Título

La Ciberseguridad en el Estado Colombiano

Autor

Juan Nicolas Gómez Rengifo

Ensayo Académico opción de Grado

Dirigido por:

Ximena Andrea Cujabante Villamil

Docente de la Universidad Militar Nueva Granada

Universidad Militar Nueva Granada

Facultad de Relaciones Internacionales, Estrategia y Seguridad

Programa de Relaciones Internacionales y Estudios Políticos

Bogotá, D.C. 2021

Resumen

El presente documento trata temas sobre las nuevas amenazas a las que se enfrenta el Estado Colombiano, la normatividad implementada por parte de Colombia y cuál de las teorías de las Relaciones Internacionales es viable para a aplicación del caso colombiano respecto a la ciberseguridad.

Se tendrá en cuenta la defensa y protección del Ciberespacio, ya que se ha convertido en uno de los retos más importantes para los Estados actualmente, debido a la continua evolución, crecimiento y complejidad de los ataques cibernéticos. De ahí surge la necesidad de disponer de personal idóneo que se adapte a entornos de continuos avances tecnológicos que permitan proteger los intereses estatales ante posibles nuevas amenazas.

Para tratar con éxito dicha problemática, se debe priorizar programas sobre ciberdefensa y ciberseguridad, para evitar el aumento de la capacidad delincuencial en el ciberespacio, y aprovechar la utilización de nuevas tecnologías y así generar un sistema de seguridad más eficiente que brinde mayor confianza para disminuir los riesgos.

Palabras Clave

Ciberseguridad, Ciberdefensa, Ciberespacio, Estado, Riegos, Peligro, Colombia, Relaciones internacionales

Abstrac

This document deals with the new threats faced by the Colombian State, the regulations implemented by Colombia and which of the theories of International Relations is viable for the application of the Colombian case with respect to cybersecurity.

The defense and protection of Cyberspace will be taken into account, since it has become one of the most important challenges for the States nowadays, due to the continuous evolution, growth and complexity of cyber attacks. Hence the need to have suitable personnel to adapt to environments of continuous technological advances that allow the protection of state interests against possible new threats.

In order to successfully deal with this problem, programs on cyber defense and cybersecurity must be prioritized to prevent the increase of criminal capacity in cyberspace, and to take advantage of the use of new technologies and thus generate a

more efficient security system that provides greater confidence to reduce risks.

Keywords

Cybersecurity, Cyberdefense, Cyberspace, State, Risks, Danger, Colombia, International relations

Introducción

De acuerdo con el Ministerio de Defensa español (2010) es importante conocer las necesidades de los gobiernos para poder guiar y orientar la ciberseguridad, de este modo poder solventar cualquier tipo de amenaza que tengan sobre esta problemática, para garantizar su seguridad, en primera medida es importante dar a conocer el término ciberseguridad, el cual es importante porque está definido como "un conjunto de herramientas, políticas, directrices, gestión de riesgos, acciones, formación en salvaguardar la seguridad y uso de tecnología"(Cárdenas, 2015).

La ciberseguridad tiene como fin proteger los activos de la organización, así como crear un ambiente idóneo para proteger el ciber entorno de los estados como de los usuarios, brindando un ambiente de seguridad en donde la población goce de niveles apropiados de seguridad.

Se debe tomar en consideración que, para estudiar el fenómeno de la ciberseguridad establecida en un Estado, es necesario hacer una recopilación de todos los sucesos históricos o corrientes teóricas que hablen respecto de dicha problemática, debido a esto que presenta un inconveniente desde el inicio del uso de la computación.

> "El Gobierno Nacional y cualquier tipo de empresa requiere conocer y actuar de forma íntegra frente al manejo de la información, es necesario contar con las instancias adecuadas que permitan ejercer una labor de "Ciberseguridad" frente a cualquier amenaza informática o ataque cibernético que pueda comprometer la información o afectar la infraestructura critica del país y poner en riesgo la seguridad y defensa del Estado". (Bautista, 2021)

Países como Estados Unidos, Brasil, Argentina, Uruguay han tomada conciencia y consecuentemente han desplegado secciones especializadas para poder atender y dar una

respuesta de manera eficiente a cualquier incidente cibernético. Estas secciones son necesarias para todos los estados además de las entidades que conforman el sector público en Colombia, teniendo en cuenta lo anterior sería idóneo que las entidades que se vean afectadas por estos problemas empiecen a invertir de manera fructífera en el desarrollo de nuevos conocimientos y capacitaciones, esto es debido que día a día se enfrentan a amenazas cada vez más complejas.

Otra manera para poder visualizar la problemática de la ciberseguridad, es la transformación de este escenario debido que gana mayor relevancia porque los entes que en el pasado generaban ataques a la seguridad humana y estatal, empiezan a implementar ataques en el ciberespacio y esto ocasiona la mutación de una guerra de tercera generación a una de quita generación, esto consiste en implementación de estrategias que no se utilizaban antes, un ejemplo claro son los ataques desarrollados en el ciberespacio ocasionando desequilibrio, además de que la guerra tuviera una mutación el Estado colombiano se vio obligado a implementar nuevas estrategias para salvaguardar su integridad.

El tema a desarrollar es de vital importancia debido que los Estados, reciben constantemente ciberataques por parte de algún otro ente. Este tema hoy en día obtiene gran valor debido las trasformaciones a las que se han visto sujetas estas instituciones, ya que usualmente hoy en día la gran mayoría de los Estados han hecho la transición de los documentos en físico a netamente utilizar documentos digitales.

Teniendo en cuenta lo anterior, los Estados que sufren algún tipo de ataque se debe a que la seguridad implementada en sus servidores no es totalmente eficiente, es importante considerar lo que plantea el autor Cárdenas (2019) respecto a este tema ya que realmente hace criticas muy directas frente a las falencias que tiene el Estado colombiano.

> “El conocimiento sobre seguridad digital y defensa es deficiente en el sector público y privado; y se demuestra que no existen instituciones u organismos a nivel nacional que logren coordinar y desarrollar operaciones de ciberseguridad. Razón por la cual, es difícil establecer mecanismos adecuados y efectivos que neutralicen, debiliten y afronten ataques cibernéticos contra las infraestructuras críticas y protejan los intereses del Estado” (Cárdenas, 2019, p 16)

Actualmente un Estado es totalmente propenso a pasar por una acción o un ataque que ponga en riesgo su estabilidad y seguridad; por esta razón la presente investigación es desarrollada porque se supone que los Estados que se ven afectados necesitan saber cuáles son las falencias o vulnerabilidades más típicas a las que se enfrentan, de esta manera podrán observar en que están fallando los sistemas de seguridad y de qué modo pueden evitar las amenazas; el ensayo pretende proporcionar información al lector sobre cuáles son las amenazas más comunes a las que se enfrentan los Estados.

Las actividades del Estado Colimbiano en el ciberespacio se construyen de acuerdo con la combinación de las fuerzas de inteligencia donde se identifican las siguientes variables esenciales: legalidad, priorización de operaciones cibernéticas, la complejidad del entorno cibernético en el que se actúa, la interacción de las diferentes fuerzas estatales y elementos cibernéticos , la cooperación y la innovación en ciberseguridad y ciberdefensa ***¿Como el Estado Colombiano solventa o contrarresta los ciberataques recibidos?*** pregunta sobre la que se abre un océano de posibilidades y en la que se espera aportar en materia de seguridad a la pregunta central propuesta.

Hoy por hoy la supervivencia depende de múltiples factores asociados con los que interactuamos cotidianamente; de hecho, la seguridad humana coincide con la articulación de los factores de riesgo en mecanismos de prevención efectivos. Esto es sencillo en la medida en que los escenarios de riesgo se constituían en un factor de estrategia visible desde el punto de vista de la vulnerabilidad; igualmente perceptible en la planeación de los mecanismos de seguridad, el objetivo general del documento es demostrar como el Estado Colombiano solventa o contrarresta los ciberataques recibidos.

La historia cambia cuando el escenario que se propone solventar es el de la virtualidad. La seguridad en el ciberespacio, comporta otro tipo de estrategias que no solo tienen que ver con la tecnología, sino también con el tipo de acciones que se pueden emprender a través del manejo de la información, lo cual concurre en diversos tipos de riesgo y determinar que teorías de la Relaciones internacionales se pueden aplicar a la problemática de la ciberseguridad en Colombia, Si bien es cierto que a nivel civil la seguridad en un 90% se ha enfocado en el valor de la información financiera, en el ciberespacio no solo se hallan datos financieros, de hecho, existen múltiples contenidos susceptibles tales como videos gore, algunos de ellos son realizados por carteles mexicanos o incluso el mismo estado islámico, también pornografía infantil entre otros tipos de que al ser expuestos pueden afectar la estabilidad humana y social, contenidos que se describen en el presente ensayo y se busca especificar cuáles son las herramientas utilizadas por parte del Estado Colombiano para evitar ciberataques, y poder buscar siempre un ciclo de

acciones, decisiones y retroalimentaciones que favorezcan a los interés de la Nación y sus ciudadanos.

Los escenarios en los que se mueve la información hoy en día están determinados por las Tecnologías de la Información (TIC) las cuales cada vez más, están reconfigurando el mundo de la información, la velocidad de acceso, la cantidad y la calidad de la información, no solo en el ámbito de las organizaciones sino también las de los ciudadanos, y por ende es de gran importancia definir cuáles son los actores y describir las amenazas en su concepción de la realidad actual, dentro de un marco Nacional, y considerar que siempre lo que se busca es salvaguardar la soberanía y el bienestar de cada ciudadano.

1. Teorías de la Relaciones internacionales frente a la problemática de la ciberseguridad en Colombia.

Las Relaciones Internacionales, en términos del sistema teórico, que logre explicar la efectividad de los mecanismos de seguridad digital del sector público en Colombia, se menciona al enfoque estructural-funcionalista, derivado del enfoque funcionalista, el cual relacionado uno con el otro, se caracteriza por identificar cuáles son las funciones para que un sistema de gobierno se desempeñe de forma adecuada, qué estructuras deben cumplirlas y a través de cuáles procesos son llevadas a cabo para cumplir determinada función, frente a diferentes situaciones, como en este caso es de riesgo y vulnerabilidad que no solo afecta al territorio Colombiano sino que es una amenaza global (Merton 1964: 61).

Por lo tanto, este enfoque es una variable que logra asentar las definiciones más importantes, a partir de elementos académicos que se ajusten en el caso de seguridad digital, que sobrepasa las fronteras y son aplicados en diferentes países como Estados Unidos, Estonia, Rusia, entre otros. Este enfoque, se ajusta en el contexto colombiano, en el ámbito político contemporáneo, complementando así, la aplicación conceptual y teórica directamente en el tema a tratar.

Las acciones que son reguladas por parte del sector público, son para hacerle frente a los ataques de tipo digital a sus infraestructuras críticas y su respectiva capacidad de respuesta. De este modo se puede demostrar el desarrollo respecto a la protección de las estructuras informáticas del Estado Colombiano, una de ellas es la capacidad de respuesta a amenazas cibernéticas latentes en el país.

Una vez identificada su existencia de manera clara, la situación colombiana en temas relacionados con la seguridad digital a nivel global; esta reacción se ejecutará por medio de las entidades y mecanismos de seguridad implementado por parte del sector público, debido que tienen herramientas necesarias para proteger las estructuras informáticas; la existencia de amenazas se establecerá por medio de los organismos públicos encargados de temas informáticos, especialmente que haya tenido relación con algún posible ataque al país y su forma de reaccionar en cada caso en el que estuvo relacionado.

En este enfoque sobresale el concepto de función reguladora, que determina la difusión de normas sobre diferentes actividades políticas, sociales, económicas, culturales o en este caso privadas. Lo anterior, para asegurar su calidad y aplicabilidad en determinado contexto como lo es la seguridad digital en Colombia, las normas que platea y en el enfoque que se traduce en mecanismos aplicables en el contexto del ciberespacio. (Dryzek, Honig & Phillips, 2006). A partir de dicho enfoque, el autor Gabriel A. Almond, menciona en el texto "Comparative politics today: A worldview" (2005), la adecuada aplicación de una teoría a contextos contemporáneos determinados. Esto será clave para el desarrollo de los objetivos específicos asociados al uso de las tecnologías de la información, como lo es ciberataques, seguridad digital y ciberespacio (Almond, 2005).

Es pertinente identificar funciones y estructuras que se deben ejecutar y aplicar en determinados casos; en este contexto se entendería como los mecanismos que se emplearían en el ciberespacio y su apropiada aplicación. Enfocado en una aplicación sistemática de la teoría en la situación de varios sistemas políticos actuales, con el objetivo de que funcione adecuadamente en el desempeño de políticas públicas (Merton 1964: 61).

En este orden de ideas la teoría de la información y cibernética planteada por Karl W. Deutsch, quien afirma que una característica de la política y de los sistemas políticos de Occidente, es el hecho de haber desarrollado diversas técnicas cuya función es acelerar la innovación y el aprendizaje social. En este punto, se destaca la técnica para formular y llevar a la práctica las decisiones, la cual es "un instrumento esencial del aprendizaje social": un "instrumento de supervivencia y desarrollo" más que de destrucción (Deutsch, 2007, Pág. 138).

Teniendo en cuenta lo nombrado con anterioridad, el enfoque teórico utilizado es parte fundamental para identificar cuál de las teorías de la Relaciones Internacionales se aplica de manera correcta al caso colombiano respecto a la presencia de amenazas a su

ciberseguridad, además de cuáles son las medidas utilizadas por parte del sector público para preservar la ciberseguridad del Estado.

2. Herramientas utilizadas por parte del Estado Colombiano para evitar ciber ataques.

El Estado Colombiano implementa el uso de programas y políticas de prevención, confrontación y resolución de las amenazas respecto a ciberseguridad y ciberdefensa, las herramientas colombianas fueron especificadas en leyes y decretos una de las leyes con gran relevancia es la ley 1623 del 2013, en esta ley se habla sobre el fortalecimiento del marco jurídico para que los organismos nacionales autorizados lleven acabo actividades de inteligencia y contrainteligencia en el Estado Colombiano , la función de estos documentos es dejar de manera clara cual debe ser el modo el accionar por parte del Estado Colombiano en el momento que se enfrenta a una amenaza que ponga en riesgos su ciberseguridad e inestabilice su ciberdefensa.

Con el desarrollo de las tecnologías y el crecimiento continuo de la globalización, cada vez más los Estados se ven interesados en proteger su información e infraestructura critica de los ataques de los delitos informáticos perpetrados por actores estatales y no estatales de diversas partes del globo, en ese sentido el gobierno Colombiano ha realizado diversos avances en materia de ciberseguridad y ciberdefensa especialmente en el ámbito jurídico ya que ha expedido varias leyes, Del mismo modo, en este documento da a conocer la distinta normatividad e iniciativas que el gobierno ha impulsado desde tiempo atrás para mejorar la calidad de la utilización en ciberseguridad, Colombia, entre ella se destacan las siguientes (DNP, 2011, P.11):

Según el CONPES 3701 del 2011 sobre lineamientos de ciberseguridad y ciberdefensa, algunas de las leyes mencionadas tienen como punto central la protección de datos sobre particulares y compañías, estos según la ley tienen validéz respecto que las personas puedan tener acceso a estos y no se limiten los datos en cuanto sea a función para desarrollar una investigación sobre su nombre o incluso archivos públicos. Estos datos se les otorgaran tal cual como lo dice la Ley 527 de 1999 ya que serán admisibles como medio de prueba en las actuaciones administrativas y judiciales, además de que no se negara la eficacia

o valides de fuerza probatoria, además de que en la Ley general de archivos todo tipo de persona tiene derecho a consultar estos documentos.

Respecto a la Ley 679 del 2001 sobre la pornografía infantil se establecen las medidas técnicas y administrativas destinadas a prevenir el acceso de este tipo de contenido para evitar que propaguen de manera masiva en internet, además esta Ley se implementa para la protección de las personas, esta ley va en conjunto con las demás debido que se centra en la protección de cualquier tipo de individuo y las compañías.

Además para la protección de datos financieros también se tienen unas Leyes, tales como la Ley 1266 del 2008 habeas data, en la cual se regula el manejo de información de bases de datos personales, igual que la protección de medios informáticos y delitos informáticos como es la Ley 1273 del 2009 que es para la protección de información de datos, estas leyes nombradas anteriormente van en conjunto debido que tiene una estrecha relación respecto a la protección de las personas, compañías y Estados, a lo que concierne la ciberseguridad y ciberdefensa de estas, también es importante la creación de las TIC debido que las personas puede adquirir y consultar información pública y gratuita sin tener ningún tipo de consecuencia ya que este es un derecho, además de que también puede presentar peticiones respetuosas ante las autoridades en los términos señalados en este código del que se habla con anterioridad, esta es la Ley 1437 del 2011 y también se estipulan Leyes para la protección del consumidor por medios electrónicos, en esta Ley se le brindan derechos a los consumidores y le da obligaciones a las compañías para comercializar o no estos productos, además de responsabilizar a las compañías siendo el caso que el producto lleguen en mal estado, esta Ley busca siempre brindarle la mayor protección al consumidor.

Muchas de estas Leyes también colaboran respecto a la protección y confidencialidad de las personal tal como la Ley 1581 del 2012 que habla sobre la protección de datos personales, la cual en esta se estipula la prohibición de transferencia de datos personales de cualquier tipo a países que no proporcionen los niveles adecuados de protección de datos, es decir las leyes del consumidor prohíben de manera rotunda compartir cualquier tipo de datos personal, debido que esto puede llegar afectar a los individuos o las empresas de manera económica, algo que tienen en común estas leyes es siempre mantener a salvo la ciberseguridad y ciberdefensa de cualquier tipo de persona, compañía o Estado.

Todas estas leyes tienen valides jurídica en el ámbito nacional debido que se apegan al marco jurídico de las instituciones internacionales debido que también velando por su ciberseguridad y ciberdefensa, es importante tener en cuenta la Ley

> de inteligencia 1623 del 2013, en la cual hablan sobre el fortalecimiento del marco jurídico para que permitan que los organismos nacionales lleven a cabo actividades de inteligencia ycontrainteligencia para cumplir con esta misión constitucional y legal.

Estas leyes nombradas anteriormente intentan proteger toda la información de vital importancia tanto para el Estado Colombiano como para las personas civiles y jurídicas, en ese orden de ideas se puede manifestar que se han implementado diversos mecanismos de defensa legislativos para garantizar la protección jurídica de la información, la protección informática de los archivos, protección de la tecnología de la información, además de la protección que se brinda al consumidor y de sus datos personales y por ultimo su protección financiera, esto se desarrolla con el objetivo de evitar ataques a la infraestructura critica de la nación.

Estos documentos, leyes y decretos de algún modo reflejan algunas realidades vigentes a las que se tuvo que enfrentar el Estado Colombiano en virtud de la ciberseguridad y ciberdefensa, el problema radica en que las amenazas tienen su propia dinámica de cambio delincuencial, esto les brinda la capacidad de innovación y diversificación frente a las acciones del Estado, de este modo generando nuevas modalidades de amenaza.

> El estado colombiano se adhiere al convenio de Budapest contra la ciberdelincuencia buscando la coordinación y la cooperación entre los estados que se ven afectados, con este convenio se busca “como fortalecer las capacidades nacionales, con el fin de prevenir, detectar, investigar y enjuiciar a la delincuencia organizada transnacional en el ciberespacio” (Cancillería, 2020).

Todas las nuevas dinámicas del accionar criminal, brinda una nueva oportunidad para que el Estado Colombiano interactúe de manera más directa en el ciberespacio, además de implementar acciones más eficaces para mantener intacta su ciberseguridad y ciberdefensa; de este modo evitando cualquier tipo de amenaza que ponga en riesgo su ciberseguridad y ciberdefensa.

3. Política Nacional de seguridad y conveniencia ciudadana

> "La política requiere del accionar de diversas entidades y actores tanto en el nivel nacional como en el territorial, atendiendo a que las manifestaciones de inseguridad y baja convivencia ciudadana se concretan en el nivel local, y son causadas en gran medida por las particularidades territoriales. La corresponsabilidad de los municipios en la implementación de la política resulta fundamental, no sólo en términos de ejecución y cofinanciación, sino de coordinación local de las distintas entidades y actores que tienen responsabilidades y participan en cada uno de los ejes estratégicos de la política" (Alta consejería presidencial, 2011).

La fórmula de la política nacional de seguridad y convivencia ciudadana, refiere que las "amenazas más evolucionadas en su concepción de realidad actualmente dentro de un marco típicamente nacional, con determinación de responsables para su confrontación, pero que no aborda la influencia de las amenazas externas" (Chinome,2017), tiene una influencia en la materialización de los actos violentos que desequilibra el Estado de seguridad.

Este tipo de política no es de carácter estatal sino gubernamental, de hecho, hay una dispersión de la normatividad de confrontación al crimen que causa que las diferentes instituciones comprometidas, gestionen por su parte fuerzas para luchar con el delito.

En 2002 se desarrolló una sesión extraordinaria de la organización de los Estados Americanos (OEA), donde se consideró el tema "enfoque multidimensional de la seguridad hemisférica", además de esto una de las partes manifestó que:

> "las amenazas, preocupaciones y otros desafíos a la seguridad en el hemisferio son de naturaleza diversa y alcance multidimensional y que el concepto y enfoque tradicionales deben ampliarse para abarcar amenazas nuevas y no tradicionales, que incluyen aspectos políticos, económicos, sociales, de salud y ambientales"(OEA, 2002).

Esta declaración abrió una nueva visión sobre el enfoque de la seguridad, debido que ya no se limitaba a un enfoque netamente militar y policial de la problemática, sino que

provoco abordar otros aspectos cotidianos como los políticos, económicos, sociales y ambientales, ya que estos aspectos también pueden afectar la seguridad estatal en general.

De acuerdo con la OEA (2003) los Estados se ven amenazados por algo denominado nuevas amenazas, en este concepto se incluyeron diversas definiciones las cuales antes no se les había brindado una clasificación, en estas nuevas amenazas se ve incluidas: el terrorismo, la pobreza extrema, desastres naturales, trata de personas, ataques a la seguridad cibernética, posibles accidentes al transportar materiales potencialmente peligrosos y por último obtención de armas de destrucción masiva.

> "la seguridad en el Hemisferio es de alcance multidimensional, incluye las amenazas tradicionales y las nuevas amenazas, preocupaciones y otros desafíos a la seguridad de los Estados del Hemisferio, incorpora las prioridades de cada Estado, contribuye a la consolidación de la paz, al desarrollo integral y a la justicia social, y se basa en valores democráticos, el respeto, la promoción y defensa de los derechos humanos, la solidaridad, la cooperación y el respeto a la soberanía nacional" (OEA, 2003)

Objetivos del Programa de Ciberseguridad según la OEA:

- Apoyar a los Estados Miembros de la OEA en el desarrollo de capacidades técnicas y políticas para prevenir, identificar, responder y recuperarse exitosamente de incidentes cibernéticos.
- Mejorar el intercambio de información, la cooperación y la coordinación sólidas, efectivas y oportunas entre las partes interesadas en seguridad cibernética a nivel nacional, regional e internacional.
- Aumentar el acceso al conocimiento e información sobre amenazas y riesgos cibernéticos por parte de los interesados públicos, privados y de la sociedad civil, así como los usuarios de Internet.

El programa se centra en: desarrollo de políticas, desarrollo de capacidades (incluyendo capacitación y ejercicios cibernéticos), e investigación y divulgación.

- Desarrollo de políticas: el programa ayuda a los Estados miembros de la OEA a desarrollar estrategias nacionales o regionales de ciberseguridad que involucren a

todas las partes interesadas relevantes y que se ajusten a la situación legislativa, cultural, económica y estructural de cada país y apoyen las evaluaciones a nivel nacional sobre la capacidad y la madurez de la ciberseguridad. Bajo esta vía, el programa apoya el desarrollo de medidas de fomento de la confianza en el ciberespacio.

- Creación de capacidad: El programa ayuda a establecer y desarrollar la capacidad de los equipos nacionales de respuesta a incidentes de seguridad informática (CSIRT) existentes y brinda asistencia técnica personalizada y oportunidades de ejercicio para fortalecer las instituciones y organizaciones nacionales y regionales. El desarrollo de una fuerza laboral de ciberseguridad también se lleva a cabo a través de diversas formas de oportunidades de desarrollo profesional.
- Investigación y divulgación: El programa desarrolla documentos técnicos, conjuntos de herramientas e informes basados en investigaciones para guiar a los responsables de políticas, CSIRT, operadores de infraestructura, organizaciones privadas y la sociedad civil, destacando los desarrollos actuales e identificando los problemas y desafíos clave de seguridad cibernética en la región (Página principal de la OEA).

La cooperación regional o internacional se debe caracterizar por interdependencia o dependencia reciproca entre los actores que la conforman, por lo tanto, su naturaleza no debe ser unilateral sino multilateral y en varias dimensiones de atención y confrontación a las organizaciones criminales, mediante políticas de seguridad de integración.

> “la función propia de las Relaciones Internacionales, de aprovechar el conjunto de mecanismos de interacción con que cuentan los Estados, las Sociedades Civiles y los Organismos Internacionales para responder mediante cooperación y colaboración a los desafíos que plantea la actividad criminal, es un menester imperativo de prevención, represión y control” (Chinome, 2017).

Determinar el grado de influencia e impacto por parte de las nuevas amenazas determinadas por parte de la OEA, en el ámbito de Seguridad en colombiana, “infieren un

claro reconocimiento de afectación, debido a que se observan una real correspondencia de impacto en los diferentes indicadores de criminalidad que se miden en el País, y que afectan el estado de Protección y Convivencia Ciudadana" (Chinome, 2017).

Colombia en materia de ciberseguridad y ciberdefensa

Según estudios realizados por el Ministerio de Defensa Nacional de Colombia, a través de la Dirección de Estudios Sectoriales (2009), "para el año 2000 tan solo el 2% de la población tenía acceso a Internet; actualmente el 50% hace uso constante de este medio ubicando al país en el cuarto lugar en el ranking de usuarios de América Latina y en el puesto 24 del mundo."

Colombia ha enfrentado numerosos ataques informáticos a 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, los cuales dejaron estas páginas fuera de servicio por varias horas (Departamento Nacional de Planeación, 2011, P.9), y 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 del hecho que el nivel de sofisticación de los ataques va en aumento y es necesario tener en cuenta ello para evitar problemas en el futuro.

> "Desde el año 2005 se creó un grupo interagencial liderado por el Ministerio de Relaciones Exteriores, en conjunto don el Ministerio del interior y de Justicia, el Ministerio de Defensa Nacional y posteriormente el Ministerios de las Tecnologías de la Información y las Telecomunicaciones (TIC's) y Entidades relacionadas con este tema, decidieron que quien levaría las riendas de la ciberseguridad y la ciberdefensa de Colombia sería el Ministerio de Defensa Nacional" (Ministerio de Defensa, 2009, P. 4) .

De este trabajo mancomunado entre las instituciones anteriormente relacionadas se gesta en 2009 el ColCERT (Equipo de Respuesta a Emergencias Informáticas de Colombia), "cuya función principal es la de coordinar las acciones necesarias para la

protección de la infraestructura crítica del Estado colombiano, frente a emergencias cibernéticas que atenten o comprometan la Seguridad y Defensa Nacional" (Ministerio de Defensa, 2009, P.4).

En primera instancia es importante el fortalecimiento jurídico e institucional, el cual se refiere a adopción y adaptación del sistema de legislativo y judicial para los temas de ciberseguridad. El plantea los asuntos internacionales como plano de vital importancia para los intereses colombianos, esto se traduce en una misión de observación de los casos internacionales y que tendencias se marcan en el ámbito de la ciberseguridad y ciberdefensa en cuanto a medidas a preventivas que lleven a una minimización del riesgo de sufrir ataques cibernéticos, así como implementación de acuerdos sobre la materia que pueda asumir el estado ya sea bilateral o multilateralmente. Se encuentran las medidas contra el delito cibernético.

Con ello se refieren a las capacidades que puede adquirir en cuanto a sistemas de defensa que mediante el ColCERT se ponen en marcha para mitigar potenciales ataques (Ministerio de Defensa, 2009, P. 4). En cuanto al ColCERT, se enfatiza que es importante trabajar de mano de las entidades privadas para obtener financiación y de ese modo se pueda evolucionar en el fortalecimiento de esta entidad y que no quede como un proyecto inconcluso.

En la actualidad esta entidad a través de su página en Internet www.colcert.gov.co, brinda información acerca de foros mundiales sobre seguridad informática, así como asesorías y actualizaciones de seguridad para sistemas operativos y de ese modo reducir la vulnerabilidad de los ordenadores.

Así mismo, el Consejo Nacional de Política económica Y social del Departamento Nacional de Planeación (DNP), emitió en 2011 un documento CONPES Sobre los lineamientos de política para ciberseguridad y ciberdefensa con colaboración de todas las instituciones que tienen que ver con este tema, como el Ministerio de Defensa, Ministerio de Interior, Ministerio de TIC's entre otras (2011).

Con el acompañamiento de organizaciones como la OEA ha venido organizando talleres y seminarios sobre la materia de ciberseguridad y ciberdefensa, así como la

creación de mecanismos y estrategias que permitan la lucha frontal contra la criminalidad cibernética y la protección de infraestructuras críticas que puedan ser objeto de ataques cibernéticos. (DNP, 2011).

Conclusiones

-En la teoría estructural funcionalista se evidencian cambios constantes que en el mundo, así que se busca la adaptabilidad a cada contexto que abarque temas de la agenda global como lo es la política exterior, economía y tecnología, estos son elementos claves para posicionar a un Estado en una mejor posición en el Sistema Internacional, este enfoque teórico será parte fundamental para lograr identificar la presencia de amenazas cibernéticas y detallar las medidas que ha efectuado el sector público del Estado Colombiano para preservar su seguridad informática.

-La normatividad actual implementada por Colombia para confrontar las amenazas que se ensañan contra la ciberseguridad y ciberdefensa realmente no se ajustan a las realidades mundiales debido que son obsoletas y les faltan herramientas organizacionales, estructurales, jurídicas, administrativas y financieras que hagan más fácil el enfrentamiento contra las actividades criminales, debido que en varios de sus enfrentamientos no cumplen con garantizar las condiciones de protección estatal.

- Colombia es un Estado propenso a las amenazas tradicionales y que las nuevas se desarrollen en nuestro entorno, porque existen condiciones desfavorable de carácter social, político y jurídico que pueden ser aprovechadas por los actores generadores de violencia para poder desarrollar sus actividades delincuenciales, de este modo Colombia debe plantearse el objetivo de adoptar y recibir el concepto de seguridad multidimensional como componente clave para diseñar una normatividad de ciberseguridad y seguridad nacional multidimensional que se apeguen a los estándares internacionales en la prevención, represión y control de estas amenazas.

-Las tecnologías de información y telecomunicaciones van avanzando a un ritmo más rápido al pasar de los días. Por ello, es importante estar a la vanguardia de los mecanismos para salvaguardar no solo la información sensible de los pobladores de un país o el ataque a una página oficial que se cataloga como un ataque de baja intensidad, sino también tener sistemas de defensa que permitan proteger las infraestructuras críticas que con el paso del tiempo son más dependientes, y si no se protegen la sociedad estaría presenciando un ataque de alta intensidad.

-Las ciberarmas deben controlarse. De lo contrario, como se observó en los casos de ataques rusos, cualquier tensión diplomática podría convertirse en un ataque informático que produciría una escalada en el conflicto, que desbordaría en una confrontación armada regular. A pesar de que en un ciberataque no se dispara una sola bala, el caos que generaría podría ser desastroso para cualquier país que sufra este tipo de agresión. Hoy en día si se comete un crimen a través del ciberespacio es muy complicado hacer justicia, dado que como muchos expertos afirman, el ciberespacio se está convirtiendo en el arma perfecta, por esto la necesidad al mismo tiempo de controlar las ciberarmas, de acabar con el cibercrimen.

-Colombia busca ponerse a la vanguardia en su región en cuanto a ciberseguridad y ciberdefensa se refiere. Desde hace aproximadamente 17 años viene adelantando gestiones para proteger la información sensible de la población, sin embargo, el gobierno es consciente que debe trabajar profundamente en la creación de estamentos e instituciones que permitan controlar aún más los delitos informáticos y ciberataques a su infraestructura crítica. Por esa razón, es muy útil el esfuerzo de crear unidades militares de policía con las que actualmente ya se cuenta, al igual que una agencia que prevenga cualquier clase de delitos informáticos, con el fin de mantener informada a la población de cualquier tipo de amenaza, si este tipo de información se mantiene bajo reserva, cualquier esfuerzo por evitar un ciberataque será infructuoso.

Bibliografía

Cardenas Moreno, W. (Junio de 2015). *CIBERDEFENSA Y CIBERSEGURIDAD EN EL SECTOR DEFENSA DE COLOMBIA*. Obtenido de Polux.unipiloto: http://polux.unipiloto.edu.co:8080/00002590.pdf

Chinome Soto, G. A. (06 de Diciembre de 2017). *SEGURIDAD MULTIDIMENSIONAL, FUNDAMENTO DE LA ESTRUCTURACIÓN DE LA DEFENSA Y SEGURIDAD NACIONAL EN COLOMBIA* . Obtenido de Repository.unimilitar: https://repository.unimilitar.edu.co/bitstream/handle/10654/17074/ChimeSotoGuillermoAntonio2017.pdf?sequence=1&isAllowed=y

Gobierno de Colombia . (18 de Agosto de 1999). *Reglamento de acceso y uso de datos* . Obtenido de GOV : https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4276

Gobierno de Colombia . (8 de Julio de 2005). *Simplificacion de Tramites* . Obtenido de GOV: http://wp.presidencia.gov.co/sitios/normativa/leyes/Documents/Juridica/Ley%20962%20de%2008%20de%20julio%20de%202005.pdf

Gobierno de Colombia . (18 de Enero de 2011). *Ley 1437 de 2011* . Obtenido de GOV : https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=41249

Gobierno de Colombia . (12 de Octubre de 2011). *Ley 1480 de 2011* . Obtenido de GOV : https://dernegocios.uexternado.edu.co/comercio-electronico/ley-1480-de-2011/

Gobierno de Colombia . (10 de Enero de 2012). *Decreto Ley 019 de 2012*. Obtenido de GOV: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=45322

Gobierno de Colombia . (17 de Abril de 2013). *Ley 1623 de 2013*. Obtenido de GOV: file:///C:/Users/USER/Downloads/LEY%201621%20DE%202013%20Inteligencia%20y%20Contrainteligencia.pdf

Gobierno de Colombia . (6 de Marzo de 2014). *Ley 1712 de 2014*. Obtenido de GOV: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882

Gobierno de Colombia. (14 de Julio de 2000). *Ley 594 de 2000*. Obtenido de GOV: https://normativa.archivogeneral.gov.co/ley-594-de-2000/?pdf=41

Gobierno de Colombia. (24 de Julio de 2001). *Ley 679 de 2001*. Obtenido de GOV: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=5551

Gobierno de Colombia. (31 de 12 de 2008). *Ley 1266 de 2008*. Obtenido de GOV: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488

Gobierno de Colombia. (30 de Julio de 2009). *Ley 1273 de 2009*. Obtenido de GOV: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=36913

Martinez Lopez , L. P. (noviembre de 2018). *EL CIBERCRIMEN EN COLOMBIA*. Obtenido de Repository.unimilitar: https://repository.unimilitar.edu.co/bitstream/handle/10654/31900/MartinezLopezLeidyPaola2019.pdf.pdf?sequence=1&isAllowed=y

Ministerio de Defensa Español . (Diciembre de 2010). *CIBERSEGURIDAD. RETOS Y AMENAZAS A LA SEGURIDAD NACIONAL EN EL CIBERESPACIO*. Obtenido de ieee.es: http://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf

Ministerio de tecnologias de la informacion y las comunicaciones de colombia . (2011). *CONPES 3701 DE 2011*. Obtenido de MinTic: http://www2.icfesinteractivo.gov.co/Normograma/docs/conpes_dnp_3701_2011.htm

Pérez Pérez , Y. (SF). *IMPORTANCIA DE LA CIBERSEGURIDAD EN COLOMBIA* . Obtenido de Repository.unipiloto: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2676/Trabajo%20de%20grado.pdf?sequence=1&isAllowed=y

Puentes León, S. (Junio de 2019). *COLOMBIA: ¿ ES UN ESTADO EFECTIVO EN TERMINO DE SEGURIDAD DIGITAL CON ENFASIS EN EL SECTOR PRIVADO?* Obtenido de Repository.javeriana: https://repository.javeriana.edu.co/bitstream/handle/10554/46540/TRABAJO%20DE%20GRADO.pdf?sequence=1&isAllowed=y#:~:text=Este%20tiene%20como%20objetivo%20enfrentar,objetivo%20de%20prevenir%20los%20delitos

Quintero Agudelo , Y. (SF). *LA SEGURIDAD Y LA CIBERDEFENSA EN COLOMBIA* . Obtenido de Polux.unipiloto: http://polux.unipiloto.edu.co:8080/00001596.pdf

Sánchez Medero, G. (SF). *LOS ESTADOS Y LA CIBERGUERRA* . Obtenido de file:///C:/Users/USER/Downloads/Dialnet-LosEstadosYLaCiberguerra-3745519.pdf

Vargas Vargas , E. (2014). *CIBERSEGURIDAD Y CIBERDEFENSA: ¿QUE IMPLICACIONES TIENEN PARA LA SEGURIDAD NACIONAL?* Obtenido de BIBLIOTECA UMNG: https://repository.unimilitar.edu.co/bitstream/handle/10654/12259/CIBERSEGURIDAD%20Y%20CIBERDEFENSA.%20TRABAJO%20DE%20GRADO.pdf?sequence=1

Alta consejeria presidencial para la convivencia y seguridad ciudadana. (2011). Obtenido de Politica nacional de seguridad y convicencia ciudadana : https://colaboracion.dnp.gov.co/CDT/Prensa/Publicaciones/1-PNSCC%20FINAL%20AGO%202011.pdf

Cancilleria . (16 de Marzo de 2020). Obtenido de Colombia de adhiere al convenio de Budapest contra ciberdelincuencia : http://www.secretariasenado.gov.co/senado/basedoc/ley_1928_2018.html

Organizacion de Estados Americanos . (23-27 de Octubre de 2003). Obtenido de Conferencia Especial para la seguridad : https://www.oas.org/36ag/espanol/doc_referencia/DeclaracionMexico_Seguridad.pdf