Capítulo 5

Economía de defensa, ciberseguridad y ciberdefensa*

DOI: https://doi.org/10.25062/9786287602069.05

Jairo Andres Cáceres García
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: Este capítulo sugiere que la ciberseguridad y la ciberdefensa requieren de asignación de presupuesto y por tanto ser tenido en cuanta para su estudio y análisis desde la visión de estudio que enfrenta la economía de defensa en la actualidad, por tanto sirve como referencia de actualidad y adición a los contenidos de recontextualización de esta especialidad.

Palabras clave: Ciberdefensa, ciberseguridad, economía, defensa, seguridad.

* Capítulo de libro resultado del proyecto de investigación "El presupuesto de la defensa, conceptos generales de economía de defensa", del grupo de investigación Masa Crítica, de la Escuela Superior de Guerra "General Rafael Reyes Prieto", categorizado en A1 por el Ministerio de Ciencia, Tecnología e Innovación (MinCiencias) y registrado con el código COL0123247. Los puntos de vista y los resultados de este capítulo pertenecen al autor y no reflejan necesariamente los de las instituciones participantes.

Jairo Andres Cáceres García
Coronel (R) del Ejército Nacional de Colombia. Especialista en Seguridad y Defensa Nacionales, Escuela Superior de Guerra "General Rafael Reyes Prieto". Profesional en Ciencias Militares, Escuela Miliar de Cadetes "General José María Córdova". Docente e investigador, Escuela Superior de Guerra "General Rafael Reyes Prieto". Orcid: https://orcid.org/0000-0002-6094-3452 - Contacto: jairo.caceres@esdeg.edu.co

Citación APA: Cáceres García, J. A. (2022). Economía de defensa, ciberseguridad y ciberdefensa. En S. Barrios Torres (Ed), *Economía de defensa: conceptos generales, asignación de presupuesto y recontextualización. Reflexiones en el caso de su aplicación en Colombia* (pp. 145-164). Sello Editorial ESDEG. https://doi.org/10.25062/9786287602069.05

**ECONOMÍA DE DEFENSA:
CONCEPTOS GENERALES,
ASIGNACIÓN DE PRESUPUESTO Y RECONTEXTUALIZACIÓN**
REFLEXIONES EN EL CASO DE SU APLICACIÓN EN COLOMBIA
ISBN impreso: 978-628-7602-05-2
ISBN digital: 978-628-7602-06-9
DOI: https://doi.org/10.25062/9786287602069
Colección Seguridad y Defensa
Sello Editorial ESDEG
Escuela Superior de Guerra "General Rafael Reyes prieto"
Bogotá D.C., Colombia
2022

Introducción

Como lo manifestaba el abogado y tratadista austríaco Peter Ferdinand Drucker (1909-2005), "La difusión de la tecnología y la mercantilización de la información transforma el rol de la información en un recurso de igual importancia a la tierra, al trabajo y al capital". Considerado el mayor filósofo de la administración del siglo XX, Drucker afirmaba un hecho innegable: hoy más que nunca, "La información es la joya de la corona de cualquier organización".

Más adelante ahondaremos en esta importante frase del señor Peter Ferdinand Drucker, toda vez que toca la economía, la tecnología y, con la emergencia sanitaria mundial ocasionada por el COVID-19, la virtualización y la transformación digital, que se venía dando lenta y progresivamente en la gran mayoría de nuestras actividades cotidianas, trabajo, academia, Gobierno, comercio y atención médica, por mencionar algunas. Hoy la ciudadanía puede acceder a un significativo volumen de información a un clic de distancia, sin importar las fronteras.

Pero no es solo el flujo de información el que lidera a una sociedad cada vez más globalizada, más tecnológica y ciber dependiente; hay que considerar la transformación digital que han sufrido los bienes y los servicios que ahora se apoyan en la tecnología por intermedio del ciberespacio, y con más fuerza luego del COVID-19.

La economía de defensa como una rama especializada de la economía que propende el estudio del gasto del presupuesto estatal y sus efectos económicos colaterales de los gastos en materia de defensa, asimismo estudia, la interrelación del sector público en este caso el defensa, para el presente escrito que nos ocupa el Colombiano con el Ministerio de Defensa Nacional, y su relación con el sistema económico privado, así como las necesidades en cada una de

las Fuerzas Armadas (Ejército, Armada, Fuerza Aérea y la Policía Nacional). La ciberdefensa y la ciberseguridad hoy día, son un aspecto fundamentalmente importante en la seguridad y defensa Nacional de los países y Colombia no es ajena a esa realidad.

El presente capítulo tiene como objetivo final incentivar al estudio de la economía de defensa y su incidencia en la ciberdefensa y ciberseguridad como nuevas amenazas consagradas en la carta de las Américas, OEA en México, 2011 dentro del contexto de la seguridad multidimensional, como en un nuevo escenario de interrelación social, cultural, económica, y presentando una reflexión sobre el ciberespacio como un nuevo y moderno ecosistema artificial donde confluyen las relaciones humanas. Este ecosistema pone de presente grandes problemas como en cualquier escenario real material y que afectan al ser desde el área de la seguridad y la defensa. Amenazas como los ciberataques, cibercrimen, ciberterrorismo entre otros varios aspectos de las ciberamenazas que reflejan una semejanza entre otros dominios o dimensiones de la guerra actuales, tierra, mar, aire y espacio, pero el ciberespacio hasta el momento no puede ser reguladas.

Los avances tecnológicos y los temas que tienen que ver con estos, hacen cada vez más difícil tener una seguridad y defensa nacional aprueba de todas la amenazas tradicionales y las nuevas amenazas como la ciberguerra. Colombia, desde el 2011, fecha en la cual el Gobierno nacional emitió el primer documento del Consejo Nacional de Política Económica y Social (Conpes) 3701, que se titula *Lineamientos de la política de ciberseguridad y ciberdefensa para Colombia*, que cuyo objetivo era sentar herramientas, normativas, organizacionales e institucionales que le permitan minimizar los riesgos y enfrentar las ciberamenazas, las cuales, en el actual momento que vive Colombia y en mundo entero, por la emergencia sanitaria ocasionada por el COVID19, se han incrementado hasta en un 150 % junto con los ciberdelitos, según información suministrada por el Centro Cibernético Policial de Colombia.

Colombia, en enero del 2012, emitió la Política Nacional de Ciberseguridad y Ciberdefensa, que ha venido implementando, actualizando y monitoreando de manera efectiva. Sin embargo, ningún plan de gobierno se puede llevar a cabo sin el adecuado y siempre limitado presupuesto asignado por el mismo Gobierno en su plan de desarrollo; los países siempre tienen necesidades ilimitadas frente a disponibilidad presupuestal absolutamente limitada.

La ciberseguridad y la ciberdefensa en Colombia

La década del 2020 al 2030 quedará marcada de forma imborrable por los efectos de la emergencia sanitaria mundial a causa de la pandemia del covid-19, que ha causado cientos de miles de muertos y ha generado una impensable crisis económica mundial. Por ende, las amenazas mutaron, y la ciberseguridad y la ciberdefensa cobran más vigencia y necesidad en la actual situación en la cual estamos viviendo.

Como ya lo he mencionado los teatros de operaciones tradicionales donde se desarrollan los conflictos armados desde la antigüedad hasta nuestros días, son tierra, mar y aire, e incluso el Instituto Español de Estudios Geoestratégicos (2011) hace referencia al espacio. Con base en los diferentes incidentes en materia de ciberdefensa y ciberseguridad que se han presentado en últimos años, como por ejemplo podemos citar: como por el ejemplo el caso mundialmente conocido "WikiLeaks", cuando la exsoldado, Chelsea Elizabeth Manning, analista de inteligencia del Ejército de los Estados Unidos de Norte América, colocó en calzas prietas, al Gobierno de los Estados Unidos, por la microfiltración de más de 700.000 documentos confidenciales, por lo cual está condenada a 35 años de cárcel, asimismo la fuga de información por parte de Edward Snowden (BBC Mundo, 2013), ex funcionario de la CIA, entre otros incidentes por no citar otros países, que más adelante haré referencia, nos confirma que estamos frente a un nuevo campo de batalla; que tiene graves consecuencias y efectos colaterales para un país en materia de seguridad y defensa, en especial en el caso colombiano.

> Las tecnologías de la información transforman nuestra manera de pensar y actuar en cualquier aspecto de nuestras vidas, introduciendo importantes cambios estructurales, al permitirnos modelar objetos de todo tipo en forma de información, permitiendo de este modo su manipulación por medios electrónicos. (Unión Internacional de Telecomunicaciones, 2007, p. 3)

Con base en lo anteriormente expuesto, es así que el mundo es cada vez más ciber dependiente a la tecnología, más específicamente a la internet, lo cual, hace a los Estados estén más vulnerables a un ciberataque, que puede poner en jaque estructuras críticas, la cual podemos definir: "Instalaciones, redes, servicios, equipos físicos y TI cuya *interrupción* o *destrucción* tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en

el eficaz funcionamiento de las instituciones del Estado y de las Administración Públicas", de un Estado, ya sea en su parte militar y no menos importante, infraestructura que puede afectar directamente a la población civil sin necesidad de disparar un solo cartucho.

El objetivo principal de este trabajo es sensibilizar como la ciberseguridad y la ciberdefensa permiten evidenciar que en el ciberespacio existen amenazas latentes a la seguridad de un Estado o una organización. A lo largo del mismo, se busca ofrecer una explicación sobre estos términos, y que sea lo más sencillo posible. Se ha realizado una compilación de varios documentos que hablan sobre el tema. Para ello, se dividirá este trabajo en tres grandes capitulo. El primero trata sobre la terminología básica sobre ciberseguridad, ciberdefensa, ciber guerreros, y los distintos métodos en que se utiliza la red, ya sea para atacar a un enemigo o proteger información valiosa. Será una especie de estado del arte sobre el tema de ciberseguridad y ciberdefensa. Y explicando de la manera más simple el funcionamiento de sistemas que son útiles para acceder a redes privadas y realizar ataques informáticos.

El nuevo campo de batalla, quinto dominio, dimensión de la guerra o el quinto teatro de operaciones, como se conoce o se ha venido denominando al ciberespacio, donde se desarrollarán las guerras del futuro, aunque yo prefiero referirme las guerras del presente, pues ya hay evidencias tangibles de ciber ataques que han sido considerados operaciones militares dentro de un marco de una guerra cibernética, como sucedió en Georgia en mayo del año 2007, atribuido a Rusia, donde primero atacó la fuerza aérea Rusa, luego de efectuar fuegos de ablandamiento, ingresó la infantería con apoyo de tanques de guerra y vehículos blindados, para finalmente entrar los ciber soldados con ciberataques entraron en la agresión con un grupo de hackers, bloqueando las comunicaciones entre otros objetivos y en Estonia en el año 2007, años más tarde en el año 2009, Rusia se atribuyó el ciberataque, como resultado de esta agresión cibernética, fue la creación del Centro de Excelencia de Ciberdefensa Cooperativa de la Organización del Tratado del Atlántico Norte (OTAN), ubicado en la ciudad de Tallin, Estonia, esta pequeña República Báltica salto de ser un satélite Ruso a convertirse en la meca de la tecnología de punta en Europa, del cómo es una realidad ante la cual, Colombia no es indiferente a oeste nuevo escenario de guerra. Actualmente, cada Estado debe establecerse como objetivo principal definir cómo hacer frente a las amenazas que atentan contra su seguridad y la defensa en el campo cibernético.

Primero que todo debemos ver algunas y definiciones de ciberseguridad y ciberdefensa, para tener claridad en el rol que cada una de estas áreas tiene que ver con la seguridad y defensa en Colombia en especial.

Algunas definiciones de ciberseguridad

- *Consejo Nacional de Política Económica y Social de Colombia* (Conpes, 3701 del 14 de julio 2011): capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética.
- *Information System Audit and Control Association* (ISACA, asociación internacional que promueve y apoya el desarrollo de metodologías y certificaciones para la realización de actividades de auditoría y control en sistemas de información): protección de los activos de información a través del tratamiento de las diversas amenazas que ponen en riesgo la información que es procesada almacenada y transportada por los sistemas de información que se encuentran interconectados
- *ISO/IEC2732:2012* (norma estándar de ciberseguridad del 2012, por la Organización Internacional de Normalización (ISO), que establece orientaciones para reforzar la ciberseguridad en las empresas): preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio, definiendo a su vez ciberespacio como el entorno complejo resultante de la interacción de personas, *software*, y servicios de internet, a través de dispositivos tecnológicos y redes interconectadas a él, que no existen en ninguna forma física.
- *Centro Conjunto de Desarrollo de Conceptos, Gobierno de España* (CCDC): campos operativos de la ciberdefensa, con una terminología común, una definición clara de sus capacidades, la necesaria coordinación con los actores que operan en el ciberespacio y en el espectro electromagnético, las operaciones militares en el ámbito del ciberespacio y su integración con el resto de capacidades operativas, así como su estructura de Mando y Control (C2), el marco legal de actuación y la imprescindible integración con el resto de actores civiles y militares en los planos nacional e internacional, todo ello para orientar el desarrollo de las capacidades necesarias para enfrentar la amenaza de hoy y del mañana.

Definición de ciberdefensa

- *Consejo Nacional de Política Económica y Social de Colombia* (Conpes 3701 del 14 de julio 2011): capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernetica que afecte la soberanía nacional.
- *Estado Mayor de Defensa* (España): conjunto de capacidades de defensa, explotación y ataque que permiten llevar a cabo operaciones en el ciberespacio, con la finalidad de preservar o ganar la libertad de acción en el ciberespacio de interés militar, impedir o dificultar su uso por parte del adversario, y contribuir a alcanzar la superioridad en el enfrentamiento en el resto de los ámbitos físicos y cognitivo.
- *Ministerio de Defensa* (Argentina): es el conjunto de acciones y/u operaciones activas o pasivas desarrolladas en el ámbito de las redes, sistemas, equipos, enlaces y personal de los recursos informáticos y teleinformáticas de la defensa a fin de asegurar el cumplimiento de las misiones o servicios.

Apoyándonos en las anteriores definiciones podemos evidenciar la importancia de la ciberseguridad y la ciberdefensa, en el nuevo escenario de riesgos y amenazas que se ha conformado en la internet, la ciberseguridad y la ciberdefensa son herramientas fundamentales, para mantener el orden interno y la soberana en el Ciber espacio, con toda la complejidad y desafíos que esto con lleva.

Hoy, en un Estado consiente de las ciberamenazas en el interior y del exterior al país, considera funcionarios entrenados y formados en ciberseguridad, pues han pasado de ser una opción a convertirse en funcionarios estratégicos y fundamentales. Lo que vemos diariamente a las noticias de incidentes de ciberseguridad y en situaciones más extremos los ataques cibernéticos, que en muchos casos pueden ir más allá de lo que podemos imaginarnos y colocar situación de riesgo la integridad de un Estado, de sus ciudadanos, y por ende en general la estabilidad de los Estados. Así podemos decir que este enemigo virtual solo se debe y se puede combatir con ciberdefensa.

La evolución de las tecnologías de la información y las comunicaciones ha provocado un cambio de paradigmas que exige la adopción de procedimientos especializados para neutralizar y controlar las amenazas cibernéticas. La ciberdefensa, además de prevenir los ataques como hace la ciberseguridad, da respuesta a los mismos con nuevos ataques con fin de salvaguardar la seguridad.

complementando lo comentado, los países industrializados y que están a la vanguardia en tecnología, como Estados Unidos, Rusia, China entre otros, buscan ostentar el dominio del ciberespacio, tanto para el ataque como para la defensa, teniendo en cuenta que el factor tiempo en el ciberespacio da un intervalo desde un par de minutos hasta milésimas de segundo para realizar un ataque. Caro (2011) ha clasificado los tipos de atacantes que se encuentran en el ciberespacio:

- Atacantes patrocinados por Estados.
- Servicios de Inteligencia y Contrainteligencia.
- Terrorismo, extremismo político e ideológico.
- Ataques de delincuencia organizada.
- Ataques de perfil bajo.

¿Cómo está Colombia en materia de ciberseguridad y ciberdefensa?

Para Colombia, desde el 2011 la ciberdefensa y la ciberseguridad han sido una prioridad. Páginas oficiales del Gobierno como la página de la Presidencia de la República, Gobierno en Línea, Ministerio del Interior y de Justicia, Defensa y Cultura fueron objetivo de varios ataques informáticos que las dejaron fuera de servicio por varias horas (Departamento Nacional de Planeación, 2011, P.9). Del mismo modo, la Policía Nacional ha reportado casos como robo de identidad, robo a cuentas bancarias que a 2009 llegaban a 50.000.000 millones de dólares (Ministerio de Defensa, 2009, p.1). Del mismo modo intento atentarse contra la infraestructura crítica de la nación, pero estos fueron repelidos. Sin embargo, los organismos de seguridad colombianos son conscientes de que el nivel de sofisticación de los ataques va en aumento y de que es necesario tener en cuenta ello para evitar problemas en el futuro.

Un caso para resaltar fue el ocurrido durante el primer semestre de 2011, cuando el grupo "hacktivista" autodenominado Anonymous atacó a los portales de la Presidencia de la República, el Senado de la República, Gobierno en Línea y de los Ministerios del Interior y Justicia, Cultura y Defensa, dejando fuera de servicio sus páginas web por varias horas. Este ataque se dio en protesta al Proyecto de Ley "por el cual se regula la responsabilidad por las infracciones al derecho de autor y los derechos conexos en Internet". Este grupo ha atacado indistintamente entidades públicas y privadas, entre las que se cuentan PayPal,

el banco suizo Post Finance, MasterCard, Visa y páginas web del Gobierno Suizo. (Información tomada del documento CONPES 3701).

En 2011, el Gobierno Colombiano elaboró el CONPES 3701 (Consejo Nacional de Política Economía Social), máximo organismo de coordinación de la política económica en Colombia. No dicta decretos, sino que da la línea y orientación de la política macro sobre un tema específico, en este caso la ciberseguridad y la ciberdefensa.

El Conpes está presidido por el primer mandatario del país y la secretaría técnica la ejerce el jefe del Departamento Nacional de Planeación, que elabora los documentos para ser tratados en cada una de las sesiones.

Fue así que nació el CONPES 3701 el 14 de julio del 2011, que trata sobre los "*Lineamientos de política para ciberseguridad y ciberdefensa de Colombia*", el cual busca generar lineamientos de política en ciberseguridad y ciberdefensa tendiente a desarrollar una estrategia nacional para contrarrestar el crecimiento de las amenazas informáticas que afectan significativamente al país. Asimismo, recopila antecedentes nacionales e internacionales, así como la normatividad del país en torno al tema.

En cumplimiento del CONPES 3701, Colombia empezó a estructurar una ciberdefensa sólida, innovadora, creativa y siempre actualizada, no solo para prevenir ataques informáticos contra instituciones estatales, sino para poder estructurar una ciberdefensa activa, algo que se debe hacer para la defensa del TI gubernamental. La ciberdefensa que se implemente debe ser proactiva, dinámica y al día con las amenazas que puedan llegar. Debe ser un laboratorio con un radar digital que permita ver en forma oportuna las posibles amenazas.

Dentro de los aspectos más resaltantes del Conpes 3701, está la conformación de la Comisión Intersectorial, con representación del Ministerio de Defensa Nacional con el ColCERT, el Comando Conjunto Cibernético (CCOC) en el Comando general de las FFMM y finalmente el Centro Cibernético Policial (CCP), a cargo de la Policía Nacional (figura 1).

Figura 1. *Comisión intersectorial*

Fuente: Conpes 3701 (2011).

El *grupo de respuesta a emergencias cibernéticas de Colombia* (ColCERT) es el encargado de coordinar a escala nacional los aspectos de ciberseguridad y ciberdefensa. El *Comando Conjunto Cibernético de las Fuerzas Militares* tiene la responsabilidad de salvaguardar los intereses nacionales en el ciberespacio y la soberanía, es decir, es el responsable de la ciberdefensa nacional. El *Centro Cibernético Policial* está a cargo de la prevención e investigación y apoya la judicialización de los delitos informáticos, protección a los ciudadanos con la ciberseguridad. Para ello, contará con un comando de Atención Inmediata Virtual (CAI Virtual), para recibir las denuncias de los ciudadanos.

La economía de defensa: su importancia en la ciberseguridad y la ciberdefensa

La economía de defensa, como una rama especializada de la economía que propende por el estudio del gasto del presupuesto estatal en seguridad y defensa con sus efectos económicos colaterales de los gastos en materia de defensa, analiza, además, la interrelación del sector público con el sector privado. Para

el contexto del presente apartado, se identifica como la relación entre la sociedad colombiana y el Ministerio de Defensa Nacional, y la relación con el sistema económico nacional, estableciendo las necesidades en cada una de las Fuerzas Armadas (Ejército, Armada, Fuerza Aérea y Policía Nacional).

Con relación a dichas necesidades, la ciberdefensa y la ciberseguridad hoy día son un aspecto fundamental en la seguridad y la defensa nacional de los países, y Colombia no es ajena a esa realidad. Al atacar infraestructuras críticas no solo se pone a prueba el mando militar u organizaciones estatales, las instituciones de carácter privado también son afectadas, como el sector financiero con los bancos, proveedores de servicios públicos y transportes, entre otros. Esto quiere decir, que la seguridad y defensa del ciberespacio tiene implicaciones civiles y económicas y esto lo convierte en un objetivo estratégico de la seguridad nacional, por lo tanto, los hombres y mujeres que ostentan esta responsabilidad deben estar intelectualmente preparados para asumir el compromiso de la defensa de un país en el teatro de operaciones del ciberespacio.

Para ambientar el contexto del tema que nos ocupa, en Latam este el balance general:

Según el informe de seguridad para América Latina de la firma Frost And Sullivan, habrá un alto crecimiento de la demanda de servicios relacionados con la seguridad de la información en más de 455,9 millones de dólares. Esto quiere decir que para el 2021, habrá un crecimiento de 936,7 millones de dólares en el campo de la seguridad de la información, cifra que representa un alza del 15 %.

Por su parte, Fortiguard destacó que herramientas para vulnerar a bancos en Chile y México impactaron a Colombia entre julio y agosto de 2018. Como es una amenaza real se requiere mayor inversión en esta área de la ciberseguridad. Toda vez que las empresas de Colombia tan solo invierten el 20 % del total del presupuesto de campo. En Colombia, como en Latinoamérica, los ciberataques están creciendo a ritmos de doble dígito, y los sectores que más lo sienten son la banca y la industria financiera", aseguró el country mánager de Fortinet para Colombia, Juan Carlos Puentes (*La República*, 2020).

Como estamos entrando en el tema de economía de defensa, recordemos que es una rama especializada de la economía que promueve el estudio del gasto del presupuesto estatal y sus efectos económicos colaterales de los gastos en materia de defensa, por lo cual es muy importante que tengamos clara la definición y el concepto de *transformación digital*, toda vez que esta tiene que ver

mucho con el desarrollo de la economía, el empleo y por ende el crecimiento en producción de un país, hoy más que nunca por la emergencia mundial sanitaria ocasionada por el COVID-19 en nuestro caso de Colombia, aquí la definición: "Integración de nuevas tecnologías en una organización con el objetivo de optimizar sus procesos, aumentar las ventas y la rentabilidad, ser más competitivo y ofrecer mayor valor agregado a sus clientes".

Con base en la definición, nos deja entrever dos aspectos clave: 1) la *información*, considerada el activo más importante de cualquier organización, pública o privada, incluso de manera personal; y 2) la *tecnología*, como resultado entre la ciencia e ingeniería que, aplicadas a través de distintos instrumentos y métodos, y la *tecnología digital* es entonces la aplicación de métodos para desarrollar sistemas que se ven expresados en números o datos y que permiten automatizar ciertos procesos (blog.enzymeadvicsinggroup.com). La tecnología como viene evolucionando nos permite planificar nuestra evolución a futuro, ya que es un recurso que promueve soluciones inteligentes a las necesidades de la humanidad.

Con base a Gartner (empresa consultora que ofrece una herramienta para saber en qué punto de innovación y nivel de desarrollo están las empresas dedicadas a la tecnología en el mercado global, convirtiéndose en un referente mundial tanto para medios especializados y marca las tendencias del mercado) 20,4 mil millones será el total de dispositivos tecnológicos interconectados entre sí, mediante el IoT (el internet de las cosas) en todo el planeta para el 2020. Lo anterior, para referenciar la importancia de la tecnología digital y la información. Es así como es fundamentalmente importante que se asigne presupuesto significativo al sector de defensa como se vio anteriormente para cumplir con la misión asignada en defender a Colombia en ciberdefensa y ciberseguridad, teniendo en cuenta, la premisa que su ciberseguridad y ciberdefensa será directamente proporcional al presupuesto que usted invierta… Colombia desde el año 2011 fecha en la cual se promulgo el primer CONPES 3701, siempre ha tenido, a mi modo de ver una política de Estado más que del Gobierno de turno, es así como que se han emitido varios Conpes.

Conclusiones sobre la economía de defensa: ciberseguridad y ciberdefensa en Colombia (2011-2019)

A modo de conclusión, es trascendental aclarar que el gasto público, particularmente en los rubros de la ciberseguridad y la ciberdefensa para el intervalo anual de 2011 a 2019, puede ser identificado a lo largo y ancho de los documentos públicos Conpes 3701 y el Conpes 3854. Además de exponer el "paso a paso" de la construcción del presupuesto, en tales textos se presenta y describe lo importante que es para las instituciones colombianas el hecho de estructurar e implementar una política o estrategia de seguridad y defensa nacional para abordar las amenazas que emergen esencialmente en el escenario cibernético y/o ciberespacial. Haciendo énfasis en cada uno de los documentos citados, es debido aclarar que, el Conpes 3701 busca explicar y mencionar los lineamientos de la Política de Ciberseguridad y Ciberdefensa (PCC) junto con su presupuesto, para los años 2011-2014.

De manera posterior, el Conpes 3854 esclarece detalladamente los parámetros y principios de la Política de Seguridad Digital, haciendo hincapié en el presupuesto y funciones del Estado con respecto a la ciberseguridad y ciberdefensa para los años 2016-2019. Es preponderante mencionar que, el Conpes 3854 se entiende como la continuación de lo que se proyecta e implementa en el Conpes 3701, dado que ambas directrices apuntan hacia el fortalecimiento institucional en contra de los mismos fenómenos y amenazas. Asimismo, cada propuesta indica de manera clara y concisa el contexto, las debilidades, objetivos y recomendaciones a seguir para cada una de las instituciones en los intervalos temporales que se evalúan en cada uno de los Conpes mencionados, 2011-2014 y 2016-2019, respectivamente.

El Conpes 3701, es un texto público aprobado en Bogotá el 14 de julio de 2011, el cual fue redactado y diseñado en el seno del Departamento Nacional de Planeación (DNP) con la colaboración de tres ministerios (Defensa Nacional, Relaciones Exteriores, y de Interior y Justicia), la Fiscalía General (FG) y el Departamento Administrativo de Seguridad (DAS). De igual forma, el Conpes 3701 busca; "generar lineamientos de política en ciberseguridad y ciberdefensa orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país" (2011, p. 2). El Conpes 3701 aborda el problema fundamental que se describe en el artículo

como; "la capacidad actual del Estado para enfrentar las amenazas cibernéticas presenta debilidades y no existe una estrategia nacional al respecto" (2011, p. 2).

Complementando lo anterior, el Conpes 3701 hace referencia a que el presupuesto y/o gasto público para todas las actividades que giran en torno a la ciberseguridad y la ciberdefensa debió ser de 1.428.444.328 de pesos para el 2011, 5.400.000.000 de pesos para el 2012, 5.000.000.000 de pesos para el 2013, y 4.600.000.000 de pesos para 2014. Gran parte de las cantidades mencionadas se destinaron para diseñar, fortalecer e implementar las capacidades intelectuales, técnicas y académicas de la comisión intersectorial de ciberseguridad y ciberdefensa. En tal comisión se destacan esencialmente tres entidades principales, entre las cuales se encuentra el Comando Conjunto Cibernético (CCOC); equipo encargado de la defensa del país en el ciberespacio, también está el Centro Cibernético Policial (CCP); organización responsable de la seguridad ciudadana en el ciberespacio, y finalmente está el ColCERT; entidad coordinadora nacional en aspectos de seguridad informática (DNP, 2011).

A posteriori, luego de presentar el problema central, el objetivo general y las cifras de los presupuestos; el Conpes 3701 plantea en su desenlace una lista de recomendaciones y sugerencias para los tomadores de decisiones y sus respectivos ministerios y oficinas enunciando que: 1) se debe implementar la institucionalidad apropiada, 2) se tiene que brindar capacitación especializada en seguridad de la información y ampliar las líneas de investigación en ciberseguridad y ciberdefensa, y, finalmente, 3) es menester fortalecer la legislación y la cooperación internacional en materia de ciberseguridad y ciberdefensa (DNP, 2011).

Para el presupuesto de ciberseguridad para el 2015, periodo que se omite tanto en el Conpes 3701 como en el Conpes 3854, se firmó un decreto el 26 de diciembre de 2014 en dónde el Ministerio de Hacienda y Crédito Público destaca que para ciberseguridad se llevaron a cabo dos inversiones importantes. Comenzando por un gasto de 2.000.000.000 de pesos para la implementación de un comando conjunto para la protección contra ataques cibernéticos en el territorio, y una suma de 1.250.000.000 de pesos que se destinó para la implementación de una unidad de ciberdefensa para el Ejército Nacional. Contemplando el presupuesto que muestra el Decreto 2710 de 2014, el gasto en ciberseguridad tuvo que alcanzar la suma aproximada de 3.250.000.000 de pesos para el 2015, si se suman los rubros que abordan el tema de la ciberseguridad y ciberdefensa en la sección de Defensa Nacional (Ministerio de Hacienda y Crédito Público, 2014).

Desde otra perspectiva, y con la finalidad de darle una continuidad prudente y acertada a lo planteado en el Conpes 370, el Conpes 3854 (sobre la Política Nacional de Seguridad Digital) se firma y aprueba en Bogotá el 11 de abril de 2016, con la participación de entidades públicas como la Dirección Nacional de Inteligencia (DNI), el Ministerio de Defensa, el Ministerio de Tecnologías de la Información y Comunicaciones y por supuesto, el DNP. De igual manera, en su resumen ejecutivo, se aclara con brevedad el contexto sociopolítico en el que se implementa el Conpes 3854 y los desafíos que abordará, espacio del texto en el que se expone que; "el creciente uso del entorno digital en Colombia para desarrollar actividades económicas y sociales acarrea incertidumbres y riesgos inherentes de seguridad digital que deben ser gestionados permanentemente. No hacerlo, puede resultar en la materialización de amenazas o ataques cibernéticos, generando efectos no deseados de tipo económico o social para el país, y afectando la integridad de los ciudadanos en este entorno" (DNP, 2016, p. 3).

Teniendo en cuenta lo anterior, el Conpes 3854 presenta el gasto ideal o presupuesto (financiamiento estimado) de lo que las entidades públicas tuvieron que haber invertido en materia de ciberseguridad y ciberdefensa entre 2016 y 2019. Contemplando lo dicho, para 2016 se tuvieron que haber destinado 23.443.000.000 de pesos, mientras que para 2017 se tenían que invertir 21.692.000.000 de pesos, para 2018, 21.483.000.000 de pesos y para 2019 se tuvieron que emplear 18.452.000.000 de pesos para este rubro (DNP, 2016). En resumidas cuentas, el Conpes 3854 muestra que, de 2016 hasta 2019 tuvo que haber un gasto aproximado de 85.070.000.000 pesos colombianos distribuidos en actividades realizadas respectivamente en seis entidades públicas.

Es trascendental aclarar que, para los proyectos que se exponen en el Conpes 3854, existe la participación del Ministerio de Educación, entidad que no participó directamente en la implementación de los programas del Conpes 3701, pero que cumple un rol preponderante en el ámbito de la capacitación de personal y en el contexto netamente investigativo. Pues por medio de las pesquisas se analizan y estudian diversos fenómenos desde distintas aristas, y finalmente se constituyen proyectos innovadores para encarar desafíos en el mediano y largo plazo. Paralelamente, a la iniciativa del Conpes 3854 también se sumó el Ministerio de Justicia y del Derecho, institución que brindó apoyo en toda la implementación y la arquitectura legal de cada objetivo y proyecto.

En el Conpes 3854 se exponen algunas cifras interesantes concentrándose en el cambio de las dinámicas y actividades cibernéticas que se llevaron a cabo

en periodos directamente anteriores (2010-2015). Por ejemplo, se hace énfasis en que; entre 2010 y 2014 el número de hogares con conexión a internet aumento de 19,02 % al 38 00 %, lo cual indica que el 38,00 % de los hogares colombianos contaban con acceso a internet para 2014, mientras que en 2010 era solo de un casi 20,00 %.

Además, el documento público enuncia que para 2015, el 42,00 % de los delitos cibernéticos afectaron a la "ciudadanía", mientras que el 23,09 % de delitos fueron en contra del Gobierno, siendo el segundo sector más afectado en términos de ciberseguridad, mientras que el menos afectado fue el de la salud, el cual solo sufrió el 0,10 % de los casos de ciberdelito. En el transcurso del texto se emplean diagramas y tablas que evidencian que entre 2012 y 2015 la mayor cantidad de denuncias por "ciberdelitos" se realizaron por la pornografía infantil (11.506 casos), seguida por el maltrato, trabajo y abuso infantil (3.441 casos). Al final, el total de denuncias en el intervalo de tiempo dicho fue de 21.272 casos.

La continuación y resultados de los proyectos establecidos en el Conpes 3854 se enuncian y analizan con lujo de detalles en el Conpes 3995, documento que se conoce como "Política Nacional de Confianza y Seguridad Digital" (firmado y aprobado en julio de 2020 en Bogotá), donde se muestran los programas a mediano plazo en temas de ciberseguridad y ciberdefensa desde el 2020 hasta el 2022. El documento hace una contextualización completa sobre el entorno de la seguridad en el ciberespacio y expone su objetivo primordial y general, el cual se enfoca en; "establecer medidas para desarrollar la confianza digital a través de la mejora la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías" (DNP, 2020, p. 27).

Finalmente, se espera que entre 2020 y 2022 se haga una inversión de al menos 8.342.000.000 de pesos en el sector de ciberseguridad, tal gasto será evaluado en cinco instantes o cortes diferentes, los cuales se llevarán a cabo el 31 de diciembre (2020), 30 de junio (2021), 31 de diciembre (2021), 30 de junio (2020), y el 31 de diciembre (2022). Para cerrar esta sección de conclusiones, es de suma trascendencia determinar que, todos los datos citados y encontrados en cada uno de los documentos (Conpes 3701, 3854 y 3995) son aproximaciones muy fidedignas sobre el gasto real que se ha hecho en cada uno de los sectores, en este caso el de la ciberseguridad en Colombia. No obstante, identificar

el número estrictamente exacto del gasto en ciberseguridad de 2011 a 2019 es una tarea casi imposible. Dado que, cada fuente oficial tiene diferentes maneras de interpretar y mostrar datos, algunas veces incluyendo o excluyendo factores de alta o baja importancia en cada uno de los estados financieros que son autorizados para ser mostrados al público.

Con base en lo expuesto, se puede evidenciar la importancia que Colombia le ha dado a la política de ciberdefensa y ciberseguridad, con la promulgación de los siguientes CONPES:

- CONPES, 3701, julio 2011, *Lineamientos y políticas ciberseguridad y ciberdefensa*.
- CONPES, 3854, abril 2016, *Políticas nacional de seguridad digital*.
- CONPES, 3975, diciembre 2019, *Política nacional para la transferencia digital e inteligencia artificial*.
- CONPES, 3995, julio 2020, *Confianza y seguridad digital*.
- CONPES, 3988, marzo 2020, *Tecnología para aprender*.

Así como considera los diferentes rubros tradicionales contemplados para la seguridad y defensa nacional de Colombia, la economía de defensa debe incluir la ciberdefensa y ciberseguridad, pues ya ha tenido la asignación de presupuesto importante para iniciar su implementación de las organizaciones que integran la comisión intersectorial dispuestas en el CONPES 3701, ya comentadas.

La ciberdefensa y la ciberseguridad de Colombia y de cualquier otro país es directamente proporcional al presupuesto invertido en estos dos campos claves para la seguridad y defensa de las naciones.

Se debe mantener un balance adecuado y prudente, entre las *políticas y procedimientos, el talento humano y la tecnología*. No asignar el presupuesto solo para adquirir Tecnología, como suele suceder muchas veces sin estudio previo de conveniencia técnica, y solo adquirirla porque está de moda… Las políticas y procedimientos deben ser claras y específicas para tener definidas y explicadas las reglas y poder tomar acciones disciplinarias o penales si hubiera la necesidad, contra un funcionario, evitando así la impunidad. Con respecto al talento o recurso humano, debemos capacitarlo especialmente en la concientización o concienciación en ciberseguridad. Nada se gana con tener los mejores equipos en tecnología de punta, definidas adecuadamente las políticas y procedimientos, y no tener al recurso humano, sensibilizado, concientizado de la importancia de la ciberseguridad para seguridad y defensa nacional.

Referencias

Assolini. F. (2018). *Analista senior de seguridad en Kaspersky Lab. Resultados presentados en la Octava Cumbre de Analistas de Seguridad para América Latina*, Ciudad de Panamá. https://latam.kaspersky.com/blog/kaspersky-lab-registra-un-alza-de-60-en-ataques-ciberneticos-en-america-latina/13266/

Comando General de las Fuerzas Armadas. (2020). *Colombia Military Strength*. Comando General de las Fuerzas Armadas. https://www.globalfirepower.com/country-military-strength-detail.php?country_id=colombia

Comando General de las Fuerzas Armadas. (2020). *Presupuesto general para la vigencia fiscal*. Comando General de las Fuerzas Armadas. https://www.cgfm.mil.co/es/transparencia-y-acceso-la-informacion-publica/presupuesto

Corletti Estrada, A. (2017). *Ciberseguridad: una estrategia informático/militar*. DarFe, Learning Consulting. http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/2018/Libro-Ciberseguridad_A.Corletti_nov2017.pd.pdf

Decreto 2710 de 2014. Por el cual se liquida el Presupuesto General de la Nación para la vigencia fiscal de 2015, se detallan las apropiaciones y se clasifican y definen los gastos. Diciembre 26 de 2014. DO. N.º 49376.

Departamento Nacional de Planeación. (2011). *Conpes 3701: Lineamientos de política para la ciberseguridad y la ciberdefensa*. Departamento Nacional de Planeación. https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

Departamento Nacional de Planeación. (2016). *Conpes 3854: Política nacional de confianza y seguridad digital*. Departamento Nacional de Planeación. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Departamento Nacional de Planeación. (2020). *Conpes 3995: Política nacional de confianza y seguridad digital*. Departamento Nacional de Planeación. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

Dinero. (2019). Guía de ciberseguridad para el 2019. *Dinero*. https://www.dinero.com/tecnologia/articulo/ciberseguridad-en-el-2019-en-colombia/265858

Dinero. (2020). Ciberataques en América Latina: ¿están expuestas las empresas colombianas? *Dinero*. https://www.dinero.com/tecnologia/articulo/que-tan-seguras-estan-las-empresas-colombianas-ante-ciberataques/296519

Infodefensa. (2020). Colombia presupuesta 10.400 millones de dólares para la defensa en 2021. *Infodefensa*. https://www.infodefensa.com/latam/2020/09/22/noticia-colombia-presupuesta-10400-millones-dolares-defensa.html

Molano, A. (2014, 1.o de octubre). Internet de las cosas: concepto y ecosistema. *Colombia Digital*. https://colombiadigital.net/actualidad/articulos-informativos/item/7821-Internet-de-las-cosas-concepto-y-ecosistema.html

Montes, S. (2018, 8 de septiembre). Empresas colombianas solo invierten 20 % de presupuesto en ciberseguridad. *La República*. https://www.larepublica.co/internet-economy/empresas-colombianas-solo-invierten-20-de-presupuesto-en-ciberseguridad-2768645

Naciones Unidas, Oficina de Asuntos de Desarme. (2018). *Los avances en la informatización y las telecomunicaciones en el contexto de la seguridad internacional*. Oficina de Asuntos de Desarme de las Naciones Unidas. https://www.un.org/disarmament/es/los-avances-en-la-informatizacion-y-las-telecomunicaciones-en-el-contexto-de-la-seguridad-internacional/

Organización de Estados Americanos. (2018). Comité Interamericano contra el terrorismo. *Organización de los Estados Americanos*. http://www.oas.org/es/sms/cicte/default.asp

Policía Nacional de Colombia. (2018). *Centro Cibernético Policial*. https://caivirtual.policia.gov.co/

Sánchez, A. (2017). *El mercado de la ciberseguridad en Colombia*. Ministerio de Industria, Comercio y Turismo. https://www.mintic.gov.co/portal/715/w3-multipropertyvalues-25384-111101.html?__noredirect=1#data=%7B%22filter%22:%2225385%22,%22page%22:0%7D

Valencia, F. (2012). *Ciberseguridad, ¿qué es?* Grupo de Investigación en Teoría y Gestión de Tecnologías de Información, Universidad Nacional de Colombia. http://pensamiento.unal.edu.co/fileadmin/recursos/focos/desarrollo-sostenible/Simposio_4a_Revolucion/8_Francisco_javier_valencia/9_Francisco_Javier_Valencia.pdf

Vargas, A. (2020). Colombia ocupa el puesto 39 en el ranking mundial sobre ciberseguridad. *La República*. https://www.larepublica.co/globoeconomia/ciberseguridad-otro-reto-que-deben-enfrentar-las-empresas-en-el-mundo-por-covid-3013083

Vargas, E. (2014). *Ciberseguridad y ciberdefensa: ¿qué implicaciones tienen para la seguridad nacional?* [Tesis de especialización]. Universidad Militar Nueva Granada. https://repository.unimilitar.edu.co/bitstream/handle/10654/12259/CIBERSEGURIDAD%20Y%20CIBERDEFENSA.%20TRABAJO%20DE%20GRADO.pdf?sequence=1&isAllowed=y