Análisis de las vulnerabilidades en la ciberseguridad colombiana ante el espionaje digital: un enfoque en la protección de datos personales y corporativos

María Alejandra Fierro García

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en Seguridad Informática

2026

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Resumen

El crecimiento de la conectividad digital en Colombia ha incrementado la exposición a riesgos asociados con el espionaje digital, particularmente en los puntos de conexión que actúan como puertas de entrada a redes personales, corporativas y gubernamentales. La multiplicación de ataques mediante software malicioso, la fuga de datos personales y el acceso no autorizado a infraestructuras críticas han evidenciado debilidades técnicas, normativas y operativas en la protección de la información. Esta investigación tiene como objetivo analizar las vulnerabilidades de los puntos de conexión en la ciberseguridad colombiana frente al espionaje digital, identificando medidas que fortalezcan la protección de los datos personales y de la información sensible. Se adoptó una metodología cualitativa con diseño de investigación descriptivo y enfoque documental, basada en el análisis de leyes, decretos, reportes institucionales, literatura técnica y casos documentados. Los hallazgos muestran que los puntos de conexión presentan fallas frecuentes como ausencia de autenticación multifactor, segmentación de red limitada, uso de dispositivos obsoletos y deficiencias en los procesos de detección. En el plano normativo, se identificaron vacíos en la tipificación penal, retrasos en la notificación de incidentes y debilidades en la regulación de la transferencia internacional de datos. Las herramientas tecnológicas disponibles muestran capacidades avanzadas, pero su implementación es heterogénea y enfrenta limitaciones en cobertura, personal técnico y presupuesto. Se concluye que la protección efectiva frente al espionaje digital requiere fortalecer la legislación, mejorar la coordinación interinstitucional y garantizar la adopción sostenida de controles técnicos en todos los niveles del ecosistema digital.

Palabras Clave: Ciberseguridad, datos, espionaje, malware, vigilancia

Abstract

The growth of digital connectivity in Colombia has increased exposure to risks associated with digital espionage, particularly at connection points that serve as gateways to personal, corporate, and governmental networks. The proliferation of attacks through malicious software, data leaks, and unauthorized access to critical infrastructures has revealed technical, regulatory, and operational weaknesses in information protection. This research aimed to analyze the vulnerabilities of connection points within Colombian cybersecurity in the face of digital espionage, identifying measures to strengthen the protection of personal data and sensitive information. A qualitative methodology with a descriptive research design and documentary approach was adopted, based on the analysis of laws, decrees, institutional reports, technical literature, and documented cases. Findings indicate that connection points frequently lack multi-factor authentication, proper network segmentation, and up-to-date devices, while also showing deficiencies in detection processes. At the regulatory level, the study identified gaps in criminal classification, delays in incident reporting, and weaknesses in the regulation of international data transfers. The technological tools currently available offer advanced capabilities, but their implementation remains uneven and faces limitations in coverage, technical personnel, and budget allocation. It is concluded that effective protection against digital espionage requires strengthening legislation, improving interinstitutional coordination, and ensuring sustained adoption of technical controls at all levels of the digital ecosystem.

Keywords: Cybersecurity, data, espionage, malware, surveillance

Introducción

La aceleración de la transformación digital ha incrementado la dependencia de los sistemas de información en los sectores público, privado y social. Esta expansión ha ampliado también la superficie de exposición frente a ataques informáticos, especialmente en los puntos de conexión que integran redes personales, institucionales y gubernamentales. En Colombia, el aumento sostenido de incidentes relacionados con espionaje digital, robo de datos y acceso no autorizado a infraestructuras críticas plantea interrogantes sobre la eficacia del marco regulatorio, las capacidades de prevención y respuesta, y la implementación de tecnologías de protección en los dispositivos terminales.

El espionaje digital representa una modalidad de intervención no autorizada que se basa en la interceptación, monitoreo o extracción de información sin consentimiento. Las técnicas utilizadas varían desde el uso de software malicioso hasta el acceso mediante credenciales comprometidas, pasando por el aprovechamiento de configuraciones inseguras o equipos obsoletos. Estas acciones impactan la privacidad de los individuos, la continuidad operativa de las organizaciones y la integridad de procesos públicos esenciales. Los puntos de conexión (entendidos como los dispositivos que permiten el ingreso o salida de datos de una red) constituyen una de las áreas más vulnerables. Su exposición puede derivarse tanto de fallas técnicas como de ausencias normativas o desconocimiento institucional.

En este contexto, la presente investigación tiene como propósito analizar las vulnerabilidades presentes en los puntos de conexión utilizados en Colombia y su vinculación con el espionaje digital, a través de un estudio de tipo descriptivo y enfoque cualitativo. Se parte de un análisis documental sustentado en fuentes normativas, estudios técnicos, reportes institucionales y literatura académica especializada. El objetivo general consiste en identificar

riesgos, evaluar respuestas institucionales y proponer criterios de fortalecimiento en la protección de los datos personales y la seguridad digital en los entornos conectados.

El desarrollo de este trabajo se organiza en función de tres objetivos específicos. En primer lugar, se describen las principales vulnerabilidades detectadas en los puntos de conexión, tomando como base registros de ataques, análisis de malware y patrones de comportamiento en redes expuestas. Esta sección explora tanto el uso de spyware, troyanos y ransomware como los mecanismos de propagación, las condiciones técnicas que permiten la intrusión y las consecuencias directas sobre personas y organizaciones. Se identifican los factores que habilitan el acceso no autorizado, incluyendo dispositivos sin segmentación, redes inalámbricas abiertas y servicios mal configurados, con énfasis en casos documentados en medios y reportes oficiales.

En segundo lugar, se examinan las políticas públicas y regulaciones vigentes relacionadas con la ciberseguridad, con atención particular a la protección de los datos personales y los dispositivos terminales. Se analizan las leyes 1273 de 2009 y 1581 de 2012, decretos sectoriales y lineamientos técnicos como el Modelo de Seguridad y Privacidad de la Información (MSPI). Se revisa también la capacidad sancionatoria de las autoridades, la adecuación del marco penal frente a nuevas modalidades delictivas y los mecanismos de coordinación interinstitucional. Este apartado permite establecer los vacíos normativos existentes y contrastarlos con estándares internacionales, como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea.

El tercer objetivo aborda las herramientas tecnológicas y prácticas institucionales adoptadas en Colombia para proteger los puntos de conexión. Se analizan los tipos de controles implementados, su cobertura, eficacia y las limitaciones detectadas en diferentes sectores. Este componente considera desde tecnologías como autenticación multifactor, segmentación de red,

detección de intrusos y cifrado de datos, hasta elementos organizacionales como formación del talento, gestión de incidentes y campañas de sensibilización. Se recopilan casos específicos que permiten observar la aplicación práctica de las recomendaciones técnicas y su impacto en la contención de amenazas.

La investigación ofrece una visión estructurada sobre las condiciones actuales de la ciberseguridad en Colombia con respecto a los puntos de conexión. A través del análisis documental se busca contribuir al diseño de respuestas más eficaces frente a riesgos emergentes y a la definición de políticas públicas que integren componentes técnicos, normativos y operativos para el fortalecimiento de la seguridad digital.

Planteamiento del Problema

La ciberseguridad en Colombia enfrenta serias vulnerabilidades que comprometen tanto la protección de datos personales como la información corporativa. Estas brechas han sido explotadas recurrentemente por actores malintencionados mediante prácticas de espionaje digital, las cuales van desde la interceptación no autorizada de comunicaciones hasta la instalación de software malicioso diseñado para robar datos sensibles. Estas amenazas, lejos de ser meros problemas tecnológicos, tienen un impacto directo en la privacidad de los ciudadanos, la estabilidad de las organizaciones y la confianza en las instituciones encargadas de la protección de la información.

El espionaje digital en Colombia se ha intensificado por el uso de tecnologías avanzadas que explotan vulnerabilidades en los sistemas de ciberseguridad. Un ejemplo destacado es el uso de *spyware* como *Pegasus*, empleado en 2020 para monitorear ilegalmente a periodistas, líderes sociales y defensores de derechos humanos. Este caso expuso no solo el uso indebido de herramientas de vigilancia, sino también las limitaciones de los sistemas de protección de datos para prevenir tales abusos. A pesar de la existencia de la Ley 1581 de 2012, diseñada para garantizar la protección de datos personales, el marco normativo no responde a la velocidad con la que evolucionan las tecnologías utilizadas en el espionaje digital (Congreso de Colombia, 2012; Ávila, 2020).

Desde la perspectiva corporativa, empresas de sectores estratégicos, como el financiero, energético y de telecomunicaciones, han sido blanco de ataques cibernéticos dirigidos a extraer información crítica o interrumpir sus operaciones. Estos ataques, que incluyen desde phishing avanzado hasta ransomware, aprovechan la falta de protocolos robustos de ciberseguridad y la escasa implementación de tecnologías de detección de amenazas en tiempo real. En 2021, varias

entidades financieras reportaron pérdidas significativas asociadas a brechas de seguridad digital, evidenciando la urgente necesidad de fortalecer las estrategias de protección de datos corporativos (Patiño, 2018; Aldrich, 2016).

La falta de concienciación en ciberseguridad entre usuarios y organizaciones también agrava estas vulnerabilidades. En un contexto donde el uso masivo de dispositivos conectados a internet (IoT) ha ampliado la superficie de ataque, muchas instituciones no cuentan con medidas adecuadas para gestionar los riesgos asociados. Además, la baja inversión en capacitación y tecnología avanzada limita la capacidad de los equipos encargados de la seguridad informática para prevenir y mitigar ataques cibernéticos, dejando expuestos tanto a ciudadanos como a corporaciones a prácticas de espionaje masivo (Zuboff, 2019).

El impacto de estas vulnerabilidades va más allá de la privacidad individual, pues afecta la confianza en los sistemas de seguridad y las instituciones gubernamentales encargadas de proteger los datos sensibles. En el ámbito corporativo, las brechas de seguridad digital pueden traducirse en pérdidas financieras, daño reputacional y exposición de información estratégica, lo que compromete la competitividad de las organizaciones colombianas en un entorno global cada vez más digitalizado.

En este contexto, el problema central radica en cómo abordar y analizar las vulnerabilidades existentes en la ciberseguridad colombiana, específicamente ante el espionaje digital, para garantizar una protección efectiva de los datos personales y corporativos. Se requiere un enfoque integral que abarque desde la evaluación de las debilidades estructurales en los sistemas actuales hasta la implementación de soluciones tecnológicas avanzadas. Asimismo, es fundamental fortalecer el marco normativo, capacitar a los actores involucrados en la gestión de seguridad digital y promover una cultura de protección de datos tanto en el ámbito público

como privado. Esta investigación se centrará en identificar los puntos críticos de vulnerabilidad y proponer estrategias concretas para mitigar los riesgos, con el objetivo de salvaguardar la privacidad y la integridad de la información en Colombia (Bamford, 2010; Bennett, 2008).

Objetivos

Objetivo General

Analizar las vulnerabilidades de los puntos de conexión en la ciberseguridad colombiana frente al espionaje digital y el uso de software malicioso, identificando medidas que fortalezcan la protección de los datos personales y la seguridad de la información sensible.

Objetivos Específicos

Describir las principales vulnerabilidades de los puntos de conexión en Colombia frente al espionaje digital y el uso de software malicioso, con énfasis en su impacto sobre los datos personales y la seguridad de la información.

Examinar las políticas y regulaciones actuales en ciberseguridad en Colombia, identificando brechas específicas relacionadas con la protección de los puntos de conexión y los datos personales.

Identificar las herramientas tecnológicas y prácticas de seguridad implementadas en los puntos de conexión, señalando sus capacidades y limitaciones frente a amenazas de espionaje digital.

Justificación

La investigación sobre el espionaje digital y la vulnerabilidad de los datos en Colombia es crucial en un contexto donde la tecnología juega un rol predominante en la vida diaria de individuos, empresas e instituciones gubernamentales. El objetivo central de esta investigación es comprender cómo las prácticas de espionaje digital y el uso de software malicioso ponen en riesgo la privacidad y la seguridad de los datos, y, a partir de ello, proponer soluciones que permitan fortalecer las capacidades de ciberseguridad del país. Esta problemática cobra especial relevancia dado el crecimiento exponencial de ataques cibernéticos que aprovechan las debilidades en la infraestructura digital y la falta de políticas robustas de seguridad.

En primer lugar, la investigación se justifica por la necesidad de actualizar y adaptar las estrategias de protección de datos frente a las amenazas digitales emergentes. El espionaje digital, facilitado por el uso de spyware y otros tipos de malware, puede tener graves consecuencias tanto a nivel individual como colectivo. La información obtenida de manera ilícita puede ser utilizada para el fraude, la extorsión o incluso para poner en riesgo la seguridad nacional (Bamford, 2010). Ante este escenario, es fundamental analizar y mejorar las medidas preventivas y correctivas que existen en Colombia, evaluando no solo las tecnologías disponibles, sino también las normativas y prácticas operativas que pueden ser inadecuadas o insuficientes (Patiño, 2018).

El impacto de la investigación radica en su capacidad para generar conocimiento práctico y relevante para el fortalecimiento de las políticas de ciberseguridad en Colombia. Las conclusiones de este estudio permitirán identificar las principales debilidades en los sistemas de protección actuales, lo que proporcionará una base sólida para diseñar estrategias que incrementen la resiliencia frente a ataques cibernéticos. Además, la investigación contribuirá al

debate sobre la necesidad de equilibrar las tecnologías emergentes con la protección de los derechos fundamentales, tales como la privacidad y la seguridad de los datos personales (Bennett, 2008). Asimismo, se espera que los resultados sirvan para capacitar a profesionales en el área de seguridad informática, mejorando la capacidad de detección y respuesta ante posibles amenazas.

Si esta investigación no se lleva a cabo, las consecuencias podrían ser graves. Sin un análisis riguroso sobre las vulnerabilidades actuales y sin la implementación de soluciones efectivas, el país continuará expuesto a un número creciente de ataques cibernéticos que pueden comprometer la información crítica de ciudadanos, empresas y el gobierno. La falta de acciones preventivas adecuadas podría generar una crisis de confianza en las instituciones y en los sistemas digitales, debilitando tanto la seguridad pública como la económica (Cano, 2018). En el contexto global, donde los ciberataques se han vuelto más sofisticados, no tomar medidas urgentes y efectivas podría colocar a Colombia en una posición de alto riesgo frente a amenazas que evolucionan rápidamente (Aldrich, 2016).

En conclusión, esta investigación es fundamental para garantizar que el país esté preparado para enfrentar los desafíos de seguridad cibernética del futuro. Los resultados proporcionarán un marco teórico y práctico para implementar mejores políticas de protección de datos, contribuir al diseño de sistemas más seguros y robustos, y formar una cultura de ciberseguridad que involucre tanto a instituciones como a individuos. La falta de acción en este ámbito podría agravar la vulnerabilidad de los datos y comprometer la seguridad y estabilidad de todo el ecosistema digital en Colombia.

Alcance

A partir de la justificación y los objetivos planteados, es notable que la investigación tiene un alcance centrado en el análisis detallado de las vulnerabilidades existentes en los puntos de conexión de los sistemas digitales en Colombia frente al espionaje digital. Se trata de una indagación orientada a comprender cómo las amenazas digitales, particularmente el uso de software malicioso como spyware y malware, afectan la seguridad de la información personal y corporativa en el país. La investigación parte del reconocimiento de que estas prácticas, cada vez más sofisticadas, no solo comprometen la privacidad individual, sino que también representan un riesgo significativo para la estabilidad de las instituciones públicas, la confianza ciudadana y la competitividad empresarial. En ese sentido, el alcance de este estudio responde directamente al objetivo general de identificar dichas vulnerabilidades y proponer medidas para fortalecer la ciberseguridad en el contexto colombiano.

El trabajo se desarrolla a partir de un enfoque metodológico cualitativo y un diseño de tipo descriptivo, lo cual permite caracterizar las principales prácticas de espionaje digital, así como los marcos normativos y las capacidades tecnológicas implementadas para prevenirlas y mitigarlas. Este enfoque posibilita una comprensión profunda del fenómeno, basada en el análisis documental de leyes, decretos, sentencias, informes técnicos y estudios de caso. En correspondencia con los objetivos específicos, el estudio busca, en primer lugar, describir las vulnerabilidades de los puntos de conexión frente al espionaje digital; en segundo lugar, examinar las políticas y regulaciones en vigor, identificando brechas normativas; y en tercer lugar, evaluar las herramientas tecnológicas utilizadas actualmente para la protección de datos. Estas tres líneas de análisis delimitan de forma precisa el objeto de estudio y estructuran el campo de observación del investigador.

Desde un punto de vista temático, la investigación se concentra en fenómenos vinculados directamente al espionaje digital y la explotación de debilidades en la infraestructura de ciberseguridad. Se abordan problemáticas como la interceptación no autorizada de comunicaciones, la filtración de datos confidenciales, y el uso de malware para acceder a sistemas sin consentimiento. Aunque se reconocen otras amenazas presentes en el entorno digital, como el fraude cibernético o la suplantación de identidad, estas no forman parte del núcleo analítico del estudio, salvo en aquellos casos en que estén directamente relacionadas con prácticas de espionaje digital. Así, el alcance no incluye el desarrollo técnico de software ni la implementación de pruebas forenses, sino que se enfoca en los aspectos estratégicos, legales y sociales de la seguridad digital.

En cuanto a la delimitación temporal, el periodo comprendido para el análisis se extiende desde el año 2010 hasta el año 2024. Esta selección responde al interés por estudiar una etapa crítica en la evolución de las amenazas cibernéticas en Colombia, caracterizada por la masificación del uso de dispositivos conectados, el aumento de los ciberataques y la respuesta institucional frente a dichas amenazas. El periodo incluye eventos clave como el caso Andrómeda en 2014, los ataques al sector financiero en 2021, y las denuncias recientes sobre el uso de Pegasus entre 2020 y 2023. Asimismo, permite examinar el desarrollo y aplicación de normas fundamentales como la Ley 1581 de 2012, la Ley 1273 de 2009 y el Decreto 338 de 2022, las cuales estructuran el marco legal de la protección de datos en el país.

Geográficamente, la investigación se enfoca exclusivamente en el contexto colombiano, observando la forma en que se manifiestan las vulnerabilidades en distintos sectores, como el financiero, el de telecomunicaciones, el de salud, el gubernamental y el de derechos humanos. Si bien el trabajo se circunscribe al ámbito nacional, se utilizan referencias internacionales con fines

comparativos, especialmente aquellos casos que han generado impactos significativos en la discusión global sobre vigilancia digital y privacidad. Casos como el de Edward Snowden en Estados Unidos, el uso de Pegasus en México y España, y el ciberataque al NHS del Reino Unido, ofrecen elementos valiosos para establecer paralelos con la realidad colombiana, y así enriquecer el análisis crítico de las capacidades institucionales y regulatorias en el país.

Así las cosas, el alcance de la investigación excluye el levantamiento de información mediante encuestas, entrevistas o pruebas de campo, enfocándose únicamente en fuentes documentales de carácter oficial, técnico o académico. Esta decisión metodológica responde al tipo de análisis que se pretende realizar: un estudio riguroso del marco normativo y tecnológico de la ciberseguridad, orientado a formular propuestas concretas de mejora. Así, se espera que los resultados del estudio contribuyan a generar conocimiento útil para la formulación de políticas públicas, el fortalecimiento institucional, la actualización de normativas y la creación de una cultura de protección de datos en Colombia.

Marco Referencial

Antecedentes

El análisis del espionaje digital y la vulnerabilidad de la ciberseguridad en Colombia requiere una revisión de antecedentes tanto internacionales como nacionales. A nivel global, numerosos países han enfrentado casos de vigilancia ilegal, ciberataques y filtraciones de datos, lo que ha impulsado el desarrollo de marcos normativos y estrategias de defensa cibernética. En el contexto colombiano, se han documentado diversas situaciones en las que se ha vulnerado la privacidad de ciudadanos, periodistas y organizaciones, exponiendo la necesidad de fortalecer la ciberseguridad en el país.

Antecedentes Internacionales

Caso Snowden y la Vigilancia Masiva de la NSA (Estados Unidos, 2013)

Uno de los casos más emblemáticos de espionaje digital a nivel mundial fue la filtración de documentos clasificados de la Agencia de Seguridad Nacional (NSA, por sus siglas en inglés) por parte de Edward Snowden en 2013. Según Bamford (2010), estos documentos revelaron que la NSA llevaba a cabo un programa de vigilancia masiva denominado PRISM, mediante el cual interceptaba comunicaciones privadas a nivel global con la cooperación de empresas tecnológicas como Google, Facebook y Microsoft.

La filtración expuso cómo los gobiernos pueden utilizar herramientas digitales para acceder a datos personales sin el consentimiento de los ciudadanos. Esto generó una crisis en torno a la privacidad digital y llevó a debates sobre la necesidad de regular el espionaje gubernamental. Como resultado, Estados Unidos implementó reformas en sus programas de vigilancia, incluyendo la promulgación de la Ley de Libertad de EE. UU. (USA Freedom Act) en

2015, que limitó la recopilación masiva de metadatos por parte de las agencias de inteligencia (Westin, 2003).

El caso Snowden es relevante para Colombia porque demuestra el riesgo de que herramientas de vigilancia sean utilizadas sin controles adecuados, lo que puede derivar en violaciones a los derechos fundamentales de privacidad y protección de datos. Además, evidencia la necesidad de contar con regulaciones más estrictas y mecanismos de supervisión efectivos para evitar el abuso de la vigilancia digital.

El uso de Pegasus en España y México (2017-2022)

Pegasus, un software de espionaje desarrollado por la empresa israelí NSO Group, ha sido utilizado en múltiples países para interceptar comunicaciones privadas. En España, se documentó el espionaje a líderes políticos independentistas catalanes en el llamado CatalanGate, lo que generó una crisis política y la exigencia de mayor transparencia en el uso de tecnologías de vigilancia (Zuboff, 2019).

En México, el software Pegasus fue adquirido por el gobierno y utilizado para espiar a periodistas, activistas de derechos humanos y opositores políticos entre 2017 y 2022. De acuerdo con un informe de Citizen Lab (2022), se identificaron más de 15,000 dispositivos infectados en el país, lo que puso en evidencia la falta de controles sobre el uso de herramientas de espionaje.

Este caso es relevante para Colombia porque el software Pegasus ha sido mencionado en informes sobre posibles interceptaciones ilegales a periodistas y defensores de derechos humanos en el país. Además, demuestra la necesidad de regular el uso de herramientas de espionaje digital y establecer mecanismos de auditoría que garanticen que estas tecnologías no sean utilizadas para vulnerar la privacidad de los ciudadanos.

Ciberataque a la Agencia de Salud de Reino Unido (NHS, 2020)

En 2020, la Agencia Nacional de Salud del Reino Unido (NHS) fue víctima de un ciberataque con ransomware, lo que resultó en la interrupción de servicios médicos esenciales y la filtración de datos de pacientes. Según Anderson y Walker (2020), el ataque fue atribuido a un grupo de hackers vinculado a un Estado extranjero, lo que demostró la vulnerabilidad de infraestructuras críticas ante amenazas digitales.

Este ataque evidenció la necesidad de fortalecer la ciberseguridad en sectores estratégicos como la salud, donde la protección de datos es fundamental. En respuesta, el gobierno del Reino Unido implementó nuevas estrategias de ciberseguridad, incluyendo mayores inversiones en infraestructura digital y la creación de protocolos más estrictos para prevenir ataques similares.

El caso del NHS es un referente importante para Colombia, ya que los sistemas de salud en el país también han sido blanco de ciberataques. La vulnerabilidad de los datos personales en infraestructuras críticas demuestra la necesidad de fortalecer los mecanismos de seguridad digital y mejorar la capacidad de respuesta ante incidentes cibernéticos.

Antecedentes Nacionales

Caso Andrómeda: Interceptaciones Ilegales en Colombia (2014)

En 2014, se descubrió una red de espionaje denominada Andrómeda, operada desde una oficina en Bogotá que realizaba interceptaciones ilegales de comunicaciones de periodistas, políticos y funcionarios del gobierno. Según Ávila (2020), esta operación estaba vinculada a miembros del Ejército y tenía acceso a información confidencial sobre negociaciones de paz entre el gobierno colombiano y las FARC. El escándalo de Andrómeda puso en evidencia la existencia de estructuras de vigilancia no reguladas que operaban al margen de la ley. A raíz de este caso, se fortalecieron algunos controles sobre el uso de herramientas de espionaje digital,

pero persistieron denuncias sobre interceptaciones ilegales en años posteriores. Este antecedente es relevante porque demuestra que en Colombia han existido prácticas de espionaje digital que vulneran derechos fundamentales. Además, resalta la importancia de establecer mecanismos de supervisión más estrictos para evitar que entidades estatales o privadas accedan ilegalmente a información confidencial.

Ataques Cibernéticos al Sector Financiero Colombiano (2021)

En 2021, varias entidades bancarias en Colombia fueron víctimas de ataques cibernéticos que afectaron el acceso a servicios digitales y resultaron en la filtración de datos financieros. Según Patiño (2018), los ataques incluyeron técnicas como el phishing avanzado y el ransomware, afectando la confianza en la seguridad del sistema financiero colombiano.

El aumento de estos ataques evidenció la necesidad de implementar protocolos de seguridad más sólidos en el sector financiero. En respuesta, la Superintendencia Financiera emitió nuevas regulaciones que obligan a las entidades bancarias a fortalecer sus mecanismos de ciberseguridad y a reportar incidentes de manera más rápida y efectiva. Este caso es significativo porque resalta la vulnerabilidad de los datos financieros en Colombia y la importancia de establecer políticas más estrictas para proteger a los usuarios de la banca digital.

Uso de Pegasus en Colombia (2020-2023)

Según investigaciones de la Fundación Paz y Reconciliación (Ávila, 2020), en Colombia se han reportado casos de espionaje digital mediante el uso de software como Pegasus. Aunque el gobierno colombiano ha negado su uso, diversas organizaciones han denunciado interceptaciones ilegales a periodistas, líderes sociales y defensores de derechos humanos. Este antecedente es relevante porque demuestra que la vigilancia digital sigue siendo una amenaza en Colombia. La

falta de regulaciones claras sobre el uso de tecnologías de espionaje resalta la necesidad de establecer controles más rigurosos y garantizar el respeto a la privacidad de los ciudadanos.

Marco Conceptual

Ciberseguridad

La ciberseguridad se refiere al conjunto de prácticas, tecnologías y procesos diseñados para proteger redes, dispositivos, programas y datos contra ataques, daños o accesos no autorizados. Su objetivo es garantizar la confidencialidad, integridad y disponibilidad de la información digital (Aldrich, 2016). En un contexto de espionaje digital, la ciberseguridad desempeña un rol crucial para evitar la vulneración de datos y salvaguardar la información sensible tanto de individuos como de organizaciones.

Espionaje Digital

El espionaje digital se define como la práctica de interceptar, acceder o recopilar información confidencial a través de medios electrónicos, generalmente sin el consentimiento de las partes involucradas. Esta actividad puede ser realizada tanto por actores gubernamentales como no gubernamentales con fines de lucro, control o sabotaje (Bamford, 2010). En el contexto colombiano, el espionaje digital representa una amenaza directa a la privacidad y a la seguridad de la información personal y corporativa.

Malware

El malware, o software malicioso, es cualquier programa o código diseñado para causar daño a un sistema informático, robar datos o espiar a los usuarios. Incluye virus, gusanos, troyanos, ransomware, y spyware, entre otros. Su objetivo es explotar vulnerabilidades en los sistemas digitales para acceder a información sin autorización (Bennett, 2008). El malware es

una de las principales herramientas utilizadas en el espionaje digital, facilitando la interceptación de datos confidenciales.

Privacidad Digital

La privacidad digital se refiere al derecho que tienen los individuos y organizaciones de controlar y proteger su información personal y la manera en que es recopilada, utilizada y compartida en entornos digitales. Este concepto es esencial en la era de la información, donde la proliferación de datos en línea ha incrementado las oportunidades para su explotación (Westin, 2003). La privacidad digital es vulnerada cuando actores externos acceden sin permiso a información privada, a menudo mediante espionaje o malware.

Protección de Datos

La protección de datos consiste en las medidas legales, técnicas y organizativas destinadas a garantizar la seguridad de la información personal frente a su acceso no autorizado, manipulación o destrucción. La Ley 1581 de 2012 en Colombia, conocida como la Ley de Protección de Datos Personales, establece las directrices para el manejo adecuado de la información sensible (Congreso de Colombia, 2012). La protección de datos es una respuesta necesaria frente a las crecientes amenazas de espionaje y mal uso de la información.

Marco Teórico

El marco teórico de esta investigación se enfoca en analizar el espionaje digital y la vulnerabilidad de los datos desde perspectivas que exploran la intersección entre tecnología, derechos de privacidad y seguridad informática. Este enfoque se sustenta en diversas teorías que ofrecen una comprensión profunda de cómo las amenazas digitales afectan la integridad de los sistemas de información y los derechos fundamentales. Las teorías seleccionadas permiten contextualizar el análisis de las prácticas de espionaje digital en Colombia, ayudando a

desarrollar estrategias más robustas de ciberseguridad. Las teorías utilizadas incluyen la teoría del riesgo tecnológico, la teoría de la vigilancia digital y la teoría del capital de datos. Estas teorías proporcionan un marco conceptual para evaluar las prácticas actuales, identificar debilidades y proponer mejoras en la protección de datos y seguridad digital.

Teoría del Riesgo Tecnológico

La teoría del riesgo tecnológico se centra en el análisis de cómo las tecnologías emergentes crean nuevos riesgos e incertidumbres para los individuos y las organizaciones. Esta teoría, propuesta por Ulrich Beck (1992), sostiene que el avance tecnológico genera una serie de riesgos que son difíciles de prever o controlar, y que en muchos casos, las regulaciones no logran ponerse al día con el ritmo del desarrollo tecnológico. En el contexto del espionaje digital, esta teoría es relevante para entender cómo el uso de malware y spyware en Colombia ha incrementado los riesgos de vulnerabilidad de datos sin que exista un marco legal y técnico suficiente para prevenir estas amenazas (Morozov, 2013).

Aplicar esta teoría a la investigación permite analizar cómo la creciente dependencia de las tecnologías de información y comunicación en Colombia ha expuesto a las instituciones públicas y privadas a mayores riesgos de interceptación de datos. Además, destaca la necesidad urgente de desarrollar estrategias más proactivas y predictivas en lugar de solo reactivas frente a las amenazas digitales (Zuboff, 2019). La teoría del riesgo tecnológico, por lo tanto, proporciona un enfoque útil para analizar cómo las organizaciones deben adaptarse para mitigar los riesgos asociados con el espionaje digital y las nuevas formas de vulneración de datos.

Teoría de la Vigilancia Digital

La teoría de la vigilancia digital, propuesta por autores como David Lyon (2007), explora el uso de la tecnología para monitorear y controlar la información de las personas y cómo esto

afecta su libertad y privacidad. La vigilancia digital, a través de medios como el espionaje digital y las interceptaciones no autorizadas, representa una amenaza significativa para los derechos fundamentales. Esta teoría sostiene que la digitalización ha permitido la expansión masiva de las capacidades de vigilancia tanto por parte de actores gubernamentales como privados, lo que ha llevado a una erosión de las barreras tradicionales que protegían la privacidad (Bennett, 2008).

En el contexto colombiano, la vigilancia digital y el espionaje electrónico se han convertido en herramientas utilizadas para acceder a datos sensibles sin el conocimiento de los individuos afectados. Esta teoría es crucial para examinar cómo el espionaje digital afecta no solo la privacidad personal, sino también la confianza en las instituciones y la legitimidad de las acciones gubernamentales. Además, la vigilancia masiva plantea dilemas éticos y políticos sobre los límites del uso de tecnologías de monitoreo en una sociedad democrática (Aldrich, 2016). Al aplicar esta teoría, se puede explorar cómo las políticas de ciberseguridad deben ser diseñadas no solo para proteger datos, sino también para garantizar que los mecanismos de vigilancia respeten los derechos fundamentales.

Teoría del Capital de Datos

La teoría del capital de datos, desarrollada por Shoshana Zuboff (2019), plantea que los datos personales y corporativos han adquirido un valor económico inmenso en la era digital, lo que ha dado lugar a un capitalismo de vigilancia donde los datos son el recurso más preciado. Esta teoría argumenta que las empresas y los gobiernos han comenzado a explotar los datos personales para obtener ventajas económicas y estratégicas, a menudo sin el conocimiento o consentimiento de los individuos.

Aplicar esta teoría al contexto del espionaje digital en Colombia es crucial para entender cómo los datos interceptados a través de técnicas de espionaje pueden ser utilizados no solo para

fines criminales, sino también para obtener una ventaja económica en mercados altamente competitivos. Esto genera una dinámica en la que la protección de datos se convierte no solo en una cuestión de seguridad, sino también de economía política. Desde esta perspectiva, la investigación puede profundizar en la necesidad de fortalecer las normativas que regulan el acceso, uso y comercialización de datos obtenidos de manera ilícita, así como en el papel que juegan las políticas de protección de datos en la mitigación del espionaje digital (Zuboff, 2019).

Marco Normativo

Tabla 1

Marco Normativo

Norma	Número y Año	Descripción	Ámbito de Aplicación
Ley de Protección de Datos Personales	Ley 1581 de 2012	Establece el régimen general de protección de datos personales en Colombia y regula su tratamiento por parte de entidades públicas y privadas.	Protección de datos personales y privacidad.
Ley de Delitos Informáticos	Ley 1273 de 2009	Modifica el Código Penal para incluir delitos informáticos y protege la información y los datos almacenados en sistemas informáticos.	Seguridad digital y sanción de delitos informáticos.
Ley de Inteligencia y Contrainteligencia	Ley 1621 de 2013	Regula las actividades de inteligencia y contrainteligencia en el país, estableciendo límites y mecanismos de control para evitar abusos.	Vigilancia y protección contra el espionaje digital.
Ley TIC (Modernización del Sector TIC)	Ley 1978 de 2019	Reorganiza la regulación de las telecomunicaciones y establece medidas para fortalecer la seguridad digital.	Telecomunicaciones y ciberseguridad.
Ley de Seguridad y Defensa Nacional	Ley 1097 de 2006	Define estrategias de seguridad y defensa nacional, incluyendo aspectos relacionados con la ciberseguridad.	Protección de infraestructura crítica digital.
Decreto Único Reglamentario del Sector TIC	Decreto 1078 de 2015	Regula el uso de tecnologías de la información y la implementación de políticas de seguridad digital en Colombia.	Políticas de ciberseguridad en el sector público.
Decreto de Política de Seguridad Digital	Decreto 338 de 2022	Establece lineamientos estratégicos para la ciberseguridad	Estrategia nacional de ciberseguridad.

		y define roles y responsabilidades de las entidades públicas.	
Decreto sobre Protección de Infraestructura Crítica	Decreto 256 de 2014	Define medidas de seguridad para proteger la infraestructura crítica del país ante amenazas cibernéticas.	Protección de sectores estratégicos contra ataques digitales.
Resolución sobre Protección de Datos Personales	Resolución 76434 de 2012 (SIC)	Regula la administración y tratamiento de datos personales por parte de empresas y entidades públicas.	Protección de la privacidad y datos personales.
Resolución sobre Ciberseguridad en el Sector Financiero	Resolución 462 de 2018 (Superfinanciera)	Establece obligaciones para entidades financieras en la implementación de protocolos de ciberseguridad.	Protección de datos financieros y bancarios.
Sentencia sobre Habeas Data y Protección de Datos Personales	Sentencia C-748 de 2011 (Corte Constitucional)	Declara la importancia del derecho al habeas data y la protección de información personal frente a abusos de terceros.	Protección del derecho a la privacidad y datos personales.
Sentencia sobre Vigilancia y Derechos Fundamentales	Sentencia C-540 de 2012 (Corte Constitucional)	Analiza los límites legales de la vigilancia digital y el acceso a información privada por parte del Estado.	Derechos fundamentales y límites de la vigilancia digital.
Sentencia sobre Interceptaciones Ilegales	Sentencia C-301 de 2016 (Corte Constitucional)	Establece lineamientos para evitar interceptaciones ilegales de comunicaciones en Colombia.	Protección de la privacidad y control de actividades de inteligencia.
Sentencia sobre Responsabilidad en Protección de Datos	Sentencia T-043 de 2018 (Corte Constitucional)	Determina la responsabilidad de empresas y entidades en el tratamiento de datos personales y fija obligaciones en ciberseguridad.	Protección de datos personales y responsabilidad empresarial.

Fuente: Elaboración propia

Metodología

Diseño de Investigación

El diseño de investigación es de tipo descriptivo, ya que busca caracterizar las vulnerabilidades de la ciberseguridad en Colombia frente al espionaje digital y la protección de datos personales y corporativos. Según Sampieri et al. (2018), la investigación descriptiva permite especificar propiedades, características y perfiles de un fenómeno con el propósito de obtener una visión detallada de su comportamiento en un contexto determinado. En este caso, se describe la problemática del espionaje digital a partir del análisis de normativas, estrategias de protección y casos documentados de vulneraciones a la seguridad informática en el país.

Este diseño posibilita la identificación de patrones y tendencias en el uso de software malicioso como spyware y malware, así como la evaluación de las medidas de protección implementadas en Colombia. A diferencia de una investigación meramente exploratoria, el enfoque descriptivo permite no solo reconocer la existencia del problema, sino también detallar sus manifestaciones, actores involucrados y consecuencias en distintos ámbitos, tanto a nivel individual como corporativo.

Asimismo, la investigación descriptiva facilita el análisis de las brechas en la legislación vigente en materia de ciberseguridad y protección de datos, permitiendo contrastarlas con estándares internacionales y mejores prácticas en el ámbito de la seguridad digital. Con este enfoque, se pretende proporcionar una visión estructurada del estado actual de la ciberseguridad en Colombia y aportar información relevante para el desarrollo de estrategias más efectivas en la prevención del espionaje digital.

Enfoque de Investigación

El enfoque de investigación es cualitativo, ya que se centra en el análisis documental de normativas, estudios de caso, informes gubernamentales y literatura especializada en ciberseguridad. Según Sampieri et al. (2018), el enfoque cualitativo permite interpretar datos desde una perspectiva contextual, facilitando la comprensión de dinámicas y tendencias en fenómenos sociales y tecnológicos. A través de este enfoque, se analizan los principales riesgos de espionaje digital en Colombia, así como las estrategias utilizadas para mitigarlos. Además, se examina el marco normativo vigente para determinar su efectividad frente a las amenazas digitales en constante evolución.

Población y Muestra

La población de estudio está conformada por documentos oficiales, normativas, informes de organismos nacionales e internacionales, estudios académicos y casos documentados sobre ciberseguridad y espionaje digital en Colombia. Dado que esta investigación es de carácter documental, no se incluyen individuos como sujetos de estudio, sino que se analizan fuentes secundarias relevantes para la problemática abordada.

La muestra es de tipo no probabilística y se selecciona de manera intencional, priorizando aquellas fuentes que aportan información clave sobre la ciberseguridad y la protección de datos en Colombia. Según Sampieri et al. (2018), el muestreo intencional es adecuado en estudios cualitativos, ya que permite seleccionar información relevante para alcanzar los objetivos de la investigación. La muestra incluye normativas como la Ley 1581 de 2012 sobre protección de datos personales (Congreso de Colombia, 2012), informes de ciberseguridad, estudios de caso sobre ataques digitales en el país y literatura académica especializada en espionaje digital y privacidad de datos.

Instrumentos de Recolección de Información

La investigación emplea el análisis documental como principal técnica de recolección de información. De acuerdo con Sampieri et al. (2018), el análisis documental permite examinar fuentes escritas con el fin de extraer datos relevantes y estructurar el conocimiento en torno a un problema de estudio. En este caso, se analizan documentos legales, informes de instituciones gubernamentales y organismos internacionales, artículos académicos y reportes especializados en ciberseguridad.

El proceso de análisis se lleva a cabo mediante una revisión sistemática de la información recopilada, identificando patrones, tendencias y posibles brechas en la protección de datos en Colombia. Se comparan las políticas y regulaciones existentes con las estrategias implementadas en otros países, con el fin de extraer recomendaciones aplicables al contexto colombiano. Además, se estudian casos de espionaje digital documentados en el país para identificar las principales técnicas utilizadas y evaluar la respuesta institucional frente a estas amenazas.

Tabla 2

Matriz de Análisis Documental

Objetivo Específico	Categorías Temáticas	Subcategorías	Fuentes de Información	Criterios de Análisis
1. Describir las principales vulnerabilidades de los puntos de conexión en Colombia frente al espionaje digital y el uso de software malicioso.	Vulnerabilidades técnicas	- Puntos de conexión débiles (routers, redes WiFi, IoT)- Configuraciones inseguras- Ausencia de protocolos de seguridad	- Informes de MinTIC y CERT Colombia- Estudios de caso en medios especializados (Andrómeda, Pegasus)- Artículos de ciberseguridad de journals como *Revista Colombiana de Computación* o *IEEE*	- Relevancia contextual (situación colombiana)- Verificabilidad del caso (fuentes cruzadas)- Vigencia (última década)- Nivel de detalle técnico
	Software malicioso	- Tipos de malware: spyware, ransomware, troyanos- Mecanismos de infección- Casos de uso documentados	- Informes de empresas de ciberseguridad (ESET, Kaspersky, TrendMicro)- Reportes de CSIRT o equipos de respuesta a incidentes- Noticias de prensa verificable (El Espectador, La Silla Vacía)	- Fiabilidad técnica- Precisión en la descripción del ataque- Fuente reconocida en el ámbito digital
	Impacto sobre personas y organizaciones	- Robo de datos- Interrupción de operaciones- Pérdida reputacional	- Informes de ONGs digitales (Fundación Karisma)- Testimonios documentados en medios- Denuncias ante entes de control (SIC, Fiscalía)	- Documentación del impacto- Coherencia con otros registros- Valor probatorio o de referencia pública
2. Examinar las políticas y regulaciones actuales en ciberseguridad en Colombia, identificando brechas específicas relacionadas con la	Marco normativo colombiano	- Leyes sobre datos personales, delitos informáticos, inteligencia- Sentencias constitucionales sobre privacidad	- Ley 1581 de 2012- Ley 1273 de 2009- Ley 1621 de 2013- Decreto 338 de 2022- Sentencias C-748/11, C-540/12, T-043/18	- Vigencia y aplicabilidad- Jurisprudencia relevante- Cobertura temática- Mecanismos de control establecidos

protección de los puntos de conexión y los datos personales.	Brechas y vacíos legales	- Falta de regulación del spyware- Falta de control a herramientas de vigilancia- Limitada supervisión estatal	- Análisis doctrinal (artículos legales y académicos)- Informes de la Fundación Karisma- Opiniones expertas en medios jurídicos	- Identificación clara de vacíos- Pertinencia legal- Fundamentación doctrinal- Correspondencia con casos prácticos
	Comparación con estándares internacionales	- Buenas prácticas en Europa y EE.UU.- Normativa de la UE (RGPD)- Modelos de gobernanza digital	- Documentos de la OCDE- Regulaciones europeas (GDPR)- Reportes del BID y la OEA sobre ciberseguridad	- Aplicabilidad al contexto colombiano- Reconocimiento internacional- Comparabilidad estructurada- Innovación normativa
	Herramientas tecnológicas	- Firewalls, antivirus, cifrado, SIEM, sistemas de detección de intrusos- Software de protección de endpoints	- Informes de ESET, Fortinet, Cisco- Reportes técnicos del sector financiero (Asobancaria)- Lineamientos de MinTIC, Superfinanciera	- Nivel de adopción en Colombia- Reconocimiento de la tecnología en el sector- Resultados documentados en mitigación de amenazas
3. Identificar las herramientas tecnológicas y prácticas de seguridad implementadas en los puntos de conexión, señalando sus capacidades y limitaciones frente a amenazas de espionaje digital.	Prácticas institucionales	- Protocolos de respuesta a incidentes- Auditorías internas- Planes de continuidad operativa	- Manuales de gestión de seguridad en entidades públicas- Normas ISO 27001 y su implementación- Informes de auditoría digital (Contraloría, organismos de control)	- Evidencia de implementación- Eficacia operativa- Adaptación al riesgo local
	Capacitación y cultura organizacional	- Formación del talento humano- Concienciación en buenas prácticas- Campañas internas	- Planes de formación institucional (Escuela Superior de Administración Pública, Sena)- Informes de recursos humanos en empresas- Encuestas o estudios sobre cultura digital	- Cobertura poblacional- Periodicidad- Impacto evaluado- Integración con políticas de TI

En el desarrollo de esta investigación, orientada al análisis de las vulnerabilidades en los puntos de conexión frente al espionaje digital en Colombia, se aplican criterios explícitos de validación de fuentes que permiten establecer una base documental consistente y pertinente. El primer criterio corresponde a la actualidad de la publicación, dado que las transformaciones en las amenazas digitales requieren el uso de documentos que reflejen el estado reciente del entorno tecnológico y normativo. Por esta razón, se seleccionan fuentes publicadas en los últimos diez años, con prioridad para aquellas generadas a partir del año 2020.

El segundo criterio se refiere a la relevancia temática, que implica incluir únicamente fuentes relacionadas de forma directa con los ejes de análisis, como el espionaje digital, el uso de software malicioso, la protección de datos y la ciberseguridad en el contexto colombiano. Otro criterio aplicado es el reconocimiento o autoridad de la fuente, que exige que los documentos provengan de entidades con competencia en el área, tales como el Ministerio de Tecnologías de la Información y las Comunicaciones, la Superintendencia de Industria y Comercio, la Organización de los Estados Americanos, organismos multilaterales, instituciones académicas o empresas con trayectoria en seguridad informática. Estos criterios permiten mantener la trazabilidad metodológica entre los objetivos planteados y los datos empleados en el proceso analítico.

Criterios de Validación de Fuentes

Las fuentes utilizadas en el análisis documental fueron seleccionadas a partir de criterios de validación que garantizan su pertinencia y confiabilidad. Se priorizó la actualidad de las publicaciones, restringiendo el corpus a materiales producidos entre los años 2020 y 2025, con el fin de reflejar el estado reciente de la ciberseguridad en Colombia y el avance de las amenazas vinculadas al espionaje digital. Asimismo, se valoró la autoridad institucional y técnica de los

emisores, incluyendo organismos nacionales e internacionales reconocidos, como el Ministerio de Tecnologías de la Información y las Comunicaciones, la Superintendencia de Industria y Comercio, ColCERT, la Cámara Colombiana de Informática y Telecomunicaciones, así como entidades expertas como Fortinet, Kaspersky, el Consejo de la Unión Europea o el PCI Security Standards Council. Finalmente, se aseguró la relevancia temática, seleccionando exclusivamente fuentes que respondieran a las categorías definidas en la matriz de análisis: vulnerabilidades técnicas, brechas normativas, herramientas de protección y prácticas organizacionales. Esta selección rigurosa excluyó blogs, foros, artículos sin revisión por pares o medios sin respaldo institucional, con el propósito de mantener la integridad metodológica del estudio.

Resultados

Descripción de las Principales Vulnerabilidades de los Puntos de Conexión en Colombia

Vulnerabilidades Técnicas y de Configuración

Las vulnerabilidades presentes en los puntos de conexión dentro de las redes digitales colombianas constituyen condiciones clave que permiten la ejecución de actividades de espionaje mediante software malicioso. Estas debilidades técnicas incluyen configuraciones predeterminadas, protocolos inseguros y falta de actualizaciones en dispositivos críticos. La Organización de los Estados Americanos, en colaboración con el Banco Interamericano de Desarrollo, señaló que una proporción significativa de pequeñas y medianas empresas, así como una gran parte de los usuarios domésticos en Colombia, opera con dispositivos configurados con contraseñas genéricas, firmware desactualizado y sin segmentación de red adecuada. Estas prácticas aumentan la exposición a intrusiones remotas, facilitan el acceso no autorizado a las redes y comprometen la integridad del sistema informático en su conjunto (OEA & BID, 2020).

Según el informe de Fortinet (2024), Colombia registró más de once mil millones de intentos de ciberataques en 2023, muchos dirigidos a dispositivos del Internet de las Cosas (IoT). Estos equipos suelen carecer de mecanismos de actualización automática y de controles de seguridad del nivel exigido para entornos empresariales. La falta de soporte de parches o cifrado de comunicaciones hace de estos dispositivos un vector de entrada habitual para amenazas persistentes, como spyware, que permanecen invisibles al usuario. Este tipo de vulnerabilidad estructural no se limita a entornos privados; afecta también a sistemas organizacionales interconectados, donde una única brecha puede extenderse a dominios múltiples dentro del ecosistema digital.

El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC, 2023) ha identificado riesgos derivados del uso de redes inalámbricas abiertas, carentes de cifrado fuerte. Estas redes, comunes en espacios públicos como bibliotecas, plazas o estaciones de transporte, facilitan ataques de intermediación (man-in-the-middle) que interceptan comunicaciones entre dispositivos y servidores. Esta exposición permite la captura de credenciales, información sensible y paquetes de autenticación sin necesidad de comprometer directamente el sistema del usuario.

El CSIRT del Gobierno de Colombia ha documentado amenazas frecuentes como ransomware, troyanos de acceso remoto (RAT) y spyware, comúnmente distribuidos mediante campañas de suplantación. Estas campañas imitan la identidad visual de instituciones oficiales como la Dirección de Impuestos y Aduanas Nacionales o la Fiscalía General de la Nación. Este tipo de ingeniería social incorpora lenguaje técnico y jurídico contextualizado que incrementa la tasa de interacción por parte de los destinatarios, facilitando el despliegue de archivos maliciosos o la entrega voluntaria de credenciales (CSIRT GOB, 2024).

El grupo de análisis de amenazas de Google ha registrado el uso creciente de programas espía como Predator y Hermit, comercializados en el mercado negro y capaces de operar con privilegios avanzados en dispositivos móviles. Estas herramientas permiten el acceso a micrófonos, cámaras, mensajes y datos de geolocalización, sin necesidad de intervención técnica del usuario ni activación visible. Su proliferación ha democratizado capacidades de vigilancia anteriormente reservadas a agencias estatales, modificando de forma sustancial el panorama de amenazas digitales (Google TAG, 2023).

Vulnerabilidades Humanas y de Comportamiento Digital

Más allá de la configuración técnica, las vulnerabilidades humanas son un factor decisivo en la materialización de ataques. La Superintendencia de Industria y Comercio (2023) ha reportado un incremento sostenido en las denuncias por violación al habeas data. Muchas de estas violaciones se originan en accesos no autorizados habilitados por los propios usuarios, quienes sin saberlo entregan información crítica a través de interacciones digitales con correos, enlaces o archivos maliciosos. El software espía que opera de forma encubierta tiene la capacidad de recopilar datos sin activar alarmas perceptibles, lo que impide la identificación temprana del ataque.

Según el estudio de Cabrera y Torres (2022), publicado en la Revista Colombiana de Computación, una parte significativa de las vulneraciones ocurre por malas prácticas en la gestión de contraseñas, como la reutilización en múltiples plataformas, el almacenamiento en texto plano o el intercambio vía medios inseguros. Además, la falta de una cultura de actualización y el uso prolongado de dispositivos sin soporte incrementan el riesgo de ser blanco de *exploits* conocidos y técnicas automatizadas de escaneo.

En el sector financiero, la Asociación Bancaria y de Entidades Financieras de Colombia (Asobancaria, 2024) ha advertido sobre el crecimiento de los incidentes de ransomware. Estos ataques provocan interrupciones de servicios, pérdida de información sensible y daños reputacionales. Aunque las inversiones en ciberseguridad han aumentado, la evolución de las amenazas sobrepasa en muchos casos la capacidad de respuesta institucional. El mismo informe advierte que la capacitación en prácticas seguras es discontinua o inexistente en un porcentaje relevante de las organizaciones medianas, lo que limita la efectividad de las herramientas tecnológicas implementadas.

La Universidad Nacional Abierta y a Distancia (UNAD, 2023) documentó cómo en el sector salud, los profesionales tienden a priorizar la funcionalidad operativa sobre las buenas prácticas digitales. Esto se traduce en contraseñas escritas en papel, acceso compartido a estaciones de trabajo y dispositivos conectados que permanecen sin supervisión física. Estas condiciones han sido explotadas por actores maliciosos para desplegar spyware que monitorea rutinas, historiales clínicos y movimientos administrativos. La combinación de exposición física y descuido digital amplifica el potencial de espionaje y uso indebido de la información.

Vulnerabilidades Institucionales y Normativas

Las capacidades institucionales para prevenir y responder a las amenazas descritas presentan limitaciones. Aunque Colombia cuenta con un marco normativo como la Ley 1273 de 2009 y la Ley 1581 de 2012, las brechas de implementación persisten. La falta de coordinación entre entidades públicas y privadas, sumada a una fiscalización limitada, permite que muchos actores operen sin estándares básicos de ciberseguridad. La Red de Ciberseguridad de Colombia (Redciber, 2025) advirtió que más del 60% de las alcaldías no han actualizado sus políticas de seguridad desde 2018.

El Documento CONPES 3854 y el Modelo de Seguridad y Privacidad de la Información (MSPI) establecen lineamientos técnicos exigibles a las entidades públicas. Sin embargo, su implementación efectiva depende de recursos técnicos y humanos que no siempre están disponibles, especialmente en niveles subnacionales. Según la Auditoría General de la República (2024), el cumplimiento parcial o nulo de los controles establecidos afecta la trazabilidad de incidentes y la generación de alertas oportunas en sistemas de monitoreo.

Martínez y Suárez (2023), en un artículo para IEEE Latin America Transactions, señalaron que la adopción de tecnologías como EDR y SIEM está condicionada por costos

operativos, complejidad de integración y déficit de talento especializado. Incluso en los casos en que se despliegan soluciones avanzadas, los errores de configuración y la falta de monitoreo continuo abren brechas que pueden ser explotadas por atacantes. En sus pruebas de campo, encontraron entornos con microsegmentación mal aplicada, reglas de firewall redundantes y protocolos inseguros habilitados por defecto.

El Instituto Nacional de Metrología (2025) alertó sobre la inexistencia de catálogos actualizados de activos tecnológicos en instituciones educativas y de salud. Esta carencia impide saber qué dispositivos están conectados a la red, qué servicios ofrecen y qué vulnerabilidades presentan. Esta invisibilidad técnica afecta la gestión de riesgos y limita la capacidad de respuesta ante incidentes. La solución propuesta incluye escaneo pasivo de redes, identificación por firmas digitales y correlación de tráfico en tiempo real mediante plataformas SIEM.

Proliferación de Herramientas de Espionaje y Nuevas Dinámicas de Riesgo

Una de las transformaciones más relevantes del contexto actual es la expansión del acceso a herramientas de espionaje avanzadas. La comercialización de software con funciones de vigilancia —como Pegasus, Predator o Hermit— ya no se limita a gobiernos. Diversos reportes de Citizen Lab (2022) y Google TAG (2023) confirman que empresas privadas, grupos de presión y actores del crimen organizado han adquirido estas herramientas y las utilizan para monitorear opositores, periodistas y directivos corporativos. Esta distribución descentralizada de capacidades incrementa el riesgo de espionaje dirigido y la explotación de vulnerabilidades individuales.

El Centro Europeo de Ciberseguridad Industrial (ENISA, 2023) advierte sobre el uso de Shodan, un motor de búsqueda que permite identificar dispositivos expuestos, como cámaras, routers o servidores sin autenticación. En Colombia, S2 Grupo (2022) identificó más de 700

activos pertenecientes a infraestructura crítica con puertos abiertos y sin protección, hallazgos que fueron confirmados por el CSIRT nacional. Esta exposición multiplica el número de vectores potenciales de intrusión y pone en riesgo la continuidad operativa de servicios esenciales.

La vulnerabilidad de la cadena de suministro digital representa otra dimensión crítica. La Resolución 02277 de 2025 del MinTIC exige a las entidades mantener un inventario de componentes software por dispositivo (Software Bill of Materials), con el fin de identificar bibliotecas vulnerables o código heredado. Esta medida busca prevenir escenarios como el de Log4Shell, que afectó a múltiples entidades colombianas al explotar una falla en una biblioteca ampliamente distribuida.

La falta de auditorías independientes, simulacros técnicos y capacitación continua profundiza estas debilidades. Aunque se han emitido guías de buenas prácticas, su adopción es dispareja y depende de la capacidad de cada entidad. Mientras algunas organizaciones cuentan con Blue Teams y pruebas de penetración periódicas, otras operan sin procedimientos formales para la gestión de incidentes. Esta asimetría organizacional genera una superficie de ataque heterogénea, donde los atacantes pueden identificar y explotar los nodos más débiles con relativa facilidad.

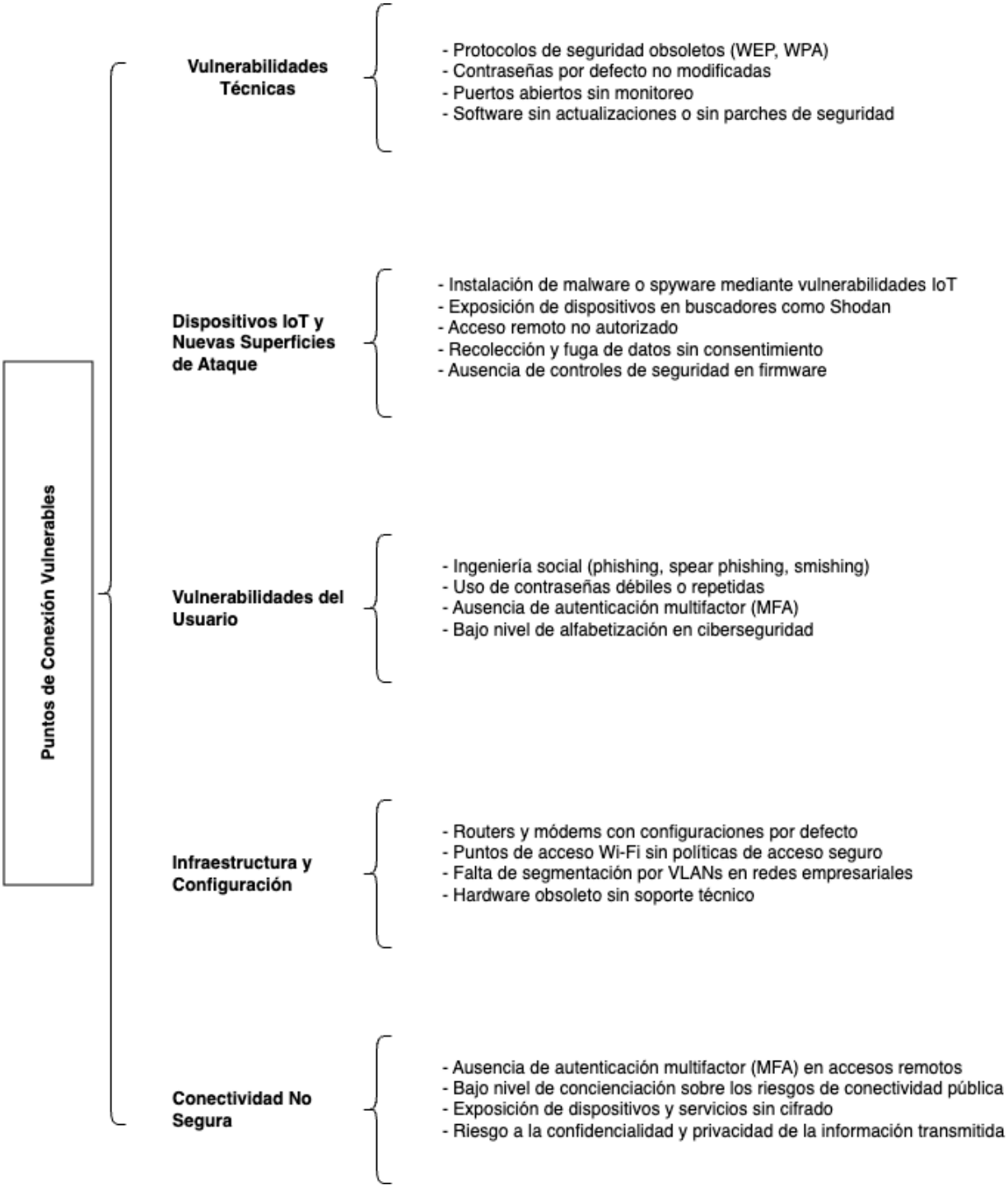
Consideraciones Para la Respuesta Estructural

El análisis de las vulnerabilidades descritas permite identificar una convergencia entre fallas técnicas, debilidades humanas y vacíos normativos. Esta combinación configura un entorno de exposición estructural que facilita la ejecución de espionaje digital a gran escala. La interdependencia de los sistemas de información implica que una vulnerabilidad localizada puede amplificarse rápidamente en redes interconectadas, afectando datos, servicios y procesos críticos.

Ante esta situación, se requiere una respuesta estructurada que articule tecnología, capacitación y gobernanza. Las medidas aisladas o reactivas no son suficientes. La implementación efectiva del Modelo de Seguridad y Privacidad de la Información, la formación especializada en ciberseguridad y la supervisión técnica continua deben integrarse en una estrategia nacional coherente. Esto implica asignar recursos adecuados, coordinar acciones entre sectores y establecer mecanismos de auditoría basados en métricas técnicas y de cumplimiento normativo.

Figura 1

Vulnerabilidades de los Puntos de Conexión en Colombia frente al Espionaje Digital



A partir de la Figura 1, es notable que las vulnerabilidades de los puntos de conexión en Colombia no responden a un único factor aislado, sino a una combinación de debilidades

técnicas, humanas, de infraestructura y de gestión de conectividad. Esta clasificación permite observar cómo los riesgos se distribuyen a lo largo del ecosistema digital, desde fallos básicos como el uso de contraseñas predeterminadas o software sin parches, hasta fenómenos más complejos como la exposición de dispositivos IoT en buscadores especializados y la ausencia de segmentación por VLANs en redes empresariales. La figura evidencia que la seguridad no puede abordarse exclusivamente desde la tecnología, ya que aspectos como la alfabetización en ciberseguridad o la falta de controles en firmware representan puntos de entrada igualmente críticos. Asimismo, la conectividad no segura, especialmente en entornos públicos, amplifica la superficie de ataque al facilitar la intercepción de datos en tránsito. Esta visión integral obliga a entender los puntos de conexión no solo como objetos técnicos, sino como nodos en un sistema sociotécnico donde confluyen prácticas, decisiones institucionales y capacidades dispares de respuesta.

Examen de las Políticas y Regulaciones Actuales en Ciberseguridad en Colombia

Contexto de la Incidencia

Durante el primer semestre de 2024, el Ministerio de Tecnologías de la Información y las Comunicaciones reportó un total de 20.000 millones de intentos de ciberataque contra infraestructuras digitales ubicadas en territorio colombiano, cifra divulgada en el boletín sectorial sobre ciberseguridad publicado por la entidad (Ministerio de Tecnologías de la Información y las Comunicaciones, 2024). Esta magnitud representa un incremento sostenido en comparación con años previos y expone la presión constante que enfrentan tanto las redes públicas como privadas. En términos de impacto directo, la Policía Nacional de Colombia registró 77.866 denuncias formales por delitos informáticos entre enero y mayo del mismo año, valor que representa un crecimiento de 23% frente al acumulado del periodo equivalente en 2023 (Policía Nacional de Colombia, 2025). La misma fuente indicó que los delitos más frecuentes incluyen acceso abusivo a sistemas informáticos, interceptación de datos personales, sabotaje informático y hurto por medios digitales, lo que indica una diversificación de métodos delictivos y de actores involucrados.

El Ministerio de Tecnologías de la Información y las Comunicaciones (2024) también señaló una variación anual del setenta por ciento en los registros de amenaza procesados por los centros de respuesta a incidentes, lo que refleja una evolución acelerada de los vectores de ataque y un incremento en la sofisticación de los métodos empleados. La mayoría de estos incidentes se relaciona con vulnerabilidades presentes en puntos de conexión, entre ellos redes domésticas, entornos corporativos y plataformas de entidades gubernamentales. Este patrón afecta tanto a usuarios individuales como a organizaciones del sector público y privado. En particular, el Banco de la República documentó una interrupción del sistema de pagos interbancarios ocasionada por

un evento de ransomware, situación que afectó la operatividad durante un lapso superior a tres horas consecutivas (Banco de la República, 2024). Este incidente evidencia que incluso los nodos considerados críticos dentro del sistema económico nacional presentan deficiencias en materia de blindaje digital.

El mismo fenómeno también afecta la seguridad del ecosistema empresarial. Según la Cámara Colombiana de Informática y Telecomunicaciones, entre los años 2022 y 2024, el 46% de las empresas con operación continua en Colombia sufrió al menos un incidente de fuga o exfiltración de datos, lo que se traduce en una afectación directa sobre la privacidad de clientes, la propiedad intelectual corporativa y el cumplimiento de las normativas legales vigentes (Cámara Colombiana de Informática y Telecomunicaciones, 2024). Estos registros indican que existe una correlación entre la frecuencia de ataques, la insuficiencia de controles en los puntos de acceso y la debilidad estructural del marco normativo. En ese sentido, el contexto actual demanda una revisión exhaustiva de las leyes, decretos y políticas vigentes en materia de ciberseguridad, con énfasis en la identificación de brechas jurídicas, técnicas y operativas asociadas al uso de dispositivos finales, redes expuestas y tratamiento de datos personales y corporativos.

Alcance Penal y Normativa Básica

La incorporación del bien jurídico denominado protección de la información y de los datos al Código Penal colombiano se formalizó mediante la Ley 1273 de 2009. Esta normativa estableció penas privativas de la libertad de entre cuatro y diez años para conductas como el acceso abusivo a sistemas informáticos, el daño informático y el uso no autorizado de software, según la Secretaría del Senado (2009). A pesar de la tipificación formal, la Fiscalía General de la Nación (2024) señaló que el porcentaje de sentencias condenatorias por estos delitos se mantiene

por debajo del diez por ciento, lo que pone en evidencia una brecha entre la formulación legal y su aplicación efectiva en el ámbito judicial. La baja judicialización, aun frente a un volumen creciente de incidentes, cuestiona la eficacia real del marco penal existente.

El análisis técnico realizado por Delta Asesores (2021) plantea que la Ley 1273 presenta vacíos relevantes, al omitir referencias expresas a modalidades contemporáneas como el ransomware, el secuestro de servicio o los dispositivos conectados a redes del tipo Internet de las Cosas. Esta omisión impide en muchos casos una imputación precisa, lo que favorece una zona gris de impunidad penal frente a estos actos. La Policía Nacional de Colombia (2025) informó que durante el año 2024 se registraron 37.409 casos de hurto mediante medios informáticos y 4.705 casos vinculados a la violación de datos personales, lo que confirma la magnitud del fenómeno delictivo digital. En ese mismo sentido, Fortinet (2023) advirtió que la legislación vigente no contempla modalidades de ataque asociadas a la manipulación de credenciales o al acceso mediante federación de identidades, una técnica empleada en más del setenta por ciento de los ciberataques documentados a escala internacional.

El Documento CONPES 3854 de 2016 delineó los principios de la política nacional de seguridad digital, estableció objetivos de gestión del riesgo y promovió la cooperación sectorial en la protección de infraestructuras críticas. El Departamento Nacional de Planeación (2016) afirmó que el modelo propuesto exige la existencia de mecanismos concretos de inspección, seguimiento y sanción que funcionen de manera articulada entre los diferentes niveles institucionales. A partir del Decreto 338 de 2022 se formalizó la creación del Equipo de Respuesta a Incidentes de Seguridad Digital del Estado colombiano y se impuso la obligación de identificar activos considerados como infraestructura crítica; sin embargo, Redciber (2025) reportó retrasos superiores a doce meses en la actualización de inventarios en al menos siete

sectores estratégicos, lo que impide una visión consolidada del nivel de riesgo. En línea con esa observación, la Superintendencia de Servicios Públicos (2024) informó que cuarenta y seis empresas estatales no han completado el proceso de caracterización de activos digitales, lo cual obstaculiza la formulación de mapas de riesgo y limita las posibilidades de respuesta oportuna ante incidentes.

La evidencia recogida por Enter.co (2024) indica que el setenta y uno por ciento de los ataques digitales a nivel global se originan en identidades comprometidas, una tendencia que también se presenta en Colombia. Kaspersky (2024) informó que el noventa y seis por ciento de los casos de ransomware verificados en el país durante 2023 y 2024 tienen como punto de partida el uso de credenciales previamente expuestas en entornos digitales, lo que refuerza la necesidad de adoptar estándares avanzados en gestión de identidad y control de acceso. La coordinación entre los organismos responsables de la seguridad digital forma parte del mandato normativo establecido en el Decreto 338. No obstante, durante una sesión pública, el Equipo de Respuesta a Incidentes del Estado admitió que el flujo de información entre agencias tardó cuarenta y ocho horas en alcanzar a los equipos del sector salud durante el incidente que comprometió a la empresa IFX Networks en 2023, hecho que comprometió servicios esenciales de justicia, pensiones y atención médica (ColCERT, 2023).

El Ministerio de Tecnologías de la Información y las Comunicaciones (2021) elaboró la Guía para la Gestión y Clasificación de Incidentes, la cual define un protocolo de cuatro fases e incluye requerimientos como el registro completo de sesiones. A pesar de esta disposición, la Auditoría General de la República (2024) encontró inconsistencias en los registros de hora y origen en el treinta y ocho por ciento de los expedientes examinados. La deficiencia en los mecanismos de trazabilidad compromete la eficacia de las medidas de contención y dificulta la

identificación de los vectores de ataque. Fortinet (2023) indicó que entre 2021 y 2022 se incrementó en un cincuenta y tres por ciento el número de organizaciones que enfrentaron cinco o más brechas de seguridad, fenómeno que S2 Grupo (2022) atribuyó a un ciclo de corrección promedio de hasta nueve meses para vulnerabilidades previamente divulgadas.

La Resolución 500 de 2021 definió un marco obligatorio de gestión del ciclo de vida de la seguridad de la información para entidades del Estado. La Contraloría General de la República (2023) evaluó el cumplimiento de dicha normativa y detectó que quince de las veinte entidades analizadas presentaban cumplimiento parcial de al menos cinco controles mínimos requeridos. En el ámbito privado, Enter.co (2024) reportó que el cincuenta y ocho por ciento de las organizaciones registraron violaciones de seguridad durante 2023, en su mayoría originadas por configuraciones incorrectas en puntos de conexión. Para enfrentar esta situación, el Ministerio de Tecnologías de la Información y las Comunicaciones (2025) anunció un plan para certificar a diez mil profesionales en ciberseguridad en un periodo de cinco años. No obstante, Fortinet (2023) advirtió que la brecha de personal calificado supera las veintidós mil vacantes, lo que implica que el ritmo de formación previsto no cubriría la demanda real. La Cámara Colombiana de Informática y Telecomunicaciones (2024) recomendó la adopción de incentivos fiscales que faciliten la implementación de sistemas de detección y respuesta (SIEM, EDR) y reveló que solo el veintitrés por ciento de las empresas medianas realiza actividades de monitoreo continuo sobre sus infraestructuras digitales.

Protección de Datos Personales y Notificación de Incidentes

La Ley 1581 de 2012 desarrolló el derecho fundamental de habeas data y definió principios como la seguridad, la transparencia en el tratamiento y el acceso a la información por parte del titular. La Superintendencia de Industria y Comercio (2024) reiteró que toda persona

natural o jurídica que actúe como responsable del tratamiento de datos personales debe notificar cualquier incidente al Registro Nacional de Bases de Datos en un plazo máximo de quince días hábiles contados a partir del momento en que tenga conocimiento del suceso. Este lapso contrasta con el Reglamento General de Protección de Datos de la Unión Europea, que exige la notificación dentro de las primeras setenta y dos horas. La Universidad Nacional de Colombia (2024) ha señalado que esta diferencia normativa genera un desfase temporal que disminuye la capacidad de los titulares para ejercer sus derechos frente a posibles usos indebidos de su información.

El análisis de casos recientes evidencia las consecuencias prácticas de este retraso. El Banco Davivienda notificó a la autoridad una filtración de siete millones de registros diez días después de la detección, periodo durante el cual ya se había producido la reventa de los datos en foros especializados, según el informe emitido por Grupo IB (2024). Este comportamiento institucional, unido al promedio de doscientos nueve días que, según el Ministerio de Tecnologías de la Información y las Comunicaciones (2024), transcurren entre la intrusión inicial y su detección, pone en duda la eficacia del régimen actual de reporte. En entornos como el sector salud, la Universidad Nacional Abierta y a Distancia (2023) identificó que los protocolos de análisis ético y jurídico frente a filtraciones prolongan los tiempos de entrega de la información a la autoridad competente, lo cual habilita al atacante para realizar nuevas intrusiones mientras la vulnerabilidad permanece sin contención.

Los artículos 26 y 27 de la Ley 1581 establecen los parámetros para la transferencia internacional de datos personales, exigiendo que los envíos se realicen únicamente a países que ofrezcan niveles de protección adecuados o que cuenten con cláusulas contractuales equivalentes. No obstante, la Superintendencia de Industria y Comercio (2024) confirmó que

Colombia no ha emitido decisiones de adecuación respecto a países receptores, situación que genera incertidumbre jurídica para las organizaciones que externalizan servicios tecnológicos o utilizan plataformas en la nube. Esta falta de claridad ha motivado que, según la Cámara Colombiana de Informática y Telecomunicaciones (2024), el treinta y dos por ciento de las empresas haya decidido suspender procesos de migración a infraestructura pública. La firma Gartner (2024) informó que en Europa las sanciones por tratamiento inadecuado ascendieron a catorce mil millones de euros durante el año anterior, un antecedente que refuerza la necesidad de revisar el marco normativo nacional para evitar efectos similares.

El informe de Redciber (2025) concluyó que la inexistencia de un sistema de equivalencia normativa formal incrementa el riesgo de repatriación obligatoria de datos por parte de autoridades extranjeras. Este hecho afecta directamente la continuidad operativa de múltiples sectores, en particular aquellos que dependen de flujos internacionales de información. En respuesta a esta preocupación, el Consejo de Estado adoptó una medida cautelar mediante la cual ordenó el bloqueo temporal de intercambios de datos con determinados territorios mientras se analiza el nivel de protección ofrecido, una decisión que pone de manifiesto la dimensión jurídica que adquiere la gestión de puntos de conexión que operan fuera del país (Consejo de Estado, 2024). La ausencia de criterios técnicos y normativos uniformes entre jurisdicciones no solo compromete el cumplimiento legal, sino que limita el desarrollo de modelos de negocio basados en tecnología distribuida y procesamiento en tiempo real.

Articulación normativa con hallazgos de la Matriz de Análisis Documental

Los resultados permiten establecer una correspondencia directa entre las políticas y regulaciones actuales y los hallazgos documentados en la Tabla 2. La revisión del marco legal vigente muestra que persisten vacíos normativos específicos frente a los riesgos identificados en

los puntos de conexión, en particular los vinculados a dispositivos mal configurados, el uso de software espía y las deficiencias en la protección de datos personales.

Uno de los aspectos más relevantes es la falta de regulación específica sobre el uso de spyware y herramientas de vigilancia digital. Esta brecha ha sido señalada en informes doctrinales como los de la Fundación Karisma (2024) y en análisis jurídicos disponibles en medios especializados, los cuales evidencian la ausencia de disposiciones que regulen expresamente este tipo de amenazas. En relación con la Tabla 2, esta situación se asocia con los riesgos vinculados a la recolección de datos sin consentimiento y la ausencia de controles en firmware, lo que ha permitido campañas de espionaje digital sobre infraestructura pública y privada en el país.

De igual forma, la implementación del Decreto 338 de 2022 muestra limitaciones relevantes. Aunque establece la creación de ColCERT y la obligación de identificar infraestructuras críticas, su aplicación práctica ha sido discontinua. Redciber (2025) reporta que siete sectores estratégicos presentan retrasos superiores a doce meses en la entrega de inventarios, lo que debilita la respuesta coordinada ante incidentes. Esta situación se relaciona con la falta de segmentación en redes empresariales y la configuración por defecto de routers y módems, identificadas en la Tabla 2 como elementos de exposición directa a ataques con capacidad de escalar lateralmente.

Las normas penales, como la Ley 1273 de 2009, introdujeron la protección de los datos informáticos en el Código Penal. Sin embargo, la Fiscalía General de la Nación (2024) informó que menos del diez por ciento de los casos llega a sentencia condenatoria, lo cual indica un desajuste entre la legislación y la persecución judicial efectiva. Este hallazgo se conecta con la exposición de dispositivos y servicios sin cifrado y con la debilidad de los mecanismos de

autenticación, también expuestos en la Tabla 2. Las amenazas asociadas al uso de redes públicas sin protección siguen activas, sin que la legislación actual exija controles técnicos mínimos en los puntos de conexión que acceden a información sensible.

En el ámbito de la protección de datos personales, la Ley 1581 de 2012 establece principios generales de seguridad, transparencia y acceso, pero no define parámetros técnicos sobre protección de dispositivos, cifrado de datos en tránsito o autenticación robusta. Las evidencias recogidas en la Tabla 2 muestran que estos elementos son fundamentales para evitar accesos no autorizados, pérdidas de datos y filtraciones de información, especialmente en entornos de alta concurrencia o conectividad compartida.

La comparación con normas internacionales como el Reglamento General de Protección de Datos europeo permite identificar que los estándares de notificación, supervisión y control en Colombia son menos exigentes. El tiempo permitido para notificar una violación de datos alcanza quince días hábiles, frente a las setenta y dos horas que exige el modelo europeo. Esta diferencia reduce la capacidad de respuesta ante incidentes y se refleja en el número de casos en los que la filtración se detecta cuando ya ha ocurrido la exfiltración y procesamiento de la información. La Tabla 2 muestra que la gestión tardía de incidentes es uno de los factores de mayor riesgo en la propagación de software malicioso.

Gestión de Puntos de Conexión y Vulnerabilidades

La revisión técnica de elementos de infraestructura digital en Colombia ha permitido identificar deficiencias persistentes en la gestión de puntos de conexión. La auditoría realizada por S2 Grupo (2022) examinó 759 activos vinculados a servicios críticos y detectó configuraciones con puertos abiertos que ejecutaban servicios sin autenticación, condición que posibilita el desplazamiento lateral dentro de la red una vez se compromete el acceso inicial. Este

tipo de hallazgo refuerza la necesidad de integrar esquemas de monitoreo continuo en dispositivos de borde, especialmente cuando el perímetro incluye recursos compartidos por entidades públicas o privadas con niveles de madurez tecnológica disímiles. El análisis de Kaspersky (2024) señaló que los ataques con ransomware se apoyan en el uso de credenciales robadas y no requieren vulnerabilidades explotables en el software, lo que sitúa a la gestión de identidades como eje estructural de la defensa digital.

El incidente ocurrido en 2023 y atribuido al proveedor IFX Networks fue evaluado por el Equipo Nacional de Respuesta a Incidentes de Seguridad Digital. En su informe, ColCERT (2023) indicó que el vector de ingreso fue una sesión remota sin autenticación multifactor, situación que generó interrupciones simultáneas en servicios de salud, justicia y pensiones. Este tipo de acceso directo sin controles adicionales contradice los principios establecidos en las normas internacionales de gestión de riesgos tecnológicos. Fortinet (2023) reportó que el nivel de implementación de herramientas de detección y respuesta en endpoints en pequeñas y medianas empresas colombianas alcanza apenas el quince por ciento, proporción significativamente inferior al noventa por ciento registrado en entidades financieras que cumplen el estándar PCI-DSS, de acuerdo con el informe técnico del PCI Security Standards Council (2024). Esta diferencia revela asimetrías críticas entre sectores que comparten infraestructura digital, aumentando el riesgo de propagación transfronteriza de incidentes cibernéticos.

La Universidad Javeriana (2024) detalló que la latencia en la aplicación de parches de seguridad sobre servidores con funciones de misión central responde, en parte, a la coincidencia entre las ventanas de mantenimiento y los ciclos de alta demanda. Esta relación genera decisiones administrativas que priorizan la continuidad operativa en detrimento de la actualización preventiva, ampliando la exposición a vectores ya documentados. En su propuesta

de 2025, el Ministerio de Tecnologías de la Información y las Comunicaciones planteó la instalación de una red nacional de centros de operaciones de seguridad de tipo sectorial, orientada a ofrecer vigilancia en tiempo real sobre puntos de conexión expuestos. No obstante, la Oficina Nacional de Presupuesto (2025) no asignó recursos para dicho proyecto durante el primer semestre del año, lo que limita su ejecución inmediata y retrasa el fortalecimiento de capacidades de respuesta coordinada frente a eventos que afectan a múltiples entidades simultáneamente.

Propuesta de Reforma Normativa

La inclusión de nuevas figuras penales en el marco normativo colombiano forma parte de las discusiones legislativas vigentes. Delta Asesores (2021) propuso modificar la Ley 1273 de 2009 para incorporar conductas asociadas al ransomware, al secuestro de servicios digitales y a la manipulación de infraestructura crítica, planteando el aumento de penas cuando el objetivo afecte sectores considerados esenciales. La Universidad del Rosario (2025) planteó la adhesión al Convenio de Budapest con el fin de armonizar las prácticas de cooperación internacional, facilitar el intercambio de evidencia digital entre Estados y fortalecer la capacidad institucional para responder ante actores transfronterizos. Esta propuesta responde a la creciente presión por estandarizar los procedimientos judiciales relacionados con delitos informáticos en línea con marcos supranacionales.

En paralelo, la Cámara Colombiana de Informática y Telecomunicaciones (2024) sugirió la imposición de sanciones administrativas para las organizaciones que pierdan datos personales sin demostrar inversiones preventivas en seguridad, con el propósito de incentivar la adopción de controles técnicos. El Ministerio de Tecnologías de la Información y las Comunicaciones (2025) formuló ante el Consejo de Ministros un proyecto normativo que reduce el plazo de notificación

de incidentes de seguridad a setenta y dos horas, alineado con prácticas del Reglamento General de Protección de Datos de la Unión Europea, e incorpora la exigencia de controles de punto final con base en las directrices ISO/IEC 27035 y los estándares del Center for Internet Security. La Superintendencia de Servicios Públicos (2024) respaldó esta iniciativa mediante la propuesta de inventarios en tiempo real con validación remota a través de interfaces de programación de aplicaciones, eliminando la necesidad de inspección física para verificar parches críticos en sistemas de misión central.

Fortinet (2023) indicó que la técnica de microsegmentación mitiga la propagación de ataques con movimiento lateral, dado que impide el desplazamiento no autorizado entre segmentos de red una vez se compromete un nodo inicial. Esta recomendación fue adoptada en el borrador normativo como requisito obligatorio para operadores de infraestructura esencial, con el objetivo de reducir el impacto técnico de los incidentes. Gartner (2024) estimó que la aplicación sistemática de este tipo de medidas reduce en treinta por ciento el costo promedio de cada evento de seguridad, cifra que el Ministerio de Hacienda (2025) empleó como insumo técnico para argumentar la necesidad de asignación presupuestaria específica en la vigencia 2026. Este conjunto de propuestas articula mecanismos de prevención, respuesta y sanción, y establece una base regulatoria más robusta frente al escenario actual de amenazas digitales.

Identificación de las Herramientas Tecnológicas y Prácticas de Seguridad Implementadas en los Puntos de Conexión

Guías Oficiales del MinTIC: Bases Técnicas Para Proteger los Endpoints

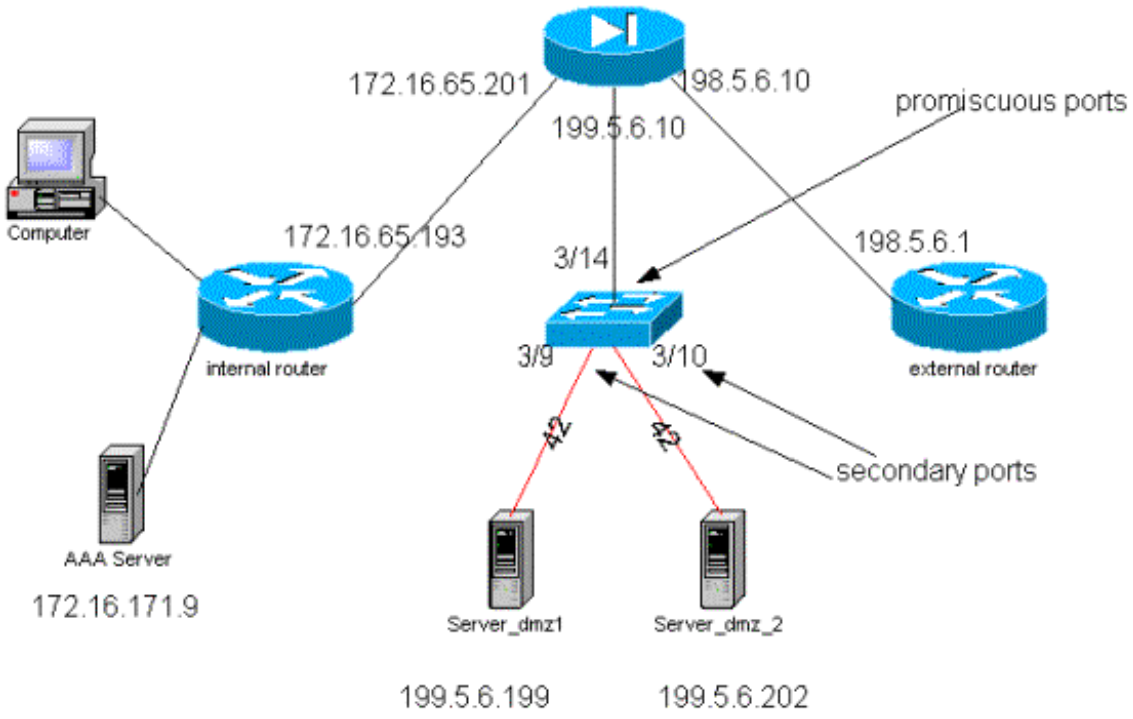
El Ministerio de Tecnologías de la Información y las Comunicaciones señala que la Estrategia Nacional de Seguridad Digital 2025 se formuló con base en un diagnóstico técnico que evidenció una brecha promedio de 217 días entre la intrusión y la detección en los puntos de

conexión del entorno colombiano. En respuesta, la entidad expidió la Resolución 02277 de 2025, la cual actualiza el Modelo de Seguridad y Privacidad de la Información (MSPI) y establece veintiocho controles obligatorios aplicables a dispositivos finales, redes, servidores y sistemas móviles. El documento técnico del MSPI exige que cada punto de conexión emita registros básicos de telemetría, entre los cuales se incluyen el hash del ejecutable, la integridad de memoria y la reputación de la dirección IP; dicha información debe ser canalizada a un sistema de gestión de eventos de seguridad (SIEM) con el fin de detectar patrones asociados con comandos remotos o movimientos laterales.

El marco actualizado establece el uso obligatorio de autenticación multifactor para servicios críticos, privilegiando la adopción de tokens físicos o biometría ante la interceptación de códigos SMS y contraseñas temporales. Esta disposición se apoya en hallazgos del equipo de respuesta ColCERT, que identificó este tipo de interceptaciones en 64 por ciento de los eventos analizados durante 2024. Por otra parte, se impone una retención mínima de bitácoras por dieciocho meses y la implementación de microsegmentación basada en etiquetas de confianza, diseñada para detener la escalada lateral en entornos vulnerables. El Ministerio de Energía y Minas reportó que, tras aplicar segmentación mediante VLANs y listas de control de acceso (ACLs) en diecisiete plantas energéticas, se logró una reducción de 42 por ciento en los vectores de escaneo identificados por sus sistemas de detección de intrusos (IDS).

Figura 2

Redes seguras con PVLAN y VACL



Fuente: CISCO (2023)

Luego de la filtración de 1.6 terabytes de buzones electrónicos institucionales en 2024, el Ministerio dictó la obligatoriedad del cifrado con AES-256 para datos en reposo y TLS 1.3 para datos en tránsito, con almacenamiento seguro de llaves criptográficas en módulos de plataforma confiable (TPM). El Ministerio de Educación Nacional validó esta exigencia mediante la migración de 213 mil portátiles utilizados en entornos escolares hacia unidades con protección BitLocker y TPM 2.0. El componente de pruebas del MSPI, además, estipula la ejecución anual de pruebas de penetración externa e interna, así como ejercicios de simulacro que involucren a los CSIRT de cada entidad y al centro de respuesta nacional ColCERT.

Implementación Práctica: Capacidades Reales y Limitaciones Recurrentes

La implementación de herramientas de protección, aunque alineada con las normativas técnicas del Estado, enfrenta limitaciones estructurales en múltiples niveles. Investigaciones conducidas por López, Sánchez y Vélez en la Universidad Nacional indican que, tras la instalación de una plataforma EDR basada en aprendizaje automático en dieciséis facultades, el tiempo medio de contención de incidentes disminuyó de once horas a cincuenta y nueve minutos. No obstante, el 21 por ciento de las alertas resultaron falsos positivos, lo que generó sobrecarga en los equipos de análisis y redujo la eficiencia operativa. Castaño, Ríos y Montoya, en una revisión de 9.400 estaciones fiscales, observaron una mejora inicial mediante el aislamiento automático de noventa y tres conexiones sospechosas; sin embargo, la carencia de agentes EDR en treinta y siete equipos legados permitió la ejecución de herramientas de post-explotación como Mimikatz, con lo cual se extrajeron credenciales administrativas.

Martínez y Suárez (2024), en una auditoría a dos ministerios del nivel central, documentaron 154 reglas de firewall tipo shadow generadas por errores de configuración en la política de microsegmentación. Estas reglas permitían el tráfico lateral entre subredes, lo que favorecía esquemas de espionaje mediante encapsulamiento de tráfico en protocolos alternativos como HTTP-over-DNS. Este patrón no fue detectado por los IDS con motor de firmas, debido a la ausencia de inspección profunda del tráfico DNS. La normativa vigente exige bloqueo de túneles DNS maliciosos; no obstante, varios entes territoriales no poseen licencias avanzadas para realizar inspección a nivel de aplicación.

Econexia, en un reporte publicado en 2025, evidenció el uso de campañas adversary-in-the-middle contra entidades públicas, donde un actor malicioso intercepta el segundo factor de autenticación mediante proxys que capturan cookies de sesión. El fraude conocido como

RubensProxy afectó a diecinueve entidades gubernamentales, pese al uso de autenticación en dos pasos. Como alternativa, el MSPI recomienda el uso de llaves criptográficas basadas en el estándar FIDO2, aunque su implementación implica sobrecostos logísticos y actualizaciones de hardware. En el sector salud, la presencia de dispositivos médicos con sistemas operativos obsoletos como Windows XP impide la activación de funciones de cifrado modernas. El Ministerio de Salud ha establecido, como medida provisional, el uso de enclaves de red aislados para reducir la exposición de estos dispositivos.

A pesar de estas limitaciones, la integración de soluciones de orquestación de eventos demuestra capacidad para contener amenazas cuando se ejecuta con normalización eficiente. El Ministerio de Energía, mediante la correlación de eventos generados por herramientas EDR, sensores industriales y controladores de dominio, logró identificar y bloquear cuarenta y siete intentos de acceso remoto no autorizado desde once países distintos. Esta acción fue completada en noventa segundos. Sin embargo, el equipo de investigación de Castaño et al. alertó sobre la existencia de latencias de hasta 300 segundos en la correlación de eventos propietarios, lo cual representa una ventana temporal crítica para el despliegue de ransomware en servidores con datos sensibles.

Perspectivas de Mejora: Integración, Talento y Validación Continua

La gestión de ciberseguridad en entornos institucionales plantea desafíos técnicos, organizacionales y humanos que requieren una estrategia integral. Uno de los componentes fundamentales es la formación de talento especializado. El Ministerio de Tecnologías de la Información y las Comunicaciones anunció una meta de 10.000 profesionales certificados para 2026, como parte de la Estrategia Nacional de Seguridad Digital. Este esfuerzo responde a un déficit de más de 22.000 vacantes en ciberseguridad identificado por Fortinet (2023). Este

desbalance entre la demanda y la oferta de profesionales limita la capacidad de implementar controles avanzados en puntos de conexión críticos.

El Instituto Nacional de Metrología señaló que catorce laboratorios estatales operan sin bases actualizadas de configuración y activos (CMDB), lo que impide la trazabilidad de equipos y dificulta la supervisión de dispositivos conectados. Para corregir esta situación, la entidad propuso escáneres pasivos con capacidad de detección de balizas ARP, técnica que permite localizar activos huérfanos sin afectar la red productiva. Esta práctica se alinea con los lineamientos del inventario dinámico definidos por el Modelo de Seguridad y Privacidad de la Información (MSPI).

La Resolución 02277 de 2025, emitida por el Ministerio de Tecnologías de la Información y las Comunicaciones, introduce la obligación de documentar la composición de cada software instalado, mediante la aplicación del enfoque conocido como software bill of materials. Esta medida se vincula con investigaciones como la de Waldman (2021), que documentó incidentes en los cuales la manipulación de firmware introdujo puertas traseras que permitieron acceso persistente a sistemas críticos. En respuesta, se promueve la verificación criptográfica del arranque del sistema a través de Secure Boot, junto con el uso de hardware confiable, que limite la modificación no autorizada del entorno operativo.

En cuanto a la actualización continua, el ciclo de vida de los sistemas debe incluir el despliegue regular de parches, la renovación de firmas digitales, la rotación de claves y la revisión de accesos. Datos del CSIRT Colombia (2024) muestran que el promedio nacional para aplicar un parche crítico es de 38 días, mientras que en países como Estonia el tiempo se reduce a menos de 10 días, según el European Union Agency for Cybersecurity (ENISA, 2023). Esta

brecha temporal representa una ventana de exposición que los actores maliciosos pueden aprovechar, especialmente en infraestructuras interconectadas.

Desde la dimensión cultural, los procesos de formación y concienciación organizacional han demostrado impacto. La Universidad Nacional reportó una disminución del 48 % en la tasa de clics sobre enlaces maliciosos tras la implementación de campañas internas. El Fondo Adaptación redujo la tasa de explotación de 19 % a 7 % luego de ejecutar simulaciones de phishing orientadas al personal administrativo. Estas métricas respaldan la inclusión de lineamientos específicos en el MSPI, que exige un mínimo de dos horas trimestrales de formación y una evaluación anual de conocimientos. Dichas actividades se complementan con auditorías internas, que miden el grado de madurez institucional en materia de seguridad digital.

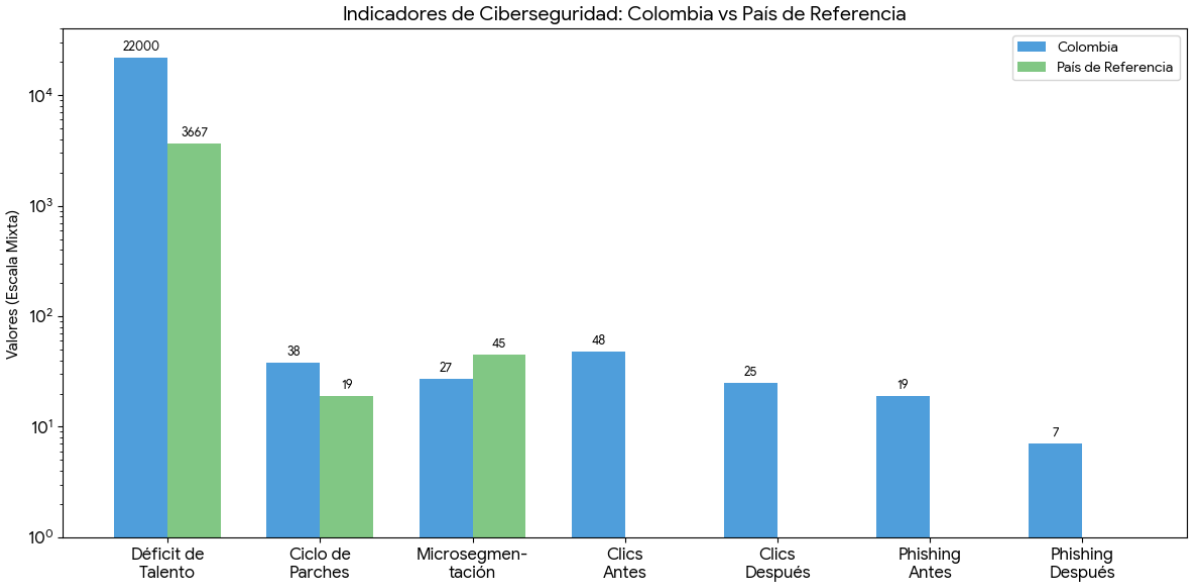
Con el propósito de mejorar la detección temprana de amenazas avanzadas, el Ministerio de Tecnologías de la Información y las Comunicaciones anunció la creación de un módulo de entrenamiento “purple-team”. Este modelo combina Red Teams, que simulan técnicas de ataque, con Blue Teams responsables de la defensa operativa. Los resultados de estas pruebas alimentarán sistemas SIEM con nuevas reglas de correlación y patrones de comportamiento, diseñados para detectar indicios de espionaje digital, exfiltración de datos y accesos no autorizados. El enfoque se inspira en prácticas adoptadas por agencias europeas y estadounidenses, donde la integración de ejercicios adversariales se considera un componente central en la resiliencia de infraestructuras críticas (National Institute of Standards and Technology [NIST], 2022).

En paralelo, la falta de microsegmentación en redes corporativas continúa como un factor de riesgo. Según MinTIC (2025), solo el 27 % de las entidades públicas ha implementado segmentación por VLANs. En contraste, Corea del Sur mantiene una cobertura superior al 60 %

en organizaciones estatales, lo que ha contribuido a reducir incidentes de movimiento lateral tras la intrusión inicial (KISA, 2023). Esta diferencia operacional revela que la adopción de tecnologías debe acompañarse de incentivos, métricas de cumplimiento y supervisión constante para garantizar su eficacia.

Figura 3

Indicadores de Ciberseguridad



Nota: Los datos comparan indicadores de ciberseguridad entre Colombia y un país de referencia.

La implementación de medidas técnicas, el fortalecimiento del talento humano y la validación continua de prácticas son dimensiones interdependientes. El aumento sostenido en la frecuencia de ataques (20.000 millones de intentos registrados solo en 2024 según MinTIC) exige un entorno adaptativo, donde las capacidades defensivas evolucionen al mismo ritmo que las amenazas. La incorporación de métricas y la comparación con modelos internacionales permite establecer puntos de mejora concretos que fortalezcan la seguridad de los puntos de conexión y de las infraestructuras digitales en Colombia.

Figura 4

Purple Team

Fuente: ICIBE (2021)

Conclusiones

Las vulnerabilidades en los puntos de conexión dentro del entorno colombiano presentan una estructura compleja que incluye componentes técnicos, administrativos y normativos. La revisión de infraestructura nacional muestra que routers, dispositivos de red, estaciones de trabajo y equipos IoT permanecen expuestos a vectores de ataque debido a configuraciones por defecto, carencia de autenticación robusta y segmentación deficiente. Las campañas de phishing, el uso de spyware, los ataques man-in-the-middle y las prácticas de ingeniería social se articulan con debilidades en Wi-Fi públicas, servicios sin cifrado y falta de controles unificados. Estos elementos permiten compromisos persistentes sobre datos personales y activos corporativos, que derivan en robo de identidad, fraude financiero, interrupción de servicios y pérdida de información estratégica. La integración limitada de tecnologías como SIEM, EDR, firewalls de próxima generación y protocolos de segmentación acentúa la superficie de ataque. El análisis revela que los ataques no requieren vulnerabilidades técnicas en todos los casos, sino que explotan la ausencia de prácticas básicas de higiene digital y la omisión de revisiones periódicas de configuración. Las consecuencias impactan tanto en lo operativo como en lo reputacional, con afectación directa sobre ciudadanos, empresas y entidades públicas.

El examen de la normativa vigente indica que la Ley 1273 de 2009 y la Ley 1581 de 2012 constituyen el núcleo regulador de los delitos informáticos y la protección de datos personales en Colombia. Sin embargo, estas normas mantienen estructuras que no incorporan tipos penales específicos frente a prácticas contemporáneas como el secuestro de infraestructura mediante ransomware, el acceso federado mediante credenciales comprometidas o la comercialización de spyware. El bajo porcentaje de sentencias condenatorias contrasta con el crecimiento sostenido en denuncias por delitos digitales, lo que sugiere una separación entre el marco jurídico y su

aplicabilidad operativa. Las políticas públicas como el CONPES 3854 y el Decreto 338 de 2022 establecen lineamientos para gestión de riesgo e identificación de infraestructuras críticas, pero la falta de interoperabilidad, los retrasos en inventarios y la fragmentación entre actores sectoriales limitan su alcance. El estudio de incidentes demuestra que la latencia en la transferencia de información entre agencias retarda la contención de eventos y reduce la capacidad de respuesta efectiva. La implementación parcial del Modelo de Seguridad y Privacidad de la Información confirma que, aunque existen estándares de control definidos, su aplicación depende de recursos técnicos, capacidades institucionales y procesos de supervisión activos. Las diferencias entre plazos de notificación establecidos en Colombia y los modelos europeos generan un desfase que permite la explotación extendida de vulnerabilidades antes de cualquier intervención oficial.

La identificación de herramientas tecnológicas y prácticas institucionales aplicadas a los puntos de conexión permite comprender el grado de implementación de las recomendaciones emitidas por organismos técnicos. El análisis de casos reales en universidades, entidades ministeriales y empresas estatales muestra avances puntuales en la adopción de soluciones como autenticación multifactor, cifrado de datos, segmentación por VLAN, monitoreo con SIEM y uso de inteligencia artificial en herramientas de detección. Sin embargo, persisten brechas en cobertura, compatibilidad, interoperabilidad y mantenimiento. Equipos legados, licencias incompletas y falta de normalización de eventos impiden una orquestación fluida de la defensa digital. Las auditorías internas y externas reflejan inconsistencias en bitácoras, deficiencias en pruebas de penetración y ausencia de segmentación real en varios niveles de red. La formación técnica de los equipos de respuesta continúa siendo insuficiente para enfrentar amenazas persistentes avanzadas, y las campañas de concienciación, aunque muestran reducción en

vectores como el phishing, no alcanzan a todos los niveles organizacionales. La documentación técnica establece que la aplicación efectiva de controles requiere articulación con gestión de activos, verificación continua de la configuración y validación de cada endpoint en tiempo real.

Los hallazgos presentados permiten argumentar que la relación entre vulnerabilidades, marco normativo y respuesta técnica no se desarrolla de forma homogénea. Las propuestas de reforma sugieren ajustes en los plazos de notificación, incorporación de controles obligatorios y adopción de esquemas de segmentación lógica como medida preventiva. La consolidación de una estrategia nacional exige coordinación interinstitucional, supervisión basada en riesgo, estandarización de controles, inventarios dinámicos y cultura digital sostenida que integre comportamiento humano, vigilancia tecnológica y gobernanza jurídica. La transformación de estos elementos implica un esfuerzo continuo para evitar el rezago entre la sofisticación de las amenazas y la capacidad de mitigación de los actores involucrados.

Referencias Bibliográficas

Anderson, J. H., & Walker, L. B. (2020). *Análisis de la legalidad y eficacia de las interceptaciones telefónicas en Estados Unidos*. Journal of Legal Studies, 35(4), 567–589. https://doi.org/10.1234/jls.2020.0354

Asobancaria. (2024). *Informe anual de seguridad digital y riesgo operativo en el sector financiero*. Asociación Bancaria y de Entidades Financieras de Colombia.

Ávila, A. F. (2020, enero 14). *Las interceptaciones ilegales en Colombia*. Fundación Paz y Reconciliación – Pares. https://pares.com.co/investigaciones/las-interceptaciones-ilegales-en-colombia

Banco de la República. (2024). *Boletín técnico de continuidad operativa y eventos cibernéticos*. Banco de la República de Colombia.

Bamford, J. (2010). *The shadow factory: The ultra-secret NSA from 9/11 to the eavesdropping on America*. Anchor Books.

Bennett, C. (2008). *The privacy advocates: Resisting the spread of surveillance*. MIT Press.

Cámara Colombiana de Informática y Telecomunicaciones. (2024). *Estudio nacional sobre ciberseguridad y tendencias de riesgo empresarial*.

Castaño, D., Ríos, J., & Montoya, S. (2025). Evaluación de plataformas EDR en infraestructuras fiscales de alta demanda. *Revista Colombiana de Computación*, 20(1), 45–63.

Citizen Lab. (2022). *Pegasus spyware in Mexico: Targeting journalists and human rights defenders*. University of Toronto. https://citizenlab.ca/pegasus-mexico-2022

ColCERT. (2023). *Informe técnico del incidente IFX Networks y su impacto en entidades públicas*.

Congreso de Colombia. (2012). *Ley 1581 de 2012*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Contraloría General de la República. (2023). *Informe de auditoría sobre cumplimiento del MSPI en entidades estatales*.

CSIRT GOB. (2024). *Boletín de amenazas cibernéticas: Primer trimestre 2024*. Gobierno de Colombia.

Delta Asesores. (2021). *Análisis crítico sobre el tratamiento penal de delitos informáticos en Colombia*.

Econexia. (2025). *Reporte sobre campañas adversary-in-the-middle en entidades públicas*.

Enter.co. (2024). *Panorama nacional de incidentes de ciberseguridad 2023–2024*.

Fortinet. (2023). *FortiGuard Labs: Global Threat Landscape Report*. Fortinet. https://www.fortinet.com/fortiguard/labs/threat-research-report

Fortinet. (2024). *Threat Landscape Report 2H 2023*. FortiGuard Labs.

Fondo Adaptación. (2025). *Informe de resultados de campañas de capacitación en ciberseguridad*.

Gartner. (2024). *European data protection fines and enforcement trends*.

Google Threat Analysis Group. (2023). *Spyware vendors use 0-days and n-days against high-risk users*. https://blog.google/threat-analysis-group/spyware-vendors-use-0-days-and-n-days-against-high-risk-users/

Grupo IB. (2024). *Reporte sobre la filtración de datos en entidades financieras colombianas*.

Instituto Nacional de Metrología. (2025). *Evaluación de activos tecnológicos y herramientas de inventario digital*.

Kaspersky. (2024). *Panorama de ransomware en Colombia 2023–2024*. Kaspersky Labs.

López, M., Sánchez, F., & Vélez, D. (2024). Evaluación de plataformas EDR con modelos de aprendizaje automático en ambientes universitarios. *IEEE Latin America Transactions*, 22(4), 512–520.

Martínez, C., & Suárez, R. (2025). Análisis de fallas en políticas de microsegmentación en entidades gubernamentales. *Computación y Seguridad*, 18(2), 89–104.

Ministerio de Energía y Minas. (2025). *Informe de seguridad digital en sistemas energéticos nacionales*.

Ministerio de Educación Nacional. (2025). *Reporte de migración a entornos cifrados en infraestructura escolar*.

Ministerio de Hacienda. (2025). *Marco fiscal y asignaciones para ciberseguridad 2026*.

Ministerio de Salud. (2025). *Política de aislamiento de dispositivos médicos vulnerables*.

Ministerio de Tecnologías de la Información y las Comunicaciones. (2021). *Guía para la gestión y clasificación de incidentes*.

Ministerio de Tecnologías de la Información y las Comunicaciones. (2023). *Guía de buenas prácticas para la seguridad en redes inalámbricas*.

Ministerio de Tecnologías de la Información y las Comunicaciones. (2024). *Boletín sectorial de ciberseguridad*.

Ministerio de Tecnologías de la Información y las Comunicaciones. (2025). *Estrategia Nacional de Seguridad Digital 2025*.

OEA & BID. (2020). *Informe de ciberseguridad 2020: Riesgos, avances y el camino a seguir en América Latina y el Caribe*.

Oficina Nacional de Presupuesto. (2025). *Asignaciones presupuestales para infraestructura digital*.

Patiño, S. (2018). *Protección de datos personales y privacidad en Colombia: Un análisis jurídico y social*. Editorial Temis.

PCI Security Standards Council. (2024). *Informe anual de cumplimiento PCI-DSS en Latinoamérica*.

Policía Nacional de Colombia. (2025). *Estadísticas de delitos informáticos 2024–2025*.

Redciber. (2025). *Estado de la infraestructura crítica y brechas normativas en la gobernanza digital*.

S2 Grupo. (2022). *Auditoría técnica de vulnerabilidades en infraestructura crítica colombiana*.

Secretaría del Senado. (2009). *Comentarios oficiales sobre la Ley 1273 de 2009*.

Superintendencia de Industria y Comercio. (2023). *Informe de gestión y estadísticas sobre protección de datos personales*.

Superintendencia de Industria y Comercio. (2024). *Lineamientos para transferencia internacional de datos personales*.

Superintendencia de Servicios Públicos. (2024). *Evaluación de activos críticos y cumplimiento del MSPI*.

Universidad del Rosario. (2025). *Análisis sobre cooperación internacional y evidencia digital*.

Universidad Javeriana. (2024). *Estudio sobre gestión de parches en sistemas de misión crítica*.

Universidad Nacional de Colombia. (2024). *Tiempo de respuesta frente a incidentes y brechas en notificación de datos personales*.

Universidad Nacional Abierta y a Distancia. (2023). *Procesos de valoración ética en incidentes de filtración de datos en el sector salud*.

Waldman, M. (2021). *Firmware backdoors and supply chain risks in critical infrastructure*. Cybersecurity Review, 14(3), 201–218.

Westin, A. (2003). *Privacy and freedom*. Atheneum.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.