EDITORIAL ESDEG

Revista
Ciberespacio, Tecnología e Innovación
Volumen 1, número 1, enero-junio 2022
Bogotá, D.C, Colombia
ISSN: 2955-0270
Página web: https://esdegrevistas.edu.co/index.php/rcit

Importancia de una Ley de Ciberseguridad y Ciberdefensa para Colombia

Importance of a Cybersecurity and Cyberdefense Law for Colombia

Julián Antonio Guzmán Pacheco

CITACIÓN APA:

Guzmán Pacheco, J. A. (2022). Importancia de una Ley de Ciberseguridad y Ciberdefensa para Colombia. *Ciberespacio, Tecnología e Innovación, 1*(1), 67-90. https://doi.org/10.25062/2955-0270.4766

Publicado en línea: **Junio 30 de 2022**

Enviar un artículo a la Revista

Revista Ciberespacio, Tecnología e Innovación
Volumen 1, número 1, enero-junio 2022 (pp. 67-90)
Bogotá, D.C, Colombia

EDITORIAL ESDEG

Importancia de una Ley de Ciberseguridad y Ciberdefensa para Colombia

Importance of a Cybersecurity and Cyberdefense Law for Colombia

DOI: https://doi.org/10.25062/2955-0270.4766

Julián Antonio Guzmán Pacheco
Escuela Superior de Guerra "General Rafael Reyes Prieto", Bogotá D. C., Colombia

Resumen

El artículo busca reflejar la importancia de la aprobación de una Ley de Ciberseguridad y Ciberdefensa para Colombia a través de un análisis reflexivo, teniendo en cuenta sus características y perspectivas tanto nacionales como internacionales. Este se realizó a partir de una metodología cualitativa, donde a través de la revisión de la literatura existente se logró comprender el fenómeno de investigación. De esta manera, se lograron descubrir los elementos constitutivos que requieren una ley de ciberseguridad y ciberdefensa desde su relevancia y aporte para la inteligencia nacional. Por último, se lograron identificar las dificultades legales con las cuales opera actualmente la Ciberseguridad y Ciberdefensa en Colombia, desde su inadecuada interpretación y ajuste de las leyes existentes, precisamente como factor clave y estratégico del desarrollo que coincide con la aparición del fenómeno web, cuya expansión ha generado la quinta dimensión de las guerras modernas, afectando la cotidianidad de los diferentes actores.

Palabras Clave: Ciberdefensa; Ciberseguridad; Derecho; Leyes; Política Pública

Abstract

The article seeks to reflect the importance of the approval of a Cybersecurity and Cyberdefense Law for Colombia through a reflective analysis, taking into account its characteristics and both national and international perspectives. This was carried out based on a qualitative methodology, where through the review of existing literature it was possible to understand the research phenomenon. In this way, it was possible to discover the constituent elements that require a cybersecurity and cyber defense law from its relevance and contribution to national intelligence. Finally, it was possible to identify the legal difficulties with which Cybersecurity and Cyberdefense currently operates in Colombia, from its inadequate interpretation and adjustment of existing laws, precisely as a key and strategic factor of development that coincides with the appearance of the web phenomenon, whose expansion has generated the fifth dimension of modern wars, affecting the daily lives of different actors.

Key words: Cyber defense; Cybersecurity; Rights; Laws; Public politics

Artículo de reflexión
Recibido: 2 de febrero de 2022 • **Aceptado:** 14 de mayo de 2022
Contacto: Julián Antonio Guzmán Pacheco guzmanja@esdeg.edu.co

Introducción

Aunque resulta difícil realizar un análisis preciso sobre la Ciberseguridad y la Ciberdefensa, lo que es claro, es que las amenazas, según Fernández (2019) no deben subestimarse. En este sentido, a pesar de que la ciberseguridad y ciberdefensa no se visibilizan fácilmente, guardan una estrecha relación, tanto a través del resguardo de la información almacenada o interconectada para la prevención de las amenazas, como de la planificación y las capacidades del Estado para defender los activos estratégicos e intereses nacionales. Precisamente, el avance tecnológico es lo que ha provocado el interés de salvaguardar la información, exigiendo procesos robustos para contrarrestar y controlar las amenazas cibernéticas, tal como lo hace la ciberdefensa, previniendo los ataques de grupos con interés contrarios al estado, y la ciberseguridad, brindando respuestas para resguardar la información que podría colocar en riesgo la infraestructura crítica del estado.

la ciberseguridad termina siendo el complemento a la ciberdefensa y se materializa, según Hannant (2021) en la defensa digital o de la información del Estado que se puede evidenciar mediante las acciones encaminadas para mitigar el Cibercrimen independientemente el grado de incertidumbre tanto interna como externa, cabe mencionar que la complejidad de dichos elementos dificulta encontrar una solución a las problemáticas relacionadas con estos (Hannant, 2021). Así, estos dos elementos se han convertido en un factor fundamental para el fortalecimiento de acciones que previenen ataques contra la institucionalidad o la seguridad de los gobiernos, como los eventos del 11 de septiembre de 2001 en el World Trade Center de Nueva York, o en el caso de Colombia, a partir de las interceptaciones ilegales del Departamento Administrativo de Seguridad (DAS); provocando la eliminación del mencionado organismo.

Las anteriores situaciones evidencian las dificultades para mitigar el riesgo interno, externo y falencias en el tema de la ciberseguridad y ciberdefensa, puesto que se refleja la incapacidad de los países para evaluar la función y desempeño de estas áreas, sin contar las carencias normativas y aplicables en estos escenarios que muestran la insuficiencia del Estado en cuanto a la prevención y mitigación con las herramientas de seguridad y defensa nacional (Lind,2017). Estas circunstancias, aunque preocupan, no sorprenden, debido a que la ciberseguridad carece de mecanismos tecnológicos y personal entrenado para prevenir y la ciberdefensa presenta un enfoque pasivo sin alternativas de defensa que contrarresten el cibercrimen. Todo esto, apunta a la debilidad del Estado colombiano, que no solo demuestra debilidades evidenciadas en la parte técnica o tecnológica, sino también desde la insuficiencia legal para llevar a cabo la prevención, rastreo y procesamiento de los mecanismos necesarios que ayuden a lograr un adecuado andamiaje entre ciberseguridad y la ciberdefensa, como variables que favorezcan al Estado a través del respeto por la ley desde un nuevo escenario que soporta la justicia y su accionar nacional (Guaqueta, 2015).

Este escenario surge por el creciente uso del ciberespacio en el mundo, en donde la globalización ha propiciado la revolución tecnológica del siglo XXI. Un ejemplo de esto se evidencia en el aumento de personas que actualmente usan sistemas conectados al ciberespacio, originando por ejemplo el internet de las cosas. Igualmente, la cantidad de datos que se originan virtualmente ha generado el *big data*, donde a través de un inmenso volumen de información se logra el análisis de patrones y tendencias de comportamiento como un activo de suma importancia para cualquier persona, organización o Estado (La Gaceta Caese, 2016).

Precisamente todo esto ha llevado a convertir la Ciberdefensa y Ciberseguridad en un aspecto fundamental a nivel estratégico, sobre todo por el enorme manejo de la información por la población en general a través de redes, medios, portales webs y su expansión concebida como la nueva dimensión de las guerras modernas. Este hecho convierte este fenómeno en un factor clave de análisis para la conducción político y estratégica en pro de los intereses de las naciones. En Colombia, estos factores ampliamente discutidos se vienen focalizando en análisis pragmáticos, que llevan a la seguridad y la defensa en el ciberespacio a ser pensada desde un modelo local de gobernanza en ciberdefensa a partir de la normativa actual, donde los hallazgos actuales requieren esfuerzos inter agénciales para su institucionalización (Rojas, 2021). En este contexto, se demuestra como el Estado colombiano carece de regulación satisfactoria en aspectos del ciberespacio, que a pesar de la utilización de los medios, no logra preservar completamente los intereses del Estado y menos salvaguardar (Becerra, et al., 2019).

Para complementar, señala Sánchez (2017) no existe actualmente una legislación clara para afrontar este contexto, ni en términos ofensivos ni mucho menos defensivos, que llevan a dificultades legales y en consecuencia a generar riesgos en la práctica cibernética, sobre todo, por la nula aplicabilidad de acuerdos internacionales. Por tal motivo, no basta con generar espacios o acceso al ciberespacio, sino también, propiciar la estructuración y puesta en marcha de políticas serias y una legislación aplicable para garantizar la seguridad del Estado colombiano, apuntándole a estándares internacionales para garantizar el cumplimiento de la ley (Ministerio del Interior y Seguridad Pública, 2018).

Lo anterior, lleva a plantear, como tesis, que tanto la ciberseguridad como la ciberdefensa carecen de una legislación ajustada a las necesidades del Estado colombiano, presentando un alto riesgo que no le permite contrarrestar con efectividad las amenazas cibernéticas, sobre todo en la protección del Estado y sus activos estratégicos (Consejo Nacional de Política Económica y Social República de Colombia, 2016). Esto evidencia la necesidad de medidas claras para ampliar la seguridad y mejorar la confianza en los medios digitales, como un espacio incluyente con capacidades digitales en los sectores públicos y privados, incrementando así, su desarrollo y crecimiento en materia tecnológica,

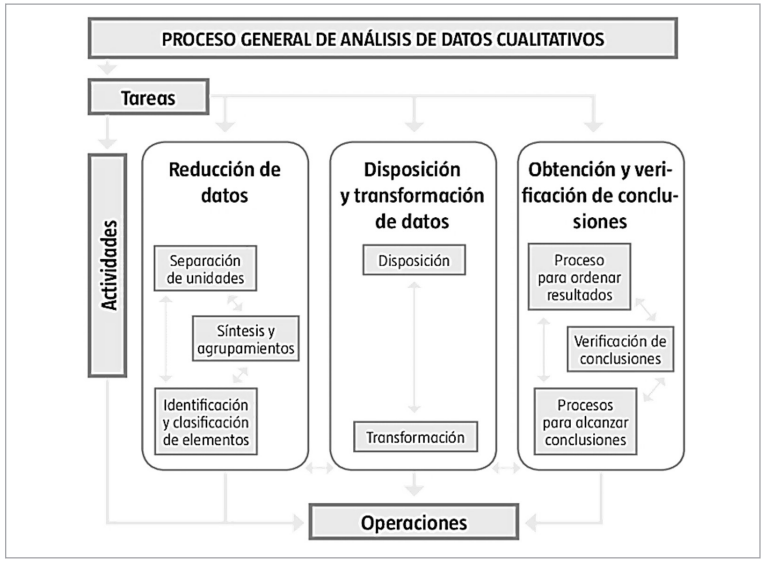
pero desde estándares destacados de seguridad digital (Consejo Nacional de Política Económica y Social República de Colombia, 2020).

Metodología

Se emplea un enfoque cualitativo a partir del análisis de fuentes abiertas y una codificación primer grado, para identificar diferentes categorías y características que no necesariamente llevan a una codificación axial. De esta manera, se agruparán dichas categorías en características asociadas al análisis de la literatura existente, para establecer las condiciones causales que requiere una ley de ciberseguridad y ciberdefensa en Colombia (Lozano, 2003).

El procedimiento se construyó desde una lógica inductiva para pasar de lo particular a lo general y con ello lograr el análisis de la información recopilada sobre la importancia de una ley de ciberseguridad y ciberdefensa para Colombia, sin que esto genere necesariamente un análisis estadístico, pero sí una clasificación e interpretación del fenómeno estudiado.

Figura 1. Proceso de análisis de datos cualitativos



Fuente: Elaboración propia

Etapa I

Inicialmente, mediante la recolección de las fuentes de información se profundizó en la problemática planteada para sintetizar la información (fuentes primarias y secundarias) que para Tamayo (2013) y Hernández et al (2014) llevan a la identificación y clasificación de los elementos relevantes de la muestra documental objeto de análisis.

Etapa II

En esta etapa se fundamentó en la trasformación de la información y la reducción de la misma mediante la separación de unidades de análisis para clasificar los elementos que respalden la importancia de una ley de ciberseguridad y ciberdefensa para Colombia y con ello brindar claridad mediante un muestreo documental (Ariza, 2007).

Etapa III

Por último, se logró la obtención de conclusiones a través de unidades y categorías de estudio por medio del análisis cualitativo proporcionado por el (ATLAS ti 9.0) que apoyan la interpretación y organización de la información de manera lógica, estructural y soportada la significancia otorgada en cada objetivo planteado.

Marco teórico y conceptual

El término de seguridad nace del latín securitas que según la RAE (2018) se define de acuerdo con el contexto, pero generalmente se asocia a la confianza y al mantenerse alejado de los riesgos y/o amenazas latentes. En este sentido, el concepto se trasforma hasta convertirse en un objetivo colectivo con el fin de garantizar la libertad individual (Vargas, 2017). En este orden se destaca también la defensa que se relaciona con las acciones militares que colaboran para mitigar dichos riesgos, amenazas o daños; por lo que sentirse seguro relaciona no solo a la respuesta, sino a la capacidad con que se cuenta.

De este modo, el Estado debe brindar una respuesta efectiva para prevenir, pero también garantizar adecuadas condiciones de vida, seguridad y confianza para satisfacer las necesidades de la sociedad. Esta relación entre la defensa y la seguridad, tal como lo afirma, se presenta intensamente por la influencia, intereses y relaciones de poder, no solo a nivel estratégico, sino del mismo modo en términos geopolíticos y tecnológicos, por el manejo de la información, las comunicaciones y los avances propiciados por la sociedad; entre los cuales se incluye el internet, las telecomunicaciones, los software, los computadores, las redes sociales y la interacción de las poblaciones y los escenarios online, también conocidos como ciberespacio que han llevado a modificar la concepción defensa y la seguridad (Nye & Villanueva, 2013).

Actualmente, el ciberespacio se estima que cuenta con alrededor de 5 mil millones de personas diarias conectadas al internet y se proyecta en los próximos 5 años a 50 mil millones y el acceso a 10 equipos por persona. En este contexto, más de 2 mil personas por minuto se encuentran comunicadas e intercambiando ideas y pensamientos a nivel mundial, generando hasta 41 millones de mensajes en un espacio de 60 segundos. De allí que los Estados basen su información en el uso de computadores, programas y aplicaciones para adaptarse a las condiciones actuales y optimizar sus recursos (Klimburg, 2020).

En este entorno, se puede afirmar que, si las economías mundiales y el bienestar están claramente relacionadas con el mundo online o el uso de la información en el ciberespacio, la seguridad y defensa deben encontrarse de igual manera cada vez más ligada a este mecanismo. Es decir, que las gestiones para defenderse de los riesgos, amenazas y peligros deben orientarse también a brindar la confianza necesaria en el contexto virtual desde la percepción real; y es que desde el ciberespacio no solo se debe buscar la seguridad individual, sino como un asunto de seguridad y soberanía nacional estrechamente ligada a la capacidad para gobernar (Choucri 2014).

Para Der Derian (2009) estos asuntos tecnológicos del ciberespacio han cobrado gran relevancia en las diferentes naciones; sobre todo por los factores asociados a las circunstancias como el resguardo de la información, el seguimiento, la seguridad, la simulación, la vigilancia y velocidad, que llevan a analizar quien tiene acceso a la información y los medios para llegar a ella. Esto lleva a advertir, cómo el uso de la información lleva a una ventana que puede vulnerar la seguridad nacional y generar pérdidas económicas, humanas, sociales y políticas, como las ocurridas en el atentado llevado a cabo en la brigada 30 en Cúcuta o la fuga de información de inteligencia colombiana hacia Venezuela, solo por mencionar algunos casos (Cepik & Brancher 2017).

Todo esto demuestra que los daños al Estado pueden verse generados a través del ciberespacio, que según Feenberg (2019) cuentan con la capacidad para asociar individuos a pesar de la distancia y fraguar planes en contra del Estado como espacio de conflicto. Esta razón precisamente ha llevado a considerar este fenómeno como una prioridad que debe ser abordada a nivel estratégico tanto a nivel nacional como internacional, con el fin de ser preventivos y menos reactivos en temas de defensa y seguridad.

En estas circunstancias emergieron ciertos términos como ciberataque, el cual se refiere a los intentos por atacar, destruir, alterar, saquear o acceder a información no autorizada de un Estado con el fin de causar una afectación gubernamental o poblacional. Esto lleva a generar el término de Ciberseguridad con dos sentidos; el primero, desde un factor estratégico en la que se identifican las condiciones del ciberespacio que se encuentren alejadas de amenazas o riesgos y el segundo, desde un concepto más operativo que busca preservar la reserva, integridad y disponibilidad de la información en el ciberespacio entre otros aspectos (Cepik, 2017).

Finalizando se encuentra el término de ciberdefensa, que resguarda su significancia a través de las acciones del Estado para protegerse y mitigar las amenazas y riesgos cibernéticos, con el objetivo de usar el ciberespacio con normalidad, pero del mismo modo, protegiendo los derechos, las libertades y brindando las garantías a todos los ciudadanos, en virtud de la soberanía y el mantenimiento territorial; pero sin eludir los nuevos escenarios que plantea la hibridez de los conflictos que de alguna manera inciden en el uso del ciberespacio (Virilio 1995). Así, no queda duda que los Estados deben fortalecer su Ciberdefensa desde su capacidad de respuesta a través de la constante evaluación del

enemigo. De esta forma, la ciberseguridad y ciberdefensa han cobrado gran relevancia y evolucionado hasta llegar a ser consideradas como una capacidad estratégica para el direccionamiento de un Estado (Samper 2015).

Dicho esto, una ley de ciberseguridad y ciberdefensa para Colombia cobra valor desde la necesidad por fortalecer al Estado, sino al mismo junto con la ley 1621, brindar herramientas para abordar el dilema jurídico que actualmente se presenta (Congreso de la República, 2013). De esta manera, lo que se busca es proteger al Estado, tal como lo mencionara Cicerón (2014) mediante las leyes se protege a la población y mientras existan, se deben respetar y hacerlas cumplir estratégicamente para aportarle soluciones a factores críticos a nivel nacional.

Regulación de Ciberseguridad y Ciberdefensa en Colombia

En Colombia la regulación en temas de ciberseguridad y ciberdefensa, aunque no presenta grandes antecedentes, si es importante realizar un análisis para reconocerla y al mismo tiempo evidenciar a los factores que apunta, explorar su enfoque y la relación con el entorno actual. En ese orden, inicialmente es relevante relacionar que a nivel nacional existe el Consejo Superior Digital de Protección y Defensa del Ciberespacio; conformado por los Ministros de Justicia, Relaciones Exteriores, Defensa, Tecnologías de la Información y las Comunicaciones (TIC) y el Director Nacional Inteligencia, el de Planeación Nacional, el Comandante de las Fuerzas Militares, el Director General de la Policía Nacional, el Fiscal General de la Nación y el consejero Presidencial de Seguridad que en medio de una crisis, podrá convocar al Presidente de la República o demás organismos para la atención de la misma (PNPICCN, 2017). Desde este consejo, se ponen en marcha las directrices generales para realizar el seguimiento, el análisis y la evaluación de diferentes amenazas que puedan afectar al Estado colombiano. Así, la coordinación y las acciones de los agentes del sistema buscan mitigar una situación crítica a nivel cibernético; buscando con estas acciones propiciar los mecanismos para prevenir afectaciones en contra de la infraestructura desde la planificación y operación del organismo, que para el caso de Colombia también se soportan en una serie de normas que se relacionan a continuación.

Normatividad Nacional

En cuanto a la normatividad nacional, según la Constitución Política de Colombia (1991) en primer lugar, es importante mencionar la existencia varios aspectos constitucionales orientados a la seguridad digital. Uno de ellos es el artículo dos que busca garantizar la efectividad de los principios, derechos y deberes consagrados en la constitución. De la misma manera, en el capítulo II, particularmente en el artículo 15, se reconoce el derecho

a la intimidad y la obligación del Estado a respetarla y hacerla respetar; y en el artículo 20, donde se le debe garantizar a toda persona la libertad de expresión para difundir sus opiniones y pensamientos, al tiempo de poder informar, recibir información veraz e imparcial y también de poder fundar medios masivos de comunicación. De igual modo, la Constitución Política de Colombia establece en su artículo 76 que el espectro electromagnético es un bien público sujeto a la gestión del Estado, donde en el mismo artículo 101 incluye este factor como parte del territorio nacional y junto a ello, señala la responsabilidad y capacidad de las Fuerzas Militares para resguardar y proteger el territorio y soberanía de Colombia (Constitución Política, 1991)

Asimismo, Colombia cuenta con el Código Penal del 2000 y la Ley 1273 del 2009 como parte normativa y procesal para hacer frente a los delitos cibernéticos; reconociendo, a su vez, los tratados internacionales de la INTERPOL Y EUROPOL. De igual modo, la Ley 1581 del 2012 como soporte o marco básico para regular la protección de datos, su divulgación y violaciones de la seguridad. Frente a estos aspectos normativos de carácter ordinario, también se evidencian diferentes herramientas legales para regular la seguridad digital en circunstancias relacionadas con los derechos de autor, la pornografía, el comercio electrónico y la explotación sexual de menores en el ciberespacio, entre otros(Giral-Ramírez et al., 2017)

También se evidencia un avance normativo a nivel nacional que aborda aspectos relacionados con la firma electrónica, el habeas data, herramientas de autenticación y el registro nacional de bases de datos (Sarmiento, 2016). Finalmente, también se pueden divisar en el panorama nacional, otros decretos y actos administrativos que reglamentan diferentes actividades que regulan el ciberespacio, como la circular 052 de 2007 que instaura las pautas de seguridad y calidad para el manejo de la información de medios y canales de distribución de productos y servicios, la Resolución la CRC 3066 y 3067 de 2011 que establece los parámetros integrales de protección de los derechos de los usuarios para el servicio de telecomunicaciones, el Decreto 1704 de 2012 que regula y condiciona las interceptaciones de comunicaciones, la resolución de la Superintendencia de Industria y Comercio Nº. 76434 de 2012, que establece la protección de datos personales y, por último, del Decreto 2573 de 2014, que regula el Gobierno en línea para la utilización y soporte de la ciudadanía; todo esto, sin dejar de lado el Consejo Nacional de Planeación (CONPES) como entidad con capacidades para la generación de políticas y el desarrollo del país (CONPES, 3701).

Consejo Nacional de Planeación (CONPES)

Aunque el CONPES no es reconocida por sí misma como una normatividad, si es la entidad encargada para liderar y presentarle al Gobierno Nacional, los elementos, políticas, planes y programas estratégicos, proyectados al desarrollo económico y social del país.

Esta busca como objetivo fundamental, a través de los documentos CONPES, el fortalecimiento de las capacidades del Estado para el enfrentamiento de las amenazas que puedan atentar contra su seguridad y defensa. De allí que surja como iniciativa fundamental la política para la Ciberseguridad y la Ciberdefensa (CONPES 3701).

CONPES 3701

Inicialmente en Colombia se generó el documento CONPES 3701, que identificó la debilidad del Estado para contrarrestar las amenazas cibernéticas, ya que el sector público no tenía una iniciativa para dicha problemática, por consiguiente, no existía una estrategia nacional, un sistema y un marco legal enfocado a la seguridad cibernética. Asimismo, el documento señalo otros factores que indicaban que Colombia era una nación vulnerable en el tema de la ciberseguridad, tales como el constante incremento de los usuarios de internet, el alto grado de dependencia de las infraestructuras críticas y la alta frecuencia de delitos informáticos

Ante la situación anterior, el documento CONPES 3701 presentó los lineamientos de la política de ciberseguridad y ciberdefensa para contrarrestar las amenazas del ciberespacio. En esta política se destacan la seguridad y defensa digital del Estado como parte primordial, buscando fortalecer las capacidades para hacerle frente a las amenazas que pueden llegar a atentar contra la defensa y seguridad nacional en el contexto cibernético (Consejo Nacional de Política Económica y Social República de Colombia, 3701).

En esta protección se destacan tres objetivos específicos primordiales; el primero de ellos, lograr implementar las capacidades para la prevención, coordinación, atención y control de las emergencias cibernéticas para enfrentar las posibles amenazas y los riesgos que puedan afectar la ciberseguridad y ciberdefensa nacional; el segundo, ampliar las líneas de investigación y capacitación en la seguridad de la información en estos aspectos; y el tercero, fortalecer permanentemente la normatividad y la cooperación internacional con el fin de estar a la vanguardia delos estándares y regulaciones exigidas (López, 2019).

CONPES 3995

El CONPES 3995 formula la política de confianza y seguridad digital que busca instaurar las medidas, generar la confianza y mejorar la seguridad a través del fortalecimiento de las capacidades de la seguridad digital para la población colombiana, el sector público y privado, actualizando constantemente el control y la gobernanza para el desarrollo nacional y con ello, adoptar modelos en materia de seguridad digital enfatizando en nuevas y mejores tecnologías (Ministerio de Tecnologías de la Información y las Comunicaciones, 2020). De igual modo, este CONPES pretende mediante la regulación,

afrontar efectivamente las nuevas amenazas a través de la formulación y actualización de estrategias relacionadas con la seguridad en el ciberespacio (Consejo Nacional de Política Económica y Social República de Colombia, 3995).

Colombia además es miembro de la INTERPOL y de la EUROPOL tal como se mencionó anteriormente, priorizando su cooperación internacional a través de la ley Nº 1928/2018 y la aprobación del convenio de Ciberdelincuencia el 16/03/2020 (Budapest, 2001) adhiriéndose como un instrumento de apoyo a la Ciberseguridad mundial, apoyado también a través de la política digital Nº 1.008/2018 para el uso y aprovechamiento de las TICs buscando consolidar el Estado mediante un entorno de confianza y cumplimiento de la regulación actual.

Dificultades Normativas de Ciberseguridad y Ciberdefensa en Colombia

Según Ceballos (2020) la ciberdefensa y ciberseguridad son elementos críticos para la prosperidad y seguridad de una nación, teniendo en cuenta que las actividades maliciosas ejecutadas por individuos o grupos al margen de la ley ponen en riesgo tanto al Estado como a sus democracias y habitantes. De allí, que la seguridad dependa en gran medida de las capacidades civiles y militares que se tengan para proteger la infraestructura de las amenazas cibernéticas; que mediante herramientas y sistemas seguros podrán prevenir y mitigar de sus impactos. Esta percepción, según Becerra et al. (2019) ha sido reconocida desde la estrategia global y/o política exterior de seguridad de la Unión Europea, considerando este aspecto como una amenaza hibrida que debe de llevar a los Estados a aumentar su capacidad tecnológica y humana para el desarrollo e implementación de un enfoque integral, para el fortalecimiento de la ciberseguridad y ciberdefensa a nivel nacional, regional y mundial (Organización de los Estados Americanos, 2004)

Dicho fortalecimiento requiere un abordaje integral, donde se conjuguen herramientas, mecanismos, estructuras eficientes y una sólida normatividad que permita promover el uso del ciberespacio desde una perspectiva de ciberdefensa y ciberseguridad, para promover el avance tecnológico, la promoción de expertos y el cumplimiento de la ley en general. Aunque para Castañeda (2019) debe ir de la mano de los operadores y proveedores de servicios que en gran medida mantienen la responsabilidad de las redes (Giral-Ramírez et al., 2017) y los sistemas de información, ajustándose a la normatividad y buscando la generación de una cultura de riesgos que permita la implementación de medidas de seguridad y control para mitigar las amenazas que enfrentan el mundo en la actualidad, sobre todo por las sofisticadas tecnologías a las que se tiene acceso (Serrano, et al., 2019)

En este sentido, tal como lo reconoce Moreno (2020) la ciberseguridad y ciberdefensa no solo dependen de un control interno, sino también de la capacidad de disuasión

sobre otras naciones; provocando o no una estabilidad cibernética que aumenta o disminuye la efectividad para contrarrestar las amenazas externas y prevenir los ataques y la afectación de los mismos. En tal sentido, en la naturaleza de la amenaza global se deben contemplar la construcción y preservación de acuerdos esenciales para la prevención y persuasión de ataques cibernéticos; cada vez más críticos para la seguridad y estabilidad de una nación, pero que también pueden mitigarse a través de un marco normativo estratégico que permita la regulación del ciberespacio y sus componentes en cuanto a la seguridad.

De esta forma la Unión Europea (UE) ha promovido la posición que el derecho internacional y particularmente la carta de las Naciones Unidas (2018) se apliquen al ciberespacio complementando el derecho internacional vinculante, alentando de igual forma el incremento de las capacidades para desarrollar e implementar medidas que permitan fomentar la confianza a nivel de la seguridad y también en términos de cooperación regional e internacional; teniendo en cuenta que estas alianzas facilitan el reforzamiento y mantienen la responsabilidad de los Estados en el control y regulación del ciberespacio en general, que para el caso de Colombia se requiere analizar desde los vacíos de la legislación existente y sobre todo desde la aplicabilidad y cumplimiento de la misma (Moreno, 2020).

Debilidades normativas

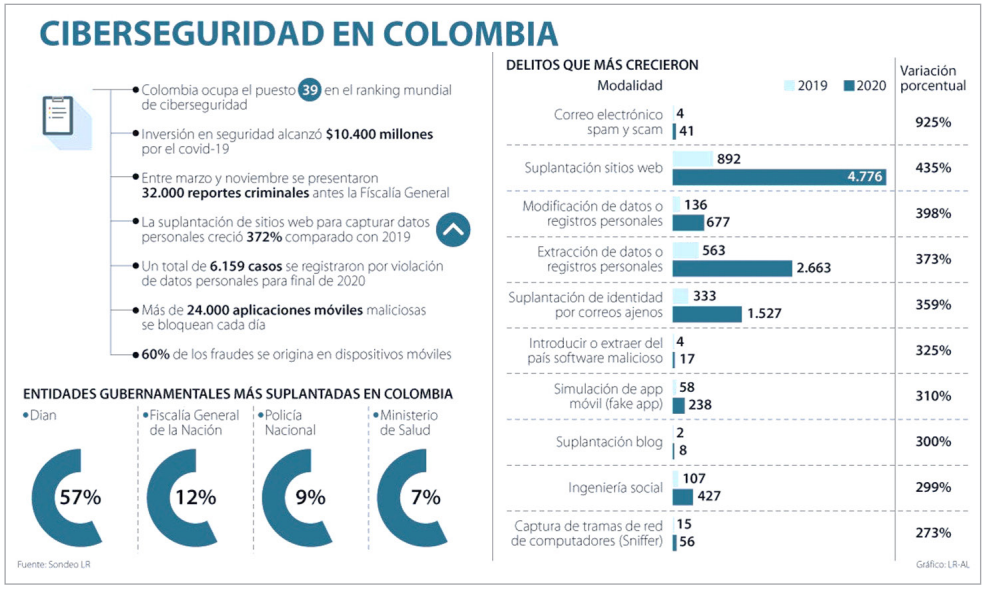
Colombia, según Ruiz (2018) viene adoptando medido y herramientas legales que en términos de ciberseguridad y ciberdefensa comenzarían a fortalecerse a partir de su segunda política en el año 2016, cinco después años de haber salido la primera. Esta buscó fortalecer las capacidades nacionales para responder, reconocer, gestionar y prevenir los riesgos en el ciberespacio, incorporando en ella un coordinador nacional de seguridad digital a cargo de la Presidencia de Colombia. Asimismo, generando un comité de seguridad digital como máximo ente para abordar situaciones intersectoriales de seguridad a cargo del coordinador nacional de seguridad digital e incluyendo, este apartado, aspectos integradores para el desempeño, la operación y seguimiento de entidades públicas y privadas.

De igual manera, el Ministerio de Tecnología y las Comunicaciones (MinTIC) buscó desplegar, a lo largo y ancho del territorio nacional, el modelo de seguridad y privacidad para gestionar e implementar estándares efectivos para salvaguardar los activos críticos de la nación (infraestructura, información y herramientas de comunicaciones); proyectando la mejora continua a nivel nacional e internacional. Además de buscar el desarrollo de un programa para el fortalecimiento de la infraestructura crítica cibernética, apuntándole a la transformación digital, que, junto a la legislación reseñada en el capítulo anterior, buscaría prevenir los ataques y los intereses del Estado (Quintero, 2019).

Después de todo, Colombia ha desplegado medidas para asegurar el ciberespacio y con ello proyectar elementos estratégicos en ciberseguridad y ciberdefensa a nivel nacional, sobre todo en la estructuración de políticas que, a pesar de sus vacíos, han brindado un punto de inicio para prevenir y mantener la estabilidad nacional; pero también generan un ambiente de poca confianza en su aplicación y respaldo jurisprudencial. Esta desconfianza preocupa, no solo por la débil regulación, sino también por su carente divulgación que, a pesar de los organismos responsables, presentan una nula precaria efectividad a nivel nacional y transnacional (Ruiz, 2018).

En este orden, según Salazar (2019) a pesar de los esfuerzos legales, esta normatividad en Colombia se ha convertido en una legislación disuasiva, carente de unas bases político militares que respalden los vacíos jurídicos presentados, sobre todo, pensando que la afectación en la ciberseguridad y ciberdefensa en Colombia, en su mayoría, son delitos cometidos desde otras naciones, dejando la regulación colombiana sin campo de aplicación en otros Estados. Estos crímenes han presentado un crecimiento exponencial, aumentando un 37% entre el 2019 y el 2020, tal como se evidencia en la figura 2, donde paralelamente se asocia al incremento y uso de nuevas tecnologías, provocando que los ciberataques convirtieran esta amenaza en una de las principales economías ilegales en Colombia (Rodrigo, 2021).

Figura 2. Ciberseguridad en Colombia



Fuente: Sondeo LR

Con respecto al documento CONPES 3701, se descuidaron aspectos relevantes dentro del mismo, tales como: la ausencia de protocolos que facilitaran acciones correctas

en relación con la seguridad cibernética (Ministerio de Tecnologías de la Información y las Comunicaciones, 2020). La falta de aplicabilidad en las entidades territoriales, ya que al ser ejecutado en las entidades estatales, el riesgo cibernético se traslada a los territorios, la falta de un órgano regulador de las agencias militares relacionadas con la Ciberdefensa de la nación, falta de equilibrio de la normatividad colombiana con los estándares internacionales promovidos por la Convención de Budapest, ausencia de políticas claras para proteger los derechos humanos de los usuarios del internet, ausencia de personal fiscal idóneo para investigar y sancionar los ciberdelitos (Parra, 2019)

En este lapso entre el 2019 y 2020 de acuerdo con el análisis de Asuntos Legales (2020) se registraron más de 7.000 mil denuncias de cibera taques equivalentes a un 27% de acuerdo con los datos suministrados por la Cámara Colombiana de informática y de telecomunicaciones, mientras los delitos ejecutados a través de medios informáticos pasaron de 21 mil a 36 mil reportando un incremento del 83% entre un año y otro, los delitos financieros presentan la mayor proporción e impacto.

Según la Universidad del Rosario (2019) el 81% de las empresas en Colombia presentan acceso a internet, pero menos del 1% de sus ingresos son destinados a reforzar sus mecanismos de prevención y, el 43, % de estas empresas no están preparadas para enfrentar algún ataque, y las del Estado incluyendo la DIAN, Fiscalía, Registraduría entre otras, no han estado exentas del uso de su nombre para ser suplantadas e incluso a pesar de sus tecnologías ser vulneradas cibernéticamente. Y en materia de Ciberseguridad y Ciberdefensa en Colombia para Vargas (2018), la criminalidad informática ha ido aumentando a partir de la vulnerabilidad de las entidades y empresas, pero también de los vacíos legales; sobre todo por la penalización tan permisiva con la que se cuenta, además de que el principal referente para atacar este tipo de crímenes es el convenio de Budapest del 16 de marzo del 2020, el cual aunque genera confianza entre los Estados, no se ha adoptado ni adaptado para propiciar los elementos e instrumentos jurídicos como un mecanismo de aplicación factible para el Estado colombiano.

Ahora bien, en Colombia la falta de una normatividad estandarizada y carecer de un bloque regional e internacional fuerte y la voluntad política, dificulta la cooperación internacional, sobre todo a nivel regional; donde incluso ni el hacer parte el convenio de Budapest, ha llevado a actualizar ni a construir una legislación procesal que refuerza las políticas existentes y castigue con mayor rigor los crímenes en el ciberespacio. Esto hace más crítico el panorama actual, reflejado en los altos índices de impunidad que, a pesar de los avances normativos, aún carece de elementos contundentes para la identificación, colaboración, definición, penalización y castigo en concordancia con la legislación interna y latinoamericana (Moreno, 2020).

De esta forma, aunque puede adaptarse a un marco normativo de mayor relevancia, entendiendo que su promedio según Ceballos (2020) que de acuerdo con el Capability

Maturity Model CMM se encuentra en 2 (donde 1 significa etapa Inicial y 5 Dinámica o Avanzada), esto demuestra que, a pesar de los avances alcanzados, aún presenta sistemas inmaduros e iniciativas pilotos sin la coordinación de los entes y elementos involucrados.

En consecución, el reto de la Ciberdefensa y la Ciberseguridad radica en la construcción y aprobación de leyes que no solo regulen el uso del ciberespacio, sino que también condenen con mayor rigor a quienes violen el marco normativo. Para ello, se debe contar con la participación de todos los actores que colaboren en el desarrollo de los mecanismos para introducir el respeto por la normatividad, la generación de una cultura del riesgo cibernético y la adquisición de competencias generadas a través de organizaciones como el *Foro para la Gobernanza de Internet* (Ceballos, 2020).

Finalmente, los esfuerzos de Colombia demuestran importantes avances, pero también grandes vulnerabilidades, que hacen necesario promover una ley de Ciberdefensa y Ciberseguridad en Colombia, donde asociadas a políticas sólidas, protejan al Estado, sus organizaciones y los bienes de los colombianos, mediante estándares de seguridad que impidan la evasión de las sanciones penales y económicas, amparándose en la carente instrumentalización de la ley y la ambigua definición técnica de los delitos que deben castigar teniendo en cuenta su gravedad y afectación.

Aspectos relevantes para una ley de Ciberseguridad y Ciberdefensa en Colombia

Los avances tecnológicos y las comunicaciones han sido desarrollos globales para beneficio de la humanidad, que para Arboe (2020) aunque no las convierte en inadecuadas, si pueden ser utilizadas para el accionar ilegal de los grupos al margen de la ley, propiciando gran afectación al Estado, sus organismos y la población en general. Por esta razón, el Estado colombiano ha estructurado una serie de normas para contrarrestar estas amenazas desde el apoyo operacional de Ciberdefensa y Ciberseguridad, pero todas ellas sin el alcance necesario para mitigar el impacto nacional generado por los grupos al margen de la ley.

La preocupación no es para menos, dado que los delitos cibernéticos se han convertido en una forma emergente de la delincuencia nacional y transnacional como uno de los fenómenos de más rápido crecimiento. Para Hernández y Fojón (2016) a medida que el Internet y la tecnología crecen, los delincuentes más se aprovechan de ello, logrando que el delito cibernético crezca a la medida en que avanza la tecnología, logrando evadir la judicialización que se hace cada vez más compleja, y convirtiendo al Estado, las instituciones y las mismas Fuerzas Militares como objetivos de mayor vulnerabilidad para estos grupos ilegales.

A pesar de que las Fuerzas Militares de Colombia cuentan dentro de la organización con unidades tácticas estructuradas y organizadas, y una serie de mandos para cumplir eficazmente la misión relacionada con las operaciones en el ciberespacio; es necesario la generación de una ley que aborde y respalde esta labor sin impedimentos, sobre todo para el abordaje adecuado de la Ciberseguridad y Ciberdefensa en Colombia. Esto debe contar inicialmente con la alineación interinstitucional que permita la planeación, ejecución, seguimiento y mejoramiento continuo desde un objeto misional que favorezca al Estado colombiano y desde allí se logre afrontar el delito Ciberespacial sin alterar las operaciones de Ciberdefensa pasivas y activas a nivel nacional y/o transnacional (Hernández y Fojón, 2016).

Iniciativas o Marco Operacional

La ley en ciberseguridad y ciberdefensa en Colombia requiere pasar de simples iniciativas para consolidar, desde una normatividad, un marco operacional que permita integrar esfuerzos institucionales (tanto privados como públicos) para propiciar organismos a nivel nacional que permitan coordinar y desarrollar operaciones, implementando los mecanismos suficientes para contrarrestar ataques cibernéticos y proteger los intereses del Estado en el ciberespacio, donde a su vez, se ataque la débil difusión, concientización y generación de una cultura de prevención para la acción segura en Ciberdefensa dirigida tanto al sector público como al privado, así como a la sociedad civil (Restrepo, 2014).

De esta forma, según Vargas (2018) se podrán defender intereses nacionales desde un marco normativo de la mano con la política de seguridad nacional, apoyando el Estado desde aspectos trascendentales como la diplomacia, el liderazgo y factores comerciales, así como sus obligaciones internacionales (Convenio de Budapest) y la sociedad global con la (OTAN) desde un entorno cambiante rápido, eficaz y exitosa ante los peligros, pero sin poner en riesgo la soberanía, la integridad del territorio nacional, el derecho y la libertad de los ciudadanos, su seguridad y la del Estado. Prevenir una crisis, conflictos nacionales, regionales o internacionales, entonces, soportan la aprobación de una ley de ciberseguridad y ciberdefensa, sobre todo pensando en las amenazas que envuelve al Estado, junto a la preocupación del acceso al ciberespacio que busca mitigar los ataques y las amenazas cibernéticas del crimen organizado (Sarmiento, 2016).

Normatividad Ciber en las Fuerzas Militares

Es importante que la ley de ciberseguridad y ciberdefensa contemple la normatividad que permita soportar las capacidades e implementación del entorno ***Ciber*** en las Fuerzas Militares y de forma paralela permita el apoyo de las Fuerzas Armadas colombianas de tierra, mar y aire, entendiendo que el ciberespacio es el nuevo campo de batalla y el mundo

continúa cambiando, presentando episodios a nivel nacional e internacional que dan muestra de los alcances y gravedad y abordaje de estas confrontaciones. Lógicamente, este apartado deberá contemplar aspectos importantes como procedimientos, personal capacitado y expertos en Ciberdefensa y Ciberseguridad orientado desde una preparación integral con capacidad para efectuar operaciones militares en el ciberespacio para preservar la integridad del Estado (Rojas, 2021).

Lo anterior, para Quintero (2019) se contrarresta a partir del marco legal que debe contemplar la forma de abordar los riesgos y/o amenazas de los activos estratégicos del Estado, que a través de una unidad de Ciberseguridad y Ciberdefensa y mediante una estructura especializada para los desafíos, implican el dominio ciberespacial. Todo esto bajo la designación de mandos responsables para el desarrollo de operaciones en el ciberespacio que permita mediante unidades fundamentales y especializadas, contar con personal idóneo y aprovechar las capacidades y la experticia en beneficio del Estado colombiano.

Siguiendo a Quintero (2019) deberá estar estandarizado y adaptado al Convenio de Budapest y la OTAN y de esta manera, según Moreno (2020) las políticas, normatividad y directrices actuales podrán reorientarse para promover un cambio pragmático de estandarización como lo exigen los retos del futuro, necesarios para el accionar de la *Ciberinteligencia y la Ciberdefensa* colombiana sin las limitantes en la conducción de la guerra de la información incorporando tácticas internacionales de la OTAN en ambientes complejos donde se respalde el actuar militar a partir de la transformación y conducción de los intereses estratégicos de Colombia, para dotar al cuerpo militar y las agencias de seguridad del gobierno para efectos de neutralizar la fuerza del enemigo, mantener el pie de fuerza propio y evitar la proliferación de los ataques controlados, dirigidos y guiados electrónicamente, para obtener información del estado como parte de una estrategia militar nacional, regional o global, para controlar los tipos de confrontación a que haya lugar.

Aplicabilidad de la normativa sobre las tecnologías militares

Hasta el momento los avances en ciberseguridad y Ciberdefensa se encuentran en la aplicabilidad del documento CONPES 3701. Parra (2019) indica la creación de las siguientes instituciones encargadas de ejecutar la política de ciberseguridad y Ciberdefensa:

Comisión Intersectorial, que se encarga de *establecer los lineamientos de política con relación a las tecnologías de la comunicación y la información y el tema de ciberseguridad y ciber defensa.* Esta comisión se encuentra conformada por el Presidente de la República, los Ministros de Defensa y de las Tecnologías de la Información y las Comunicaciones, los directores de la Policía Nacional, Planeación Nacional y el ColCERT (Parra, 2019).

El Grupo de Respuesta a Emergencias Cibernéticas de Colombia – ColCERT, integrado por personal civil, militar y de otras instituciones y tiene a cargo la coordinación de todas las acciones relacionadas con la protección de la infraestructura crítica del gobierno con respecto a los temas de ciberseguridad y ciberdefensa que puedan comprometer la seguridad de la nación (Parra, 2019).

El Comando Conjunto Cibernético de las Fuerzas Militares – CCOC, conformado por el Comando General de las Fuerzas Militares, con la ayuda de las unidades cibernéticas del Ejército, la Armada y la Fuerza Aérea. Previniendo y contrarrestando los ciberataques contra la infraestructura crítica del gobierno colombiano (Parra, 2019).

El Centro Cibernético Policial: es una plataforma virtual que se encarga de regular todo lo relacionado con los delitos cibernéticos, tales como el extraer información confidencial de bases de datos de las empresas, suplantar sitios web y realizar pornografía infantil, también persigue y sanciona las nuevas redes criminales que usan las nuevas tecnologías para lograr sus acciones delictivas, también realiza campañas de prevención de los ciberataques, y realizar investigaciones en compañía del ColCERT para identificar las vulnerabilidades y eventos informáticos que se encuentran relacionados con la afectación de la seguridad de la infraestructura crítica cibernética del gobierno (Parra, 2019).

El CSIRT PONAL, que es un grupo conformado para brindar ayuda, prevenir e investigar los eventos relacionados con la seguridad de la información, y disminuir el impacto causado por los riesgos de las tecnologías de la información y las comunicaciones (Parra, 2019).

Adicionalmente, a causa de la implementación del documento CONPES 3701, el gobierno colombiano ha dispuesto algunas normativas y doctrinas, las cuales son:

- Política de defensa y seguridad para la nueva Colombia
- Plan estratégico militar PEM 2030
- Ley Estatutaria 1621 de 2013, que fortalece la normativa relacionada con actividades de inteligencia y contrainteligencia
- Resolución 3933 de 2013, que reestructura el Ministerio de Defensa
- Resolución 7436 de 2012, que contribuye a la creación del Comando Conjunto Cibernético
- Oficio no. 05289/cgfm-jemc-jeimc-disai-29-25 del 24 de agosto de 2012, referente a la creación de unidades de Ciberdefensa en las fuerzas militares

Igualmente, surge el CONPES 3854 en el año 2016, referente a la Política Nacional de Seguridad Digital, enfocada en el fortalecimiento de las capacidades de los organismos encargados de la seguridad digital en Colombia, para gestionar los riesgos relacionados

con entornos digitales, aspectos que no se incluyeron en el anterior CONPES 3701, lo cual toma forma en el Modelo Nacional de Gestión de Riesgos de Seguridad Digital creado por el MinTic (Parra, 2019).

La aplicación de las tecnologías y su utilización desde el marco legal deben de presentarse con toda la claridad en una ley de Ciberdefensa y Ciberseguridad en Colombia, sobre todo teniendo en cuenta el nivel de desarrollo operacional y estratégico requerido en cualquier tipo de escenario; estableciendo los intereses del Estado como el factor primordial para contrarrestar o neutralizar las nuevas amenazas emergentes. Ahora bien, como dentro del amplio concepto de aplicabilidad; se encuentran diversos enfoques para el afrontamiento de este aspecto, considerando el entendimiento de la naturaleza del empleo de la tecnología, su transición y posicionamiento a través de (Comandos, Controles, Comunicaciones, Computadores, Inteligencia, Vigilancia y Reconocimiento), de acuerdo con los objetivos de defensa y seguridad para responder de manera oportuna a los ataques y cambios tecnológicos en el futuro (López, 2019).

Por otra parte, para Lind (2017) se debe fortalecer la taxonomía del marco de referencia internacional de ciberdefensa y ciberseguridad, como principal herramienta militar para la protección del Estado colombiano en cuanto a aspectos de conducción y manejo del Ciberespacio por parte de las Fuerzas Militares y los organismos nacionales para atender el funcionamiento y aplicabilidad de las tecnologías militares complejas disponibles en el mercado y producidas principalmente por empresas subsidiarias del estado o del sector privado de los Estados Unidos, Israel, Reino Unido Rusia, China, Francia, Dinamarca, Suráfrica, entre otros. Asimismo, este factor colaborará en resolver los problemas de origen taxonómico del abordaje de la Ciberdefensa y la Ciberseguridad para optimizar los recursos aportados por el Estado y desarrollando de manera efectiva por la fuerza pública, logrando un impacto social positivo de acuerdo a la utilización de nuevas herramientas tácticas operacionales en el modo de conducción de este contexto como parte de la inteligencia militar.

Estándares de Ciberdefensa y Ciberseguridad

Los estándares mínimos se convierten, según Murillo (2016) en un factor de suma importante en el origen y generación de un marco normativo para la Ciberseguridad y la Ciberdefensa en Colombia; en el cual se alberga su producción, directrices y tareas tácticas sobre el desarrollo de operaciones y las maniobras de armas combinadas y sus dimensiones para fundamentar el direccionamiento y conducción del ciberespacio en cualquier campo de combate. Esto deberá explicarse claramente desde el amplio rango de tácticas, técnicas y procedimientos de inteligencia, mediante el empleo de sistemas militares electrónicos para el desarrollo de operaciones, altamente útiles para la identificación de procedimientos, tácticas y técnicas utilizadas para el diseño de estrategias

militares; asimismo aportando al fundamento lógico para la implementación y optimización de las estrategias requeridas.

Los procedimientos y actividades deberán describirse junto al empleo de la inteligencia, de comunicaciones, electrónica, de imágenes, ataques electrónicos y de sensores activos, de acuerdo con el artículo 17 de la ley estatutaria 1621 del 17 de abril del 2013 ley de inteligencia y contrainteligencia, con el fin de obtener información para el posterior análisis con el fin de apoyar el proceso militar para la toma de decisiones. Esto, tal como lo menciona Pollit (2017) propone una precisión aclaratoria de los procedimientos y acontecimientos en la intervención de sistemas de seguridad y redes complejas de información, teniendo en cuenta la importancia en el empleo y acondicionamiento de tecnologías para la seguridad y defensa nacional con la preservación de la reserva legal por un término máximo de treinta (30) años contados a partir de la recolección de la información y con el carácter de información reservada según la Ley de Inteligencia y Contrainteligencia 1621 (2013).

Resultados

Los resultados generados para el artículo *Importancia de una Ley de Ciberseguridad y Ciberdefensa en Colombia* se generan a partir del tratamiento de la información analizada para responder a la problemática planteada. Para ello, en primera instancia se efectuó un análisis unidimensional desde la frecuencia y repeticiones de palabras a partir de las similitudes asociadas a la categoría de importancia de una ley de ciberseguridad y ciberdefensa, para lograr en segunda instancia, la representación gráfica del fenómeno analizado a partir de la utilización del ATLAS ti 9.0. Así, se logró sintetizar la información establecida en 5 variables (Contexto, Escenario, Intereses, Falencias, Necesidades) por su incidencia y 18 códigos por su frecuencia igual o superior a 20, tal como se evidencia en la Tabla 1.

Tabla 1. Matriz de Categoría – Importancia Ley de Ciberdefensa y Ciberseguridad

Nº	Variables	Códigos	Frecuencia
1	Contexto	Nacional	56
		Internacional	60
2	Escenario	Legal	133
		Militar	140
		Operacional	150

Continúa tabla...

Nº	Variables	Códigos	Frecuencia
3	Intereses	Grupos Ilegales	60
		Políticos	62
		Defensa y Seguridad	84
		Operacionales	92
4	Falencias	Aplicación	60
		Persuasiva	66
		Normativas	72
		Legales	84
5	Necesidades	Unificar el Marco Normativo	60
		Marco Operacional	69
		Aplicabilidad de tecnologías	70
		Estándares de Ciber	93
		Respaldo Legal	106

Fuente: Elaboración propia

En este análisis se demuestra elementos comunes que certifican la importancia de una ley de ciberseguridad y ciberdefensa en Colombia. De esta forma, la simplificación de la información demuestra variables de mayor relevancia (Contexto, Escenario, Intereses, Falencias y Necesidades) en el cual, el contexto evidencia cómo esta problemática se relaciona directamente con el entorno nacional, pero con una mayor preponderancia a nivel Internacional.

En cuanto al escenario, se vinculan el legal, militar y operacional, con una preponderancia similar en su importancia, al tiempo que demuestra su relevancia en estos tres indicadores. Referente a los intereses relacionados en la temática analizada, se denotan los grupos ilegales, la política asociada al fenómeno, pero con mayor incidencia la necesidad de la defensa y seguridad nacional al tiempo del actuar operacional. Respecto a las falencias presentadas, se evidencia la falta de aplicación en la normatividad existente, la cual pasa a ser un tema más de persuasión, presentando a su vez grandes vacíos normativos y una necesidad legal efectiva.

Por último, en cuanto a las necesidades detectadas en el estudio, es importante mencionar que se requiere la generación de una ley en ciberdefensa y ciberseguridad desde la unificación del marco normativo existente, donde se fortalezca el soporte operacional, la aplicación de nuevas tecnologías y los estándares para lograr operar las Fuerzas Militares de Colombia bajo el respaldo de la ley y la aplicación de la misma. Por lo tanto, una posible propuesta para de una ley que integrase a todas las normativas mencionadas en el tema

de ciberseguridad y ciberdefensa, y que corrige la necesidad que señala la tesis planteada en este documento, estaría fundamentada en las siguientes condiciones:

- Adopción de estándares internacionales para fortalecer la seguridad de las redes de telecomunicaciones, incluyendo a empresas del sector privado.
- Formulación de disposiciones relacionadas con la protección de datos del usuario de las tecnologías de la información y comunicación
- Identificación de políticas de seguridad adicionales para garantizar el derecho al habeas data y la intimidad del usuario.
- Establecimiento de procedimientos claros para investigar los delitos informáticos y preservar la evidencia digital.

Conclusiones

Es importante destacar que el proceso de transformación tecnológica a nivel mundial requiere complementar el marco legal en materia de ciberseguridad y ciberdefensa en Colombia, implementando los procedimientos a nivel legal para que se puedan desarrollar las actividades operacionales ajustadas a las normas, parámetros y documentos soportados en la ley y no únicamente bajo el convenio de Budapest o bajo los parámetros establecidos por la OTAN. Adicionalmente, esta ley brindaría un aval jurídico de los resultados generados, dándole un valor tangible en el aspecto legal a estas actividades ejecutadas a través de técnicas, tácticas y procedimientos enmarcados en misiones de trabajo, acompañadas de órdenes operacionales de inteligencia, documentadas y descritas de forma detallada para abordar las amenazas y neutralizar las acciones de las mismas y con ello proteger al Estado colombiano.

Las amenazas de ciberseguridad y ciberdefensa en Colombia deben entenderse como eventos impredecibles y con un gran potencial para hacer daño, pero que adoptando medidas preventivas y ofensivas se puede obtener una ventaja sobre el adversario, sobre todo, si se cuenta con el soporte legal para operar desde una normatividad que respalde el accionar del Estado colombiano y sus funcionarios. En este contexto, las operaciones militares se podrán desarrollar abordando el ciberespacio de una forma legal, planeada a través del empleo de nuevas tecnologías, con el propósito de garantizar la seguridad y defensa del estado de la nación y reducir o neutralizar la acción del poder enemigo, con el fin de asegurar la ventaja operacional y adecuada acción del poder militar propio.

La creación de una ley integral de ciberseguridad y la ciberdefensa en Colombia sólida desde el contexto nacional e internacional depende de condiciones tales como la necesidad de implementar una cultura de seguridad digital en la sociedad, a través de mecanismos legales que hagan tomar conciencia sobre los riesgos y manifestaciones del delito informático que puedan afectar la seguridad de la nación, adopción de estándares internacionales de seguridad digital en las empresas del sector público y privado,

implementación de políticas relacionadas con la protección de los derechos humanos del usuario de la internet, además de protocolos que definan una línea a seguir para la investigación y sanción de los delitos informáticos en Colombia y de carácter transnacional.

La ciberseguridad y ciberdefensa necesitan de herramientas, mecanismos, estructuras eficientes y una sólida normatividad para regular el ciberespacio colombiano desde una perspectiva de seguridad nacional que permita promover el avance tecnológico, la promoción de expertos y el cumplimiento de la ley en general. Lógicamente, del ajuste de la normatividad se podrá generar una cultura de riesgos que permita la implementación de medidas de seguridad y control para mitigar las amenazas que enfrenta Colombia debido a las sofisticadas tecnologías que actualmente se presentan.

El identificar el marco legal de la seguridad informática en Colombia, permite conocer el avance del gobierno en relación con los continuos cambios de las tecnologías de la información y la comunicación, y cabe mencionar que esta problemática no solamente es exclusiva del gobierno, sino de la sociedad en general, pues se necesita la integración de todas las esferas sociales y políticas para contrarrestar los riesgos relacionados con el ciberespacio.

Los esfuerzos legales en Colombia en temas de ciberseguridad y ciberdefensa son en la actualidad más disuasivos y menos efectivos, ya que carecen de unas bases político militar que respalden los vacíos jurídicos presentados, sobre todo por el nulo campo de aplicación actual y el crecimiento del 37% entre el 2019 y el 2020 de delitos relacionados con este contexto que lo convierten en una de las principales amenazas para Colombia por la evasión de las sanciones penales y económicas amparadas en la carente instrumentalización de la ley y la ambigua definición técnica de los delitos que deben castigar.

Declaración de divulgación

El autor declara que no existe ningún potencial conflicto de interés relacionado con este artículo.

Autor

Julián Antonio Guzmán Pacheco. Magister en Escuela Superior de Guerra General "Rafael Reyes Prieto", Colombia. Gerente en Seguridad y Análisis Sociopolítico, Escuela de Inteligencia y Contrainteligencia Brigadier General Ricardo Charry Solano, Colombia. Especialista en Administración y Conducción de Unidades Militares, Escuela de Armas Combinadas Ejército, Colombia. Especialista en Administración de Recursos para la Defensa Nacional, Escuela de Armas Combinadas Ejército, Colombia. Profesional en Ciencias Militares, Escuela de Cadetes José María Córdova, Colombia.

ORCID: https://orcid.org/0000-0003-0950-0733
Contacto: guzmanja@esdeg.edu.co

Referencias

Alcaide, Joaquín. (2019). *Delitos electrónicos ante el Derecho Internacional Contemporáneo*. Madrid: Editorial Tecnos.

Arboe, F. (2020). *Chile y legislación en Ciberseguridad ¿en qué punto nos encontramos?* https://blog.nivel4.com/noticias/chile-y-legislacion-en-ciberseguridad-en-que-punto-nos-encontramos/.

Asuntos Legales. (2020). *Ciberdelitos aumentaron 37% durante el primer trimestre de 2020.* https://www.asuntoslegales.com.co/actualidad/ciberdelitos-subieron-37-durante-el-primer-trimestre-de-2020-en-los-peores-meses-de-la-crisis-3126480#:~:text=A%20pesar%20de%20la%20reactivaci%C3%B3n,en%202019%20a%2036.834%20delitos.

Becerra, A. Sánchez, E. Castañeda, A. Bohórquez, A. Páez, R. Contreras, A. y León, I. (2019). *La Seguridad en el Ciberespacio un desafío para Colombia*. Sello Editorial ESDEG.

Ceballos L., A. (2020). *Tendencias Cibercrimen en Colombia 2019-2020*. https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Cepik, M. A. C., & Brancher, P. T. L. (2017). Structure and agency in international relations: state-building and the evolution of the international political system. *Austral. Porto Alegre.* Vol. 6, n. 11 (Jan./Jun. 2017), p. 154-189.

Choucri, N. (2014). Co-Evolution of Cyberspace and International Relations: New Challenges for the Social Sciences.

Congreso de la República. (17 de Abril de 2013). *Ley Estatutaria 1621 del 2013* . Bogota DC, Colombia.

Consejo Nacional de Política Económica y Social República de Colombia. (2011). CONPES 3701 *Lineamientos de Política Para Ciberseguridad Y Ciberdefensa*. Departamento Nacional de Planeación.

Consejo Nacional de Política Económica y Social República de Colombia. (2016). CONPES 3854 *POLITICA NACIONAL DE SEGURIDAD DIGITAL*. Departamento Nacional de Planeación.

Consejo Nacional de Política Económica y Social República de Colombia. (2020). CONPES 3995 *Politica Nacional de Confianza y Seguridad Digital*. Departamento Nacional de Planeación.

Der Derian, J. (2009). *Virtuous war: Mapping the military-industrial-media-entertainment-network*. Routledge.

Feenberg, A. (2019). Postdigital or predigital?. *Postdigital Science and Education, 1*, 8-9.

Giral-Ramírez, W., Celedón-Flórez, H., Galvis-Restrepo, E., y Zona-Ortiz, A. (2017). *Redes inteligentes en el sistema eléctrico colombiano: Revisión de tema.* Tecnura, 21 (53), 119-137. ISSN: 0123-921X. https://www.redalyc.org/articulo.oa?id=257054721009

Guaqueta, F. (2015). *Dimensiones políticas y económicas de la seguridad en el Hemisfeio Latinoamericano: Relaciones Internacionales*. Nuevo Milenio.

Hannant, L. (2019). *Letter to the Editor: A Commentary on Patrizia Gentile's "Resisted Access? National Security, the Access to Information Act, and Queer(ing) Archives"*. Library and Archives Canada .

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2014). *Metodología de la investigación* (6a. ed. --.). McGraw-Hill.

Hernández, A., & Fojón, E. (2016). Ciberseguros: la última línea de defensa. *Revista SIC: ciberseguridad, seguridad de la información y privacidad, 25*(120), 98-100.

Hernández, J. (2016). Infraestructura crítica cibernética (2016). Comando General de las Fuerzas Militares de Colombia.

Klimburg, A. (2020). Mixed Signals: A Flawed Approach to Cyber Deterrence. ***Survival***, ***62***(1), 107-130.

La Gaceta Caese. (2016). *Los ciberataques. Publicación de la Cámara de Comercio de Bogotá y Fundación País Libre No. 19*. Colombia. Rez Impresores.

Lind, M. (2017). Comprendiendo la importancia de la informacion de inteligencia "La guerra cibernetica" en Military Review. *Revista Politica.* Mexico DF.

López, O. (2019). *Caracterización de las organizaciones colombianas en la era de las nuevas tecnologías y sus controles. Un análisis documental*. En-Contexto *Revista de Investigación en Administración, Contabilidad, Economía y Sociedad*, 7 (11), 231-252. [Fecha de Consulta 03 de Abril de 2021]. ISSN: 2346-3279. https://www.redalyc.org/articulo.oa?id=551861265009

Ministerio de Tecnologías de la Información y las Comunicaciones. (2020). *Política Nacional De Confianza Y Seguridad Digital 3995 (2020). Consejo Nacional De Política Económica Y Social República De Colombia Departamento Nacional De Planeación*. Ministerio de Defensa Nacional. Dirección Nacional de Inteligencia. Departamento Nacional de Planeación.

Ministerio de Tecnologías de la Información y las Comunicaciones. (2020b). *Política nacional de confianza y seguridad digital 3701 (2011). Consejo nacional de política económica y social república de Colombia departamento nacional de planeación*. Ministerio de Defensa Nacional. Dirección Nacional de Inteligencia. Departamento Nacional de Planeación.

Ministerio del Interior y Seguridad Pública. (2018). *Estrategia Nacional de Ciberseguridad*. https://www.camara.cl/verDoc.aspx?prmID=176320&prmTIPO=DOCUMENTOCOMISION

Moreno, A. (2020). *Riesgos, avances y el camino a seguir en américa latina y el caribe (2020)*. Banco Interamericano de Desarrollo https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf.

Naciones Unidas. (2018). *Resolución aprobada por la Asamblea General (2018) Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional*. Organización de las Naciones Unidas.

Nye, Jr., J. S., & Villanueva Rivas, C. (2017). El poder en el siglo XXI. Entrevista con Joseph S. Nye, Jr. *Revista Mexicana De Política Exterior*, (111), 165–179. https://revistadigital.sre.gob.mx/index.php/rmpe/article/view/318

Organización de los Estados Americanos. (2004). *Adopción de una estrategia interamericana integral de seguridad cibernética: un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética*. Organización de los Estados Americanos OEA.

Parra, J. (2019). *Delitos informáticos y marco normativo en Colombia*. Universidad Nacional Abierta y a Distancia (UNAD).

Pollitt, M. (2019). *Economics and Policy of (Electrical) Energy Storage*. https://conferences.ncl.ac.uk/media/wwwnclacuk/engineering/Michael%20Pollitt.pdf

Quintero, Y. (2019). *La seguridad y Ciberdefensa en Colombia*. Universidad Piloto de Colombia. http://polux.unipiloto.edu.co:8080/00001596.pdf.

Real Academia Española. (2018). *Seguridad*. Real Academia Española.

Rodrigo, O. (2021). *Las acciones estatales contra el delito en Colombia*. Investigación realizada por solicitud de IKV Pax Christi.

Rojas, J. C. O. (2021). *Ciber seguridad de transacciones en sistemas de medición inteligente usando cadenas de bloques* (Doctoral dissertation, Instituto Tecnológico De Morelia).

Ruiz, S. (2018) *Protección de Datos y Seguridad Digital en Colombia Una propuesta sobre la necesidad de adhesión al Convenio de Budapest* (2001). Universidad de los Andes.

Salazar, P. G. (2019). *El libro blanco del hacker*. Ra-Ma Editorial.

Sánchez, L. (2017). *Por imperativo legal de las redes. Una vision desdes la perspectiva de la Ciberseguridad y la Ciberdefensa*. Murcia, España.

Sarmiento, J. (2016). La responsabilidad contractual por los riesgos previsibles, entre la autonomía de la voluntad privada y la rigurosidad de las normas de contratación pública. *Revista Derecho del Estado*, (37),189-211. https://www.redalyc.org/articulo.oa?id=337650446006

Serrano, A. X. O., Vaca, M. J. M., Rivadeneira, L. I. T., & Páez, C. F. (2019). Revisión sistemática del estado del arte de las Tecnologías de Información y Comunicación (TICS) y Seguridad Alimentaria. *Debates sobre innovación, 3*(2).

Universidad del Rosario. (2019). *Colombia no está preparada ante un ciberataque*. https://urosario.edu.co/static/UCD/Colombia-no-esta-preparada-ante-un-ciberataque/index.html

Vargas, M. (2018). *Ciberseguridad y Ciberdefensa: ¿qué implicaciones tienen para la seguridad nacional?* [Trabajo de Grado] Universidad Militar Nueva Granada.