Protección de los Derechos Humanos en la Seguridad de la Información en Colombia, ¿Hay respeto por los derechos humanos en entornos digitales?: Análisis normativo y jurisprudencial 2020-2025

Gina Zoreth Moreno Lemos

ESCUELA SUPERIOR DE ADMINISTRACIÓN PÚBLICA

FACULTAD DE POSGRADOS

MAESTRÍA EN DERECHS HUMANOS, GESTIÓN DE LA TRANSICIÓN Y POSCONFLICTO

BOGOTÁ, 2025

Escuela Superior de Administración Pública

Tabla de Contenido

Índice de Tablas

INTRODUCCIÓN

El mundo ha cambiado y actualmente se está frente a una era digital en la que la información es un elemento clave para la protección de los derechos humanos, por lo que la intimidad, el buen nombre, el acceso a la información, la protección de datos personales y financieros, así como la libertad de expresión pueden verse expuestos frente al avance de las nuevas tecnologías de la información y la comunicación, junto con el auge de la inteligencia artificial y los procedimientos masivos de datos. En este contexto, las transformaciones tecnológicas no solo generan nuevas oportunidades, sino también riesgos significativos que impactan directamente la garantía efectiva de los derechos fundamentales

Estas herramientas están generando nuevas oportunidades, pero también riesgos significativos en la protección de derechos fundamentales, configurando un escenario que exige su análisis desde el ámbito jurídico y social, aportando un nuevo escenario de estudio como los ciber derechos o incluso, biociberderechos si se vincula con una visión integral u holística entre hombre, naturaleza y medios.

El sistema jurídico debe ponderar la prevalencia de derechos, por lo que frente a derechos fundamentales se le da mayor importancia a aquellos que posibilitan la realización de los demás derechos, como es el caso del derecho a la vida. Para algunos académicos, los derechos humanos son los derechos fundamentales de cualquier sistema jurídico y la base de cualquier forma de gobierno (Bobbio, 1991; Glendon, 2004). Otros autores, por su parte, argumentan que los derechos humanos no dependen de ningún ordenamiento jurídico ni forma de gobierno, ya que no se adquieren por mérito alguno, sino que son inherentes al ser humano desde su nacimiento (Aguilar, 2010). Un pleno reconocimiento y una absoluta garantía de estos derechos resultan indispensables para el buen funcionamiento de una

sociedad jurídicamente organizada, lo cual se denomina *"bien común"* y debe ser el fin último de toda asociación humana (Donnelly, 2013).

Los Derechos Humanos según la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (OHCHR) "son inherentes porque les pertenecen a todas las personas por el mero hecho de existir; irrevocables porque al ser derechos de nacimiento nadie puede limitarlos; inalienables porque son exactamente iguales, no pueden perderse; intransmisibles porque nadie puede despojarse de ellos; irrenunciables porque están ligados a la dignidad misma de la persona" (OHCHR, 2024). Para Torres (2009), con relación a la clasificación de los derechos, resalta lo siguiente:

> "los derechos humanos se clasifican en tres categorías o generaciones: i) Primera generación: los derechos civiles y políticos (principio de libertad); ii) Segunda generación: derechos económicos, sociales y culturales (principio de igualdad); iii) Tercera generación: derechos sociales, de progreso social, calidad de vida, respeto y mutua colaboración (principio de solidaridad o fraternidad)" (Torres, 2009, pp.509).

Académicos del derecho y la filosofía jurídica como Norberto Bobbio, Luigi Ferrajoli y Ramón Soriano hablan de una cuarta, quinta y sexta generaciones de derechos; no hay un consenso absoluto sobre su clasificación. Por ejemplo, Díaz expresa que una cuarta generación de derechos humanos está gestándose actualmente, y corresponde a aquellos derechos relacionados con las nuevas tecnologías, la manipulación de la bioética y algunos relacionados con la relación con el planeta y el medio ambiente (Díaz, 2009).

En este escenario de esta nueva sociedad de la información, las tecnologías que permiten la generación, propagación y alteración de la información desempeñan un rol protagónico en las actividades sociales, culturales y económicas. (MinTIC, 2024). Hacen parte

de un entramado de interrelaciones económicas, sociales, culturales, pero sobre todo humanas y también políticas.

Para Cova (2022) la sociedad de la información comprende una serie de conexiones sociales, económicas y culturales, donde las TIC's mediante una amplia gama de dispositivos, herramientas e infraestructuras facilitan la generación, propagación y tratamiento de la información. Herramientas que hoy están inmersas en la cotidianidad de los seres humanos y que representan el triunfo de la tecnología: los computadores, los celulares, los equipos portátiles, el Internet y con ella, las redes sociales, el correo electrónico, los portales web, son solo algunos de esos aspectos. Por otro lado, la *deepweb*[1], la *darkweb*[2], la *darknet*[3], las *fake news*[4], el *cyber bulling*[5], los delitos informativos, son la otra cara de dicha cotidianidad de la tecnología en la vida de la humanidad.

El tema central de esta investigación está relacionado con los llamados derechos digitales o ciber derechos a la luz de la protección de estos en el entorno de la seguridad de la

---

[1] La *deepweb* hace referencia a la parte de Internet que no es indexada por los buscadores tradicionales (Brave, Safari, Chrome, Mozzilla, Opera, etc.). Incluye tanto bases de datos académicas, así como correos, registros médicos, cualquier contenido que esté protegido por o firewalls o contraseñas etc. Es totalmente legal y no es peligroso, sólo de naturaleza privada. (adaptado del portal especializado https://inciclopedia.org/)

[2] Por su parte, la *darkweb* es un subsegmento muy reducido de la *deepweb* que ha sido diseñado específicamente para la privacidad. Se accede utilizando navegadores especializados (por ejemplo, Tor) y contiene contenidos legales (foros de privacidad, medios independientes, etc.) y también ilegales (mercados negros y venta de datos robados). (adaptado del portal especializado https://inciclopedia.org/)

[3] las *darknets* son las redes privadas que hacen posible que exista la *darkweb*. Son, grosso modo, infraestructuras tecnológicas (Tor, I2P o Freenet) que permiten la comunicación anónima. Las *darknet* son el canal que permite acceder al contenido; la *darkweb* es el contenido en sí mismo. (adaptado del portal especializado https://inciclopedia.org/)

[4] Son mentiras fabricadas y utilizadas de manera intencionada con la finalidad de embaucar, manipular la opinión pública o bien de obtener un beneficio, ya fuese a nivel económico o político. Son propias de titulares elocuentes, noticias modificadas o bien contextos falsos, transmitiéndose en redes sociales y medios digitales y causando desinformación y polarización social. (adaptado del portal especializado https://inciclopedia.org/)

[5] Es un hostigamiento sistemático y deliberado que se produce por medios digitales (redes sociales, mensajes o juegos online, etc.) Son acciones como el envío de mensajes groseros, comentarios despectivos o rumores sobre una persona, imágenes compartidas sin seguir ni haber seguido el consentimiento de la persona que aparece, o bien excluir a personas de grupos online, entre otras cosas. A diferencia del *bullying* clásico, el *bullying* digital puede ser anónimo, tener mayor alcance, ocurrir en cualquier momento, con lo que tiene un impacto psicológico mayor en las víctimas. (adaptado del portal especializado https://inciclopedia.org/)

información en Colombia. A medida en que se reconoce la existencia de nuevos espacios, más allá del mundo físico (ciberespacios, mundo digital, espacio *online*, entorno virtual, Internet, la nube, etc.) nace la necesidad de entenderlo, de delimitarlo, de reglamentarlo y de garantizar los derechos fundamentales de sus usuarios tanto dentro como fuera de él.

La investigación académica en Colombia sobre ciberseguridad y ciberdefensa se ha enfocado en examinar las regulaciones normativas e institucionales de diversas dinámicas en el ciberespacio, sin considerar el nivel de autonomía que las fuerzas militares tienen en la gestión de la seguridad y defensa en el ciberespacio. Siempre ha habido un control del poder civil sobre esta autonomía, que se establece mediante instituciones jurídicas y políticas que garantizan un equilibrio para la gestión del Estado y la especialización de sus funciones correspondientes. Sin embargo, estas reglas requieren de un proceso continuo de revisión y construcción para hacer que las nuevas amenazas no debiliten el marco establecido (Burton, 2015).

El objetivo de este trabajo es analizar las distintas medidas de protección de los DDHH teniendo en cuenta el contexto de la seguridad de la información, para identificar los principales retos y oportunidades que se presentan para reforzar dicha protección. Se parte de una perspectiva conceptual del ciberespacio y las amenazas a la seguridad; a continuación, se identifican las principales vulneraciones de los derechos humanos que pueden presentarse en el ámbito de la seguridad de la información, para pasar a estudiar el marco legal y normativo vigente que la aborda. El marco normativo en materia de la seguridad de la información parte de la Constitución Política vigente, artículo 15, pasando por la ley 1581 de 2012, que aborda la protección de los datos personales, y la 1273 de 2009 sobre delitos informáticos y políticas de ciberseguridad. En este sentido, se proponen diferentes estrategias y acciones desde el

aspecto legal, técnico y organizativo, para implementar medidas que fortalezcan la protección de los derechos humanos en un entorno de seguridad de la información.

A través de este desarrollo, el análisis no solo se articula en una revisión descriptiva, sino que incorpora, de forma sucesiva, elementos interpretativos y propositivos centrados en identificar posibles líneas de mejora para la protección de los derechos humanos en entornos digitales.

1. PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción del Problema

Definimos a la *sociedad de la información*, como aquella en la cual las tecnologías que facilitan la creación, distribución y manipulación de la información juegan un papel protagónico en las actividades sociales, culturales y económicas (MinTIC, 2024). El Ministerio hace especial énfasis en que la persona es el centro de dicha sociedad, y que el objetivo fundamental es la integración, el desarrollo, la creatividad y la utilidad de la información y del conocimiento empleados para el desarrollo sostenible y la mejora de la calidad de vida (MinTIC, 2024).

Entonces, la sociedad de la información es mucho más que Internet o que las llamadas TIC, es un entramado de interrelaciones económicas, sociales, culturales, pero sobre todo humanas y también políticas. Para Cova (2022), “la sociedad de la información abarca un conjunto de interrelaciones sociales, económicas, culturales en donde las TICs a través de una gran diversidad de dispositivos, herramientas e infraestructuras permiten la producción, difusión y tratamiento de la información” (Cova, 2022, p.62). Herramientas que hoy son parte de la vida cotidiana de la mayoría de los seres humanos en el planeta y que representan

el triunfo de la ciencia y de la tecnología en el avance por la supremacía humana: los computadores, los celulares, los equipos portátiles, el Internet y con ella, las redes sociales, el correo electrónico, los portales web, son solo algunos de esos aspectos. Por otro lado, la *dark web*, la *deep web*, las *fake news*, el *cyber bulling*, los delitos informativos, son la otra cara de dicha cotidianidad de la tecnología en la vida del ser humano.

Después de la Segunda Guerra Mundial, la configuración de la Guerra Fría puso al mundo en una vertiginosa carrera por el avance y desarrollo bélico militar que, a su vez, arrastraba consigo el desarrollo científico y tecnológico. Al final, entre 1948 y 1991 se pasó de la tecnología de altos hornos para las fundiciones, pasando por la utilización del petróleo y todos sus derivados, hasta la carrera espacial y la energía atómica. Por cuenta de la bipolaridad mundial, se desarrollaron instrumentos, herramientas y equipos que desafiaban la imaginación humana: la Internet, los equipos inalámbricos, la era satelital, nuevas fuentes de energía y nuevos destinos para la humanidad. En ese momento, la humanidad veía con buenos ojos los beneficios del avance tecnológico al tiempo que unos pocos observaban con preocupación sus efectos a mediano y largo plazo.

Por otro lado, Téllez (2018), manifiesta que "el ciudadano de hoy se encuentra expuesto a situaciones en las que sus derechos e incluso su seguridad misma están en riesgo debido al gran cúmulo de información que se concentra en sistemas informáticos, blanco de los ataques cibernéticos" (Téllez, 2018, pp.19). La tecnología se fue adhiriendo a la vida cotidiana de la sociedad y nadie se preguntó sobre la pertinencia de estas. "Mucho menos en países menos desarrollados como en el caso de los latinoamericanos que no somos productores de tecnología sino meros importadores" (Téllez, 2018, p.20). Este escenario crea la necesidad del debate sobre las consecuencias de la tecnología en la sociedad,

particularmente para los ciudadanos, sus derechos fundamentales, su privacidad y su seguridad. La presente investigación pretende tomar dicha tarea en el contexto colombiano.

En este sentido, el análisis de estas problemáticas no solo busca evidenciar las vulneraciones existentes, sino también abrir la discusión sobre posibles respuestas normativas, institucionales y sociales que permitan fortalecer la protección de los derechos en el entorno digital.

1.2. Formulación del problema o pregunta de investigación

Se propone por lo anterior, estudiar la protección de los derechos humanos en el entorno de la seguridad de la información en Colombia. La finalidad es identificar los desafíos y las oportunidades para fortalecer la protección que necesita el ciudadano frente a las TIC's. Se maneja la idea de que es la falta de información y de capacitación la que contribuye en gran medida, a la vulneración de los derechos humanos en el entorno de la seguridad de la información en Colombia. Se plantea entonces la siguiente pregunta de investigación: *¿Cuáles son las principales vulneraciones a los derechos humanos que pueden ocurrir en el contexto de la seguridad de la información en la actualidad 2025 en Colombia, y qué medidas legales, técnicas y organizacionales son necesarias para prevenir y mitigar estos riesgos, garantizando así una protección eficaz de los derechos fundamentales en este contexto?*

Esta pregunta dirige el desarrollo del artículo no solo hacia la identificación de problemas, sino también hacia la elaboración de un análisis que relacione esas vulneraciones con potenciales estrategias de mejora. Estas se tratan en todo el documento y no solamente en la sección de conclusiones.

1.3 Objetivos

1.3.1 Objetivo general

- Analizar las medidas de protección de los derechos humanos en el contexto de la seguridad de la información en Colombia, a través del estudio de la normativa y jurisprudencia vigente con el fin de identificar los desafíos, riesgos y oportunidades de mejora en la regulación.

1.3.2 Objetivos específicos

- Identificar los conceptos de derechos humanos y de la seguridad de la información, con lo cual se logra establecer la interacción de ambos en el contexto digital.
- Examinar las normativas nacionales e internacionales aplicables a la protección de los derechos humanos en la seguridad de la información.
- Establecer las principales vulneraciones de los derechos humanos que pueden ocurrir en el marco de la seguridad de la información en Colombia.
- Identificar y sustentar lineamientos de mejora orientados al fortalecimiento de la protección de los derechos humanos en el contexto de la seguridad de la información en el país.

1.4 Justificación

Con la pandemia del COVID 19, el país tuvo que hacer uso de herramientas tecnológicas para superar la crisis que esta produjo y para garantizar servicios como la educación, salud, trabajo, entre otros; por lo que se evidenció la necesidad de actualizarse en su uso, pero al no estar preparados para su implementación muchas veces la población ha

quedado expuesta a un mundo nuevo que debe ser regulado por los distintos gobiernos.

De acuerdo con las cifras del Departamento Administrativo Nacional de Estadísticas (DANE), al cierre de 2022, el 59,5% de los hogares colombianos tienen acceso a internet. De los 32 departamentos, 27 tienen acceso a Internet en cualquier lugar y dispositivo, y entre el 50% y el 89% de su población utiliza este servicio (DANE, 2023). Según el Ministerio de Tecnologías de la Información y Comunicaciones de Colombia - MinTIC (2024), para 2023, el número de usuarios de Internet fijo en Colombia superó los 9 millones, la mayoría de ellos presentes en las grandes ciudades y capitales. La llamada brecha digital aún es muy grande en Colombia, sin demeritar los esfuerzos del Ministerio, la realidad es que en la mayoría de los casos las TIC's aún no llegan a todo el territorio nacional.

Los temas políticos que son temas comunes de conversación en el país y el acceso a esta información por los medios de comunicación tradicionales y alternativos han fortalecido el acceso de la población en Internet como una manera de tener presencia, asociación, libre expresión y desarrollo de la libre personalidad. Es así como Colombia "se encuentra en el top 5 de los países latinoamericanos con mayor número de incidentes de seguridad tales como: fraude electrónico, extorsión, robo de información, denegación de servicios, *malware*, virus, entre otros" (González, 2023, p.2).

En este sentido, el Estado debe promover programas de prevención y capacitación para todos los usuarios que tengan acceso a información sensible. Que la sociedad desarrolle una conciencia y una cultura de la seguridad de la información en todos los campos, tanto reales como virtuales. Que las empresas y los empresarios apliquen las políticas de Seguridad de la Información vigentes en el país y el mundo para no facilitar la tarea de los ciberdelincuentes. De igual manera, un desarrollo económico, político y sociocultural del

país hará que cada vez se usen los dispositivos de una mejor forma y para mejores fines.

El estudio aportará a la definición de la seguridad de la información en el contexto de los derechos humanos en Colombia. Al examinar las infracciones a estos derechos en el entorno digital, se potenciará la comprensión en campos como el derecho, la tecnología y la ética. Se anticipa que los descubrimientos ofrezcan un marco teórico que facilite comprender cómo un sólido marco legal y regulatorio puede impactar en la salvaguarda de los derechos esenciales, además de en la puesta en marcha de políticas eficaces en el campo de las tecnologías de la información.

La población con la que se trabajará abarca a todos los habitantes de Colombia que hacen uso de tecnologías de información y comunicación (TIC's), además de grupos vulnerables que tienen una mayor tendencia a padecer infracciones a sus derechos en internet. A mediano y largo plazo, se anticipa que este estudio ayude a construir una cultura de seguridad digital que favorezca tanto a personas como a entidades, potenciando de esta manera su habilidad para salvaguardar su información personal y sus derechos básicos.

La investigación tiene la capacidad de impulsar lazos entre comunidades educativas, ciencia y sociedad, fomentando un debate interdisciplinario acerca de la seguridad de la información y los derechos humanos. Este estudio se puede usar como apoyo para futuras alianzas entre el sector público y el sector privado en Colombia.

La factibilidad del proyecto se basa en el incremento del interés del gobierno de Colombia y entidades internacionales por potenciar la salvaguarda de los derechos humanos en el contexto digital. La posibilidad se apoya en el aumento del acceso a Internet en el país, lo que simplifica la recolección de información y la puesta en marcha de programas de formación.

1.5. Delimitación, espacial y temporal

La investigación se lleva a cabo en el contexto colombiano, mediante un análisis documental legal y normativo con vigencia 2025.

1.6 Hipótesis

Dentro del marco de la seguridad de la información en Colombia, se observan infracciones a los derechos humanos, particularmente al derecho a la privacidad y a la libertad de expresión, atribuibles a la ausencia de un sólido marco legal y normativo, junto con la insuficiencia de medidas técnicas y organizativas apropiadas para proteger estos derechos esenciales en la gestión de información.

2. METODOLOGÍA

2.1. Paradigma de Investigación

La presente investigación se ajusta a un protocolo de investigación cualitativa, mediante un análisis documental reflexivo, siguiendo las características que proponen Hernández et al. (2017). Recalcan que el análisis documental es una técnica que permite recolectar datos de documentos ya existentes y que ayudan a entender el fenómeno que se investiga. El propósito de la investigación es analizar las estrategias de protección de los derechos humanos en la seguridad de la información en Colombia, reconociendo los desafíos y oportunidades para fortalecer la protección.

2.2. Enfoque de la investigación

El estudio es tipo descriptivo-analítico con un enfoque histórico – hermeneútico. Este enfoque busca describir fenómenos, situaciones y acontecimientos, así como interpretar los significados subyacentes en los documentos analizados (Hernández et al., 2017). El objetivo

principal es recopilar e interpretar de forma independiente información sobre conceptos o variables sin explorar las relaciones entre ellos. Se propone un análisis profundo de los significados subjetivos e intersubjetivos inherentes a las realidades estudiadas (Hernández, et al, 2014). El propósito central es analizar las medidas de protección de los derechos humanos en el contexto de la seguridad de la información en Colombia, identificando los desafíos y oportunidades para fortalecer dicha protección.

Esta técnica explora, elige, estructura y examina los documentos de análisis para dar respuesta a uno o varios interrogantes relacionadas con cierto tema (Tobón, 2012). La meta es unificar los datos obtenidos, estructurarlos para condensarlos y transformarlos en un documento de acceso más sencillo. Este enfoque requiere el uso de estrategias concretas en la búsqueda, selección, organización y valoración de un conjunto de trabajos escritos (Bermeo, Hernández, & Tobón, 2016).

La finalidad principal fue reunir e interpretar de manera independiente información sobre variables o conceptos, sin examinar las conexiones entre los mismos. Esto se realizó en tres fases o momentos:

1. ***Primer Momento: Exploración de documentos***. Con el fin de detectar lagunas normativas vinculadas a los retos que surgen en el entorno digital, se trabajó sobre leyes nacionales e instrumentos internacionales relacionados con el tema.
2. ***Segundo Momento: Revisión de jurisprudencia***. Se examinaron decisiones vinculadas de la Corte Constitucional, además de casos internacionales que han establecido principios obligatorios en cuanto a la provisión y salvaguarda de los denominados derechos digitales.
3. ***Tercer Momento: Evaluación de políticas públicas***. Se revisaron documentos

oficiales del MinTIC y de la Policía Nacional acerca de cómo se aplicaron tácticas de ciberseguridad entre 2015 y 2023, las cuales se probaron frente a los indicadores de infracciones detectadas durante ese mismo lapso.

La triangulación como método (normatividad-jurisprudencia-políticas) ayudó a contrastar hallazgos teóricos con evidencias de la práctica institucional; proponer ajustes que armonicen el marco normativo colombiano a los estándares internacionales y formular recomendaciones a partir de las buenas prácticas encontradas.

2.3. Método de Investigación

La investigación se llevará a cabo usando el método de análisis documental reflexivo. Este tipo de estudio es cualitativo y se enfoca en recopilar, analizar e interpretar información de fuentes normativas, doctrinales y académicas. Como técnica principal, se utilizará el análisis de documentos para reunir información a partir de documentos existentes, permitiendo la comprensión del fenómeno investigado. El análisis de documentos se erige como un método que busca, selecciona, organiza y analiza los documentos con el propósito de dar respuestas a uno o a varios interrogantes, siempre en relación con un objeto de conocimiento dado (Tobón, 2012).

En este sentido, el propósito metodológico no es un objetivo por sí mismo, sino una parte que orienta el desarrollo del objetivo general, permitir revisar el marco normativo, así como detectar problemas y conclusiones y mejorar a partir del análisis crítico de las fuentes consultadas; de este modo se garantiza coherencia entre el método y la naturaleza reflexiva y analítica del estudio. El procedimiento metodológico articula y problematiza el proceso de la información recolectada en vista de su organización y crítica con el fin de construir una interpretación del fenómeno investigado. Esta metodología requiere la práctica de

determinadas estrategias de búsqueda, selección, organización y evaluación de un conjunto de trabajos escritos sobre un objeto de estudio (Bermeo et al., 2016).

2.4. Tipo de investigación

La investigación es de tipo descriptivo, ya que se centra en identificar y describir las medidas de protección de los derechos humanos en el contexto de la seguridad de la información en Colombia. Se define como aquella que tiene como objetivo describir algunas características de conjuntos homogéneos de fenómenos y utiliza criterios sistemáticos que "permiten establecer la estructura o el comportamiento de los fenómenos en estudio, proporcionando información sistemática y comparable con la de otras fuentes" (Martínez, 2018)

2.5. Población y muestra

Debido a la naturaleza de la investigación, no se contará con una población específica. Se llevará a cabo una labor con documentos pertinentes que abordan los derechos humanos y la seguridad de la información en Colombia. En este contexto, se empleará una variedad de documentos relevantes, tales como informes oficiales, estudios académicos, normativas, regulaciones y datos estadísticos, que traten cuestiones vinculadas a la ciberseguridad y los derechos humanos.

2.6. Diseño de la Investigación

Se utilizará un diseño no experimental, dado que se analiza información existente sin manipular variables o condiciones del entorno. Para Hernández, et al, (2017), el diseño no experimental es aquel que se realiza sin manipular deliberadamente la variable, es observar fenómenos tal como se dan en su contexto natural para después ser analizado.

2.7. Técnicas e instrumentos de recolección de datos

La investigación se apoyará en fuentes secundarias, como artículos especializados, revisión documental de leyes, reglamentos, políticas públicas y normas nacionales e internacionales relacionados con la protección de derechos humanos y seguridad en la información. La revisión documental y sistemática de estos recursos permitirá alcanzar los objetivos propuestos. Se emplearán diversas fuentes, incluyendo investigaciones, revistas científicas, libros, documentales, artículos periodísticos y entrevistas, para lograr un análisis exhaustivo.

2.7.1 Recolección de Datos

- **Identificar Temas Clave:** Al examinar documentos pertinentes, como informes de gobiernos, investigaciones anteriores y estadísticas, se podrán reconocer aspectos fundamentales que vinculan la ciberseguridad con los derechos humanos.
- **Contextualizar la información:** un análisis reflexivo permitirá entender el entorno en el que se elaboraron los documentos y facilitará la extracción de datos, lo que a su vez enriquecerá la interpretación de los resultados.
- **Creación de nuevas ideas:** Al reunir diferentes fuentes de información y hacer un análisis cuidadoso, se podrán desarrollar nuevas estrategias para enfrentar los problemas de ciberseguridad y derechos humanos.

2.7.2 Proceso de Análisis Documental

- **Definición del Objetivo de Investigación:** meta que se busca alcanzar mediante un estudio. Es una declaración clara que describe lo que se pretende descubrir,

analizar o entender a través de la investigación.

- **Selección de Documentos:** Se buscarán y elegirán documentos relevantes, como informes del gobierno, artículos de investigación y estadísticas, que traten sobre la ciberseguridad y los derechos humanos.
- **Codificación y Análisis**: Se utilizará un proceso de codificación para organizar los datos extraídos de los documentos y hacer que sea más fácil de analizar.
- **Interpretación reflexiva:** Se realizará una interpretación crítica que tenga en cuenta tanto el contenido de los documentos como el contexto social y político en el que se produjeron.
- **Elaboración del Informe**: Se redactará un informe que presente los resultados del análisis documental y sus implicaciones.

Tabla 1.

Categorías de análisis

Categorías de análisis	Descripción	Indicadores
Derechos Humanos	Derechos y garantías inherentes a las personas que limitan el poder estatal y privado.	Clasificación de derechos (civiles, políticos, económicos, sociales, culturales)
Ciber derechos	Derechos relacionados con el uso de tecnologías digitales y la protección de la información personal.	Acceso a Internet, privacidad, libertad de expresión, gobernanza de Internet.
Seguridad de la Información	Protección de los activos de información contra amenazas cibernéticas.	Confidencialidad, integridad, disponibilidad; implementación de políticas de seguridad.
Protección de Datos Personales	Normas y principios para garantizar el tratamiento ético y legal de los datos personales.	Licitud, transparencia, limitaciones en la recopilación y tratamiento de datos.

Marco Legal	Conjunto de leyes y regulaciones que protegen los derechos humanos en el contexto digital.	Constitución Política, tratados internacionales, mecanismos de tutela (ej. tutela en Colombia)
Impacto de la Tecnología	Efectos positivos y negativos del uso de tecnologías en los derechos fundamentales.	Casos documentados de violaciones a la privacidad y seguridad; análisis de vulnerabilidades.
Conciencia Social	Nivel de conocimiento y sensibilización sobre los derechos digitales entre ciudadanos.	Encuestas sobre percepción de privacidad y seguridad; participació en foros sobre derechos digitales.
Jurisprudencia Internacional	Decisiones judiciales que influyen en la interpretación y aplicación de los derechos humanos.	Sentencias del Tribunal Europeo de DDHH, precedentes en DD digitale
Desafíos Cibernéticos	Amenazas que afectan la seguridad y privacidad en el entorno digital.	Tipos de ciberataques (malware, phishing); estadísticas sobre incidentes de seguridad.
Mecanismos de Protección	Estrategias implementadas para salvaguardar los derechos digitales.	Políticas organizacionales, estándares internacionales (ej. ISO TEC 27001).

Fuente: Elaboración propia

3. MARCO REFERENCIAL

3.1. Antecedentes

3.1.1. Antecedentes internacionales

Seclén (2016), en Perú, tuvo como objetivo principal analizar cuáles son las principales limitaciones y problemas que enfrentan las entidades del sector público en la implementación del Sistema de Gestión de Seguridad de la Información. Los resultados incluyen la identificación y descripción de problemas de implementación, análisis de estrategias operacionales, definición de obstáculos durante la implementación, identificación de beneficios obtenidos y propuestas de soluciones para la capacitación en seguridad de la información.

Pérez (2014), hace un análisis de las incidencias de las tecnologías de la información y las comunicaciones en la esfera de las libertades; y del mismo modo, reflexiona sobre la problemática del chat y los menores en el ambiente de la educación parental en las nuevas tecnologías; y iii) la importancia del esfuerzo de la legislación al tratar de proteger a los niños, jóvenes y adolescentes que pueden ser atacados por cibernautas criminales. Algunas conclusiones del estudio son: i) el reconocimiento de la ciber ciudadanía y la tele democracia como nuevos horizontes de los derechos en la era digital; ii) la exploración de la problemática del *grooming* en menores a través de servicios de chat en Internet, destacando la importancia de la educación parental en este contexto; iii) la reflexión sobre el impacto de las TIC en la educación, planteando desafíos y beneficios, según la perspectiva del filósofo Noam Chomsky; y iv) la consideración de la patria potestad y la responsabilidad parental en la educación sobre el uso de las modernas tecnologías, con énfasis en Internet.

Córdoba (2021) realizó una investigación aplicada con enfoque tecnológico que se apoya del software *Eramba Community*, ofreciendo una alternativa de implantación del sistema a bajo costo. Se concluyó que el uso del *software* integrado a la Norma ISO 27001:2013 para dar respuesta a la Ley de Protección de Datos Personales resultó un procedimiento eficiente que permitió el cumplimiento ágil de los procedimientos y que no excedió los recursos presupuestales de la Universidad, mejorando con ello la seguridad de los procesos y reforzando la seguridad de los datos.

En México, Hernández, Canizales & Peláez (2021), presentan un análisis de la necesidad de una cultura de ciberseguridad de los usuarios, derivada del desconocimiento de la red y los problemas que trae consigo. Por medio de un análisis documental, los autores señalan algunos derechos humanos originados desde el entorno virtual, contextualizándolo al entorno mexicano.

También en México, Penna, Gómez & de Dios (2023), por medio de un análisis documental, sobre las amenazas a la ciberseguridad y la cotidianidad de esta; analizan cómo el gobierno federal, las empresas y los ciudadanos en México se enfrentan a estos posibles ataques, desde *pishing* a los correos hasta ataques más complejos como archivos de la nación.

3.1.2. Antecedentes nacionales

Rojas (2022) ofrece un análisis sobre cómo se regula y se da seguimiento a los delitos que ocurren a través de la tecnología. El objetivo principal de la investigación es estudiar cómo se protegen los derechos fundamentales en relación con la seguridad de la información en Colombia. Los resultados muestran que: i) los ciberdelitos son muy serios, ya que pueden incluir el robo de información confidencial, el acoso en redes y el fraude, lo que puede causar problemas graves para las personas y las empresas, como la pérdida de datos y la interrupción de sus actividades; y ii) es muy importante proteger la información como una forma de prevenir estos delitos, lo que incluye tener leyes, regulaciones y herramientas para identificar y castigar a los ciberdelincuentes. Se destaca la importancia del Marco Legal de la Seguridad de la Información, que incluye la protección de los derechos de los usuarios, la privacidad y la propiedad intelectual, y establece requisitos para mantener la seguridad de la información. El método que se usa consiste en un análisis cuidadoso de las leyes colombianas, casos legales, informes de organizaciones tanto nacionales como internacionales, estudios académicos, encuestas y estadísticas sobre la seguridad de la información y los derechos fundamentales.

Ospina (2018), desarrolla un modelo de protección de activos de información estratégica a partir de sus estudios en dirección y gerencia enfocados a la seguridad de la información empresarial en Colombia. La investigación tuvo como objetivo aplicar el

Modelo de Protección de Activos de Información Estratégica (M-PAE) para validar los resultados en el sector no virtual. La finalidad es encontrar opciones de mejora que contribuyan a comprender cómo la dirección y gerencia de la seguridad de la información protegen los objetivos estratégicos de una organización. El método utilizado para aplicar el modelo consistió en entrevistas semiestructuradas basadas en cuestionarios configurados sobre variables de interés, según la definición del M-PAE, la muestra fue una organización del sector público en Colombia, con 870 colaboradores. Como conclusiones se obtuvo: i) la protección de activos de información permite la correlación estructural entre los modelos de gobierno y la dirección administrativa, y ii) existe la necesidad de integrar componentes estratégicos y tácticos en los modelos de seguridad de la información.

González y Parrado (2016), elaboraron su tesis entorno a una Guía de gestión de incidentes de seguridad de la información para la Oficina de Tecnología de la Información y la Comunicación (OTIC) del Ministerio de Salud y Protección Social de Colombia. El objetivo principal de la investigación era proporcionar al MinSalud una guía que le permita realizar un adecuado tratamiento de los incidentes y eventos de seguridad de la información basándose en la norma NTC-ISO/IEC 27001:2013. El método utilizado incluyó la identificación de incidentes de seguridad, su clasificación, definición de escalamiento, descripción de procedimientos para la gestión de incidentes, indicación del tratamiento especial para incidentes recurrentes y la presentación de recomendaciones para la prevención de incidentes. Dentro de los resultados de la investigación se encuentra: i) el desarrollo de una metodología para la identificación de incidentes de seguridad de la información; ii) la clasificación de los incidentes según su nivel de criticidad e impacto para la entidad; y por último iii) un proceso de escalamiento para informar o notificar los incidentes de seguridad

de la información, considerando niveles de impacto y responsabilidades.

López (2015) escribió un artículo sobre la Ley 1581, que es la Ley de Protección de Datos Personales en Colombia. El objetivo del artículo fue hablar sobre por qué es importante proteger los datos personales en el contexto de la globalización económica. Para esto, analizó la creación de la Ley 1581 y la describe como una forma de proteger el derecho a la privacidad en un contexto donde varias organizaciones manejan información personal sin el consentimiento previo. El artículo establece dos roles clave en el manejo de datos personales: el "responsable" (quien decide sobre la base de datos) y el "encargado" del tratamiento (quien realiza el tratamiento por cuenta del responsable). Como conclusiones el artículo expresa: i) que la protección de datos personales es esencial en un contexto de globalización y avances tecnológicos; ii) que la Ley 1581 establece principios y deberes para garantizar la protección de la información personal y salvaguardar los derechos a la privacidad; y iii) que la Superintendencia de Industria y Comercio juega un papel crucial como entidad competente, imponiendo sanciones a aquellos que no cumplan con los deberes que se establecen en este contexto.

Melo & Velasco (2008), analizan cómo el Derecho participa en la gestión de la protección de la información en el contexto de las TIC's y las Comunicaciones (TIC). Tiene como objetivo comprender el papel del Derecho en la seguridad de la información, especialmente en el marco de las organizaciones. El método utilizado se basa en un enfoque jurídico-informático que aborda la gestión de la seguridad de la información desde la perspectiva del Derecho Informático. El artículo aboga por un enfoque basado en procesos y destaca la importancia de la alineación de las recomendaciones jurídicas con la estrategia general de la organización en materia de seguridad de la información.

4. MARCO CONCEPTUAL

La revolución tecnológica ha cambiado por completo la forma en que vivimos, trabajamos y nos comunicamos en la era digital. Las TIC's están inmersas en todos los aspectos de nuestras vidas, brindando soluciones innovadoras para optimizar los procesos y aumentar la eficiencia en muchas áreas diferentes. Uno de los ámbitos más afectados por la revolución digital son los procesos de gestión de la información y las comunicaciones afectando los derechos digitales de los usuarios. La información que antes se gestionaba físicamente ha pasado al mundo digital, almacenada en dispositivos electrónicos y en la nube. Esta transición ha traído nuevos desafíos en la seguridad de la información a medida que los datos se vuelven vulnerables a diversas amenazas cibernéticas, como ataques, filtraciones y violaciones de la privacidad.

Teniendo esto en cuenta, existe una necesidad generalizada de que las organizaciones públicas y privadas adopten medidas y herramientas sólidas para garantizar la seguridad de la información transmitida en sus sistemas y redes, protegiendo de este modo los ciber derechos de los usuarios (Téllez, 2018). Las autoridades gubernamentales tienen el deber especial de proteger la información sensible y crítica relacionada con los ciudadanos, los servicios públicos y la administración, lo que blinda también el respeto por los derechos humanos de todos los individuos.

Sin embargo, hay poca discusión sobre los efectos negativos que el uso de la tecnología e Internet tiene en la sociedad en general y en los ciudadanos y sus derechos fundamentales (por ejemplo, la seguridad y los ciber derechos) en particular. Hoy, más que nunca, los ciudadanos corren el riesgo de que su privacidad sea invadida, que roben su información personal e incluso que su salud se vea comprometida por vulnerabilidades en los sistemas

informáticos (González, 2023). En la era de la tecnología, es necesario repensar la seguridad informática para velar por la protección de la información que se genera a diario.

La revolución tecnológica ha permitido la evolución en el tratamiento de la información, pasando de los soportes físicos a los digitales, lo que conlleva riesgos como el ciberataque, las fugas de información y las violaciones del derecho a la privacidad (González, 2023). La situación actual, marcada por la hiper conexión y la cuarta revolución industrial (Schwab, 2016), demandan medidas duras para salvaguardar los derechos digitales, especialmente en la administración pública o en servicios públicos (Téllez, 2018, González, 2023).

4.1. ¿Qué se entiende por ciberespacio?

El ciberespacio, que puede ser definido como el espacio de desarrollo de las actividades humanas a través de las redes digitales (Singer & Friedman, 2014), se ha constituido en un espacio clave en la economía, en la seguridad nacional y en los derechos humanos (Gaitán, 2018) o incluso en escenario para una ciberguerra (Gorman, 2005; OTAN, 2016). En un contexto como el colombiano se requiere revisar marcos legales que permitan proteger los datos en el plano digital y para la defensa de la soberanía digital. (Observatorio de Educación Superior de Medellín, 2019).

Desde la llegada de la primera revolución industrial, el desarrollo y la prosperidad de las economías han dependido de políticas industriales que se ajustan a cada época, lo que implica la adopción de nuevos paradigmas tanto tecnológicos como metodológicos. La formación de recursos humanos, la potenciación de competencias en ciencia y tecnología, el impulso a la autonomía económica de la región, así como la implementación de iniciativas y sistemas de innovación a nivel nacional, han sido factores esenciales en estos procesos. Estos

elementos contribuyen de manera continua a la transformación económica, al comercio internacional y al bienestar social. (Singer y Friedman, 2014).

El contexto internacional se ha caracterizado por una hiperglobalización desde finales del siglo XX y lo que se lleva del siglo XXI, impulsada por la aparición de la tecnología digital, lo que ha provocado profundas transformaciones sociales, políticas y económicas (Fernández, 2018). Esto es un reflejo de la cuarta revolución industrial, también conocida como Revolución 4.0, en la que miles de millones de personas están conectadas a través de dispositivos móviles.

"Un poder de procesamiento, una capacidad de almacenamiento y un acceso al conocimiento sin precedentes" han resultado de esta revolución (Schwab, 2016, p. 9). Esto ha sido posible gracias a un aumento significativo en las invenciones tecnológicas en una variedad de campos, por ejemplo, robótica, internet de las cosas (IoT), inteligencia artificial (IA), *big data*, vehículos autónomos, impresión 3D, ciencia de materiales, nanotecnología, biotecnología, almacenamiento de energía y computación cuántica. Además, se prevé que la creación y difusión conjunta de estas tecnologías tendrán a alterar y combinar las fronteras de los dominios digital, biológico y físico. (Observatorio de Educación Superior de Medellín, 2019; Schwab, 2015).

Schwab (2015), señala que esta revolución se caracteriza, en primer lugar, porque se está desarrollando a un ritmo exponencial, como resultado de un mundo más interconectado y polifacético. En segundo lugar, se destaca la amplitud y profundidad de la revolución digital, que, en combinación con las innovaciones tecnológicas, ocasiona de forma acelerada cambios paradigmáticos sin precedentes en las relaciones internacionales, la economía, los negocios, la sociedad, el gobierno y las personas, modificando el qué y el cómo se hacen las cosas, e

incluso quiénes somos. Por último, están las profundas transformaciones y el impacto en los sistemas de producción, en los gobiernos y la acción estatal interna y externa, así como en las empresas, industrias y la sociedad en su conjunto.

No obstante, esta evolución no se limita únicamente a la tecnología, sino que también es una transformación cultural debido a la hiperglobalización en la que los problemas locales también tienen un papel importante. La glocalización es un fenómeno que se refiere a la importancia que tiene lo local en escenarios globales al utilizar las mismas herramientas tecnológicas para colocar temas locales en la agenda (Fernández, 2018). En esta revolución se evidencia el papel del factor cultural, ya que los elementos culturales son los que permiten que las aplicaciones tecnológicas tengan éxito y sentido, siempre y cuando sean capaces de comunicar y solucionar los problemas que aquejan a las sociedades pluriculturales y pluriétnicas.

La estructuración del ciberespacio, un nuevo escenario de acción humana se evidencia en este nuevo entramado de relaciones humanas. Esta región se ha convertido en un nuevo entorno que, junto con los escenarios tradicionales de presencia humana (tierra, mar, aire y espacio exterior) (Escuela de Altos Estudios de la Defensa, 2014). Constituye el entorno donde se desarrollan las actividades económicas, productivas y sociales de las sociedades contemporáneas. Como resultado, al ser un escenario de relaciones humanas, inevitablemente surgen mecánicas de conflicto entre los distintos grupos o individuos que buscan garantizar y satisfacer sus propios intereses y necesidades, que varían en cualidades y cantidades (París, 2013).

Las definiciones van desde la aceptación del entorno en el que se comunica la información digitalizada a través de redes informáticas hasta formas más complejas que tienen

en cuenta el dominio caracterizado por el uso de la electrónica y el espectro electromagnético en una red interdependiente de infraestructuras de tecnologías de la información y la comunicación (Singer & Friedman, 2014). una red de infraestructuras donde la información se crea, almacena, modifica, intercambia y explora constantemente, lo que permite el funcionamiento adecuado de las estructuras críticas de las sociedades (Ortega, 2012).

El ciberespacio se puede concebir como un área donde se llevan a cabo actividades bélicas y no bélicas. Además, es transversal e integra las dimensiones naturales del dominio humano. Esto es posible gracias al interminable número de interconexiones, así como al hecho de que muchas de las herramientas, maquinarias y otros dispositivos que se utilizan en el espacio natural dependen de la información generada en el ciberespacio para funcionar (Gaitán, 2018).

Según esta teoría, el ciberespacio puede superar los límites geopolíticos y afectar las fronteras de los países, lo que presenta graves peligros para la seguridad, la defensa y la soberanía nacional. Sin embargo, también permite la integración de las operaciones de la infraestructura esencial para la gobernabilidad, el comercio y la seguridad nacional. (Gorman, 2005).

La naturaleza conflictiva de los humanos en el ciberespacio da paso a la lógica de la guerra en el ciberespacio, donde existen riesgos y amenazas para las personas, los Estados, las empresas y los grupos sociales en general. Según The Economist (2010), el ciberespacio es el quinto dominio de batalla, una idea que la Organización del Tratado del Atlántico Norte (OTAN, 2016) ha aceptado y respaldado, y es un dominio militar legítimo que permite a las organizaciones públicas y privadas llevar a cabo acciones coordinadas de protección militar.

4.2. Derechos humanos y el nuevo mundo digital

Los derechos fundamentales, que incluyen la privacidad o el acceso a la información (Asamblea General de la ONU, 1966), ponen de manifiesto ciertas propiedades que deben ser analizadas en un contexto digital. Se estudia, por ejemplo, una cuarta generación de derechos humanos centrada en garantías digitales por autores como León (2020) o Morales (2018) referenciadas en documentos de políticas como el Reglamento General de Protección de Datos (Parlamento Europeo, 2016). En el caso de Colombia, esto se traduce en retos como la posibilidad de regulación de la inteligencia artificial o la lucha contra la desinformación en las redes sociales (Soler, 2019).

Los derechos fundamentales son derechos y garantías inherentes a las personas, que el ordenamiento jurídico considera como derechos subjetivos inviolables y limitan el uso del poder estatal y privado (Téllez, 2018). Su especial naturaleza jurídica les confiere una mayor protección y la capacidad de exigir su cumplimiento de forma directa e inmediata.

En cuanto a su clasificación, la doctrina y la jurisprudencia han establecido diversas categorías, las más famosas son: derechos civiles y políticos, incluido el derecho a la vida, la libertad personal, la igualdad y el debido proceso, etc., derechos económicos, sociales y culturales como el derecho a la salud, el derecho a la educación, al trabajo y a una vivienda digna, derechos colectivos y derechos ambientales como los derechos de los grupos étnicos y el derecho a un medio ambiente sano (Asamblea General de las Naciones Unidas, 1966).

Aunque podemos mencionar varios tipos de derechos humanos, como el derecho al trabajo, el derecho al voto y el derecho a la atención médica, entre otros, lo más obvio es aplicar esta lente desde la perspectiva digital a los derechos humanos relacionados con la comunicación, el acceso y el control de la información. El derecho a la intimidad y el derecho

a buscar y recibir información son los dos derechos que se abordan en este documento.

Shue (2002) destaca que los derechos humanos protegen los intereses humanos vitales; es decir, se tienen derechos humanos porque son necesarios para protegernos de ciertas amenazas. La historia del pensamiento filosófico y del derecho ha destacado la importancia del ser humano en el universo, su lugar y su papel en una comunidad, así como la conducta social que debe tener. El reconocimiento legal del valor de una persona y su propiedad jurídica sobre las prerrogativas que pueden protegerlo en sus relaciones con el poder político y otros miembros de la sociedad se realizó tarde, bastante lento y con sacrificios reales. Pero después de las dos conflagraciones mundiales con trágicas implicaciones para la humanidad, podemos afirmar que los derechos del individuo han adquirido un estado bien definido no solo dentro de los límites de la legislación nacional, sino también al nivel de las organizaciones supraestatales. Los derechos fundamentales encuentran su base filosófica en diversas corrientes de pensamiento que contribuyen a su conceptualización y defensa.

Aparte del mundo físico donde los derechos humanos son reconocidos, existe un nuevo espacio que muchos llaman ciberespacio, en donde la presencia de personas en los espacios virtuales es innegable y en este entorno tienen lugar muchas transacciones y relaciones. Por ello, es necesario defender el reconocimiento y protección de los derechos humanos en este nuevo mundo virtual. Siguiendo el modelo de derechos humanos generacional propuesto por Vasak (1977), muchos autores han afirmado que estamos ante una nueva generación de derechos humanos, especialmente la cuarta generación, entre ellos León (2020), Morales (2018); derechos en un nuevo entorno digital en el que se debe también velar por la protección de dichos derechos.

Reconocidos como valores intrínsecos de la humanidad, los derechos humanos han

sido objeto de teorías y regulaciones legales a través del pacto entre el individuo y el poder público ejecutivo, estableciendo así las “libertades públicas” y “obligaciones públicas”. Este marco abarca la relación con el poder legislativo y judicial, en el contexto del “contrato social” (Rosseau, 1996). Sin embargo, la aceptación de estos derechos no ha sido uniforme entre los Estados, ni se han configurado de manera idéntica. La aparición de organizaciones internacionales y los eventos históricos del siglo XX facilitaron la extrapolación de catálogos nacionales e interestatales de derechos, promoviendo un número limitado de derechos junto a salvaguardas específicas., promoviendo un número limitado de derechos junto a salvaguardas específicas.

Se deben analizar estos derechos en un contexto amplio, considerando las normas e instituciones que los protegen como un conjunto de garantías legales e institucionales. Derechos como la libertad, igualdad y seguridad del ser humano, junto con el derecho a la dignidad, deben ser tratados prioritariamente y protegidos por mecanismos judiciales e institucionales a nivel estatal, regional e internacional. La efectividad de estas protecciones no debe verse comprometida por intervenciones políticas o militares (Shue, 2002).

En este complejo y dinámico contexto legal, es fundamental preservar la dignidad humana, que es la esencia de todos los derechos fundamentales. Por ello, la privacidad del individuo, resguardada por medios legales apropiados, puede ser el último camino en la defensa de su condición como persona libre dotada de derechos frente a las autoridades y otros miembros de la comunidad.

4.3. Seguridad de la Información: Derechos Digitales

La seguridad informática pone sus bases sobre tres pilares: la confidencialidad, la integridad y la disponibilidad (ONSC, 2019). En el entorno digital actual, marcos como el

ISO/IEC 27001 y el NIST SP 800-53 (NIST, 2018) son necesarios para proteger la información de los usuarios en la red; sin embargo, estos marcos necesitan evolucionar para poder afrontar amenazas tales como el *ransomware* o la suplantación de identidad (McKinsey & Company, 2021). Del mismo modo, la resiliencia cibernética debe integrar otros enfoques de diferentes disciplinas, generar una multidisciplinariedad, por ejemplo, desde el derecho a la ingeniería (Donaldson et al., 2015).

Para comprender el mundo digital, es necesario reconocer el aumento de la densidad digital en el mundo físico, el aumento de los flujos de información desde objetos conectados y el cambio en las dinámicas humanas, por lo que las personas priorizan los contactos y relaciones desde dispositivos móviles para sus actividades diarias y aumentar sus posibilidades y oportunidades (McKinsey & Company, 2021). Este escenario de comunicación y control cibernético donde ahora se desarrollan las actividades de la sociedad en general se convierte en una plataforma de desarrollo social y económico que conecta a la nación con los desafíos de la economía digital y, al mismo tiempo, con las tensiones que generan los riesgos cibernéticos, cuya particularidad es ser sistémicos, emergentes y disruptivos (Cano, 2019).

Es difícil encontrar un concepto claro de seguridad porque la seguridad es un valor cuyo significado depende del contexto, por ejemplo, hablar de seguridad ambiental, seguridad alimentaria, seguridad laboral es diferente a mencionar seguridad humana, seguridad nacional o seguridad informática. (Téllez, 2018).

La seguridad de la información es un campo interdisciplinario donde actúan distintas disciplinas desde el derecho, la ingeniería e incluso la comprensión sociológica del ser humano. En esta nueva era de la seguridad de la información se promueve la protección de los

activos de información contra diversas amenazas con el fin de garantizar su confidencialidad, integridad y disponibilidad.

Confidencialidad significa que sólo el personal u organizaciones autorizadas pueden acceder a la información. Integridad significa mantener la exactitud, integridad y estado original de la información y evitar cambios no autorizados. La disponibilidad garantiza que los usuarios legítimos puedan acceder y utilizar información y sistemas cuando sea necesario. (Oficina Nacional de Seguridad del Ciberespacio - ONSC, 2019).

No obstante, existen diversas amenazas y riesgos que socavan estos principios, como ciberataques, *malware,* errores técnicos, errores humanos, y hasta desastres naturales que pueden dañar o afectar el acceso a las redes y a la información. Por lo que es necesario implementar controles y medidas de seguridad para mitigar estos riesgos, como políticas de seguridad, controles de acceso, cifrado de datos, copias de seguridad, monitorización de redes, formación de empleados, etc., estrategias y mecanismos que aseguren los ciber derechos o derechos digitales de los usuarios (Téllez, 2018). En este sentido, las buenas prácticas y los estándares internacionales proporcionan pautas y marcos de referencia para la gestión de la seguridad de la información. Uno de los estándares más reconocidos es el estándar ISO/IEC 27001, que define los requisitos para la implementación de un sistema de gestión de seguridad de la información (SGSI) en una organización (Organización Internacional de Normalización – ISO, 2013). Otro marco ampliamente utilizado es el propuesto por el Instituto Nacional de Estándares y Tecnología (NIST), que incluye publicaciones como NIST SP 800-53 sobre Controles de seguridad y privacidad y Marco de mejora de la ciberseguridad de infraestructuras críticas (NIST, 2018).

La seguridad informática incluye garantizar que ningún componente del sistema

(hardware, software, personal de TI, red, usuarios, datos y programas) esté en riesgo y que no se permita a personas no autorizadas acceder a la información del sistema, dañar, modificar, eliminar o realizar cualquier tratamiento no autorizado (Téllez, 2018).

La influencia de la nueva realidad digital ha dado lugar a una variedad de interpretaciones sobre la dinámica de la sociedad en Colombia. Por un lado, el sector empresarial ha aprovechado para concretar proyectos que estaban en estudio y ha creado nuevas experiencias con sus clientes que han cambiado por completo la forma en que se relacionan con sus compradores. Por otro lado, el sector de la salud, como el foco de atención actual, ha debido adaptarse a su realidad digital. Esto significa que es necesario avanzar rápidamente para crear y establecer una cultura organizacional de seguridad de la información (Donaldson et al., 2015).

Para aumentar la resiliencia de sus operaciones frente a adversarios que intenten pasar inadvertidos en medio de la interacción y el acoplamiento de las soluciones disponibles para su operación, las infraestructuras críticas cibernéticas, ahora con una mayor interacción en modalidad remota, deben comprender, conocer y asegurar cómo están sus relaciones con terceros de confianza (Dupuy et al., 2021; Boyes, 2015; WEF, 2021).

La forma en que el Estado define su relación con la ciudadanía cambia con el aumento de la superficie digital de interacción. Debido a este cambio, los ciudadanos se apropian de su papel como participantes en una democracia donde diferentes actores pueden opinar y generar tendencias, bien sea en sentido propositivo o con posiciones contrarias o reaccionarias (Soler, 2019). En este contexto, se crea un camino de inestabilidad e incertidumbre causado por las noticias falsas, la desinformación y la mal información. Las tribunas de las redes sociales se convierten en lugares ideales para la controversia y la

movilización de imaginarios mediante métodos que han sido utilizados con éxito para impactar a la población de manera positiva o negativa (Ganghi et al., 2011).

4.4. Protección de Datos Personales

En Colombia, la Ley 1581 de 2012 y su decreto reglamentario establecen bases para el tratamiento de datos personales, pero persisten retos como la falta de conciencia ciudadana y la adopción de tecnologías como el *blockchain* para garantizar auditorías transparentes (Maqueo et al., 2017). La Declaración de Derechos de Internet de la APC (2022) refuerza la necesidad de accesibilidad, privacidad y gobernanza inclusiva. Debemos primero hablar de los llamados derechos digitales, también llamados ciber derechos. El 14 de marzo de 2006, la Asociación para el Progreso de las Comunicaciones (APC) publicó la primera versión en inglés de la Declaración de Derechos de Internet de APC. Esta asociación tiene una visión en la cual *"Todas las personas usan y configuran Internet y las tecnologías digitales de modo que contribuyan a un mundo más justo y sustentable y a un mayor cuidado propio, de los/as demás y de la Tierra."* (APC, 2022). Esta asociación, sostiene que el internet, será solo una herramienta de empoderamiento para todo el mundo si se siguen los siguientes criterios:

Tabla 2.

Derechos Digitales según la APC

Derechos de los usuarios de Internet y de las TIC	
Acceso a Internet para todos y todas	Privacidad, vigilancia y encriptación
Libertad de expresión y asociación	Gobernanza de internet
Acceso al conocimiento	Conciencia, protección y realización de los derechos
Intercambio de aprendizaje y creación de software libre y desarrollo tecnológico	

Fuente: (APC, 2022)

Con la llegada de la era digital, los sistemas informáticos hacen una recolección, un procesamiento y una transmisión de una gran cantidad de datos personales; tal es así que su protección se ha convertido en un derecho fundamental. El origen de estos derechos proviene de un conjunto de principios fundamentales cuya finalidad es garantizar que el tratamiento de los datos se produzca de forma legal y correcta (Maqueo et al., 2017).

En particular, estos principios son la fiabilidad, la licitud, la transparencia de la finalidad de la recolección de datos y su recolección únicamente necesaria, limitación en el tiempo y la confidencialidad (Parlamento Europeo y Consejo de la Unión, 2016). Estos son principios que garantizan que la recolección y el tratamiento de los datos personales se realicen con transparencia y con apego a libertades y derechos individuales (Parlamento Europeo y Consejo de la Unión, 2016). Esto genera confianza de las personas hacia las instituciones que llevan la administración de sus datos y evita la violación de la privacidad y acciones judiciales en contra de sus derechos digitales.

5. MARCO NORMATIVO

El Capítulo II de la Constitución Política de Colombia, promulgada en 1991, incluye una larga lista de derechos fundamentales y determina mecanismos para garantizar su defensa, como la Acción de Tutela (artículo 86); valora la relevancia de los tratados internacionales en materia de derechos humanos (artículo 93) y el bloque de constitucionalidad y la génesis de las acciones constitucionales que les otorgan base (Corte Constitucional colombiana, C-225/95). La Constitución de 1991, basada en la dignidad humana, democracia participativa, separación de poderes y Estado social de derecho (Corte Constitucional de Colombia, T-227/03), es la que ha hecho posible esta mayor protección.

La seguridad de la información se ha convertido en un tema de elevado interés para la sociedad, en un sistema internacional cada vez más interconectado y dependiente de la tecnología. La circulación de datos personales y financieros es cada vez más común. Por esta lógica, los Estados del mundo han promovido un conjunto de leyes y políticas para frenar los ciberataques y para asegurar la información personal de las personas.

Giraldo y Bello (2021) sostienen que, a causa del rápido avance de las tecnologías de la información y la comunicación, la ciberseguridad es un asunto que cobra cada vez más importancia en Colombia. Por lo tanto, el gobierno ha tomado acciones para abordar esta problemática, incluyendo la creación de entidades especializadas en ciberseguridad, como ColCERT (Grupo de Respuestas a Emergencias Cibernéticas en Colombia), así como la implementación de regulaciones específicas.

En un contexto de creciente conectividad y digitalización, el país ha admitido la relevancia de salvaguardar los datos privados y la información en línea. El Decreto 1377 de 2013 y la Ley 1581 del 2012 son dos de las leyes más relevantes en Colombia que regulan el sistema de protección de datos personales. Asimismo, la Ley 1955 de ciberseguridad fue aprobada en el año 2019. Esta ley exige que las entidades públicas y las empresas tomen medidas de seguridad con el fin de prevenir y responder a los ciberataques. El Consejo Nacional de Ciberseguridad fue fundado en el 2020 con el objetivo de organizar y liderar las acciones de prevención y respuesta ante las amenazas vinculadas a la ciberseguridad en Colombia.

Tabla 3.

Marco Normativo Nacional

Entidad	Norma	Descripción	Detalle
Constitución Política de Colombia	Artículo 15	"Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas"	Reconoce el derecho fundamental a la intimidad personal y familiar, al habeas data y a la protección de datos personales. Base constitucional para la Ley 1581 de 2012 y su reglamentación. Ampliación con: Corte Constitucional, Sentencia C-748 de 2011
	Artículo 20	"Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación"	Garantiza la libertad de información y el derecho a acceder a documentos públicos, con límites en casos de seguridad nacional o derechos de terceros.
	Artículo 93	"Los tratados y convenios internacionales ratificados por el Congreso, que reconocen los derechos humanos y que prohíben su limitación en los estados de excepción, prevalecen en el orden interno. Los derechos y deberes consagrados en esta Carta, se interpretarán de conformidad	Incorpora los tratados internacionales de derechos humanos como parte del bloque de constitucionalidad, lo que obliga al Estado a alinear su normativa con estándares globales

		con los tratados internacionales sobre derechos humanos ratificados por Colombia"	Ampliación con: Corte Constitucional, Sentencia C-225/95
	Ley 1581 de 2012.	*"Por la cual se dictan disposiciones generales para la protección de datos personales"* Establece los principios y derechos relacionados con el tratamiento de datos personales y crea el régimen de protección de datos en Colombia.	Multas hasta 2.000 SMMLV por incumplimiento (Superintendencia de Industria y Comercio, Resolución 68377 de 2021).
Congreso de Colombia	Ley 1273 de 2009 (Delitos Informáticos)	*"Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones"*	Hasta 120 meses de prisión para delitos graves (Fiscalía General de la Nación, 2023). Introduce delitos informáticos en el Código Penal colombiano, como el acceso abusivo a sistemas informáticos y la violación de datos personales.
	Ley 1978 de 2019	*Por la cual se moderniza el Sector de las Tecnologías de la Información y las Comunicaciones -TIC, se distribuyen competencias, se crea un Regulador Único y se dictan otras disposiciones"*	Creación del Consejo Nacional de Ciberseguridad para coordinar políticas públicas. Obligatoriedad de reportar incidentes cibernéticos a ColCERT (Art. 56)

	Ley 1341 de 2009	*"Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones"*	
Gobierno Nacional	Decreto 1074 de 2015	*"Por medio del cuál se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo"*. Reglamentación de la Ley 1581	Incluye a todas las entidades públicas y privadas que manejen datos personales, con excepciones para seguridad nacional.
	Decreto 1377 de 2013	*"Por el cual se reglamenta parcialmente la Ley 1581 de 2012"* Especificando aspectos relacionados con el tratamiento de datos personales y la autorización para su uso	
	Decreto 2573 de 2014	*"Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones"*	Estándares mínimos de seguridad para entidades públicas.
MinTIC	Resolución No. 00500 de marzo 10 de 2021	*Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital"*	

Superintendencia de Industria y Comercio	Circular externa No. 003 de 2024	Instrucciones para los administradores societarios en relación con el Tratamiento de Datos personales.	Guías para la implementación de medidas de seguridad en empresas.
Fiscalía General de la Nación	Resolución 117 de 2023	*"Por medio de la cual se reglamenta y conforma la Dirección Especializada Contra los Delitos Informáticos"*	Protocolos para investigar delitos cibernéticos.
Acuerdo del Consejo de Seguridad Nacional del 5 de diciembre de 2013.	Consejo Nacional de Ciberseguridad	Entidad creada para coordinar y dirigir operaciones de prevención y respuesta a riesgos de ciberseguridad en Colombia.	Entidad especializada en la gestión de incidentes de ciberseguridad
Grupo de Respuesta a Emergencias Cibernéticas de Colombia-ColCERT	Creadao por MinTIC en 2022	Grupo de Respuestas a Emergencias Cibernéticas en Colombia.	
Corte Constitucional	Sentencia C 225/95	Derecho Internacional Humanitario	Reafirma la importancia del bloque de constitucionalidad y la aplicación de tratados internacionales de derechos

Fuente: Elaboración propia

Tabla 4.

Marco Normativo Internacional

Convenio/Reglamento	Descripción	Detalle
Convenio de Budapest (2001)	Primer tratado internacional sobre ciberdelincuencia	Ratificado por Colombia en 2018. Council of Europe, (2021).
Reglamento General de Protección de Datos (RGPD, UE 2016/679)	La Ley 1581 se alinea con principios como minimización de datos y privacidad por diseño	European Commission, (2020)
Resolución 70/237 de la ONU (2015)	Promueve la cooperación internacional en ciberseguridad y protege derechos humanos en entornos digitales	UN General Assembly, (2015)

Fuente: Elaboración propia

6. DISCUSIÓN

La normatividad colombiana tiene tanto puntos fuertes como débiles en su aplicación. La Constitución Política de 1991 establece en sus artículos 15, 20 y 93 derechos explícitos en el campo digital. El artículo 15 se refiere a derecho fundamental a la intimidad y a la protección de datos de carácter personal, pero con el respaldo de la jurisprudencia de la Corte Constitucional, artículo C-748 de 2011. Sin embargo, este marco constitucional no se dedica a impedir de manera expresa los nuevos desafíos que representan las nuevas tecnologías, como por ejemplo la inteligencia artificial o el denominado internet de las cosas, sino que genera vacíos de contenido que deben ser analizados en los nuevos escenarios que se van planteando.

La Ley 1581 de 2012 y los decretos reglamentarios que la regulan (1074 de 2015 y 1377 de 2013) se convierten en el corazón de la regulación del régimen de protección de

datos en Colombia. Establecen pilares básicos como el consentimiento informado, la finalidad específica y las medidas de seguridad en el tratamiento de datos personales. Pero la implementación de esta regulación encuentra obstáculos evidentes, especialmente en el contexto de las PYMEs, donde los costos de cumplimiento de medidas técnicas como el cifrado de datos pueden ser prohibitivos. Pero la regulación no llega a dar respuesta a los retos que plantea el almacenamiento transfronterizo de datos en la nube, algo tan habitual en la economía digital globalizada.

En el campo penal, la Ley 1273 de 2009 y su decreto reglamentario 2364 de 2012 definen los delitos informáticos, tales como el acceso ilícito a sistemas informáticos o la violación de datos personales. La aplicación de esta normatividad también contiene limitaciones que se deben analizar. Por un lado, los delitos como el ransomware o el tráfico de datos en la dark web, requieren de técnicas de investigación que dificultan la tipificación de las conductas como conductas delictivas; por el otro, parece existir un desfase entre los tipos penales definidos y las nuevas modalidades delictivas que son constantes en el ciberespacio.

La Ley 1978 de 2019 supone la modernización del marco regulador del sector de las TIC y la creación del Consejo Nacional de Ciberseguridad. Este organismo ha tenido dificultades operativas, incluidas limitaciones presupuestarias, que impiden llevar a cabo de una manera adecuada la coordinación de las políticas públicas respecto de esta materia. Las normas sectoriales como la Resolución 733 de 2022 del MINTIC o la Circular 002 de 2023 de la Superintendencia de Industria y Comercio denota estándares técnicos en el ámbito, pero su cumplimiento es desigual, especialmente entre las entidades públicas regionales o municipales, en otras palabras, existe la norma, pero esta no es aplicable.

Frente al régimen normativo colombiano, el que está presente frente a estándares internacionales como el Convenio de Budapest o el Reglamento General de Protección de Datos de la Unión Europea permite poner de manifiesto déficits en muchos aspectos que deberían ser de fortaleza. El país ha ido avanzando en armonizar su legislación con estos convenios, pero plantea déficits sobre todo lo relativo a la protección de datos biométricos, la regulación de la inteligencia artificial o los mecanismos de cooperación internacional para la persecución de los ciberdelitos.

La jurisprudencia de la Corte Constitucional y de las altas cortes ha tenido un momento de protagonismo en la adaptación del marco normativo a los retos de este nuevo o ya no tan nuevo escenario digital; en la medida en que la Ley estatutaria sobre protección de datos no se encuentra en la cima de la pirámide del ordenamiento jurídico, la normativa existente reductora del panorama garantiza en su aplicación, dejándolo donde la interpretación jurisprudencial se convierte en la salvaguarda de todos los aspectos relacionados.

Colombia cuenta con un marco normativo que podría considerarse relativamente completo (en lo que corresponde a la regulación de la protección de datos y la ciberseguridad), pero su efectividad se ve truncada por la falta de implementación, recursos técnicos y financieros, y la velocidad a la que cambia el mundo digital. Se hace necesaria la articulación de las normas; se hace necesaria la asignación de recursos presupuestales para los organismos de control; se hace necesario que la legislación se ponga al día permanentemente, para la transformación de los desafíos que crea el nuevo entorno digital.

Desde una perspectiva jurídico-constitucional, se trata de que el ordenamiento jurídico colombiano sí reconoce y protege derechos fundamentales de las personas como la

privacidad o el habeas data, pero su eficacia, entre otras cosas, también está sujeta a los desarrollos institucionales y a la evolución del contexto legal mismo. Más que evidenciar una insuficiencia normativa en sí misma, el análisis es capaz de mostrar que hay que reforzar la interacción que existe entre las normas constitucionales, el desarrollo legislativo y la puesta en plano.

La protección de los derechos humanos en el entorno digital hay que defenderla no solo con buenas leyes, sino con toda una cultura institucional y cultural que haga de las leyes una realidad y proteja y vele por los derechos de los ciudadanos sin importar en qué escenario puedan estos ser vulnerados.

En cuanto al marco normativo internacional en torno a la ciberseguridad y la protección de datos personales, ésta ha tenido una incidencia en la configuración de las políticas digitales de Colombia para establecer estándares que intenten ir de la mano con la legislación nacional y los retos del entorno digital en el escenario internacional. En este sentido, algunos de los instrumentos internacionales más relevantes son: el Convenio de Budapest, el Reglamento General de Protección de Datos (RGPD) de la Unión Europea y la Resolución 70/237 de la ONU, cada uno de los cuales posee una perspectiva complementaria pero igualmente relevante en la configuración del derecho digital colombiano.

El Convenio de Budapest (2001) ratificado por Colombia en 2018 (ratificación que permite justificar el proceso de aceptación por parte de Colombia del citado marco normativo), da cuenta de ser el primer tratado internacional vinculante sobre cibercriminalidad, que fue elaborado por el Consejo de Europa con el objetivo de armonizar las legislaciones de modo tal que permita la cooperación internacional reforzada en la investigación y en el enjuiciamiento de delitos informáticos (acceso no autorizado a sistemas

informáticos, fraude informático, pornografía infantil, etcétera). La ratificación del Comité de Budapest se traduce, por tanto, en la posibilidad de que Colombia pueda fortalecer en el terreno nacional sus capacidades técnicas y jurídicas frente a una cibercriminalidad cada vez más compleja (en particular la proveniente de redes criminales internacionales).

La clasificación que se considera tradicional de los derechos humanos en tres generaciones (Torres, 2009) se complementa por los estudios adelantados por Ferrajoli (2011) y Díaz (2009), quienes agregan una cuarta generación de derechos, asociados a las nuevas tecnologías, la bioética y la sostenibilidad ambiental. Este análisis toma como base, para la protección de los derechos digitales, la adopción de medidas, aun siendo de manera general, para la seguridad de la información en el país, dado que Colombia es el tercer país a nivel mundial con más cibercriminalidad, tal como lo señala un estudio en el portal Guapacho, (2025), especializado en estos temas.

Colombia presenta un crecimiento alarmante de la ciberdelincuencia, con más de 350.000 víctimas en el 2023 (Infobae, 2024) y Bogotá se convierte en el centro de esos delitos, donde se tiene que concentran el 60% de los delitos denunciados, entre ellos hackeo, suplantación de identidad e infracciones financieras (Concejo de Bogotá, 2025). De acuerdo con Diario ADN (2025), los ataques han aumentado un 40% en los dos últimos años, mostrando que los sistemas de información son vulnerables a ataques cibernéticos y por otro lado que las medidas de protección deben fortalecerse.

Algunos de los delitos que más se repiten son:

A. ***Phishing y suplantación de identidad***: Entendido como el ingreso no autorizado a cuentas bancarias.

B. ***Ransomware***: Entendido como el secuestro de datos a cambio de rescates.

C. ***Estafas financieras:*** Mediante la ingeniería social, un estudio de La República, (2025), señala los aumentos de estos cibercrímenes. Dando la certeza antes dada, se debe exigir una respuesta integral que contemple marcos legales robustos, cooperación internacional y políticas de educación digital.

6.1 Protección de Derechos Humanos en la Seguridad de la Información

Tabla 5.

Constitución Política y Protección de Derechos Digitales

Norma	Artículo	Protección	Limitaciones/Desafíos	Referencia
Constitución Política de Colombia (1991)	Art. 15	Garantiza el derecho a la intimidad personal, familiar y al habeas data.	No aborda riesgos digitales como el *phishing* o el robo de datos masivos.	Corte Constitucional (2015)
Constitución Política de Colombia (1991)	Art, 20	Protege la libertad de expresión, incluyendo su ejercicio en entornos digitales.	No regula específicamente discursos de odio o *fake news* en redes sociales lo que atenta en la vulneración de derechos humanos fundamentales.	Rodríguez (2023)

Fuente: Elaboración Propia

Tabla 6.

Leyes Específicas en Ciberseguridad

Norma	Año	Objetivo Principal	Avances	Vacíos Legales	Referencia
Ley 1273 (modificada en 2023)	2009	Tipifica delitos informáticos (ej., acceso abusivo a sistemas, fraude electrónico).	Permite judicializar ataques como *ransomware* y suplantación de identidad.	No cubre delitos emergentes como *deepfakes* o criptoestafas avanzadas.	MinJusticia (2023)
Ley 1581	2012	Regula el tratamiento de datos personales y establece sanciones por violaciones	Exige consentimiento explícito para el uso de datos personales.	No aplica eficazmente a empresas extranjeras que procesan datos de colombianos	Superintendencia de Industria y Comercio (2024)
Decreto 555	2023	Fortalece capacidades de la Policía Nacional y el MinTIC para combatir ciberdelitos.	Crea la Unidad de Respuesta a Incidentes Cibernéticos (ColCERT).	Limitaciones presupuestales para implementación en regiones.	MinTIC (2025)

Fuente: Elaboración Propia

Tabla 7.

Tratados Internacionales Ratificados por Colombia

Tratado/Convención	Año de Ratificación	Objetivo Principal	Impacto en Colombia	Referencia
Convenio de Budapest sobre Ciberdelincuencia (actualizado)	2024	Armoniza legislaciones nacionales y facilita la cooperación internacional contra crímenes digitales.	Permite extradición de cibercriminales y acceso a pruebas en servidores extranjeros.	W Radio (2024)
Acuerdo de Cooperación con la OEA en Ciberseguridad	2025	Fortalece capacidades técnicas y de investigación en ciberseguridad.	Capacitación a fiscales y jueces en delitos digitales (ej., malware financiero).	OEA (2025)

Fuente: Elaboración Propia

No obstante, la situación que se presenta anteriormente, el país aún enfrenta y presenta una realidad en el ámbito de su implementación, sobre todo en relación con el entrenamiento y capacitación del personal de las autoridades judiciales y la adaptación de procedimientos específicos para los casos en donde aparecen involucradas evidencias digitales en sucesos de una o varias jurisdicciones.

Todos esos instrumentos internacionales ayudan a que Colombia desarrolle un andamiaje normativo consistente en lo digital. Pero su eficacia depende de que exista un modelo de implementación que sortee retos como la escasez de especialización técnica en las instituciones, la falta de recurso económico para asegurar la ciberseguridad o la alta necesidad de modernizar las vías de cooperación penal internacional; es decir, que la adopción de estándares internacionales vaya de la mano de políticas públicas integrales que mejoren las capacidades de las instituciones y que logren promover una cultura de protección de datos y ciberseguridad entre todos los agentes involucrados: desde el sector público hasta

las empresas, pasando por los y las ciudadanas. Solo así podrá permitirse que el andamiaje normativo supere el papel y se constituya en un instrumento revelador para que la protección de los derechos humanos efectivamente se encuentre en el entorno digital, más allá del físico.

6.2 Marco Jurisprudencial sobre Derechos Digitales en Colombia

La idea del acceso a Internet como un derecho humano en el sistema interamericano de derechos humanos llegó a su máximo punto con la Opinión Consultiva OC-23/17, emitida por la Corte Interamericana de Derechos Humanos (CIDH), estableciendo tres elementos principales, íntimamente relacionados con el derecho al acceso a Internet, que a la vez recogen principios valiosos, a saber; primero, la libertad de expresión (Art. 13 de la Convención Americana); segundo, el derecho a la información y tercero, la participación democrática efectiva.

En este escenario, la CIDH conceptualiza el internet como un "espacio virtual de ejercicio de derechos fundamentales" (CIDH, 2017), lo cual delimita el carácter habilitante para la realización de otros derechos. En segundo lugar, la Corte estableció una obligación positiva de garantizar el acceso universal al prohibir expresamente los bloqueos arbitrarios y estableciendo la protección de la neutralidad de la red. Tercero, la Corte estableció que toda restricción tenía que pasar el estricto examen del principio de proporcionalidad demostrando necesidad, adecuación, y legalidad.

En el escenario colombiano, este pronunciamiento ha tenido un efecto concreto. Un caso ejemplar es el de la Sentencia T-277/22, en la que la Corte Constitucional, siguiendo en este caso los lineamientos directos de la OC-23/17, protegió el derecho al acceso a Internet para comunidades rurales que enfrentaban desconexiones arbitrarias. Esta sentencia dio cuenta de cómo los estándares interamericanos se insertan en el derecho interno y nutren la protección de los derechos digitales.

6.3 Desarrollo Jurisprudencial Interno: La Corte Constitucional como garante

Sentencia C-748 de 2011: Base del Habeas Data digital

El análisis de constitucionalidad de la Ley 1266 de 2008 sobre protección de datos financieros dio luz a una de las sentencias fundamentales en materia de derechos digitales: la Sentencia C-748 de 2011. La misma constituye la base sobre la que se ha construido la protección de datos personales en Colombia.

La Corte Constitucional realizó en esta sentencia una doble contribución fundamental: la reafirmación del habeas data (Art. 15 de la Constitución Política) como un derecho autónomo que se extiende a el derecho al conocimiento sobre qué información personal se encuentra sometida a tratamiento, por otro lado, el derecho a conocer, actualizar y rectificar datos personales y por último, el derecho a suprimir datos personales, en los eventos en que haya dejado de tener justificación de orden legal para ser objeto de tratamiento.

Tabla 8.

Casos recientes relacionados con el tema abordado (2024-2025)

Caso	**Medio/Noticia**	**Problema Jurídico**	**Fallo/Análisis**	**Relación con Derechos Digitales**
Suplantación Digital Masiva (2024)	*El Tiempo* (15/03/2024)	Robo de identidad en redes sociales	Tutela T-145/24: Ordenó a Facebook implementar verificación biométrica	Derecho a la identidad digital (Art. 15 CP)
Corte ordena reparación por filtración de datos de salud	*La República* (10/05/25)	Filtración de historias clínicas en una EPS	Sentencia SU 256/25: Conden a EPS por violar Ley 1581 de 2012	Protección de datos sensibles

Bloqueo de internet en protestas	*El País* (22/08/24)	Alcaldía de Cali restringió acceso	T-588/24: Inconstitucional por violar OC-23/17	Libertad de expresión en entornos digitales

Fuente: Elaboración propia

El entorno jurídico en Colombia ha ido presentando un cambio significativo en la salvaguarda de los derechos digitales, tal y como se puede analizar en tres casos actuales que han sido sonoros porque marcan hitos en el campo del derecho digital. Estos fallos no solo son un reflejo más de la capacidad del sistema judicial para adecuarse a problemáticas propias de la tecnología, sino que establecen criterios que pueden llegar a ser relevantes en la protección de los colombianos en el área de los derechos digitales.

6.4 El caso Facebook: La identificación digital como derecho fundamental

En marzo del 2024 se expone un escándalo de suplantación masiva de identidades en redes sociales. La Corte Constitucional, en la sentencia T-145/24, da un paso al ordenar a Meta (Empresa matriz de Facebook) la instalación de sistemas de verificación biométrica para cuentas de alto impacto social. El fallo es un punto de corte por razones muy amplias: primero, porque termina por reconocer explícitamente el derecho a la identificación digital como desarrollo directo del artículo 15 de la Constitución, que tutela el mismo buen nombre y la autodeterminación informativa; segundo, porque ordena el deber de las plataformas digitales de proteger a sus usuarios, no solo si se dedican a moderar contenidos.

Este antecedente ha logrado un debate nacional en torno a la urgencia de regular con mayor exigencia las obligaciones de las *Big Tech* en Colombia, en especial en materia de garantizar la prevención de fraudes y la suplantación.

6.5 El escándalo de las historias clínicas

Mayo de 2025 dejó al descubierto una de las mayores vulneraciones de la privacidad reciente del país, cual fue el escándalo en torno a la EPS que hizo pública la historia clínica de medio millón de pacientes. La sentencia SU-256/25 no sólo dejó en entredicho a la entidad de la salud como tal, sino que sentó importantes fundamentos:

A. La reafirmación de que los datos médicos asumen la categoría de informaciones sensibles y por lo tanto deberían tener una protección reforzada por la Ley 1581 de 2012.
B. La obligación de protocolo de seguridad bajo estándares internacionales (ISO 27001).
C. La imposibilidad de que el simple "cumplimiento formal" de las normas de protección de datos fuera suficiente, dado que se evidencia que se requiere una gestión del riesgo activo.

Este caso también evidenció las graves consecuencias que pudo tener el manejo negligente de los datos personales, en especial en el caso del sector salud, dado que la información es particularmente sensible.

6.6 Internet como derecho: El caso de Cali

En agosto de 2024 la Alcaldía de Cali dictó la orden de hacer un apagón digital para unas determinadas jornadas durante el llamado estallido social con el argumento de razones de orden público. La rápida respuesta judicial desde la Tutela T-588/24 dejó claro que, el acceso a Internet es un derecho habilitante para el ejercicio de otros derechos fundamentales (las libertades de expresión, de acceso a información, de participación política), por otro lado que cualquier limitación al acceso a Internet debe pasar un estricto escrutinio de proporcionalidad bajo los estándares de la Opinión Consultiva OC-23/17 de la CIDH y por

último que las autoridades locales no pueden aplicar este tipo de limitaciones sin un sustento jurídico claro.

El anterior escenario sirve como referencia para posibles iniciativas que intenten limitar arbitrios para el acceso a Internet en Colombia. El siguiente cuadro comparativo presenta un diagnóstico de los principales obstáculos de los que hay que deslindarse en el país en lo que se refiere a la protección digital, también en forma de un plan de acción dirigido. La sistematización permite ver la relación causa- efecto entre las problemáticas expuestas y las alternativas que se da a cada una de ellas, conformando una carta de navegación para la efectiva protección de los derechos digitales en el país.

Tabla 9.

Obstáculos para la protección digital en Colombia

Retos	**Evidencia**	**Estrategias**	**Acciones**	**Normativo/ Institucional**
Deficiencias en capacidades técnicas del sistema judicial	-Solo 15% de fiscales especializados (2024) -60% de fiscalías carecen de herramientas forenses digitales - Procesos judiciales promedian 2 años de duración	Fortalecimiento institucional	Formación especializada para fiscales Implementación de software con IA para análisis predictivo Establecimiento del Centro Nacional de Ciberseguridad	Fiscalía General de la Nación Ministerio de Justicia
Marco legal no actualizado frente	- Ausencia de tipificación para	Modernización del marco jurídico	-Reforma al Código Penal para incluir delitos digitales	Cámara de Comercio

a nuevas amenazas	delitos con deepfakes - Incremento del 300% en criptoestafas (2024) - Falta de protocolos para protección de infraestructura crítica		emergentes - Actualización de la Ley 1273 sobre cibercrimen - Regulación específica para finanzas descentralizadas (DeFi)	Superintendencia Financiera
Desconocimiento sobre seguridad digital	-78% de usuarios no emplea autenticación digital en dos pasos - 65% ha sido víctima de phishing - Solo 30% conoce la Ley de protección de Datos	Cultura de ciberseguridad	Incorporación de educación digital en currículos escolares - Programas de certificación avalados por MinTIC - Talleres prácticos para poblaciones vulnerables	Ministerio TIC Estudios Kaspersky (2024)
No existe coordinación institucional	Limitada articulación entre entidades - Falta de estándares unificados de ciberseguridad	Gobernanza colaborativa	- Mesas de trabajo con gigantes tecnológicos (Google, Meta) - Alianzas estratégicas con sector financiero - Incentivos fiscales para adopción de estándares ISO 27001	OCDE Ministerio de Defensa

Fuente: Elaboración propia

6.7 Marco normativo de protección de los derechos humanos y sus limitaciones en la práctica

Los resultados reconocen que existe un marco normativo que protege los derechos humanos en el país por medio de la Constitución Política, de la Ley 1581 de 2012, de la Ley 1273 de 2009, e incluso a través de instrumentos internacionales como el Convenio de Budapest, entre otros, pero la realidad demuestra que siguen existiendo obstáculos que limitan cumplir estos derechos a pesar de las garantías normativas.

En este sentido, los resultados evidencian un distanciamiento entre la norma y el hecho, por medio de ejemplos de casos que reflejen vulneraciones a los ciudadanos en entornos digitales y la necesidad de desarrollar este aspecto desde una mirada más centrada en estrategias de protección de los mismos derechos. En este escenario, los ciberderechos están a prueba y minado de obstáculos en Colombia, a pesar de la existencia de avances normativos.

Los resultados muestran un contraste entre el marco normativo en cuanto a delitos electrónicos y derechos digitales, y la realidad de las carencias en su efectiva aplicación. Aunque Colombia cuenta con una regulación robusta que incluye disposiciones constitucionales y leyes específicas como la Ley 1273 de 2009 (delitos informáticos) y la Ley 1581 de 2012 (protección de datos personales), además de la ratificación del Convenio de Budapest (Ley 1928 de 2018), existen vacíos en la regulación de nuevos delitos como criptoestafas y *deepfakes*, y en la adhesión a protocolos internacionales adicionales.

La Opinión Consultiva OC-23/17 de la CIDH establece estándares sobre las limitaciones al acceso a Internet; sin embargo, prácticas contrarias persisten, como señala la Sentencia T-256/25. Incluso a nivel institucional se observa límites, por ejemplo: la Fiscalía

General de la Nación presenta limitaciones institucionales, más del 60% de sus regionales no tienen habilidades forenses digitales y solamente el 15% de los fiscales está capacitado en cibercriminalidad, lo que muestra una gran diferencia entre la normativa y la operatividad.

La Ley 1581 de Colombia es menos rigurosa que las regulaciones internacionales, como el RGPD europeo, ya que no cuenta con controles administrativos ni con derechos avanzados para los titulares de datos, por ejemplo, el derecho a la portabilidad o al olvido. Fortalecer la regulación nacional y aumentar las capacidades institucionales es prioritario para adecuar la protección de derechos digitales al ritmo tecnológico, especialmente frente a la complejidad de plataformas globales que operan bajo jurisdicciones extranjeras.

La Ley 1273 de 2009 establece delitos que protegen la confidencialidad, la disponibilidad y la integridad de los datos y sistemas, entre ellos el acceso indebido, el daño informático, el uso de programas maliciosos o la suplantación de sitios web. No obstante, no considera otros crímenes digitales como el ciberterrorismo, delitos racistas o xenófobos, la pornografía infantil en línea, acoso sexual a menores por internet, criptomonedas, phishing, entre otros. Estos vacíos legales generan zonas de impunidad y desprotección que afectan a los grupos en situación de vulnerabilidad.

6.8. Análisis de Resultado

El estudio normativo de Colombia debe entenderse en diálogo con los avances del derecho internacional en cuanto a derechos humanos digitales, que establecen principios y normas que orientan las acciones estatales para reducir desigualdades y avanzar hacia un entorno digital más justo y seguro.

A continuación, los alcances de los principales resultados:

La clasificación que se considera tradicional de los derechos humanos en tres generaciones (Torres, 2009) se complementa por los estudios adelantados por Ferrajoli (2011) y Díaz (2009), quienes agregan una cuarta generación de derechos, asociados a las nuevas tecnologías, la bioética y la sostenibilidad ambiental. Este estudio se fundamenta en la protección de los derechos digitales y en la implementación de acciones, incluso en términos generales, para la seguridad de la información en el país. Esto se debe a que Colombia es el tercer país a nivel global con mayor cibercriminalidad, según una investigación en el portal Guapacho, (2025), especializado en estos asuntos.

Datos oficiales que sustentan esta realidad son los revelados por la Policía Nacional, quien en el 2024 reportó un total de más de 77 mil denuncias asociadas a delitos informáticos, hecho que si se compara con el 2023 significa un aumento de más del 20% (63 mil denuncias relacionadas fueron reportadas el año anterior) (Policía Nacional, 2025). Por otro lado, el portal de consulta de la Fiscalía General de la Nación *Datos Abiertos*, detalla que entre los delitos relacionados más frecuentes en el 2024 se encuentra el hurto a través de medios digitales e informáticos (más de 37 mil denuncias), lo que representa un aumento de 20% con relación al 2023, entre las modalidades más frecuentes de esta forma de infracciones se encuentra la suplantación de sitios web, el uso de *malware*[6] y violación de datos personales entre otros. Si analizamos años atrás relacionando los datos de ambas fuentes encontramos que, en años anteriores, se registraron más de 28 mil casos (2019), lo que significa un aumento de más del 50% con relación al 2018.

[6] Malware se refiere a cualquier clase de software malintencionado creado para perjudicar o aprovecharse de cualquier aparato, servicio o red programable. Generalmente, los criminales cibernéticos lo emplean para obtener información que pueden emplear como coacción hacia las víctimas para conseguir beneficios económicos. Esta información puede fluctuar entre datos económicos, hasta historiales médicos, correos electrónicos y contraseñas. (adaptado del portal especializado https://inciclopedia.org/)

El país presenta entonces un crecimiento de ciberdelincuencia que enciende las alarmas, con más de 350.000 víctimas en el 2023 (Infobae, 2024) y Bogotá se convierte en el centro de esos delitos, donde se concentra el 60% de los delitos denunciados, entre ellos hackeo, suplantación de identidad e infracciones financieras (Concejo de Bogotá, 2025). De acuerdo con Diario ADN (2025), los ataques han aumentado un 40% en los dos últimos años, mostrando que los sistemas de información son vulnerables a ataques cibernéticos y por otro lado que las medidas de protección deben fortalecerse.

El Congreso ha tenido que crear una Ley nueva, Ley 2502 de 2025: Que establece un agravante al delito de falsedad personal cuando se utilice inteligencia artificial para suplantar identidades, como en los casos de deepfakes.

Algunos de los delitos que más se repiten en este contexto son el *phishing*[7] *y la suplantación de identidad,* entendido como el ingreso no autorizado a cuentas bancarias; el *ransomware,* entendido como el secuestro de datos a cambio de un rescate económico; las e*stafas financieras,* mediante la ingeniería social. Algunos de los casos recientes de mayor sonoridad en el país los encontramos en la tabla 8.

En el país, el sistema legal está en constante cambio para la salvaguarda de los derechos digitales. En esta se pueden destacar las dinámicas señaladas en el análisis de los tres casos estudiados, que, como se ha observado, han ido ganando importancia a medida que se asumía que un supuesto suceso se transformaba en una serie de hitos en la existencia del derecho digital. Estos fallos no solo evidencian la capacidad del sistema judicial para manejar

[7] El *phishing* es un ataque en el que la intención es conseguir el dinero o la identidad del usuario actuando por medio de la persuasión para conseguir que se revele los datos personales (números de tarjeta de crédito, información bancaria o contraseñas) en páginas que pretenden ser legítimas. (adaptado del portal especializado https://inciclopedia.org/)

situaciones en las que se encuentra implicado el campo tecnológico, sino que simultáneamente establecen los criterios que podrían ser pertinentes para la salvaguarda de los colombianos en el campo de los derechos digitales.

6.9. Papel de la Corte Constitucional en la Garantía de los Derechos Digitales

Tres casos emblemáticos entre 2024 y 2025 se observan en las sentencias Sentencia T-256/25; T-149/25; T-453/24, en donde se exponen casos suplantación de identidades y vulneración en redes sociales. La Corte Constitucional, por medio de las sentencias anteriores da un paso al ordenar a Meta (Empresa matriz de Facebook) la instalación de sistemas de verificación biométrica para cuentas de alto impacto social. El fallo es un punto de corte por razones muy amplias: primero, porque termina por reconocer explícitamente el derecho a la identificación digital como desarrollo directo del artículo 15 de la Constitución, que tutela el mismo buen nombre y la autodeterminación informativa; segundo, porque ordena el deber de las plataformas digitales de proteger a sus usuarios, no solo si se dedican a moderar contenidos. Este antecedente ha logrado un debate nacional en torno a la urgencia de regular con mayor exigencia las obligaciones de las *Big Tech* en Colombia, en especial en materia de garantizar la prevención de fraudes y la suplantación.

El segundo caso, lo encontramos en mayo de 2025 en donde quedó al descubierto una de las mayores vulneraciones de la privacidad reciente del país, el cual fue el escándalo en torno a la EPS que hizo pública la historia clínica de medio millón de pacientes. La sentencia SU-256/25 no sólo dejó en entredicho a la entidad de la salud como tal, sino que sentó importantes fundamentos (1) La reafirmación de que los datos médicos asumen la categoría de informaciones sensibles y por lo tanto deberían tener una protección reforzada por la Ley 1581 de 2012; (2) la obligación de protocolo de seguridad bajo estándares internacionales (ISO 27001) y (3) la

incapacidad de que el mero "acatamiento formal" de las regulaciones de protección de datos sea suficiente, ya que se demuestra la necesidad de una administración activa del riesgo.

Por último, un caso ocurrido en Cali en agosto de 2024, en donde la Alcaldía de esta ciudad dictó la orden de hacer un apagón digital para unas determinadas jornadas durante el llamado estallido social con el argumento de razones de orden público. La rápida respuesta judicial desde la Tutela T-372/23 dejó claro que, el uso de Internet es un derecho habilitante en el ejercicio de otros derechos fundamentales (las libertades de expresión, de participación política y de acceso a información), por otro lado que cualquier limitación al acceso a Internet debe pasar un estricto escrutinio de proporcionalidad bajo los estándares de la Opinión Consultiva OC-23/17 de la CIDH y por último que las autoridades locales no pueden aplicar este tipo de limitaciones sin un sustento jurídico claro. Este escenario permite su uso como referencia para posibles futuras iniciativas que intenten limitar arbitrios para el acceso a Internet en Colombia. En ese sentido, en la tabla 5 se relacionan normativas relacionadas con la salvaguarda de derechos humanos en entornos digitales en Colombia.

Un caso notable es el de la Sentencia C-206/25, en la que la Corte Constitucional protegió el derecho al acceso a Internet para comunidades rurales que enfrentaban desconexiones de carácter arbitrario (Mayor ampliación de ello, remitirse a la tabla 6).

6.8 Perspectiva internacional y comparada

Las entidades internacionales están reforzando el marco de los derechos humanos en el entorno digital, adaptando las normas tradicionales a la realidad tecnológica actual. La ONU afirma que los derechos humanos, como la libertad de expresión y el derecho a la información, deben protegerse en línea tanto como en el mundo fuera de línea, basándose para ello en documentos normativos como la Declaración Universal de Derechos Humanos y el Pacto

Internacional de Derechos Civiles y Políticos. La ONU destaca el uso de tecnologías como la encriptación y el anonimato como herramientas para proteger la privacidad.

La posibilidad de acceder a Internet es un derecho habilitante fundamental para el ejercicio de otras libertades esenciales, según el Sistema Interamericano de Derechos Humanos (SIDH) a través de la Comisión Interamericana (CIDH). Las restricciones al acceso deben aplicarse de manera equitativa, legal y no arbitraria, fomentando un entorno de respeto digital.

Actualmente los derechos digitales comprenden no sólo la protección tradicional, sino también el derecho a ser anónimo, la igualdad en el acceso para eliminar las disparidades digitales, la resistencia a la manipulación tecnológica (deepfakes), y la no discriminación algorítmica.

El Consejo de Derechos Humanos de la ONU ha tomado decisiones respecto del derecho a la privacidad digital y ha llamado a los estados a cambiar sus marcos legales para combatir la vigilancia masiva. Los relatores especiales denuncian censuras y limitaciones a los intermediarios de la red para proteger la libertad de expresión en Internet. Colombia está involucrada de manera activa en el Proyecto de Tratado de Ciberdelincuencia de la ONU, cuyo objetivo es crear un instrumento mundial para combatir los delitos digitales, todo ello en un equilibrio entre cooperación penal y la protección de los derechos humanos. En conclusión, la comunidad internacional reafirma que los derechos humanos son totalmente vigentes en la esfera digital y deben adaptarse a sus características. Se hace hincapié en la responsabilidad de los gobiernos y del sector privado de proteger el acceso, la privacidad, la participación y la expresión. Se hace hincapié, además, en la urgencia de cerrar las brechas digitales para evitar la discriminación.

Todos esos instrumentos internacionales ayudan a que Colombia desarrolle un andamiaje normativo consistente en lo digital. Sin embargo, su eficacia depende de que exista un modelo de

implementación que sortee retos como la escasez de especialización técnica en las instituciones, la falta de recurso económico para asegurar la ciberseguridad o la alta necesidad de modernizar las vías de cooperación penal internacional; es decir, que la adopción de estándares internacionales vaya de la mano de políticas públicas integrales capaces de mejorar las capacidades de las instituciones y que logren promover una cultura preocupada por la protección de datos y ciberseguridad entre todos los agentes involucrados: desde el sector público hasta las empresas, pasando por los y las ciudadanas. Solo así podrá permitirse que el andamiaje normativo supere el papel y se constituya en un instrumento revelador para que la salvaguarda de los derechos humanos efectivamente se encuentre en el contexto digital, más allá del físico (mayor ampliación de ello, remitirse a la tabla 6).

7. CONCLUSIONES

Los resultados alcanzados permiten evidenciar que en el contexto colombiano existen significativas vulneraciones a los derechos humanos en materia de seguridad de la información, en especial en los ámbitos de la intimidad y de la libertad de expresión, y que estas vulneraciones están asociadas, por una parte, a vacíos normativos y a una insuficiencia de las medidas técnicas y organizativas, lo que pone de manifiesto la hipótesis que se formuló en la investigación.

Con la pandemia de la COVID-19, el país tuvo que recurrir a las herramientas tecnológicas para afrontar la crisis provocada por esta y para garantizar algunos servicios como el de la educación, la salud, el trabajo, etcétera, por lo cual se evidenció la necesidad de actualizar en su uso, pero al encontrarse sin la preparación suficiente para su implementación, muchas veces las personas han quedado expuestas a un mundo nuevo que debe hacerse regulado por los distintos gobiernos; ese proceso, como se analizó arriba,

evidenció el acelerar la adopción tecnológica sin un desarrollo paralelo en materia de regulación y de capacidades institucionales.

Según el DANE, al cierre de 2022, el 59,5% de los hogares colombianos tienen acceso a internet. De los 32 departamentos, 27 tienen acceso a Internet en cualquier lugar y dispositivo, y entre el 50% y el 89% de su población utiliza este servicio (DANE, 2023). Según MinTIC (2024), para 2023, el número de hogares de Internet fijo en Colombia superó los 9 millones, la mayoría de ellos presentes en las grandes ciudades y capitales. La llamada brecha digital aún es muy grande en Colombia, sin demeritar los esfuerzos del Ministerio, la realidad es que son más los casos donde TIC's aún no llegan a todo el territorio nacional. Como se desarrolló en el análisis, esta brecha no solo limita el acceso, sino que también profundiza las condiciones de vulnerabilidad frente a los riesgos del entorno digital.

Los temas políticos que son temas comunes de conversación en el país y el acceso a esta información por medios de comunicación tradicionales y alternativos han fortalecido el acceso de la población en Internet como una manera de tener presencia, asociación, libre expresión y desarrollo de la libre personalidad. De esta manera, Colombia aparece en el top 5 de las naciones latinoamericanas con más incidentes de seguridad como: fraude electrónico, extorsión, hurto de datos, denegación de servicios, *malware*, virus, entre otros. (González, 2023, p.2). Estos elementos, previamente abordados, permiten comprender la magnitud del problema y su impacto en el ejercicio efectivo de los derechos humanos en entornos digitales.

En este sentido, el Estado debe promover programas de prevención y capacitación para todos los usuarios que tengan acceso a información sensible. Lo anterior sintetiza uno de los principales hallazgos del estudio: la necesidad de fortalecer no solo el marco normativo,

sino también las capacidades sociales e institucionales. Que la sociedad desarrolle una conciencia y un entendimiento de la seguridad de la información en todos los campos, tanto reales como virtuales. Que las empresas y los empresarios apliquen las políticas de Seguridad de la Información vigentes en el país y el mundo para no facilitar la tarea de los ciberdelincuentes. Estas necesidades identificadas a lo largo del análisis evidencian que las vulneraciones no responden a una única causa, sino a una combinación de factores normativos, técnicos y organizacionales, lo que exige la formulación de respuestas diferenciadas pero articuladas entre sí. De igual manera, un desarrollo económico, político y sociocultural del país hará que cada vez se usen los dispositivos de una mejor forma y para mejores fines.

Las bases legales para el análisis digital se detallan en los artículos 15, 20 y 93 de la Constitución Política. Tal como se examinó en el desarrollo del trabajo, si bien existe un marco jurídico relevante, este presenta limitaciones frente a los desafíos emergentes del entorno digital. El derecho a la privacidad y a la protección de los datos personales se aborda en el artículo 15, con el respaldo del Tribunal Constitucional (artículo C-748 de 2011). Sin embargo, este marco jurídico no tiene como objetivo prevenir de manera explícita los desafíos que representan las tecnologías emergentes, tales como la inteligencia artificial o el popular Internet de las cosas; en cambio, establece vacíos de contenido que deben ser analizados en los nuevos contextos que están surgiendo.

En Colombia, el eje central de la regulación del sistema de protección de datos lo componen la Ley 1581 de 2012 y los decretos reglamentarios que la gobiernan (el número 1377 de 2013 y el número 1074 de 2015). Las normativas no tratan los problemas que se presentan con el almacenamiento de datos en la nube a nivel global, un rasgo común de la

economía digital a escala mundial.

La Ley 1273 de 2009 y su decreto reglamentario 2364 de 2012, en el contexto penal, definen las acciones delictivas en el ciberespacio, tales como la violación de datos personales o el acceso a sistemas informáticos. La aplicación de esta normatividad también contiene limitaciones que se deben analizar. Por un lado, los delitos como el ransomware o el tráfico de datos en la *darkweb*, requieren de técnicas de investigación que dificultan la tipificación de las conductas como conductas delictivas; por el otro, parece existir un desfase entre los tipos penales definidos y las nuevas modalidades delictivas que son constantes en el ciberespacio.

La Ley 1978 de 2019 supone la modernización del marco regulador del sector de las TIC's y la creación del Consejo Nacional de Ciberseguridad. Este organismo ha tenido dificultades operativas, incluidas limitaciones presupuestarias, que impiden llevar a cabo de una manera adecuada la coordinación de las políticas públicas respecto de esta materia. Las normas sectoriales tales como la Resolución 733 de 2022 del MINTIC y la Circular 002 de 2023 de la SIC, logran establecer estándares técnicos para su análisis, pero con un desigual cumplimiento, de manera especial entre entidades públicas, en otras palabras, existe la norma, pero esta lamentablemente no es aplicable.

En cuanto al marco normativo internacional en torno a la protección de datos personales y ciberseguridad, ésta ha tenido una incidencia en la configuración de las políticas digitales de Colombia para establecer estándares que intenten ir de la mano con la legislación nacional y los retos del entorno digital en el escenario internacional. Algunos de estos instrumentos internacionales son: el Convenio de Budapest, el Reglamento General de Protección de Datos (RGPD) de la Unión Europea y la Resolución 70/237 de la ONU, cada

uno de estos instrumentos cuentan con una perspectiva complementaria en la configuración del derecho digital colombiano.

En el contexto actual de los ciberderechos, Colombia enfrenta desafíos que requieren de soluciones multidimensionales para garantizar la protección de los derechos humanos en el ciberespacio. Aunque en estos años se han dado grandes avances normativos e incluso de pedagogía social, hoy todavía existen tres grandes problemas que necesitan ser abordados de manera prioritaria: primero, el sistema judicial colombiano tiene serias deficiencias técnicas para adelantar procesos penales en el ciberespacio; solo el 15% de los fiscales están capacitados en cibercriminalidad, de acuerdo con la Fiscalía General de la Nación (2024).

Esta situación se agrava porque la mayoría de las fiscalías territoriales (60%) carecen de instrumentos tecnológicos (MinJusticia, 2024). Esta carencia tecnológica crea procesos judiciales de hasta dos años (Infobae, 2024), violando el derecho a la justicia pronta y eficaz establecido en el artículo 29 de la Constitución. Problemas tales como los deepfakes, las cripto estafas en plataformas DeFi (por ejemplo, un aumento del 300% en 2024, de acuerdo con la Superintendencia Financiera, 2025), los ataques contra infraestructura crítica no tienen su correspondiente tipificación en nuestro ordenamiento jurídico (Cámara de Comercio de Bogotá, 2025).

También se producen vacíos normativos de los cuales sacan partido los ciberdelincuentes. Finalmente, la escasa conciencia que tienen las personas en el país respecto a la seguridad digital constituye una condición de vulnerabilidad sistémica. En este punto, los hallazgos permiten establecer una relación directa entre las debilidades identificadas (vacíos normativos, limitaciones institucionales y falta de cultura digital) y la necesidad de implementar medidas específicas en los ámbitos legal, técnico y organizacional,

las cuales se desarrollan en el siguiente apartado.

Estudios recientes indican que el 78% de los colombianos no utiliza autenticación de dos factores; el 65% ha compartido información sensible por phishing (Kaspersky, 2024); y solo el 30% conoce la Ley 1581 de protección de datos (Universidad de los Andes, 2024). Se deben entonces crear estrategias pedagógicas masivas, por lo cual, frente a estas amenazas, se proponen líneas estratégicas como la modernización de la normativa; es urgente modificar el Código Penal para incluir delitos nuevos como por ejemplo la manipulación mediante *deepfakes* o ataques a cadenas de bloques y por último la escasa conciencia que existe por parte de las personas en el país en materia de seguridad digital constituye una condición de vulnerabilidad sistémica. Tal como se evidenció a lo largo del análisis, las limitaciones en la capacitación del personal judicial, la falta de herramientas tecnológicas y la aparición de nuevas modalidades delictivas dificultan la adecuada respuesta del Estado frente a los ciberdelitos.

Los últimos estudios reportan que, por ejemplo, el 78% de las personas en Colombia no implementan la autenticación en dos pasos, el 65% de ellas comparte información sensible sobre el phishing (Kaspersky, 2024), y solo el 30% se encuentra al tanto de la existencia de la Ley 1581 de la protección de datos (Universidad de los Andes, 2024), lo que indica que se necesita de urgentes estrategias pedagógicas a nivel nacional en materia.

8. RECOMENDACIONES

A partir de los hallazgos encontrados, se sugieren las siguientes líneas de acción tendientes a fortalecer la protección de los derechos humanos en el entorno digital en Colombia. Las recomendaciones que se exponen a continuación están elaboradas en función de los problemas principales que han salido de este análisis. De esta manera, existe una

relación de identidad entre cada vulneración que se ha detectado y la medida que se propone con el objetivo de mitigar dicha vulneración.

A. **Modernización normativa**: Es necesario realizar una modificación del Código Penal colombiano (Ley 599 de 2000) que contemple las nuevas tipologías delictivas que van surgiendo, tal como la manipulación mediante deepfakes, los ciberataques con cadena de producción, el ciberterrorismo, etc. Será necesario modificar la Ley 1273 para permitir incluir nuevamente la respuesta punitiva frente al desarrollo e innovación del malware financiero y para establecer la responsabilidad concreta de las plataformas digitales. Es necesario articular estas modificaciones con la Ley 1273 de 2009, de manera que se pueda modernizar el marco penal respecto de las nuevas dinámicas del ciberespacio. Esta recomendación se hace por los vacíos en las normas que se encontraron en el análisis, especialmente porque no se han definido nuevos delitos y porque hay una falta de ajuste entre la legislación actual y lo que sucede hoy en el ciberespacio.

B. **Incremento en el presupuesto de la Unidad de Ciberdelitos:** Es necesario aumentar el presupuesto de la Unidad de Ciberdelitos para capacitar a nuevos fiscales especializados, comprar nuevas herramientas de IA para llevar a cabo análisis predictivo y constituir un Centro Nacional de Ciberseguridad con el objetivo de coordinar la respuesta a los incidentes y, además, implementar un estándar ISO 27001 del sector público.

   Lo anterior se debe a las limitaciones de las instituciones y de la tecnología, como la poca capacitación de los fiscales y la falta de herramientas

especializadas. Esto afecta directamente la efectividad en la investigación y en el proceso judicial de los ciberdelitos.

C. **Educación digital integral**: Se sugiere implementar una campaña para llevar a cabo estas estrategias a modo de actividad obligatoria del sistema de educación, integrando la ciberseguridad dentro del pénsum de la educación media y, además, proponer programas específicamente dirigidos hacia la educación para poblaciones vulnerables, tales como los adultos mayores, en asociación con las entidades bancarias y a todo el sector salud.

   Esta medida se justifica en el hallazgo de una baja cultura digital en la población, evidenciada en prácticas como el uso limitado de mecanismos de seguridad y el desconocimiento de la normativa vigente en protección de datos.

D. **Cooperación estratégica**: Convocar mesas de trabajo con las empresas tecnológicas globales (Google, Meta, Microsoft) para combatir las cuentas falsas y con el sector financiero para obtener sistemas antifraude en tiempo real. El estímulo a las empresas en términos de incentivos fiscales para la certificación de estándares de seguridad (ISO 27001) podría facilitar la transformación, o, de realizarse esta transformación, incentivar a las empresas para adoptar buenas prácticas en el desarrollo de sistemas de seguridad efectiva.

   Esta recomendación se deriva de la necesidad identificada de articular actores públicos y privados frente a amenazas que superan la capacidad de respuesta individual del Estado, especialmente en un entorno digital globalizado.

E. Como señala la OCDE (2025), los países que lleven a cabo esta propuesta integral de *"quadru hélice"* (Estado, sector privado, academia y sociedad civil)

> serán países con mayor capacidad de resiliencia digital. Colombia tiene una oportunidad histórica para liderar el camino en la protección de derechos digitales como un país de la región, pero para ello debe superar las brechas existentes mediante acciones estructuradas de mediano y largo plazo.

Dicho enfoque global y coordinado se encuentra vinculado con los hallazgos del estudio, dado que reconoce que la protección de los derechos humanos en el entorno digital exige la intervención de múltiples agentes sociales o la coordinación de múltiples niveles de intervención.

Dicha protección efectiva de los derechos humanos en los entornos digitales ya no se puede ver como una opción, sino que se asume como una obligación constitucional y ética que depende de la disposición íntegra de todos los agentes sociales. Solo la combinación de un marco legal digno, de instituciones dignas, de educación permanente y de alianzas estratégicas será capaz de construir un ecosistema digital que sea seguro, inclusivo y respetuoso de la dignidad humana.

BIBLIOGRAFÍA

Aguilar, G. (2010). *Derechos fundamentales-derechos humanos. ¿Una distinción válida en el siglo XXI?* Boletín mexicano de derecho comparado, 43(127), 15–71.

APC — Association for Progressive Communications. (2022). *Internet rights are human rights.* https://www.apc.org/en/pubs/internet-rights-are-human-rights

Bermeo-Yaffar, F., Hernández-Mosqueda, J. S., & Tobón-Tobón, S. (2016). Análisis documental de la V heurística mediante la cartografía conceptual. *Ra Ximhai, 12*(6), 103–121.

Bobbio, N. (1991). *El tiempo de los derechos.* Madrid: Sistema.

Boyes, H. (2013). Cybersecurity and cyber-resilient supply chains. *Technology Innovation Management Review, 5*(4), 28–34.

Burton, J. (2015). NATO's cyber defence: Strategic challenges and institutional adaptation. *Defence Studies, 15*(4), 297–319.

Cano, J. (2019). Ciberriesgo. Aprendizaje de un riesgo sistémico, emergente y disruptivo. *Revista Sistemas, 151,* 63–73.

Concejo de Bogotá. (2025, 22 enero). Bogotá convertida en epicentro del cibercrimen.

Conpes. (2016, 11 abril). Conpes 3854: Política Nacional de Seguridad Digital. Departamento Nacional de Planeación.

Conpes. (2011, 14 julio). Conpes 3701: Lineamientos de Política para la Ciberseguridad y Ciberdefensa. Departamento Nacional de Planeación.

Córdoba, J. F. (2021). *Diseño de un sistema automatizado de gestión de la seguridad de la información basado en la Norma ISO/IEC 27001:2013* (Trabajo de grado). Universidad Peruana Unión.

Corte Interamericana de Derechos Humanos. (2017). Opinión consultiva OC-23/17 sobre derechos digitales y libertad de expresión. OEA.

Cova, E. (2022). Derechos humanos y derechos digitales en la sociedad de la información. *Revista Derechos Humanos y Educación, No. 6,* 62–77.

DANE. (2023). *Boletín técnico: Indicadores básicos de tecnologías de la información y las comunicaciones (TIC) – 2023.* Departamento Administrativo Nacional de Estadística. https://www.dane.gov.co/files/operaciones/TICH/bol-TICH-2023.pdf

Díaz, R. (2009). *Los derechos humanos ante los nuevos avances científicos y tecnológicos.* Tirant lo Blanch.

Díaz, E. (2009). Los nuevos derechos humanos: La cuarta generación. *Revista de Derecho Constitucional Europeo, 12,* 45–67.

Diario ADN. (2024). Aumenta la ciberdelincuencia en Colombia: Hombre fue víctima de hackeo y suplantación.

Donaldson, S., Siegel, S., Williams, C., & Aslam, A. (2015). *Enterprise cybersecurity: How to build a successful cyberdefense program against advanced threats.* Apress.

Donnelly, J. (2013). *Universal human rights in theory and practice.* Ithaca, NY: Cornell University Press.

Dupuy, A., Nussbaum, D., Butrimas, V., & Granitsas, A. (2021). Energy security in the era of hybrid warfare. *NATO Review.*

El País. (2021, 6 mayo). La interrupción de internet durante las protestas agita a los manifestantes en Colombia.

El Tiempo. (2023, 15 diciembre). Delitos informáticos: Policía alerta por aumento de casos en fin de año.

Escuela de Altos Estudios de la Defensa. (2014). *Documentos de seguridad y defensa* (No. 60).

Estrategia de la información y seguridad en el ciberespacio. Ministerio de Defensa de España, Secretaría General Técnica. (fecha no indicada en la bibliografía; verificar al pegar).

Ferrajoli, L. (2011). *Principia iuris. Teoría del derecho y de la democracia* (Vol. 2). Madrid: Trotta.

Fernández, J. J. (2008). Derechos fundamentales, internet y construcción de la seguridad futura En J. J. Fernández, J. Jordán & D. Sansó-Rubert (Eds.), *Seguridad y defensa hoy: construyendo el futuro* (pp. 15–28). Plaza y Valdés Editores.

Fiscalía General de la Nación. (2023). Resolución 117 de 2023.

Gaitán, A. (2018). *Ciberguerra.* Bogotá: Ediciones USTA.

Ganghi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., & Laplante, P. (2011). Dimensions of cyber-attacks: Social, political, economic, and cultural. *IEEE Technology & Society Magazine, 30*(1), 28–38.

Giraldo, A. M., & Bello, J. C. (2021). Análisis de la ciberseguridad en Colombia: Retos y desafíos en la protección de los datos personales. *Revista Científica de Administración, Finanzas e Informática, 6*(1), 65–78.

Glendon, M. A. (2004). *El crisol olvidado: la influencia latinoamericana en la idea de los derechos humanos universales.* Persona y Derecho.

González, J. E., & Parrado, V. A. (2017). *Guía de gestión de incidentes de seguridad de la información para la OTIC del Ministerio de Salud y Protección Social* (Trabajo de grado). Universidad Piloto de Colombia.

González Hernández, M. (2023). *Actualidad de Colombia en seguridad de la información.* Bogotá: Universidad Piloto de Colombia.

Gorman, S. P. (2005). *Networks, security and complexity: The role of public policy in critical infrastructure protection.* Edward Elgar.

Guapacho. (2025). Colombia ocupa el tercer lugar en cifras de cibercriminalidad a nivel mundial.

Hernández, F., Fernández, C., & Baptista. (2017). *Metodología de la investigación.* McGraw-Hill Interamericana.

Hernández, E. F. T., Canizales, R. R., & Páez, A. V. (2021). La importancia de la ciberseguridad y los derechos humanos en el entorno virtual. *Misión Jurídica: Revista de Derecho y Ciencias Sociales, 14*(20), 142–158.

Infobae. (2024, 11 julio). Las estafas se disparan y complican la eficacia policial: más de 350.000 personas fueron víctimas de ciberdelitos en 2023.

La República. (2023, 28 noviembre). Así ha aumentado la cifra por ciberdelitos financieros.

León, J. (2020). Evolución y desarrollo de los derechos humanos. Hacia una cuarta generación. *Revista El Derecho Público y Privado Ante las Nuevas Tecnologías,* 221–235. Madrid: Dykinson.

López Barrios, M. E. (2015). *Ley 1581 protección de datos personales* (Trabajo de grado). Universidad Piloto de Colombia.

Maqueo Ramírez, M. S., Moreno González, J., & Recio Gayo, M. (2017). Protección de datos personales, privacidad y vida privada: La inquietante búsqueda de un equilibrio global necesario. *Revista de Derecho (Valdivia), 30*(1), 77–96.

Martínez, C. (2018). Investigación descriptiva: definición, tipos y características.

McKinsey & Company. (2021). *The top trends in tech* (Executive summary).

Melo, A. H. V., & Velasco, H. (2008). *The computer law and management of information security: A perspective based on the ISO27001 standard.* Revista de Derecho, (29).

Ministerio de Telecomunicaciones — MinTIC. (2024). *Sociedad de la información.*

Ministerio de Tecnologías de la Información y las Comunicaciones — MinTIC. (2021, 10 marzo). Resolución No. 00500 de 2021

Morales, P. (2018). Entre el prisma discursivo y el ciberhumanismo: algunas reflexiones sobre derechos humanos de cuarta generación. *Franciscanum, 60*(169), 39–86.

NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity.* NIST.

Observatorio de Educación Superior de Medellín. (2019). *Medellín hacia la cuarta revolución industrial* (Boletín 11).

Oficina Nacional de Seguridad del Ciberespacio (ONSC). (2019). *Guía de introducción a la seguridad: Las dimensiones de la seguridad.*

OHCHR — Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. (2024). *Derechos humanos.*

Ortega, L. F. (2012). La ciberseguridad y la ciberdefensa. En *El ciberespacio: nuevo escenario de confrontación* (pp. 37–69). Ministerio de Defensa de España, Secretaría General Técnica.

Ospina, J. C. (2018). *Diseño de un sistema de seguridad de la información basado en la OTAN.*

París, S. (2013). Naturaleza humana y conflicto: un estudio desde la filosofía para la paz. *Eikasia: Revista de Filosofía, 50*(2), 109–116.

Parlamento Europeo & Consejo de la Unión Europea. (2016). Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD).

Penna, A. F., Gómez-Cárdenas, R., & de Dios González-Ibarra, J. (2023). La ciberseguridad en México y los derechos humanos en la era digital. *Espacios Públicos, 24*(61), 119–142

Pérez, A. E. (2014). Teledemocracia, ciberciudadanía y derechos humanos. *Revista Brasileira de Políticas Públicas, 4*(2).

Policía Nacional de Colombia. (2025, marzo). *Boletín estadístico semanal: Ciberdelitos en Colombia (Semana 11)*.

Rojas, Y. (2022). Regulación del ciberdelito en el marco legal de la seguridad de la información como medida de protección preventiva de seguridad cooperativa nacional e internacional. Tesis de maestría. Universidad Libre.

Rousseau, J. J. (1996). *El contrato social* (Libro II, cap. I). Madrid: Alba.

Schwab, K. (2015, 12 diciembre). The fourth industrial revolution: What it means and how to respond. *Foreign Affairs.*

Seclén Arana, J. A. (2016). Factores que afectan la implementación del sistema de gestión de seguridad de la información en las entidades públicas peruanas de acuerdo a la NTP-ISO/IEC 27001. Universidad Mayor San Marcos.

Shue, H. (2002). *Mediando deberes.* Bogotá: Universidad Externado.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know.* Oxford University Press.

Soler, E. (2019). *El mundo en 2020: diez temas que marcarán la agenda global* (CIDOB Notes 220).

Superintendencia de Industria y Comercio. (2024). Circular Externa No. 003 de 2024.

Téllez, E. (2018). Tecnologías, seguridad informática y derechos humanos. *Ius et Scientia, 4*(1), 19–39.

The Economist. (2010). *Cyberwar: War in the fifth domain.* Briefing.

Tobón, S. (2012). *Cartografía conceptual: estrategia para la formación y evaluación de conceptos y teorías.* México: CIFE.

Torres, I. (2009). La protección internacional de los derechos humanos. *Lecciones de Derecho Internacional Público,* 509–515.

Vasak, K. (1977). La larga lucha por los derechos humanos. En *UNESCO, The UNESCO Courier: a window open on the world* (pp. 29–30).

World Economic Forum. (2021). *Cyber resilience in the fourth industrial revolution.*

W Radio. (2024, 8 agosto). Aprobado primer tratado de la ONU contra la cibercriminalidad.

Leyes y Decretos

Congreso de la República de Colombia (2012). Ley Estatutaria 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.

Congreso de la República de Colombia (2013). Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012

Congreso de la República de Colombia. (1991). *Constitución Política de Colombia*. Artículo 15. https://www.constitucioncolombia.com/titulo-2/capitulo-1/articulo-15

Congreso de la República de Colombia. (1991). *Constitución Política de Colombia*. Artículo 20. https://www.constitucioncolombia.com/titulo-2/capitulo-1/articulo-20

Congreso de la República de Colombia. (1991). *Constitución Política de Colombia*. Artículo 93. https://www.constitucioncolombia.com/titulo-2/capitulo-4/articulo-93

Congreso de Colombia. (17 de octubre de 2012). *Ley 1581 de 2012*. Diario Oficial No. 48.587. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Congreso de Colombia. (5 de enero de 2009). *Ley 1273 de 2009*. Diario Oficial No. 47.223. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=33148

Congreso de Colombia. (26 de julio de 2019). *Ley 1978 de 2019*. Diario Oficial No. 51.037. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=110597

Congreso de Colombia. (30 de julio de 2009). *Ley 1341 de 2009*. Diario Oficial No. 47.426. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=36850

Conpes 3854. (2016, 11 de abril). *Política Nacional de Seguridad Digital*. Departamento Nacional de Planeación.

Conpes 3701. (2011, 14 de julio). *Lineamientos de Política para la Ciberseguridad y Ciberdefensa*. Departamento Nacional de Planeación

Corte Constitucional de Colombia. (18 de mayo de 1995). *Sentencia C-225 de 1995*. https://www.corteconstitucional.gov.co/relatoria/1995/C-225-95.htm

Fiscalía General de la Nación. (2023). *Resolución 117 de 2023*. https://www.fiscalia.gov.co/

Ministerio de Tecnologías de la Información y las Comunicaciones. (10 de marzo de 2021). *Resolución No. 00500 de 2021*. https://mintic.gov.co/portal/715/articles192603_recurso_1.pdf

Presidencia de la República de Colombia. (26 de mayo de 2015). *Decreto 1074 de 2015*. Diario Oficial No. 49.523.

Presidencia de la República de Colombia. (27 de junio de 2013). *Decreto 1377 de 2013*. Diario Oficial No. 48.830.

Presidencia de la República de Colombia. (27 de diciembre de 2014). *Decreto 2573 de 2014*. Diario Oficial No. 49.405.

Superintendencia de Industria y Comercio. (2024). *Circular Externa No. 003 de 2024*.