1.

Diseño de un modelo de ciberseguridad basado en la norma ISO/IEC 27032 para pequeñas empresas del sector comercial de la ciudad de Manizales

Andrés Castaño Cardona

Trabajo de grado presentado para optar al título de Ingeniero en Seguridad de la Información

Asesor

Mauricio Mejía-Lobo, Doctor (PhD) en Sociedad del Conocimiento

Asesores de recursos académicos: Juan Pablo Charry Osorio (asesor bibliográfico), Claudia Marcela Cerón Rubio (asesora Centro de Escritura) y Elvia Lucía Sánchez García (asesora de integridad académica)

Universidad de Manizales

Facultad de Ciencias e Ingeniería

Ingeniería en Seguridad de la Información

Manizales, Caldas, Colombia

2025

Cita	Andrés Castaño Cardona [1]
Referencia Estilo IEEE (2020)	[1] A. Castaño Cardona, “Diseño de un modelo de ciberseguridad basado en la norma ISO/IEC 27032 para pequeñas empresas del sector comercial de la ciudad de Manizales”, Trabajo de grado profesional, Universidad de Manizales, Manizales, Caldas, Colombia 2025.

Línea de Investigación Sistemas de Gestión de Seguridad de la Información - SGSI.

Declaración de inteligencia artificial: el o los autores de este trabajo de grado declaran que han utilizado herramientas de inteligencia artificial (IA), tales como Copilot, DeepSeek y Napkin de manera ética y responsable, tal como se establece en el Acuerdo UManizales 002 (julio 26 de 2023) sobre propiedad intelectual e IA. Estas herramientas son empleadas como apoyo en la redacción, revisión gramatical y generación de ideas, pero en ningún caso sustituyen el análisis crítico, la argumentación académica ni la originalidad del trabajo. Asimismo, cualquier contenido generado con asistencia de IA está citado y referenciado adecuadamente, garantizando la integridad académica y el cumplimiento de los principios éticos de la investigación.

Dedicatoria

A mis padres, por enseñarme que el compromiso y la honestidad son más valiosos que cualquier título.

Agradecimientos

Expreso mi más sincero agradecimiento a quienes hicieron posible este proyecto.

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

RESUMEN

La presente investigación tiene como propósito diseñar un modelo de ciberseguridad basado en la norma ISO/IEC 27032, orientado a pequeñas empresas del sector comercial en la ciudad de Manizales. El estudio parte del reconocimiento de la creciente exposición a riesgos digitales en entornos con recursos limitados y baja madurez en seguridad informática. Se enmarca en el enfoque metodológico de investigación aplicada[1]que permite intervenir directamente en contextos profesionales para identificar problemas, proponer soluciones y evaluar su efectividad en tiempo real. A partir de los hallazgos, se estructuró un modelo que integra políticas de protección de activos digitales, gestión de incidentes, capacitación del personal y mecanismos de monitoreo. Los resultados evidencian una mejora significativa en la capacidad de respuesta ante amenazas, así como avances en el cumplimiento de buenas prácticas internacionales. Se concluye que la implementación de estándares como ISO/IEC 27032, ajustados a las condiciones operativas de las pequeñas empresas, contribuye a fortalecer su resiliencia digital y a fomentar una cultura organizacional orientada a la seguridad.

PALABRAS CLAVE: ISO/IEC 27032, Modelo de Ciberseguridad, buenas prácticas

ABSTRACT

This research aims to design a cybersecurity model based on the ISO/IEC 27032 standard, tailored to small commercial enterprises in the city of Manizales. The study begins by recognizing the growing exposure to digital risks in environments with limited resources and low maturity in information security. It follows an applied research methodology, which enables direct intervention in professional contexts to identify problems, propose solutions, and evaluate their effectiveness in real time. Based on the findings, a model was structured that integrates digital asset protection policies, incident management, staff training, and monitoring mechanisms. The results show a significant improvement in threat response capabilities, as well as progress in aligning with international best practices. The study concludes that implementing standards such as ISO/IEC 27032 adapted to the operational conditions of small businesses helps strengthen digital resilience and foster an organizational culture oriented toward security.

KEYWORDS: ISO/IEC 27032, Cybersecurity Model, Best Practices

I. INTRODUCCIÓN

La ciberseguridad se ha convertido en un tema cada vez más presente en medios digitales, artículos especializados y espacios de discusión técnica, con el propósito de generar conciencia sobre los riesgos que pueden materializarse dentro de las organizaciones. En este contexto, surgen preguntas recurrentes como: ¿qué es la ciberseguridad?, ¿para qué sirve?, ¿cómo una empresa se puede proteger? Para brindar respuesta a estas inquietudes, se hará uso de la norma ISO/IEC 27032, con el propósito de establecer un modelo de ciberseguridad adaptable a las capacidades técnicas y financieras de las pequeñas empresas del sector comercial de la ciudad de Manizales.

La norma ISO/IEC 27032 ofrece un marco integral para abordar la ciberseguridad en entornos interconectados, reconociendo los desafíos específicos que surgen en el ciberespacio. Su aplicación en pequeñas empresas permite traducir buenas prácticas internacionales en soluciones viables, sostenibles y adaptadas a las realidades locales.

A diferencia de otras normas de la familia ISO/IEC 27000, centradas en la seguridad de la información desde una perspectiva organizacional amplia, la ISO/IEC 27032 se enfoca en los riesgos propios del ciberespacio, tales como el malware, el phishing, el robo de identidad digital y los ataques dirigidos. Su propósito es establecer directrices claras para fortalecer la ciberseguridad, promover la colaboración entre actores relevantes y facilitar un lenguaje común para la gestión de amenazas.

Dado que la norma fue concebida para ser aplicable a organizaciones de cualquier tamaño, este trabajo plantea un modelo adaptativo orientado a las pequeñas empresas del sector comercial en la ciudad de Manizales. Estas organizaciones comparten características estructurales que condicionan su capacidad de respuesta ante incidentes informáticos, entre ellas:

- Recursos financieros y técnicos limitados
- Infraestructura tecnológica básica o desactualizada
- Ausencia de personal especializado en seguridad informática
- Cultura organizacional enfocada en la operación diaria, más que en la gestión del riesgo

En este contexto, la adaptación de la norma ISO/IEC 27032 implica:

- Simplificar los controles sin desvirtuar su propósito, priorizando aquellos de mayor impacto y bajo costo
- Promover la capacitación del personal mediante materiales visuales y sesiones breves
- Aprovechar herramientas disponibles para automatizar respaldos de información
- Establecer políticas mínimas viables, como el uso de contraseñas seguras, la protección del correo electrónico y la gestión básica de copias de seguridad

Este enfoque busca fortalecer la resiliencia digital de las pequeñas empresas sin comprometer su operatividad, integrando la ciberseguridad como un componente esencial de su sostenibilidad.

Esta tesis aborda la problemática de ciberseguridad en pequeñas empresas del sector comercial de la región, las cuales, debido a limitaciones presupuestarias, no cuentan con sistemas de protección adecuados, ni con personal idóneo para hacer frente a las diferentes amenazas cibernéticas. Esta situación las hace vulnerables a ataques que comprometen sus activos digitales más críticos. En este contexto, es importante tener en cuenta que, entre enero y noviembre del año 2024, se reportaron 77.866 denuncias de delitos informáticos en Colombia lo que representa un incremento del 23% respecto al año anterior. Esta cifra incluye ataques a empresas, instituciones públicas y usuarios individuales, y posiciona a Colombia como el cuarto país más atacado en Latinoamérica, según el Informe Ransomware 2024.[2]. De acuerdo con el reciente congreso Andicom 2025 celebrado en Colombia, el panel titulado “Blindaje Digital: IA como defensa contra las amenazas cibernéticas” el entorno digital enfrenta diversos desafíos. En particular, el segundo punto se enfocó en las pymes como el eslabón más vulnerable del ecosistema. Estas representan el 99,7% del aparato productivo en Colombia y concentran cerca del 70% de los ataques. Sin embargo, muchas empresas aún perciben la ciberseguridad como un gasto elevado y prescindible.

A partir de esta perspectiva, y para dar respuesta a las problemáticas de seguridad señaladas, tal como se describió anteriormente, el estándar internacional ISO/IEC 27032 será la base para poner en funcionamiento el modelo propuesto en una empresa de insumos eléctricos y artículos de

ferretería. El modelo mencionado incorpora buenas prácticas para la gestión de riesgos, la respuesta a incidentes y la capacitación del personal.

II. PLANTEAMIENTO DEL PROBLEMA

La mayoría de las pequeñas empresas del sector comercial en nuestro país cuenta con sistemas de información basados en una arquitectura cliente-servidor para la gestión de los inventarios, la base de datos de los clientes y las ventas realizadas[3]. Aunque estos sistemas son funcionales y cumplen con las necesidades básicas, la mayoría de estos presentan debilidades críticas en cuanto a la seguridad de la información. En la mayoría de las veces, el servidor que almacena los datos sensibles es utilizado por un usuario que accede a Internet desde el mismo equipo, realizando actividades como pagos en línea y consulta de correo electrónico. Esta práctica expone la infraestructura a riesgos como infecciones por malware, secuestro de información (ransomware) y pérdida de datos.

El software utilizado por estas empresas cuenta con licencias perpetuas sin derecho a recibir actualizaciones ni soporte técnico por parte del desarrollador, lo que lo hace vulnerable frente a amenazas conocidas y limita su capacidad de integración con nuevas tecnologías.

Ante este escenario, se plantea la necesidad de diseñar e implementar un modelo de ciberseguridad que permita mitigar los riesgos actuales, fortalecer la protección de los activos digitales y garantizar la continuidad operativa de la empresa buscando además que se ajuste a las capacidades técnicas y presupuestarias.

III ANTECEDENTES

Las tendencias globales en ciberseguridad revelan una creciente sofisticación en las amenazas explotando las vulnerabilidades comunes en entornos empresariales con poca protección, aprovechándose de sistemas operativos obsoletos, correos electrónicos sin filtros de protección y desconocimiento por parte del personal operativo. Muchas de estas vulnerabilidades afectan directamente a las pequeñas empresas debido a su infraestructura limitada convirtiéndolas así en blancos fáciles para los atacantes.

A continuación, se mencionan algunos antecedentes basados en el estudio de una tesis centroamericana y tendencias en ciberseguridad actuales en América.

Diseño de una estrategia de ciberseguridad basada en las normas ISO/IEC 27001:2022 y 27032:2023. Caso microfinanciera Prisma de Honduras (2025). Esta tesis demuestra que es posible adaptar estándares internacionales de seguridad a organizaciones con recursos limitados. En el caso de la microfinanciera Prisma, se identificaron brechas críticas en la gestión de activos, control de accesos y respuesta a incidentes, lo que motivó el diseño de una estrategia escalable y sostenible.

El estudio destaca que la norma ISO/IEC 27032:2023, (una versión más actualizada de la norma aplicada en la tesis personal) centrada en la seguridad en el ciberespacio colaborativo, ofrece herramientas prácticas para fortalecer la resiliencia digital en organizaciones pequeñas, especialmente cuando se complementa con los controles estructurados de la ISO/IEC 27001:2022. Esta combinación permite abordar tanto los aspectos técnicos como los humanos de la seguridad, integrando capacitación al personal y monitoreo continuo a través del diseño de un plan.[4]

Este antecedente refuerza la importancia de implementar modelos adaptativos basados en normas internacionales de ciberseguridad de manera eficaz en pequeñas empresas del sector comercial de la ciudad de Manizales, siempre que se consideren sus limitaciones operativas, técnicas y financieras.

Tendencias en ciberseguridad 2025: Evolución de la protección digital: Según el Global Cybersecurity Outlook 2025 del Foro Económico Mundial, citado por Prosegur, a través de su unidad especializada Cipher (unidad de ciberseguridad de Prosegur), “el 71% de los expertos advierte que estas organizaciones (pequeñas empresas) han alcanzado un punto crítico en el que

sus defensas tradicionales ya no son suficientes para contrarrestar los riesgos digitales emergentes". Esta afirmación reafirma la necesidad de modelos adaptativos y resilientes, como el que propone esta investigación, especialmente en entornos con baja madurez tecnológica.[5]

La ciberseguridad está evolucionando desde un enfoque preventivo hacia uno centrado en la resiliencia. Integrar esta resiliencia en la cultura organizacional permite minimizar el impacto de los incidentes y garantizar una recuperación efectiva. Este cambio de paradigma es especialmente relevante para pequeñas empresas que no pueden evitar todos los ataques, pero sí pueden prepararse para responder de forma eficiente.

¿Qué pasa con la explotación de vulnerabilidades más recientes? De acuerdo con el Security Report Latinoamérica 2024 de ESET, titulado "12 datos sobre el estado de la ciberseguridad de las empresas de América Latina", el panorama actual muestra una evolución preocupante en las tácticas de los atacantes. Aunque tradicionalmente se han explotado vulnerabilidades antiguas y tecnologías obsoletas, "los datos de la telemetría de ESET indican que también existen detecciones para vulnerabilidades más recientes. Esto muestra que el negocio del cibercrimen está compuesto por un ecosistema heterogéneo de actores maliciosos dispuestos a aprovechar el amplio espectro de vulnerabilidades existentes en busca de tecnologías desactualizadas. Incluso si esto implica ataques más sofisticados o que demandan el desarrollo de nuevos exploits."[6]

En particular, se han identificado vulnerabilidades en sistemas operativos como Windows 10 y Windows Server que permiten el escalamiento de privilegios, otorgando al atacante control total del sistema sin que el usuario se dé cuenta. Esta situación representa un riesgo crítico para las pequeñas empresas que no cuentan con procesos formales de actualización de sistemas ni monitoreo continuo.

La ciberseguridad, protagonista en Andicom 2025: siete conclusiones claves. Durante el Congreso Internacional de TIC, Andicom 2025, se evidenció que la ciberseguridad ha dejado de ser un asunto exclusivamente técnico para convertirse en un eje estratégico de competitividad empresarial. Según el reporte de Portafolio, uno de los puntos tratados se enfocó en las pymes como el eslabón más vulnerable del ecosistema. Estas representan el 99,7% del aparato productivo en Colombia y concentran cerca del 70% de los ataques. Sin embargo, muchas aún perciben la ciberseguridad como un gasto elevado y prescindible.

Jonathan Ardila, vicepresidente de Tecnología y Líder de Transformación Digital e Innovación de Cámara de Comercio de Bogotá, subrayó que esa visión debe cambiar, y expresó: “Protegerse no siempre implica grandes inversiones. Existen soluciones asequibles, colectivas y escalables que permiten reducir riesgos de manera efectiva. El verdadero peligro está en no hacer nada”.[7]

El panorama de ciberseguridad en Colombia ha mostrado un incremento alarmante en la frecuencia y sofisticación de los ataques digitales, según el análisis presentado por Pralogy[2] las organizaciones enfrentan amenazas cada vez más dirigidas, lo que exige una respuesta estructurada y proactiva. Entre las recomendaciones específicas entregadas por los expertos hacia las organizaciones para mitigar los riesgos y que a su vez sean adoptadas, se destacan la implementación de sistemas de autenticación multifactor, la actualización constante de sistemas y aplicaciones, la realización de copias de seguridad fuera de línea, la capacitación continua del personal frente a amenazas de ingeniería social, el desarrollo de planes de respuesta a incidentes y la contratación de seguros especializados contra riesgos cibernéticos.

Por otro lado, es importante citar el siguiente antecedente en torno a la aplicación de la norma ISO. Para tal fin, un referente pertinente para esta investigación es el trabajo de grado desarrollado por Sandra Liliana Guzmán Solano en la Universidad Católica de Colombia (2019), titulado Guía para la implementación de la norma ISO 27032. Este estudio propone una metodología práctica para adaptar las buenas prácticas de ciberseguridad definidas en la norma ISO/IEC 27032 a organizaciones colombianas, especialmente aquellas carecen de procedimientos formales de seguridad.

La autora parte del reconocimiento de que muchas pequeñas empresas han migrado sus operaciones al entorno digital sin contar con controles adecuados para proteger sus activos de información. En respuesta, diseña una guía basada en el ciclo PHVA (Planear, Hacer, Verificar, Actuar), que permite identificar activos críticos, evaluar riesgos, establecer controles y fortalecer la postura frente a amenazas como el malware, el phishing y el acceso no autorizado.

Aunque la norma ISO/IEC 27032 no es certificable, el estudio demuestra que puede ser utilizada como marco de referencia para mejorar la ciberseguridad organizacional. La propuesta incluye herramientas diagnósticas, plantillas de evaluación y recomendaciones alineadas con otras

normas complementarias como ISO/IEC 27001, además de considerar la legislación colombiana vigente. [8]

Este antecedente resulta valioso para el presente trabajo, ya que evidencia la viabilidad de adaptar estándares internacionales a contextos locales mediante metodologías accesibles, y refuerza la necesidad de fortalecer la capacitación del personal y la gestión de riesgos en pequeñas empresas del sector comercial.

IV. JUSTIFICACIÓN

En el contexto donde las pequeñas empresas del sector comercial dependen cada vez mas de sistemas de información para el desarrollo de sus actividades diarias, se ha incrementado la exposición a amenazas cibernéticas, especialmente cuando no se cuenta con políticas de seguridad adecuadas ni con infraestructura tecnológica actualizada. En el caso de la empresa objeto de estudio, esta enfrenta riesgos reales derivados de prácticas operativas inseguras y de una infraestructura tecnológica obsoleta, lo que pone en peligro su información crítica y la sostenibilidad del negocio.

Ante esta situación, se ha evidenciado que la empresa cuenta con sistemas y dispositivos que no cumplen con los estándares actuales de seguridad. Esta brecha identificada a nivel tecnológico incrementa la vulnerabilidad frente a diferentes amenazas como el malware, secuestro de información (ransomware) y pérdida de datos. El modelo propuesto busca introducir controles mínimos y procedimientos adaptados al entorno técnico actual sin requerir de grandes inversiones y que se ajuste a la empresa.

Este proyecto se justifica en la necesidad de implementar un modelo de ciberseguridad que sea viable técnica y económicamente, y que esté alineado con estándares internacionales como la norma ISO/IEC 27032. La implementación de buenas prácticas en ciberseguridad permitirá reducir la exposición a amenazas, mejorar la gestión de riesgos, y fomentar una cultura organizacional orientada a la protección de la información.

Las pequeñas empresas siempre se van a enfrentar a restricciones presupuestarias que limitan la implementación de diferentes soluciones de seguridad. Sin embargo, los costos derivados de un incidente de seguridad pueden ser mucho mayores que los de implementar herramientas de protección de manera preventiva. El modelo propuesto busca ofrecer una estrategia viable, con controles de bajo costo y alto impacto, orientados a proteger la sostenibilidad del negocio sin comprometer sus recursos financieros.

Además, el desarrollo de este modelo puede servir como referencia para otras empresas de distintos sectores, tanto en Manizales como en otras regiones que enfrentan desafíos similares, contribuyendo al fortalecimiento de la seguridad digital y a la protección de la información. Esto, a su vez, brinda confianza a clientes y proveedores, especialmente en un entorno como el de la ciudad, donde las relaciones comerciales son cercanas y la reputación empresarial tiene un valor significativo. En este contexto, se busca minimizar el riesgo de que se materialice un incidente que pueda generar consecuencias sociales relevantes.

La presente tesis promueve una cultura organizacional consciente del riesgo digital entendiendo que la seguridad de la información no depende únicamente de herramientas tecnológicas, sino también del comportamiento humano dentro de la empresa y, además, fomenta la capacitación del personal como eje de transformación.

V. OBJETIVOS

Objetivo General

Diseñar un modelo de ciberseguridad contextualizado para pequeñas empresas del sector comercial de Manizales, alineado con la norma ISO/IEC 27032, que se ajuste a sus capacidades técnicas y contribuya al fortalecimiento de la protección de activos digitales frente a amenazas cibernéticas. El modelo integrará buenas prácticas en gestión de riesgos, respuesta a incidentes y formación del personal, con enfoque preventivo y adaptable.

Objetivos Específicos

Establecer el alcance del modelo de ciberseguridad, considerando las características operativas, técnicas y económicas de las pequeñas empresas del sector comercial, así como los activos críticos que requieren protección.

Realizar un análisis de riesgos cibernéticos, identificando vulnerabilidades, amenazas y niveles de exposición que puedan comprometer la continuidad operativa y la protección de la información.

Definir controles de seguridad adecuados, seleccionando medidas técnicas, administrativas y de capacitación que respondan a los riesgos priorizados, en función de los recursos disponibles y en alineación con las buenas prácticas de la norma ISO/IEC 27032.

Implementar el modelo de ciberseguridad propuesto, mediante la elaboración de políticas, la asignación de roles, la capacitación del personal y la puesta en marcha de mecanismos de seguimiento que permitan evaluar su eficacia y facilitar su mejora continua.

VI. MARCO CONCEPTUAL

En la presente tesis, emergen conceptos que interactúan entre sí en el abordaje del problema de investigación en torno a la no existencia de buenas prácticas para el uso seguro de la infraestructura tecnológica. Estos permiten guiar el proceso investigativo de la tesis. En este orden de ideas, se citan los siguientes:

Ciberseguridad

La ciberseguridad se refiere a cualquier tecnología, práctica y política para prevenir los ataques cibernéticos o mitigar su impacto. Su objetivo es proteger sistemas, aplicaciones, dispositivos, datos y personas frente a amenazas como ransomware, phishing y robo de información.[9]

Ciberespacio

El ciberespacio se refiere al ámbito digital de las redes informáticas, Internet y otras formas de comunicación electrónica. Es un espacio virtual donde las personas y las organizaciones pueden interactuar y compartir información a nivel mundial, independientemente de su ubicación física.[10]

Activo

Según la norma ISO/IEC 27001 Un activo de información es “todo aquello que tiene valor para la organización”.[11]

Malware

Software malicioso diseñado para dañar, interrumpir o acceder sin autorización a sistemas informáticos. Incluye virus, troyanos, ransomware, spyware, entre otros. Puede robar datos, cifrar archivos o espiar actividades del usuario.[12]

Vulnerabilidad

Una vulnerabilidad informática es cualquier fallo o error en el software o en el hardware que hace posible a un atacante o hacker comprometer la integridad y confidencialidad de los datos que procesa un sistema.[13]

Riesgos

Los riesgos de ciberseguridad son los posibles ataques o fallos en el sistema de información digital que pueden ocasionar daños y consecuencias como accesos no autorizados, robo de datos, interrupción de actividades, pérdidas económicas o afectación a la reputación de la empresa.[14]

VII. MARCO TEÓRICO

La ciberseguridad abarca un conjunto prácticas y políticas orientadas a prevenir ataques cibernéticos. Su propósito esencial es proteger sistemas, aplicaciones, dispositivos, datos y personas frente a amenazas como malware, ransomware, robo de información, entre otras formas de intrusión digital.

Desde la mirada empresarial, especialmente en pequeñas empresas del sector comercial que operan con recursos limitados, la ciberseguridad no se reduce a instalar herramientas técnicas, sino que también implica fomentar practicas seguras en el día a día, establecer políticas claras que orienten el comportamiento digital, y capacitar al personal sobre los riesgos de ciberseguridad. Al final, cualquier estrategia de protección se sostiene sobre tres pilares esenciales:

Confidencialidad: Garantizar que la información sólo sea accesible por personas autorizadas.
Integridad: Asegurar que los datos no sean alterados de forma indebida.
Disponibilidad: Mantener los sistemas y servicios operativos cuando se necesiten.

Estos principios deben aplicarse de forma proporcional al contexto. En entornos como el de las pequeñas empresas comerciales en Manizales, donde los recursos técnicos y humanos pueden ser limitados, resulta clave priorizar controles esenciales, fomentar la cultura de seguridad y diseñar soluciones sostenibles que se ajusten a la realidad operativa.

Los riesgos más comunes suelen estar vinculados al uso de hardware obsoleto, software desactualizado o sin licencia, ausencia de soluciones antivirus y prácticas de respaldo manual sin una frecuencia definida. Estas condiciones elevan significativamente la probabilidad de que una amenaza se materialice, poniendo en riesgo la continuidad operativa y la integridad de la

información, especialmente en empresas que no cuentan con medidas de protección ni un modelo de ciberseguridad adecuado.

En el contexto actual, donde muchas pequeñas empresas enfrentan desafíos técnicos y presupuestarios, la norma ISO/IEC 27032 se convierte en una aliada estratégica para implementar

prácticas de ciberseguridad a través de un modelo que se ajusten a sus capacidades y necesidades sin requerir de una infraestructura robusta ni grandes inversiones, lo que facilita una adopción continua y sostenible.

La norma define la ciberseguridad como “la preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio”[15], y propone una estructura que contempla la gestión de incidentes, la protección de activos digitales y la concienciación del usuario. Esta visión integral permite abordar los riesgos digitales desde múltiples frentes, lo cual resulta especialmente pertinente en entornos con baja madurez en seguridad informática.

Además, la norma ISO/IEC 27032 clasifica las amenazas más comunes en el ciberespacio como el malware, el phishing y la explotación de vulnerabilidades entre otras, lo que facilita la elaboración de una matriz de riesgos ajustada al entorno local. Esta clasificación técnica, combinada con la asignación clara de roles y responsabilidades de los usuarios frente al uso de los recursos informáticos refuerza la necesidad de capacitar al personal no técnico y establecer protocolos internos de seguridad.

Para brindar respuesta a este conjunto de afirmaciones, la presente investigación busca diseñar un modelo de ciberseguridad que integre políticas de protección de activos digitales, gestión de incidentes, capacitación del personal y mecanismos de monitoreo. Estos elementos se articulan bajo el marco normativo de la ISO/IEC 27032, que propone un enfoque colaborativo para la protección del ciberespacio. En esta perspectiva, se presenta a continuación, un flujo del diseño del modelo de ciberseguridad propuesto con el cual se busca que las pequeñas empresas mejoren sus buenas prácticas en torno a este aspecto.

Fig. 1. Flujo del diseño del Modelo de Ciberseguridad. Imagen elaborada con napkin AI.

Nota: Fuente https://app.napkin.ai/

Este modelo de ciberseguridad se apoya en una norma que logra equilibrar el rigor técnico con la flexibilidad operativa, permitiendo que las pequeñas empresas del sector comercial fortalezcan su postura frente a las amenazas digitales sin comprometer su capacidad productiva. Más que una lista de controles, con el diseño del modelo se busca estar alineados con la norma ISO/IEC 27032 que ofrece una guía adaptable, pensada para contextos reales, donde la seguridad no depende exclusivamente de la tecnología, sino también del compromiso, la capacitación y la colaboración entre todos los actores del entorno digital de la empresa.

VIII. METODOLOGÍA

La presente investigación se desarrollará bajo un enfoque metodológico de investigación-aplicada (Vargas Cordero, 2009), que enfatiza la investigación aplicada como herramienta para comprender y transformar realidades con evidencia científica, especialmente en contextos profesionales el cual permite intervenir directamente para identificar problemas, proponiendo soluciones y evaluar su efectividad en tiempo real. Este enfoque resulta pertinente para pequeñas empresas del sector comercial, donde la participación por parte de los actores involucrados es clave para el éxito de las medidas de ciberseguridad.

El diseño e implementación del modelo se estructurará conforme al Ciclo PHVA (Planear-Hacer-Verificar-Actuar), garantizando una mejora continua en cada fase del proceso:

Planear

Se establecerá el alcance del modelo, identificando los activos digitales críticos, los procesos vulnerables y los recursos disponibles. En esta fase se realizará el diagnóstico inicial y el análisis de riesgos, utilizando herramientas como matrices de impacto y probabilidad, entrevistas y revisión documental.

Hacer

Se definirán e implementarán los controles de seguridad seleccionados, incluyendo medidas técnicas, administrativas y de capacitación. Se elaborarán políticas internas, se asignarán responsabilidades y se desarrollarán guías de carácter formativo para todo el personal.

Verificar

Se evaluará la eficacia de los controles mediante indicadores de desempeño, listas de verificación y retroalimentación del personal. Esta fase permitirá identificar desviaciones, brechas o áreas de mejora en la aplicación del modelo.

Actuar

Con base en los resultados obtenidos y la retroalimentación del personal, se ajustarán las estrategias implementadas, se actualizará la documentación y se fortalecerán los mecanismos de monitoreo. Esta fase busca consolidar una cultura organizacional orientada a la seguridad de la información y a la mejora continua.

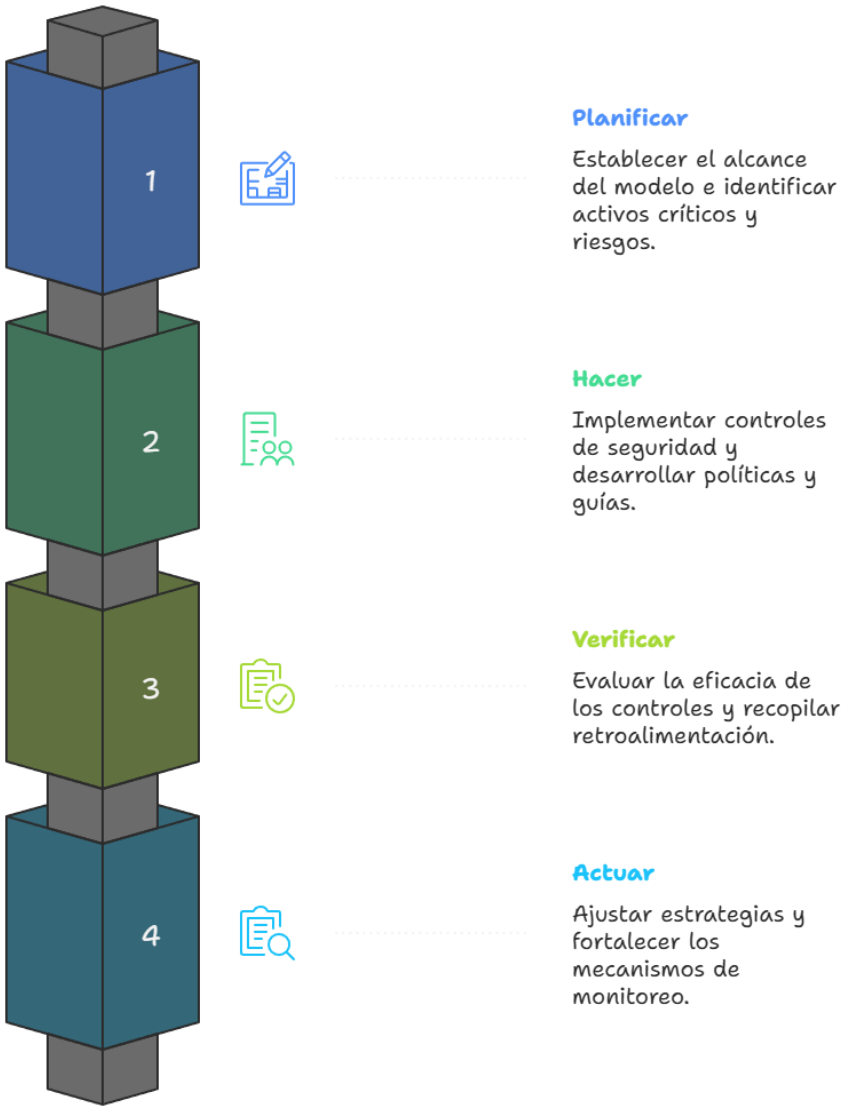

Fig. 2. Ciclo PHVA. Imagen elaborada con napkin AI.

Nota: Fuente https://app.napkin.ai/

IX RESULTADOS

Tras realizar el diseño del modelo de ciberseguridad basado en la norma ISO/IEC 27032 y su implementación en una empresa del sector comercial dedicada a la venta de insumos eléctricos y artículos de ferretería, se obtuvieron resultados significativos que evidencian mejoras tanto en la gestión de riesgos como en la cultura organizacional.

Durante el diagnóstico inicial se llevó a cabo un levantamiento detallado de la infraestructura tecnológica de la empresa, con el objetivo de identificar los activos críticos que sustentan su operación. Este proceso incluyó la revisión de los equipos de cómputo, sistemas de información, medios de respaldo y canales de comunicación digital.

Así mismo, se realizaron encuestas al personal administrativo y operativo para comprender el uso cotidiano de los recursos tecnológicos, su interacción con el sistema de facturación, y las prácticas asociadas al manejo de la información. Se evidenció que las copias de seguridad se realizan de forma manual y sin una frecuencia definida, lo que representa un riesgo significativo en términos de disponibilidad y recuperación de datos.

TABLA 1

RESULTADOS ENCUESTA AL GERENTE: ESTADO GENERAL DE CIBERSEGURIDAD

Categoría	Valor Actual	Escala Ideal
¿Su empresa cuenta con software antivirus instalado?	2	5
¿Actualizan regularmente el software y sistemas operativos?	1	5
¿Realizan Copias de Seguridad de manera automatizada?	1	5

Categoría	Valor Actual	Escala Ideal
¿Existen políticas escritas sobre uso de contraseñas?	1	5
¿Han capacitado a empleados en ciberseguridad los últimos 12 meses?	1	5

Para la aplicación de la encuesta se empleó una escala de Likert de cinco puntos, diseñada para evaluar el grado de frecuencia con que se implementan prácticas de ciberseguridad en la empresa.

TABLA 2

RESULTADOS ENCUESTA A EMPLEADOS: CONCIENCIACION Y PRACTICA

Categoría	Promedio
Sé cómo identificar un correo de phishing	1.8
Uso contraseñas diferentes para cada servicio.	2.1
Actualizo mis aplicaciones y dispositivos regularmente.	1.5
Conozco las políticas de seguridad de la empresa.	1.0
Recibo capacitación periódica en ciberseguridad.	1.0

La encuesta fue aplicada a una población de cinco empleados, y los resultados obtenidos fueron procesados mediante cálculo de promedios, tal como se muestra en la tabla anterior.

En cuanto al correo electrónico de la empresa objeto de estudio, se identificó que es utilizado como canal principal para el envío de información a los clientes y la recepción de facturas por parte de los proveedores. Sin embargo, el correo no cuenta con un dominio asociado al nombre de la

empresa y por ende se usa un buzón gratuito que no cuenta con mecanismos de protección específicos frente a amenazas como el phishing o la suplantación de identidad, lo que lo convierte en un vector crítico de riesgo.

La aplicación del modelo permitió establecer políticas internas claras, fortalecer los controles técnicos básicos y capacitar al personal en prácticas de seguridad digital. Asimismo, se logró identificar y mitigar vulnerabilidades previamente no documentadas, lo que contribuyó a una mayor protección de la información operativa.

TABLA 3

ANALISIS DE RIESGOS

Activo crítico	**Riesgo identificado**	**Impacto**	**Probabilidad**
Sistema de facturación	Pérdida o alteración de datos por malware	Alto	Alta
Bases de datos de clientes	Acceso no autorizado o fuga de información	Alto	Media
Credenciales de acceso	Las credenciales no se actualizan, se mantienen activas tras cambios de personal, o se configuran sin estándares mínimos.	Medio	Alta
Infraestructura tecnológica	Fallos por obsolescencia o falta de mantenimiento	Medio	Alta
Recurso humano	Ingeniería social o errores operativos	Alto	Alta
Copias de seguridad	Pérdida de información por respaldo manual o incompleto	Alto	Media
Correo electrónico	Phishing, suplantación de identidad, fuga de información	Alto	Alta

X. DISCUSIÓN

El diagnóstico realizado sobre la empresa objeto de estudio revela una infraestructura tecnológica obsoleta y prácticas operativas que la exponen a riesgos críticos, como pérdida de información, infecciones por malware y accesos no autorizados. La ausencia de soluciones antivirus y el uso de sistemas sin soporte oficial constituyen amenazas persistentes, especialmente en un entorno donde los empleados carecen de formación básica en ciberseguridad. Estos hallazgos confirman la creciente exposición a riesgos digitales en contextos con recursos limitados y baja madurez informática.

Al contrastar estos resultados con estudios previos, se observa una coincidencia significativa en cuanto a las vulnerabilidades que afectan a este tipo de empresas. La escasa formación técnica, junto con la ausencia de políticas internas que regulen el uso de los sistemas y recursos informáticos, demuestra que el problema no es únicamente técnico, sino también formativo y estratégico. En muchas de estas organizaciones, no existen protocolos claros para la gestión de contraseñas, el control de accesos o la realización de copias de seguridad, lo que agrava la vulnerabilidad operativa y dificulta la prevención de incidentes.

Estos hallazgos refuerzan la necesidad de implementar modelos adaptativos de ciberseguridad en las pequeñas empresas, considerando sus limitaciones reales. La aplicación del modelo propuesto, construido bajo estándares como la ISO/IEC 27032, establece una base operativa que facilita la construcción de soluciones sostenibles, priorizando la simplicidad, la capacitación progresiva del personal y el aprovechamiento de recursos existentes. En este sentido, el estudio no solo diagnostica, sino que propone una ruta viable para la transformación digital segura en contextos de alta vulnerabilidad, con posibilidades reales de adaptación en otras empresas del sector comercial, tanto en la ciudad de Manizales como en otras ciudades del país.

XI. CONCLUSIONES

El diagnóstico realizado confirma que la pequeña empresa enfrenta diferentes riesgos significativos en sus activos críticos, estos riesgos son derivados de las diferentes prácticas operativas evidenciadas durante el levantamiento de información. Al contar con una infraestructura tecnología obsoleta y ante la falta de controles básicos de seguridad la probabilidad de que estos riesgos se materialicen es alta.

Se identificaron siete activos críticos con riesgos de alto impacto, entre ellos se destacan el sistema de facturación, las bases de datos de clientes y el correo electrónico. La probabilidad de que ocurran incidentes es media o alta por lo cual se exige una respuesta ágil y estructurada.

El análisis realizado a la infraestructura permitió recopilar la suficiente evidencia para aplicar el modelo de ciberseguridad buscando priorizar las acciones correctivas, la aplicación de las políticas propuestas, y la orientación y concienciación a través de capacitaciones del personal.

A pesar de las limitaciones con las que cuentan las pequeñas empresas de la ciudad de Manizales a nivel presupuestario y tecnológico, se logró aplicar el modelo de ciberseguridad basado en la norma ISO/IEC 27032, proponiendo soluciones viables, sostenibles y alineadas con las capacidades reales de la empresa.

Los resultados obtenidos durante la implementación del modelo de ciberseguridad permiten avanzar hacia la evaluación y mejora continua del modelo propuesto. La información recopilada será clave para medir el impacto de las medidas adoptadas y ajustar el enfoque según sea necesario.

Este tipo de análisis aplicado al grupo de empresas objeto de estudio permite realizar una radiografía profunda de las dificultades tecnológicas que enfrentan diariamente las organizaciones en la ciudad de Manizales y en Colombia en general. La limitada disponibilidad de recursos, sumada al desconocimiento en materia de ciberseguridad, las expone a escenarios críticos que, de materializarse alguno de los riesgos identificados, podrían comprometer seriamente la continuidad operativa del negocio, llegando incluso a situaciones de no retorno.

XII. RECOMENDACIONES

Desarrollar programas de capacitación en ciberseguridad para personal no técnico

Diseñar manuales y guías con contenidos accesibles que aborden las buenas prácticas digitales, que permitan realizar la identificación de las amenazas más comunes y frecuentes. (phishing, ingeniería social) y uso seguro de herramientas cotidianas.

Cuantificar las pérdidas potenciales por interrupciones operativas, fuga de información o daño reputacional, para sensibilizar a los tomadores de decisiones sobre la importancia de invertir en seguridad.

Explorar mecanismos de seguimiento periódico (checklists, auditorías internas, indicadores básicos) que permitan mantener la seguridad sin requerir infraestructura avanzada.

XIV REFERENCIAS

[1] Z. R. Vargas Cordero, “La Investigación aplicada: Una forma de conocer las realidades con evidencia científica”, *Rev. Educ.*, vol. 33, núm. 1, p. 155, jul. 2009, doi: 10.15517/revedu.v33i1.538.

[2] “Tendencias de ciberataques en Colombia 2025: ¿Qué sectores están en la mira? – Pralogy”. Consultado: el 22 de septiembre de 2025. [En línea]. Disponible en: https://pralogy.co/wp/2025/05/12/tendencias-de-ciberataques-en-colombia-2025-que-sectores-estan-en-la-mira/

[3] “Arquitectura Cliente-Servidor: Guía Completa para su Implementación | Linformatiu”. Consultado: el 22 de septiembre de 2025. [En línea]. Disponible en: https://linformatiu.com/tecnologia/arquitectura-cliente-servidor-guia-completa-para-su-implementacion

[4] R. H. A. Medina y M. E. C. Macías, “FACULTAD DE POSTGRADO TRABAJO FINAL DE GRADUACIÓN”.

[5] “Tendencias en ciberseguridad 2025: Evolución de la protección digital |”. Consultado: el 14 de septiembre de 2025. [En línea]. Disponible en: https://www.prosegur.com.co/articulo/sala-de-prensa/tendencias-en-ciberseguridad-2025-evolucion-de-la-proteccion-digital

[6] “ESET-Security-Report_2024_ESPAÑOL”.

[7] “La ciberseguridad, protagonista en Andicom 2025: siete conclusiones claves”, Portafolio.co. Consultado: el 14 de septiembre de 2025. [En línea]. Disponible en: https://www.portafolio.co/tecnologia/la-ciberseguridad-protagonista-en-andicom-2025-siete-conclusiones-clave-639215

[8] S. L. G. Solano, “PROYECTO DE TRABAJO DE GRADO GUÍA PARA LA IMPLEMENTACION DE LA NORMA ISO 27032.”.

[9] “¿Qué es la ciberseguridad? | IBM”. Consultado: el 16 de septiembre de 2025. [En línea]. Disponible en: https://www.ibm.com/mx-es/think/topics/cybersecurity

[10] “¿Qué es el Ciberespacio? Historia, Origen y Definición”, Estudyando. Consultado: el 16 de septiembre de 2025. [En línea]. Disponible en: https://estudyando.com/ciberespacio-historia-origen-y-descripcion-general-que-es-el-ciberespacio/

[11] "Qué es un activo de información - TI Rescue". Consultado: el 16 de septiembre de 2025. [En línea]. Disponible en: https://tirescue.com/que-es-un-activo-de-informacion/

[12] "¿Qué es el Malware? Definición de Malware, Tipos y Protección". Consultado: el 16 de septiembre de 2025. [En línea]. Disponible en: https://www.malwarebytes.com/es/malware

[13] "¿Qué es una vulnerabilidad informática y cómo protegerse?" Consultado: el 22 de septiembre de 2025. [En línea]. Disponible en: https://www.deltaprotect.com/blog/vulnerabilidad-informatica

[14] "¿Qué es el riesgo de ciberseguridad y cómo evaluarlo?", Sectigo® Oficial. Consultado: el 16 de septiembre de 2025. [En línea]. Disponible en: https://www.sectigo.com/es/recursos/que-es-el-riesgo-de-ciberseguridad-y-como-evaluarlo

[15] "ISO 27032 - 2018".