DEFENDIENDO EL CIBERESPACIO: UNA APROXIMACIÓN AL ESTADO DE COLOMBIA FRENTE A LA CIBERDEFENSA

ESPECIALIZACIÓN EN ALTA GERENCIA DE SEGURIDAD Y DEFENSA

ENSAYO

AUTOR: JONATAN CRUZ RUBIO

U4500254

FEBRERO DE 2021

Resumen

En el presente ensayo se presenta una aproximación al estado de Colombia frente a la ciberdefensa nacional, con la globalización se lograron avances importantes y uno de ellos fue la tecnología y las telecomunicaciones, dando gran importancia al ciberespacio, que se ha convertido en una oportunidad de desarrollo económico y social, pero a su vez ha vuelto vulnerable a varios actores involucrados en el mismo, poniendo al descubierto la infraestructura crítica de cada nación, debido a que los actos ilícitos han migrado hacia el ciberespacio se hace necesario generar estrategias de ciberdefensa del Estado. Este panorama se presenta a nivel internacional, motivo por el cual dentro del presente documento se realiza una comparación entre las políticas establecidas en Colombia y las estrategias desarrolladas en otros países, dejando al descubierto los avances que a nivel nacional se han logrado y que le han permitido al país ser pionero en la región, en lo referente a ciberdefensa.

Abstract

This article presents an approach to the state of Colombia in the face of national cyber defense, with globalization important advances were achieved and one of them was technology and telecommunications, giving great importance to cyberspace, which has become an opportunity for economic and social development, but at the same time it has made several actors involved in it vulnerable, exposing the critical infrastructure of each nation, due to the fact that illicit acts have migrated to cyberspace, it is necessary to generate State cyber defense strategies . This panorama is presented at the international level, which is why within this document a comparison is made between the policies

established in Colombia and the strategies developed in other countries, revealing the advances that have been achieved at the national level and that have allowed the country to be a pioneer in the region, in terms of cyberdefense.

INTRODUCCIÓN

Nos encontramos en una nueva era, la era digital que conlleva modificaciones en la forma como vivimos y nos relacionamos; gracias a la tecnología se han evidenciado cambios importantes desde diversos ámbitos tanto económicos, como sociales, incluyendo la cultura, la educación, la política y especialmente lo militar, en donde la información tiene un gran valor y la defensa del ciberespacio, siendo este el quinto dominio de guerra, se ha convertido en un tema de interés para el Estado, debido al aumento en los niveles de riesgo ante las ciberamenazas, es así como a medida que los "ataques cibernéticos crecen en número y sofisticación, la amenaza se percibe cada vez más como un problema tanto en el contexto de Seguridad Nacional como en el internacional" (Becerra et al., 2019. pg.18). Lo anterior genera que nuestra sociedad, organizaciones y la población en general sean sensible a numerosas amenazas.

Hoy en día se evidencia la falta de madurez en cuanto al tema de ciberterrorismo, en la medida que se tiene una visión errada de lo que en realidad es, estamos en un estado nuevo a nivel mundial y con nuevos desafíos que Colombia debe enfrentar en cuanto a la ciberdefensa y ciberseguridad, resaltando la importancia que todos los sectores tanto privados como públicos deben asumir para evaluar y disminuir los posibles riesgos a los que se pueden enfrentar (Becerra, et al., 2019 pg. 13). generando de esta manera que la aplicación y puesta en marcha de las políticas de seguridad y ciberdefensa

se vean afectadas, especialmente en países latinoamericanos. No cabe duda que ahora la guerra está basada en armas digitales que son difíciles de detectar, con un ataque digital al sistema informático se pueden generar daños de difícil recuperación afectando de manera directa el buen funcionamiento de una nación.

Teniendo en cuenta lo anterior, el objetivo de este artículo es indagar acerca de la situación actual de Colombia frente a la ciberdefensa, en este orden de ideas, se inicia con la conceptualización de lo que se entiende por ciberespacio, infraestructura crítica, ciberdefensa, se continúa con la situación general en Chile y España y específicamente en Colombia. Finalmente se presentan algunas conclusiones frente a la situación descrita. Este ensayo pretende dar un acercamiento inicial al campo de la ciberdefensa en Colombia.

EL CIBERESPACIO COMO UN SITIO DE CONFLICTO

¿Qué Entendemos Por Ciberespacio?

Todo surge con la primera revolución industrial, en donde las economías mundiales se han regido desde las políticas industriales, que ha generado modelos tecnológicos según la época en la que se encuentra, lo que conlleva cambios en la formación de la mano de obra, los avances científicos, la instauración de nuevas políticas y sistemas institucionales en busca de una mejor condición social a nivel regional. Este modelo productivo responde a una proyección nacional de desarrollo que es continuamente vigente (Delfín, Acosta, 2016). A finales del siglo XX y en este tiempo del siglo XXI, se ha evidenciado una hiperglobalización debido a la aparición de la era digital,

que ha generado cambios profundos y acelerados en lo social, la política y la economía (Fernández, 2018)

Estos cambios se han visto reflejados a partir del uso de las invenciones tecnológicas relacionadas con la robótica, el internet, la inteligencia artificial, las impresiones en 3D; el uso de la tecnología se ha visto inmerso en diferentes campos como la biología, están innovaciones han generado transformaciones en la forma como se hacen las cosas y por ende ha cambiado al mundo, generando una revolución cultural, en la cual se vela por los asuntos internos pero sin descuidar las demandas internacionales. Estas transformaciones han permitido cambios positivos en la comunicación global, pero también ha generado manifestaciones negativas como, por ejemplo, las brechas tecnológicas y de acceso a la información en muchas ocasiones por las condiciones sociales (Fernández, 2008).

Es así como, se evidencia una nueva forma de concebir las relaciones humanas, ahora es el ciberespacio el entorno para llevar a cabo las actividades productivas, económicas, educativas, sociales de las sociedades contemporáneas (Escuela de Altos Estudios de la Defensa, 2014). De esta manera, al hablar de este aspecto se puede mencionar que se cuenta con un escenario donde las relaciones humanas pueden originar conflictos entre individuos o grupos (París, 2013), debido a que cada uno cuenta con intereses particulares de acuerdo a sus intereses.

Uno de los primeros países en identificar este nuevo espacio de conflicto, fue Estados Unidos desde su Departamento de Defensa y desde allí empezó la conceptualización de este nuevo escenario llamado ciberespacio, que fue creado por humanos y empleado para su servicio, es así como se puede mencionar, que es una dimensión donde se llevan a cabo diversos procesos de interconexión, de los cuales

dependen para su funcionamiento variedad de herramientas y máquinas que son empleadas en el espacio natural (Gaitán, 2018). Desde esta perspectiva, el ciberespacio trasciende todo límite geopolítico, lo que permite eliminar las fronteras de las soberanías, generando de esta manera riesgos tanto para la seguridad y la defensa de la nación. El ciberespacio combinado con la naturaleza conflictiva del ser humano, da paso a una guerra cibernética, que trae consigo riesgos y amenazas tanto para las personas, las empresas y la sociedad en general.

El ciberespacio es definido por The Economist (2010) como el quinto dominio de batalla, legitimando de esta manera, las acciones de protección desde las fuerzas militares en conjunto con las instituciones públicas y privadas. Dando paso así al concepto de ciberdefensa y las implicaciones que conlleva.

Pero, ¿por qué es tan importante la defensa del espacio?, pues bien, con los avances tecnológicos y la internet, han cambiado también las acciones del Estado, quienes ahora monitorean el funcionamiento de diversos campos como lo son los servicios públicos, los sistemas de comunicación entre otra información que es de interés para la seguridad nacional, pero estos avances trajeron consigo amenazas que ponen en riesgo el funcionamiento adecuado tanto del Estado como de sus habitantes, en tanto que la infraestructura se ha visto vulnerable a los ataques desde la red en donde el anonimato es el atractivo para quienes cometen actos ilícitos y los recursos que requieren no son grandes, además de la dificultad técnica que implica rastrear estos hechos. (Candau, 2010).

Actos como el ciberterrorismo, ciberespionaje, el cibercrimen o hacktivismo, no necesitan principalmente un respaldo estatal; por el contrario, muchas veces los grupos que realizan estos crímenes, lo que desean es un reconocimiento intelectual y no

ganancias económicas (Villanueva, 2015), esta modalidad implica es robar información importante con fines comerciales, políticos o militares, que le permiten al Estado que la recibe tener una ventaja estratégica.

La Infraestructura Crítica

Se puede definir a la infraestructura crítica como las instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto importante en la salud, la seguridad o el bienestar económico de los ciudadanos y en el funcionamiento de las instituciones del Estado (Sánchez Gómez-Merelo, 2011).

De igual manera se puede definir como la “Información interconectada e infraestructuras de comunicación esenciales para el mantenimiento de los servicios básicos de la sociedad (salud, seguridad, bienestar económico o social de las personas) cuyos daños o destrucción tendría serias consecuencias” (Meridian, 2016, pg. 7). La Infraestructura Crítica de la Información (ICI), del gobierno es la esfera más sensible para el funcionamiento del Estado en el ciberespacio, de allí la importancia de las políticas y estrategias empleadas para la protección de la misma. Esta infraestructura crítica de la información, es la red de activos que son fundamentales para el funcionamiento social y económico, es el cimiento de una sociedad, incluye los datos personales, esta información es altamente sensible y al ser interferida afectaría la seguridad de la población.

Cuando esa seguridad se ve afectada, se puede hablar de ciberterrorismo, siendo este el mayor desafío en seguridad. El ciberterrorismo es definido por Rudner en el año

2013, como el uso de la información que se encuentra en la web, para las operaciones en el área digital, con el objetivo de generar caos o miedo, este ingreso se hace de manera violenta, la meta de este tipo de operaciones es la infraestructura crítica. Rudner menciona de igual manera que este concepto es algo discutible y emplea de igual manera la palabra hacktivismo, generando una confusión en términos, lo que demuestra que aún se desconoce información al respecto, la diferencia entonces estaría en que el ciberterrorismo conlleva muerte y profundo temor, mientras que el hacktivismo, son acciones de protesta, que pueden alterar el orden junto con una manera de llamar la atención mediática. De todas formas, las ciberamenazas son el reto en seguridad de la actualidad, por esta razón la capacidad de inteligencia de los Estados debe estar atenta frente a las posibles situaciones de conflicto que se puedan presentar.

Es así, como el Estado debe estar actualizado en cuanto a ciberdefensa y ciberseguridad, siendo estos temas importantes en los planes de seguridad y las respectivas políticas, en Colombia, la atención en este tema se dio en el año 2011 con el CONPES 3701 de 2011, que fue sustituido en el año 2016 con el CONPES 3854, en estos documentos están consignados los lineamientos de política pública para las instituciones encargadas de gestionar la ciberseguridad y ciberdefensa del país. (Villanueva, 2015).

Ciberdefensa

Se puede definir la ciberdefensa, como las acciones que lleva a cabo el Estado para proteger y controlar los posibles riesgos cibernéticos, con el objetivo de poder hacer

uso del ciberespacio con tranquilidad, protegiendo de igual manera la integridad del territorio. La ejecución de la ciberdefensa está al mando de las Fuerzas Armadas, quienes protegen las infraestructuras críticas del Estado. La diferencia entre ciberseguridad y ciberdefensa radica en que la primera maneja las labores preventivas del uso del ciberespacio; mientras que la segunda, conlleva ejercicios preventivos y reactivos, lo que le permite reaccionar frente a los ciberataques, es así, que se puede mencionar que la ciberdefensa, es la capacidad del Estado para prevenir y neutralizar las amenazas cibernéticas que afectan la soberanía, esta defensa es tanto activa como pasiva de todo el ciberespacio, donde se protege la información institucional y se resiste contra los ciberataques, su principal arma es la comunicación militar que protege de esta manera la infraestructura crítica del país, según lo presentado por las Fuerzas Militares de Colombia (FF.MM. y Ejército Nacional, 2015)

PANORAMA INTERNACIONAL: Chile Y España

La ciberseguridad en Chile, cuenta con una plataforma web denominada DataChile, el objetivo principal de este espacio es tanto la optimización como la eficacia de las decisiones públicas, en la cual se recopilan los datos públicos de los chilenos, dicha plataforma es un bien público y de esta manera los chilenos pueden estar enterados de la situación de su país (DataChile, S.f.). Los datos encontrados en este sitio web, son obtenidos de diferentes organizaciones como: Ministerio de Desarrollo Social (MDS), Instituto Nacional de Estadísticas (INE), Aduanas Chile, Ministerio de Economía (MINECON), Ministerio de Educación (MINEDUC), Departamento de Medición y Registro Educacional (DEMRE), Departamento de Extranjería y Migración, Ministerio del Interior, y, Subsecretaría de Telecomunicaciones (SUBTEL). Chile es un país donde sus

habitantes están utilizando el ciberespacio constantemente, de allí, la necesidad del Estado de garantizar una ciberseguridad, adecuada a sus ciudadanos mediante la implementación de políticas de seguridad. La ciberseguridad en Chile se da a raíz de un millonario ciberataque al Banco Chileno por parte de piratas informáticos, el 24 de Mayo de 2018, se presume que el ataque fue de una banda de Europa del Este o Asia, según las investigaciones se trató de un virus de tipo SWAPQ, los expertos mencionan que es un virus mutado, pues antes no se había presentado uno similar, por esta razón se denominó como virus de día cero, ya que no se conocía sus vulnerabilidades. A raíz de esta situación, se declaró que en el mes de octubre de cada año se realicen actividades con el fin de fomentar ejercicios, en los cuales tanto los actores públicos como privados puedan participar y de esta manera garantizar la ciberseguridad en Chile. (Cámara de Diputados de Chile, 2018). El NC-SI sitúo a Chile en el 2018 en el primer lugar en el ranking Internacional de protección de ciberseguridad en América Latina.

El tercer puesto del ranking lo ocupa España, en su estrategia de ciberseguridad tiene el Consejo Nacional de Ciberseguridad, además de este consejo cuenta con una unidad especializada en estrategias nacionales, también con el Centro Criptológico Nacional y el Centro Nacional de Inteligencia que se alinea con el equipo de respuesta ante emergencias informáticas. Su Esquema Nacional de Ciberseguridad, es un servicio que ofrece el Gobierno de España, con el fin de llevar a cabo los requisitos de seguridad informática de las TIC, bajo el Decreto-ley Real 12/2018. La ciberdefensa está bajo el poder del Mando Conjunto de Ciberdefensa (MCCD), su función es ejecutar las acciones relacionadas con la ciberdefensa del ciberespacio. España por medio de una publicación

cada año mantiene informada a su población acerca de las amenazas cibernéticas que ha afrontado.

De igual manera, ha participado en el Centro de Excelencia de Defensa Cibernética Cooperativa de la OTAN, el Instituto de Ciberseguridad de España, en alianza con la OEA, anualmente ofrecen un programa de capacitación especializada de alto nivel, con contenido exclusivo y sin costo para las personas interesadas en desarrollar políticas nacionales, que brinden seguridad al ciberespacio.

Dentro de la normatividad española, se cuenta en su esquema nacional de ciberseguridad, tanto el Decreto Real N° 3/2010 como el Decreto-ley Real 12/2018, que trata la seguridad de las redes y sistemas de información de servicios digitales públicos y privados. En el caso de la ciberdefensa, España cuenta con un Mando Conjunto de Ciberdefensa (MCCD), desde allí se planean y ejecutan las acciones para la defensa del ciberespacio frente a cualquier tipo de amenaza.

COLOMBIA

Las operaciones Militares en el ciberespacio protegiendo la infraestructura crítica cibernética nacional, han tomado fuerza a partir del 2010 cuando el expresidente Juan Manuel Santos asumió su cargo, en el año 2011, el gobierno expidió el primer documento CONPES, en el cual se parametriza la institucionalidad en cuanto a la ciberseguridad y ciberdefensa, con este evento se da origen al Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT) y el Comando Conjunto Cibernético (CCOC), encargado de la protección de la infraestructura crítica cibernética militar y nacional, en

este punto las fuerzas militares desarrollan su capacidad en ciberdefensa mientras que la policía lo hacía en ciberseguridad.

Lo anterior, se llevó a cabo debido a los diversos ataques cibernéticos recibidos en la nación, en donde se evidenció, cómo se puede aprender de las situaciones que se viven y a partir de ellas fomentar estrategias que permitan fortalecer la infraestructura crítica nacional. Los hallazgos de estos ataques se conocen gracias al estudio de tendencias del cibercrimen, realizados por investigadores de la Cámara Colombiana de Informática y Telecomunicaciones (CCIT), el Centro de Capacidades para la ciberseguridad de Colombia (C4) y el Tanque de Análisis y creatividad de las TIC (Tic Tac).

En el ColCERT, se enmarca tanto la ciberdefensa como la ciberseguridad que están a cargo del Ministerio de Defensa Nacional, su principal función, es la de disponer los movimientos necesarios para proteger la infraestructura crítica de la nación ante emergencias de ciberseguridad. Según el ColCERT, el CSIRT de la Policía Nacional Colombiana registró una disminución en los incidentes cibernéticos, ubicando al país junto a Chile como uno de los pocos países latinoamericanos en obtener este logro, gracias a los avances en Ciberseguridad y Ciberdefensa según el Índice Mundial de Ciberseguridad de la Unión Internacional de Telecomunicaciones (UIT), en el 2014 se ubicó en el quinto lugar del Ranking y el noveno a nivel mundial junto a Dinamarca, Egipto, Francia y España (Conpes3854,2016, p.16).

Este logro, se ha obtenido en parte por las estrategias de prevención que han venido desarrollando el centro Cibernético Policial Colombiano, por medio de campañas

para concientizar, sensibilizar y educar acerca de los riesgos de Seguridad Digital, siendo coherentes con las recomendaciones dadas desde el Consejo Mundial de la industria de tecnologías de la información (ITI por sus siglas en inglés).

Del mismo modo, según se contempla en el Conpes 3854 de 2016, en cuanto al riesgo se tiene una gestión sistemática y cíclica que permite determinar una actividad, evaluarla, ver cuáles son sus riesgos, proyectando los posibles resultados tanto a nivel social como económicos y de esta manera permite modificarlos. (Conpes 3854,2016, pg.26). Dicha gestión se lidera desde el gobierno para la Defensa y Seguridad Nacional.

Colombia, ha desarrollado una mejor articulación para prevenir, controlar y manejar los resultados de este mundo globalizado, la cooperación con otros países en cuestión de Ciberseguridad, es apoyada por las innovaciones en las soluciones desde las TIC, permitiendo de esta manera que tanto los ciudadanos como el Estado, tenga la capacidad para identificar, analizar y evaluar información de naturaleza cibernética (MinTIC,2014, pp.5–10).

Colombia Y Su Marco Legal

Colombia ha logrado ser pionero en su región en cuestiones de ciberdefensa y ciberseguridad, gracias a la creación de dos estructurados lineamientos de política pública para el dominio del ciberespacio y salvaguardar su seguridad y defensa (Conpes 3854,2016). El primero es el Conpes 3701 de 2011, que pone como objetivo “fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético (ciberseguridad y ciberdefensa), creando el ambiente

y las condiciones necesarias para brindar protección en el ciberespacio" (pg. 20). Para poder cumplir con este objetivo entre los pilares están:

- Adoptar un marco interinstitucional adecuado con la prevención, coordinación y control para asumir las amenazas o riesgos que se puedan presentar.
- Desarrollar programas para capacitar y formar de manera especializada en seguridad de la información
- Fortalecer la legislación colombiana y la cooperación internacional en lo referente a este tema (Conpes 3701, 2011).

A partir de este documento, el encargo de los asuntos de ciberdefensa pasa al Ministerio de Defensa, donde se crean nuevas instituciones, que son el punto máximo de coordinación y orientación en torno a la seguridad digital (Contreras, 2019), estas a su vez se conforman por una comisión intersectorial, encargada de las estrategias, gestión y políticas relacionadas con la ciberdefensa de la información pública y la infraestructura tecnológica. Gracias a este documento, Colombia se denominó entre los primeros países de la región en establecer planes de acción concretos en la defensa del ciberespacio. (Conpes 3854, 2016).

El cumplimiento del objetivo del Conpes 3701 de 2011, se encuentra encabezado por el presidente de la República, y acompañado por los ministros de Defensa y de las Tecnologías de la Información y Comunicaciones, el asesor para la Seguridad Nacional, también por los directores del Departamento Administrativo de Seguridad (DAS) y de Planeación Nacional, de igual manera hace parte el coordinador del Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT). Así mismo, pueden extender la

invitación a representantes de los sectores académico y privado, como a expertos internacionales u otras instituciones del Estado (Conpes, 3701, 2011, pp. 21-22). De igual manera, se crean el ColCERT, quien se encarga de coordinar a nivel nacional, las acciones necesarias para la protección de la infraestructura crítica del Estado y el Comando Conjunto Cibernético (CCOC) responsable de la ciberdefensa, bajo la dirección del General de las Fuerzas Militares, quien delega funciones a las Fuerzas Militares, por sectores específicos para prevenir y neutralizar las amenazas o ataques al ciberespacio que puedan afectar los intereses de la nación.

En el año 2015, al realizar la evaluación del Conpes 3701, en cuanto a las políticas de ciberseguridad y ciberdefensa, se concluyó que el manejo inadecuado de la información y la descoordinación institucional, generaron un cruce de información de datos que no concluían mucho. Dentro de los logros se obtuvo la institucionalidad en ciberseguridad y ciberdefensa (Conpes 3854, 2016). El 11 de abril de 2016, se crea el Conpes 3854, con el propósito de suplir las falencias del anterior documento. Esta vez se identificó, clasificó y priorizó la infraestructura crítica cibernética nacional.

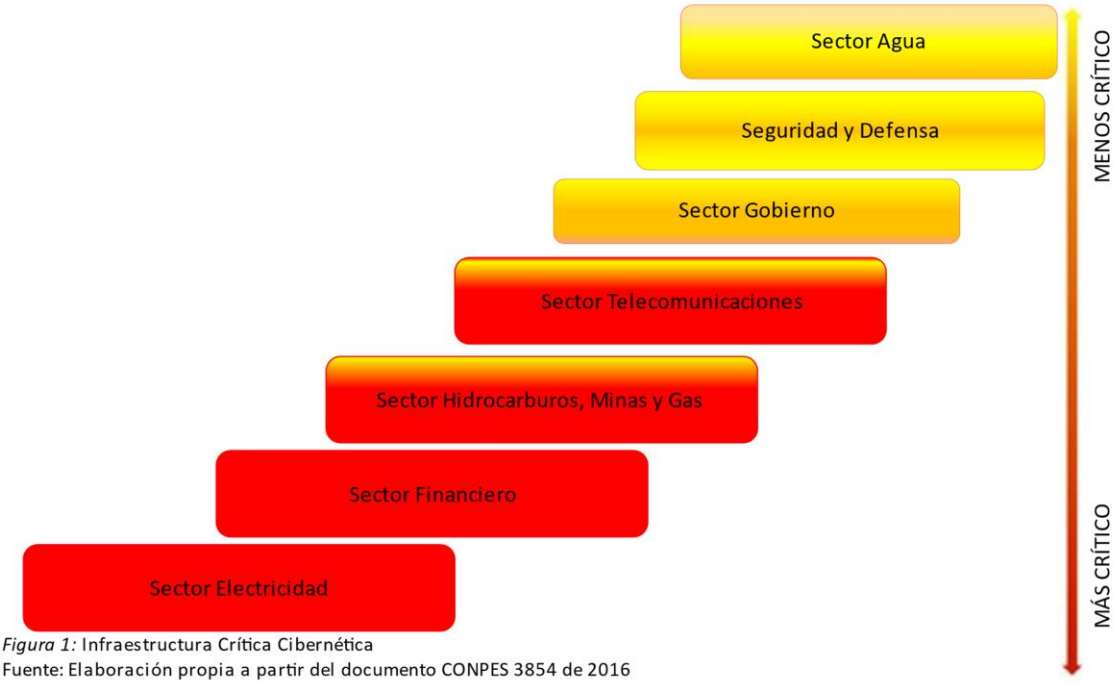

Figura 1: Infraestructura Crítica Cibernética
Fuente: Elaboración propia a partir del documento CONPES 3854 de 2016

Su objetivo principal es:

> "Fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país". (Conpes 3854, 2016, p. 47).

Este documento tiene un enfoque de seguridad digital que pretende la sensibilización, la identificación y la gestión adecuada del riesgo, promover prácticas digitales adecuadas, en donde se vinculen más actores que posibiliten el maximizar las oportunidades del entorno digital, permitiendo un desarrollo económico y social (Conpes 3854, 2016). En el 2005 la organización para la cooperación y el desarrollo económicos-

OCDE recomienda implementar una gestión del riesgo como eje articulador, lo anterior debido a que actividades criminales, de terrorismo, inteligencia de Estados, entre otros, han migrado al ciberespacio. Es así como se pasa de un enfoque que busca la preservación de la seguridad de los sistemas de información y las redes, a uno centrado

Figura 2: Política trazada por el documento Conpes 3854 de 2016
Fuente: Elaboración propia a partir del documento CONPES 3854 de 2016

en la gestión del riesgo inherente de las actividades sociales y económicas dentro del entorno digital (Conpes 3854, 2016). De esta manera se incluye una visión sobre temas técnicos, jurídicos, económicos y sociales, como de los actores involucrados, promoviendo la corresponsabilidad en relación con los lineamientos de la ONU (Conpes 3854, 2016). La gestión de riesgo y la fundamentación de la política de seguridad digital, complementan de igual manera el Conpes anterior, presentando las oportunidades que desde el ciberespacio se dan para el desarrollo de la sociedad y la economía colombiana. A continuación, se presenta la política de gestión del riesgo.

De igual manera en el documento Conpes 3854 de 2016, se encuentran las dimensiones en las cuales se enfoca la Seguridad Digital que se puede representar así gráficamente.

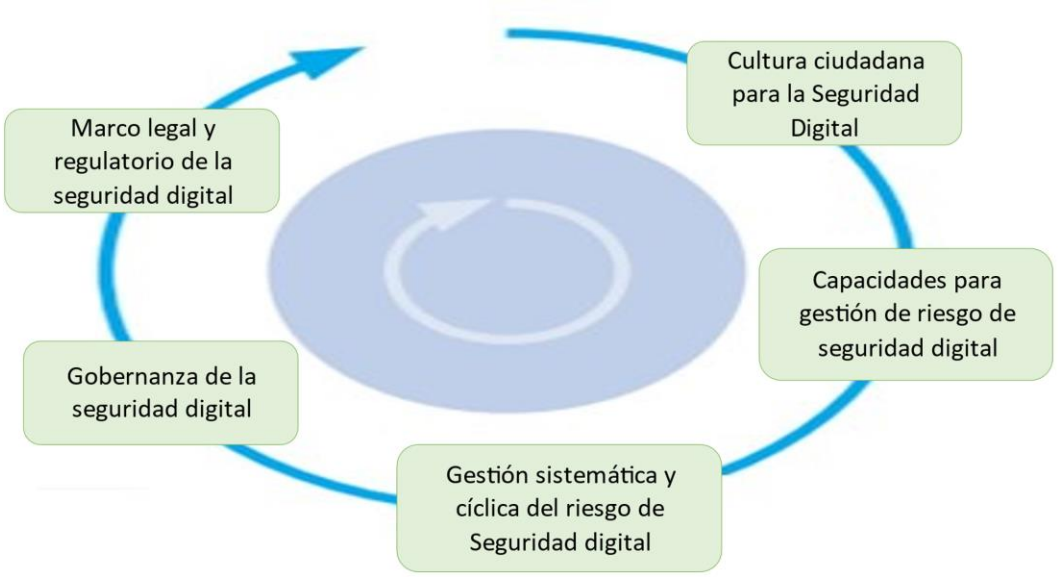

Figura 3: Las cinco dimensiones estratégicas del documento CONPES 3854 de 2016
Fuente: Elaboración propia a partir del documento CONPES 3854 de 2016

Algunos de los componentes del documento Conpes 3854, incluye la creación de la figura de coordinador Nacional de Seguridad Digital, los principios fundamentales se enmarcan desde el enfoque de Gestión de Riesgos, en donde se pretende establecer un marco institucional articulado que involucre a todas las partes interesadas. Otra estrategia, es la de fortalecer la seguridad de los individuos y el Estado en el entorno digital, consolidando las capacidades del país para hacer frente al crimen (Conpes, 2016, pg.50). El proceso de gestión del riesgo requiere la selección entre varias alternativas con diferentes costos y beneficios para reducir el riesgo restante a un nivel aceptable (Becerra, et al.,2019).

De esta manera queda evidenciado que tanto la defensa como la seguridad del ciberespacio, no está solo en las manos del Estado o las fuerzas militares, por lo que entre las estrategias planteadas en el Conpes 3854 de 2016, se encuentra la concientización de las múltiples partes involucradas.

Figura 4: Múltiples partes involucradas
Fuente: Elaboración propia a partir del documento CONPES 3854 de 2016

Con la estrategia 4 se pretende fortalecer la Defensa y soberanía del entorno digital, para lo cual se debe desarrollar capacidades de prevención, detección, contención, respuesta, recuperación y Defensa garantizando los fines del Estado. Otro punto fundamental que se aborda, es el de generar mecanismos permanentes y estratégicos permitiendo la cooperación, colaboración y asistencia en Seguridad Digital, tanto a nivel nacional como internacional.

Sumado a lo anterior, entre las estrategias de la Ciberdefensa en el Estado Colombiano en las que las fuerzas Militares han soportado el desarrollo de capacidades,

se destaca en una primera instancia la selección del personal que trabaja para la ciberdefensa, el cual es capacitado y entrenado continuamente; de igual manera los procesos fueron estandarizaron, se aplican normas y estándares internacionales, la tecnología se adquiere teniendo en cuenta su funcionamiento y servicios, se fortalecieron las operaciones en ciberdefensa, la investigación, el desarrollo e innovación, la investigación y los laboratorios.

Al tener este documento Conpes, se ha protegido las dinámicas en el ciberespacio y la infraestructura crítica de Colombia, de esta manera se favorecen los procesos de resiliencia que conlleva las amenazas, esto se logra gracias a la flexibilización y recuperación de la seguridad ante situaciones de adversidad, que permite una revisión continua, fortaleciéndose incesantemente (Becerra et al., 2019), lo anterior permite tener en el ciberespacio una manera de favorecer el desarrollo social y económico.

Entidades encargadas de la ciberdefensa en Colombia

- ***Ministerio de Defensa Nacional***

La defensa y ciberdefensa de la nación colombiana está a cargo de esta institución. El Ministerio de Defensa (Mindefensa) tiene como objetivo proteger la democracia, a través de la seguridad y defensa al igual que la aplicación de capacidades que salvaguarden la integridad nacional, en el decreto 1512 de 2000 en su artículo 5, se estipula que este Ministerio participa en el desarrollo y ejecución de políticas de defensa y seguridad en el territorio nacional, garantizando su soberanía, integrando a todo el territorio. Brindando las condiciones para ejercer el derecho de libertades públicas y garantizar que los colombianos convivan en paz.

- ***Comando Conjunto Cibernético de las Fuerzas Militares (CCOC)***

Es la dependencia de las fuerzas militares encargada de la coordinación de respuestas a incidentes o ataques que afecten la seguridad nacional. Los objetivos de esta dependencia son:

La ejecución de medidas de defensa a nivel de hardware y/o software y la implementación de protocolos de ciberdefensa, el análisis forense, defender la infraestructura crítica y minimizar los riesgos informáticos, asociados con la información estratégica del país, así, como reforzar la protección de los sistemas informáticos de la Fuerza Pública de Colombia, está a cargo también de las operaciones de inteligencia, de desarrollar capacidades de neutralización y reacción ante incidentes informáticos, que atenten contra la Seguridad y Defensa Nacional, de las auditorias y evaluaciones de seguridad. Este comando Desarrolla labores de prevención, atención, investigación y judicialización de los delitos informáticos en el país, informando en su página web sobre vulnerabilidades cibernéticas. Recibirá y atenderá los lineamientos nacionales en ciberseguridad y trabajará de forma coordinada con el colCERT. También debe ofrecer capacitación especializada en ciberseguridad y ciberdefensa y finalmente asegurar los portales FF.MM.

- ***Ministerio de Tecnologías de la Información y las Telecomunicaciones***

El Ministerio de Tecnologías de la Información y las Comunicaciones se ha propuesto como meta ejecutar o desarrollar la gestión de riesgos de seguridad digital en un gran número de entidades colombianas, independientemente si son públicas o privadas, la intención es que construyan guías que orienten el proceso de gestión de riesgos, en algún nivel de la organización.

A partir de la Ley 1341 de 2009 o ley de TIC, se destina a este Ministerio a plantear, adoptar y fomentar las políticas y proyectos del sector de las tecnologías de la información y las comunicaciones, incrementando el uso de las tecnologías y sus beneficios para todos los habitantes de Colombia, promoviendo el uso efectivo y apropiado de las TIC, con políticas y programas para mejorar la calidad de vida de todos los colombianos y el desarrollo del país. (MinTic, 2020)

- ***Grupo de Respuesta a Emergencias Cibernéticas de Colombia (colCERT)***

Este grupo es el encargado de regular la ciberseguridad y la ciberdefensa nacional, a partir, de la coordinación para resguardar al estado colombiano de acciones que comprometan la integridad nacional. Dentro de sus objetivos está la Coordinación y asesoría a entidades públicas y privadas, ante incidentes informáticos, ofreciendo servicios de prevención frente a posibles amenazas informáticas contra la nación. Es el contacto a nivel internacional, también promueve el desarrollo de capacidades, así como la creación de sectores para la gestión operativa de los incidentes de ciberseguridad, desarrolla procedimientos, y guías de buenas prácticas y recomendaciones de ciberseguridad y ciberdefensa en las infraestructuras de la nación, promueve el sistema de gestión de conocimiento de ciberseguridad y ciberdefensa, encaminado al mejoramiento de estos servicios. Prepara los documentos primarios y secundarios pertinentes, relativos a la seguridad nacional, en el orden externo e interno, así mismo, apoya a los organismos encargados de la investigación y la seguridad del estado para la prevención de amenazas donde se impliquen las tecnologías de la información y las comunicaciones.

Colombia frente a otros países como Chile y España

Colombia, a diferencia de otros países, estipula un rubro específico para la protección del ciberespacio, de igual manera, tiene estructurado lineamientos de estrategia de ciberseguridad y cuenta con la Policía Nacional de seguridad Digital. De igual manera está establecida una estrategia de ciberseguridad planteada en el 2011 en el CONPES 3701 y actualizada en el 2016 con el CONPES 3854.

En el contexto de la Seguridad internacional y como respuesta a las amenazas potenciales a la Seguridad de los Estados, la comunidad internacional ha adoptado políticas orientadas por la Gestión del Riesgo en materia digital y tecnológica, con el propósito de salvaguardar la seguridad del ciberespacio entre otros, el fortalecimiento de la Seguridad Digital pasa por la consolidación de marcos jurídicos supranacionales y un sentido de la Defensa y la Seguridad Nacional. Así mismo, se ha considerado que el desarrollo tecnológico y digital es fundamental para el fortalecimiento de las economías y para la prosperidad social (organización para la cooperación y el desarrollo económicos OCDE,2015, pg.415).

Son varios los avances logrados en el Territorio Colombiano, lo que le permite ser pionero en Ciberseguridad y ciberdefensa en su región, de igual manera se han fortalecido alianzas con países como chile para general mejores estrategias y programas educativos para que todos los actores involucrados en el ciberespacio aprendan a protegerse y navegar con seguridad, política que también es aplicada en España, país en el que el mes de febrero de 2021 se celebró el día de la internet segura. Es así, como podemos mencionar a partir de la aproximación que se ha realizado del estado en Ciberdefensa en Colombia, que el país está trabajando en mejorar las estrategias para

defender su ciberespacio y que este se convierta en una oportunidad de crecimiento económico y social, siendo un país de referencia en su región y ubicándose en el ranking en puestos cerca a países como España, Francia y Dinamarca, gracias al trabajo conjunto entre los sectores público, privado y militar, según el reporte de la UIT.

CONCLUSIONES

Se puede concluir y resaltar la importancia tanto la ciberdefensa como la ciberseguridad, basados en los peligros presentes en el ciberespacio y que pueden afectar a las organizaciones y a nuestra nación. Pero cabe destacar que Colombia gracias a sus políticas de ciberdefensa busca enfrentar los retos a los que se encuentra expuesta la seguridad de la nación y de la sociedad en general.

Es así como se debe tener presente que para poder generar y aplicar estrategias válidas y efectivas es necesario contar tanto con el sector privado, sector público y el sector militar. Es clara la importancia de crear mecanismos e instrumentos además de la educación y divulgación de la información a toda la sociedad en cuanto a las políticas de ciberseguridad y ciberdefensa.

Algunos de los elementos de seguridad digital colombiana, que se deben fortalecer son la investigación, el desarrollo y la innovación de las capacidades operativas, administrativas, humanas y científicas, así como en infraestructura física y tecnológica.

En la actualidad Colombia es seguidor de innovación, pero no generador de la misma, por eso precisa un modelo que le permita generar estrategias y dinámicas acordes a sus recursos económicos limitados.

En cuanto a la actualidad, se puede mencionar que las ciberamenazas son un gran reto y que es necesario continuar capacitándose para estar en la capacidad de anticiparlas, atenderlas y ser resilientes ante ellas.

A nivel mundial, Colombia es un caso representativo en la región, gracias a que ha manteniendo de manera constante y fiable información sobre amenazas y vulnerabilidades que se presentan en el ciberespacio y determinando las acciones que le permiten responder ante estos incidentes, recuperándose de los mismos, en coherencia con las recomendaciones y acciones de organizaciones supranacionales como la ONU, OEA, OCDE y la Comunidad Andina de Naciones.

Otro punto, son los delincuentes informáticos y terroristas que hacen uso del ciberespacio con fines ilícitos, son una amenaza tanto para la infraestructura nacional como para el desarrollo social y económico. Impidiendo el crecimiento de las nuevas Tecnologías de Información y Comunicación, pues los ciudadanos y las entidades gubernamentales no se sienten seguros de emplear el ciberespacio, por lo que es importante continuar fortaleciendo los marcos jurídicos nacionales y las alianzas internacionales para brindar seguridad a todos los actores involucrados.

REFERENCIAS

Becerra, J., Castañeda, C., Bohórquez, A., Páez, R., Baldomero, A., & León, I. (2019). La Seguridad en el Ciberespacio. Un desafío para Colombia. En G. Medina. Escuela Superior de Guerra “General Rafael Reyes Prieto” Recuperado de https://esdeguelibros.edu.co/index.php/editorial/catalog/view/42/48/741-1

Candau, J. (2010). Estrategias nacionales de ciberseguridad. Ciberterrorismo. En Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio (pp. 259-322). Ministerio de Defensa. Recuperado de https:// bit.ly/3dvHjze

colcert, «El Grupo de Respuesta a Emergencias Cibernéticas de Colombia,» (2017) Recuperado de http://www.colcert.gov.co/?q=acerca-de.

colCERT, «GRUPO DE RESPUESTAS A EMERGENCIAS CIBERNETICAS DE COLOMBIA,» Recuperado de http://www.colcert.gov.co/.

Conpes 3854. (2016, 11 de abril). Política Nacional de Seguridad Digital. Departamento Nacional de Planeación. Recuperado de https://bit.ly/3brazVR

Contreras, A. (2019). Gestión de riesgo en seguridad digital en el sector privado y mixto - contexto general. En G. Medina (Ed.), La seguridad en el ciberespacio: un desafío para Colombia (pp. 169-199). Escuela Superior de Guerra “General Rafael Reyes Prieto”. Recuperado de https://doi.org/10.25062/9789585216549.05

CONGRESO, «MinTic,» (29 Julio, 2009). Recuperado de https://www.mintic.gov.co/portal/inicio/3707:Ley-1341-de-2009

Delfín Pozos, F. L., & Acosta Márquez, M. P. (2016). Importancia y análisis del desarrollo empresarial. *Revista científica Pensamiento y gestión*, (40).

Documento Conpes 3701 de 2011 Recuperado de http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

Escuela de Altos Estudios de la Defensa. (2014). Documentos de Seguridad y Defensa 60. Estrategia de la información y seguridad en el ciberespacio. Ministerio de Defensa de España, Secretaría General Técnica. Recuperado de https://bit.ly/2xloBcZ

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 (1.ª ed., pp. 15-28). Plaza y Valdés Editores. Recuperado de https://bit.ly/2UkhhYg

Fernández, J. J. (2018). La hiperglobalización y su impacto. Cuadernos de estrategia, 199, 83-118. Recuperado de https:// dialnet.unirioja.es/servlet/articulo?codigo=6831584

Gaitán, A. (2018). Ciberguerra. La consolidación de un nuevo poder en las relaciones internacionales contemporáneas. Ediciones USTA.

Meridian. (2016). Guía de buenas prácticas de GFCE-MERIDIAN sobreprotección de infraestructuras críticas de la información para responsables de políticas gubernamentales. Holanda: GFCE. Recuperado de https://www.meridianprocess.org/siteassets/web_106011_tno_brochure-good-practice-guide---spaans-def.pdf

Ministerio de Defensa. (2014). Reseña Histórica Recuperado de https://www.mindefensa.gov.co/irj/portal/Mindefensa/contenido?NavigationTarget=navurl://37b759d0e31f2044d8e555a205cf4444.

Ministerio de Defensa. (2016). Plan Estratégico del Sector Defensa y Seguridad. Guía de Planeamiento Estratégico 2016-2018. Recuperado de https://bit.ly/39q6IqY

MinTic, (03 Agosto, 2020) Recuperado de https://www.mintic.gov.co/portal/inicio/Ministerio/Acerca-del-MinTIC/

P.D.L. República, «ACNUR,» Recuperado de https://www.acnur.org/fileadmin/Documentos/BDL/2002/01031.pdf?file=fileadmin/Documentos/BDL/2002/01031

París, S. (2013). Naturaleza humana y conflicto: un estudio desde la filosofía para la paz. Eikasia. Revista de Filosofía, 50(2), 109-116. Recuperado de http://www.revistadefilosofia.org/50-09.pdf

Rudner, M. (2013). Cyber-threats to critical national infrastructure: An intelligence challenge. International Journal of Intelligence and CounterIntelligence, 26(3), 453-481. Recuperado de https://doi.org/10.1080/0885060 7.2013.780552

Sánchez Gómez-Merelo, M. (6 de julio de 2011). Infraestructuras Críticas y Ciberseguridad. Recuperado de https://manuelsanchez.com/2011/07/06/infraestructurascriticas-y-ciberseguridad/

The Economist. (2010, 1.º de julio). Cyberwar. War in the fifth domain. Briefing. Recuperado de https://econ.st/2UFdDHc

Villanueva, J. C. (2015). La ciberdefensa en Colombia. Universidad Piloto de Colombia. Recuperado de http://polux.unipiloto. edu.co:8080/00002646.pdf