Revisión bibliográfica de las amenazas cibernéticas que enfrenta Colombia

Luis Enrique Guzmán Rojas

Tutor

Salomón González García

Universidad Nacional Abierta y a Distancia - UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería - ECBTI

Ingeniería de Sistemas

Bogotá D.C

2025

Revisión bibliográfica de las amenazas cibernéticas que enfrenta Colombia

Luis Enrique Guzmán Rojas

Salomón González García

Trabajo de grado para optar por el título de Ingeniero de Sistemas

Universidad Nacional Abierta y a Distancia - UNAD

Bogotá, 2025

Dedicatoria

Dedico este logro, con profunda gratitud y amor, a mi madre. Que ha sido el faro constante que me ha guiado con esperanza, esperando con ilusión verme alcanzar esta meta. A mis 38 años, este momento no solo me pertenece, también es suyo, porque fue su fe en mí la que no me dejo renunciar.

A mi jefe, por estos 13 años de apoyo incondicional, paciencia infinita y confianza genuina. Gracias por creer en mí incluso cuando las circunstancias no eran fáciles. Su respaldo ha sido clave para que hoy pueda sostener con orgullo este resultado.

Y a mi primo, compañero y hermano, con quien recorrí este proceso hombro a hombro. Juntos enfrentamos los retos, nos impulsamos en los momentos difíciles y celebramos cada pequeño avance. Culminar este camino representa para ambos una felicidad inmensa que guardaremos como un logro compartido para siempre.

Resumen

En la actualidad, la creciente digitalización de los procesos empresariales y la expansión del teletrabajo han generado numerosos desafíos significativos para la protección de datos y sistemas digitales, haciendo de la ciberseguridad un elemento indispensable para el crecimiento sostenible de las organizaciones. Esta revisión bibliográfica busca describir el panorama actual en el que se encuadra la ciberseguridad en Colombia, mediante el análisis de las principales amenazas cibernéticas que se han documentado en el contexto nacional, examinando las estrategias de protección implementadas y evaluando el impacto del marco regulatorio vigente, con el objetivo de proponer estrategias efectivas de mitigación.

A nivel general en el ámbito normativo, Colombia ha establecido importantes avances mediante el Decreto 338 de 2022 y la implementación del modelo de seguridad y privacidad de la información de la Política de Gobierno Digital. Lo cual se ha complementado con la adopción de estándares internacionales como ISO/IEC 27001 y 27032 por parte del sector empresarial. Estas iniciativas buscan fortalecer la ciberresiliencia nacional ante un panorama de amenazas donde predominan el phishing, el ransomware y las vulnerabilidades en entornos cloud, siendo los sectores financieros, de salud y telecomunicaciones los más afectados.

Como respuesta, las organizaciones están implementando estrategias tecnológicas avanzadas que incluyen sistemas de inteligencia artificial para la detección temprana de amenazas, soluciones de seguridad basadas en cloud computing y políticas de seguridad by design. Sin embargo, aún persisten varios desafíos y vacíos críticos en el área, como los relacionados con la capacitación especializada, la asignación de recursos y la coordinación interinstitucional.

Esta investigación enfatiza en la importancia de tener estándares de ciberseguridad actualizadas en el entorno empresarial colombiano, adoptando prácticas globales como el fomento de

programas de capacitación continua, la inversión en tecnologías avanzadas y el fortalecimiento de la cooperación entre los sectores público-privado. De este modo, una gestión integral de ciberseguridad que combine estrategias proactivas, cumplimiento normativo riguroso y el desarrollo de una cultura organizacional centrada en la seguridad digital, será esencial para garantizar la continuidad operativa y la protección de los activos digitales para garantizar la competitividad empresarial en un entorno digital en constante evolución y creciente complejidad.

Palabras clave: Ciberseguridad, Amenazas Cibernéticas, Ciberresiliencia, Organizaciones, Colombia.

Abstract

Currently, the growing digitization of business processes and the expansion of teleworking have generated numerous significant challenges for data and digital systems protection, making cybersecurity an indispensable element for the sustainable growth of organizations. This literature review seeks to describe the current landscape of cybersecurity in Colombia by analyzing the main cyber threats that have been documented in the national context, examining the protection strategies implemented, and evaluating the impact of the current regulatory framework, with the aim of proposing effective mitigation strategies.

At the general regulatory level, Colombia has made significant progress through Decree 338 of 2022 and the implementation of the information security and privacy model of the Digital Government Policy. This has been complemented by the adoption of international standards such as ISO/IEC 27001 and 27032 by the business sector. These initiatives seek to strengthen national cyber resilience in the face of a threat landscape dominated by phishing, ransomware, and vulnerabilities in cloud environments, with the financial, healthcare, and telecommunications sectors being the most affected.

In response, organizations are implementing advanced technological strategies that include artificial intelligence systems for early threat detection, cloud computing-based security solutions, and security-by-design policies. However, several challenges and critical gaps remain in this area, such as those related to specialized training, resource allocation, and inter-institutional coordination.

This research emphasizes the importance of having up-to-date cybersecurity standards in the Colombian business environment, adopting global practices such as promoting continuous training programs, investing in advanced technologies, and strengthening cooperation between

the public and private sectors. Thus, comprehensive cybersecurity management that combines proactive strategies, rigorous regulatory compliance, and the development of an organizational culture focused on digital security will be essential to ensure operational continuity and the protection of digital assets to guarantee business competitiveness in an ever-evolving and increasingly complex digital environment.

Key Words: Cybersecurity, Cyber Threats, Cyber Resilience, Organizations, Colombia.

Tabla De Contenido

Lista De Tablas

Planteamiento Del Problema

En un contexto empresarial cada vez más digitalizado, la ciberseguridad se ha convertido en una necesidad estratégica fundamental para las organizaciones de todos los sectores. En Colombia, factores como la rápida adopción de tecnologías digitales, el auge del comercio electrónico y la creciente dependencia de soluciones basadas en la nube han sido muy útiles tanto a nivel empresarial a la hora de mejorar los procesos y facilitar el alcance de objetivos, como a nivel social generando un notable desarrollo económico. Sin embargo, esta misma transformación digital también implica un nuevo riesgo para las empresas ya que ha incrementado sustancialmente la exposición a amenazas cibernéticas.

Según el informe *Global digital trust insights 2024 de PwC Colombia* (PwC, 2024), las empresas del país consideran que los riesgos cibernéticos se encuentran entre las principales amenazas que enfrentarán en un futuro cercano, reflejando una preocupación por la seguridad en el entorno digital. Además, el mismo estudio reveló que el 28% de las organizaciones en Colombia han reportado costos superiores al millón de dólares como consecuencia de incidentes cibernéticos, lo que evidencia el elevado impacto económico que representan estos ataques.

Entre las amenazas más comunes y preocupantes para las empresas colombianas se encuentran: phishing y ataques de ingeniería social, ransomware, ataques a infraestructuras en la nube y la falta de actualización y parches de seguridad. Los ataques cibernéticos se presentan principalmente en sectores críticos y con alto impacto económico y social como el sector financiero, las empresas de salud y las de telecomunicaciones, causando interrupciones y pérdidas significativas que no solo afectan a la organización, sino que tienden a afectar a un alto número de usuarios de este tipo de organizaciones.

> Entre los factores clave que empeoran la situación de ciberseguridad en Colombia destacan: insuficiente inversión en ciberseguridad, déficit de talento especializado, cumplimiento deficiente de regulaciones, incremento en la sofisticación de los ataques y escasa cultura organizacional en ciberseguridad. Esta situación es especialmente crítica en las Pymes, que representan el 99% del tejido empresarial del país, muchas de las cuales no poseen los recursos técnicos ni financieros para implementar medidas adecuadas de protección (MinTIC, 2023).

Las consecuencias derivadas de la débil gestión de la ciberseguridad son diversas y preocupantes, destacando principalmente: las pérdidas económicas significativas, el daño reputacional, las sanciones legales y regulatorias, y la interrupción de servicios esenciales en sectores estratégicos.

En síntesis, la rápida digitalización en Colombia ha ampliado la exposición de las empresas, especialmente aquellas en el sector financiero, de salud y de telecomunicaciones, y de las Mipymes a amenazas como phishing, ingeniería social, ransomware y fallas de actualización, ahora exacerbadas por el uso extendido de nube, trabajo remoto y canales móviles. A esto se suman brechas persistentes de inversión, déficit de talento especializado, controles débiles en la cadena de suministro y un cumplimiento irregular de buenas prácticas, que se traducen en pérdidas económicas, interrupciones operativas, sanciones y deterioro de la confianza de clientes y usuarios. El problema, por tanto, no es solo tecnológico, sino de capacidades organizacionales pues muchas compañías no logran priorizar, prevenir, detectar o responder a tiempo ante estos riesgos.

Ante esta realidad, se evidencia la urgente necesidad de fortalecer las estrategias de ciberseguridad en el contexto empresarial colombiano, implementando medidas robustas para

mitigar efectivamente los riesgos digitales. Por ello, esta revisión bibliográfica busca responder ¿Cómo pueden las empresas colombianas fortalecer su ciberseguridad para mitigar las amenazas digitales y garantizar una adecuada protección de su información crítica?

Para abordar esta interrogante se analizarán las tendencias actuales en ciberseguridad, las prácticas más efectivas adoptadas internacionalmente y las políticas gubernamentales que pueden contribuir a mejorar significativamente la seguridad digital dentro del ámbito empresarial colombiano.

Justificación

La ciberseguridad se ha convertido en un elemento crucial para garantizar la sostenibilidad y competitividad de las empresas en Colombia. A medida que las organizaciones intensifican su transformación digital, los ciberataques han incrementado en frecuencia, complejidad y severidad. Pero las consecuencias de los ciberataques no se limitan a costos financieros, sino que también impactan en la reputación y operatividad de las empresas. El estudio *Benchmark de ciber riesgo cuantificado por industria en Colombia 2024* (KPMG, 2024) resalta pérdidas económicas, daños reputacionales, y sanciones legales como principales impactos derivados del incumplimiento normativo, pagos de rescates y costos operativos. Por lo que esta investigación es esencial para comprender la magnitud del problema y plantear estrategias robustas para su mitigación efectiva.

Colombia ha registrado un incremento en incidentes cibernéticos, y como se mencionó anteriormente, pese a esto muchas empresas colombianas carecen de planes robustos y efectivos de ciberseguridad; particularmente aquellas empresas que enfrentan serias limitaciones en recursos. Además, el déficit de talento especializado en ciberseguridad es otro desafío considerable; según el informe Brecha de competencias en ciberseguridad 2024 (Fortinet, 2024), Latinoamérica tiene un déficit superior a 700.000 profesionales en ciberseguridad, lo cual limita la capacidad empresarial para afrontar adecuadamente las amenazas digitales; y aunque existen regulaciones específicas en Colombia, muchas empresas no logran implementarlas correctamente por desconocimiento o falta de recursos.

De igual forma, según el *Estudio anual de ciberseguridad (2022-2023)* (CCIT, 2024) muchos incidentes se deben a errores humanos, evidenciando la necesidad de fortalecer la capacitación y sensibilización. Por lo que esta investigación tiene un objetivo social clave al

ayudar a crear conciencia sobre la importancia de la ciberseguridad y reducir esta brecha mediante la sensibilización y desarrollo de competencias especializadas.

Por otro lado, en cuanto a la normativa de ciberseguridad en el país, lineamientos como el Decreto 338 de 2022 y la Política de Gobierno Digital aún tienen limitada implementación práctica en el sector privado de acuerdo con el *Informe tercer cuatrimestre riesgos de seguridad de la información - 2024* (SuperTransporte, 2024). Por lo que este estudio fomentara el cumplimiento efectivo de marcos regulatorios y estándares internacionales como ISOIEC 27001, ISOIEC 27032 y NIST Cybersecurity Framework.

Así, esta revisión bibliográfica responde directamente a la creciente sofisticación y frecuencia de los ciberataques en Colombia, así como al notable incremento de incidentes de seguridad en el ámbito empresarial, lo cual exige un enfoque integral y sistemático. La relevancia se fundamenta en la necesidad de ofrecer soluciones prácticas y aplicables que mejoren las capacidades defensivas de las organizaciones, minimicen su exposición a riesgos digitales y aseguren la continuidad operativa en un entorno económico altamente dependiente de la tecnología y la conectividad. Este estudio proporcionará información estratégica para que directivos y responsables de TI implementen medidas efectivas de protección digital, contribuyendo al fortalecimiento integral de la ciberseguridad en Colombia.

La complejidad del panorama cibernético en Colombia demuestra que no se trata solo de un asunto técnico, sino de un desafío estratégico que impacta la sostenibilidad, competitividad y confianza de las organizaciones. En este contexto, la necesidad de fortalecer las estrategias de ciberseguridad adquiere una relevancia central, ya que de ello depende no solo la protección de la información crítica empresarial, sino también la estabilidad de sectores clave para el desarrollo económico y social del país.

Por esto, esta revisión integra fuentes oficiales y privadas recientes del contexto colombiano (2022-2025) con el fin de mostrar la evolución del riesgo y, sobre todo, traducir ese diagnóstico en acciones concretas: conecta la regulación vigente con controles prácticos de prevención, detección y respuesta ajustados al tamaño, sector y nivel de madurez de cada organización (desde Mipymes hasta grandes empresas), incorpora amenazas emergentes fraude móvil, aplicaciones falsas y suplantación con IA y sus implicaciones operativas, y propone métricas e hitos para medir avances y justificar inversión ante la alta dirección. Así, no se limita a describir el problema: ofrece una guía contextualizada y accionable que otros estudios no entregan con este grado de articulación normativa-operativa para reducir exposición al riesgo y asegurar la continuidad del negocio en Colombia.

Objetivos

Objetivo General

Desarrollar una revisión bibliográfica que identifique y analice las principales amenazas cibernéticas que enfrenta Colombia, con el fin de proponer lineamientos estratégicos de mitigación aplicables al entorno empresarial, orientados a fortalecer la seguridad digital y la resiliencia organizacional.

Objetivos Específicos

Revisar las principales amenazas cibernéticas que enfrenta Colombia a partir de la literatura existente.

Describir el impacto de las amenazas cibernéticas en el entorno empresarial colombiano según los estudios y datos analizados.

Analizar las tendencias y estrategias de ciberseguridad reportadas en la bibliografía reciente aplicables al contexto colombiano.

Examinar el estado actual de las capacidades de protección cibernética en Colombia, con base en la información bibliográfica disponible.

Marco Conceptual

Ciberseguridad: Es el conjunto de prácticas, tecnologías y medidas organizativas destinadas a proteger los sistemas de información, redes y datos frente a accesos no autorizados, ataques o daños (CCIT, 2024).

Resiliencia cibernética: Capacidad de una organización para anticiparse, resistir, adaptarse y recuperarse de incidentes cibernéticos, asegurando la continuidad de sus operaciones críticas (CISO, 2023).

Confianza digital: Es la percepción de los usuarios, clientes y socios sobre la capacidad de una organización para proteger sus datos y operar de manera segura en el entorno digital (PwC, 2024).

Transformación digital segura: Integración de tecnologías digitales en los procesos empresariales de manera que se priorice la protección de los datos, sistemas e infraestructura crítica (PwC, 2024).

Seguridad en la nube: Conjunto de estrategias y tecnologías utilizadas para proteger datos, aplicaciones y servicios alojados en entornos de computación en la nube (PwC, 2024).

Protección de infraestructura crítica: Implementación de medidas de seguridad específicas para garantizar la integridad y disponibilidad de los activos esenciales para el funcionamiento económico y social (MinTIC, 2024).

Continuidad del negocio: Conjunto de estrategias y procedimientos que aseguran que una organización pueda mantener operaciones esenciales durante y después de un incidente cibernético (CCIT, 2024).

Ciberinteligencia: Proceso de recopilación, análisis y difusión de información relevante sobre amenazas, vulnerabilidades y actores maliciosos que puede ser utilizada para fortalecer las estrategias de defensa (MinTIC, 2024).

Amenaza cibernética: Evento potencial, interno o externo, que busca explotar vulnerabilidades con el objetivo de causar daño, interrupciones o pérdidas a una organización (MinTIC, 2016).

Riesgo cibernético: Probabilidad de que una amenaza explote una vulnerabilidad en los activos de información de una organización, generando un impacto negativo en sus operaciones o reputación (PwC, 2024).

Phishing: Técnica utilizada para engañar a los usuarios y obtener información confidencial mediante correos electrónicos o sitios web falsos (MinTIC, 2016).

Ransomware: Tipo de programa maligno que cifra los archivos de un sistema víctima, exigiendo un rescate económico a cambio de la clave de descifrado (KPMG, 2024).

Malware: Programas maliciosos diseñados para infiltrarse, dañar o robar información de sistemas informáticos (MinTIC, 2016).

Amenaza interna: Riesgo asociado a empleados o exempleados que, intencional o accidentalmente, comprometen la seguridad de los sistemas de información (MinTIC, 2016).

Vulnerabilidad: Debilidad o falla en un sistema de información que puede ser explotada por una amenaza para comprometer la seguridad de la organización (MinTIC, 2016).

Gestión de incidentes de ciberseguridad: Proceso sistemático de preparación, detección, análisis, contención, erradicación, recuperación y aprendizaje frente a eventos que comprometen la seguridad de los sistemas de información (MinTIC, 2024).

Análisis de vulnerabilidades: Proceso de evaluación de los sistemas de información para identificar debilidades que puedan ser explotadas por amenazas cibernéticas (CCIT, 2024).

Cumplimiento normativo (Compliance): Adopción y aplicación de leyes, regulaciones y estándares internacionales que establecen requisitos mínimos de protección de la información (CCIT, 2024).

Protección de datos personales: Conjunto de medidas destinadas a garantizar la privacidad, seguridad y uso adecuado de la información personal almacenada o procesada por organizaciones (MinTIC, 2024).

Fraude económico: Acto deliberado cometido para obtener un beneficio indebido o evitar obligaciones financieras a través del engaño o manipulación (PwC, 2024).

Corrupción: Uso indebido del poder confiado para obtener beneficios privados, incluyendo prácticas como el soborno, malversación y tráfico de influencias (PwC, 2023).

Delitos cibernéticos: Actividades criminales llevadas a cabo mediante el uso de tecnologías digitales, incluyendo hackeos, phishing, ransomware y violaciones de datos (PNC, 2025).

Riesgos de trabajo forzoso en la cadena de suministro: Amenaza de que las operaciones de una organización estén vinculadas a prácticas laborales coercitivas o inhumanas en su red de proveedores (PwC, 2024).

Concientización sobre riesgos de fraude: Programas internos diseñados para sensibilizar a los empleados sobre los riesgos de fraude y promover prácticas éticas de conducta (CCIT, 2024).

Tecnologías de monitoreo antifraude: Herramientas digitales utilizadas para detectar anomalías, prevenir actividades fraudulentas y fortalecer los controles internos (PwC, 2024).

Marco Teórico

La ciberseguridad se ha convertido en una prioridad importante para las empresas, no solo dentro de las áreas técnicas, sino también en el nivel estratégico de las organizaciones. El informe *Brecha de Competencias en ciberseguridad 2024* (Fortinet, 2024), destaca que la falta de profesionales calificados en ciberseguridad representa una de las amenazas más críticas a nivel global. Esta carencia de talento incrementa la probabilidad de ataques exitosos, eleva los costos asociados a los incidentes y extiende considerablemente los tiempos de recuperación. En este entorno, las organizaciones reconocen que ya no es viable dejar la ciberseguridad solo en el área tecnológica; sin embargo, se requiere un compromiso activo de las juntas directivas.

El informe enfatiza que la seguridad debe ser vista como una parte fundamental de la estrategia empresarial, donde las políticas y decisiones de alto nivel tengan en cuenta los riesgos digitales de manera explícita. De igual forma, la obtención de certificaciones en ciberseguridad se presenta como una herramienta clave para cerrar la brecha de habilidades, mejorando la confiabilidad y adaptabilidad de los profesionales (Fortinet, 2024).

Además de este análisis sobre la necesidad de fortalecer las capacidades internas de ciberseguridad, surge la reflexión sobre las normas necesarias para la protección digital a nivel nacional. En ese sentido, el artículo *¿Necesita Colombia una Agencia Nacional de Seguridad Digital?* (IMPACTOTIC, 2023), aborda la importancia de crear una entidad especializada que coordine la ciberseguridad del Estado colombiano. Aunque la propuesta no fue inicialmente aprobada en el *Plan Nacional de Desarrollo 2022-2026* (DNP, 2022), el debate sigue abierto debido a la creciente exposición del país frente a ciber amenazas de gran escala.

La Agencia Nacional de Seguridad Digital, según el artículo, tendría el objetivo de coordinar esfuerzos entre el sector público y privado, mejorar la capacidad de recuperación de

las infraestructuras y promover estándares de protección en todo el ecosistema digital colombiano. Para su estructuración, el Gobierno Nacional ha establecido alianzas estratégicas con empresas tecnológicas globales como Amazon Web Services, Cisco, Crowdstrike, Google y Palo Alto Networks, demostrando así un enfoque de cooperación internacional enfocado en mejorar las capacidades locales. De este modo, tanto el fortalecimiento de las competencias individuales en las organizaciones como la construcción de un marco institucional robusto a nivel estatal son pilares fundamentales para enfrentar las amenazas cibernéticas contemporáneas (IMPACTOTIC, 2023).

En paralelo al fortalecimiento de capacidades técnicas y gubernamentales, resulta esencial incorporar mecanismos de control que aseguren la eficacia de los sistemas tecnológicos y la adecuada gestión de riesgos. El documento *Informe de gestión 2023* (MinTIC, 2024) enfatiza que la auditoría de tecnologías de la información constituye una herramienta indispensable para garantizar que los sistemas digitales respalden los objetivos estratégicos de las organizaciones y que los riesgos inherentes sean gestionados de manera adecuada.

El crecimiento acelerado en el uso de tecnologías de la información ha expuesto a las organizaciones a una variedad de amenazas, incluyendo riesgos cibernéticos, fraudes tecnológicos y errores operativos. Frente a este escenario, se hace indispensable contar con procesos de auditoría especializados que permitan identificar vulnerabilidades en los controles internos, evaluar la efectividad de la seguridad informática y proteger la integridad, disponibilidad y confidencialidad de los datos. Para llevar a cabo una auditoría efectiva, destaca la importancia de utilizar marcos de referencia reconocidos internacionalmente, como COBIT (Control Objectives for Information and Related Technologies) y COSO (Committee of Sponsoring Organizations of the Treadway Commission). Estos estándares ofrecen guías

estructuradas para la gobernanza de TI y la administración de riesgos, orientadas hacia la alineación estratégica, la optimización de recursos y la generación de valor sostenible (MinTIC, 2024).

En estrecha relación con lo anterior, subraya la necesidad de integrar la gestión de riesgos de TI con la estrategia organizacional global, identificando los riesgos tecnológicos importantes, evaluando su impacto y probabilidad, y estableciendo planes de tratamiento adecuados para mantener la exposición a niveles aceptables. La resiliencia tecnológica, concebida como la capacidad de las organizaciones para adaptarse y recuperarse de incidentes disruptivos, convertirse en un aspecto clave para la continuidad del negocio. Complementariamente, el rol de los auditores de TI cobra especial relevancia. No basta con detectar fallas; los auditores deben actuar como facilitadores de mejora continua, apoyándose en un conocimiento técnico profundo, habilidades analíticas y una comprensión integral de los procesos de negocio. De esta forma, la auditoría de TI se convierte en un pilar fundamental para fortalecer la seguridad organizacional en un entorno cada vez más digitalizado y amenazante (MinTIC, 2024)

Siguiendo con el análisis del panorama de ciberseguridad en Colombia, resulta fundamental examinar el comportamiento del delito informático en el país, el cual ha mostrado una tendencia creciente en los últimos años. En este sentido, el *Balance anual 2024* (PNC, 2025), ofrece un diagnóstico integral sobre la evolución de las amenazas digitales.

Según el informe, durante 2024 se registró un incremento del 23% en las denuncias de delitos cibernéticos en comparación con 2023, consolidando una tendencia de crecimiento sostenido en este tipo de delitos. Las modalidades más reportadas incluyen el hurto por medios informáticos, el acceso abusivo a sistemas, la violación de datos personales y la suplantación de sitios web. Las ciudades de Bogotá, Medellín, Cali, Barranquilla, Ibagué y Cartagena concentran

el 53% de las denuncias, evidenciando la necesidad urgente de fortalecer las capacidades de prevención y respuesta en estos centros urbanos estratégicos. Además de los métodos tradicionales, el informe destaca la aparición de amenazas emergentes como el uso de tecnologías de inteligencia artificial para la creación de deepfakes y deep voice, herramientas empleadas por ciberdelincuentes para suplantar identidades y perpetrar fraudes cada vez más sofisticados. Estos fenómenos representan desafíos adicionales para las autoridades y para la ciudadanía, dado que elevan el nivel de complejidad de las amenazas (PNC, 2025).

A nivel operativo, el informe resalta la desarticulación de redes criminales transnacionales a través de operaciones como: “CriptoEspaña-CanMoney”, “Iserver”, “Reserve”, “Los Criptocitas” y “Hacker Remoto”. Dichas acciones permitieron neutralizar actividades delictivas vinculadas al fraude financiero, acceso abusivo a sistemas, tráfico de datos y distribución de malware (PNC, 2025).

Un componente adicional de gran valor es la actividad del CAI Virtual, que en 2024 gestionó más de 54.098 incidentes mediante atención a correos electrónicos, chats de WhatsApp, llamadas telefónicas y reportes vía web. Esta plataforma ha consolidado su papel como herramienta clave de atención, orientación y prevención en el ecosistema digital colombiano. Así, el panorama nacional de ciberseguridad no solo exige fortalecer las capacidades internas de las organizaciones y consolidar marcos regulatorios adecuados, sino también desarrollar mecanismos de cooperación interinstitucional que permitan anticiparse, responder y mitigar de manera efectiva el impacto de los delitos cibernéticos en la sociedad (PNC, 2025).

Profundizando en la necesidad de gestionar adecuadamente los riesgos asociados a la ciberseguridad, resulta relevante considerar no solo su identificación cualitativa, sino también su medición en términos económicos. En este Marco, el estudio Benchmark de ciber riesgo

cuantificado en Colombia 2024 (KPMG, 2024), proporciona un análisis detallado sobre la importancia de medir los riesgos cibernéticos como herramienta estratégica para la toma de decisiones en las organizaciones. El estudio sostiene que la cuantificación del riesgo permite traducir las amenazas tecnológicas en impactos económicos comprensibles para los líderes empresariales, facilitando una mejor asignación de recursos de protección y optimizando la gestión general de riesgos. Para ello, se utilizan modelos de simulación, como la metodología de Montecarlo, que permiten estimar escenarios de pérdidas financieras derivadas de distintos tipos de incidentes cibernéticos (KPMG, 2024).

La capacidad de dimensionar no solo la probabilidad de ocurrencia de eventos críticos, sino también su impacto económico potencial, se vuelve clave para establecer prioridades en las inversiones de ciberseguridad. De acuerdo con el informe, existe una correlación directa entre la madurez de los programas de ciberseguridad y la reducción efectiva de riesgos materiales: organizaciones que adoptan buenas prácticas en gobernanza de seguridad, gestión de vulnerabilidades, respuesta a incidentes y monitoreo continuo tienden a experimentar menores impactos económicos tras un ciberataque (KPMG, 2024).

Entre las principales amenazas identificadas se encuentran el ransomware, los ataques a aplicaciones web y las brechas de seguridad en proveedores de terceros, vectores de ataque que representan un riesgo significativo para sectores estratégicos como el financiero, el de la salud, el energético y el de servicios públicos. En el contexto colombiano, el estudio estima que el impacto promedio anual del riesgo cibernético ronda los 10.000 millones para organizaciones medianas y grandes, dependiendo de su nivel de exposición y madurez en ciberseguridad. Esta cifra pone en claro la necesidad de integrar plenamente la gestión de riesgos digitales dentro del gobierno corporativo y los sistemas de gestión de riesgos empresariales, consolidando así una

postura de ciber resiliencia que permita enfrentar los desafíos de un entorno tecnológico cada vez más incierto (KPMG, 2024).

Complementando el panorama sobre la gestión de amenazas digitales en el país, el articulo Ciberseguridad en Colombia: Estrategias y Desafíos Actuales publicado por (IMPACTOTIC, 2025), ofrece una visión actualizada acerca de los riesgos, vulnerabilidades y respuestas implementadas tanto por el sector público como por el privado.

Durante 2024, Colombia registró aproximadamente 36.000 millones de intentos de ciberataques, posicionándose como el cuarto país más afectado de América Latina. Las amenazas más frecuentes incluyeron el phishing, el ransomware, el malware y los ataques a infraestructura crítica, impulsados por una creciente sofisticación de los cibercriminales y la expansión acelerada de la digitalización.

Dentro de las principales debilidades detectadas, el informe señala la débil gestión de contraseñas, la falta de protección de dispositivos finales (endpoints) y la exposición de datos sensibles, factores que evidencian la necesidad urgente de fortalecer la ciberseguridad mediante educación continua, mejores prácticas tecnológicas y políticas públicas efectivas.

En respuesta a este escenario, el Gobierno colombiano ha impulsado iniciativas estratégicas, entre ellas la propuesta de creación de la Agencia Nacional de Seguridad Digital y el impulso del CONPES 3995, orientado a construir una infraestructura digital resiliente. De igual forma se destacan proyectos como el establecimiento del Centro de Operaciones de Seguridad Nacional (SOC) y la campaña (En TIC Confío), que busca promover una cultura de protección digital en la ciudadanía.

Por parte del sector privado, se evidencia un creciente compromiso en materia de protección de datos: el 92% de las organizaciones colombianas aumentó su inversión en

ciberseguridad durante 2023, en especial frente a amenazas como el ransomware y el spear phishing. Esta tendencia refleja una mayor conciencia empresarial sobre la importancia de proteger los activos digitales críticos y construir ecosistemas de negocio más seguros. Así, la interacción entre esfuerzos públicos y privados se convierte en un componente esencial para fortalecer la postura de seguridad del país y enfrentar de manera efectiva los desafíos de un entorno cibernético cada vez más dinámico y complejo.

En línea con los retos anteriormente expuestos, el documento *Conozca los principales desafíos de seguridad digital que tiene Colombia para el 2024*, (CCCE, 2024), analiza el escenario de amenazas emergentes y plantea estrategias para fortalecer la protección digital en el país.

El informe destaca que en 2023 Colombia fue víctima de un ciberataque masivo que afectó a más de 20 entidades públicas y 78 privadas, evidenciando no solo un aumento en la frecuencia de los ataques, sino también en su nivel de sofisticación. Estas acciones delictivas, dirigidas en gran medida hacia entidades públicas debido a la sensibilidad de la información que gestionan, pusieron de manifiesto la necesidad urgente de modernizar y robustecer los sistemas de defensa cibernética.

Entre las medidas adoptadas para mejorar la postura de seguridad digital, se resalta la creación de la Dirección de Ciberseguridad dentro del Ministerio de Tecnologías de la Información y las Comunicaciones. Esta nueva instancia tiene como misión formular políticas públicas, ejecutar proyectos de protección digital y promover la cooperación internacional en materia de ciberseguridad. Además, identifica que tanto los atacantes como las organizaciones están utilizando tecnologías de Inteligencia Artificial (IA) y Machine Learning. Mientras que los ciberdelincuentes emplean estas herramientas para automatizar vulnerabilidades y mejorar sus

técnicas de ataque, las empresas las adoptan para fortalecer sus capacidades de detección, prevención y respuesta ante incidentes (CCCE, 2024).

En cuanto a las recomendaciones estratégicas, el informe sugiere:

- Fortalecer los sistemas de protección implementando tecnologías avanzadas como firewalls, antivirus, inteligencia artificial y soluciones contra malware.
- Capacitar continuamente al personal para prevenir errores humanos, reconocidos como una de las principales fuentes de incidentes.
- Fomentar la colaboración interinstitucional para compartir información y mejores prácticas en seguridad.
- Promover la educación en ciberseguridad en toda la sociedad, generando conciencia sobre las amenazas y las buenas prácticas de protección digital.

Es importante destacar la importancia de la certificación digital como un mecanismo clave para proteger la información sensible, recomendándose el uso de certificados SSL y otras herramientas que garanticen la integridad y la confidencialidad de los datos.

La necesidad de integrar la seguridad digital como parte esencial del crecimiento empresarial también es abordada en el informe *Global digital trust insights 2024 de PwC Colombia* (PwC, 2024). A través de una encuesta aplicada a altos ejecutivos de diversas industrias, el estudio analiza los riesgos prioritarios, las amenazas emergentes, las inversiones en ciberseguridad y el impacto de nuevas tecnologías como la nube y la inteligencia artificial generativa.

Uno de los principales hallazgos destaca que los costos y la frecuencia de las brechas de seguridad continúan en aumento. Particularmente en Colombia, los ataques a infraestructuras en la nube, las campañas de phishing y las amenazas dirigidas a dispositivos conectados figuran

entre las principales preocupaciones de los líderes empresariales. No obstante, solo una parte de las organizaciones cuenta con planes de gestión de riesgos en la nube estructurados y actualizados, lo que deja una ventana de exposición considerable. En respuesta a esta situación, el informe subraya la necesidad de simplificar los entornos tecnológicos como una estrategia para mejorar la postura de seguridad. La consolidación de soluciones y la modernización de infraestructuras son identificadas como prácticas clave para reducir vulnerabilidades, eliminar redundancias y aumentar la eficiencia operativa. De igual manera, se advierte que la sobreabundancia de herramientas de ciberseguridad no integradas puede, paradójicamente, aumentar los riesgos en lugar de mitigarlos (PwC, 2024).

Respecto al uso de la inteligencia artificial generativa, revela un creciente interés por parte de las organizaciones en aprovechar estas tecnologías para mejorar las capacidades defensivas. Sin embargo, también alerta sobre los nuevos riesgos asociados, haciendo énfasis en la importancia de establecer políticas de gobernanza sólidas antes de su adopción masiva (PwC, 2024).

Se destaca que el entorno regulatorio está evolucionando rápidamente. La armonización de las leyes de protección de datos, los informes obligatorios de incidentes de seguridad y los requisitos de resiliencia operativa se perfilan como factores críticos para el crecimiento y la competitividad futura de las empresas en un ecosistema digital cada vez más interconectado. Además de las amenazas puramente tecnológicas, la ciberseguridad empresarial debe tener un enfoque integral que incluya riesgos asociados a fraudes y delitos económicos. En esta línea, la *Encuesta global de crimen y fraude económico 2022-2023* (PwC, 2023) revela un incremento preocupante en la volatilidad del panorama de riesgos debido a presiones ambientales, geopolíticas, financieras y sociales.

La encuesta muestra que en Colombia el 56% de las organizaciones reportaron haber experimentado algún tipo de fraude, corrupción u otro delito económico en los últimos 24 meses, una cifra que supera el promedio global del 32%. A pesar de los esfuerzos por fortalecer políticas internas, ofrecer capacitación y establecer controles, las acciones de mitigación no siempre han sido suficientes para evitar incidentes (PwC, 2023).

Entre los riesgos más comunes, el estudio destaca el riesgo de conducta, el cual se materializó con una frecuencia del 86% a nivel global y del 84% en América Latina. Otros riesgos significativos incluyen el riesgo cibernético, el riesgo de plataformas y el uso indebido de información privilegiada. Estos factores evidencian la necesidad de adoptar estrategias de control y prevención mucho más robustas y adaptativas (PwC, 2023).

Un hallazgo relevante señala que las pérdidas asociadas a fraudes tienden a ser más elevadas cuando los perpetradores ocupan cargos de alto nivel, dado su acceso privilegiado a los sistemas y su capacidad para eludir los mecanismos de control. Del mismo modo se alerta sobre la creciente sofisticación de los grupos de crimen organizado, que recurren a tácticas como la falsificación documental, la destrucción de evidencia y la creación de empresas fachada para ocultar sus actividades ilícitas. Frente a este panorama, el informe recomienda fortalecer los controles antifraude tras la ocurrencia de incidentes, documentar adecuadamente los eventos, analizar las fallas sistémicas y priorizar acciones preventivas en los departamentos más vulnerables como Finanzas, Tecnología de la Información y Compras. Involucrar a todas las áreas de la organización en la gestión del riesgo de fraude se plantea como una estrategia fundamental para construir entornos empresariales más resilientes y seguros (PwC, 2023).

El análisis de la ciberseguridad no puede limitarse únicamente al contexto nacional; resulta indispensable observar las dinámicas regionales para entender los retos y oportunidades

en el entorno latinoamericano. En esta perspectiva, el documento *Estado de la ciberseguridad en Latinoamérica 2024* (ManageEngine, 2024), ofrece una visión actualizada sobre las principales amenazas, el impacto de la inteligencia artificial en la seguridad y el nivel de cumplimiento regulatorio en Colombia y otros países de la región.

De acuerdo con la investigación, el 86% de los ejecutivos encuestados considera que la inteligencia artificial será fundamental para defenderse de los ataques cibernéticos durante 2024. Sin embargo, también se reconoce que los actores maliciosos están aprovechando la IA generativa para diseñar ataques más sofisticados y difíciles de detectar.

En cuanto a las causas principales de los incidentes de ciberseguridad, el informe identifica dos factores predominantes: los errores accidentales de los empleados 68% y las acciones maliciosas de entidades externas 67%. Este hallazgo pone de relieve la importancia crítica de fortalecer los programas de capacitación en ciberseguridad, dado que el 63% de los participantes considera que los empleados sin formación representan un riesgo significativo para la organización.

Respecto a la gestión de incidentes, se observa que el 54% de las empresas colombianas han realizado reclamaciones exitosas ante sus aseguradoras de ciberseguridad en 2023. Para acceder a estas pólizas, las compañías debieron demostrar cumplimiento con regulaciones de protección de datos, políticas de control de acceso y evaluaciones periódicas de riesgos. Un aspecto adicional relevante es el aumento del estrés entre los profesionales de seguridad: el 65% reportó un incremento en sus niveles de presión laboral, atribuido principalmente al crecimiento de incidentes, la escasez de talento especializado y el escaso apoyo institucional.

En términos de cumplimiento regulatorio, el 79% de las organizaciones colombianas afirma estar en conformidad con normativas locales e internacionales de protección de datos,

reflejando avances importantes, aunque todavía persisten desafíos relacionados con la capacitación continua y el fortalecimiento de capacidades técnicas especializadas.

Profundizando en el análisis específico de la situación nacional, el *Estudio anual de ciberseguridad en Colombia 2022-2023* (CCIT, 2024), constituye una fuente clave para comprender los principales riesgos que enfrentan las organizaciones y las tendencias que moldean la evolución de la protección digital en el país. Este estudio basado en encuestas y entrevistas a líderes empresariales y expertos en tecnologías de la información revela un incremento significativo tanto en el número como en la sofisticación de los ciberataques, especialmente en sectores como los servicios financieros, la salud y la educación. Entre las amenazas más relevantes se destacan el ransomware, el phishing, el compromiso de correos electrónicos empresariales (BEC) y las vulnerabilidades en la cadena de suministro digital (CCIT, 2024).

Los impactos de estos incidentes no solo se reflejan en los costos directos de recuperación, sino también en las multas regulatorias, la pérdida de confianza de los clientes y el daño reputacional, factores que amenazan directamente la sostenibilidad organizacional. En consecuencia, el estudio enfatiza la necesidad de adoptar estrategias de ciber resiliencia que combinen prevención, detección temprana, respuesta rápida y recuperación efectiva (CCIT, 2024).

Un elemento fundamental abordado es la importancia de cumplir con los marcos regulatorios vigentes en Colombia, tales como la Ley 1581 de Protección de Datos Personales y las directrices de la Superintendencia de Industria y Comercio (SIC). El cumplimiento normativo no solo minimiza riesgos legales, sino que también fortalece la reputación y la confianza en el mercado (CCIT, 2024).

En cuanto a tendencias emergentes, el estudio destaca la creciente adopción de tecnologías como la inteligencia artificial, la automatización de respuestas a incidentes y los enfoques de Zero Trust, los cuales están siendo implementados para enfrentar amenazas cada vez más sofisticadas. Sin embargo, también se alerta sobre nuevos riesgos derivados del trabajo remoto y la hiperconectividad de dispositivos IoT, factores que amplían la superficie de exposición de las organizaciones. Además de los riesgos que enfrentan las grandes corporaciones, resulta imprescindible considerar la vulnerabilidad de las micro, pequeñas y medianas empresas (Mipymes) en el entorno digital actual. El artículo *La gestión de riesgos es para todas las empresas, no solo las gigantes* (WEF, 2023), enfatiza la importancia de que las Mipymes adopten procesos estructurados de gestión de riesgos como estrategia para fortalecer su resiliencia.

Según datos de Naciones Unidas, las Mipymes representan el 90% de todas las empresas, generan entre el 60% y el 70% del empleo mundial y contribuyen con el 50% del PIB global. A pesar de su relevancia económica, históricamente han percibido la gestión de riesgos como una práctica reservada exclusivamente para las grandes corporaciones, lo que ha incrementado su exposición a múltiples amenazas. El artículo señala que las Mipymes son vulnerables a una amplia gama de riesgos, incluyendo los financieros, operativos, geopolíticos y tecnológicos. Asumir riesgos es parte inherente del emprendimiento; sin embargo, resulta fundamental que estas organizaciones definan claramente su apetito y tolerancia al riesgo, evitando así que decisiones impulsivas comprometan su estabilidad.

Para fortalecer sus capacidades de gestión de riesgos, se recomienda que las Mipymes:

Promuevan una cultura organizacional que valore la identificación y el tratamiento proactivo de riesgos desde los niveles directivos.

Designen un responsable interno de riesgos o capaciten a un líder existente en gestión de riesgos empresariales (ERM).

Establezcan políticas y procedimientos formales que definan claramente los niveles de tolerancia al riesgo.

Realicen evaluaciones periódicas de riesgos, priorizando aquellos de mayor impacto y desarrollando estrategias de respuesta adecuadas.

Implementen sistemas de monitoreo continuo que permitan detectar cambios en el perfil de riesgo utilizando herramientas tecnológicas accesibles.

El fortalecimiento de la gestión de riesgos en las Mipymes no solo mejora su capacidad de anticipar incertidumbres, sino que también optimiza la toma de decisiones, refuerza la confianza de sus partes interesadas y aumenta su capacidad de resiliencia frente a crisis económicas o tecnológicas. De esta manera, incluso en ambientes altamente volátiles, las Mipymes pueden consolidarse como motores esenciales del desarrollo económico sostenible.

La protección de los activos de información constituye otro pilar esencial en el fortalecimiento de la ciberseguridad organizacional. En este sentido, *el Informe de gestión año 2023* (MinTIC, 2024). proporciona un marco detallado para comprender la importancia de integrar procesos de protección de datos en las operaciones de las organizaciones modernas. El texto establece que, en un entorno cada vez más digitalizado, la información debe ser considerada un activo estratégico cuya confidencialidad, integridad y disponibilidad deben resguardarse frente a amenazas tanto internas como externas. Para lograrlo, se propone abordar la gestión de la seguridad de la información de manera sistemática, siguiendo un ciclo de mejora continua, basado en el modelo Planificar-Hacer-Verificar-Actuar (PHVA), ampliamente adoptado en estándares internacionales como la ISO/IEC 27001. Este enfoque no solo implica la

implementación inicial de controles de seguridad, sino también su monitoreo constante y la realización de ajustes proactivos que permitan adaptarse a la evolución de las amenazas. En el corazón de este modelo se encuentra la gestión de riesgos, que requiere la identificación, análisis y evaluación de amenazas para priorizar esfuerzos de mitigación eficaces (MinTIC, 2024).

A su vez se enfatiza la necesidad de definir roles y responsabilidades claras dentro de la organización. La alta dirección debe asumir un compromiso visible, asignando recursos suficientes y estableciendo políticas que reflejen la importancia estratégica de la seguridad de la información. A su vez, la concientización y capacitación de todos los colaboradores se plantean como pilares fundamentales para consolidar una cultura organizacional segura (MinTIC, 2024).

Otro componente clave del sistema de gestión es la medición y evaluación periódica de su eficacia. Esto implica establecer indicadores clave de desempeño (KPIS), realizar auditorías internas regulares y llevar a cabo revisiones de la alta dirección para asegurar la alineación entre los objetivos estratégicos y las prácticas de protección de la información (MinTIC, 2024).

Complementando la visión sobre los riesgos organizacionales, la *Encuesta global de crimen y fraude económico de PwC Colombia 2024* (PwC, 2024), analiza la evolución de los delitos económicos y su impacto en las empresas a nivel mundial, con especial énfasis en las amenazas cibernéticas. Señala que el fraude sigue siendo una amenaza persistente, afectando a un 46% de las organizaciones globalmente en los últimos 24 meses. Entre los tipos de fraude más comunes se destacan el fraude cibernético, el abuso de activos y el fraude al consumidor, siendo el cibercrimen la categoría de mayor prevalencia (PwC, 2024).

Dentro de las amenazas cibernéticas más críticas identificadas se encuentran los ataques de ransomware, las violaciones de datos y las estafas de ingeniería social. Estos incidentes no solo generan pérdidas financieras considerables, sino también daños reputacionales,

interrupciones operativas y pérdida de confianza por parte de clientes y socios estratégicos. Un aspecto importante que resalta el estudio es que los perpetradores internos, aunque siguen representando un riesgo significativo, están siendo superados en frecuencia por los atacantes externos, quienes aprovechan las debilidades en las infraestructuras digitales y los errores humanos para ejecutar sus actividades ilícitas (PwC, 2024).

Frente a este escenario, las organizaciones que han adoptado estrategias de prevención basadas en el uso de análisis avanzados y tecnologías de inteligencia artificial han demostrado una mayor capacidad de detección temprana de incidentes y una mitigación más efectiva de sus impactos. El monitoreo continuo de transacciones y la identificación de patrones anómalos se consolidan como prácticas esenciales en la lucha contra el fraude económico. El informe enfatiza que aquellas organizaciones que cuentan con sólidos programas de ética, cumplimiento y canales internos de denuncia confiables presentan una incidencia significativamente menor de delitos económicos. Así mismo, proteger a los denunciantes se perfila como una estrategia crítica para fomentar una cultura de integridad y transparencia en todos los niveles de la organización (PwC, 2024).

En concordancia con la necesidad de fortalecer las capacidades de protección digital en organizaciones de todos los tamaños, la Guía para la implementación de seguridad de la información en una MIPYME" (MinTIC, 2016), destaca la importancia estratégica de resguardar los activos de información, especialmente en las pequeñas y medianas empresas. Recalca que, en el contexto colombiano, las Mipymes representan un pilar fundamental de la economía, pero también uno de los sectores más vulnerables frente a los incidentes de ciberseguridad. Diversos informes, como los de KPMG y Kaspersky, así como datos del Centro Cibernético Policial, evidencian un crecimiento constante en los ataques dirigidos a este segmento empresarial. Ante

esta realidad, la guía plantea que la seguridad de la información debe abordarse mediante políticas claras que definan objetivos, principios de actuación, alcance y roles de responsabilidad dentro de cada organización. Estas políticas no solo buscan proteger los datos sensibles, sino también fortalecer la confianza de clientes, proveedores y aliados estratégicos, consolidando así una ventaja competitiva en mercados cada vez más digitalizados.

Otro aspecto clave desarrollado es la necesidad de concientizar y capacitar a los empleados. Se enfatiza que los usuarios internos representan tanto una línea de defensa crítica como un posible factor de riesgo si no se encuentran adecuadamente sensibilizados sobre buenas prácticas de seguridad, manejo seguro de contraseñas y reconocimiento de correos electrónicos sospechosos, entre otros temas (MinTIC, 2016).

La guía también insta a las Mipymes a adoptar medidas prácticas como:

- La implementación de controles de acceso adecuados.
- La actualización constante de los sistemas.
- El respaldo periódico de la información crítica.
- La definición de procedimientos claros para la respuesta ante incidentes de seguridad.

Así, se promueve una visión integral de la seguridad de la información como un componente esencial para la sostenibilidad y el crecimiento de las pequeñas y medianas empresas en el entorno digital contemporáneo (MinTIC, 2016).

Ampliando el análisis hacia la perspectiva de los líderes de ciberseguridad en América Latina, el informe *perspectivas de ciberseguridad los lideres de la industria* (Digi Americas Alliance, 2024), ofrece un panorama integral sobre la evolución de las amenazas y las

capacidades defensivas en la región, con un énfasis particular en sectores estratégicos como el financiero.

El estudio, basado en la opinión de líderes de ciberseguridad de 195 organizaciones de diversos tamaños e industrias, evidencia un incremento sostenido en la frecuencia de los ataques cibernéticos, más del 70% de las organizaciones reportaron un aumento en comparación con el año anterior. Entre los tipos de ataques más recurrentes destacan el phishing, el ransomware, el malware, y las amenazas basadas en ingeniería social y vulnerabilidades de día cero (Digi Americas Alliance, 2024).

Respecto al nivel de inversión, el informe revela que, si bien el 65% de las organizaciones incrementaron sus presupuestos de ciberseguridad, aún existe un porcentaje considerable 59% que maneja recursos inferiores a USD 500.000, lo cual limita sus capacidades defensivas, especialmente en las organizaciones de menor tamaño (Digi Americas Alliance, 2024).

La autenticación multifactor (MFA) se identifica como una de las estrategias más efectivas para prevenir ataques. No obstante, se observa que el 30% de las organizaciones aún no implementa soluciones de MFA resistentes al phishing, reflejando un nivel bajo de madurez en su gestión de riesgos (Digi Americas Alliance, 2024).

En términos de cooperación institucional, el informe resalta un nivel moderadamente bajo de confianza en las agencias nacionales de aplicación de la ley y los CERTs. Solo el 16% de las organizaciones expresa alta confianza en estos entes, y más del 50% no participa activamente en intercambios públicos-privados de información sobre amenazas, lo que debilita los mecanismos de respuesta a incidentes a gran escala (Digi Americas Alliance, 2024).

Entre las principales recomendaciones planteadas se encuentran:

- Incrementar la cooperación regional en materia de ciberseguridad.
- Aumentar significativamente la inversión en capacidades defensivas.
- Priorizar la capacitación continua de los empleados en temas de seguridad digital.
- Implementar políticas de evaluación periódica de riesgos.
- Adoptar tecnologías de inteligencia artificial y análisis de amenazas para anticiparse a los ataques emergentes.

Estos hallazgos nos dicen la necesidad de construir ecosistemas de ciberseguridad más colaborativos, resilientes y adaptativos en América Latina para enfrentar los desafíos de un entorno digital cada vez más hostil (Digi Americas Alliance, 2024).

A nivel global, los riesgos interconectados y de rápida evolución están configurando un panorama cada vez más volátil y fragmentado. El *The global risks report 2024 19th edition* (WEF, 2024), ofrece una radiografía detallada de las amenazas más críticas que podrían afectar al planeta en horizontes de corto y mediano plazo. En su decimonovena edición, el informe destaca el impacto simultáneo de múltiples transformaciones estructurales: desde los avances en inteligencia artificial y las tensiones geopolíticas, hasta los efectos del cambio climático y la erosión de la cohesión social.

Uno de los hallazgos más relevantes es la consolidación de la inseguridad cibernética como el cuarto riesgo más probable en los próximos dos años y el sexto más severo en el horizonte de diez años. La expansión acelerada de tecnologías como la inteligencia artificial generativa ha permitido a los actores maliciosos llevar a cabo ataques más sofisticados, difíciles de detectar y con un impacto potencialmente devastador. Esta tendencia, además de amplificar la frecuencia y severidad de las amenazas, profundiza la brecha de equidad cibernética, ya que las

organizaciones con menores recursos quedan más expuestas ante ataques complejos (WEF, 2024).

El informe advierte también sobre los efectos adversos asociados a la IA: la concentración del poder tecnológico en pocas manos, el potencial para agravar conflictos armados asistidos por algoritmos, y el riesgo de una fragmentación digital a escala global. Frente a este escenario, el WEF hace un llamado urgente a fortalecer los marcos de gobernanza tecnológica internacional que aseguren un desarrollo más inclusivo y responsable de estas tecnologías emergentes.

En cuanto a los riesgos climáticos, se posicionan como los más severos a mediano y largo plazo. Los eventos meteorológicos extremos encabezan el ranking de riesgos en los próximos diez años, seguidos por los cambios críticos en los sistemas terrestres y la pérdida de biodiversidad. Esta situación exige acelerar las estrategias de adaptación climática, así como implementar mecanismos efectivos de mitigación para evitar sobrepasar los puntos de inflexión planetarios (WEF, 2024).

A pesar del panorama desafiante, el informe mantiene una visión propositiva: existe una ventana de oportunidad para construir resiliencia global. El fortalecimiento de la cooperación internacional, la inversión en capacidades de respuesta, la adopción de nuevas formas de gobernanza tecnológica y la promoción de acciones colectivas y localizadas, se presentan como rutas clave para afrontar los riesgos que amenazan la seguridad, la prosperidad y la sostenibilidad del mundo en esta década crítica (WEF, 2024).

A nivel institucional, el fortalecimiento de la gestión de riesgos de seguridad de la información también se refleja en iniciativas implementadas dentro del sector público colombiano. El *Informe de riesgos de seguridad de la información tercer cuatrimestre 2024*

(SuperTransporte, 2024), presenta un análisis detallado sobre los principales riesgos identificados y las medidas adoptadas para su mitigación. Se estructura conforme a la Política de Administración de Riesgos, el Manual de Gestión de Riesgos de Seguridad y el Modelo de Seguridad y Privacidad de la Información adoptados por la entidad. A través de un proceso sistemático de identificación, análisis, tratamiento y monitoreo, se abordan amenazas que afectan la disponibilidad, integridad y confidencialidad de los activos de información.

Entre los riesgos más relevantes destacan:

- La pérdida de disponibilidad de datos por fallas en las copias de seguridad.
- Las afectaciones a la infraestructura tecnológica crítica causadas por desastres naturales o daños físicos.
- La materialización de incidentes de ciberseguridad.

Para mitigar estos riesgos, la Superintendencia implementó diversos controles, tales como la verificación periódica de licencias y planes de respaldo, el análisis de vulnerabilidades, la ejecución de re-test de plataformas y el fortalecimiento de la infraestructura tecnológica mediante la contratación de servicios especializados (SuperTransporte, 2024).

Según el estudio un logro importante: durante el tercer cuatrimestre de 2024 no se reportaron materializaciones de riesgos, lo cual evidencia la efectividad de las medidas de control implementadas. Igualmente se resalta el uso de herramientas avanzadas de monitoreo de red, la implementación de mecanismos de autenticación multifactorial, la actualización constante de las políticas de seguridad y la realización periódica de campañas de sensibilización para fomentar una cultura organizacional segura (SuperTransporte, 2024).

Es importante destacar la colaboración con entidades externas como CSIRT Colombia y COLCERT, la cual ha permitido fortalecer los procesos de detección y mitigación de amenazas

mediante análisis especializados de vulnerabilidades y el intercambio de conocimientos técnicos avanzados (SuperTransporte, 2024).

En el ámbito de la administración pública, el fortalecimiento de la gestión de riesgos de seguridad de la información ha sido impulsado mediante lineamientos normativos y estratégicos. Los *Lineamientos del modelo nacional de gestión de riesgo de seguridad de la información en entidades públicas* (MinTIC, 2025), constituye el marco de referencia para la implementación de procesos efectivos de identificación, análisis, valoración, tratamiento y monitoreo de riesgos en las entidades gubernamentales. Este modelo se basa en principios de proporcionalidad, responsabilidad, efectividad, prevención, mejora continua y coordinación interinstitucional, buscando que cada entidad adopte mecanismos de protección de acuerdo con su nivel de exposición y su misión estratégica. De esta manera, se promueve una gestión del riesgo alineada a las características particulares de cada organización pública, evitando enfoques generalizados que puedan resultar ineficaces.

El modelo establece fases claras para su implementación:

- Identificación de activos de información críticos.
- Análisis de amenazas y vulnerabilidades asociadas.
- Valoración de riesgos mediante criterios de impacto y probabilidad.
- Definición de tratamientos apropiados para cada riesgo identificado.
- Seguimiento y monitoreo continuo del perfil de riesgo.

De igual manera se promueve la adopción de controles técnicos, administrativos y físicos basados en buenas prácticas internacionales como las normas ISO/IEC 27001 e ISO/IEC 27005. El uso de estos estándares mejora la compatibilidad de los sistemas de gestión, mejora la eficiencia en la asignación de recursos de protección y fortalece la resiliencia de las entidades

frente a ciber amenazas. Una característica destacada del modelo es su énfasis en la cultura organizacional: se reconoce que la seguridad de la información no depende exclusivamente de las tecnologías implementadas, sino de la conciencia, el compromiso y las acciones de todos los servidores públicos. Por ello, se insta a las entidades a desarrollar programas de sensibilización y formación continua en gestión de riesgos y buenas prácticas de seguridad (MinTIC, 2025).

En síntesis, el Modelo Nacional representa una herramienta clave para elevar los niveles de madurez en ciberseguridad del sector público colombiano, contribuyendo al cumplimiento de principios constitucionales de eficiencia, transparencia y protección de derechos fundamentales en el entorno digital (MinTIC, 2025).

Un componente esencial para el fortalecimiento de la ciberseguridad en Colombia es el marco normativo que regula la protección de los activos de información y establece obligaciones para las entidades públicas y privadas. La legislación nacional ha evolucionado significativamente en los últimos años, buscando adaptarse a los nuevos desafíos del entorno digital (MinTIC, 2025).

Marco legal

Dentro de las principales normativas se destacan:

- Ley 1273 de 2009, que tipifica los delitos informáticos y establece mecanismos de protección de la información y los datos personales. Esta ley incorporó nuevos tipos penales como el acceso abusivo a sistemas informáticos, la interceptación de datos informáticos, el daño informático y el uso de software malicioso (Congreso de Colombia, 2009).
- Ley estatutaria 1581 de 2012, que establece disposiciones generales para la protección de datos personales. A través de esta normativa, se reconocen los derechos de los titulares de la información y se crean obligaciones específicas para los responsables y encargados del tratamiento de datos (Congreso de Colombia, 2012).
- Decreto 1377 de 2013, que reglamenta parcialmente la Ley 1581, especialmente en aspectos relacionados con la autorización para el tratamiento de datos recolectados antes de la expedición de la ley (Presidencia de la República, 2013).
- CONPES 3701 de 2011, que define la política nacional de seguridad digital, estableciendo estrategias para mejorar la ciberseguridad y promover una cultura de prevención frente a las amenazas digitales (DNP, 2011).
- Política Pública de Confianza y Seguridad Digital, actualizada mediante el CONPES 3995 de 2020, que busca fortalecer la resiliencia del ecosistema digital colombiano a través de la cooperación público-privada, el desarrollo de capacidades técnicas, la protección de infraestructuras críticas y la promoción de la confianza ciudadana en el entorno digital (DNP, 2020).

- La Política Nacional de Ciencia, Tecnología e Innovación, actualizada mediante el CONPES 4145 de 2025, incorpora como eje estratégico el fortalecimiento de la seguridad digital y la inteligencia artificial, buscando aumentar la inversión en I+D, cerrar brechas en capacidades técnicas, promover la resiliencia del ecosistema digital y garantizar la protección de los derechos ciudadanos en el entorno virtual (DNP, 2025).
- Resolución 500 de 2021, que adopta el Modelo de Gestión de Riesgos de Seguridad de la Información en entidades públicas, estructurando procesos sistemáticos para la protección de activos digitales (MinTIC, 2021).

Aparte de estas normas, Colombia cuenta con iniciativas como el *Plan de acción 2025* (MinTIC, 2025) que orienta acciones prioritarias para mitigar riesgos cibernéticos y fortalecer la respuesta a incidentes a nivel nacional. El marco normativo colombiano en materia de ciberseguridad no solo busca proteger los derechos fundamentales de los ciudadanos en el entorno digital, sino también garantizar la integridad de las infraestructuras críticas, fomentar la confianza en el ecosistema digital y posicionar al país como un actor comprometido con la seguridad cibernética a nivel internacional.

En conclusión, la revisión bibliográfica de diferentes informes, estudios y lineamientos normativos y evidencias de la ciberseguridad permitirá realizar un análisis de las amenazas que enfrentan las empresas de Colombia.

Metodología

La presente monografía utiliza un enfoque mixto, en el que combina componentes cualitativos y cuantitativos dentro de un diseño descriptivo y documental, con el fin de caracterizar y analizar las principales amenazas cibernéticas que enfrentaron las empresas colombianas durante el periodo 2022-2024, a partir del estudio sistemático de fuentes oficiales. Esta estrategia metodológica responde a la necesidad de comprender un fenómeno complejo desde una doble perspectiva: por un lado, a través de la interpretación contextual de las modalidades delictivas y sus implicaciones organizacionales (enfoque cualitativo); y por otro, mediante la comparación numérica y evolutiva de los datos reportados en los informes técnicos (enfoque cuantitativo).

La elección de este enfoque se debe a la naturaleza del objeto de estudio. El cibercrimen, como fenómeno dinámico y en constante evolución, es abordado desde una mirada integral que permite comprender tanto las cifras duras que evidencian su crecimiento como las lógicas sociales y organizacionales que explican su consolidación. Desde esta perspectiva, el uso de fuentes secundarias no representa una limitación, sino una oportunidad para construir una visión panorámica, fundamentada en evidencia previamente procesada por entidades especializadas.

En este sentido, el enfoque cualitativo permite explorar con profundidad los significados, patrones y estructuras subyacentes en los textos revisados, mientras que el enfoque cuantitativo aporta herramientas para establecer comparaciones entre años, visualizar tendencias y generar indicadores claves sobre la evolución del cibercrimen. La complementariedad entre ambos enfoques fortalece la validez del estudio y genera una base más sólida para la formulación de recomendaciones estratégicas.

Proceso De Recolección Documental

La fase de recolección de información se desarrolló bajo una lógica sistemática y rigurosa. Se establecieron criterios de inclusión y exclusión para garantizar la pertinencia, calidad y confiabilidad de las fuentes analizadas. Los principales criterios de selección fueron: actualidad (documentos publicados entre 2016 y 2025); enfoque temático (relación directa con amenazas cibernéticas en Colombia); respaldo institucional (emisión por entidades reconocidas a nivel nacional o internacional); y cobertura sectorial (impacto en empresas de distintos tamaños y sectores económicos).

La búsqueda de documentos se realizó a través de plataformas oficiales del Gobierno Nacional, sitios web de entidades oficiales, y repositorios de estudios técnicos. A cada documento seleccionado se le asignó una ficha de registro, donde se sistematizó información relevante como el año de publicación, la entidad emisora, la estructura temática, el tipo de datos contenidos, los hallazgos principales y las citas más relevantes.

Estos informes constituyen una fuente confiable y proveen una base sólida al estudio, ya que reúnen datos consolidados sobre la evolución de los delitos informáticos en Colombia, ya que reportan estadísticas oficiales sobre denuncias y capturas y documentan las principales respuestas institucionales frente a los ciberataques. Adicionalmente, se consultaron fuentes complementarias como informes de gestión, reportes de consultoras internacionales, artículos especializados y documentos normativos, que aportaron contexto y profundidad al análisis.

Procedimiento De Revisión

La revisión de los documentos se desarrolló en tres fases sucesivas que garantizaron un análisis detallado y estructurado:

Fase exploratoria: se realizó una lectura preliminar de cada documento, identificando su estructura general, ejes temáticos, tipo de datos presentados y metodología de elaboración. Esta etapa permitió filtrar los documentos más pertinentes y organizar el cuerpo documental según año y entidad emisora.

Fase analítica: se diseñó una matriz documental con categorías previamente definidas: tipos de amenazas cibernéticas, sectores empresariales afectados, cifras de denuncias, modalidades delictivas, mecanismos de prevención y reacción, y acciones institucionales. Esta matriz facilitó la organización de la información de forma sistemática, permitiendo el desarrollo de comparaciones interanuales y el reconocimiento de patrones de comportamiento delictivo.

Fase interpretativa: a partir de los datos sistematizados, se realizó una lectura crítica y contextualizada, identificando relaciones entre fenómenos, explicaciones plausibles sobre la evolución de ciertas amenazas, y vínculos entre las cifras y las decisiones institucionales adoptadas. Esta fase permitió construir una narrativa analítica coherente y argumentada, alineada con los objetivos de la investigación.

Durante todo el proceso se utilizaron herramientas auxiliares como esquemas de contenido, cronologías, diagramas comparativos y tablas resumen. Esto permitió visualizar con mayor facilidad las trayectorias del cibercrimen en Colombia, sus fluctuaciones por año y las acciones más relevantes emprendidas en respuesta a los riesgos identificados.

Técnica de Análisis

Análisis Cuantitativo Descriptivo

Se extrajeron y organizaron cifras relevantes sobre el comportamiento del cibercrimen, tales como: número total de denuncias, tipos de delitos más reportados, volumen de capturas realizadas por las autoridades, cantidad de operaciones articuladas y evolución interanual de los incidentes. Estas cifras fueron organizadas en tablas y gráficos para facilitar su visualización y se utilizaron como base para identificar tendencias, picos de actividad y posibles correlaciones temporales o sectoriales.

Análisis Cualitativo Temático

Se estructuró la información en torno a ejes analíticos que permitieron profundizar en el sentido de los datos. Los cuatro ejes centrales definidos fueron: (1) tipologías delictivas (suplantación de identidad, phishing, ransomware, entre otros); (2) sectores económicos más afectados (financiero, salud, educación, Mipymes); (3) patrones temporales de actividad cibercriminal (meses críticos, eventos desencadenantes, variaciones interanuales); y (4) respuestas institucionales (programas de prevención, campañas de concientización, estrategias policiales, cooperación internacional).

Ambas técnicas fueron integradas y aplicadas de manera complementaria. Mientras el análisis cuantitativo permitió dimensionar el fenómeno en términos numéricos, el análisis cualitativo ofreció una comprensión más amplia sobre los factores que subyacen a esas cifras, sus implicaciones y los desafíos que representan para las empresas y las autoridades. Esta articulación metodológica enriqueció la investigación y posibilitó el desarrollo de conclusiones fundamentadas y pertinentes para el contexto colombiano actual.

Exploración Documental de las Amenazas Cibernéticas en Colombia: Evolución y Respuesta (2022-2024)

Tipologías Delictivas Predominantes

El análisis de las tipologías delictivas en Colombia entre el 2022 y 2024 evidenció un panorama en transformación constante. A lo largo de estos tres años, el cibercrimen no solo amplió su alcance, sino que también diversificó sus métodos, consolidó nuevas modalidades y penetró sectores económicos críticos con técnicas cada vez más sofisticadas. Los documentos oficiales de la Policial Nacional, El Centro cibernético policial y el estudio anual de ciberseguridad 2022-2023 ofrecieron evidencia clara sobre el crecimiento de amenazas digitales, basadas tanto en datos cuantitativos como en el análisis cualitativo de casos y operaciones.

Año 2022: Consolidación de los Delitos Clásicos Digitales

En 2022, Colombia registró un total de 65.794 denuncias por delitos informáticos, con un incremento del 21,6% respecto al año anterior. Este crecimiento reflejó tanto una mayor actividad criminal en entornos digitales como una mejora en los mecanismos de denuncia y visibilidad del fenómeno.

Las tipologías delictivas más reportadas fueron:

- Hurto por medios informáticos: 26.366 casos
- Acceso abusivo a sistemas informáticos: 13.081 casos
- Violación de datos personales: 13.588 casos
- Suplantación de sitios web y redes sociales: 5.751 casos
- Transferencia no consentida de activos: 3.578 casos
- Intercepción de datos informáticos: 1.989 casos

La suplantación de identidad y la violación de datos personales marcaron una fuerte incidencia sobre usuarios comunes, con casos repetidos de robo de credenciales a través de plataformas como WhatsApp, Instagram y sitios de comercio electrónico. El uso de phishing tradicional fue recurrente, mediante enlaces engañosos enviados a través de redes sociales o mensajes SMS, con objetivo de obtener acceso a cuentas bancarias o plataformas institucionales.

Año 2023: Diversificación Operativa y Aumento de Fraudes por Suplantación

Durante 2023, las denuncias por cibercrimen bajaron ligeramente a 59.033 casos, lo que representó una disminución del 10% respecto al año anterior. Sin embargo, esta reducción no significó una menor actividad delictiva, sino una mutación en las estrategias empleadas y una concentración en delitos de mayor impacto económico.

El hurto por medios informáticos aumentó de 26.366 a 28.512 casos, consolidándose como la modalidad más frecuente. La suplantación de identidad se mantuvo entre los delitos más reportados, con 4.393 casos específicos de suplantación de sitios web. La violación de datos personales descendió a 9.639 casos, lo que implicó una reducción del 29% respecto a 2022.

Otros delitos destacados incluyeron:

- Hurto por medios informáticos: 28.512 casos
- Acceso abusivo a sistemas informáticos: 10.883 casos
- Violación de datos personales: 9.639 casos
- Transferencia no consentida de activos: 3.303 casos
- Intercepción de datos informáticos: 1.311 casos

En este año, los ciberdelincuentes aprovecharon con mayor frecuencia plataformas como Facebook Marketplace, WhatsApp Business y páginas web falsas que simulaban tiendas en línea. Se reportaron múltiples casos de usuarios que transferían dinero por productos que nunca eran

entregados. Este patrón afectó especialmente a las pequeñas y medianas empresas, así como a consumidores de comercio digital sin entrenamiento en ciberseguridad.

Año 2024: Emergencia de Nuevas Amenazas y Uso de Inteligencia Artificial

Las cifras de denuncias aumentaron drásticamente de 59.033 en 2023 a 77.866 en 2024. Este año se caracterizó por la aparición de nuevas formas delictivas con un componente tecnológico más sofisticado.

Las tipologías más reportadas fueron:

- Hurto por medios informáticos: 37.409 casos
- Acceso abusivo a sistemas informáticos: 16.955 casos
- Violación de datos personales: 11.954 casos
- Suplantación de sitios web: 6.209 casos
- Transferencia no consentida de activos: 3.542 casos

Uno de los fenómenos más críticos del año fue el robo de cuentas de WhatsApp, con al menos 1.487 casos reportados directamente al CAI Virtual. Este delito implicaba el acceso no autorizado a la cuenta del usuario mediante códigos de verificación engañosos y posteriormente se utilizaba la cuenta para extorsionar o cometer fraudes con sus contactos.

También se consolidó el uso de phishing dirigido, con técnicas de ingeniería social mucho más elaboradas, e incluso se comenzaron a detectar casos de deep voice y deepfake utilizados para suplantar identidades o manipular comunicaciones. Aunque los informes no ofrecieron cifras exactas sobre estos casos, sí alertaron sobre su presencia creciente y su potencial riesgo, especialmente en procesos de contratación pública, transferencias empresariales y manipulación de evidencia digital.

Tabla 1

Comparativo transversal: evolución y persistencia del delito

Tipología	2022	2023	2024
Hurto por medios informáticos	26.366	28.512	37.409
Acceso abusivo a sistemas	13.081	10.883	16.955
Violación de datos personales	13.588	9.639	11.954
Suplantación de sitios web	5.751	4.393	6.209
Transferencia no consentida	3.578	3.303	3.542
Intercepción ilícita de datos	1.989	1.311	910

Nota: Resumen comparativo por tipología de los casos reportados de cibercrimen en los balances anuales de ciberseguridad para los años 2022, 2023 y 2024 documentados por el Centro Cibernético Policial (Colombia, 2022. 2023. 2024).

La evolución de estas cifras muestra que el hurto informático creció de manera sostenida durante los años, mientras que delitos como suplantación de sitios y acceso a sistemas mostraron una leve disminución, posiblemente como efecto de campañas de prevención. Sin embargo, la aparición de modalidades como el robo de cuentas móviles y el uso de herramientas impulsadas por inteligencia artificial plantea nuevos retos de seguridad digital.

La transformación de las tipologías delictivas en Colombia entre 2022 y 2024 reveló una expansión del cibercrimen tanto en volumen como en complejidad técnica. Aunque las cifras muestran algunos descensos puntuales en ciertas modalidades, el fenómeno general se intensificó. El uso de plataformas móviles, redes sociales y tecnologías emergentes por parte de los delincuentes digitales evidenció una profesionalización creciente, que requiere respuestas más ágiles por parte de las autoridades.

El hurto por medios informáticos continuó siendo el principal delito en volumen, mientras que fenómenos como el robo de cuentas personales o la manipulación de información mediante IA abrieron nuevas dimensiones del problema. La capacidad del Estado para responder a estos desafíos dependerá no solo de la tecnología, sino también de su capacidad para formar ciudadanos informados, consolidar canales de denuncia eficaces y articular una política pública integral en ciberseguridad.

Patrones Temporales de Actividad Cibercriminal en Colombia (2022-2024)

Observar los patrones temporales del cibercrimen es fundamental para comprender la dinámica del fenómeno delictivo digital y su evolución en el tiempo. Estos patrones permiten identificar si los delitos se comportan de manera cíclica, si tienden a concentrarse en ciertos momentos del año, si responden a coyunturas tecnológicas o sociales específicas, y, sobre todo cómo han evolucionado en volumen, naturaleza y complejidad. A partir de los balances anuales de ciberseguridad 2022, 2023 y 2024 elaborados por el Centro Cibernético Policial es posible reconstruir de manera detallada el comportamiento del cibercrimen en Colombia durante estos tres años, contrastando aumentos, disminuciones y momentos críticos.

Año 2022: Crecimiento Sostenido y Alta Incidencia Urbana

El comportamiento mensual mostró picos en las temporadas de campañas políticas, bonificaciones laborales, y jornadas masivas de compras electrónicas, como el Día sin IVA y el Black Friday. Las modalidades predominantes durante estos meses fueron el phishing bancario, la suplantación en redes sociales y el hurto por medios informáticos.

A nivel geográfico, Bogotá, Medellín y Cali concentraron más del 50% de las denuncias, lo que confirmó la tendencia urbana del cibercrimen en el país. Sin embargo, el informe alertó

sobre el crecimiento sostenido de incidentes en ciudades intermedias como Bucaramanga, Ibagué, Villavicencio y Neiva.

Año 2023: Disminución Global con Fluctuaciones Sectoriales

El comportamiento mensual de 2023 fue más irregular. Se evidenció una concentración de denuncias en marzo, agosto y diciembre, asociadas a períodos de movimiento económico elevado, como pagos de impuestos, matrículas escolares y primas navideñas. En estos momentos, el cibercrimen se enfocó en plataformas gubernamentales, instituciones educativas y servicios financieros.

Se mantuvo la concentración de incidentes en grandes ciudades, pero se amplió la afectación a entornos rurales conectados, especialmente en el eje cafetero y algunas zonas de la costa Caribe. Además, comenzó a observarse un uso más extendido de troyanos bancarios y técnicas de ingeniería social más avanzadas, lo que podría explicar la disminución de las denuncias frente al aumento de daños económicos.

Año 2024: Repunte Crítico y Diversificación del Riesgo

Este año se caracterizó por una mayor sofisticación de las amenazas y una expansión transversal del cibercrimen hacia sectores críticos, como salud, educación y gobierno. Según el informe, los incidentes más reportados estuvieron relacionados con hurto por medios informáticos (37.409 casos), acceso abusivo a sistemas (16.955), y violación de datos personales (11.954).

Tabla 2

Comparativo global y evolución interanual

Año	Total de denuncias	Picos mensuales	Modalidades más activas
2022	65.794	Junio, julio, noviembre	Phishing, hurto digital, suplantación
2023	59.033	Marzo, agosto, diciembre	Troyanos, fraudes educativos, ataques a EPS
2024	77.866	Mayo, octubre, diciembre	Ransomware, robo de WhatsApp, fraude móvil

Nota: Resumen comparativo del total de denuncias y modalidades más activas destacando los picos mensuales para los años 2022, 2023 y 2024 documentados por el Centro Cibernético Policial (Colombia, 2022. 2023. 2024).

La evolución temporal mostró que el cibercrimen en Colombia no se comportó de forma lineal ni predecible. Mientras que 2022 y 2024 evidenciaron crecimiento sostenido, 2023 representó una aparente pausa que, según los expertos, pudo corresponder a la adopción de modalidades menos visibles y de mayor impacto, como los ataques a infraestructuras críticas y el uso de técnicas avanzadas de evasión digital.

El comportamiento temporal del cibercrimen entre 2022 y 2024 en Colombia mostró tres características principales: crecimiento general del volumen, mayor sofisticación tecnológica, y cambios en los momentos de mayor actividad. Las autoridades enfrentaron no solo un aumento en los incidentes, sino también una mayor dificultad para anticiparse a los ciclos delictivos, ya que los delincuentes comenzaron a adaptar sus operaciones a eventos sociales, económicos y tecnológicos específicos.

Esto exige que las estrategias de prevención y reacción no se basen únicamente en el volumen de denuncias, sino en modelos predictivos que integren datos contextuales. Las

capacidades analíticas del CAI Virtual deben ser reforzadas para detectar patrones emergentes, anticipar ataques masivos y generar alertas tempranas efectivas.

En un entorno digital cada vez más dinámico, comprender los patrones temporales no solo ayuda a visualizar el fenómeno en el tiempo, sino que constituye una herramienta clave para tomar decisiones estratégicas, proteger infraestructuras sensibles y educar a la ciudadanía de forma oportuna.

Vectores Tecnológicos y Canales de Ataque Utilizados (2022-2024)

Comprender los vectores tecnológicos y los canales de ataque empleados por los ciberdelincuentes es fundamental para dimensionar el nivel de sofisticación, adaptación y persistencia de las amenazas digitales. En el contexto colombiano, entre 2022 y 2024, se observó una evolución marcada tanto en las herramientas tecnológicas utilizadas por los agresores como en los entornos a través de los cuales ejecutaron sus ataques. El uso de tecnologías móviles, redes sociales, suplantación digital, troyanos bancarios, aplicaciones falsas y, recientemente, técnicas con inteligencia artificial, conformó un ecosistema delictivo cada vez más profesionalizado. Esta sección presenta un análisis detallado de estos vectores y canales, basados en información oficial de los balances anuales ciber del centro cibernético policial.

Principales vectores de ataque: definición y evolución

Ingeniería social

Durante los años revisados, la ingeniería social se consolidó como el eje transversal de la mayoría de los ataques. Esta técnica consistió en manipular psicológicamente a las víctimas para que entregaran voluntariamente su información personal o financiera. En 2022, esta modalidad se evidenció principalmente a través de mensajes engañosos enviados por WhatsApp y SMS. En 2023 y 2024, evolucionó hacia formatos más complejos como llamadas automatizadas, uso de

perfiles falsos en redes sociales, e incluso imitación de voz mediante inteligencia artificial, reportada por el CAI Virtual en casos de estafa digital empresarial.

Phishing

El phishing fue uno de los vectores más frecuentes durante todo el período. Según el balance anual 2024, esta modalidad representó el 11,4% del total de incidentes. En 2022 y 2023 se emplearon masivamente correos electrónicos con enlaces maliciosos que redireccionaban a portales clonados de entidades bancarias, plataformas de pago o servicios estatales. En 2024, se identificaron campañas más elaboradas de phishing dirigido (spear phishing), donde los atacantes adaptaban el contenido a la víctima con base en información obtenida de redes sociales o filtraciones previas.

Malware, troyanos y aplicaciones maliciosas

El uso de malware fue constante en los tres años. En 2022, predominaron los troyanos bancarios clásicos, distribuidos por correo o archivos adjuntos. Para 2023 y 2024, aumentó el uso de aplicaciones móviles maliciosas, muchas de las cuales imitaban plataformas legítimas como bancos, billeteras digitales o aplicaciones de envío. Estas aplicaciones eran instaladas desde enlaces enviados por mensajería o desde tiendas no oficiales. En varios casos, permitían a los delincuentes tomar control del dispositivo, registrar pulsaciones del teclado (keyloggers) o capturar códigos de autenticación.

Suplantación de identidad digital

El robo y uso indebido de identidades digitales fue uno de los fenómenos más persistentes. En 2022, se reportaron múltiples casos de cuentas falsas en redes sociales que suplantaban a empresas o funcionarios. En 2023 y 2024, este vector se expandió hacia plataformas como WhatsApp y Facebook Marketplace.

Tabla 3

Canales Digitales Usados Por los Agresores (2022-2024)

Canal	2022	2023	2024
Correo electrónico	Phishing masivo básico	Archivos adjuntos con malware	Spear phishing con personalización avanzada
WhatsApp	Mensajes con enlaces falsos	Clonación de perfiles	Robo de cuentas y estafas directas
Facebook / Instagram	Suplantación de perfiles	Fraudes por Marketplace	Venta falsa de productos y estafa organizada
SMS	Enlaces a portales falsos de bancos	Campañas masivas tipo “premios”	Robo de códigos de verificación y 2FA
Aplicaciones móviles	Mínimo uso	Primeros reportes de apps falsas	Apps clonadas de bancos y wallets
Sitios web fraudulentos	Clones de bancos y entidades públicas	Plataformas de envío / pasarelas falsas	Suplantación de portales de gobierno y salud

Nota: Resumen comparativo anual de los canales digitales usados más comúnmente por los agresores en los años 2022, 2023 y 2024 reportados por el Centro Cibernético Policial (Colombia, 2022. 2023. 2024).

Durante los años, los atacantes mantuvieron un enfoque multicanal. En 2022, los correos electrónicos fueron el principal canal, pero desde 2023 se observó una migración clara hacia canales móviles y redes sociales, especialmente WhatsApp y Facebook. El crecimiento de los

fraudes en plataformas de compraventa y el robo de cuentas personales marcó un nuevo frente de riesgo.

Tabla 4

Evolución Interanual De Herramientas y Técnicas

Año	Herramientas emergentes	Técnicas dominantes	Plataformas más usadas
2022	Troyanos bancarios	Phishing básico, ingeniería social directa	Correo electrónico, SMS
2023	Apps falsas, bots en redes	Spear phishing, acceso no autorizado	WhatsApp, Marketplace
2024	Deepfakes, IA de voz, SIM swapping	Ingeniería social avanzada, clonación de identidad	WhatsApp, portales de gobierno

Nota: Resumen comparativo de la Evaluación Interanual de las herramientas, técnicas y plataformas más usadas en los años 2022, 2023 y 2024 por cibercrimen reportados por el Centro Cibernético Policial (Colombia, 2022. 2023. 2024).

En este periodo, los vectores tecnológicos evolucionaron no solo en complejidad técnica, sino en su capacidad de adaptación. Mientras en 2022 el enfoque era técnico (troyanos, malware), para 2024 lo fue socio-tecnológico, combinando ingeniería social, suplantación de canales oficiales y manipulación digital con IA. Esta evolución hizo que muchas víctimas no pudieran identificar el engaño hasta después del daño.

El análisis de vectores tecnológicos entre 2022 y 2024 demuestra que el cibercrimen en Colombia dejó de depender exclusivamente de herramientas técnicas para pasar a integrar conocimiento psicológico, plataformas sociales y tecnologías emergentes, como la inteligencia

artificial. Esta convergencia permitió a los delincuentes escalar sus ataques con menor esfuerzo y mayor impacto.

La suplantación de canales oficiales como bancos, entidades públicas o empresas de mensajería fue cada vez más verosímil. El uso de aplicaciones móviles falsificadas, bots automatizados y clonación de identidad por voz configuró un entorno donde la víctima rara vez tenía medios para detectar el ataque a tiempo.

Este escenario plantea desafíos urgentes. El Estado necesita fortalecer el marco normativo para identificar y sancionar estas nuevas modalidades, mientras que las empresas deben revisar y reforzar sus canales de atención digital, implementar sistemas de verificación robustos y formar a su personal en reconocimiento de vectores emergentes. La ciudadanía, por su parte, debe entender que no basta con tener antivirus, sino que se requiere criterio crítico y conocimiento de los mecanismos usados por los atacantes.

Respuestas Institucionales y Operativas Frente al Cibercrimen en Colombia (2022-2024)

El cibercrimen representa uno de los desafíos más complejos para los Estados modernos, en tanto se manifiesta en un entorno altamente dinámico, transnacional y en constante evolución técnica. En Colombia, el crecimiento sostenido de los delitos informáticos entre 2022 y 2024 no solo requirió una respuesta reactiva por parte de las autoridades, sino la implementación de estrategias institucionales, planes de acción y capacidades especializadas. Este eje examina las respuestas articuladas desde el gobierno nacional, con énfasis en el rol del Centro Cibernético Policial, así como iniciativas legislativas, tecnológicas y operativas que marcaron el periodo analizado.

Estructuras y Estrategias Institucionales

Centro Cibernético Policial y CAI Virtual

La columna vertebral de la respuesta institucional frente al cibercrimen ha sido el Centro Cibernético Policial. Esta unidad concentra labores de monitoreo, atención a incidentes, ciberinteligencia y coordinación operativa con otras entidades. A su vez, el CAI Virtual ha funcionado como canal de contacto directo entre la ciudadanía y las autoridades, permitiendo la recepción de denuncias, orientación a víctimas y atención a incidentes cibernéticos en tiempo real.

PMU Ciber y Planes Operativos

A partir de 2023, se consolidó el PMU Ciber, una mesa nacional de articulación estratégica para la atención de incidentes cibernéticos de alto impacto. Esta plataforma multientidad permite activar protocolos conjuntos entre Policía, Fiscalía, Ministerio de Defensa, Ministerio TIC y otras autoridades, a fin de contener amenazas en tiempo real, especialmente aquellas que afectan infraestructura crítica.

Campañas de Prevención y Alfabetización Digital

Entre las campañas más destacadas se encuentran:

La Secretaría de Seguridad, Convivencia y Justicia, lanza la campaña #NoCaigaEnLaRed, dirigida a padres de familia, cuidadores y educadores para alertar sobre riesgos cibernéticos. Con esta campaña se busca prevenir delitos como el Grooming, el Ciberbullying y los retos virales, entre otros, a los que se enfrentan los niños, niñas y adolescentes en los entornos digitales, entre otros, especialmente en temporada de vacaciones donde tienen mucho tiempo libre para acceder a las redes sociales.

El Grooming es uno de los ciberdelitos a los que más están expuestos los jóvenes. En este caso los delincuentes tratan de acceder a los menores de edad, por medios digitales, ganándose su confianza con engaños, para conseguir imágenes o videos con contenido sexual y hasta un contacto físico para abusar de ellos (Gov.co, 2024).

El Ministerio TIC, a través del programa '1,2,3 X TIC', empodera a padres y docentes con las herramientas necesarias para guiar a las jóvenes generaciones en el mundo digital. La Institución Educativa Distrital Enrique Olaya Herrera fue el lugar del lanzamiento de esta iniciativa del manejo responsable de la tecnología a la que asistieron más 1.000 personas.

El ministro TIC, Mauricio Lizcano, invitó a los padres a estar en un constante diálogo con sus hijos, "esta campaña que estamos lanzado es muy importante, de prevención de la amenaza que tiene hoy nuestros niños. En Bogotá tenemos 195.000 denuncias por sexting, 250.000 por cyberbullying y grooming. Tenemos que prevenir que nuestros hijos sean acosados o sean acosadores, estar pendientes a los indicadores, cuando muestran señales que no quieren ir al colegio. Tener en cuenta que los niños menores de 14 años no deben tener redes sociales y los que los tengan debemos tener sus claves y saber qué están publicando" (MinTIC, 2023).

La Dirección de Tecnología, Informática y Comunicaciones lanza una campaña para sensibilizar a la comunidad Rosarista sobre los peligros que existen en el ciberespacio. Ataques cibernéticos, robo de información, spam y programas maliciosos son algunos de los temas que se pretende sensibilizar a través de tips y recomendaciones para aprender a navegar el ciberespacio.

Con el slogan “No te confíes en el ciberespacio, #RosaristaDigital” La Coordinación de Telecomunicaciones y Ciberseguridad pretende sensibilizar a la comunidad Rosarista sobre los peligros a los que se enfrentan en el ciberespacio. Los tips, recomendaciones y pistas para

identificar un posible ataque cibernético, robo de información, ‘spam’ son una de las líneas de acción ante las amenazas en la seguridad informática (Universidad del Rosario, 2024).

Desde el Centro Cibernético de la Policía Nacional, este año se han identificado y bloqueado 22.114 páginas en el país, con contenido de explotación sexual infantil en línea, evitando con ello la descarga, distribución o venta de este material.

Marco Normativo y Cooperación Internacional

Durante los años 2022, 2023 y 2024 Colombia fortaleció su marco legal mediante la ratificación del Convenio de Budapest sobre Ciberdelincuencia, y la implementación de normativas como el CONPES 3995 de 2020, la Ley 1273 de 2009, y el Marco Nacional de Referencia de Seguridad Digital. Asimismo, el país incrementó su participación en operaciones coordinadas por INTERPOL, Europol y Ameripol.

Operaciones Destacadas Por Año

2022: Alertas Preventivas y Capturas Iniciales

En este año se realizaron operativos como:

Operación “Némesis”, que permitió la desarticulación de una banda dedicada a fraudes por suplantación en redes sociales.

2023: Ofensiva Contra Aplicaciones Falsas y Robo de Identidad

Se destacan:

Captura de nueve individuos implicados en el desarrollo de aplicaciones maliciosas para acceso a datos personales (octubre 2023).

Operación “APOLO”, con resultados frente a redes criminales que suplantaban empresas legales para ejecutar fraudes laborales.

2024: Ciberinteligencia y Uso de IA Forense

Fue el año con mayores avances tecnológicos:

Activación de una nueva unidad de inteligencia artificial forense para análisis de videos deepfake y voz clonada.

Ejecución de 4.228 planes operativos de ciberseguridad, con capturas en tiempo real.

Desarrollo de 20.000 alertas automatizadas al sector financiero, mediante sistemas de monitoreo basados en inteligencia artificial.

Tabla 5

Avances logrados y desafíos persistentes

Avances alcanzados (2022-2024)	**Desafíos y brechas actuales**
Consolidación del CAI Virtual y aumento en atención a víctimas	Baja tasa de judicialización y lentitud en sentencias
Creación del PMU Ciber para incidentes críticos	Limitaciones tecnológicas en entidades territoriales
Uso de IA y OSINT en investigaciones	Débil articulación entre sector privado y fuerza pública
Campañas masivas de prevención ciudadana	Falta de cultura digital en población vulnerable
Fortalecimiento de cooperación con INTERPOL y Europol	Escasa inversión en talento humano especializado

Nota: Resumen comparativo por tipología de los casos reportados de cibercrimen en los balances anuales de ciberseguridad para los años 2022, 2023 y 2024 documentados por el Centro Cibernético Policial (Colombia, 2022. 2023. 2024).

Aunque se avanzó significativamente en capacidades institucionales, el crecimiento del cibercrimen exige un ritmo de adaptación aún mayor. Las respuestas tienden a ser reactivas,

El periodo 2022-2024 evidenció que Colombia no ha sido pasiva frente al avance del cibercrimen. Por el contrario, consolidó estructuras como el CAI Virtual y el PMU Ciber, lideró operaciones con alcance nacional e internacional, y adoptó tecnologías avanzadas como la inteligencia artificial forense. Sin embargo, el carácter dinámico y transnacional de las amenazas exige una evolución constante en las capacidades estatales. Las respuestas deben ser integrales, articuladas y adaptadas a la realidad territorial del país, considerando tanto las megaciudades como las zonas rurales conectadas. El reto no es solo de infraestructura tecnológica, sino de cultura digital, normatividad eficiente y formación permanente de talento especializado.

Impacto Del Cibercrimen En Las Empresas y La Ciudadanía Colombiana (2022-2024)

El análisis del impacto del cibercrimen en Colombia entre 2022 y 2024 permite dimensionar no solo la evolución técnica del delito, sino también sus consecuencias reales sobre el tejido económico, institucional y social del país. Las cifras crecientes de incidentes reportados, sumadas a los informes del CAI Virtual y del Centro Cibernético Policial, evidencian que las afectaciones han sido cada vez más amplias, complejas y transversales. Este eje expone los daños concretos que el cibercrimen ha generado en las empresas especialmente Mipymes y en la ciudadanía, así como los efectos en la confianza digital, el bienestar psicológico y la percepción de seguridad tecnológica.

Afectación en el sector empresarial

Mipymes: Alta Vulnerabilidad y Baja Preparación

Durante los años 2022 y 2023, las micro, pequeñas y medianas empresas se consolidaron como uno de los blancos más recurrentes del cibercrimen en Colombia, debido a su bajo nivel de

madurez en ciberseguridad. Según el *Estudio anual de ciberseguridad 2022-2023* (CCIT, 2024), el sector pyme fue el más afectado por los ciberataques, en gran medida por la falta de estrategias de protección y por el desconocimiento sobre las amenazas digitales. El informe advierte que solo el 7% de las pymes logra subsistir después de sufrir un ciberataque, dado que las pérdidas suelen superar el capital inicial.

Los principales impactos reportados en este segmento incluyeron:

- Suplantación de identidad comercial en portales falsos y redes sociales.
- Estafas en ventas digitales, especialmente en Marketplace y WhatsApp.
- Acceso indebido a cuentas empresariales, con fraudes financieros o bloqueo de operaciones.

Estos incidentes han generado consecuencias graves sobre la continuidad del negocio, la reputación comercial y la confianza del cliente.

Afectación en la Ciudadanía

Suplantación, fraude y pérdida de datos

Durante los tres años analizados, las personas naturales fueron víctimas frecuentes del cibercrimen. Entre 2022 y 2024, el CAI Virtual recibió más de 160.000 denuncias ciudadanas, principalmente por hurto por medios informáticos, suplantación de identidad y violación de datos personales.

Los casos más recurrentes fueron:

- Robo de cuentas de WhatsApp para realizar estafas a los contactos.
- Phishing bancario, mediante enlaces falsos enviados por SMS o redes sociales.

- Estafas en compras electrónicas, donde se pagaban productos que nunca eran entregados.

Extorsiones digitales, a través de videos falsos, amenazas en línea o manipulación de contenido.

Consecuencias Psicológicas y Sociales

Más allá de la pérdida económica, muchas víctimas manifestaron sentimientos de angustia, inseguridad y desconfianza. El hecho de ser engañadas por un canal aparentemente familiar, como WhatsApp o una página bancaria, generó un profundo cuestionamiento sobre la seguridad del entorno digital. Varios informes mencionaron la aparición de síntomas de estrés postraumático, sobre todo en personas mayores o en casos de extorsión con contenido íntimo.

Costos Sociales y Percepción de Inseguridad Digital

Brechas Digitales y Exclusión

Las regiones más afectadas por el cibercrimen también coincidieron con zonas de baja alfabetización digital, lo que aumentó la vulnerabilidad de sus habitantes. El Centro Cibernético Policial identificó un crecimiento de incidentes en ciudades intermedias y municipios de la costa Caribe y el Eje Cafetero, donde las campañas de prevención aún no han logrado cobertura suficiente.

El impacto del cibercrimen en Colombia entre 2022 y 2024 fue profundo, multisectorial y de alto costo social. Afectó por igual a microempresas, grandes corporaciones, entidades públicas y ciudadanos comunes. Las consecuencias no se limitaron a lo económico: incluyeron pérdidas operativas, quiebras empresariales, daño reputacional, traumas psicológicos y una creciente sensación de inseguridad digital.

Si bien el Estado ha avanzado en mecanismos de respuesta y prevención, el nivel de afectación demuestra que el cibercrimen no es un fenómeno marginal, sino una amenaza estructural al desarrollo económico y a la cohesión social. En este sentido, comprender y atender sus impactos resulta imprescindible para fortalecer la resiliencia digital del país.

Análisis Evolutivo y Comparativo del Cibercrimen en Colombia (2022-2024)

Este eje final integra los hallazgos obtenidos en el análisis del cibercrimen en Colombia durante los años 2022, 2023 y 2024, con el fin de establecer patrones, contrastes y aprendizajes clave en cinco dimensiones fundamentales: tipologías delictivas, sectores afectados, vectores tecnológicos, respuestas institucionales, e impacto social y económico. Su propósito es ofrecer una visión holística de cómo se ha comportado el fenómeno, qué tendencias se han consolidado y cuáles retos persisten para el país.

Evolución de tipologías delictivas

El análisis comparado de las modalidades delictivas permitió identificar una consolidación del hurto por medios informáticos y el acceso abusivo a sistemas informáticos como los delitos más frecuentes en todo el periodo. En 2022 se reportaron 26.366 casos de hurto digital, cifra que se aumentó a 28.512 en 2023, y volvió a incrementarse en 2024 con 37.409 denuncias, confirmando su persistencia como amenaza estructural.

Asimismo, la suplantación de identidad digital pasó de representar un fenómeno secundario a ser uno de los principales vectores en 2024, especialmente a través de WhatsApp y redes sociales. La aparición de técnicas como el voice cloning y el uso de deepfakes en contextos de extorsión o fraude representa una transformación cualitativa en la complejidad del delito.

Cambios en Sectores Afectados

El comportamiento sectorial del cibercrimen evidenció dos grandes dinámicas:

- Una afectación sostenida del sector financiero, que lideró las denuncias en todo el trienio.
- Una expansión progresiva hacia sectores críticos como salud, educación, gobierno local y Mipymes.

Variaciones en Vectores Tecnológicos

Entre 2022 y 2024, se observó un paso acelerado de técnicas simples (phishing por correo, enlaces engañosos) hacia vectores más complejos como:

- Aplicaciones móviles maliciosas (2023)
- Bots y troyanos bancarios automatizados (2023-2024)
- Inteligencia artificial para suplantación, voz y video (2024)

El uso de plataformas móviles como WhatsApp y aplicaciones falsas para distribuir malware y ejecutar fraudes mostró un crecimiento considerable.

Respuesta Institucional a lo Largo del Tiempo

Las capacidades del Estado colombiano también evolucionaron. En 2022, se centraron en campañas de prevención y fortalecimiento del CAI Virtual. En 2023 se consolidó el PMU Ciber para respuesta coordinada a incidentes, y en 2024 se implementaron herramientas de inteligencia artificial forense para enfrentar nuevas amenazas como los deepfakes.

A lo largo del trienio, el CAI Virtual atendió más de 163.000 incidentes, consolidándose como el principal canal de reacción inmediata. Sin embargo, los desafíos relacionados con la judicialización de casos, la articulación con el sector privado y la brecha tecnológica en regiones persisten como limitaciones estructurales.

Impacto Social y Económico Acumulado

El cibercrimen ha generado impactos acumulativos importantes en tres niveles:

Empresarial: Pérdidas económicas, afectación reputacional, bloqueo operativo, especialmente en Mipymes y sectores críticos como salud y educación.

Ciudadano: Estafas por suplantación, fraudes digitales, extorsiones por contenido falso, y pérdida de confianza en canales digitales.

Social: Aumento de la desconfianza digital, afectación psicológica en víctimas, y creciente percepción de inseguridad en internet.

El análisis comparativo de los años 2022-2024 demuestra que el cibercrimen en Colombia no solo creció en volumen, sino que se transformó en su naturaleza, expandiendo sus objetivos, sofisticando sus métodos, y desafiando las capacidades de respuesta del Estado. Aunque las autoridades han mejorado notablemente sus herramientas y coordinación interinstitucional, la velocidad de adaptación de los ciberdelincuentes obliga a repensar permanentemente las estrategias de prevención, monitoreo y contención. (CCIT, 2024).

Este eje permite cerrar la etapa de análisis con una visión clara: Colombia enfrenta un cibercrimen más organizado, más transversal y tecnológico que nunca. Comprender su evolución no solo es clave para proteger a los ciudadanos, sino para garantizar la estabilidad institucional, económica y social del país.

Ciberseguridad en Colombia en 2025: Ejecución, Gobernanza y Resiliencia

Según el documento *Estrategia nacional de seguridad digital de Colombi a 2025 - 2027* (Gobierno de Colombia, 2025). En 2025 Colombia entra en una fase de ejecución ambiciosa. El país adopta una estrategia nacional tres veces al año que exige pasar de marcos declarativos a capacidades operativas, consolidar la gobernanza creando una instancia nacional especializada que planifique, coordine y haga seguimiento de la seguridad digital; a la par, revisar y adecuar el modelo establecido en el Decreto 338 de 2022 para que responda al nuevo contexto de amenazas y a estándares internacionales. Este giro no es cosmético implica liderazgo con representación diversa y mecanismos de coordinación efectivos a todos los niveles del Estado.

La columna vertebral de esta gobernanza se completa con infraestructura de inteligencia y gestión de crisis, un sistema de intercambio de información de amenazas entre sector público y privado, un observatorio nacional que identifique patrones y oriente la respuesta, y herramientas vinculantes para asegurar la acción coordinada del Estado. Además, se despliegan plataformas de colaboración y alianzas públicas y privadas para investigación y adopción de tecnologías de seguridad. Todo esto se conecta con cooperación internacional (Convenio de Budapest y trabajo con la Ransomware Task Force) para compartir inteligencia y reforzar la respuesta a incidentes.

El vector técnico de 2025 prioriza la protección de infraestructuras críticas y servicios esenciales, identificación e inventario detallado de activos, adopción de arquitecturas Zero Trust, y monitoreo continuo con evaluación sistemática de vulnerabilidades. Estas acciones se extienden a cadenas de suministro y empujan la idea de (seguridad por defecto) en servicios públicos. Con esto, el país cierra la brecha entre los avances metodológicos de 2024 como la actualización del inventario de infraestructuras críticas y su despliegue operativo a nivel nacional en 2025.

En paralelo, 2025 marca un punto de madurez en la integración de IA y ciberseguridad. Se establecen capacidades mínimas de uso seguro y responsable de IA para el sector público con mecanismos de compra para implementarlas y recomendaciones para el sector privado, incluyendo la evaluación de instrumentos vinculantes. Se articula, además, un programa de concientización sobre riesgos asociados a IA y la promoción de autenticación sin contraseñas, señalando un desplazamiento claro hacia controles de identidad más robustos.

Este énfasis se alinea con la política nacional de inteligencia artificial (CONPES 4144 de 2025), que fija seis ejes (ética y gobernanza; datos e infraestructura; I+D+i; talento; mitigación de riesgos; uso y adopción en sector público, privado y territorios) y compromete $479.273 millones de pesos del presupuesto nacional para impulsar dichas líneas a 2030, con liderazgo interinstitucional del DNP, MinTIC, MinCiencias, MEN, DAPRE y MinTrabajo. Su relevancia para ciberseguridad es directa, más IA en procesos productivos y públicos exige mejores salvaguardas de seguridad y privacidad desde el diseño (CCIT, 2025).

La actualización normativa es otro eje definitorio de 2025. Se reconoce la obsolescencia de marcos como la Ley 1273 de 2009 frente a modalidades delictivas actuales, la falta de mecanismos de revisión periódica y la necesidad de alinear el régimen sustantivo y procesal con obligaciones internacionales. Como respuesta, se propone un mecanismo bienal de revisión, reglas claras de notificación de violaciones de datos y privacidad por diseño, y regulaciones específicas para tecnologías emergentes (IA, IoT, nube). Se enfatiza, además, clarificar la responsabilidad ejecutiva en seguridad digital dentro de las organizaciones.

Implicaciones para Empresas y Sector Público en 2025

Para el tejido empresarial, 2025 redefine prioridades, la seguridad deja de ser gasto discrecional y se convierte en condición estratégica para continuidad y reputación. Las empresas

críticas y sus proveedores deben integrarse a esquemas de inventario y monitoreo continuo, fortalecer controles de identidad (migración hacia passwordless y MFA robusta) y adoptar gradualmente Zero Trust en redes y aplicaciones. Las cadenas de suministro pasan a ser objeto de planes de resiliencia específicos, con métricas de evaluación y exigencias de reporte coordinado con la autoridad. La gestión del riesgo de IA entra en la agenda diaria, toda adopción (desde copilotos hasta analítica) debe alinearse con las capacidades mínimas exigidas, y con marcos de privacidad por diseño y notificación de incidentes que el país impulsa para 2025. Esto se traduce en evaluaciones de impacto, controles contra sesgos y trazabilidad de decisiones automatizadas, tanto en servicios al cliente como en procesos internos (Gobierno de Colombia, 2025).

El talento es un cuello de botella reconocido, 2025 acelera programas de retención en el sector público, formación y certificación para profesionales, becas y pasantías, y entrenamiento de líderes de TI en seguridad. Para las organizaciones, esto implica revisar sus planes de carrera, crear rutas de certificación y cerrar brechas de competencias en detección, respuesta, gestión de vulnerabilidades y gobierno de datos. En el sector público, 2025 pone foco en los niveles territorial y operativo, adopción efectiva del MSPI, actualización del inventario de infraestructuras críticas, y ejercicios de respuesta a incidentes con evaluación periódica. A esto se suma la coordinación entre CSIRTs y defensa con analítica avanzada e IA para detección temprana, y simulaciones regulares incluidas amenazas emergentes como deepfakes para medir preparación institucional.

Normativamente, 2025 es un año de transición hacia un ecosistema más exigente, revisiones bienales, mayores obligaciones de reporte de brechas, y clarificación de deberes del C-suite. Esta trayectoria converge con iniciativas legislativas en curso para una Agencia Nacional de Seguridad Digital que articule actores y capacidades del ecosistema. En términos prácticos,

las organizaciones deben anticiparse, ajustar sus políticas, mapear datos sensibles, definir umbrales de notificación, y documentar responsabilidades ejecutivas.

Como telón de fondo, las tendencias de 2024 que cierran el año con incremento global de malware 30% y un 51% de alza en ransomware en Latinoamérica a junio no se disipan; justifican la urgencia de 2025 y explican por qué la combinación de gobernanza, tecnología (Zero Trust, monitoreo continuo), talento y actualización normativa es la única vía para sostener ciber-resiliencia.

Recomendaciones

Se plantean algunas recomendaciones generales teniendo como punto de referencias los siguientes documentos: *Conpes 4145* (DNP, 2025), *Estrategia nacional de seguridad digital de Colombia 2025 - 2027* (Gobierno de Colombia, 2025), *Estado de la ciberseguridad y la inteligencia artificial en Colombia*" (CCIT, 2025).

A lo largo de este documento se ha evidenciado que, en 2025, Colombia enfrenta el desafío de consolidar un ecosistema digital seguro y resiliente, para ello, es clave fortalecer la gobernanza y la coordinación interinstitucional mediante una entidad nacional con mandato para planear, coordinar y dar seguimiento a la seguridad digital. Esta debe articular al Estado, el sector privado y la academia, promover alianzas internacionales y asegurar una inversión en I+D coherente con los lineamientos del CONPES 4145, con reportes estandarizados y seguimiento anual.

La hoja de ruta incluye, en el corto plazo, activar la entidad coordinadora, mesas de trabajo y programas de cultura digital; en el mediano, completar el inventario de infraestructuras críticas, implementar certificaciones y realizar simulaciones; y en largo plazo, adoptar Zero Trust en sistemas críticos, ejecutar auditorías y evaluar la efectividad de la respuesta. El avance se medirá mediante indicadores de gobernanza, resiliencia, talento, privacidad y adopción de estándares, asegurando que tanto el sector público como las empresas especialmente las Mipymes incrementen su preparación y capacidad de respuesta frente a un panorama de amenazas cada vez más sofisticado.

Teniendo en cuenta esto a continuación, se plantean recomendaciones específicas y concretas aplicables para el contexto colombiano que pueden mejorar la ciberseguridad para las organizaciones del país:

Órgano Nacional de Coordinación en Seguridad Digital

El Departamento Nacional de Planeación y el Ministerio de Tecnologías de la Información y las Comunicaciones deben constituir un órgano de coordinación con mandato explícito para planear, priorizar inversiones y supervisar la ejecución de la agenda de seguridad digital. Su diseño debe incluir una secretaría técnica que mantenga el ritmo de trabajo y comités sectoriales para finanzas, salud, educación, servicios públicos y gobierno, de modo que las decisiones técnicas y presupuestales se tomen con conocimiento del terreno. Desde el primer día, el órgano debe publicar un plan anual con metas verificables, responsables y calendario, y sostener sesiones mensuales con actas públicas y seguimiento de tareas.

Para que la coordinación no se diluya, el órgano debe disponer de un tablero de control que muestre avances e incumplimientos por sector, indique cuellos de botella y active alertas cuando un hito crítico se retrasa. En el corto plazo, la señal de que la nueva gobernanza funciona será la instalación y operación efectiva de al menos tres comités, la publicación del plan anual, y la demostración de que decisiones priorizadas pasan a ejecución con responsables y fechas visibles.

Sistema Nacional de Intercambio de Inteligencia de Amenazas

La instancia coordinadora debe implantar un mecanismo seguro para compartir señales de ataque, indicadores técnicos, tácticas observadas y medidas de mitigación probadas, de la mano de los Equipos de Respuesta a Incidentes de Seguridad Informática de cada sector y con apoyo metodológico para estandarizar campos y definiciones del Departamento Administrativo Nacional de Estadística. El sistema debe iniciar con pilotos en los sectores financiero y salud, donde el intercambio temprano de información reduce impactos y acelera parches, y escalar luego al resto de sectores.

El mecanismo debe proteger la confidencialidad, pero al mismo tiempo registrar quién aporta y quién utiliza la información para poder medir su utilidad. Cada quince días se publicarán boletines con las amenazas más relevantes, las firmas técnicas para detectarlas y ejemplos de bloqueo. La prueba de efectividad no será la cantidad de documentos emitidos, sino la evidencia de acciones concretas: parches aplicados con mayor oportunidad, dominios fraudulentos dados de baja y campañas de concientización que nazcan directamente de las señales compartidas.

Inventario Completo de Infraestructuras

El Ministerio de Tecnologías de la Información y las Comunicaciones, en conjunto con ministerios y superintendencias sectoriales, debe completar un Registro Nacional de Infraestructuras Críticas que incluya activos tecnológicos y procesos operativos, interdependencias entre sectores, criticidad, impacto, controles actuales, proveedores clave y planes de continuidad. Cada activo debe tener un responsable de riesgo con nombre y cargo, para evitar zonas grises donde nadie responde.

Con el inventario consolidado, el país podrá programar pruebas anuales de continuidad, ejercicios de evaluación de vulnerabilidades y simulacros por sector que verifiquen que los controles funcionan también bajo presión. El avance real se observará cuando el mapa de interdependencias permita aislar fallas sin detener servicios esenciales y cuando los dueños de riesgo reporten correcciones cerradas con fechas y evidencias verificables.

Evolución de la Respuesta Policial Para la Detección Temprana Basada en Datos

La Policía Nacional a través del CAI Virtual y del Centro Cibernético Policial debe pasar de una lógica centrada en la denuncia a un enfoque preventivo sustentado en analítica de datos. Para lograrlo, es necesario integrar fuentes diversas: reportes ciudadanos, avisos de sectores sensibles, listados de dominios y aplicaciones fraudulentas, y señales abiertas que anticipan

campañas coordinadas. Con esa base, se entrenarán modelos que identifiquen patrones repetidos de fraude y suplantación, capaces de emitir alertas preventivas a entidades públicas y privadas antes de que la operación maliciosa alcance su pico.

El éxito de este cambio se notará en la reducción del tiempo promedio de detección y recuperación, en la oportunidad de las advertencias que reciban las entidades expuestas y en la proporción de campañas que se desactivan o degradan antes de producir pérdidas importantes. Para sostener la confianza, cada trimestre se publicará un informe de desempeño que muestre qué alertas se emitieron, qué bloqueos se lograron y qué aprendizajes operativos se incorporaron.

Simulacros Nacionales de Ciber Crisis

La instancia coordinadora debe organizar dos simulacros intersectoriales por año que involucren alta dirección, equipos técnicos, áreas jurídicas y de comunicaciones. Los guiones deben reflejar la realidad actual: suplantación con inteligencia artificial de voces y autoridades, portales clonados que capturan credenciales, interrupciones en proveedores críticos y efectos en cadena que rebasan fronteras sectoriales. Cada simulacro debe terminar con un informe público de lecciones aprendidas, un listado concreto de acciones correctivas y fechas de cumplimiento acordadas con los responsables.

Estos simulacros conllevan a mejoras cíclicas, puesto que lo ideal es que en el simulacro siguiente, las recomendaciones del ejercicio anterior aparezcan resueltas, la coordinación entre actores sea más fluida y los tiempos de decisión y recuperación disminuyan de manera comprobable.

Adopción por Fases de Arquitecturas de “Confianza Cero”

Las entidades que operan servicios esenciales deben migrar gradualmente hacia un modelo de verificación continua. El primer paso es asegurar la identidad: autenticación

multifactorial obligatoria en aplicaciones críticas y controles de privilegios mínimos para reducir superficies de ataque. El segundo paso es segmentar redes y aislar aplicaciones y datos sensibles, de forma que una intrusión no comprometa todo el entorno. La tercera fase es el monitoreo continuo del comportamiento en equipos, servidores y servicios en la nube, con capacidad de respuesta automatizada para contener rápidamente actividades anómalas. Finalmente, el modelo debe extenderse a proveedores y terceros, con requisitos de seguridad explícitos en contratos y auditorías periódicas.

El progreso se medirá semestralmente en tres indicadores simples y comprobables: qué proporción de aplicaciones críticas exigen autenticación reforzada, qué porción de redes críticas ya está segmentada, y qué cobertura real tiene la telemetría y la respuesta automatizada sobre los equipos y servicios que sostienen los procesos más sensibles.

Rutas de Certificación, Becas e Incentivos y Formación

El Ministerio de Educación Nacional, el Ministerio de Tecnologías de la Información y las Comunicaciones y el Servicio Nacional de Aprendizaje deben establecer rutas formativas diferenciadas para analistas, arquitectos, auditores y gestores de riesgo, acompañadas de becas y compromisos de permanencia mínima en el sector público. Al mismo tiempo, es necesario ajustar escalas salariales y planes de carrera para evitar que la inversión en capacitación se pierda por rotación temprana.

La Escuela Superior de Administración Pública y las universidades deben ofrecer módulos específicos para alta dirección en gobierno de riesgos, decisiones bajo presión y uso seguro de inteligencia artificial. El impacto se verá en el aumento sostenido de profesionales certificados por rol, en la estabilidad de los equipos críticos y en decisiones de directivos mejor informadas durante incidentes y grandes proyectos tecnológicos.

Ciclo Bienal de Actualización Normativa y Obligación de Notificación

El Ministerio de Justicia y del Derecho, el Ministerio de Tecnologías de la Información y las Comunicaciones y el Departamento Nacional de Planeación deben implementar una agenda de revisión cada dos años que cubra ciberdelito, protección de datos y tecnologías emergentes. Esa agenda debe acompañarse de una obligación clara de notificar incidentes significativos mediante un punto único de reporte, con plazos definidos, formatos homogéneos y salvaguardas de confidencialidad que incentiven la denuncia responsable.

El beneficio de este esquema será doble: por un lado, un marco jurídico que no se vuelve obsoleto frente a técnicas y herramientas que cambian rápido; por otro, un flujo de información confiable que permite ver tendencias, identificar sectores con brechas persistentes y dirigir mejor la supervisión y la asistencia técnica. La eficacia se reflejará en una mayor proporción de incidentes reportados a tiempo y cerrados con medidas correctivas verificadas.

Integración Segura y Verificable de Inteligencia Artificial

El Departamento Nacional de Planeación, el Ministerio de Tecnologías de la Información y las Comunicaciones y el Ministerio de Ciencia, Tecnología e Innovación deben exigir que cada entidad disponga de un inventario de sistemas algorítmicos, una evaluación de impacto antes del despliegue y un comité de aprobación técnica y ética que revise riesgos para seguridad, privacidad y servicio. Ese ciclo debe dejar huella documental: orígenes de datos, pruebas de robustez y seguridad, resultados esperados, medidas de mitigación y responsables de operación.

La trazabilidad permitirá auditar decisiones y ajustar modelos cuando se detecten sesgos o fallas de seguridad. Teniendo inventarios actualizados, dictámenes previos a la puesta en producción y un registro de incidentes y correcciones que genere confianza en la ciudadanía y en los usuarios internos.

Servicios Compartidos para Micro, Pequeñas y Medianas Empresas

El Ministerio de Tecnologías de la Información y las Comunicaciones, junto con cámaras de comercio y gremios, debe ofrecer a las micro, pequeñas y medianas empresas un esquema proporcional de cumplimiento que combine políticas básicas claras, copias de seguridad verificadas, autenticación multifactorial en servicios críticos y capacitación práctica enfocada en riesgos reales del día a día. Como muchos de estos negocios no pueden sostener equipos especializados, la estrategia debe incluir servicios compartidos de monitoreo y respuesta operados por un centro con economías de escala, a los que se acceda por una tarifa accesible.

Para alinear incentivos, los beneficios tributarios y las preferencias en compras públicas deben condicionarse a la adopción de estos mínimos. Auditorías ligeras y reportes semestrales por gremio o territorio permitirán demostrar que el porcentaje de empresas con controles básicos va en aumento y que los incidentes graves en este segmento se reducen de manera sostenida, lo que impacta directamente la resiliencia de la economía real.

Estas son algunas recomendaciones que se plantean tras el análisis realizado en esta revisión bibliográfica.

Conclusiones

Durante el periodo comprendido entre 2022 y 2024, el cibercrimen en Colombia experimentó una expansión significativa tanto en volumen como en complejidad. En 2022 se registraron 65.794 denuncias por delitos informáticos, cifra que descendió a 59.033 en 2023, pero que repuntó con fuerza en 2024, alcanzando un total de 77.866 casos. Este comportamiento demuestra que, pese a los esfuerzos institucionales, la amenaza cibernética no ha sido contenida de manera estructural. El delito más recurrente en los tres años fue el hurto por medios informáticos, con 26.366 casos en 2022, 28.512 en 2023 y 37.409 en 2024, lo que evidencia un patrón sostenido de vulnerabilidad en canales financieros digitales.

Los vectores tecnológicos también se transformaron sustancialmente. En 2022 predominaban técnicas como el phishing básico y el uso de troyanos bancarios; sin embargo, en 2024 se incorporaron herramientas avanzadas como la clonación de voz con inteligencia artificial, la creación de sitios web falsos idénticos a portales oficiales y la distribución masiva de malware desde aplicaciones móviles falsificadas. Además, en ese mismo año se documentaron campañas capaces de generar más de 10.000 correos falsos diarios, simulando comunicaciones de entidades oficiales como la Fiscalía o INTERPOL.

Frente a esta evolución delictiva, el Estado colombiano implementó diversas respuestas. El CAI Virtual recibió más de 163.000 incidentes en el trienio, con un promedio anual superior a 54.000 casos. Se consolidó el PMU Ciber como plataforma de atención a incidentes de alto impacto, se desarrollaron más de 4.000 planes operativos y se emitieron 20.000 alertas preventivas al sector financiero en 2024. No obstante, persistieron limitaciones estructurales, como la baja tasa de judicialización, la escasa articulación con el sector privado y la débil cobertura de estrategias de prevención en regiones intermedias.

En cuanto al impacto, el cibercrimen generó pérdidas económicas relevantes, afectó la continuidad de negocios, y comprometió datos personales y operativos de entidades públicas y privadas. La afectación también fue emocional: miles de ciudadanos denunciaron haber sido víctimas de suplantación, fraude, extorsión o violación de privacidad. En 2023, el 43% de los colombianos declaró sentirse inseguro al usar internet y un 65% manifestó no confiar plenamente en plataformas digitales, lo que refleja una crisis de confianza digital con implicaciones estructurales para el desarrollo del país.

Este análisis confirma que el cibercrimen en Colombia no es una amenaza ocasional, sino un fenómeno estructural, persistente y altamente adaptativo. Aunque se han logrado avances en vigilancia, respuesta operativa y cooperación internacional, el país sigue enfrentando desafíos urgentes en materia de cultura digital, protección de datos, fortalecimiento de talento humano y regulación de tecnologías emergentes. Comprender con rigor la evolución del cibercrimen entre 2022 y 2024 no solo es clave para enfrentar el presente, sino indispensable para anticipar y contener las amenazas del futuro.

El marco institucional avanzó en capacidades de vigilancia, respuesta y cooperación, pero la coordinación sigue fragmentada. La ausencia de una autoridad con mandato operativo claro para priorizar, asignar y exigir resultados dificulta convertir lineamientos en ejecución consistente. La gobernanza debe pasar de mesas y convenios a decisiones vinculantes con responsabilidades y seguimiento público.

En el plano operativo, la respuesta mejoró en volumen y cobertura, aunque persisten cuellos de botella en detección temprana, judicialización y articulación con el sector privado. La evidencia respalda que pasar de la reacción a la anticipación mediante analítica, intercambio de inteligencia y ejercicios regulares reduce impacto y tiempos de recuperación. La resiliencia

depende menos de adquisiciones puntuales y más de disciplina en procesos, pruebas y mejora continua.

Las micro, pequeñas y medianas empresas concentran una vulnerabilidad crítica: carecen de personal, presupuesto y procedimientos para sostener controles básicos de manera estable. Un enfoque proporcional estándares mínimos claros, servicios compartidos y verificación ligera es el camino realista para elevar el piso de seguridad del tejido productivo sin imponer cargas inviables. La política pública debe alinear incentivos para que adoptar estos mínimos sea la opción dominante.

Actualmente el talento es un factor limitante tanto como la tecnología. Sin rutas de formación por rol, certificaciones pertinentes, retención en el sector público y alfabetización de la alta dirección, las inversiones no se traducen en capacidades sostenibles. Es vital formar y mantener equipos competentes para manejar riesgos, operar arquitecturas modernas y cumplir marcos normativos exigentes.

La integración de inteligencia artificial abre oportunidades concretas para detección y defensa, pero sin inventarios, evaluaciones de impacto y controles de seguridad y privacidad, puede introducir nuevas superficies de riesgo. La adopción responsable exige trazabilidad técnica y decisiones informadas, especialmente en el sector público, donde la confianza ciudadana es un activo que debe protegerse con transparencia y evidencia.

La medición comparada y periódica es un déficit transversal. Sin indicadores estables de gobernanza, preparación, respuesta y recuperación, el país no puede distinguir entre actividad y resultado, ni asignar recursos donde más retorno ofrecen. Por lo que es clave institucionalizar métricas simples y verificables para sostener prioridades, corregir rumbos y rendir cuentas.

Finalmente, esta monografía aporta una línea base integrada para 2022-2025, identifica brechas accionables y propone una ruta de implementación realista que articula gobernanza, operaciones, talento, regulación e inteligencia artificial. El valor del trabajo no yace solo en describir el problema, sino en traducirlo en decisiones concretas que pueden ejecutarse y medirse. Con continuidad política y disciplina técnica, Colombia puede transformar avances aislados en resiliencia sostenida.

Bibliografía

Accenture. (2023). *State of cybersecurity resilience* 2023. https://www.accenture.com/content/dam/accenture/final/accenture-com/document/Accenture-State-Cybersecurity.pdf#zoom=40

ACIEM. (2024). En 2023, *Colombia reportó 28.000 millones de ciberataques financieros*. https://aciem.org/noticias-tecnologia-en-2023-colombia-reporto-28-000-millones-de-ciberataques-financieros/

Cámara Colombiana de Comercio Electrónico. (2024). *Conozca los principales desafíos de seguridad digital que tiene Colombia para el 2024*. https://ccce.org.co/noticias/conozca-los-principales-desafios-de-seguridad-digital-que-tiene-colombia-para-el-2024/

CCIT. (2023). *Estudio anual de ciberseguridad 2022-2023*. https://www.ccit.org.co/estudios/estudio-anual-de-ciberseguridad-2022-2023/

CCIT. (2024). *Ciberseguridad en Colombia: desafíos y perspectivas*. https://www.ccit.org.co/articulos-tictac/ciberseguridad-en-colombia-desafios-y-perspectivas/

CCIT. (2024). *Ciberseguridad en el sistema financiero colombiano: entre la amenaza y la resiliencia*. https://www.ccit.org.co/articulos-tictac/ciberseguridad-en-el-sistema-financiero-colombiano-entre-la-amenaza-y-la-resiliencia/

CCIT. (2025). *Estado de la ciberseguridad y la inteligencia artificial en Colombia*. https://www.ccit.org.co/estudios/estado-de-la-ciberseguridad-y-la-inteligencia-artificial-en-colombia/

COSO. (2017). *Enterprise risk management integrating with strategy and performance*. https://static.poder360.com.br/2023/09/Diretriz-Enterprise-Risk-Management-Coso-2017.pdf

Departamento Nacional de Planeación [DNP]. (2011). *Conpes 3701*. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

Departamento Nacional de Planeación [DNP]. (2020). *Conpes 3995*. https://colaboracion.dnp.gov.co/cdt/Conpes/Econ%C3%B3micos/3995.pdf

Departamento Nacional de Planeación [DNP]. (2022). *Plan nacional de desarrollo 2022-2026: Colombia potencia mundial de la vida*. Departamento Nacional de Planeación. https://colaboracion.dnp.gov.co/CDT/Prensa/Publicaciones/plan-nacional-de-desarrollo-2022-2026-colombia-potencia-mundial-de-la-vida.pdf

Departamento Nacional de Planeación [DNP]. (2025). *Conpes 4145*. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/4145.pdf

Departamento Nacional de Planeación [DNP]. (s. f.). *Dirección de desarrollo digital*. https://www.dnp.gov.co/LaEntidad_/subdireccion-general-prospectiva-desarrollo-nacional/direccion-desarrollo-digital/Paginas/documentos-conpes-confianza-y-seguridad-digital.aspx

Digi Americas Alliance. (2024). *Informe de ciberseguridad LATAM CISO 2023: Perspectivas de resiliencia cibernética en América Latina* [Informe]. Digi Americas Alliance. https://digiamericas.org/wp-content/uploads/2024/05/Report2023SPA.pdf

Fortinet. (2024). *Brecha de competencias en ciberseguridad 2024*. https://www.fortinet.com/content/dam/fortinet/assets/reports/es_la/2024-cybersecurity-skills-gap-report.pdf

Función Pública. (2009, 5 de enero). *Ley 1273 de 2009*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Función Pública. (2012, 17 de octubre). *Ley 1581 de 2012*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Función Pública. (2013, 27 de junio). *Decreto 1377 de 2013*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

IBM. (2024). ¿Qué es la ciberseguridad?. https://www.ibm.com/es-es/topics/cybersecurity

IMPACTOTIC. (2025). *Ciberseguridad en Colombia: Estrategias y desafíos actuales*. https://impactotic.co/ciber-seguridad/ciberseguridad-en-colombia-riesgos-a-los-que-se-enfrenta-el-pais/

IMPACTOTIC. (s. f.). *¿Necesita Colombia una Agencia Nacional de Seguridad Digital?*. https://impactotic.co/politicas-tic/agencia-nacional-de-seguridad-digital/

ISACA. (2019). *Drive innovation and value in a changing world*. https://www.isaca.org/resources/cobit

ISO. (2022). *ISO/IEC 27001:2022*. https://www.iso.org/standard/27001

ISO. (2022). *ISO/IEC 27005:2022*. https://www.iso.org/es/contents/data/standard/08/05/80585.html

itseller.co. (2024, 5 de diciembre). *Fortinet reporta que Colombia sufrió 36 mil millones de intentos de ciberataques los primeros 11 meses del 2024*. https://itseller.co/2024/12/05/fortinet-reporta-que-colombia-sufrio-36-mil-millones-de-intentos-de-ciberataques-los-primeros-11-meses-del-2024/

KPMG. (2024, marzo). *Consideraciones en ciberseguridad 2024*. https://kpmg.com/co/es/home/insights/2024/03/consideraciones-en-ciberseguridad-2024.html

LatinPyme. (2024). *Ciberataques en Colombia 2024: Cuando el error humano abre la puerta a miles de millones de amenazas*. https://latinpyme.com/ciberataques-en-colombia-2024-cuando-el-error-humano-abre-la-puerta-a-miles-de-millones-de-amenazas/

LinkTic. (2024). *Ciberseguridad en Colombia: panorama completo de su estado en 2023*. https://linktic.com/blog/panorama-completo-de-la-ciberseguridad-en-colombia/

ManageEngine. (2024). *Estado de la ciberseguridad en América Latina para 2024*. https://www.manageengine.com/latam/encuesta/estado-de-la-ciberseguridad-2024/

MinTIC. (2016). *Guía para la implementación de seguridad de la información en una Mipyme*. https://gobiernodigital.mintic.gov.co/692/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf

MinTIC. (2021, 10 de marzo). *Resolución número 00500 de marzo 10 de 2021*. https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_2.pdf

MinTIC. (2024). *Estrategia nacional digital 2023-2026*. https://www.mintic.gov.co/portal/715/articles-334120_recurso_1.pdf

MinTIC. (2024). *Informe de gestión año 2023*. https://www.mintic.gov.co/portal/715/articles-334075_recurso_1.pdf

MinTIC. (2025). *Estrategia nacional de seguridad digital de Colombia 2025-2027*. https://www.mintic.gov.co/portal/715/articles-403023_recurso_2.pdf

MinTIC. (2025). *Informe de gestión 2024*. https://www.mintic.gov.co/portal/715/articles-399819_recurso_1.pdf

MinTIC. (2025). *Lineamientos del modelo nacional de gestión de riesgo de seguridad de la información en entidades públicas*. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-401774_recurso_1.pdf

MinTIC. (2025). *Plan de acción 2025*. https://www.mintic.gov.co/portal/715/articles-399586_recurso_1.pdf

Policía Nacional de Colombia. Observatorio del Cibercrimen. (2025). *Balance anual del cibercrimen 2024*. https://caivirtual.policia.gov.co/sites/default/files/observatorio/BALANCE%20ANUAL%20CECIP%202024_1.pdf

Policía Nacional de Colombia. Observatorio del Cibercrimen. (2023). *Balance anual del cibercrimen 2022*. https://caivirtual.policia.gov.co/sites/default/files/observatorio/Balance%20anual%202022.pdf

Policía Nacional de Colombia. Observatorio del Cibercrimen. (2024). *Balance anual del cibercrimen 2023*. https://caivirtual.policia.gov.co/sites/default/files/observatorio/Balance%20anual%202023_0.pdf

PwC. (2023). *Encuesta global de crimen y fraude económico 2022-2023*. https://www.pwc.com/co/es/publicaciones/gecs/infografias/gecs-inf1-fraude.pdf

PwC. (2024). *Global digital trust insights de 2024 de PwC Colombia*. https://www.pwc.com/co/es/publicaciones/digital-trust-insights/2024/digital-trust-insights-2024-pwc-colombia.pdf

PwC. (2024). *Global economic crime survey 2024 de PwC Colombia*. https://www.pwc.com/co/es/publicaciones/encuesta-crimen-fraude-economico.html

SuperTransporte. (2024). *Informe tercer cuatrimestre riesgos de seguridad de la información - 2024*. https://www.supertransporte.gov.co/documentos/2025/enero/Planeacion_27/1/INFORME_RIESGOS_SEGURIDAD_DE_LA_INFORMACION_TERCER_CUATRIMESTRE.pdf

World Economic Forum. (2023, 20 de septiembre). *La gestión de riesgos es para todas las empresas, no solo las gigantes*. https://es.weforum.org/stories/2023/09/la-gestion-de-riesgos-es-para-todas-las-empresas-no-solo-las-gigantes/

World Economic Forum. (2024). *The global risks report 2024* (19th ed.). https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf