Continuity (Continuidad Operativa)

El objetivo DSS04 de COBIT 2019 exige que las organizaciones garanticen la continuidad de los servicios de información ante interrupciones, mediante planes documentados, pruebas periódicas de recuperación y procedimientos de gestión de crisis (ISACA, 2019). El análisis de los datos obtenidos muestra diferencias relevantes entre las dos empresas. La Empresa A demuestra capacidad básica de continuidad: ante una caída del sistema, el participante E1-AF describió un procedimiento claro de contingencia basado en trabajo en Excel con posterior carga al sistema, y el cuestionario confirmó la existencia de "un sistema alterno o procedimiento manual documentado" (pregunta 12, opción a). Sin embargo, este procedimiento no ha sido probado formalmente ni socializado con todos los empleados como política institucional. La Empresa B, en contraste, no realiza copias de seguridad regularmente (pregunta 10: "No se realizan copias de seguridad regularmente") y nunca ha verificado la recuperación de sus respaldos (pregunta 11: "No lo hemos hecho"). Estos hallazgos llevan a asignar nivel 2 (Repetible) a la Empresa A y nivel 1 (Inicial) a la Empresa B para el objetivo DSS04, reconociendo que la primera tiene prácticas de contingencia operativas, aunque informales, mientras la segunda carece de cualquier mecanismo documentado de continuidad (ISACA, 2019).

En síntesis, la evaluación desde COBIT 2019 permite concluir que ambas organizaciones operan con tecnología funcional para sus necesidades contables básicas, pero sin los procesos de gobierno, documentación y monitoreo que el modelo requiere para garantizar la seguridad, integridad y continuidad de la información financiera. Los niveles de capacidad identificados predominantemente 0 y 1 en los dominios de gobierno y seguridad, con un nivel 2 en continuidad operativa para la Empresa A confirman que el principal desafío no es técnico sino organizacional:

las empresas necesitan construir una cultura de gobierno TI que convierta las prácticas informales existentes en procesos reconocidos, documentados y sujetos a mejora continua (ISACA, 2019).

Las respuestas individuales que sustentan las asignaciones de nivel descritas en este apartado se encuentran sistematizadas en el Anexo C, Tabla C.1, permitiendo verificar la coherencia entre los datos recopilados y la interpretación analítica presentada.

Tabla 11 *Asignaciones de nivel*

Nivel	**0**	**1**	**2**	**3**	**4**	**5**
Descripción	Inexistente	Inicial	Repetible	Definido	Gestionado	Optimizado

Figura 3 *Niveles de capacidad (0 a 5)*

Nota. Imagen tomada de ISACA Argentina. (2019). COBIT 2019.Imagen. IAIA

Tabla 12 *Hallazgos*

Dominio COBIT 2019	**Empresa A**	**Empresa B**	**Justificación**
DSS05- Gestión de Servicios de Seguridad	Nivel 2	Nivel 1	Empresa A revisa accesos mensualmente de forma informal; Empresa B sin proceso de gestión de accesos. Ambas con uso compartido de credenciales frecuente
APO12- Gestión del riesgo	Nivel 1	Nivel 1	Ambas empresas llaman directamente al ingeniero o proveedor sin protocolo definido; ningún incidente ha sido documentado formalmente

Dominio COBIT 2019	Empresa A	Empresa B	Justificación
DSS04- Continuidad operativa	Nivel 2	Nivel 1	Empresa A tiene procedimiento alterno documentado (Excel); Empresa B no cuenta con una forma de continuidad alterna.
Soporte TI	Nivel 2	Nivel 1	Empresa A: No cuentan con proceso formalizados, ni trazabilidad, pero si hay una persona encargada. Empresa B: no hay estructura, no hay continuidad, no hay control pero cuentan con ayuda del ingeniero.
APO13 – Gestión de Seguridad	Nivel 0	Nivel 0	Ninguna empresa cuenta con política de seguridad escrita ni roles formales de protección de información. Conciencia informal sin institucionalización
EDM01 – Marco de Gobierno TI	Nivel 0	Nivel 0	Ninguna empresa dispone de marco de gobierno TI. Decisiones tecnológicas sin criterios documentados ni alineación estratégica

Conclusiones

La investigación permitió identificar que las MiPymes analizadas presentan una alta dependencia de herramientas tecnológicas para el desarrollo de sus procesos contables y administrativos; sin embargo, la adopción de estas tecnologías no se encuentra acompañada de controles formales suficientes para gestionar los riesgos cibernéticos asociados.

En respuesta al primer objetivo específico, ambas organizaciones cuentan con software contable en la nube y también utilizan el almacenamiento digital y los medios electrónicos para gestionar la información financiera. No obstante, se observaron ciertas prácticas que aumentaron la exposición al riesgo cibernético: el uso frecuente de WhatsApp para el intercambio de documentos financieros, la ausencia de procedimientos formalizados y documentados para la gestión de accesos y la falta de validación periódica de las copias de seguridad.

Respecto al segundo objetivo, se comprobó que estas prácticas interfieren con el funcionamiento y la confiabilidad de la información contable, ya que generan riesgos de pérdida de trazabilidad, errores en los registros, interrupciones en las operaciones y un posible acceso no autorizado a datos sensibles. Estas situaciones generan intervenciones manuales, algunas de las cuales tienen un impacto directo sobre la autenticidad, la disponibilidad y la precisión de la información financiera utilizada para la toma de decisiones.

En cuanto al tercer objetivo, el análisis desde COSO-ERM permitió evidenciar debilidades principalmente en los componentes de evaluación de riesgos, supervisión y formalización de controles internos. Aunque ambas empresas cuentan con mecanismos básicos de control, gran parte de los procesos depende de prácticas informales y del conocimiento empírico del personal. Ninguna de las dos organizaciones incorpora formalmente el riesgo cibernético en su planeación estratégica ni cuenta con políticas documentadas que soporten el componente de Gobierno y Cultura que COSO (2017) establece como fundamento de un sistema de control interno efectivo. Esta ausencia no es un vacío técnico aislado, sino una condición organizacional que limita estructuralmente la capacidad de respuesta ante incidentes y refuerza la gestión reactiva identificada en ambas empresas (Gordillo, 2024; Gómez Guevara, 2025).

De igual manera, el análisis desde COBIT 2019 permitió identificar que ambas organizaciones operan con niveles de capacidad predominantemente iniciales o inexistentes en los dominios de gobierno y seguridad. En particular, la asignación del nivel 0 (Inexistente) en EDM01

para ambas empresas evidencia que las decisiones tecnológicas se toman sin criterios documentados ni alineación estratégica, lo que según COSO-ERM constituye una debilidad en el componente de Gobierno y Cultura que trasciende lo puramente tecnológico y afecta la integración entre control interno y gestión TI. El nivel 1 (Inicial) identificado en APO13 confirma que, si bien existe conciencia individual sobre la necesidad de proteger la información, esta no ha sido institucionalizada, por lo que no es posible hablar de un sistema de gestión de seguridad en términos formales (ISACA, 2019; El Ferjani El Ferjani et al., 2025).

En conclusión, el riesgo cibernético en las MiPymes analizadas no se explica únicamente por factores tecnológicos, sino también por aspectos organizacionales como la cultura de control, la formalización de los procesos y la gestión proactiva del riesgo. El desarrollo de un marco de controles internos documentados, prácticas de seguridad formalizadas y principios básicos de gobernanza tecnológica resulta fundamental para mejorar la confiabilidad y la resiliencia de la información contable en entornos digitales (COSO, 2017; ISACA, 2019; Sarmiento Suárez et al., 2024).

Recomendaciones

A partir de los hallazgos obtenidos en el presente estudio de caso múltiple y de la evaluación realizada desde los marcos COSO-ERM y COBIT 2019, se formulan a continuación recomendaciones dirigidas a las MiPymes analizadas. Estas propuestas tienen como propósito orientar la mejora progresiva de las prácticas de seguridad de la información, el fortalecimiento del control interno y el desarrollo de una cultura organizacional más estructurada frente a la gestión del riesgo cibernético.

Recomendaciones asociadas al Objetivo Específico 1

Las recomendaciones se presentan organizadas por objetivo específico, con el fin de garantizar su coherencia con los propósitos planteados en la investigación.

a) Formalización de los controles de acceso a los sistemas contables

Una de las vulnerabilidades identificadas con mayor frecuencia en ambas organizaciones corresponde a la ausencia de procedimientos documentados para la gestión de accesos a los sistemas contables. Se evidenció que los usuarios de empleados desvinculados permanecen activos de manera temporal sin un proceso formal de baja, y que las credenciales son compartidas entre compañeros ante necesidades operativas puntuales. Estas situaciones incrementan el riesgo de accesos no autorizados y dificultan la trazabilidad de las operaciones registradas en el sistema.

Con el fin de mitigar esta exposición, se recomienda a ambas organizaciones establecer un procedimiento escrito y de aplicación obligatoria para la creación, modificación y eliminación de usuarios. Dicho procedimiento debe contemplar que la desactivación de un usuario sea ejecutada por el coordinador financiero el mismo día en que se produce la desvinculación del colaborador, sin excepciones. Adicionalmente, se debe prohibir de manera formal el préstamo o uso compartido de credenciales, incluso entre miembros del mismo equipo de trabajo.

Como medida de apoyo, se sugiere mantener un registro actualizado de los usuarios activos del sistema contable en un documento de fácil acceso para el coordinador financiero, en el que se consignen el nombre del usuario, el cargo, la fecha de creación del acceso y la fecha de su eventual desactivación. Este registro puede gestionarse en una hoja de cálculo sencilla y revisarse mensualmente como práctica de control mínimo.

b) Sustitución del canal informal para el intercambio de información financiera

El uso frecuente de aplicaciones de mensajería instantánea como WhatsApp para compartir soportes contables, autorizaciones de pago e información financiera sensible representa un factor de riesgo significativo en ambas organizaciones. Esta práctica genera dispersión de la información en dispositivos personales, dificulta su trazabilidad y compromete la confidencialidad de los datos.

Se recomienda adoptar un canal institucional formal para la comunicación y el intercambio de documentos financieros. En el corto plazo, esto puede lograrse mediante el uso de una cuenta de correo electrónico corporativa destinada exclusivamente a este tipo de comunicaciones, con copia al área contable y respaldo automático. A mediano plazo, se sugiere evaluar la implementación de plataformas de colaboración con control de acceso y registro de actividad, como las disponibles en entornos de productividad empresarial de bajo costo. En cualquier caso, el criterio fundamental es garantizar que toda comunicación relacionada con operaciones financieras quede registrada en un medio institucional trazable y recuperable.

Recomendaciones asociadas al Objetivo Específico 2

a) Verificación periódica de la integridad de las copias de seguridad

Ambas organizaciones realizan copias de seguridad automáticas a través de los sistemas en la nube que utilizan; sin embargo, ninguna de las dos ha verificado en algún momento si dicha información puede ser efectivamente recuperada ante una falla o pérdida de datos. Esta situación implica que la continuidad operativa de los procesos contables descansa sobre un supuesto de funcionamiento que no ha sido comprobado.

Se recomienda establecer una prueba trimestral de recuperación de información, la cual no requiere restaurar la totalidad del sistema, sino verificar que al menos un conjunto representativo de registros o documentos pueda ser accedido y recuperado desde el respaldo disponible. El resultado de cada prueba debe quedar consignado en un documento de seguimiento con la fecha de realización, el responsable y el resultado obtenido. Esta práctica, aunque simple, constituye un control documentado que fortalece la confiabilidad operativa de los sistemas de respaldo.

b) Documentación de un procedimiento de contingencia operativa

El análisis realizado permitió identificar que, ante una caída del sistema contable, las organizaciones no cuentan con un protocolo formalmente definido y socializado para garantizar la

continuidad de los registros. Si bien la Empresa A dispone de una práctica informal basada en el uso de hojas de cálculo como alternativa temporal, esta no se encuentra documentada ni es conocida de manera uniforme por todos los integrantes del equipo.

Se recomienda redactar un procedimiento de contingencia de una sola página, en el que se describa claramente qué debe hacer cada miembro del área contable en caso de que el sistema no esté disponible: qué actividades pueden continuar de forma manual o en herramientas alternas, cómo deben registrarse temporalmente las operaciones y cuál es el proceso para cargar esa información al sistema una vez restablecido el servicio. Este documento debe ser socializado con todo el equipo y revisado al menos una vez al año.

c) Implementación de un registro de incidentes tecnológicos

En ninguna de las dos organizaciones estudiadas existe un registro formal de los incidentes relacionados con los sistemas de información. Las situaciones inusuales, como correos sospechosos, errores en el sistema o accesos inesperados, se resuelven de manera individual sin dejar constancia de lo ocurrido ni de las acciones tomadas. Esta ausencia de documentación impide identificar patrones de riesgo y limita la capacidad de respuesta preventiva de las organizaciones.

Se recomienda crear un registro de incidentes en un formato sencillo, que puede ser una hoja de cálculo compartida entre el área contable y el soporte técnico, donde se registre como mínimo la fecha del incidente, una descripción breve de lo ocurrido, quién lo detectó y qué acción se tomó. El registro no debe concebirse como un mecanismo de control punitivo, sino como una herramienta de aprendizaje organizacional que permite mejorar la gestión del riesgo tecnológico a partir de la experiencia acumulada.

Recomendaciones asociadas al Objetivo Específico 3 (COSO-ERM)

Las debilidades identificadas en la evaluación desde el modelo COSO-ERM apuntan principalmente a la ausencia de una cultura formal de gestión del riesgo dentro de las organizaciones. Las recomendaciones que se presentan a continuación buscan fortalecer los componentes del modelo que evidenciaron mayores oportunidades de mejora.

a) Gobierno y cultura: asignación formal de responsabilidades en seguridad

Ninguna de las dos organizaciones cuenta con una política escrita de seguridad de la información ni con roles formalmente asignados para la protección de los datos contables. Las

decisiones relacionadas con la seguridad tecnológica se toman de manera reactiva y dependen del criterio individual del personal disponible en cada momento.

Se recomienda que el coordinador financiero asuma formalmente, dentro de su perfil de cargo, la responsabilidad de supervisar el cumplimiento de los controles de acceso, la validación de copias de seguridad y el registro de incidentes. Esta asignación no implica la contratación de nuevo personal, sino la formalización de funciones que ya se ejercen de manera parcial e informal. Igualmente, se sugiere redactar un documento breve de política de seguridad que establezca las reglas básicas para el manejo de la información financiera, el uso de dispositivos y el acceso a los sistemas contables.

b) Evaluación de riesgos: incorporación del riesgo cibernético en la planeación

El análisis evidenció que ninguna de las organizaciones incorpora formalmente el riesgo cibernético dentro de sus procesos de planeación o evaluación organizacional. Las amenazas tecnológicas son reconocidas a nivel individual por el personal del área contable, pero no se gestionan desde una perspectiva institucional estructurada.

Se recomienda incluir, al menos una vez al año, una revisión del entorno tecnológico como parte de los procesos de planeación de cada organización. Esta revisión puede realizarse en un formato muy básico, identificando las principales amenazas a los sistemas contables (pérdida de acceso, errores de registro, acceso no autorizado), evaluando si los controles existentes son suficientes y definiendo acciones concretas de mejora para el siguiente periodo.

c) Supervisión y mejora: capacitación periódica en seguridad de la información

Las capacitaciones en seguridad de la información se realizan de forma ocasional y sin una estructura programada en ambas organizaciones. El personal manifiesta tener nociones generales sobre amenazas como el phishing o el uso inadecuado de contraseñas, pero estas no han sido consolidadas en prácticas institucionales sostenidas.

Se recomienda destinar al menos treinta minutos mensuales, dentro de las reuniones de equipo ya existentes, para abordar un tema específico de seguridad de la información. Los temas pueden rotar entre aspectos como la identificación de correos fraudulentos, el manejo seguro de contraseñas, el uso adecuado de dispositivos personales y corporativos, y la protección de documentos financieros. Esta práctica no requiere inversión económica adicional y puede apoyarse en los recursos gratuitos disponibles en plataformas como el SENA o el Ministerio TIC de Colombia.

La siguiente tabla resume la alineación de las recomendaciones planteadas con los componentes del modelo COSO-ERM:

Tabla 13 *Recomendaciones para el componente del modelo COSO-ERM*

Recomendación	Componente COSO-ERM fortalecido
Formalización de controles de acceso	Actividades de control
Sustitución del canal informal (WhatsApp)	Información, comunicación y reporte
Verificación de copias de seguridad	Actividades de control / Supervisión
Procedimiento de contingencia operativa	Supervisión y revisión
Registro de incidentes tecnológicos	Evaluación de riesgos
Asignación formal de responsabilidades	Gobierno y cultura
Incorporación del riesgo cibernético en planeación	Evaluación de riesgos
Capacitación periódica en seguridad	Gobierno y cultura

Recomendaciones asociadas al Objetivo Específico 4 (COBIT 2019)

Con base en los niveles de capacidad identificados para cada dominio de COBIT 2019, las recomendaciones formuladas en los apartados anteriores contribuyen directamente a avanzar en la escala de madurez tecnológica de las organizaciones. A continuación, se presenta una síntesis del impacto esperado de dichas recomendaciones sobre los dominios evaluados.

En relación con el dominio APO12 (Gestión del Riesgo), la implementación del registro de incidentes y la incorporación del riesgo cibernético en los procesos de planeación permitirían a ambas organizaciones avanzar del nivel 1 (Inicial) al nivel 2 (Repetible), al establecer una práctica sistemática de recopilación de datos sobre amenazas y una evaluación básica del perfil de riesgo tecnológico.

Respecto al dominio DSS05 (Gestión de Servicios de Seguridad), la formalización de los controles de acceso y la prohibición del uso compartido de credenciales contribuirían a que la Empresa A consolide su nivel 2 (Repetible) y a que la Empresa B avance del nivel 1 al nivel 2, mediante la definición de prácticas consistentes y documentadas para la protección de los accesos al sistema contable.

En cuanto al dominio APO13 (Gestión de la Seguridad), la elaboración de una política de seguridad básica y la asignación formal de responsabilidades sobre la protección de la información permitirían a ambas organizaciones transitar del nivel 1 (Inicial) al nivel 2 (Repetible), al contar con un marco mínimo de referencia para la toma de decisiones en materia de seguridad.

Para el dominio DSS04 (Continuidad Operativa), la documentación del procedimiento de contingencia y la verificación periódica de las copias de seguridad posibilitarían que la Empresa A consolide su nivel 2 (Repetible) y que la Empresa B avance desde el nivel 1, al establecer mecanismos documentados y probados de respuesta ante interrupciones del servicio.

Finalmente, en lo que corresponde al dominio EDM01 (Marco de Gobierno TI), la asignación formal de responsabilidades tecnológicas al coordinador financiero y la elaboración de lineamientos básicos para el uso de los sistemas de información representarían el primer paso para que ambas organizaciones avancen del nivel 0 (Inexistente) al nivel 1 (Inicial), al contar con al menos un referente documentado que oriente las decisiones tecnológicas desde la perspectiva del gobierno organizacional.

La siguiente tabla presenta de manera consolidada el estado actual y el avance esperado en los dominios de COBIT 2019 evaluados, a partir de la implementación de las recomendaciones propuestas:

Tabla 14 *Avance esperado en los dominios de COBIT 2019 evaluados*

Dominio COBIT 2019	Empresa A Actual	Empresa A Esperado	Empresa B Actual	Empresa B Esperado
APO12 – Gestión del Riesgo	Nivel 1	Nivel 2	Nivel 1	Nivel 2
DSS05 – Gestión de Seguridad	Nivel 2	Nivel 2-3	Nivel 1	Nivel 2
APO13 – Gestión de Servicios de Seguridad	Nivel 1	Nivel 2	Nivel 1	Nivel 2
DSS04 – Continuidad Operativa	Nivel 2	Nivel 2-3	Nivel 1	Nivel 2
EDM01 – Marco de Gobierno TI	Nivel 0	Nivel 1	Nivel 0	Nivel 1

En síntesis, las recomendaciones formuladas no demandan inversiones tecnológicas de gran envergadura ni transformaciones estructurales inmediatas. Su valor radica en la formalización progresiva de prácticas que ya existen de manera informal en las organizaciones, convirtiéndolas en procesos reconocidos, documentados y sujetos a revisión periódica. Este enfoque gradual resulta especialmente pertinente para el contexto de las MiPymes, donde los recursos disponibles son limitados pero la necesidad de fortalecer la gestión del riesgo cibernético es igualmente real y urgente.

Bibliografía

Alonso, M. M. (2023). El estudio de casos como método de investigación cualitativa: Aproximación a su estructura, principios y especificidades. *Diversidad académica, 2*(2), 243–260. https://diversidadacademica.uaemex.mx/article/view/20623

Barreto Ascona, J. I., & Lezcano Mencia, A. (2023). Análisis y fundamentación de los diseños de investigación: explorando los enfoques cuantitativos, cualitativos y mixtos basados en Creswell y Creswell (2018). *Revista UNIDA Científica*, *7*(2), 110–117. https://revistacientifica.unida.edu.py/publicaciones/index.php/cientifica/article/view/179

Chávez Buitrago, Y. A. (2024). *Impacto de la implementación de la factura electrónica en la lucha contra el lavado de activos: análisis jurídico y tecnológico en Colombia* [Tesis de grado, Universidad Externado de Colombia]. Repositorio Institucional. https://doi.org/10.60909/bdigital/handle.001.12013

Chidukwani, A., Zander, S., & Koutsakis, P. (2026). Beyond self-reporting: Uncovering the operational realities of SME cybersecurity through expert assessment. *Computers & Security*. 164. 1-23. https://doi.org/10.1016/j.cose.2026.104839

Comisión de Regulación de Comunicaciones (CRC). (2025). *Análisis prospectivo en materia de ciberseguridad*. https://www.crcom.gov.co/system/files/Biblioteca%20Virtual/An%C3%A1lisis%20prospectivo%20en%20materia%20de%20ciberseguridad/analisis-prospectivo-ciberseguridad-261225.pdf

Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Gestión del riesgo empresarial: Integrando estrategia y desempeño: Resumen ejecutivo*. COSO. https://iaiecuador.org/documentos/Resumen_ejecutivo_cosoERM.pdf

El Ferjani El Ferjani, I., Alcañiz Zanón, M., & Santolino Prieto, M. A. (2025). Ciberseguridad en pequeñas y medianas empresas: vulnerabilidades, amenazas y desarrollo del ciberseguro. *Anales Del Instituto De Actuarios Españoles*, (31), 1–17. https://doi.org/10.26360/2025_01

Gómez Guevara, L. E. (2025). *Ciberseguridad en PYMES del sector digital y publicitario en Colombia: Guía práctica para mitigar riesgos compartidos entre empresas que contratan o prestan servicios digitales*. [Trabajo de grado, Universidad Nacional Abierta y a

Distancia (UNAD)]. Repositorio Institucional. https://repository.unad.edu.co/jspui/bitstream/10596/75862/1/legomezgue.pdf

Gordillo, A. (2024). Estrategias de ciberseguridad para MiPymes del sector terciario. *European Public & Social Innovation Review, 9*, 1–19. https://epsir.net/index.php/epsir/article/view/293

Hoong, Y., & Rezania, D. (2024). Navigating cybersecurity governance: The influence of opportunity structures in sociotechnical transitions for small and medium-sized enterprises. *Technology in Society*. 142. 1-15. https://www.sciencedirect.com/science/article/pii/S0167404824001536

Hoong, Y., Rezania, D., & Baker, R. (2024). When traditional SME managers encounter cybersecurity: Discourse analysis of opportunities and dilemmas in meeting the demands. *Technology in Society*. 78. 1-11. https://doi.org/10.1016/j.techsoc.2024.102650

Information Systems Audit and Control Association (ISACA). (2019). *COBIT 2019 framework: Governance and management objectives*. ISACA. https://www.isaca.org/resources/cobit

Information Systems Audit and Control Association (ISACA). (2019). *COBIT 2019*. https://iaia.org.ar/wp-content/uploads/2019/07/COBIT2019-IAIA.pdf

Rey, M. L. (2024). Análisis de los riesgos regulatorios en la información contable de las PyMES de Villavicencio según la normativa internacional de auditoría en Colombia. *Revista Dilemas Contemporáneos: Educación, Política y Valores*. 71(1). 1-24. https://dilemascontemporaneoseducacionpoliticayvalores.com/index.php/dilemas/article/view/4345/4193

Sarmiento Suárez, J. E., Gutiérrez Navas, E. B., & Ramírez Montañez, J. C. (2024). Oportunidades y desafíos para la digitalización de las MiPymes en Colombia. *Revista científica Pensamiento y Gestión* 57(57):128-154. https://doi.org/10.14482/pege.57.240.855

Suescum Coelho, C.-E., Monasterio-Pérez, J., Palumbo, A., & Suescum Coelho, C. (2025). Estrategia para la Gestión de Riesgos Financieros de las Entidades Aseguradoras Venezolanas. *Ciencia Latina Revista Científica Multidisciplinar*, *9*(2), 1842-1866. https://doi.org/10.37811/cl_rcm.v9i2.17017

Anexos

Anexo A. *Guía de entrevista semiestructurada*

Guía de entrevista semiestructurada dirigida a MiPymes de Villavicencio

Objetivo: Comprender la gestión del riesgo cibernético en la operatividad y en la información contable desde la perspectiva de los responsables administrativos y contables.

a) Contexto tecnológico

Si hoy necesitan revisar un registro contable del año pasado, ¿cómo lo buscarían? ¿Qué herramienta o sistema abrirían primero? • Revela qué software usan realmente, sin que nombren uno por compromiso.
Si hoy el computador principal de contabilidad dejara de funcionar, ¿desde dónde podrían seguir accediendo a la información? • Descubre dónde está almacenada la información realmente (nube, local, ambos).
¿Quién más, además del área contable, puede consultar los estados financieros o registros en el sistema? ¿Cómo se le da ese acceso a alguien nuevo? • Mapea quién tiene acceso real y si existe un proceso formal de asignación.
Si una persona de otra área quisiera consultar información del sistema contable, ¿qué tendría que hacer para lograrlo? • Evidencia si hay controles de acceso o si el sistema es abierto en la práctica.
Cuénteme cómo es el proceso cuando el software contable lanza una actualización: ¿quién decide cuándo actualizarlo, ¿quién lo hace? • Identifica si las actualizaciones se gestionan o si simplemente "se instalan cuando toca".
Si pudiera elegir una sola mejora tecnológica para el área contable en este momento, ¿cuál sería y por qué? • Al proponer mejoras, el entrevistado revela lo que siente que falta.

b) Experiencia con riesgos cibernéticos

Imagine que alguien intenta ingresar al sistema contable sin permiso. ¿Cómo se enterarían? ¿Qué pasaría después? • Si no saben responder el escenario, ese silencio ya es un dato: no tienen mecanismo de detección.
Pensando en los últimos meses, ¿ha habido algún momento en que el sistema no funcionó como se esperaba? ¿Qué ocurrió y cómo lo resolvieron? • Enmarca los incidentes como algo "normal" que les pasa a todos, reduciendo la defensiva.
Si mañana encontraran que la información contable fue modificada sin que nadie del área lo haya hecho, ¿qué harían? ¿A quién llamarían primero? • Examina si existe un protocolo de respuesta a incidentes o si la reacción fuera improvisada.
¿Ha recibido usted o alguien del equipo, mensajes, correos o llamadas sospechosas relacionadas con la empresa o sus sistemas? ¿Qué hicieron en ese momento? • Sondea exposición a phishing o ingeniería social de manera no amenazante.

c) Impacto en la operatividad y en la información contable

Si hoy, por la mañana, ¿el sistema contable se encuentra caído?, ¿cómo continuarían trabajando ese día? ¿Tiene la empresa un plan para eso? • Evalúa la continuidad operativa real sin preguntar directamente "¿tienen plan de continuidad?".
Si tuvieran que reconstruir toda la contabilidad del último mes desde cero hoy, ¿podrían hacerlo? ¿Desde dónde sacarían la información?

• Prueba la existencia y accesibilidad real de los respaldos.
¿Cuánto tiempo creen que tardarían en retomar operaciones normales si el sistema principal fallara completamente? • Obliga a estimar un tiempo real, lo que revela qué tan preparados están.
¿Cómo verifican que un registro contable es correcto antes de cerrarlo? ¿Hay alguien que revise lo que otro ingresó? • Identifica controles de doble revisión o si una sola persona registra y aprueba.
¿Alguna vez han tenido que rehacer un informe contable o corregir información porque algo salió mal en el sistema? ¿Qué implicó eso? • Normaliza el error para que cuenten experiencias reales sin sentirse juzgados.
Imagine que alguien del equipo contable renuncia hoy. Paso a paso, ¿qué haría la empresa con su usuario, sus contraseñas y sus accesos al sistema? • Revela si existe un procedimiento real o si los accesos simplemente quedan activos.
¿Cómo sabría usted si alguien revisó o modificó un registro contable que no debía? ¿El sistema guarda ese tipo de información? • Indaga sobre trazabilidad y auditoría de registros sin usar el término técnico.
¿Quién puede modificar un registro que ya fue guardado en el sistema? ¿Eso queda registrado en algún lugar? • Evalúa si hay restricciones de modificación o si cualquiera puede cambiar lo que sea.
¿Con qué frecuencia alguien revisa que los accesos al sistema estén actualizados? ¿Cómo se hace esa revisión? • Si no recuerdan cuándo fue la última vez, eso ya dice mucho. Si alguien de fuera de la empresa le pidiera prestado el usuario para consultar algo puntual en el sistema, ¿qué pasaría? ¿Hay algo que lo impida? • Sondea el uso compartido de credenciales de forma no confrontaciones. ¿Alguna vez alguien externo, como un contador asesor o un técnico, ha tenido que acceder al sistema? ¿Cómo se manejó eso? • Detecta accesos de terceros sin controles, que suelen ser el punto más débil. ¿Qué aspectos de la seguridad de la información cree usted que la empresa debería fortalecer primero? • Pregunta de cierre que captura la percepción del entrevistado sobre sus propios vacíos.

d) Cultura organizacional y capacitación

Cuando alguien nuevo entra al área contable, ¿cómo aprende a usar el sistema? ¿Hay alguien que lo guíe o aprende solo? • Revela si la inducción incluye aspectos de seguridad o si es solo operativa.
Si alguien del equipo no supiera cómo proteger bien la información que maneja, ¿cómo podría aprenderlo dentro de la empresa? • Detecta si hay capacitación real o si el conocimiento de seguridad es informal.
Si usted pudiera cambiar una sola cosa en la forma en que el equipo maneja la información contable, ¿qué sería? • Pregunta de cierre de sección: siempre revela el dolor más real del entrevistado.

Anexo B. *Cuestionario de control*

Accesos y uso de sistemas		
N.º	**Pregunta**	**Opciones de respuesta**
1	Cuando un empleado del área contable se va de la empresa, ¿qué ocurre con su acceso al sistema?	a) Se elimina el mismo día de su salida
		b) Se elimina en los días siguientes
		c) Queda activo por un tiempo mientras se organiza
		d) No tenemos un procedimiento definido para esto
2	¿Es posible que alguien acceda al sistema contable usando el usuario de un compañero si lo necesita?	a) Sí
		b) No
3	¿Los accesos al sistema están diferenciados según el rol (quien registra no puede también aprobar)?	a) Sí
		b) No
4	¿Con qué frecuencia se revisa quién tiene acceso al sistema contable para verificar que los permisos estén actualizados?	a) Hay una revisión programada periódicamente (mensual, trimestral o similar)
		b) Se revisa cuando cambia algún empleado
		c) No se ha revisado formalmente
Calidad e integridad de la información		
N.º	**Pregunta**	**Opciones de respuesta**
5	Cuando alguien registra un dato en el sistema contable, ¿qué sucede antes de que ese dato quede guardado definitivamente?	a) El sistema tiene validaciones automáticas
		b) Otra persona lo revisa antes de confirmarlo
		c) Quien lo ingresa lo verifica antes de guardar
		d) Se guarda directamente sin pasos adicionales
6	¿Cualquier persona con acceso al sistema puede modificar registros ya guardados sin necesidad de autorización?	a) Sí
		b) No
7	Si se detecta una inconsistencia en un registro contable, ¿qué ocurre normalmente?	a) Se analiza la causa antes de corregirlo
		b) Se corrige de inmediato sin mayor análisis
		c) Depende de quién lo encuentre
		d) No tenemos un proceso definido para eso
Respaldo y continuidad		
N.º	**Pregunta**	**Opciones de respuesta**
8	¿Con qué frecuencia se realizan copias de seguridad de la información contable?	a) Automáticamente, con una frecuencia programada
		b) Manualmente, cuando alguien lo recuerda
		c) Se hacen, pero sin frecuencia definida
		d) No se realizan copias de seguridad regularmente
9	¿Se ha comprobado alguna vez que los respaldos realmente funcionan (que la información se puede recuperar)?	a) Sí
		b) No
10	Si el sistema contable principal dejara de funcionar hoy, la empresa podría continuar sus operaciones porque…	a) Tiene un sistema alterno o procedimiento manual documentado
		b) El equipo sabe qué hacer, aunque no esté documentado
		c) Se improvisaría según la situación

Accesos y uso de sistemas		
		d) Las operaciones se detendrían hasta restaurar el sistema
11	¿Las copias de seguridad se guardan en un lugar separado del equipo principal (otra ubicación física o en la nube)?	a) Sí
		b) No
Supervisión y control interno		
N.º	**Pregunta**	**Opciones de respuesta**
12	¿De qué manera se documentan los procesos contables en la empresa?	a) Están documentados en manuales o procedimientos escritos actualizados
		b) Están anotados informalmente (correos, notas, mensajes)
		c) El conocimiento está en las personas, no en documentos
		d) No están documentados
13	Si los controles de seguridad de la información no funcionaran bien, ¿cómo se enterarían?	a) Hay alertas o reportes automáticos que lo indicarían
		b) Alguien lo detectaría en una revisión rutinaria
		c) Probablemente cuando ya hubiera un problema visible
		d) No tenemos un mecanismo claro para detectarlo
14	¿Existe un conjunto de reglas o políticas escritas sobre cómo proteger la información contable?	a) Sí
		b) No
15	Cuando algo inusual ocurre en el sistema, ¿qué pasa normalmente?	a) Se sigue un protocolo definido de atención
		b) Se llama a quien habitualmente resuelve los problemas
		c) Cada persona lo maneja a su manera
		d) Se espera a ver si se resuelve solo
16	Cuando se presenta un problema en los sistemas, ¿se documenta lo ocurrido para evitar que vuelva a pasar?	a) Sí
		b) No
17	Cuando alguien nuevo ingresa al área contable, ¿qué formación recibe sobre el manejo seguro de la información?	a) Hay un proceso de inducción estructurado que incluye seguridad de la información
		b) Un compañero lo guía informalmente
		c) Aprende usando el sistema directamente
		d) No hay una formación específica para esto
18	¿El personal comparte información confidencial de la empresa por canales no seguros (WhatsApp personal, correo externo, memorias USB)?	a) Sí
		b) No
19	¿El personal sabe exactamente qué puede y qué no puede hacer con la información contable que maneja?	a) Sí
		b) No

Anexo C. *Consolidado de resultados del cuestionario de control*

El instrumento fue aplicado de manera complementaria a las entrevistas semiestructuradas, con el propósito de obtener información estructurada sobre el nivel de implementación de controles, la frecuencia de exposición a riesgos cibernéticos y las prácticas de gestión tecnológica en cada organización.

Los participantes se identifican mediante los siguientes códigos, de acuerdo con la empresa y el cargo desempeñado:

Tabla 15 *Consolidación de respuestas por participante*

Código	Empresa	Cargo
E1-AF	Empresa A	Auxiliar financiero / contable
E1-C	Empresa A	Contador (Coordinador financiero)
E2-AF	Empresa B	Auxiliar financiero / contable
E2-C	Empresa B	Contador (Coordinador financiero)

La siguiente tabla presenta, de forma consolidada, las respuestas obtenidas de cada participante para las 19 preguntas del cuestionario de control. Las respuestas se registran conforme a las opciones definidas en el instrumento original o como afirmación/negación, según el tipo de pregunta.

Tabla 16 *Respuestas del cuestionario de control*

N°	Pregunta (resumida)	E1-AF Emp. A	E1-C Emp. A	E2-AF Emp. B	E2-C Emp. B
1	Cuando un empleado se va, ¿qué ocurre con su acceso al sistema?	c) Queda activo un tiempo	c) Queda activo un tiempo	c) Queda activo un tiempo	d) Sin procedimiento definido
2	¿Es posible acceder con el usuario de un compañero si se necesita?	Sí	No	Sí	Sí
3	¿Los accesos están diferenciados por rol?	Sí	Sí	No	No
4	¿Con qué frecuencia se revisa quién tiene acceso al sistema?	b) Al cambiar empleados	a) Revisión mensual informal	c) No se ha revisado formalmente	c) No se ha revisado formalmente
5	Cuando alguien registra un dato, ¿qué ocurre antes de guardarlo?	a) Validaciones automáticas	a) Validaciones automáticas	c) Quien lo ingresa lo verifica	c) Quien lo ingresa lo verifica

N°	Pregunta (resumida)	E1-AF Emp. A	E1-C Emp. A	E2-AF Emp. B	E2-C Emp. B
6	¿Cualquier persona con acceso puede modificar registros sin autorización?	No	No	Sí	Sí
7	Si se detecta una inconsistencia, ¿qué ocurre normalmente?	c) Depende de quién lo encuentre	a) Se analiza la causa	c) Depende de quién lo encuentre	d) Sin proceso definido
8	¿Con qué frecuencia se hacen copias de seguridad?	a) Automáticamente	a) Automáticamente	a) Automáticamente	a) Automáticamente
9	¿Se ha comprobado que los respaldos realmente funcionan?	No	No	No	No
10	Si el sistema fallara hoy, la empresa podría continuar porque...	a) Tiene procedimiento alterno	a) Tiene procedimiento alterno	c) Se improvisaría	d) Operaciones se detendrían
11	¿Las copias se guardan en lugar separado al equipo principal?	Sí	Sí	Sí	No
12	¿De qué manera se documentan los procesos contables en la empresa?	b) Manuales	a) Manuales	b) WhatsApp	c) WhatsApp
13	¿Cómo sabría que los controles de seguridad no funcionan bien?	c) Cuando ya hubiera problema visible	c) Cuando ya hubiera problema visible	c) Cuando ya hubiera problema visible	d) Sin mecanismo claro
14	¿Existen reglas o políticas escritas sobre protección de información?	No	No	No	No
15	Cuando algo inusual ocurre en el sistema, ¿qué pasa normalmente?	b) Llama a quien resuelve	b) Llama a quien resuelve	b) Llama a quien resuelve	b) Llama a quien resuelve
16	Cuando hay un problema, ¿se documenta para evitar que vuelva a pasar?	No	No	No	No
17	Cuando alguien nuevo ingresa, ¿qué formación recibe en seguridad?	b) Un compañero lo guía	b) Un compañero lo guía	c) Aprende usando el sistema	c) Aprende usando el sistema
18	¿El personal comparte información confidencial por canales no seguros?	Sí	Sí	Sí	Sí
19	¿El personal sabe exactamente qué puede y no puede hacer con la información?	No	Sí	No	No

Nota: Las respuestas corresponden a los hallazgos sistematizados durante la aplicación del instrumento. Las menciones explícitas de opciones específicas en el análisis de resultados (capítulo 8) sirvieron como referencia directa para la reconstrucción de esta tabla.

Frecuencias y porcentajes por hallazgo

Se calcularon frecuencias absolutas (n) y porcentajes para los principales hallazgos identificados en el cuestionario. Dado el tamaño reducido de la muestra (n = 4 participantes), los resultados se presentan como estadísticas descriptivas de carácter ilustrativo y no como inferencias estadísticas generalizables.

Tabla 17 *Frecuencias y porcentajes por hallazgo*

Categoría	Hallazgo identificado	N	%	Interpretación
Gestión de accesos	Usuarios inactivos no eliminados de inmediato	3	75%	Debilidad compartida
Gestión de accesos	Uso compartido de credenciales	3	75%	Riesgo de acceso no autorizado
Gestión de accesos	Sin revisión periódica formal de permisos	3	75%	Control insuficiente
Copias de seguridad	Realizan copias automáticas	4	100%	Práctica positiva base
Copias de seguridad	Nunca han verificado recuperación de respaldos	4	100%	Vulnerabilidad crítica
Continuidad operativa	Sin procedimiento formal documentado (Emp. B)	2	50%	Alta exposición Empresa B
Canales de comunicación	Usan WhatsApp para información financiera	4	100%	Riesgo de trazabilidad
Políticas de seguridad	No existen políticas escritas de seguridad	4	100%	Ausencia total de formalización
Documentaciones incidentes	No documentan incidentes tecnológicos	4	100%	Gestión reactiva
Capacitación	Sin inducción estructurada en seguridad	3	75%	Baja cultura de seguridad

Nota: Los porcentajes se calculan sobre el total de cuatro (4) participantes. Los valores de 100% indican unanimidad en la respuesta; 75% corresponde a tres de cuatro participantes; 50% a dos de cuatro.

Análisis comparativo por empresa

Esta comparación complementa el análisis cualitativo de las entrevistas semiestructuradas y permite evidenciar de forma estructurada las similitudes y diferencias en la gestión del riesgo cibernético entre las dos organizaciones.

Tabla 18 *Análisis comparativo por empresa*

	Empresa A	Empresa B
Gestión de accesos	Control informal mensual; usuario compartido ocasional	Sin proceso de gestión; uso compartido frecuente
Copias de seguridad	Automáticas; sin validación de recuperación	Automáticas (inconsistente); sin validación

	Empresa A	Empresa B
Continuidad operativa	Procedimiento alterno en Excel (informal, documentado)	Sin procedimiento; operaciones se detendrían
Documentación de procesos	Manuales escritos parciales para procesos contables	Conocimiento en personas; sin manuales formales
Políticas de seguridad	Ausentes; conciencia individual sin institucionalización	Ausentes; dependencia de soporte externo
Canal de comunicación	WhatsApp para autorizaciones e información financiera	WhatsApp como canal principal de operación
Capacitación en seguridad	Ocasional; guiada informalmente por compañeros	Sin formación específica; aprendizaje en uso
Documentaciones incidentes	No se registran; correos sospechosos ignorados	No se registran; respuesta completamente reactiva

b) *Interpretación académica de los resultados*

- **Gestión de accesos y control de usuarios**

El 75% de los participantes indicó que los accesos de empleados desvinculados no se eliminan de manera inmediata, y la misma proporción reconoció el uso compartido de credenciales como práctica habitual. Estos resultados evidencian ausencia de procedimientos formales de gestión de accesos, lo que incrementa el riesgo de acceso no autorizado a los sistemas contables y dificulta la trazabilidad de las operaciones registradas.

- **Respaldo de información y continuidad operativa**

El 100% de los participantes reportó la realización de copias de seguridad automáticas; sin embargo, la totalidad también reconoció no haber verificado en ningún momento la efectiva recuperación de los respaldos almacenados. Esta situación implica que la continuidad operativa descansa sobre un supuesto de funcionamiento no comprobado. Adicionalmente, el 50% de los participantes de la Empresa B indicó que ante una falla del sistema las operaciones se detendrían hasta su restauración, lo que refleja una vulnerabilidad significativa en términos de continuidad del negocio.

- **Canales de comunicación y manejo de información financiera**

El 100% de los participantes reconoció el uso de aplicaciones de mensajería instantánea (WhatsApp) para compartir información financiera, autorizaciones de pago y soportes contables. Esta práctica compromete la trazabilidad documental y la confidencialidad de los datos, dado que la información queda dispersa en dispositivos personales sin control institucional.

- **Políticas de seguridad y documentación de incidentes**

La totalidad de los participantes (100%) indicó la ausencia de políticas escritas de seguridad de la información y la no documentación de incidentes tecnológicos. Esta condición confirma una gestión predominantemente reactiva del riesgo cibernético, caracterizada por la dependencia de conocimiento empírico individual y la ausencia de procedimientos institucionales que permitan identificar patrones de riesgo y fortalecer la respuesta organizacional.

- **Consideración metodológica sobre el tamaño de la muestra**

Conforme al diseño metodológico de estudio de caso múltiple adoptado en esta investigación, los resultados del cuestionario no tienen pretensión de representatividad estadística. Su propósito es complementar y triangular los hallazgos cualitativos obtenidos en las entrevistas semiestructuradas. Los porcentajes presentados deben interpretarse como indicadores descriptivos del comportamiento organizacional observado en las dos unidades de análisis estudiadas, y no como datos generalizables al total de MiPymes de Villavicencio.