LA CIBERSEGURIDAD EN EL ÁMBITO DE LA SEGURIDAD COLOMBIANA ¿AVANCE O RETROCESO?

CAMILA ANDREA OSORIO MORENO

UNIVERSIDAD MILITAR NUEVA GRANADA
FACULTAD DE RELACIONES INTERNACIONALES, ESTRATEGIA Y SEGURIDAD
DIPLOMADO EN GERENCIA DE LA SEGURIDAD
BOGOTÁ D.C.
2018

RESUMEN

Se suspira una era y se vive en un tiempo en donde la información va tomada de la mano de la tecnología. Es allí en donde la población y los Estados generan una gran cantidad de significados a tan poca distancia de donde se encuentran, sin importar la ubicación. Es entonces, en donde no solo los avances de la información entran en vigor o en amenaza, todos estos servicios se prestan a través del ciberespacio.

Este trabajo pretende conocer los conceptos de ciberseguridad y comprender cómo estos avances en Colombia han generado un impacto significativo en el ámbito de la seguridad y por último si nos enfrentamos a avances o a retrocesos.

Palabras claves: ciberseguridad, amenazas, seguridad informática y desafíos.

Abstract

An era is sighing and one lives in a time where information goes hand in hand with technology. It is there where the population and the States generate a great amount of meanings at such a short distance from where they are, regardless of the location. It is then, where not only the advances of information come into force or threat, all these services are provided through cyberspace.

This work aims to know the concepts of cybersecurity and understand how these advances in Colombia have generated a significant impact in the field of security and finally if we face a setback.

Key words: cybersecurity, threats, computer security and challenges

INTRODUCCIÓN

En la última década el mundo ha cambiado de manera radical, hoy en día se puede obtener cualquier información con tan solo abrir un ordenador, prenderlo y buscar cualquier información con los diferentes navegadores que existen. La tecnología influye en el desarrollo social de un grupo de individuos, lo que importa es satisfacer las necesidades del hombre, en otras palabras, el consumismo.

La autora María Belén Albornoz en su escrito Cibercultura y las nuevas nociones de privacidad de la revista Nómadas afirma que: “No caer en la tentación de considerar lo virtual y lo real como categorías opuestas”. Cabe señalar que la era virtual y la vida real no están muy alejadas del todo. La era virtual es una demostración de “mi otro yo”, de las posibles acciones u cosas que en la vida real no se puede hacer o tener el coraje de realizarlo. Esto lleva a que los avances tecnológicos empiecen a reemplazar la realidad.

La sociedad emplea la tecnología para sus propios beneficios e intereses, usándola de manera correcta o incorrecta, desde la óptica o perspectiva que se analice; la tecnología en la medida que transcurre el tiempo está más involucrada dentro de la vida del ser humano y llegará al punto de reemplazarlo, en múltiples escenarios de la cotidianidad.

En consecuencia, se podría decir que la humanidad asume el riesgo de mayor resultado hacia un contexto de poder, aspirando a obtener más capacidad, fuerza y recursos, mediante el empleo de la tecnología. Los sujetos detrás de las pantallas manipulan la mente de los individuos como juguetes, para ejercer control sobre los demás.

Los avances de la ciencia y la tecnología en temas de cibernética, nanotecnología, telecomunicaciones, entre otros, no han sido del todo bien utilizados por los seres humanos, ellos liberan una opresión y dependencia en temas de poder, al concentrarlo en sus manos, la humanidad refleja condiciones de impotencia.

La guerra ha crecido en estrecha relación con los avances científicos y tecnológicos, es una muestra del alcance y de impacto para la sociedad, sobre las capacidades que se obtienen para ejercer el control y poder. Se expresa entre los Estados, principalmente en el armamento e involucra factores políticos, económicos y sociales obligando a los Estados a proteger y brindar apoyo a la sociedad.

En América Latina, durante décadas, muchas de las políticas públicas en temas de defensa y seguridad han sido dirigidas a una optimización que pone en marcha la administración en donde los resultados de protección no están enfocados a sus ciudadanos, por el contrario, han sido violatorias de las libertades, las cuestiones relacionadas con seguridad son ancladas a la violencia y a la problemática de las dinámicas sociales

En este trabajo, se abordarán los nuevos escenarios que la historia ha mostrado en temas de información y en cómo la ciencia y la tecnología han avanzado con un breve conteo de la evolución tecnológica. Posteriormente, se hablará de la ciberseguridad como concepto amplio, las normatividades nacionales e internacionales aplicadas y reconocidas en Colombia en temas de ciberseguridad y por último un breve análisis sobre si Colombia implementa herramientas acertadas para la defensa en dicho tema.

NUEVOS ESCENARIOS DE INFORMACIÓN

El ciberespacio es la dimensión formada en el tiempo, que entrelaza interconexiones e interoperabilidad de las redes relacionadas con los sistemas informáticos y de las telecomunicaciones que lo une. Clarke y Knake (2011) dicen que: “el ciberespacio lo conforman todas las redes informáticas del mundo y todo lo que ellas conectan y controlan”, en otras palabras, no solamente es internet el que ayuda con estos avances, es también el papel que juega el incremento de las acciones ilícitas cometidas por el medio informático en el mundo y en cómo afectan en la vida cotidiana.

Las transformaciones, los cambios y la velocidad con que la sociedad va avanzando se han vuelto previsibles y a la vez inadvertidos, estos cambios alcanzan los más altos niveles de información. Hoy en día, se construye un proceso de aprendizaje colaborativo de comunicación, que implementa una visión de la Web 2.0.

Se puede deducir que esa evolución ocurre dependiendo del espacio en el que el mundo se mueve, el ciberespacio, en la sociedad, la cibercultura como medio de evolución, la cibersociedad hacia una nueva cultura, los centros virtuales, las áreas virtuales, el aprendizaje virtual, entre otros. Todo esto caracterizado por la evolución de las TICS, en lo particular como medio de información y comunicación en la red.

Lo virtual ha hecho de la vida el establecimiento característico de lo análogo y de lo presencial a lo que señala el nuevo elemento estratégico del siglo XXI. El problema es que, si se llega a una gran velocidad, el uso mal empleado podrá causar daño incluso la destrucción del hombre.

El ser humano es la especie más importante en temas de inteligencia en todo el mundo, cuenta con un alma en espíritu de búsqueda permanente, gracias a ello, ha podido descubrir y analizar los misterios de la naturaleza, transformándolos en servicios. La construcción tecnológica y la aplicación de la ciencia se han convertido en los cimientos de los cambios de esta nueva era, en ese sentido, se tiene en

cuenta que son conscientes del dominio de las nuevas tecnologías como surgimiento de un contexto educativo y después incorporarlo a lo que rodea.

Los cibercriminales son sigilosos a la hora de tomar partida y acceder a las fuentes de información, en busca de dinero, información, secretos, robo de diseños, modificación de datos, base de datos, entre otros, manteniéndose a la sombra, las medidas de seguridad que se toman no son efectivas y permiten que las filtraciones duren años y que los datos de las instituciones sean vulnerables y con ello causar daños irreparables.

Ya no se habla de una guerra cibernética sino de poner la vida en riesgo a través de los artefactos tecnológicos. Esta fusión entre tecnología y ciencia se ha convertido en blanco fácil para los *hackers*. Existen cientos de artefactos que se pueden conectar a internet. Los dispositivos electrónicos se han convertido en el mercado en los más vulnerables para la piratería informática.

La guerra se ha ido transformando a medida que la tecnología avanza, las armas digitales son más difíciles de detectar. En el sistema informático un ataque digital causa inmensos daños y el tiempo de recuperación es largo.

Toda manera de tecnología tiene su propia estructura de conocimiento y se categoriza según la ciencia como, inteligencia artificial. Haugeland lo relacionaba con los sistemas que piensan como seres humanos y decía “El esfuerzo por hacer a las computadoras pensar... máquinas con mentes en el sentido amplio y literal” (1985). Rich y Knight lo asociaba a los sistemas pero que actúan como seres humanos y plasmaban: “El estudio de cómo hacer computadoras que hagan cosas que, de momento, la gente hace mejor” (1991). En otras palabras, esta inteligencia artificial, se convierte en esa nueva tecnología que se relaciona con el proceso cognitivo de los seres humanos.

El conflicto visto como una contraposición entre dos partes, es un escenario que lleva a implementar diferentes estrategias, motivos y tácticas para poder

determinar un ganador, y, permite al individuo desarrollar la capacidad de crear cuerpos de tropa listos para él conflicto. Los ejércitos por mucho tiempo buscaron la supremacía sobre su contrincante como un juego de mesa, o un partido de fútbol, pero claro está, los riesgos eran más altos, era de una derrota simple o de perder con dignidad sino de una consecuencia que ningún ser humano podría imaginar.

En 1914, antes del inicio de la Primera Guerra Mundial, la discusión era acerca de cuál arma era más letal en el campo de batalla: si la bayoneta o el lanzallamas. El conflicto finalizo y después de 4 años, la discusión se centraba en que las ametralladoras habían ganado, los proyectiles que podían viajar a 30 metros de distancia, y claro está, los ataques de armas químicas con gas y cloro, a esto se agregó carros bomba, y aviones bomba.

Con el inicio de la primera Guerra y la confrontación de ejércitos de las potencias militares se da prioridad al avance de la ciencia y tecnología, enfocado en investigación, innovación y desarrollo de artefactos militares, equipos y sistemas que superaran al sistema rival, con ello se buscaba la supremacía militar en el mundo. Pero ¿hasta dónde pretende llegar el ser humano con tal de mantener la supremacía militar y cumplir su meta de ganar?

Algunos avances que han demostrado la aplicación de la ciencia y la tecnología en los conflictos se enuncias así:

- En 1935 con Robert Watson-Watt[1], quien basado en los avances científicos previos, diseño un equipo de detección que permitió a los Ingleses localizar a través de ondas de radio los aviones y submarinos enemigos a 120 kilómetros de distancia.
- En 1960 con el nacimiento del 1ARPAnet hacia una necesidad de una comunicación interna hacia el Departamento de Defensa de los Estados Unidos, pero con el tiempo se convirtió en la 2red de redes acéfala. La investigación militar hacia las grandes innovaciones del siglo XX era tener

[1] Físico Escoces que patento el empleo del RADAR (Radio Detection And Ranging).

conexiones entre las líneas militares que no fueran destruidas. Hoy en día lo conocemos como la ciberguerra.

- Se habla de un debate acerca del uso de las aeronaves no tripuladas (A.R.T), para el ejercicio de la guerra. Los drones, son artefactos que toman vuelo y de ellos surgen unos pequeños dispositivos capaces de vigilar en tiempo real. Pero aquí se evaluará las innovaciones científicas y tecnológicas que ahora se entabla al hablar de invadir a otro Estado.
- Darpa, agencia estadounidense, que se encarga de desarrollar tecnología para uso militar, aprobó la munición de calibre 12,7milimetros que se puede redirigir, la llamaron, Exacto. El proyectil tiene la capacidad para que los francotiradores fijen un objetivo, la bala puede cambiar la trayectoria luego de ser disparada, esto debe ser difícil. Las balas están diseñadas para que cualquier causa natural, por ejemplo, el viento, no pueda interferir en su objetivo.
- Los Robots, son el reemplazo de los soldados, el valor fundamental de las fuerzas armadas es reducir al máximo el riesgo para las vidas humanas. Estas máquinas sustituyen a las personas en forma de rescate. Así como la tecnología inteligente artificial es de gran ayuda también tiene peligros, en mayo del año pasado, *Human Rights Watch* anunció que los robots de combate son capaces de matar humanos si no hay intervención alguna.
- La compañía inglesa *British Aerospace Systems*, *Striker II*, funciona con las características del *Oculus Rift* y los lentes de *Google Glass*. Es un casco de moto, pero es hecha para pilotos capaces de proyectar la información en el visor, en donde muestran datos e imágenes en tiempo real unido a los movimientos de las personas. Está hecho para visión nocturna y diurna para que el piloto pueda realizar maniobras más especializadas.
- Darpa anunció un proyecto que se trataba de estimular la memoria y podría restaurar los recuerdos del individuo, “Si resultaste herido en el cumplimiento de tu deber y no puedes recordar a tu familia, queremos ser capaces de restaurar este tipo de funciones”, El gerente del programa del Darpa, Justin

Sánchez aduce que Después de grandes enfrentamientos en el campo de batalla, el soldado queda con problemas sicológicos de la guerra.

Hoy en día existen armas inteligentes que incluyen tecnología de sensores, microchips y detectores biométricos para tener por seguro que solo el operador autorizado dispare. La Oficina de Investigación Naval de los Estados Unidos declaró que están trabajando en un arma especial que pueda desviar los proyectiles y enfrentar los drones, se están haciendo más frecuentes y con los avances más peligrosos.

Las innovaciones y el desarrollo se agudizan en los peores momentos. Los avances de la ciencia y la tecnología también son claves para el mejoramiento de la medicina y de las telecomunicaciones

Estos avances hicieron que la ciencia y la tecnología fueran fundamentales en el campo de batalla, y no solo eso, sino también la puerta de la nueva era en temas de comunicación. El ingenio y el trabajo son los pilares fundamentales a los que hoy en día se enfrenta: la ciberseguridad.

CIBERSEGURIDAD EN COLOMBIA

Legislación a nivel internacional

En septiembre del año 2013 a nivel internacional, el Consejo de Ministros de Europa le dio su visto bueno a invitar a Colombia en la Convención de Budapest, que hablan sobre los “Delitos Cibernéticos”, es el convenio de carácter global que habla de la protección a la sociedad frente la delincuencia digital, por medio del fortalecimiento de la cooperación internacional. Para Colombia la estrategia es poder formar una ruta para las estrategias operacionales y que no se violen los Derechos Humanos.

En 2014 se acentuó Declaración de la Cumbre de Gales de la OTAN, existen acuerdos que hablan de la ciberseguridad de los países que tienen alianza.

El 20 de marzo de 2015, está la Declaración sobre la protección de infraestructura crítica ante las amenazas emergentes.

La secretaria del CICTE de la OEA, estipula la asistencia que permiten a los Estados americanos miembros a realizar una infraestructura basada en sistemas, redes, funciones, entre otros.

Normas Nacionales y legislación

El desarrollo acelerado de la ingeniería genética, biotecnología, cibernética y telecomunicaciones le ha dado al mundo un giro de 360 grados en las estrategias. Actualmente, los gastos militares se enfocan en las innovaciones y desarrollos en temas de tecnología, en 2005 se gastó 10.000.118.000 millones de dólares. El mayor consumidor fue Estados Unidos, recopilando un 48% de mayor participación. (CONPES 3854, 2016)

La carrera armamentista que hoy en día se presenta un enfoca en 3 direcciones:

· Militarización del espacio extraterrestre.

· Armamento inteligente.

· Desarrollo de tecnologías cibernéticas.

Los avances tecnológicos, el auge del uso de internet y el crecimiento de las transacciones financieras por medio de la red, ha ido incrementando el delito informático, que claro está, amenaza la seguridad, la integridad, la disponibilidad y la confiablidad de los activos información más importantes que se poseen. Con la información no solo se afecta la seguridad de los ciudadanos sino también la del Estado, colocando así en riesgo la infraestructura de las entidades públicas y privadas.

Para analizar las dimensiones de las amenazas a las que hoy en día se enfrenta en el mundo cibernético, el gobierno trabaja con aliados extranjeros, con la finalidad de generar una gobernabilidad en temas de ciberseguridad. Se plantean algunas estrategias, leyes e iniciativas que dan las pautas necesarias para la protección y el fortalecimiento del Estado Colombiano sin que se atente contra la Seguridad y la Defensa Nacional.

La ciberseguridad es el conjunto de acciones que toman los Estados y las personas de manera preventiva y que tienen como fin asegurar el uso de las redes propias y negarlo a terceros.

El Ministerio de las Telecomunicaciones de la Información y la Comunicación (TIC) (2018) lo define como:

> Los vectores de desarrollo que se presentan en el NDI corresponden a directrices marco que se han identificado como prioritarias para Colombia, orientadas a fortalecer la posición del país en términos de Ciberseguridad, alineados con las diferentes estrategias nacionales provenientes desde las entidades del Estado y del sector privado, y que con su fortalecimiento conlleven a mejorar la posición estratégica del país en estos temas.

Como se muestra, los Nodos de innovación (NDI) Buscan las adaptaciones tecnológicas para generar nuevas tecnologías, minimizar los riesgos en temas de cibernética, con el fin de fortalecer las posiciones estratégicas en temas de ciberespacio, enfrentar de una mejor manera los riesgos y las amenazas, y salvaguardar la seguridad de la infraestructura digital del Estado y la protección de los servicios que obtienen los ciudadanos colombianos.

De acuerdo con el aumento revelador del uso de la tecnología y las conexiones a Internet en banda ancha, Colombia en 2010 pasó de tener 2.132.640 millones de conexiones a 5.888.148 millones en 2016 de acuerdo con el informe de estadísticas trimestral del Ministerio de la Información y la Comunicación (MINTIC),

que ha causado bastantes vulnerabilidades a las que ahora se está más expuesto, por ende, es lo que transmite toda la información.

Figura 1: Tabla Internet por Banda Ancha

TRIMESTRE	BANDA ANCHA	BANDA ANGOSTA	TOTAL
2010-1T	2.132.640	212.219	2.344.859
2010-2T	2.306.812	151.840	2.458.652
2010-3T	1.815.810	749.509	2.565.319
2010-4T	1.971.477	704.071	2.675.548
2011-1T	2.056.485	800.746	2.857.231
2011-2T	2.408.667	635.924	3.044.591
2011-3T	2.860.599	360.349	3.220.948
2011-4T	3.050.108	317.053	3.367.161
2012-1T	3.097.861	417.200	3.515.061
2012-2T	3.377.497	222.931	3.600.428
2012-3T	3.560.751	218.405	3.779.156
2012-4T	3.772.471	145.659	3.918.130
2013-1T	4.024.063	90.301	4.114.364
2013-2T	4.235.438	61.120	4.296.558
2013-3T	4.329.914	78.231	4.408.145
2013-4T	4.430.946	66.732	4.497.678
2014-1T	4.632.911	53.872	4.686.783
2014-2T	4.360.620	371.934	4.732.554
2014-3T	4.887.805	44.239	4.932.044
2014-4T	4.936.182	115.383	5.051.565
2015-1T	5.253.961	57.148	5.311.109
2015-2T	5.293.777	56.993	5.350.770
2015-3T	5.397.207	61.571	5.458.778
2015-4T	5.490.534	60.779	5.551.313
2016-1T	5.605.535	61.207	5.666.742
2016-2T	5.713.797	51.073	5.764.870
2016-3T	5.832.329	57.297	5.889.626
2016-4T	5.888.148	48.291	5.936.439

Fuente: Tomado de la página oficial del Ministerio de las TIC – SIUST

CONPES 3701

Teniendo como referencia los ataques cibernéticos en países como Rusia, Estados Unidos, China, Estonia, entre otros. Colombia en julio del 2011 decidió realizar una política para la Ciberseguridad y la Ciberdefensa, con el fin de poder anular las amenazas informáticas, por medio del Consejo Nacional de Política Económica y Social en un documento llamado, CONPES 3701.

El documento CONPES 3701, busca generar lineamientos nacionales de política en Ciberseguridad orientada al desarrollo de una estrategia nacional que anule el incremento de las amenazas cibernéticas, basándose así en 3 de las problemáticas más significativas del país:

1. Falta de coordinación en operaciones en temas de Ciberseguridad y Ciberdefensa.

2. Falta de personal capacitado en especialidades en Ciberseguridad y Ciberdefensa.

3. Debilidad en la regulación y legislación de la protección de información de datos.

Tomando en cuenta estas 3 problemáticas se determinaron 3 objetivos primordiales:

1. Adopción de un marco interinstitucional apropiado para prevenir, coordinar, controlar, generar recomendaciones para afrontar las amenazas y los riesgos que se presenten.

2. Brindar capacitación especializada en seguridad de la información y ampliar las líneas de investigación en Ciberdefensa y Ciberseguridad.

3. Fortalecer la legislación en estas materias, la cooperación internacional y adelantar la adhesión de Colombia a los diferentes instrumentos internacionales.

En primera medida el Gobierno Nacional creó el COLCERT en septiembre de 2011, formado por civiles, militares y otras entidades, su función es coordinar las acciones necesarias para proteger la infraestructura del Estado frente a momentos de emergencia de Ciberseguridad que transgreden la seguridad nacional.

En segunda medida, fue creado el Comando Conjunto Cibernético de las Fuerzas Militares, en cual está conformado por 20 especialistas en sectores de comunicación, ingeniería, aviación e inteligencia, con el fin de preservar la defensa cibernética del Estado, respondiendo a los ataques y asegurar la protección de la infraestructura del Estado, también, en defender la información militar. Como medida de aseguramiento se crearon en el Ejército, Armada y Fuerza Aérea, las Unidades de Comando Cibernético.

En tercera instancia, se creó el Centro Cibernético Policial que se hace responsable de la investigación, prevención y apoyo en los delitos informáticos, cuenta con un comando de Atención Inmediata Virtual (CAI VIRTUAL) para que los ciudadanos puedan hacer denuncias.

Figura 2: Modelo de coordinación intersectorial

Fuente: Tomada del CONPES 3701-Ministerio de Defensa

El Centro Cibernético Policial y el COLCERT trabajan de la mano, debido a que utilizan la información suministrada para identificar perfiles de integrantes no reconocidos y el Centro Cibernético Policial brinda apoyo constante en temas de investigación digital y judicial, esto como medio para involucrar la Ciberseguridad en las entidades del Estado y del sector privado. Este apoyo mutuo invita al país a dar apoyo en otros países de América Latina, de igual manera se ha podido recibir ayuda de las Organizaciones de los Estados Americanos (OEA) por medio del Comité Interamericano contra el Terrorismo (CICTE), con el fin de adelantar grandes esfuerzos y avances al Gobierno para poder prevenir las amenazas cibernéticas.

No obstante, estos esfuerzos fueron dudosos en 2014 cuando el país fue afectado en el ámbito de la ciberseguridad, como es el caso de las intercepciones Andrómeda y el rastreo de los correos electrónicos, chats, personajes, entre otros.

Esto obligó al Estado colombiano a formalizar y doblegar la Comisión Digital, que obedecía de la Agencia Nacional de Seguridad Cibernética.

La Comisión y la Agencia unieron fuerzas públicas y privadas y crearon nuevas políticas en temas de Ciberdefensa y de Ciberseguridad para Colombia, dado que acordaron implementar convenios internacionales para la ciudadanía en torno a la seguridad digital.

Por medio de la Organización de los Estados Americanos (OEA), países como Canadá, España, Estados Unidos, Reino Unido, República Dominicana, Estonia, Israel, Corea del Sur y Uruguay en marzo de 2014, analizaron los temas de Ciberseguridad para Colombia y llegaron a la conclusión que, en el ámbito de estrategias, operatividad y de coordinación, Colombia necesitaba un lineamiento más específico en temas de seguridad digital.

Si bien se puede ignorar las circunstancias que obligan a los Estados a tomar medidas estratégicas para contrarrestar estos ataques. Es aquí en donde se toma el documento CONPES, y se asocia con las causas del porqué el fortalecimiento en temas de Ciberseguridad.

CONPES 3854

El documento CONPES 3854 en el que señala la Política Nacional de Seguridad Digital, fue aprobada el 11 de abril de 2016, el cual adopta la gestión de riesgo como médula central. Esta política busca nivelar al país con los avances digitales, y así evitar las amenazas, hurto de dinero en las transacciones *online*, suplantación, pérdida de información, entre otros.

El CONPES 3854, cuenta con fortalecer las múltiples identidades de gestión para atenuar los riesgos de la seguridad digital en sus formaciones económicas y sociales en todo el mundo digital, tomando en cuenta la educación, la regulación, la cooperación, desarrollo, investigación e innovación, esto con el fin de luchar contra

el crimen en internet, dar auge a la economía nacional digital y a la vez sobrellevar la prosperidad del país.

Cuenta con 5 planes de acción:

1. Establecer un marco institucional claro en torno a la seguridad digital, basado en la gestión de riesgos.
2. Crear las condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital.
3. Fortalecer la seguridad de los individuos y del Estado en el entorno digital, a nivel nacional y trasnacional, con un enfoque de gestión de riesgos.
4. Fortalecer la defensa y soberanía nacional en el entorno digital con un enfoque de gestión de riesgos.
5. Impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional.

Para realizar este plan de acción que se ejecutará en un tiempo de 3 años (2016-2019) con una inversión de 85.070 millones de pesos. El Ministerio de Tecnología de la Información y la Comunicación, el Ministerio de Defensa Nacional, la Dirección Nacional de Inteligencia y el Departamento Nacional de Planeación serán las entidades operadoras para ello.

Según el informe de la Política Nacional de Seguridad Digital se estima que si esa implementación resulta acertada, en el año 2020 impactara de manera positiva la economía colombiana, generando 307.000 empleos con un aproximado del 0,1% del Producto Interno Bruto (PIB).

LEGISLACIÓN EN TEMAS DE CIBERSEGURIDAD EN COLOMBIA

Legislación a nivel nacional

Existen fundamentos constitucionales con base a la seguridad digital:

Art 2, fin esencial del Estado la prosperidad general y garantizar a los ciudadanos la efectividad de los principios, derechos y deberes.

Art 15, reconoce el derecho a la intimidad personal y familiar y al buen nombre, y la obligación del Estado de respetarlos y hacerlos respetar.

Art 20, se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación.

Art 76, el espectro electromagnético es un bien público inajenable e imprescriptible sujeto a la gestión y control del Estado.

Art 101, espectro electromagnético como parte del territorio colombiano.

Art 217, establece que las Fuerzas Militares tendrán como finalidad primordial la defensa de la soberanía, la independencia, la integridad del territorio nacional y del orden constitucional.

En el documento CONPES 3701, uno de sus principales objetivos es fortalecer la legislación colombiana en temas de seguridad digital, es por esto que

en carácter jurídico existe la Ley 1273 del 2009, que habla de la protección informática y de los datos para preservar integralmente los sistemas en los que el uso de las tecnologías de la información y la comunicación estén salvaguardados. Sin embargo, cuenta con una legislación procesal penal integral y efectiva para emprender delitos cibernéticos y reconoce los tratados internacionales de la INTERPOL y EUROPOL.

La Ley 1581, marco básico para proteger los datos, divulgación y denuncias de las violaciones en la seguridad.

Por otro lado, en enero de 2013 nace la Comisión Digital y de información estatal del Documento CONPES 3701, el cual orienta y coordina el uso de la infraestructura tecnológica para la interacción de los ciudadanos y el uso efectivo de la información en el Estado, emitiendo así Grupos de Respuesta de emergencias Cibernéticas en Colombia dentro de los lineamientos del Ministerio de Defesa en materia de tecnología.

Gobierno en Línea, del Ministerio de las TICs en su Manual 3.0, realizó una especie de seguimiento en la ciberseguridad para implementar estándares internacionales en el sector público.

No obstante, el avance tecnológico es preocupante y la legislación se va quedando atrás, es por ello, que se deben crear normas para atacar delitos cibernéticos que surgen en el momento de la situación.

Delitos más comunes

Tabla 1 Los virus más destructivos en la red

Virus	Año de aparición	
Iloveyou	2000	Sus creadores son: Reonel Ramones y Onel de Guzmán. Causo daños en os sistemas informáticos de todo el mudo, un total de $10 mil millones de dólares. Modo de uso: utiliza la red social para que la gente pueda abrir un archivo adjunto, forma de carta de amor. el archivo adjunto era en realidad una secuencia de comandos que se hace pasar por un archivo TXT, el cual ocultaba la extensión real del archivo. Una vez se hace clic, se enviará en sí a todo el mundo en la lista de correo del usuario y procede a sobrescribir archivos, por lo que el equipo deja de funcionar correctamente. (HostDime, 2014)
Code Red	2001	Fue descubierto por dos empleados de eEye Digital Security. Se infecta y empieza a crear copias de sí mismo, luego empieza a tener un ataque de denegación de servicio en diferentes direcciones IP. Se puede robar más de $dos mil millones de dólares.
Melissa	1999	Su creador fue David L. Smith. Inicia en descargar un documento Word, que supuestamente contiene una lista de contraseñas a sitios de adultos. La gente lo abre y es un virus que evia el mismo archivo a 50 personas de la libreta personal de la personal, esto hace que exista una interrupción en los servicios electrónicos de los gobiernos y de las corporaciones.
Sasser	2004	Su creador fue un estudiante de ciencias de la computación, Steven Jaschan.

	Este virus aprovecha la vulnerabilidad de los servicios de autoridad de las seguridades locales, a la cual conecta directamente con las cuentas.

Fuente: Tomado de (Hostdime, 2014)

CONCLUSIONES

Tomando como referencia la vulnerabilidad que tiene Colombia en el ciberespacio hace falta una mayor partición en cooperación internacional, esto para construir una administración más sólida, sin embargo, se observa que existen los Estados fuertes y con alta concentración en armamento cibernético, la asimetría en el poder es notoria**.** Los dispositivos de seguridad hacen esfuerzos para poder regular o disminuir el impacto de estos ataques en la red, no obstante, se deben tomar medidas más rigurosas para debilitar/evitar un ciberataque.

En los últimos años las tecnologías de la información y de la comunicación en Colombia han implementado diferentes controles en temas de ciberseguridad y de ciberdefensa, sin embargo, es importante que se continúe trabajando en temas de seguridad virtual, tanto en el sector público y privado, tomado de la mano con las ayudas internacionales.

Las amenazas que el mundo presenta en temas de ciberseguridad están cada vez más fuertes, es por ello, que se necesitan nuevas infraestructuras en seguridad con un buen financiamiento que permitan una actuación adecuada para contrarrestar o evitar un posible ataque y así poder prevenir los incidentes y estar más atentos en temas de defensa.

El crecimiento en la superioridad de la tecnología no se logra si no se dispone de una industria nacional más avanzada y de defensa impulsada a la protección de infraestructuras de comunicación y políticas exclusivas de seguridad informática, en el espacio y aún más en la falta de cooperación en poder construir una

administración más amena en temas de declive informática, y fuertes en los avances que las Fuerzas Militares toman y han venido trabajando para poder tener una seguridad más amplia y correcta.

Es claro evidenciar que el eslabón más débil son las personas, es por ello, que se debe trabajar de manera meticulosa y constante con los ciudadanos acerca del poder de la información y concientizarlos acerca de la ciberseguridad y el impacto que genera, es por ello, que se debe de tener capacidad de prevención y en caso necesario de ataque en vez de defensa, de esta manera se puede disminuir la vulnerabilidad en las infraestructuras que pueden estar afectadas.

Colombia ha progresado en los temas de ciberseguridad y de ciberdefensa. Hace 7 años que se han venido gestionando los temas de protección a la información en la red, y como esto pone sensibilidad a los ciudadanos, no obstante, el gobierno debe trabajar y mejorar en la creación de nuevas defensas e infraestructura a la hora de enfrentar un delito informático. De la misma manera generar políticas de información hacia la población manteniéndolos al tanto del riesgo frente a cualquier tipo de vulnerabilidad o amenaza cibernética. Al paralelismo estratégico, es importante garantizar las nuevas comunicaciones en estrategia de prevención con información compartida, alertas, procesos, entre otros. Es necesario dar a conocer la gestión de riesgos que tiene la ciberseguridad.

Bibliografías

- s.n. (2012). *¿Qué es la Inteligencia Artificial?* Recuperado de: http://www.cs.upc.edu/~bejar/ia/transpas/teoria/1-IA-introduccion.pdf
- Bernardo, A. (2015*). La ciencia y la tecnología en los tiempos de guerra*. Blogthinkbig. Recuperado de: https://blogthinkbig.com/la-ciencia-en-guerra
- Cromo (2014), *ciencia y tecnología al servicio de la guerra*. Recuperado de: https://www.cromo.com.uy/ciencia-y-tecnologia-al-servicio-la-guerra-n575247
- Clarke, R. & Knake, R. (2011). Guerra en la red, los nuevos campos de batalla. Barcelona. Editorial Planeta.
- Almenara, J. (2007). *Las necesidades de las TIC en el ámbito educativo: oportunidades, riesgos y necesidades*. Universidad de Sevilla. España. Recuperado de: http://cmapspublic2.ihmc.us/rid=1M92QZKRZ-XM42B8-1QZZ/caberne.pdf
- López, D. (s.f). CONPES 3701: *Colombia hacia un futuro con ciberseguridad y ciberdefensa*. Universidad Piloto de Colombia. Bogotá. Recuperado de: http://polux.unipiloto.edu.co:8080/00002383.pdf
- Departamento Nacional de Planeación. (2016). Documento CONPES 3854.Recupera de: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf
- Hostdime. (2014). *Los 5 virus informáticos más destructivos de todos los tiempos*. Premier Globla Data Centers. Recuperado de: http://blog.hostdime.com.co/los-5-virus-informaticos-mas-destructivos-de-todos-los-tiempos/