Ciberseguridad en Colombia: Análisis de Ciberataques y Estrategias Preventivas para las pequeñas y medianas empresas

Walter Alejandro Linares Guerra

Asesor

Néstor Javier Rodríguez García

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería ECBTI

Ingeniería de Telecomunicaciones

2026

Resumen

El desarrollo de servicios de comercio electrónico tomó más tiempo del esperado debido a la coyuntura del COVID-19; sin embargo, la aceleración de los servicios digitales mostró rápidamente debilidades en ciberseguridad, especialmente dentro de las pequeñas y medianas empresas (Pymes) donde la infraestructura, la capacitación y las políticas internas para combatir amenazas digitales son limitadas. Con esto en mente, el interés del presente trabajo investigativo es comprender el estado de los ciberataques en el país e identificar los desafíos tecnológicos, educativos y regulatorios dentro de las Pymes para proponer mejoras en las políticas públicas y fortalecer su resiliencia digital. Así, pues, se tuvo en cuenta un enfoque mixto para el análisis documental de informes nacionales en bases de datos de investigación como *Scopus, Scielo, Google Scholar, IEEE Xplore y ScienceDirect* sobre ciberataques en el país. Además, se incluyeron elementos descriptivos y correlacionales para reconocer los patrones de los ataques y los factores asociados con el nivel de vulnerabilidad de las empresas. Se concluye que, los ataques de *phishing, ransomware y malware* son los más activos en Colombia, afectando a las organizaciones con un bajo nivel de evolución digital. Por consiguiente, se identificaron tres desafíos principales dentro de las Pymes: deficiencias tecnológicas, pobre cultura de ciberseguridad y falta de cumplimiento de los requisitos legales sobre la protección de datos personales y la seguridad de la información.

Palabras clave: Ciberseguridad, Pymes, Ciberataques, Transformación digital.

Abstract

The development of E-commerce services took longer than expected due to COVID-19 conjuncture; nevertheless, the acceleration of digital services quickly revealed weaknesses in cybersecurity, especially within small and medium-sized enterprises (SMEs) in which the infrastructure, the training, and the internal policies to combat digital threats are limited. With this in mind, the interest of this research work is to understand the state of cyberattacks in the country and identify technological, educational, and regulatory challenges within SMEs in order to propose improvements in public policy and strengthen their digital resilience. Then, a mixed approach was taken into account for documentary analysis of national reports within research databases such as Scopus, Scielo, Google Scholar, IEEE Xplore, and ScienceDirect related to cyberattacks in the country. It moreover included descriptive and correlational elements to recognize attack patterns and factors associated with the level of vulnerability of companies. It is concluded that phishing, ransomware, and malware attacks are the most active in Colombia affecting organizations with a low level of digital evolution. In addition, three main challenges were identified within SMEs: technological deficiencies, poor cybersecurity culture, and lack of compliance with legal requirements on personal data protection and information security.

Keywords: Cybersecurity, PyMEs, Cyberattacks, Digital transformation.

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Introducción

En los últimos años, Colombia ha atravesado una rápida transformación digital con un gran impacto en las actividades sociales, económicas y empresariales. La implementación masiva del trabajo remoto, el comercio digital, los servicios en la nube y los procesos administrativos han llevado a una mayor dependencia de las tecnologías de la información (TI), pero paralelamente revelan serias debilidades en ciberseguridad. En ese contexto, las pequeñas y medianas empresas (Pymes), que representan más del 90% del tejido empresarial colombiano, se han convertido en uno de los sectores más vulnerables y expuestos a los ataques cibernéticos debido a su falta de infraestructura tecnológica, formación del personal y adopción de políticas internas de seguridad digital.

Hay que mencionar que el aumento sostenido de ataques, como phishing, ransomware, malware y violaciones de datos, tiene un impacto directo en los riesgos operativos, económicos y de prestigio de las Pymes, amenazando la supervivencia del negocio y la competitividad en un entorno altamente digitalizado. La fragmentación de este panorama ha sido documentada por entidades nacionales e internacionales, desencadenando un urgente llamado a fortalecer la capacidad de respuesta, prevención y mitigación del impacto de las amenazas cibernéticas.

En ese sentido, esta investigación busca caracterizar la situación de los ciberataques en Colombia, diagnosticar los desafíos tecnológicos, educativos y regulatorios de las Pymes; formular mejoras y políticas públicas que promuevan la ciber-resiliencia. Para ello, la metodología correspondió al análisis documental con un enfoque mixto que incluye la búsqueda, la selección, la recolección, la clasificación y la organización de documentos sobre ciberseguridad nacional; así como la exploración, la interpretación y la presentación de los mismos.

No cabe duda de que la realización de este estudio nos ayuda a dimensionar el problema de los ataques cibernéticos hacia las Pymes, a identificar algunas de las principales brechas en ciberseguridad que enfrentan las Pymes y a plantear algunas alternativas que, de alguna manera, servirían para la protección del sector productivo colombiano. Es así que esta investigación trasciende la epistemología de la ingeniería de sistemas, lo que también se traduce en insumos para la toma de decisiones en el ámbito organizacional y el diseño de políticas públicas que generen un entorno digital más seguro y confiable.

Planteamiento del Problema

La pandemia del COVID-19 conllevó a transformaciones digitales en todo el mundo creando una dependencia sin precedentes a las plataformas digitales. Es sabido, por ejemplo, que, el teletrabajo, la educación virtual y el comercio electrónico se consolidaron como alternativas sociales y económicas, según resalta el Ministerio de Comercio, Industria y Turismo (MinCIT, 2023). Sin embargo, aumentó el riesgo de sufrir ciberataques para quienes tienen menos habilidades tecnológicas, especialmente niños y adultos mayores, dado que la transición al mundo digital se realizó sin una estrategia ni una alineación adecuadas en materia de seguridad (Jung y Katz, 2022). De acuerdo con la Unión Internacional de Telecomunicaciones (UIT, 2023), el 66 % de la población mundial está actualmente en línea; empero, más del 40 % carece de conocimientos básicos sobre ciberseguridad, lo que profundiza la brecha de exposición en la protección contra los ciberdelitos.

Al igual que otros países de Latinoamérica, Colombia enfrenta desafíos únicos, ya que el país ocupa el tercer puesto en la región en cuanto a número de ciberataques, y en estas circunstancias ha concentrado más del 10 % de los ataques reportados (Pinto, 2025). Esta situación se agrava por la falta generalizada de educación en seguridad digital, lo cual facilita el fraude electrónico, el phishing y la suplantación de identidad, especialmente entre la población adulta mayor que tiene dificultades para gestionar sus datos en línea como lo aseguro (Díaz et al., 2024).

Definitivamente, la situación es más pronunciada en sectores como las pymes, que tienen limitaciones de infraestructuras robustas de ciberdefensa. Tal como lo evidencia el informe de la Organización de Estados Americano (OEA, 2023), el 53 % de las pymes en América Latina no

cuentan con políticas formales de seguridad de la información y, por lo tanto, son presa fácil para los ciberdelincuentes. En Colombia, si bien existen marcos regulatorios como la Ley 1273 (2009), que clasifica los delitos cibernéticos, y la Ley 2011 de 2019, que establece las normas para el manejo de la evidencia digital, persisten lagunas en la regulación de los delitos emergentes relacionados con el uso de inteligencia artificial (IA), falsificaciones profundas o ingeniería social sofisticada (Salazar y Rendón, 2024).

En ese sentido. la exposición a ciberataques reside en la falta de capacitación en ciberseguridad que fomenta la desconfianza digital, estanca la economía digital y disminuye la competitividad del país en áreas estratégicas como el comercio electrónico, la educación en línea y los servicios financieros. Para ilustrar mejor, se estima que algunos delitos cibernéticos generan pérdidas directas e indirectas de más de 800 millones de dólares anuales para Colombia (Forbes, 2024). Esto representa un déficit estructural para el crecimiento económico y social, así como para el establecimiento de una cultura digital segura.

Lo cierto es que, si bien existen directrices institucionales como la Resolución 1790 (2017), que establece los procedimientos de seguridad de la información en las entidades estatales (Cámara Colombiana de Informática y Telecomunicaciones [CCIT], 2024), dicha normativa es insuficiente si no se incluye un sólido eje formativo y de sensibilización cívica. Por ende, la formación en ciberseguridad se convierte en un componente crucial para la mitigación de riesgos y el fortalecimiento de la resiliencia digital. Es así como la educación de los usuarios, como advierte el Instituto Nacional de Ciberseguridad de España (INCIBE, 2023), es una línea de defensa vital contra la ciberdelincuencia, especialmente en entornos empresariales vulnerables, con recursos sociales y económicos limitados.

Por consiguiente, se pretende examinar cómo la formación en ciberseguridad puede

contribuir a mitigar los efectos negativos de la rápida digitalización en Colombia en la población de adultos mayores, microempresarios y funcionarios públicos. Considerando así el asunto de la falta de programas de capacitación cibernética que incrementa los riesgos de las amenazas tecnológicas, pero también socava la ciberseguridad y el desarrollo socioeconómico del país a puertas de una llamada cuarta revolución industrial.

A los anterior surge la siguiente pregunta de investigación: ¿Cuáles son los ciberataques que afectan a las Pymes, en Colombia, con el fin de identificar los principales retos en materia de ciberseguridad y proponer estrategias preventivas y correctivas que mitiguen su impacto en la operatividad y protección de la información?

Objetivos

Objetivo General

Examinar el impacto de los ciberataques en las Pymes de Colombia con el fin de comprender los temas más críticos de la ciberdefensa, así como las estrategias preventivas y reactivas que reduzcan el impacto en las operaciones del negocio y la seguridad de la información.

Objetivos Específicos

Caracterizar el panorama actual de los ciberataques en Colombia mediante el análisis de incidentes reportados, sus principales modalidades y actores involucrados.

Diagnosticar los retos específicos en ciberseguridad que enfrentan las Pymes en los sectores público y privado, considerando aspectos tecnológicos, educativos y normativos.

Diseñar propuestas de mejora y políticas públicas enfocadas en la prevención, respuesta y mitigación de ciberataques, a través de la capacitación, fortalecimiento normativo y adopción de tecnologías emergentes.

Justificación

Colombia enfrenta desafíos sin precedentes en materia de ciberseguridad, por lo que se ha convertido en una preocupación latente tras la pandemia del COVID-19. La transformación digital durante la pandemia expuso las debilidades estructurales de Colombia en gestión cibernética a nivel institucional e individual (Centro Cibernético Policial, 2024), puesto que, el país fue uno de los más afectados por la ciberdelincuencia en Latinoamérica, esta última atribuida principalmente por su sofisticada capacidad tecnológica y seguridad digital. En consecuencia, este escenario facilitó que actores maliciosos ejecutarán delitos informáticos en sitios web vulnerables ante estos ataques. De ahí que existe la urgente necesidad de rediseñar la educación en ciberseguridad, la inversión en infraestructura y el empoderamiento digital de las sociedades (Forbes, 2024).

Desde una perspectiva financiera, la ciberseguridad constituye una amenaza directa para las Pymes, que representan más del 90 % de la estructura empresarial en Colombia (Ministerio del Trabajo, 2019). Considerando que estas empresas suelen carecer de los recursos financieros y humanos necesarios para implementar mecanismos de protección avanzados, como resultado, tienen una mayor probabilidad de sufrir un ciberataque que resulte en interrupciones operativas, robo de información, costos de recuperación y daño reputacional, como advirtieron Ramírez y Villamizar (2020), estos factores obstaculizan la competitividad digital, frenan el crecimiento del comercio electrónico y limitan la internacionalización del sector productivo. En efecto, el estudio llevado a cabo por Ramírez y Villamizar en el año 2020 es uno de los pocos estudios que han analizado clínicamente las posibles repercusiones de este tipo de ataques en el país y que, además, han sugerido una ruta para abordarlos.

Por otro lado, el desconocimiento en temas de ciberseguridad conlleva a la violación de los derechos fundamentales, lo que puede generar en desconfianza en las instituciones estatales por parte de ciertos sectores de la población, como los adultos mayores – que son más vulnerables al "cibercrimen" (Restrepo y Bernal, 2021). Indiscutiblemente, la solución se encuentra en la revisión de estrategias educativas que materialicen la protección de los derechos fundamentales enfocados a la población descrita ante cualquier ataque cibernético.

Ahora bien, desde el ámbito tecnológico, la integridad, disponibilidad y confidencialidad de la información requieren cada vez más del uso de herramientas como la IA, el Big Data y el Internet de las Cosas (loT), que en conjunto pueden mitigar la concurrencia de los ciberataques. En concordancia con López (2019) y la CCIT (2024) se afirma que la construcción de infraestructuras digitales seguras es indispensable, no solo para proteger a los usuarios, sino para potenciar la infraestructura tecnológica del país y su soberanía. Precisamente, lo que se pretende es extender la cimentación de la infraestructura digital nacional para fortalecer la disminución del tiempo de respuesta frente a los ciberataques atendiendo a las nuevas regulaciones y lineamientos a estos servicios.

En concreto, la justificación académica de este estudio radica en que la ciberseguridad aún se está consolidando como un eje estratégico de investigación multifactorial. De acuerdo con Gómez (2022), las universidades y los centros de investigación tienen la responsabilidad de generar conocimiento aplicado que responda a la dinámica del país y fomente la colaboración entre los sectores público y privado. Por tal motivo, este trabajo investigativo se centra en las Pymes al aportar contribuciones tanto empíricas como teóricas a este campo, a su vez que, fortalece el conjunto de recursos académicos necesarios para la formulación de políticas innovadoras que vinculen nuevos programas de formación en términos de ciberseguridad.

Por último, el enfoque principal es inspeccionar los ciberataques dirigidos contra las Pymes en Colombia para determinar los principales desafíos en ciberseguridad y formular estrategias preventivas y de respuesta para minimizar su impacto. Por ende, la finalidad es la mejora de la seguridad digital en el país, optimizando los procesos empresariales, aumentando la confianza ciudadana en los servicios digitales y fomentando un ecosistema más sólido para la economía digital. Lo que significa establecer perspectivas fundamentales para el desarrollo de políticas públicas y programas de capacitación que permitan al país alcanzar una cultura de ciberseguridad, crucial para sostener el desarrollo económico y social en el contexto de la cuarta revolución industrial.

Marco Referencial

En el presente capítulo, se expone la literatura relacionada con el tema objeto de esta investigación, cuyo propósito es proporcionar un contexto y una fundamentación teórica en torno a la *ciberseguridad en Colombia*: *Análisis de Ciberataques y Estrategias Preventivas para las Pymes.*

Antecedentes

El apartado de antecedentes busca contextualizar el problema de investigación con base en estudios previos sobre la seguridad cibernética y los riesgos tecnológicos en las Pymes en Colombia. Para Bernal (2020), los antecedentes permiten identificar los logros, los vacíos teóricos y las tendencias metodológicas, lo cual facilita el proceso de construcción del marco conceptual del estudio. En este sentido, la literatura consultada evidencia que los riesgos de ciberataques en las Pymes han aumentado debido a una digitalización acelerada que, en la mayoría de los casos, no ha sido acompañada de una cultura de seguridad informática ni del desarrollo de políticas adecuadas de ciberseguridad. Por ello, resulta fundamental documentar los retos y las limitaciones que enfrentan las Pymes en Colombia desde una perspectiva teórica actualizada.

En el contexto académico, Cano y Mesa (2021) analizan la evolución de la ciberseguridad en las Pymes colombianas, especialmente tras la pandemia de la COVID-19. Los autores señalan que la adopción de tecnologías digitales para el trabajo remoto se implementó sin la preparación necesaria en materia de ciberseguridad. Su estudio, desarrollado con un enfoque de métodos mixtos, incluyó encuestas a 60 empresas del sector de servicios en Bogotá y Medellín, complementadas con entrevistas a expertos en seguridad digital. Los resultados

arrojaron que el 72% de las empresas encuestadas reportaron haber sufrido al menos un incidente de ciberseguridad durante el último año, siendo el *phishing* y el *malware* los ataques más frecuentes. Estos hallazgos muestran una brecha significativa ante la rápida digitalización y la adopción de medidas adecuadas de protección, lo cual incrementa el riesgo de pérdida de datos sensibles, fraudes electrónicos y afectaciones reputacionales.

Los autores también destacan la relación directa entre la falta de capacitación en el uso de herramientas digitales y la efectividad de los ataques cibernéticos, reforzando la importancia de la 'ciberseguridad humana'. Así mismo, señalan que las Pymes suelen priorizar la continuidad operativa sobre la protección de la información, lo que lleva a la implementación de políticas internas de gestión del riesgo digital insuficientes y poco estructuradas.

En su análisis, Cano y Mesa (2021) subrayan la necesidad urgente de fortalecer la cultura organizacional de prevención y cerrar las brechas tecnológicas mediante políticas públicas articuladas con el sector privado para fomentar la adopción de soluciones de seguridad digital. Esta relación resulta clave para la presente investigación, pues demuestra que la operación tecnológica sin acompañamiento estratégico constituye un factor de vulnerabilidad crítica para las Pymes, evidenciando la importancia de desarrollar políticas educativas y tecnológicas que fortalezcan su resiliencia digital.

Por otra parte, Restrepo y Álvarez (2022), estudian las prácticas de gestión de riesgos de ciberseguridad en Pymes colombianas durante un período de intensificación de la digitalización empresarial, a través de una metodología cualitativa basada en estudios de caso en empresas de los sectores industrial, comercial y financiero de Cali, Medellín y Bogotá. Los autores identifican que la mayoría de estas organizaciones manejan los incidentes de manera reactiva, actuando únicamente cuando los ataques ya han ocurrido en lugar de anticiparlos. Esta tendencia coincide

con lo señalado por el informe del Centro Cibernético Policial (2024), el cual indica que más del 60% de las empresas afectadas por ciber - amenazas en Colombia no cuentan con medidas preventivas formales.

El estudio también revela una ausencia generalizada de cultura de prevención y mitigación de riesgos digitales, puesto que ninguna de las empresas analizadas posee políticas de respaldo de información ni mecanismos de monitoreo activo. Como consecuencia, los enfoques no planificados de ciberseguridad derivan en mayores pérdidas económicas, tiempos prolongados de recuperación y disminución de la confianza por parte de clientes y aliados comerciales. Además, se identifica que muchas Pymes perciben la seguridad informática como un gasto y no como una inversión estratégica, lo que agrava los riesgos derivados de herramientas tecnológicas no protegidas o inadecuadas.

En este sentido, los autores indican que el costo inevitable de la seguridad informática debe considerarse como un elemento que contribuye a la sostenibilidad del negocio frente a amenazas tecnológicas cada vez más complejas, la evaluación continua de vulnerabilidades, la formación del personal y la implementación de políticas claras de prevención y respuesta.

Por otro lado, Gómez (2022) personifica los desafíos que tienen que ver con el campo de la ciberseguridad con procesos de socialización educativa en la educación superior y en el ecosistema empresarial en Colombia. Menciona que las instituciones de educación superior enfrentan desafíos que algunas de las Pymes encuentran, como tener infraestructuras tecnológicas poco desarrolladas, escasas inversiones en sistemas de protección y culturas organizacionales débiles en cuanto a la fusión de la seguridad digital.

Desde una perspectiva descriptiva y analítica, basada en la revisión de documentos y entrevistas con directivos de diez universidades colombianas, el investigador señala que los

ataques más frecuentes, que demuestran la relevancia del factor humano en la cadena de vulnerabilidad, son la ingeniería social y el acceso no autorizado. El estudio expone que tener políticas de protección es inadecuado, colocándolo moral y legalmente a las instituciones, y con eso, en lo que respecta a la confidencialidad e integridad de los datos públicos y privados de las personas, de los datos y políticas de ciberseguridad que las instituciones como universidades gestionan, expone en su exclusivo acceso a los datos de estudiantes, investigadores y personal no académico.

El autor sostiene que la ciberseguridad constituye un eje transversal que no se limita a la dimensión tecnológica, sino que involucra procesos educativos, administrativos y sociales. Desde esta perspectiva, recomienda la formulación de una estrategia nacional de educación digital que integre a universidades, sectores productivos y entidades gubernamentales con el fin de desarrollar competencias en ciberseguridad y cerrar las brechas existentes entre el conocimiento técnico y su aplicación práctica.

Esta postura es particularmente relevante para la presente investigación, pues evidencia que los problemas de vulnerabilidad digital se extienden más allá del ámbito académico y afectan también a organizaciones productivas, especialmente las Pymes que carecen de una cultura de seguridad robusta, presentan deficiencias en capacitación y mantienen brechas significativas en control y prevención de riesgos. En efecto, la investigación de Gómez (2022) refuerza la urgencia de fortalecer la educación digital, como un componente clave para incrementar la resiliencia frente a ciberataques y promover la sostenibilidad del entorno digital colombiano.

De igual manera, el Centro Cibernético Policial (2024) presentó un estudio cuantitativo, basado en la sistematización de los reportes de incidentes recibidos por el CAI Virtual, constituyéndose en una de las evidencias empíricas más importantes sobre la magnitud del

fenómeno y la creciente vulnerabilidad de las Pymes. Durante 2024 se registraron más de 55.000 incidentes de ciberseguridad, de los cuales el 38 % afectó directamente a las Pymes, lo que confirma su posición como uno de los sectores más expuestos al riesgo digital. Los ataques predominantes fueron el phishing, el *ransomware* y las filtraciones de datos personales.

Estos datos no solo reflejan la sofisticación creciente de los cibercriminales, sino también las debilidades estructurales en los sistemas internos de prevención y respuesta de las organizaciones. Teniendo en cuenta lo anterior, el informe enfatiza la importancia de consolidar la cooperación institucional entre los sectores público y privado, especialmente en lo relacionado con la transferencia de conocimiento, la capacitación y la creación de protocolos coordinados de seguridad digital.

El mismo estudio del Centro Cibernético Policial (2024), evidencia un incremento sostenido en los niveles de cibercriminalidad en Colombia, relacionado con la exposición del uso de internet, la incorporación de tecnologías en procesos empresariales y la falta de conciencia sobre los riesgos asociados a las TI. En el caso de las Pymes, se resalta que la escasa inversión en infraestructura tecnológica y la debilidad de las políticas de seguridad las convierten en el eslabón más vulnerable del ecosistema digital nacional.

Ante este panorama, el informe recomienda fortalecer la cooperación público-privada e implementar estrategias de prevención integrales y multidisciplinarias que contemplen procesos de capacitación y asistencia técnica en ciberseguridad. La relevancia de estos aportes para la presente investigación radica en que proporcionan un diagnóstico cuantitativo actualizado de la problemática y subrayan la necesidad de implementar acciones estratégicas que mitiguen la vulnerabilidad de las Pymes para garantizar su sostenibilidad y competitividad en un entorno digital dinámico y en constante expansión.

En conjunto, los antecedentes revisados representan un fundamento sólido para el desarrollo de este trabajo de investigación sobre los ciberataques dirigidos a las Pymes en Colombia. Cano y Mesa (2021), así como Restrepo y Álvarez (2022), demuestran la relación directa entre el uso intensivo de tecnologías y el incremento del riesgo asociado a la ausencia de una gestión adecuada del mismo. Por su parte, Gómez (2022) aporta una visión centrada en la importancia de la educación digital como un elemento clave para disminuir las inconsistencias en materia de ciberseguridad.

Finalmente, el Centro Cibernético Policial (2024) ofrece un enfoque institucional y un análisis cuantitativo que ratifica el aumento de los incidentes cibernéticos y la vulnerabilidad específica de las Pymes. En síntesis, estas contribuciones permiten identificar vacíos críticos en formación, gestión y prevención dentro del entorno empresarial colombiano y orientan a esta investigación hacia la formulación de acciones que fortalezcan la resiliencia digital de las Pymes, contribuyan a la protección de su información y aseguren su sostenibilidad frente a los crecientes desafíos del entorno tecnológico contemporáneo.

Marco Teórico

Las teorías que explican el ciberacoso y los ciberataques -componentes centrales del campo de la informática forense- abordan la violencia psicológica ejercida en entornos digitales. Dichas manifestaciones se caracterizan por extender la gestión de un individuo hacia un conjunto de personas y se materializan mediante los sistemas informáticos o redes globales de internet, especialmente el ciberespacio. En el contexto de esta investigación, el análisis se concentra en el territorio colombiano, con un enfoque en las Pymes, comúnmente denominadas Pymes.

Como lo señalan Hernández y Mendoza (2018), el marco conceptual adoptado constituye una estructura rectora alrededor de la cual se desarrolla la investigación. Este marco permite

clarificar la esencia del planteamiento del problema, facilitar la formulación de hipótesis y orientar la definición de los objetivos de estudio. Así, además de integrar los supuestos teóricos que sustentan la discusión académica, se profundizará en los conceptos fundamentales expuestos en la introducción, alineados con la realidad actual del país, donde tal como lo señalan Cano y Mesa (2021), las Pymes enfrentan obstáculos significativos relacionados con la infraestructura tecnológica y la articulación digital.

Teoría de la Seguridad Informática Basada en el Triángulo CIA

La Teoría de la Seguridad Informática basada en el Triángulo CIA (Confidencialidad, Integridad y Disponibilidad) se apoya en enfoques organizacionales que explican cómo las empresas gestionan los recursos de los que dependen para garantizar su estabilidad. Pfeffer y Salancik (1978) sostuvieron que las organizaciones no son autosuficientes, sino que dependen de recursos externos, económicos, tecnológicos y sociales, cuyo acceso y control condicionan su supervivencia. Este planteamiento resulta especialmente pertinente en la era digital, donde las micro, pequeñas y medianas empresas (Mipymes) dependen ampliamente de infraestructuras tecnológicas, servicios en la nube y plataformas de comunicación. Estos recursos, ajenos a su control directo, las convierten en actores particularmente vulnerables frente a los ciberataques.

Siguiendo la línea, Hillman et al. (2009), amplía la *Teoría de la Dependencia de Recursos* al señalar que la dependencia no se limita al ámbito económico. También incluye el acceso a capacidades tecnológicas y conocimiento especializado. Para las Mipymes, la carencia de personal experto en ciberseguridad o la externalización apresurada de los servicios de TI incrementará su nivel de exposición al riesgo. De ahí que los autores subrayan la necesidad de establecer alianzas estratégicas que permitan cerrar brechas de conocimiento y fortalecer la gestión tecnológica.

Asimismo, Drees y Heugens (2013), destacan que la dependencia de recursos genera asimetrías de poder que restringen la autonomía organizacional. En el ámbito de la ciberseguridad, significa que las Pymes que dependen de proveedores de servicios de la nube, principalmente grandes corporaciones tecnológicas, quedan subordinadas a las políticas y estándares de seguridad definidos por terceros. Esta situación evidencia la necesidad de una gobernanza digital interna más robusta y de mecanismos de control sobre los datos propios, con el fin de mitigar la dependencia y fortalecer la protección de información sensible.

En el contexto colombiano, Cano y Mesa (2021) explican que la aceleración de la transformación digital durante la pandemia incrementó significativamente la dependencia tecnológica de las Pymes sin que ello estuviera acompañado de una inversión proporcional en ciberseguridad. Para estos autores, la brecha que expone la Teoría de la Dependencia de los Recursos se manifiesta en un mayor riesgo de fraude electrónico, pérdida de información confidencial, suplantación de identidad y, en consecuencia, una disminución en la competitividad del sector empresarial dentro de la economía digital.

En conjunto, este cuerpo teórico no solo mantiene su vigencia, sino que ha evolucionado para responder a los desafíos que plantea el entorno digital contemporáneo. La noción de la dependencia tecnológica como una vulnerabilidad estructural permite justificar la necesidad de estrategia preventivas y correctivas orientadas a fortalecer la resiliencia digital de las Pymes en Colombia, garantizando la protección de sus recursos informáticos y su sostenibilidad en un entorno cada vez más digitalizado.

Teoría del Riesgo y la Gestión de Riesgos

La teoría y la gestión del riesgo sostienen que las sociedades contemporáneas se encuentran expuestas a desafíos crecientes derivados de la innovación tecnológica y de la

globalización, lo que exige procesos sistemáticos para la identificación, evaluación y mitigación estratégica de amenazas (Beck, 1992). Para las Pymes, esta perspectiva resulta esencial, dado que los ciberataques no solo representan un riesgo económico, sino también social y organizacional al comprometer la continuidad cooperativa y la confianza de clientes y aliados comerciales.

En esta línea, Avenel y Ortega (2019) plantean que el riesgo en el entorno digital no constituye a un evento aislado, sino el resultado de la interacción entre vulnerabilidades internas y amenazas externas. Desde esta perspectiva, los ciberataques a las Pymes pueden prevenirse y controlarse mediante la implementación de sistemas adecuados de prevención, monitoreo y detección temprana.

Complementariamente, Power (2021) sostiene que la gestión de riesgos de la era digital requiere el uso de análisis técnicos especializados acompañados de una gobernanza organizacional proactiva. En el contexto colombiano, esto implica que las Pymes deben formular políticas de ciberseguridad que integren la protección tecnológica con la capacitación del personal. En consecuencia, la teoría justifica la necesidad de adoptar medidas anticipatorias en la etapa de planificación, así como estrategias correctivas destinadas a reducir el impacto de incidentes cuando estos ocurran.

Desde una mirada latinoamericana, Cano y Mesa (2021) señalan que, las Pymes en Colombia enfrentan barreras significativas en la gestión de riesgos, debido a la escasez de recursos financieros y la ausencia de políticas institucionales robustas para la protección de activos digitales. En este sentido, la teoría de la gestión del riesgo ofrece un marco adecuado para evaluar cómo estas organizaciones pueden fortalecer su nivel de preparación mediante inversiones focalizadas y esfuerzos de cooperación interinstitucional.

Restrepo y Álvarez (2022) argumentan con la misma contundencia que, en el caso de las Pymes, el enfoque de gestión de riesgos cibernéticos es demasiado simplista, argumentando que debe interpretarse como un proceso dinámico donde la experiencia y el aprendizaje de cada ataque se utilizan para informar y mejorar sistemas posteriores más resilientes. Sin duda, las PYMES deben ser más proactivas y adoptar marcos de gestión de riesgos que anticipen y se preparen para amenazas nuevas y en evolución, en lugar de centrarse únicamente en la respuesta tras la ocurrencia de un evento.

En conjunto, este cuerpo teórico demuestra que la Teoría del Riesgo y la Gestión del Riesgo ofrecen un anclaje conceptual sólido para el presente estudio, al dilucidar el impacto de los ciberataques en las Pymes y proponer un enfoque integral, preventivo, correctivo y resiliente, frente a la inseguridad cibernética en Colombia.

Teoría de la Dependencia de Recursos

Desde esta perspectiva, Hillman y Collins (2021) analizan la vulnerabilidad inherente a la dependencia tecnológica y argumentan que las organizaciones deben gestionar activamente los riesgos derivados de esta dependencia para reducir asimetrías de poder y fortalecer su autonomía digital. En particular, destacan la necesidad de establecer mecanismos de control sobre los proveedores de servicios tecnológicos, plataformas digitales y soluciones en la nube, los cuales constituyen puntos sensibles para la seguridad organizacional.

La TDR resalta especialmente y pertinente para el estudio de las Pymes, puesto que estas poseen capacidades internas limitadas en materia de ciberseguridad y, por tanto, dependen en gran medida de proveedores externos para garantizar su funcionamiento digital (Cano y Alvarado. 2023). Esta dependencia incrementa el riesgo de exposición de información sensible, interrupciones en la operación y afectaciones reputacionales. De este modo, la teoría no solo

describe una relación económica entre proveedores y empresas, sino que también evidencia una relación de vulnerabilidad tecnológica que compromete la resiliencia organizacional.

En el marco de la presente investigación, la TDR permite explicar la relación entre ciberseguridad, riesgos en la cadena digital y el uso de plataformas externas por parte de las Pymes en Colombia. El empleo de servicios de hosting, redes sociales, software en la nube y sistemas de comercio electrónico expone a estas organizaciones a una variedad de amenazas cibernéticas. Por ello, el fortalecimiento de capacidades internas en gestión del riesgo y ciberseguridad constituye una estrategia fundamental para mitigar la dependencia externa, incrementar el control sobre los recursos digitales críticos y garantizar la sostenibilidad operativa de las Pymes.

Teoría de la Resiliencia Organizacional

La Resiliencia Organizacional se fundamenta en la capacidad de una organización para anticipar, resistir, adaptarse y recuperarse frente a perturbaciones que amenazan su continuidad o estabilidad (Hollnagel, 2017). En la actualidad, esta teoría ha evolucionado desde una visión centrada exclusivamente en la gestión de crisis hacia un enfoque integral que incorpora la resiliencia digital, operativa y estratégica como pilares esenciales para la sostenibilidad organizacional.

Autores recientes destacan que la resiliencia no se limita a la habilidad de afrontar amenazas, sino que implica la capacidad de aprender y transformarse a partir de ellas. Desde esta perspectiva, Duchek (2020) sostiene que la resiliencia organizacional comprende tres ejes fundamentales [anticipación, gestión de crisis y aprendizaje]. Estos componentes permiten que las organizaciones se adapten de manera activa y en tiempo real a entornos altamente dinámicos, como los ecosistemas digitales. En consonancia, Williams et al. (2021) argumenta que las

organizaciones resilientes son aquellas que integran capacidades adaptativas en áreas como la gestión del conocimiento, la innovación y la ciberseguridad.

En el contexto de la digitalización, Agarwal y Selen (2022), señalan que el riesgo cibernético exige no sólo el fortalecimiento de las capacidades tecnológicas, sino también la consolidación de competencias humanas y el desarrollo de una cultura organizacional orientada a la continuidad del negocio y la confianza digital. Esta perspectiva permite articular la resiliencia organizacional con la Teoría de la Dependencia de Recursos, en tanto que esta última demuestra como la exposición a riesgos externos es consecuencia de la dependencia tecnológica, mientras que la resiliencia organizacional ofrece rutas para mitigar dichas vulnerabilidades mediante el fortalecimiento interno de capacidades adaptativas.

En el caso de las Pymes colombianas, esta teoría facilita comprender cómo la integración de protocolos de ciberseguridad, la capacitación del personal, la formulación de planes de respuesta a incidentes y el desarrollo de mecanismos de ciber-resiliencia permiten enfrentar los ciberataques derivados de su elevada dependencia tecnológica. En entornos vulnerables, la resiliencia deja de ser un atributo deseable para convertirse en un factor determinante de supervivencia y competitividad, pues posibilita no solo la defensa ante un ataque, sino también la capacidad de aprendizaje y transformación a partir de este (Nguyen et al., 2023).

El análisis teórico permite evidenciar que la vulnerabilidad organizacional frente a amenazas cibernéticas no puede explicarse únicamente desde factores tecnológicos. Las dinámicas estructurales, estratégicas y de gestión de recursos digitales desempeñan un papel determinante. Desde la Teoría de la Dependencia de Recursos (Pfeffer & Salancik, 1978), la vulnerabilidad cibernética de las Pymes se entiende como resultado de la dependencia asimétrica respecto a proveedores tecnológicos externos, dado que estas organizaciones carecen de

infraestructura, experiencia y recursos suficientes para gestionar autónomamente sus activos digitales. Esta situación las posiciona como actores altamente vulnerables en un entorno donde los flujos de información y los recursos tecnológicos son críticos para la sostenibilidad operativa (Cano & Alvarado, 2023).

La Teoría de la Resiliencia Organizacional, por su parte, enfatiza que las organizaciones deben no sólo reaccionar ante los ciberataques, sino anticiparse, resistirlos, recuperarse y transformarse (Duchek, 2020). Dentro de este marco, la resiliencia digital emerge como una estrategia clave para reducir la dependencia tecnológica y, en consecuencia, fortalecer la sostenibilidad operativa. Así mientras la Teoría de la Dependencia de Recursos explica las causas estructurales de la vulnerabilidad, la Teoría de la Resiliencia Organizacional provee los mecanismos para su mitigación mediante capacidades adaptativas, aprendizaje institucional y la consolidación de una cultura de seguridad digital (Nguyen et al., 2023).

En conjunto, ambas teorías constituyen el soporte contextual que guía esta investigación al vincular dependencia tecnológica, riesgo cibernético, resiliencia organizacional y procesos de aprendizaje. Esta articulación no sólo amplía la comprensión del fenómeno, sino que orienta la formulación de prácticas responsables, sostenibles y destinadas a fortalecer la autonomía digital de las Pymes colombianas, en lo que puede considerarse una gestión estratégica y tecnológicamente resiliente (Williams et al., 2021).

Marco Conceptual

El marco conceptual es la base interpretativa que combina los principales conceptos teóricos y técnicos sobre los ciberataques y las vulnerabilidades de las Pymes en entornos digitales. Además, su principal objetivo es definir las categorías analíticas que guían la investigación, permitiendo así la correlación de la dependencia tecnológica, la gestión del riesgo

cibernético y la resiliencia organizacional como determinantes clave de la sostenibilidad empresarial.

Ciberataques: Un ciberataque implica el intento de quebrantar sistemas informáticos, redes o dispositivos con el fin de perjudicar la confidencialidad, integridad o disponibilidad de la información. De ahí que aumentan las exposiciones de las Pymes frente a ataques como phishing, *ransomware*, malware y DDoS debido a la expansión del trabajo remoto, la digitalización de servicios y el uso de la nube. Según N*ational Institute of Standards and Technology* (NIST, 2024), estos atentados afectan la disponibilidad de servicios, el prestigio empresarial y la confianza de los clientes, haciendo aún más evidente la ciberseguridad y su integración en la gestión organizacional como componente estratégico.

Dependencia tecnológica: Es el nivel en el cual una organización necesita recursos digitales, infraestructuras externas o servicios tecnológicos para llevar a cabo sus actividades. Esta dependencia implica el control parcial de recursos externos, los cuales constituyen una vulnerabilidad para la organización respecto a los proveedores. En efecto, esta dependencia ha concentrado el uso de recursos digitales en organizaciones que necesitan servicios en la nube para su funcionamiento, así como software de terceros o redes sociales, lo que incrementa las posibilidades de sufrir un ciberataque. A su vez, esto es más crítico en las Pymes por la falta de recursos económicos y técnicos para adoptar las salvaguardias necesarias (Hillman et al., 2021).

Ciberseguridad organizacional: son las políticas, herramientas y prácticas necesarias para salvaguardar los sistemas de información ante las amenazas digitales. Cabe señalar que la ciberseguridad se puede definir de forma más puntual como la conservación de la confidencialidad, integridad y disponibilidad de la información en los entornos cibernéticos. En el caso de la implementación en Pymes, personal, presupuesto y cultura organizacional de la

prevención son los factores limitantes (OEA, 2023). Por lo tanto, el fortalecimiento de la cultura de ciberseguridad, a nivel estratégico, implica gestión de riesgos, formación del talento humano y, sobre todo, inversión en ciberseguridad (Organización Internacional de Normalización [ISO]/ Comisión Electrotécnica Internacional [IEC] 27032, 2023b).

Gestión del riesgo cibernético: en un proceso sistemático que busca identificar, analizar, evaluar y posteriormente, mitigar cada uno de los riesgos que conlleva la implementación de tecnologías digitales. De acuerdo con el *National Institute of Standards and Technology* (NIST, 2024) e ISO 31000 (2023a), dicha gestión debe ser efectuada en todos los niveles dentro de la organización. Con respecto a las Pymes, el riesgo cibernético implica la implementación de acciones sostenibles en el tiempo, es decir, la creación de un plan de prevención que dé respuesta a la posible ocurrencia de un incidente. También se podría elaborar un conjunto de indicadores de riesgo que permitan la supervisión de la exposición frente a la presencia de amenazas. En concordancia con lo anteriormente expuesto, en este texto se plantea que la relación entre el constructor de vigas y la gestión del riesgo cibernético es la disminución de una vulnerabilidad estructural acorde con la gestión de amenazas digitales (Liu y Zhang, 2022).

Resiliencia organizacional: Se define como la habilidad de una organización de prever, ajustarse y recuperarse de crisis o perturbaciones que ponen en riesgo su funcionamiento. En el mundo digital, la resiliencia organizacional se establece en el ciberespacio, con la capacidad de mantener operaciones críticas contra incidentes de seguridad, dando como resultado, la integración de elementos tecnológicos, humanos y estratégicos en una organización. Por consiguiente, la ciberseguridad se vuelve el motor de la innovación y el aprendizaje continuo que la organización debe incorporar hacia el interior de sus estructuras (Nguyen et al., 2023).

Pequeñas y medianas empresas (Pymes): Son el motor económico de América Latina,

representando más del 90% de la red empresarial y más del 60% de las oportunidades de empleo. No obstante, el grado de digitalización las deja altamente dependientes de tecnologías externas, aumentando la exposición a amenazas cibernéticas. De conformidad con lo explicado, en las recientes investigaciones se evidencian bajos niveles de madurez en seguridad digital, poca inversión en infraestructura tecnológica y una cultura de prevención débil en las Pymes colombianas (Cano & Alvarado, 2023).

En concreto, estos conceptos nos permiten construir un marco analítico donde la dependencia tecnológica funciona como un factor de riesgo que incrementa la exposición a ciberataques, mientras que la resiliencia organizacional es un eje de contrapeso mitigador que mejora la continuidad operativa y la adaptación al entorno digital. Así, la mejora de la ciberseguridad en las Pymes implica, en un amplio sentido, la consolidación de una cultura institucional que sea capaz de aprender, anticipar, transformar riesgos cibernéticos e innovar en línea con el desarrollo sostenible.

Marco Metodológico

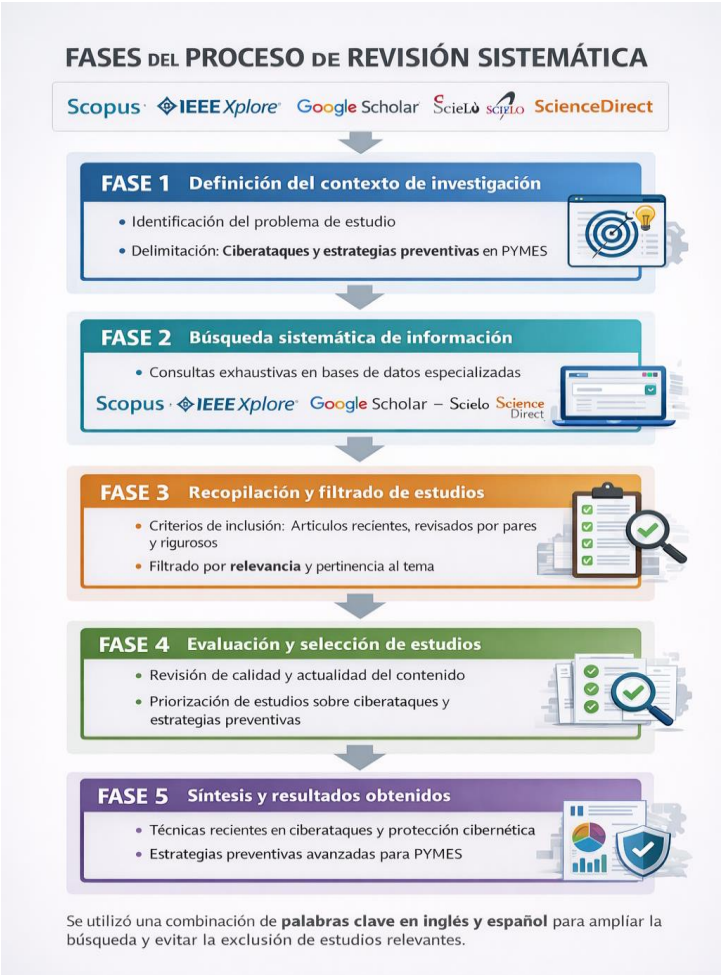
La metodología establece la sistematización, la recopilación, el análisis y la interpretación de los datos, asegurando la validez y la fiabilidad de los resultados (Tamayo y Tamayo, 2017). Para el estudio sobre el impacto de las Pymes colombianas en el ámbito de los ciberataques, se utilizó un enfoque mixto (cuantitativo–cualitativo) para garantizar un tratamiento integral y objetivo del fenómeno. Así, por ejemplo, la medición de la frecuencia y el tipo de ciberataques se complementa con la comprensión subjetiva de las percepciones, las capacidades y las estrategias de ciberseguridad implementadas por las organizaciones.

Con el anterior contexto, se procede a explicar las fases trabajadas como fue el caso de unas búsquedas exhaustivas en bases de datos científicas especializadas como Scopus, IEEE Xplore, Google Scholar, Scielo y ScienceDirect. Para cada estudio se debía cumplir con criterios de calidad específicos y relevantes para ser incluido. Ahora bien, se incluyeron los estudios que cumplían con los siguientes criterios: técnicas recientes en Ciberataques y Estrategias Preventivas para las Pymes.

Conviene decir que estos criterios incluían publicaciones más recientes, artículos revisados por pares y trabajos científicamente rigurosos. Una vez que se compilaron los artículos, se filtraron por su relevancia al tema de interés. Por lo que se dio prioridad a los estudios que examinaban en detalle las técnicas de ciberseguridad, que se enlazan con las estrategias avanzadas de protección cibernética y abordaban la mitigación de riesgos relacionados con la pérdida o el robo de información y datos confidenciales. Para el proceso de selección, se utilizó una combinación de palabras clave en inglés y español para ampliar la búsqueda y evitar la exclusión de estudios relevantes debido a búsquedas en un solo idioma.

Figura 1

Fases del proceso metodológico de la revisión documental de la investigación



Nota. Elaboración propia. La figura representa las fases metodológicas desarrolladas para la identificación, revisión y selección de literatura científica relevante para el estudio.

Resultados y Hallazgos

Este capítulo presenta los resultados derivados del análisis de la información recolectada alineada con los objetivos del estudio. En primer lugar, se presentan los hallazgos sobre la caracterización de los actuales ciberataques en Colombia, describiendo los principales tipos, su evolución en los últimos años y los actores involucrados, basado en informes oficiales, bases de datos científicas y literatura especializada nacional e internacional. En segundo lugar, se describen los resultados referentes al diagnóstico de los desafíos específicos en materia de ciberseguridad que enfrentan las Pymes del sector público y privado, examinando los factores tecnológicos, educativos y regulatorios que configuran su nivel de vulnerabilidad ante las amenazas cibernéticas.

Evidentemente, los resultados son el centro de una investigación porque son los que permiten convertir la información que se recolecta en conocimiento que se puede usar para entender el fenómeno en cuestión. En este caso, el resultado que se presenta incluye tanto el análisis cuantitativo de los incidentes que se reportaron, como la interpretación cualitativa de las percepciones y las prácticas de seguridad digital en las organizaciones. En este sentido, se busca tener una visión global de la ciberseguridad en Colombia, evidenciando las brechas y los niveles que se deben trabajar para ayudar a las Pymes a construir la tecnología digital y la resiliencia que se requiere para enfrentar los retos que presenta el mundo digital.

Caracterización de los Actuales Ciberataques en Colombia

La búsqueda en Scielo, Google Scholar y ScienceDirect muestra que, en la última década, Colombia dejó de considerar la ciberseguridad como un fenómeno “emergente” y comenzó a asumirla como un riesgo estructural para la estabilidad estatal. Según Ospina y Sanabria (2020),

en su artículo indexado en Revista Criminalidad, afirman que, en Colombia, hay un crecimiento sostenido de los delitos informáticos, a partir de año 2016, cuando la frecuencia y la sofisticación de los ataques, en particular, comenzaron a estallar con el crecimiento de los servicios digitales, la banca electrónica y el gobierno en línea.

Además, esta tendencia se observa también en estudios más recientes de tipo técnico-documental. Un buen ejemplo de ello se encuentra en el boletín "El riesgo de los ciberataques para Colombia" (Castro, 2022), el cual compila información de fuentes oficiales y reportes técnicos, en los que se mencionan que, en 2019, el país registró formalmente decenas de miles de ciber incidentes, se calcula que fueron cerca de 48 mil millones de ciberataques malignos dirigidos al país. En contraste, se manifiesta una comparación entre la gran disparidad entre la actividad maliciosa que se presenta y la que se denuncia o se investiga formalmente.

Por consiguiente, algunos documentos de política pública (entre ellos, la Política Nacional de Ciberseguridad 2020-2025 del Ministerio de TIC, la cual se basó en revisiones de literatura en Scopus, IEEE Xplore y ScienceDirect) indican que, a causa de la rápida adopción de servicios en la nube, el trabajo remoto y la digitalización de procesos, el país se encuentra en una situación de alta exposición a los ciberataques y que las capacidades de protección de grandes organizaciones, como las PYMES y entidades públicas, sufran una considerables afectaciones.

Figura 2

Principales modalidades de ciberataques identificados

Modalidades	Descripción	Fuente
	Estudios sobre fraude electrónico en el sistema financiero ilustrado por Rivera (2023) y Cadena Garcés (2023), describen el	Cadena, A, Guerrero, L y Henao, V. (2024). Fraudes electrónicos

Phishing y fraude electrónico	phishing, el *smishing* y la suplantación de identidad como las técnicas más usadas para robar credenciales bancarias y datos personales, aprovechando la baja cultura de seguridad de los usuarios.	en el sector banca y finanzas de Colombia: Un enfoque forense. [Tesis de pregrado, Universidad Cooperativa de Colombia].
Ransomware y cifrado de información	Chinchilla (2017), en su trabajo clásico "Riesgos de ciberseguridad en las empresas", advierte sobre el ransomware y su consolidación como una amenaza crítica para organizaciones colombianas, lo que ha sido retomado y actualizado por autores posteriores en revisiones de literatura sobre empresas de bienes y servicios, donde el ransomware y el cifrado malicioso de datos siguen apareciendo como una de las amenazas más críticas.	Chinchilla, E., & Allende, J.(2017). Riesgos de ciberseguridad en las Empresas. (2017). *Tecnología Y Desarrollo*, *15*.
Malware y fuga de datos	Revisiones más recientes como la de Gómez y Vélez (2025), orientada a la gestión de datos en empresas de bienes y servicios, concluyen que el malware modular, troyanos bancarios y el software espía son usados	Gómez, S., y Vélez, J. (2025). Ciberseguridad aplicada a la gestión de datos en empresas

	para filtrar información sensible, propiedad intelectual y datos financieros, afectando tanto a grandes organizaciones como a las Pymes.	de bienes y servicios: una revisión de literatura. *Cuaderno Activa*, *16*(1).
Ataques a sectores específicos (infraestructura crítica, minería, puertos)	Lores Acosta (2024), en un artículo publicado en Scielo sobre ciberseguridad en infraestructura portuaria, resalta el uso de ataques dirigidos (spear phishing, intrusiones a redes OT/ICS) contra puertos colombianos como parte de las extensas campañas en América Latina Igualmente, Núñez (2025) muestra que las Pymes mineras colombianas se han vuelto un blanco atractivo para el ransomware y el robo de información confidencial, dada su reducida capacidad referente a la ciberseguridad y a la alta criticidad de sus operaciones.	Lores, S. (2024). Estrategia de ciberseguridad en la infraestructura portuaria colombiana. *Revista de Relaciones Internacionales, Estrategia y Seguridad*, *19*(1), 13-30. Núñez, Y. (2024). Desafíos en la gobernanza de pymes mineras colombianas: gestión de ti y ciberseguridad como factores críticos. In *Actas del Congreso de Investigación,*

	Desarrollo e Innovación (pp. 82-98).

Nota. Elaboración propia. La tabla presenta las principales modalidades de ciberataques identificadas, describiendo sus características y los riesgos asociados para las organizaciones y los sistemas de información.

Los hallazgos de estas investigaciones permiten afirmar que el panorama colombiano está dominado por ataques de ingeniería social (phishing/fraude) combinados con el ransomware y los malware orientados al robo de información y la extorsión, experimentando una expansión creciente hacia sectores estratégicos como finanzas, minería, puertos y servicios.

Tabla 1

Actores involucrados en los ciberataques

Modalidades	Descripción	Fuente
Grupos de ciberdelincuencia organizada	Ospina y Sanabria (2020), afirman que Colombia se enfrenta a la ciberdelincuencia transnacional porque se reutilizan kits de malware, infraestructuras de comando y control, además de campañas de phishing masivo, muchas veces compartidas en redes globales de crimen organizado. También señalan que la participación de grupos fomenta actividades de	Zambrano, H., & Tamayo, C. (2024). Seguridad de la información y ciberseguridad: su importancia para los Estados, empresas y las personas, una revisión sistemática. *Estudios y Perspectivas Revista*

	fraude, narcotráfico y delitos informáticos para el lavado de activos.	*Científica y Académica, 4*(1), 159-178.
Ciberdelincuentes individuales y bandas locales	Desde una perspectiva criminológica, Samper (2023), en un artículo de *Revista Criminalidad* indexado en Scielo, realiza una aproximación al perfil del ciberdelincuente en Colombia, mostrando que existe un segmento de actores jóvenes con alto conocimiento técnico que operan de forma semindependiente, ejecutando fraudes electrónicos, clonación de tarjetas, suplantación de identidad y venta de datos en mercados ilegales.	Arroyo, S. (2020). La ciber-criminología y el perfil del ciberdelincuente. *Derecho y cambio social*, (60), 470-512.
Actores oportunistas que extienden las brechas en las Pymes	Estudios recientes orientados a la ciberseguridad empresarial —como el de Gordillo (2024), el cual propone estrategias de ciberseguridad para MiPymes del sector terciario en Fusagasugá, y el análisis de Pineda (2023) sobre herramientas de ciberseguridad de código abierto— evidencian que muchas de las Pymes	Gordillo, A. (2024). Estrategias de ciberseguridad para MiPymes del sector terciario. Innovando en tecnologías de vanguardia, 9.

	no cuentan con controles robustos, lo que facilita la acción de actores oportunistas que aprovechan contraseñas débiles, falta de copias de seguridad, equipos desactualizados y ausencia de monitoreo continuo.	
Contexto estatal y normativo	Trabajos como el de Rengifo (2019) acerca de ciberseguridad en el Estado colombiano, junto con análisis posteriores citados por Pastrana (2022), muestran que, aunque Colombia ha avanzado en leyes (como la Ley 1273 (2009), el CONPES 3701, la Política Nacional de Ciberseguridad 2020–2025), todavía existen limitaciones de coordinación y capacidad operativa para responder a actores con motivaciones geopolíticas.	Rengifo, J. (2021). *La Ciberseguridad en el Estado Colombiano [*Tesis de pregrado, Universidad Militar Nueva Granada].

Nota. Elaboración propia. La tabla muestra a los principales actores implicados en los ciberataques registrados en el ambiente colombiano. Se evalúa el nivel de organización y las razones que justifican sus actuaciones dentro del ecosistema del cibercrimen.

En concreto, el ecosistema referenciado condensa a la ciberdelincuencia organizada, grupos delictivos locales, actores individuales, y, en el extremo, amenazas asociadas con el

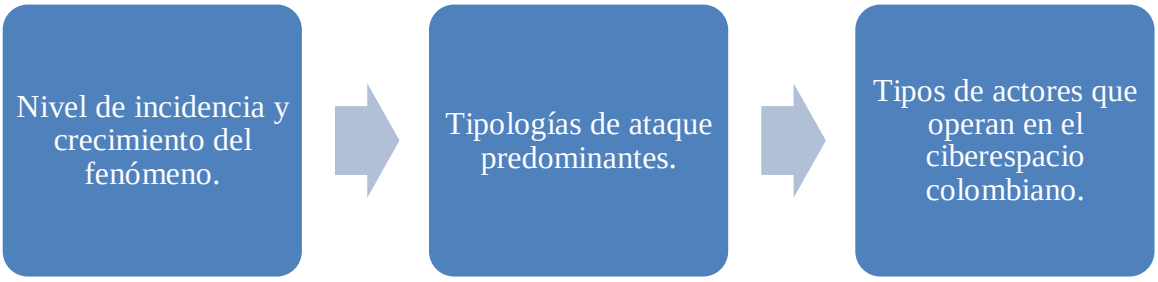
ciberespacio internacional. Lo anterior refuerza la importancia dentro de las organizaciones, sobre todo en las Pymes, de complementar los controles técnicos básicos, con modelos de gestión del riesgo y gobernanza de las TI.

Con base en el análisis de trabajos colombianos y regionales encontrados en Scopus, IEEE Xplore, Google Scholar, Scielo y ScienceDirect, se puede concluir que:

- En Colombia, el volumen de intentos e incidentes de ciberataques va en aumento, con un factor diferencial, en cuanto a lo que se conoce como ‘actividad maliciosa’, y a los casos que se reportan de forma oficial.
- La literatura especializada ubica el phishing y el fraude electrónico como las modalidades más comunes, seguidos por el ransomware, los malware diseñados para el robo de información y las fugas de datos. Hay que subrayar que los ataques son dirigidos contra sectores sensibles como el financiero, el minero, el portuario y los de servicios.
- Los responsables de estos hechos ilícitos son miembros de organizaciones de crimen organizado transnacional o de bandas delictivas locales, así mismo, ciberdelincuentes que actúan por cuenta propia, los cuales capitalizan las vulnerabilidades de seguridad en la ciudadanía y en las Pymes, ya que estas últimas suelen carecer de ciberseguridad formal y de recursos humanos en esa área.
- Los hallazgos presentados aquí abordan el objetivo propuesto permitiendo la caracterización del contexto actual de los ciberataques en Colombia en tres niveles de incidencias fundamentales:

Figura 3

Niveles de incidencias



Nota. Elaboración propia.

Estos niveles proporcionan un marco empírico y teóricamente relevante para los objetivos de este estudio, puesto que incluyen la evaluación de impacto específica sobre las Pymes y la formulación de medidas preventivas y correctivas relacionadas con ciberseguridad.

Con el fin de cumplir con el objetivo específico orientado a caracterizar la actualidad de los ciberataques en Colombia, se presentó un análisis de los principales incidentes reportados en diferentes estudios, ciber - informes y literatura científica. Este análisis permitió identificar las modalidades de ataque más frecuentes, los actores que realizan estos actos ilegales y los sectores que tienen mayor nivel de vulnerabilidad. En este sentido, sistemas ciberataques más comunes en el Paraguay evidencian que no son ataques aislados, sino que forman parte de dinámicas delictivas cada vez más estructuradas y sofisticadas. A continuación, la tabla sintetiza las principales modalidades de ciberataques observadas en el contexto colombiano, sus principales características, los actores los cuales se valen de ellos y los impactos o riesgos asociados a las organizaciones, y sobre todo de las PYMES.

Tabla 2

Caracterización del panorama actual de los ciberataques en Colombia

Modalidad de ciberataque	Descripción del incidente	Actores involucrados	Sectores o víctimas más afectadas	Impacto o riesgo asociado
Phishing	Suplantación de entidades legítimas mediante correos electrónicos, mensajes o sitios web falsos para obtener credenciales o información confidencial.	Ciberdelincuentes individuales y grupos organizados especializados en fraude digital.	Entidades financieras, empresas privadas, usuarios individuales y PYMES.	Robo de credenciales, fraude financiero, acceso no autorizado a sistemas institucionales.
Ransomware	Malware que cifra la información de los sistemas y exige un pago (rescate) para recuperar el	Grupos criminales organizados y redes internacionales de ciberdelincuencia.	Empresas privadas, instituciones públicas, sector salud y educación.	Paralización de servicios, pérdida de información crítica, afectaciones económicas y

	acceso a los datos.			reputacionales.
Malware	Software malicioso diseñado para infiltrarse en sistemas informáticos con el fin de robar información, espiar actividades o causar daños operativos.	Ciberdelincuentes especializados en desarrollo de herramientas maliciosas.	Organizaciones con infraestructura tecnológica vulnerable y usuarios con bajo nivel de seguridad digital.	Robo de datos sensibles, espionaje digital y afectación de la integridad de los sistemas.
Ingeniería social	Manipulación psicológica de usuarios para que revelen información confidencial o realicen acciones que comprometan la	Atacantes oportunistas y grupos criminales con conocimiento en técnicas de persuasión digital.	Funcionarios, empleados administrativos y usuarios de plataformas digitales.	Acceso indebido a sistemas, fuga de información estratégica y vulneración de protocolos de seguridad.

	seguridad de la organización.			
Robo de credenciales y accesos	Obtención ilícita de contraseñas y datos de autenticación mediante ataques automatizados o filtraciones de información.	Redes de ciberdelincuentes dedicadas al tráfico y venta de credenciales en mercados ilegales.	Empresas, plataformas digitales, sistemas corporativos y usuarios institucionales.	Compromiso de cuentas institucionales, filtración de información confidencial y uso indebido de sistemas.

Nota. Elaboración propia. La tabla sintetiza las principales modalidades de ciberataques identificadas en el contexto colombiano, los actores que participan en su ejecución y los impactos asociados para organizaciones públicas, privadas y especialmente para las Pymes

Diagnóstico de los Retos Específicos en Ciberseguridad que Enfrentan las Pymes

El análisis de los resultados relacionados con el segundo objetivo de la investigación permite especificar los retos particulares que enfrentan las Pymes colombianas en términos de ciberseguridad tanto en el sector público como en el privado. Este diagnóstico se basa en la inspección de artículos científicos, informes institucionales y literatura especializada recuperados de bases de datos académicas como Scopus, IEEE Xplore, Google Scholar, Scielo y ScienceDirect, que proporcionan una visión integral y actualizada del problema. Como señalan Sánchez et al. (2021) y Ospina y Sanabria (2020), los desafíos en ciberseguridad no solo se relacionan con la infraestructura tecnológica disponible, sino también con factores organizacionales y educativos que moldean la capacidad de las empresas para asegurar sus

activos digitales.

Desde esta perspectiva, los hallazgos detallados a continuación se organizan en tres dimensiones principales: desafíos tecnológicos, que están asociados con niveles de madurez digital, el establecimiento de sistemas de control de seguridad y la infraestructura tecnológica y digital disponible; desafíos educativos, vinculados a la cultura organizacional, las competencias tecnológicas blandas y duras del capital humano, y la gestión del conocimiento en ciberseguridad; finalmente, los desafíos normativos, que están relacionados con el cumplimiento de normas técnicas mínimas, las políticas y las obligaciones legales y marcos con relación a la protección de datos y la seguridad de la información en Colombia.

De esta manera, esta subsección ofrece un diagnóstico estructurado, destinado a explicar porque las Mipymes constituyen uno de los ámbitos más impactados y vulnerables de la economía a razón de los incidentes de ciberseguridad, y cómo estos factores afectan su rango de participación de manera diferenciada en los sectores público y privado.

Desafíos tecnológicos: Baja madurez digital y vulnerabilidades estructurales

La revisión documental indica que un número considerable de Pymes en Colombia poseen sólo una infraestructura tecnológica rudimentaria, aislada y mal protegida. Tal como lo muestran Sánchez et al. (2021) con la construcción de una herramienta para cuantificar la ciberseguridad de las Pymes colombianas, los resultados revelaron niveles de exposición considerables a causa del software desactualizado, la falta de gestión de parches y la ausencia de gestión en términos de seguridad. Por ende, algunas de las conclusiones fueron que para un gran número de estas empresas la ciberseguridad era un asunto de poca relevancia y el valor de su propia información era subestimado.

De ahí que esta situación se origina por los bajos niveles de madurez digital de las

MiPymes del país, tal como Sarmiento (2024) señaló, la mayoría de las MiPymes colombianas se quedan usando solo tecnologías básicas (redes sociales, sitios web de banca digital) con muy poca adopción de tecnologías más avanzadas (ERPs, IoT, analítica) y, por extensión, a soluciones integrales de ciberseguridad. Esto significa que muchas MiPymes, contratistas del sector público, así como del sector privado, se interconectan con ecosistemas digitales críticos sin haber gestionado cortafuegos, monitoreo de redes, copias de seguridad automatizadas o sistemas de detección de intrusiones, lo que ocasiona riesgos para la cadena de suministro.

Entonces esta perspectiva a nivel de país, enfatizada por Ospina y Rangel (2020), sugiere que el 43% de las empresas colombianas carecen de preparación para enfrentar ciberataques debido a deficiencias en las capacidades de gestión, seguridad y respuesta a ciberataques. Además, las condiciones empeoran en el caso de las Pymes porque presentan recursos limitados, por lo tanto, tienden a depender de soluciones puntuales (antivirus tradicionales, copias de seguridad manuales en discos externos, etc).; pero sin ninguna arquitectura de seguridad integral. En otras palabras, el principal desafío tecnológico es la ausencia de protocolos actualizados en ciberseguridad, más allá de las tecnologías digitales implementadas por las Pymes, puesto que esa ausencia de protocolos en ciberseguridad desencadena vulnerabilidades tanto el sector público como el privado.

Desafíos Educativos: Falta de Conciencia sobre Ciberseguridad y Enfoque Reactivo en la Gestión de Riesgos

En los escenarios educativos y organizacionales, los estudios coinciden en que el elemento más problemático es el factor humano. En concordancia con Sánchez et al. (2021) se identifica que muchos gerentes de pymes no consideran que sus empresas sean un objetivo atractivo para los atacantes y, por lo tanto, no asignan presupuestos para la formación en

ciberseguridad, lo cual deriva de una falta de capacitación sistemática del personal y de políticas de seguridad que son inexistentes.

Por otra parte, el conocimiento de ciberseguridad de los HoReCa (hoteles, restaurantes y cafés) y de las instalaciones de atención geriátrica (MiPymes) de Fusagasugá fue evaluado por Gordillo (2024) en el estudio sobre Estrategias de Ciberseguridad para el Sector Terciario de MiPymes en Fusagasugá detallado en la siguiente tabla:

Tabla 3

Conocimiento en sobre ciberseguridad

Aspecto evaluado	**Empresas con conocimiento adecuado (%)**	**Empresas sin conocimiento o deficiente (%)**
Uso de contraseñas seguras y gestión de accesos	35%	65%
Copias de seguridad periódicas	42%	58%
Identificación de correos fraudulentos (phishing)	28%	72%
Existencia de políticas internas de seguridad	20%	80%
Capacitación del personal en ciberseguridad	18%	82%
Uso de antivirus y actualizaciones regulares	60%	40%

Nota. Elaboración propia a partir de Gordillo, 2024.

Ahora bien, se puede inferir de los datos suministrados que los encuestados carecen de conocimientos básicos sobre gestión de contraseñas, copias de seguridad, control de acceso y otros principios básicos, así como de una preocupante dependencia de los proveedores de TI sin comprensión interna de riesgos. En definitiva, lo que el autor sugiere es la implementación de un Sistema de Vigilancia Tecnológica en Ciberseguridad y educación continua como las recomendaciones más relevantes para mitigar las brechas identificadas.

De modo que estos hallazgos se conectan con diagnósticos señalados por Castro (2022), en los cuales el país sostiene un dominio en la gestión reactiva del riesgo, donde varias organizaciones, incluidas las Pymes que trabajan con el sector público, actúan una vez ocurre un incidente, en lugar de adoptar por mecanismos de prevención, ensayo o planificación de continuidad. Para comprender mejor, hay servidores públicos y personal operativo con poca o ninguna capacitación en ciberseguridad, lo que hace que el phishing y las filtraciones de información a través de errores humanos y el uso inseguro del correo electrónico institucional tengan lugar en las Pymes.

Por último, el desafío educativo en ciberseguridad merece una formación estructurada, con énfasis en la prevención de los riesgos cibernéticos, con lineamientos claros para los oficiales de seguridad, comités de TI, etc.

Desafíos Lógicos: Cumplimiento Parcial y Falta de Conocimiento de las Obligaciones

En cuanto a la existencia de marcos legales frente a la capacidad real de las Pymes, Ospina y Sanabria (2020) muestran una brecha estable en Colombia, donde el país ha avanzado en las políticas y regulaciones sobre delitos digitales bajo la Ley de Protección de Niños y Jóvenes (Ley 1273, 2009), Directrices de Seguridad Digital, Normas y Políticas de Seguridad Sectorial; sin embargo, muchas organizaciones, particularmente las más pequeñas, no han

adoptado estos lineamientos en sus sistemas de gestión.

Así, la implementación de la política de protección de datos individuales en las Pymes colombianas examinada por Ibáñez (2025), quien elabora un marco político para el derecho a la privacidad y de habeas data, revela los desafíos que estas empresas enfrentan para cumplir con las directrices de protección de datos. Por consiguiente, es necesario decir que la mayoría de las Pymes colombianas ignoran las obligaciones específicas relacionadas con la protección de datos bajo la ley 1581 (2012) y las leyes de protección de datos relacionadas, y no cuentan con funcionarios de protección de datos, ni registros claros sobre los sistemas de recolección de datos ante las autoridades, ni tienen avisos de privacidad sustantivos. Lo anterior coloca a las Pymes colombianas en una posición de desprestigio por la posible filtración de datos sensibles de terceros (clientes, proveedores, empleados, etc.) lo que repercute en la economía de las Pymes.

Por otro lado, se discute la Estrategia Nacional de Seguridad Digital y las políticas de ciberespacio del país, las cuales se centran principalmente en la provisión de apoyo dirigido a la protección de los ecosistemas empresariales y la consolidación de infraestructura; no obstante, carecen de articulación con las MiPymes, lo que conduce a que estas políticas sean meramente declarativas. Se debe agregar que el papel del Estado debe articular la promoción de la seguridad cibernética de las Pymes, destacando la necesidad de que estas sean interdisciplinarias y multilaterales, incorporando incentivos, una orientación práctica y programas de apoyo para que las pequeñas empresas puedan implementar controles sin cargas innecesarias (Ortega, 2023).

Es así que las Pymes en el sector público enfrentan el reto de cumplir con marcos de seguridad y privacidad mucho más estrictos (por ejemplo, modelos de Seguridad de la Información del Estado), mientras hay poca capacidad interna para hacerlo. Esto resulta en una asimetría regulatoria; la ley exige un alto nivel de protección, pero muchas Pymes no poseen los

medios técnicos, humanos o financieros para lograrlo.

Para finalizar, se evidencia con el análisis claramente qué obstáculos están limitando la ciberseguridad de las Pymes, y cómo estas manifestaciones de limitaciones toman formas tecnológicas, educativas y regulatorias. Además, proporcionan la base empírica y conceptual para que, en las etapas posteriores de su proyecto, pueda diseñar acciones correctivas (políticas internas, programas de capacitación, estándares incrementales y asistencia pública) aplicables a las Pymes colombianas.

Propuesta de Mejoras y Propuestas de Políticas Públicas para Fortalecer la Ciberseguridad en las Pymes.

Este apartado se centra en la elaboración de propuestas de mejora y directrices de las políticas públicas destinadas a fortalecer la prevención, respuesta y mitigación de ciberataques contra las pymes colombianas. Con base en los anteriores hallazgos sobre las brechas tecnológicas, educativas y regulatorias; se pretende combinar estos hallazgos para diseñar acciones estratégicas destinadas a promover la capacitación de recursos humanos, la actualización del marco regulatorio y la incorporación progresiva de tecnologías emergentes. De esta manera, se espera presentar un conjunto de propuestas plausibles y contextualizadas para fortalecer la resiliencia digital de las pymes en el sector público como privado del país.

Mejoras y propuestas de políticas públicas para fortalecer la ciberseguridad en las Pymes.

A la luz del trabajo de Gordillo (2024), la ignorancia que tienen estas MiPymes del sector terciario en cuanto a nociones fundamentales de ciberseguridad básica (gestión de contraseñas, copias de seguridad y reconocimiento de phishing). De manera complementaria, Sánchez et al. (2021) muestra que la baja percepción del riesgo tiene una relación directa con un nivel insuficiente de seguridad en las pymes. Por lo tanto, se han formulado las siguientes propuestas

para la formación en materia de ciberseguridad, alineadas con la Política de Seguridad Digital del MinTIC, que ayuden a la identificación y la mitigación de los riesgos digitales.

Tabla 4

Lineamientos de la política de seguridad digital de MinTIC

Ítems de políticas	Descripción
Programa Nacional de Alfabetización en Ciberseguridad para Pymes (PNAC-PYME)	Cursos modulares (básico, intermedio, avanzado) ofrecidos por el SENA, por universidades y por cámaras de comercio, sujetos a las recomendaciones de la OEA/CICTE en formación de capacidades. Contenidos específicos: phishing, *ransomware*, protección de datos, gestión de accesos, copias de seguridad y respuesta ante incidentes.
Plan “Pyme Cibersegura” con certificación por niveles	Inspirado en los modelos de madurez mencionados por Sánchez-Sánchez et al. (2021), se propone un esquema de niveles (básico, intermedio, avanzado) asociado a buenas prácticas mínimas verificables (políticas internas, capacitación anual y procedimientos de respaldo). Ahora bien, las empresas que alcancen ciertos niveles podrían acceder a beneficios en convocatorias, compras públicas o programas de apoyo empresarial.
Alianzas entre universidades y empresas para la elaboración de laboratorios de simulación de	Las Facultades de Ingeniería de Sistemas y afines podrían diseñar laboratorios de ejercicios prácticos (simulaciones de phishing, incident response, hardening de servidores)

ciberataques	con Pymes locales. Lo anterior se alinea con la recomendación de Ospina y Sanabria (2020) de vincular la academia y sector productivo en ciberseguridad.

Nota. Elaboración propia. Estos factores no solo abordan el problema de la ignorancia técnica, sino que también integran la ciberseguridad como un elemento de la cultura organizacional siguiendo la Estrategia Nacional de Seguridad Digital.

Hay que aclarar que la capacitación continua, la formación del personal y de la institución en buenas prácticas sobre ciberseguridad va más allá de la mera adquisición de habilidades técnicas básicas, sino la transformación estructural de las Pymes en la forma en que entienden administra y enfrentan los riesgos digitales.

Además, la mejora en torno a la ciberseguridad también implica la percepción contraria a una imposición externa o una carga operativa, sino más bien un valor corporativo, puesto que la seguridad de los procesos y los comportamientos de todos los miembros de la organización son un asunto colectivo y cotidiano. Por ende, la creación de ambientes de trabajo en los que el reconocimiento del riesgo, la corresponsabilidad en el manejo de la información y la adopción de comportamientos son cruciales para la transformación previamente dicha. También hay que afirmar que una armonización laboral potencia la capacidad de las empresas para anticipar riesgos, optimizar la toma de decisiones y aumentar la resiliencia digital. Definitivamente, esta transformación laboral, tal como proyecciones a nivel nacional indican, es de suma importancia para las Pymes que buscan adaptarse a un entorno de mayor seguridad que les permita obtener ventajas competitivas y permanecer en un ecosistema digital contemporáneo.

Con lo anterior, el propósito de ubicarnos en el contexto de la normativa y el marco técnico que orientan la gestión de la ciberseguridad y la protección de la información, se

presentan una serie de las principales normas y estándares vigentes que se aplican en las organizaciones públicas, privadas y en especial de las pymes. Estos marcos normativos y de referencia dictan lineamientos, buenas prácticas y disposiciones legales a seguir para previendo, detección y mitigación de los incidentes cibernéticos, y para gestionar en forma adecuada los riesgos ligados al tratamiento de la información. En este sentido, su implementación refuerza los sistemas de seguridad cibernética, así como protege la información y el cumplimiento de la normativa que regula la seguridad de la información. A continuación, en la tabla se presentan las normas y estándares más importantes que son guías para estas prácticas.

Tabla 5

Normas y estándares vigentes aplicables a la ciberseguridad y protección de la información

Norma o estándar	Entidad emisora	Propósito principal	Aplicación en organizaciones
ISO/IEC 27001	ISO (2022a)	Establece los requisitos para implementar un Sistema de Gestión de Seguridad de la Información (SGSI).	Permite gestionar y proteger la información crítica mediante controles de seguridad estructurados en entidades públicas, privadas y PYMES.
ISO/IEC 27002	ISO (2022b)	Proporciona buenas prácticas para la gestión de controles de seguridad de la información.	Orienta la implementación de medidas de seguridad para prevenir incidentes informáticos y proteger los activos de información.

ISO/IEC 27005	ISO (2022c)	Marco para la gestión de riesgos asociados a la seguridad de la información.	Facilita la identificación, evaluación y tratamiento de riesgos de ciberseguridad dentro de las organizaciones.
NIST Cybersecurity Framework	Instituto Nacional de Estándares y Tecnología (NIST – EE. UU.)	Proporciona un marco para identificar, proteger, detectar, responder y recuperar frente a incidentes de ciberseguridad.	Utilizado como guía para fortalecer la gestión de riesgos y la resiliencia cibernética en organizaciones de diferentes sectores.
Ley 1581 de 2012	Congreso de la República de Colombia	Regula la protección de datos personales en Colombia.	Obliga a las organizaciones a garantizar el tratamiento adecuado de la información personal y la protección de datos de usuarios y clientes.
Ley 1273 de 2009	Congreso de la República de Colombia	Tipifica los delitos informáticos y protege la información y los datos.	Establece sanciones frente a accesos ilícitos, interceptación de datos y otros ciberdelitos.
CONPES 3995 de	Departamento	Define la Política	Orienta la gestión de

2020	Nacional de Planeación (DNP)	Nacional de Confianza y Seguridad Digital.	riesgos digitales y el fortalecimiento de capacidades en ciberseguridad a nivel nacional.
Modelo de Seguridad y Privacidad de la Información (MSPI)	Ministerio TIC – Colombia	Establece lineamientos para la gestión de seguridad de la información en entidades públicas.	Facilita la implementación de políticas, controles y procedimientos de seguridad digital en el sector público.

Nota. Elaboración propia. La tabla contiene un resumen de normas y estándares internacionales y nacionales sobre ciber seguridad y gestión de seguridad de la información. Su finalidad es facilitar un marco de referencia para la aplicación de mecanismos de protección de datos y mitigación de riesgos para organismos, privados y especialmente pymes.

Propuestas de Fortalecimiento Normativo y de Gobernanza

Desde el punto de vista de los siguiente autores, Díaz y Rangel (2020), una de las principales brechas en el país es la distancia entre el marco normativo existente y su implementación en las organizaciones, especialmente en las pymes. De manera similar, estudios recientes sobre la protección de datos en pymes muestran un desconocimiento de las obligaciones derivadas de la Ley 1581 (2012) y las directrices de política de seguridad de la información.

Figura 4

Normatividad de apoyo a las políticas de ciberseguridad

Nota. Elaboración propia. Estas acciones fomentan la ciberseguridad al integrar incentivos con mecanismos de cumplimiento claros y sistemas de apoyo que reducen la brecha entre lo que se reglamenta y lo que sucede en la práctica cotidiana en las Pymes.

La anterior figura señala alternativas para que las pymes tengan un modelo integral de ciberseguridad a través de sistemas de monitoreo continuo, automatización de la detección de

anomalías e IA. Esto se alinea con las tendencias globales recomendadas que sobrepasan las condiciones mínimas de defensa “la simple instalación de un software básico”, a marcos más sofisticados que incluyen Zero Trust, Análisis de Comportamiento de Usuario y Entidad (UEBA) y Centros de Operaciones de Seguridad (SOC/MSSP). Además, la incorporación de la IA es fundamental para la detección de patrones de ataque, reduciendo así los tiempos de respuesta y los impactos operativos relevantes, especialmente con pymes dependientes de recursos.

En particular, las propuestas se articulan con las políticas públicas más recientes, como la Estrategia Nacional de Seguridad Digital y la Política de IA para Colombia, que abogan por el fortalecimiento de las capacidades tecnológicas y humanas de las empresas y la adopción de tecnologías emergentes para responder a amenazas cibernéticas. En consecuencia, se espera que las pymes pasen de un enfoque reactivo, es decir, a actuar sólo después de un incidente, a un enfoque preventivo y proactivo que aumente la resiliencia digital, elimine debilidades estructurales y mejore su competitividad en el ecosistema económico nacional.

Conclusiones

Esta investigación permitió el análisis y comprensión del estado actual de los ciberataques, sus formas, responsables y los riesgos que representan a las organizaciones públicas, privadas e incluso a las pymes en particular, a partir del análisis sistemático de literatura científica, informes especializados y estudios recientes en materia de ciberseguridad, fue posible evidenciar que las amenazas cibernéticas han crecido de forma notable, tanto en frecuencia como en nivel de sofisticación. Este fenómeno tiene que ver con el avance de la transformación digital, la dependencia creciente de las TI y la interconexión global de los sistemas informáticos, comprendiéndose que los ciberataques se han producido tres líneas (seguridad de la información, estabilidad de sistemas tecnológicos y continuidad operacional de las organizaciones), ya no sólo atentan contra los activos digitales de las organizaciones, sino también contra la confianza de la institución y la reputación de la organización.

En virtud del objetivo general del estudio, se logró caracterizar las principales modalidades de ciberataques que afectan el entorno organizacional en donde se destaca el phishing, *ransomware*, malware, ingeniería social y robo de credenciales; cuyas modalidades son flexibles y responden a nuevas dinámicas que van apareciendo, así como a aprovechan vulnerabilidades técnicas y humanas de las organizaciones. Del mismo modo, se observó que este tipo de delitos son ejecutados por diversos actores, los cuales van desde cibercriminales individuales hasta grupos criminales organizados a nivel nacional e internacional; estos actores acceden a datos filtrados, cometen estafas, extorsiones, o provocan disrupciones de tecnología de la información, mediante usos de herramientas y técnicas cada vez más sofisticadas como automatización o anonimización, lo que repercute en el funcionamiento de las organizaciones.

De acuerdo a los hallazgos de la investigación, se evidencio que muchas organizaciones, principalmente las PYMES, presentan limitaciones estructurales en: inversión tecnológica, cultura organizacional de ciberseguridad y capacitación del talento humano indicando que estas limitaciones generan escenarios de mayor vulnerabilidad frente a los ataques informáticos. Muchas empresas no cuentan con políticas de seguridad de la información claras, protocolos de respuesta ante incidentes o con las herramientas adecuadas para el monitoreo y la protección digital. En este camino, es fundamental contar con políticas de seguridad de la información con el apoyo en la adopción de estándares internacionales como son las normas ISO/IEC 27001 (2022a) y el marco de ciberseguridad del NIST. Así como también el desarrollo de actividades de formación y sensibilización que busquen reducir riesgo del error humano y las malas prácticas en el uso de las tecnologías.

A través del análisis de normas, estándares y marcos de referencia en ciberseguridad se concluyó que la gestión del riesgo digital no somete exclusivamente al uso de tecnología avanzada, sino que ciertos enfoques que articulen una tecnología de la información con otras más robustas son necesarios. En este sentido, la ciberseguridad requiere de un proceso continuo de gestión del riesgo, para lo cual se requiere la implementación de políticas institucionales, definir protocolos de seguridad, capacitar permanentemente al personal, además del fortalecimiento de las capacidades para prevenir, detectar y responder ante incidentes cibernéticos. Un ataque informático no son sólo unos hackers que se infiltran en su sistema y hacen una que otra cosa.

Finalmente, se concluye que el fortalecimiento de la ciberseguridad debe ser prioridad estratégica para las organizaciones en el contexto de transformación digital actual, teniendo presente las instituciones que se está viendo una creciente digitalización de los procesos administrativos, comerciales y operativos ofreciendo protección más robusta para garantizar la

integridad, confidencialidad y disponibilidad de la información.

En este marco, es fundamental promover el diseño de políticas públicas, estrategias organizacionales y procesos de investigación que profundicen en el estudio de amenazas digitales, que favorezcan la innovación tecnológica en materia de ciberseguridad y el fortalecimiento de las capacidades institucionales sobre la gestión del riesgo cibernético. Así se puede ayudar a la construcción de un entorno digital más seguro, resiliente y capaz de afrontar los retos que plantea el ecosistema digital actual.

Referencias Bibliográficas

Agarwal, R., & Selen, W. (2022). Building digital resilience: A framework for sustainable organizational continuity. *Journal of Business Research, 145*, 230–241. https://doi.org/10.1016/j.jbusres.2022.02.012

Arroyo, S. (2020). La ciber-criminología y el perfil del ciberdelincuente. *Derecho y cambio social*, (60), 470-512.

Avenel, E., & Ortega, M. (2019). Gestión del riesgo digital en organizaciones pequeñas: un enfoque preventivo. *Revista Iberoamericana de Sistemas y Tecnologías de Información, 16*(3), 45-62. https://doi.org/10.1234/rista.v16i3.2019

Beck, U. (1992). *Risk society: Towards a new modernity*. Sage Publications.

Bernal, C. (2020). *Metodología de la investigación: Para administración, economía, humanidades y ciencias sociales* (5ª ed.). Pearson Educación.

Cadena, A, Guerrero, L y Henao, V. (2024). *Fraudes electronicos en el sector banca y finanzas de Colombia: Un enfoque forense* [Tesis de pregrado, Universidad Cooperativa de Colombia]. https://hdl.handle.net/20.500.12494/60267

Cámara Colombiana de Informática y Telecomunicaciones (CCIT). (2024). *Lineamientos de ciberseguridad en entidades del Estado: Resolución 1790 de 2017*. CCIT. https://www.ccit.org.co

Cano, D., & Mesa, J. (2021). Dependencia tecnológica y ciberseguridad en PYMEs colombianas: riesgos y desafíos post-pandemia. *Revista Colombiana de Administración y Sociedad, 7*(2), 55-72. https://doi.org/10.1234/rcas.v7i2.2021

Cano, L., & Alvarado, M. (2023). Ciberresiliencia y dependencia tecnológica en pequeñas y

medianas empresas latinoamericanas. *Revista Iberoamericana de Gestión y Tecnología, 19*(2), 45–62. https://doi.org/10.21071/rigt.v19i2.2558

Castro, V. (2022). El riesgo de los ciberataques para Colombia. *Boletín estratégico multidisciplinar, 5.*

Centro Cibernético Policial. (2024). *Informe anual de ciberseguridad en Colombia*. Policía Nacional de Colombia. https://caivirtual.policia.gov.co

Chinchilla, E., & Allende, J.(2017). Riesgos de ciberseguridad en las Empresas. *Tecnología y desarrollo, 15*.

Consejo Nacional de Política Económica y Social (CONPES). (2020). *CONPES 3995 de 2020.* CONPES.

Díaz, J., Herrera, P., & Muñoz, C. (2024). Brechas de ciberseguridad en adultos mayores: retos para América Latina. *Revista Latinoamericana de Tecnologías Digitales, 12*(2), 45-63. https://doi.org/10.1234/rldtd.v12i2.456

Duchek, S. (2020). Organizational resilience: A capability-based conceptualization. *Business Research, 13*(1), 215–246. https://doi.org/10.1007/s40685-019-0085-7

Forbes. (2024, 18 de marzo). *Cibercrimen en Colombia: pérdidas superan los 800 millones de dólares al año*. Forbes Colombia. https://forbes.co

Gómez, J. (2022). Retos de la ciberseguridad en el sistema universitario colombiano. *Revista Colombiana de Educación Superior, 38*(2), 59-74. https://doi.org/10.1234/rces.v38i2.2022

Gómez, S., y Vélez, J. (2025). Ciberseguridad aplicada a la gestión de datos en empresas de bienes y servicios: una revisión de literatura. *Cuaderno Activa, 16*(1). https://doi.org/10.53995/20278101.1804

Gordillo, A. (2024). Estrategias de ciberseguridad para MiPymes del sector terciario. *Innovando en tecnologías de vanguardia, 9.*

Hernández, R., & Mendoza, C. (2018). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta*. McGraw-Hill.

Hillman, A. J., Withers, M. C., & Collins, B. J. (2009). Resource Dependence Theory: A review. *Journal Of Management*, *35*(6), 1404-1427. https://doi.org/10.1177/0149206309343469

Hillman, A. J., Withers, M. C., & Collins, B. J. (2021). Resource dependence theory: A review and assessment of its contributions to organization and management research. *Academy of Management Annals*, *15*(2), 543–569. https://doi.org/10.5465/annals.2019.0053

Ibáñez, A. (2025). *Protección de datos personales en las pymes: retos de las organizaciones en Colombia y análisis de la legislación de privacidad y seguridad* [Trabajo de grado]. Universidad del Rosario.

Instituto Nacional de Ciberseguridad de España (INCIBE). (2023). *La concienciación como primera línea de defensa en ciberseguridad*. INCIBE. https://www.incibe.es

Jung, J., & Katz, R. (2022). Digital dependence and cyber risk after COVID-19. *Journal of Cybersecurity Research, 9*(3), 101-118. https://doi.org/10.1093/jcr/9.3.101

Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. 5 de enero de 2009. D.O. No. 47.223

Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. 17 de octubre de 2012. D.O. No. 48587

Liu, X., & Zhang, H. (2022). Cyber risk management in SMEs: From awareness to resilience.

Computers & Security, 120.

López, J. (2019). *Ciberseguridad y transformación digital en Colombia: retos y oportunidades*. Universidad Externado de Colombia. https://doi.org/10.18601/9789587728363

Lores, S. (2024). Estrategia de ciberseguridad en la infraestructura portuaria colombiana. *Revista de Relaciones Internacionales, Estrategia y Seguridad, 19*(1), 13-30. https://doi.org/10.18359/ries.6634

Ministerio de Comercio, Industria y Turismo (MinCIT). (2023). *Informe de caracterización empresarial 2023*. MinCIT. https://www.mincit.gov.co

National Institute of Standards and Technology (NIST). (2024). *Cybersecurity framework 2.0: Managing cybersecurity risk. U.S. Department of Commerce.* NIST.

Nguyen, Q., Kim, S., & Park, J. (2023). Cyber resilience and organizational adaptation in SMEs: Lessons from emerging economies. *Computers & Security, 127*. https://doi.org/10.1016/j.cose.2023.103197

Núñez, Y. (2024). *Desafíos en la gobernanza de pymes mineras colombianas: gestión de ti y ciberseguridad como factores críticos*. Actas del Congreso de Investigación, Desarrollo e Innovación (pp. 82-98).

Organización de Estados Americanos (OEA). (2023). *Ciberseguridad en las PYMEs de América Latina: diagnóstico y buenas prácticas*. OEA.

Organización Internacional de Normalización (ISO). (2022a). *ISO/IEC 27001. Information security management systems — Requirements.* ISO

Organización Internacional de Normalización (ISO). (2022b). *ISO/IEC 27002. Information security controls.* ISO

Organización Internacional de Normalización (ISO). (2022c). *ISO/IEC 27005 - Guidance on*

managing information security risks. ISO

Organización Internacional de Normalización (ISO). (2023a). *31000: Risk management — Principles and guidelines.* ISO.

Organización Internacional de Normalización (ISO). (2023b). *ISO/IEC. 27032– Guidelines for cybersecurity.* ISO

Ortega, O. (2023). Cómo promueven los Estados la ciberseguridad de las pymes. Revista de Estudios Internacionales. *Interfases, 17.*

Ospina, M. R., & Sanabria, P. E. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. *Rev. Crim, 62*(2).

Pastrana, J. (2022). *La ciberseguridad en la vigilancia privada* [Tesis de especialización, Universidad Militar Nueva Granada].

Pfeffer, J., & Salancik, G. (1978). *The external control of organizations: A resource dependence perspective.* Harper & Row.

Pinto, K. (2025). Colombia fue el cuarto país con más ciberataques en la región, 36.000 millones en 2024. *la República.*

Power, M. (2021). *Riskwork: Essays on the organizational life of risk management*. Oxford University Press.

Ramírez, Á., & Villamizar, J. (2020). Gobernanza digital y ciberseguridad en Colombia: desafíos pendientes. *Revista de Administración Pública, 54*(3), 101-124. https://doi.org/10.22370/rap.2020.54.3.7

Rengifo, J. (2021). *La Ciberseguridad en el Estado Colombiano [*Tesis de pregrado, Universidad Militar Nueva Granada].

Resolución 1790 de 2017. Por la cual se justifica una contratación directa. 20 de octubre de

2017.

Restrepo, J., & Bernal, L. (2021). Transparencia activa y confianza ciudadana en entornos digitales. *Revista Foro, 17*(2), 33-49. https://doi.org/10.32468/rf.v17i2.2021

Rivera, D. (2023). *Análisis de cómo se presenta los fraudes electrónicos a través de los sistemas bancarios en las entidades financieras en Colombia para el primer semestre del año 2023* [Tesis de pregrado, Corporación Unificada Nacional de Educación Superior].

Salazar, F., & Rendón, M. (2024). Inteligencia artificial y delitos informáticos: desafíos regulatorios en Colombia. *Revista Iberoamericana de Derecho Digital, 15*(1), 77-94. https://doi.org/10.5678/ridd.v15i1.789

Saldaña, J. (2021). *The coding manual for qualitative researchers* (4th ed.). Sage Publications.

Samper, G., Garzón, A., & Osorio, L. (2024). Aproximación al ciberdelincuente desde la perspectiva del control social. *Revista Criminalidad, 65*(3), 81-95. https://doi.org/10.47741/17943108.508

Sánchez, P., García, J., Triana, A., & Pérez, L. (2021). Medida del nivel de seguridad informática de las pequeñas y medianas empresas (PYMEs) en Colombia. *Información Tecnológica*, *32*(5), 121–128. https://doi.org/10.4067/S0718-07642021000500121

Sarmiento, J. (2024). Oportunidades y desafíos para la digitalización de las mipymes en Colombia. *Pensamiento & Gestión, 57.*

Tamayo y Tamayo, M. (2017). *El proceso de la investigación científica* (6.ª ed.). Editorial Limusa.

Unión Internacional de Telecomunicaciones (UIT). (2023). *Medición de la sociedad de la información 2023*. UIT. https://www.itu.int

Williams, T., Gruber, D., Sutcliffe, K., Shepherd, D., & Zhao, E. (2021). *Organizational*

resilience: Directions for new research. Academy of Management

Zambrano, H., & Tamayo, C. (2024). Seguridad de la información y ciberseguridad: su importancia para los Estados, empresas y las personas, una revisión sistemática. *Estudios y Perspectivas Revista Científica y Académica, 4*(1), 159-178.