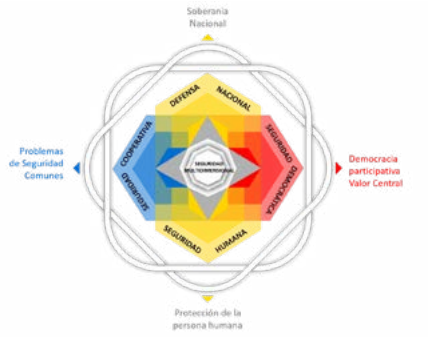
Estrategia Nacional de **Ciberdefensa y Ciberseguridad**

- ECDCS -

2020-2030

Estrategia Nacional de Ciberdefensa y Ciberseguridad - ECDCS - 2020-2030

MINISTERIO DE DEFENSA NACIONAL
COMANDO GENERAL FUERZAS MILITARES
ESCUELA SUPERIOR DE GUERRA



Estrategia Nacional de Ciberdefensa y Ciberseguridad - ECDCS
Escuela Superior de Guerra ¨General Rafael Reyes Prieto¨ - ESDEG
Departamento Curso de Altos Estudios Militares y Curso Integral de Defensa Nacional (CAEM –CIDENAL) Carrera 11 No. 102-50 Bogotá D.C., Colombia

Editores
Mayor General Helder Fernán Giraldo Bonilla
Director Escuela Superior de Guerra

Brigadier General (RA) Fabricio Cabrera Ortiz
Jefe Departamento CAEM CIDENAL

Autores

Curso de Altos Estudios Militares No.61

Estudiantes internacionales:
CR. Glauco Corbari Corrêa (Ejército Brasileño)
CR. Carlos Roberto Alvarez Astengo (Fuerza Aérea del Perú)

Estudiante nacionales:
CR. David Leonardo Gómez Pulido (Ejército Nacional)
CR. Royer Gómez Herrera (Ejército Nacional)
CR. Raul Fernando Vargas Idárraga (Ejército Nacional)
CR. Juan Jaime Martínez Ossa (Fuerza Aérea Colombiana)

Estudiantes Curso Integral de Defensa Nacional No. 47
CR. Oscar Antonio Moreno Miranda (Policia Nacional)
CR. Luis Carlos Hernández Aldana (Policía Nacional)
Pilar Acero González
Angela María Durán Niño
Juliana Andrea Ferreira Aldana
Eduardo Lleras Losada
Juan Carlos Moscote Gnecco
María Mercedes Osorio Rodríguez
Jorge Arturo Ramos Valenzuela
Hugo Alejandro Saavedra León
Diego Jesús Tovar Novoa

Diseño y Diagramación
Antonio José Rosero Torres
José Noel Muñetón Medina

Corrección de estilo
Giovana Elisabeth Román Robayo

Asistentes editoriales
Mayor Gregorio Niño Rodríguez
María Johanna Alarcón Moreno

ISBN: 978-958-52545-5-8
Primera edición: Septiembre 2020
Bogotá DC. - Colombia

Impresión
Opciones Gráficas Editores Ltda.
www.opcionesgraficas.com

Contenido

Resumen ejecutivo

La Estrategia de Ciberdefensa y Ciberseguridad establece los lineamientos para desarrollar capacidades ofensivas, defensivas, disuasivas y de inteligencia para la protección del Estado, definiendo estándares y compromisos para asegurar el manejo de la información digital como una forma de gestionar y mitigar el riesgo frente a un ciberataque, manteniendo la capacidad de resiliencia para responder, recuperar y restaurar las áreas afectadas.

La Estrategia se centra en la integración, interacción y cooperación entre el sector público y privado de manera transversal, comprometiendo todos los campos político, económico, sicosocial y militar. Integra aspectos legales y estratégicos y la coordinación internacional con énfasis en dos áreas: tecnológico y judicial.

Define riesgos, amenazas y desafíos; traza un límite no superior al 2024 para el desarrollo de la industria digital nacional y la gobernanza del internet, teniendo en cuenta los cinco pilares establecidos por la Unión Internacional de Telecomunicaciones: medidas legales; medidas técnicas; medidas organizacionales; capacidades de construcción y desarrollo; y medidas de cooperación..

Así mismo, se considera de vital importancia establecer el diseño específico de los diferentes planes de carrera y de capacitación al interior de cada una de las instituciones, lo que finalmente, nos permitirá fortalecer los mecanismos defensivos en Ciberdefensa y Ciberseguridad en nuestro país.

CAPÍTULO
UNO

INTRODUCCIÓN

Introducción

Ante los retos que demanda la acelerada transformación digital, caracterizada por un ambiente volátil, incierto, complejo y ambiguo, que amenaza la Seguridad y Defensa Nacional, como consecuencia del riesgo latente por el uso del Ciberespacio, riesgo que se extiende no solo al componente estatal, sino a diversos actores no estatales, primordiales para el desarrollo de la nación; la Estrategia de Ciberdefensa y Ciberseguridad (ECDCS), se constituye en una apuesta por redefinir el concepto del alcance y postura del Estado, a través de una Estrategia que tiene como estructura central un componente integrador, desde la cooperación entre el sector público y privado.

La transversalidad que caracteriza la presente Estrategia de Ciberdefensa y Ciberseguridad tiene su origen en la alineación y convergencia con las directrices emanadas del Sistema de Seguridad Nacional, fundamentadas en la Constitución Política de Colombia, Plan Nacional de Desarrollo y su relación con la Seguridad Nacional, la Política de defensa y Seguridad nacional, la Apreciación Política Estratégica Nacional (APEN) y la Estrategia multidimensional de Seguridad Nacional (EMSN). Entender que la (ECDCS) se extiende más allá del campo tecnológico y abarca todos los campos del poder nacional político, económico, sicosocial y militar, nos dará la llave para abrir la puerta de la integración e interacción de las entidades estatales con el sector privado y la ciudadanía en general.

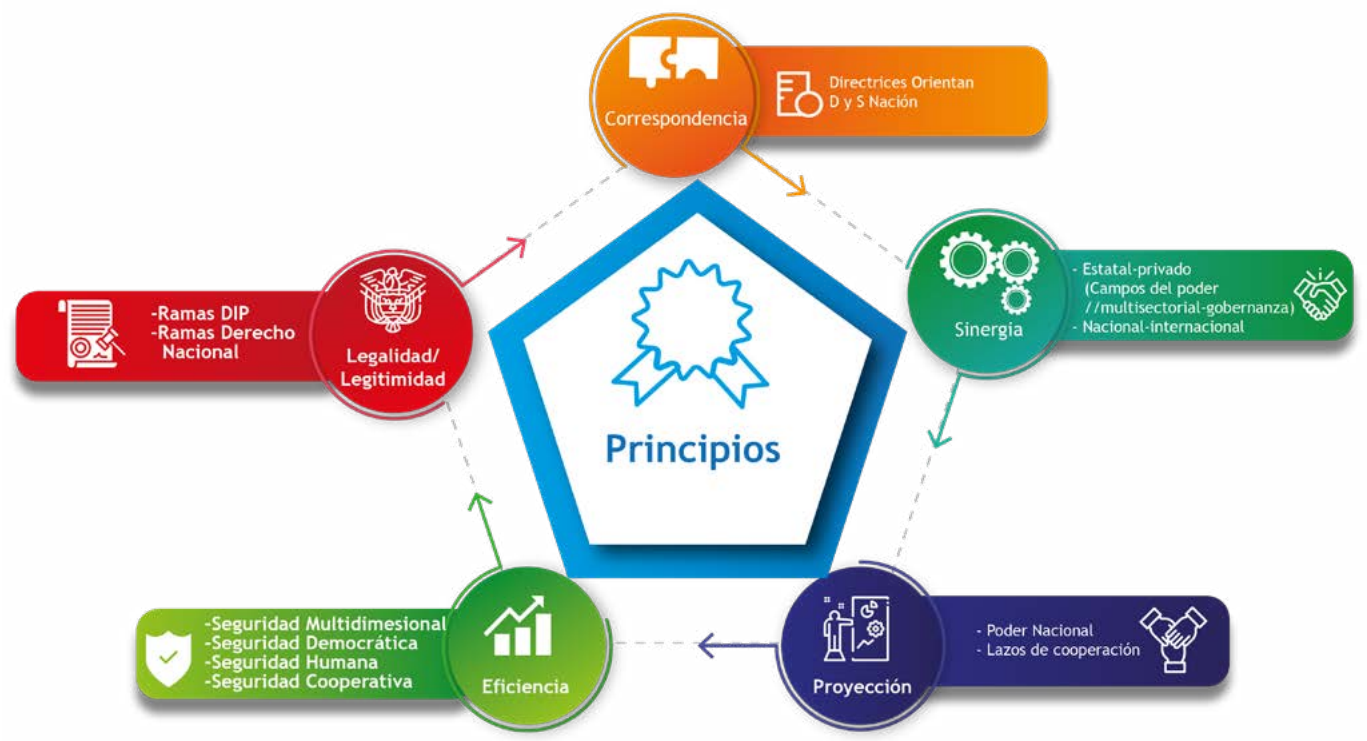
El peligro que implica el uso del Ciberespacio por actores antagónicos significa un riesgo latente para los intereses nacionales estrechamente relacionados con los imperativos geopolíticos; los intereses nacionales se clasifican en vitales, estratégicos y transitorios; la ECDCS, busca establecer lineamientos y una orientación para desarrollar capacidades ofensivas, defensivas, disuasivas y de inteligencia para la protección del Estado, y en atención a la inevitable interconexión característica de este mundo globalizado, cobra aún más importancia establecer unos estándares y compromisos para el aseguramiento del manejo de información digital como una forma de gestionar y mitigar el riesgo, y en caso de que ocurra un ciberataque con éxito, tener una gran capacidad de resiliencia que permita mantener, responder, recuperar y restaurar áreas afectadas .

La amalgama entre lo público y privado, demandan el diseño de un modelo de gobernanza en temas de Ciberdefensa y Ciberseguridad, implica una combinación de capacidades para proteger la seguridad de los usuarios del ciberespacio, ante una amenaza que combina actores estatales y no estatales. La cooperación se constituye en un factor clave al momento de diseñar una arquitectura transversal de CDCS, que permita mitigar los riesgos del Ciberespacio. Un ciberconflicto, contempla ciberactividades, ciberoperaciones, ciberataques y ciberguerra; el camino para afectar el Estado, no siempre inicia con una acción directa sobre el mismo, el ámbito del Ciberespacio es tan complejo y variado como las posibilidades y objetivos que motivan realizar ataques, cada vez más sofisticados.

La ECDCS, es un componente nuevo de la Estrategia que por su transversalidad se situa en el orden del primer y segundo nivel, demanda que su diseño tenga una alineación estratégica armonizada con los principios formulados en la Estrategia de Seguridad Nacional, con un análisis riguroso del entorno global y regional, una introspección incluyente de actores que de una u otra forma participen en el entramado digital en el contexto nacional, sumado a la necesidad de definir con exactitud los riesgos, amenazas y desafíos, los cuales permitirán establecer unos objetivos y líneas de acción coherentes y transversales para gestionar un ciberespacio más seguro, con la libertad y restricciones que demanda garantizar la seguridad de los conciudanos.

Los principios son fundamentales para la ECDCS, toda vez que se constituyen en los parámetros sobre los cuales orbita de manera sincrónica con la Estrategia de Seguridad Nacional y su transversalización con las directrices emanadas por el Estado relacionadas con la Seguridad y Defensa de la Nación.

Principios para la ECDCS



a. Correspondencia.

La ECDCS, debe estar en concordancia, con las directrices que orientan la Defensa y Seguridad de la Nación: Constitución Política de Colombia, Plan Nacional de Desarrollo, Política de Defensa y Seguridad, Estrategia Multidimensional y los CONPES 3701 “, para la búsqueda de una simetría y complementación que conduzcan a la gestión de un Ciberespacio mas libre y seguro.

b. Sinergia.

La estructura transversal de la ECDCS se basa en la cooperación entre el sector estatal y el privado, y un alto componente de coordinación internacional y nacional con especial énfasis en dos áreas: tecnológico y judicial. La ECDCS involucra la totalidad de los campos del poder nacional: político, económico, sicosocial y militar. El

involucramiento, la participación y aporte multisectorial desde diversas competencias, permite una mayor cobertura y de paso minimizar las probabilidades de áreas frágiles en ese gran circuito de interconexión abierta. En atención a la naturaleza del Ciberespacio, es fundamental generar las condiciones para que a través de una verdadera Gobernanza se amplié el ámbito de participación de diferentes actores con intereses en la seguridad del Ciberespacio. Definir el aporte multisectorial

c. Proyección.

La ECDCS, por ser una estrategia transversal, impacta los cuatro elementos del poder nacional -político, económico, sicosocial y militar-, buscar estructurar un sistema de previsión y respuesta adecuada a las amenazas latentes en el Ciberespacio; fomenta los lazos de cooperación, a través de la coordinación, integración, articulación y sincronización. El trabajo mancomunado es la esencia para mitigar los riesgos que se desprenden de la interconexión digital.

d. Eficiencia.

La ECDCS, alineada con otras Estrategias relacionadas con la Seguridad y Defensa de la Nación, incorpora los componentes de la seguridad multidimensional - seguridad democrática, seguridad humana, seguridad cooperativa -, bajo la premisa de considerar un alcance amplio con el máximo aprovechamiento de recursos limitados y medios disponibles. En la medida en que haya una sumatoria equilibrada y articulada de esfuerzo de los intervinientes en la ECDCS, habrá un uso racional del presupuesto y de los medios destinados a la seguridad del Ciberespacio.

e. Legalidad / Legitimidad.

El ciberespacio involucra diversidad de actores, estatales y no estatales, actores internos y externos, en ese orden de ideas adaptar las diferentes ramas del derecho internacional público e integrarlas con las ramas del derecho nacional, siempre bajo la premisa de actuar conforme al marco normativo y legal de la nación, se constituye en la hoja de ruta de la ECDCS.

CAPÍTULO
DOS

CONTEXTO GLOBAL Y SU RELACIÓN CON COLOMBIA

Contexto global y su relación con Colombia

La expansión de internet y del uso de las tecnologías de la información y la comunicación (TIC) durante los últimos años permiten, como nunca, la circulación de ingentes volúmenes de información y el establecimiento de comunicaciones de manera rápida y fácil. En mayor medida las actividades sociales, económicas e incluso militares de un Estado se hacen más dependientes del uso de las TIC, lo que implica una mayor vulnerabilidad y exposición a los ciberataques.

2.1. Ciberdefensa y ciberseguridad en el mundo

A nivel mundial existen diferentes tipos de actores, organizaciones y estados, que desarrollan diferentes acciones para permitir el uso seguro de las TIC, mediante el establecimiento de acuerdos de cooperación y asesoramiento que fijen el cumplimiento de determinados estándares a nivel internacional, o mediante el establecimiento de políticas que regulen esta actividad.

Resulta importante indicar que Colombia es uno de los 20 países que conforman este Grupo de Expertos Gubernamentales

El Foro de la Cumbre Mundial de la Sociedad de la Información (CMSI) es una plataforma mundial de la Organización de las Naciones Unidas (ONU), representa la mayor reunión mundial de la comunidad de las TIC que busca con el empleo de estas tecnologías avanzar para alcanzar los Objetivos de Desarrollo Sostenible (ODS). Para contribuir al logro de los ODS la CMSI diseño 11 líneas de acción, siendo la quinta (fomentar la confianza y la seguridad en el uso de las TIC) y la sexta (ambiente posibilitador) los directamente relacionados con aspectos de ciberseguridad, la gobernanza en ***internet***, y los roles y responsabilidades de los gobiernos en ***internet*** (CMSI, 2019).

El Grupo de Expertos Gubernamentales en Seguridad de Información (Group of Governmental Experts on Information Security, GGE) en Ciberseguridad de la ONU, en sus informes de los años 2010, 2013 y 2015, presento un diagnóstico del impacto de las TIC en la paz y seguridad internacional, identificando amenazas y riesgos

emergentes en el empleo extensivo de las tecnologías digitales de información; y propuso a la vez una serie de medidas y acciones que los Estados podrían desarrollar para contener estas amenazas y riesgos. Resulta importante indicar que Colombia es uno de los 20 países que conforman este Grupo de Expertos Gubernamentales, y que en el Informe del Secretario General sobre ***los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional*, del 24 de junio del 2019, se encuentra la respuesta del gobierno colombiano sobre este tema** (Asamblea General de las Naciones Unidas- AGNU, 2019).

El Foro para la Gobernanza de Internet (***Internet Governance Forum***, en adelante IGF), se reúne anualmente desde el año 2006, la decimocuarta reunión anual del Foro fue organizada por el Gobierno de Alemania en Berlín, del 25 al 29 de noviembre de 2019, bajo el tema general: ***Un mundo. Una red. Una visión*. El programa de la reunión desarrollo paneles que trataron sobre temas relacionados a la gobernanza, seguridad, estabilidad y resiliencia de datos en internet (IGF, 2019).**

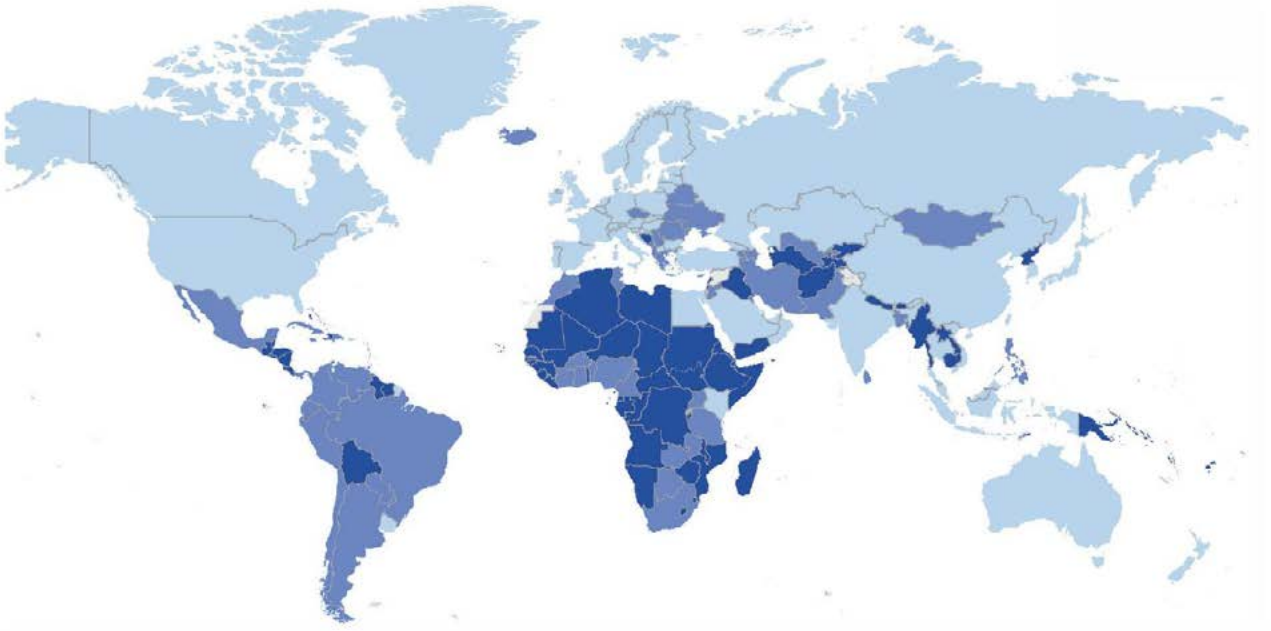
El Foro Económico Mundial (World Economic Forum - WEF) define como factores claves para el desarrollo tecnológico y económico a la resiliencia y la seguridad cibernética. El Concejo de la Agenda Global en Ciberseguridad presento en abril de 2016 su Libro Blanco donde se señalan tensiones existentes entre los sectores público y privado, que dificultan la colaboración y la adopción de medidas de ciberseguridad (WEF, 2016).

El WEF identifica en su Informe de Riesgo Global 2020 dentro de los 10 principales riesgos en términos de probabilidad al fraude y robo de datos en el sexto lugar y a los ciberataques en el séptimo lugar; en cuanto a los 10 principales riesgos en términos de impacto ubica al colapso de la infraestructura de información en el sexto lugar y a los ciberataques en el octavo lugar; asimismo advierte sobre una ***nueva carrera armamentista digital*, en la que el ciberespacio se ha convertido en una extensión del dominio militar, desencadenando nuevas carreras tecnológicas de armas (WEF, 2020).**

La Unión Internacional de Telecomunicaciones (International Telecommunications Union - ITU), publica el Índice Global de Ciberseguridad, que mide el compromiso de los países en ciberseguridad evaluándolos según una serie de indicadores agrupados en cinco pilares: medidas legales; medidas técnicas; medidas organizacionales; capacidades de construcción y desarrollo; y medidas de cooperación. Los países son clasificados según su nivel de compromiso en: alto, medio y bajo (ITU, 2020).

En el Índice Global de Ciberseguridad del año 2018, Colombia se encuentra dentro de los países con un nivel de compromiso *medio*, **ocupando el puesto 73 de 175 países evaluados (ITU, 2019).**

Mapa de Calor de Compromiso en Ciberseguridad por Países



Los países se clasifican según su nivel de compromiso: alto, medio y bajo.

Nivel de Compromiso Alto
Países que demuestran un alto compromiso en los cinco pilares del índice.

Nivel de Compromiso Medio
Países que han desarrollado acuerdos complejos y participan en programas e iniciativas de ciberseguridad.

Nivel de Compromiso Bajo
Países que han comenzado a iniciar compromisos en ciberseguridad.

Fuente: Global Cybersecurity Index (GCI) 2018

En abril del presente año, la Organización para la Cooperación y Desarrollo Económicos (OCDE), le dio la bienvenida a Colombia como nuevo miembro de esa organización, luego de un proceso de adhesión que inicio el 2013. En el año 2016, Colombia junto a los países miembros de OCDE de entonces y otros siete países, firmo la Declaración de la Reunión Ministerial de Economía Digital de la OCDE de Cancún, de acuerdo con ella los países firmantes se comprometieron trabajar juntos para preservar la apertura del ***internet***, disminuir las brechas digitales, promover las habilidades digitales y en general hacer más para aprovechar el potencial de la economía digital (OCDE, 2016). En lo relacionado a ciberseguridad, los países firmantes declararon:

- Promoveremos la gestión del riesgo de seguridad digital y la protección de la privacidad al más alto nivel decisorio**, con el fin de reforzar la confianza y establecer, a estos efectos, estrategias de colaboración que reconozcan que la trascendencia de estas cuestiones para la prosperidad económica y social, apoyen la implantación de prácticas coherentes de gestión de los riesgos de seguridad digital y privacidad, con especial atención a la libertad de expresión y a las necesidades de las pequeñas y medianas empresas y de los particulares, incentiven la investigación y la innovación y promuevan una política general de rendición de cuentas y transparencia; y**

- Estimularemos el comercio electrónico y contribuiremos a reducir impedimentos al mismo dentro y a través de las fronteras **en beneficio de los consumidores y empresas, mediante la adopción de políticas y marcos reguladores que refuercen la confianza de los consumidores y la seguridad de los productos, fomenten la competencia y la innovación orientada a los consumidores, y favorezcan la cooperación entre las autoridades de defensa de los consumidores y otras autoridades competentes dentro de y entre los países.**

Con respecto a los Estados Unidos (EE.UU.)**,** en septiembre de 2018, el Presidente Donald Trump firmó la Estrategia Cibernética Nacional, la primera estrategia cibernética totalmente articulada para EE.UU. desde 2003 (Presidente de los Estados Unidos de América, 2018).

Entre los hitos importantes para el desarrollo de las capacidades cibernéticas ofensivas de los EE.UU., se encuentra el reconocimiento por la Organización del

Tratado del Atlántico Norte (OTAN), de la cual Colombia hace parte como socio global, del ciberespacio como un dominio para las operaciones militares en su Cumbre de Varsovia, en 2016. La nueva Estrategia de Ciberdefensa de los EE.UU. responde a esta mayor agresividad que demanda la confrontación geopolítica con China y Rusia y en ella se pide al Departamento de Defensa que compita, disuada y gane en el dominio del ciberespacio (Departamento de Defensa de los EE.UU., 2018). Se pide a las fuerzas de ciberdefensa que se preparen para la guerra y construyan una fuerza más letal, que establezcan alianzas y asaciaciones y que compitan y disuadan activamente a sus rivales. La nueva Estrategia amplía el campo de la disuasión a la protección de las infraestructuras críticas, lo que se entiende que afecta a las acciones ofensivas, porque de las defensivas ya se encarga el Departamento de Seguridad Interior (Arteaga, 2019).

Ahora hablando de China, la primera regulación integral de China sobre privacidad y seguridad digital, la Ley de Seguridad Cibernética (LSC) **se aprobó el 7 de noviembre de 2016 y entró en vigencia por primera vez el 1 de junio de 2017. Desde entonces, ha habido una aplicación esporádica de ciertos artículos de la ley, mientras que otros están siendo con menos frecuencia** (Edwards, 2019).

La enorme distancia que separa la cultura del País asiático de la cultura occidental limita la posibilidad de poder utilizar totalmente esta norma como referencia para el desarrollo de nuevas normativas nacionales en otros países (Morán, 2017), como en Colombia, por ejemplo. Sin embargo, no es esfuerzo inútil recorrer la LSC para identificar problemas latentes que deben ser tratados con las distintas aproximaciones compatibles con el sistema legislativo del País en cuestión.

Se destaca en la estrategia de China sobre seguridad cibernética la creación de un ciberespacio abierto, legalizado, seguro y pacífico. Además, según la LSC, China debe cooperar con otros países en estos temas, haciendo lo posible para proteger la seguridad de la información del País y de sus ciudadanos, pero defendiendo su soberanía, seguridad nacional y su infraestructura de información (Geopolitica.ru, 2016).

Para sintetizar brevemente la Estrategia de China para Ciberdefensa y Ciberseguridad, se puede describir sus objetivos de la siguiente manera: salvaguardar la soberanía en el ciberespacio; gobernanza mundial justa y transparente; libre flujo de la información bajo los parámetros chinos; y la no injerencia en los asuntos de otro Estado (Schreiber, 2019).

Delante de este contexto, se concluye que las Estrategias Cibernéticas de otros países, así como las orientaciones y directivas de organizaciones de ámbito mundial, pueden contribuir no solo al análisis, sino también a la construcción de una Estrategia sólida y sinérgica por parte de Colombia.

2.2. Ciberdefensa y ciberseguridad en el hemisferio

Si es posible aceptar la existencia de un espacio geográfico cibernético, también es posible hablar de una geopolítica cibernética, con características específicas en cada lugar y de acuerdo con los actores involucrados y las políticas que lo manejan, así como conflictos, crímenes, delitos, políticas y estrategias diseñadas para gestionar, proteger, expandir, atacar, es decir, políticas y relaciones de poder en y para el ciberespacio (Gonzales & Portela, 2018). Y en el caso del hemisferio sur, y especialmente en América del Sur, no es diferente.

Aunque el tema cibernético no respeta las fronteras políticas, se puede ver que en el espacio sudamericano todavía es tratado principalmente dentro de las fronteras de los estados-nación, como un asunto interno. Algunas iniciativas, como los Planes de Acción de 2012 y 2013 de la Unión de Naciones Suramericanas (UNASUR), que propusieron la creación de un grupo de trabajo para evaluar la viabilidad de establecer políticas y mecanismos regionales para enfrentar las amenazas cibernéticas o informáticas en el campo de la defensa, son ejemplos. Sin embargo, aún no hay efectividad en las políticas promovidas, en el sentido de crear una conformación regional, aunque tampoco se verificó la resurrección de una vieja agenda en las relaciones de poder, teniendo en el ciberespacio el catalizador de posibles obstáculos que conducen a litigios cibernéticos entre los estados (Gonzales & Portela, 2018).

La OCDE y el Banco Interamericano de Desarrollo (en adelante, BID) publicaron de manera conjunta el manual Políticas de Banda Ancha para América Latina y el Caribe, que dedica capítulos sobre el gobierno digital, la protección del consumidor y comercio electrónico, la gestión de riesgo de seguridad digital y la protección de la privacidad, los cuales contienen aspectos que son de interés de la ciberseguridad (OCDE & BID, 2016).

La Agenda Digital para América Latina y el Caribe (eLAC) fijada en la Quinta Conferencia Ministerial sobre la Sociedad de la Información de América Latina y el Caribe, de agosto del 2015, cuenta con cinco áreas de acción. Dentro de la quinta área de acción Gobernanza para la Sociedad de la Información**, en aspectos de ciberseguridad destacan los siguientes objetivos** (Comisión Económica para América Latina y el Caribe- CEPAL, 2015):

Objetivo 19: Promover la seguridad y la confianza en el uso de Internet, garantizando el derecho a la privacidad y la protección de los datos personales.; y confianza en el uso de internet; y

Objetivo 20: Prevenir y combatir el cibercrimen mediante estrategias y políticas de ciberseguridad, la actualización de legislación y el fortalecimiento de capacidades. Promover la coordinación local y regional entre equipos de respuesta a incidentes informáticos

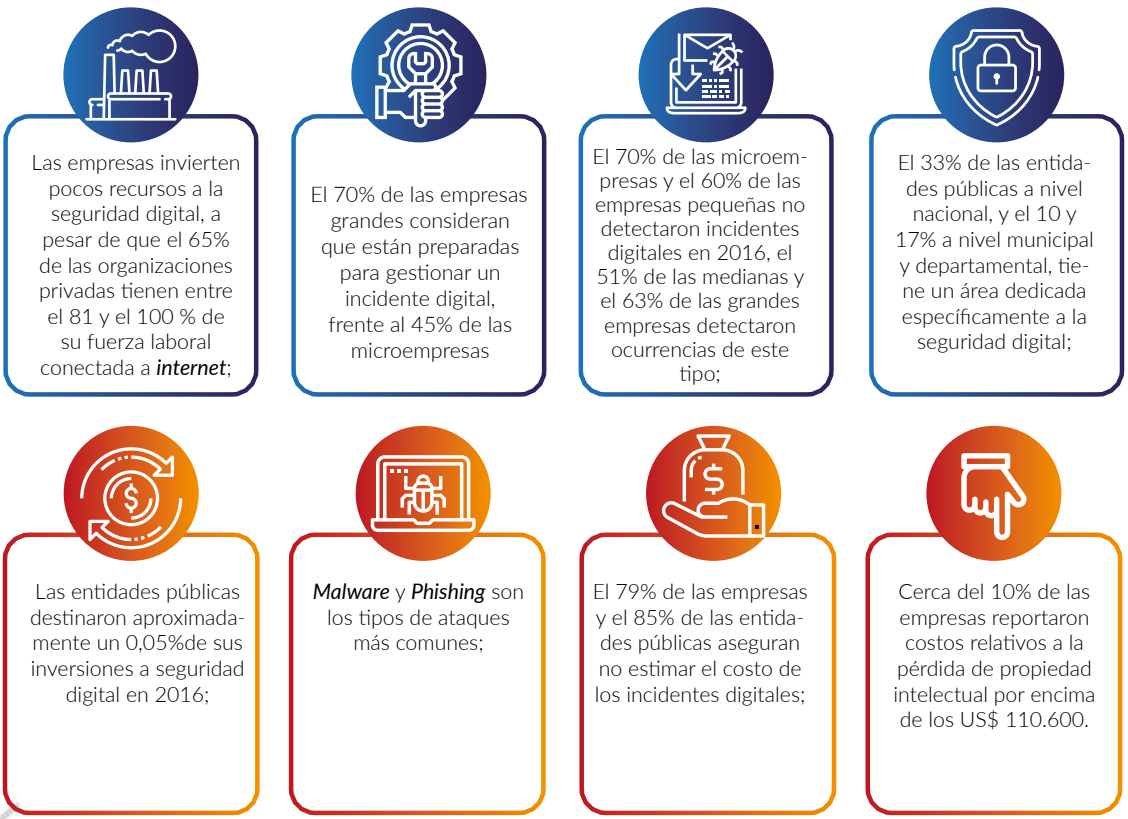
El Informe 2016 del Observatorio de la Ciberseguridad en América Latina y el Caribe es el resultado de una colaboración entre BID, la Organización de los Estados Americanos (OEA) y el Centro Global de Capacitación de Seguridad Cibernética (GCSCC) de la Universidad de Oxford, presenta una imagen completa y actualizada del estado de la seguridad cibernética de los países de América Latina y el Caribe. El informe consta de dos secciones: la primera sobre ***contribuciones de expertos***, consta de ensayos sobre las tendencias de la seguridad cibernética en la región, aportados por expertos internacionales en seguridad cibernética; y la segunda reporte de países presenta una visión general del estado actual de la seguridad cibernética en los países de la región del Caribe y América Latina. El reporte analiza datos de los países en función a 49 indicadores del modelo de madurez de la capacidad de seguridad cibernética desarrollado por el GCSCC, que se divide en cinco dimensiones: política, sociedad, educación, legislación y tecnología. Colombia se encuentra con un desarrollo sobre el promedio de los países sudamericanos, al mismo nivel de Chile y superado por Uruguay, Brasil y Argentina. Este informe también indica que el cibercrimen le cuesta al mundo hasta US$ 575.000 millones al año, es decir un 0,5% del PIB global. En América Latina y el Caribe, este tipo de delitos cuestan alrededor de US$ 90.000 millones al año (BID, OEA, & GCSCC, 2016).

Perfil de Colombia de acuerdo al Informe de Ciberseguridad 2016 del Observatorio de la Ciberseguridad en América Latina y el Caribe

Fuente: Informe de Ciberseguridad 2016 del Observatorio de la Ciberseguridad en América Latina y el Caribe

El Comité Interamericano contra el Terrorismo (CICTE) de la OEA, es la única entidad regional que tiene como propósito prevenir y combatir el terrorismo en las Américas. La Secretaría del CICTE tiene la tarea de apoyar a los Estados Miembros en sus esfuerzos de prevenir y contrarrestar el terrorismo. Brinda asistencia política y técnica a sus Estados Miembros a través de diferentes programas tales como: Ciberseguridad, Controles Fronterizos, Financiamiento de Terrorismo, Prevención de la Proliferación de Armas de Destrucción Masiva y Extremismo Violento. El programa de Ciberseguridad del CICTE se centra en tres pilares: desarrollo de políticas, desarrollo de capacidades (incluyendo capacitación y ejercicios cibernéticos), e investigación y divulgación (OEA, 2020).

Como resultado de un esfuerzo conjunto entre el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, el BID, la OEA y el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (MINTIC) se publicó el Informe ***Impacto de los Incidentes de Seguridad Digital en Colombia 2017***. Del contenido del informe se recogen los siguientes puntos que resultan de interés (OEA, BID, &MINTIC, 2017):



Aún en términos de América del Sur, Brasil ha buscado adaptarse a los avances de la guerra híbrida y de quinta generación, por ello el Presidente de la República de Brasil aprobó el 5 de febrero de 2020, la publicación de la Estrategia Nacional de Ciberseguridad. (Presidencia de la República- PR, 2020). Uno de los grandes retos presentados en este documento es que la ciberseguridad debe entenderse de manera holística y multisectorial, no es apropiado abordarla de manera restringida por las agencias gubernamentales, sin la participación adecuada del sector privado y sin mirar al usuario final de todas las tecnologías que usan el ciberespacio.

Alineado con el reto presentado y según el Libro Blanco de Defensa Nacional, la amenaza cibernética se ha convertido en una gran preocupación en Brasil por poner en riesgo la integridad de infraestructuras sensibles, esenciales para la operación y el control de diversos sistemas y organismos directamente relacionados con la seguridad nacional (Ministerio de Defensa- MD, 2012), es decir, la característica sinérgica de la ciberseguridad.

Además, como una forma de enfrentar los desafíos de ciberseguridad y ciberdefensa de manera cooperativa, el 27 de mayo de 2016 se redactó la carta de intención para cooperar en Defensa Cibernética entre las Fuerzas Armadas de Argentina, Brasil, Chile, Colombia, España, México, Portugal y Perú, uno de cuyos propósitos es el de colaborar académicamente, en el intercambio de conocimiento, entre los países del Foro Iberoamericano. Poco después, el Centro de Defensa Cibernética del Ejército Brasileño fue responsable de la protección cibernética durante los Juegos Olímpicos Río 2016, y, en 2017, presentó en Madrid los resultados de su labor en el Primer Seminario Iberoamericano de Ciberdefensa (Bonilla, 2019), siendo una buena referencia para la construcción de la Estrategia de Ciberdefensa y Ciberseguridad de Colombia.

Países en Sudamérica que cuentan con documentos normativos con respecto a ciberseguridad además de Brasil y Colombia son: Paraguay (Secretaría Nacional de la Información y Comunicación, 2017), Chile (Comité Interministerial sobre Ciberseguridad, 2017) y Argentina (Poder Ejecutivo Nacional, 2019).

Es importante tener en cuenta que cada País aborda el tema de la Ciberseguridad y Ciberdefensa de una manera diferente, y esto depende de los factores políticos, económicos, sociales y culturales imperantes. Mientras que algunos países

consideran la Ciberseguridad principalmente como una cuestión de seguridad y defensa nacional, otros defienden que tiene un mayor impacto en el desarrollo económico o en la competitividad internacional. Otros lo ven como un factor fundamental para la educación, la interacción social y el bienestar de los ciudadanos, tratando de incorporar todas estas consideraciones en sus Estrategias Nacionales de Ciberseguridad y Ciberdefensa (Leiva, 2015).

Siendo así, se puede decir que el Gobierno debe demostrar una determinación política efectiva para enfrentar los riesgos y las amenazas cibernéticas al establecer objetivos y prioridades. La creación de un Sistema y de una Estrategia Nacional de Ciberseguridad y Ciberdefensa reducirá los riesgos de que cada organismo involucrado decida sus propias líneas de actuación, debiendo actuar en coordinación y bajo un marco regulatorio estable e integral. En cualquier caso, esta política deberá fomentar las relaciones internacionales (Leiva, 2015).

2.3. Contexto Nacional

En primer lugar, debemos recordar que el uso masificado de la tecnología, como lo son las comunicaciones e información, sobrellevan consigo riesgos en contra de la Ciberdefensa y Ciberseguridad, de los intereses nacionales, de la infraestructura crítica, de las entidades gubernamentales y privadas, las cuales, en forma directa o indirecta, finalmente pueden afectar los derechos fundamentales de nuestra población y la Seguridad Nacional.

Es por lo anterior, que la Ciberseguridad y Ciberdefensa, se han convertido en un objetivo prioritario para el Estado Colombiano, de tal manera que se pueda garantizar la Seguridad Nacional, a través de las entidades estatales y privadas, participando activamente y de forma segura en el ciberespacio, facilitando elementos de entendimiento y confianza mutua, con unas relaciones sólidas en el ámbito de la seguridad y Ciberdefensa.

Los riesgos a los que Colombia actualmente se puede enfrentar, pueden provenir de fuentes múltiples y de actividades como: el sabotaje, espionaje, fraudes o ciberataques, desde el exterior por otros países, grupos organizados o particulares, entre otros. De igual forma, dichos ataques también se pueden desarrollar desde el interior de nuestro país.

Es así como, se hace necesario ante la rápida evolución de las ciberamenazas, desarrollar en el país en forma activa la ciberinteligencia, la cual debe estar integrada en forma conjunta y coordinada en las Fuerzas Armadas y sobre todo, en forma interagencial con las demás instituciones del Estado y del sector privado, lo cual, nos permitirá desarrollar una alerta temprana y en especial, el poder lograr anticipar los riesgos de los potenciales adversarios y de esta manera poder bloquear sus capacidades e intenciones en contra de nuestros activos estratégicos, siendo lo más importante, el lograr desarrollar una estrategia de Ciberseguridad y Ciberdefensa, que nos permita contar con un ciberespacio abierto y seguro para todo el pueblo colombiano.

2.3.1. Alineación Estratégica

En la actualidad, la ciberseguridad, se encuentra distribuida en varios organismos e instituciones, factor de riesgo, que hace necesaria una alineación y coordinación estratégica por parte del Estado, definiendo a cada una de dichas organizaciones, sus roles, funciones y, sobre todo, los criterios técnicos en materia de ciberseguridad, logrando de este modo, mejorar nuestra respuesta eficiente y técnica ante cualquier peligro. Al respecto, en el presente capítulo, se encontrará un compendio de la normatividad nacional e internacional, como marco jurídico clave para el desarrollo del ciberespacio a nivel nacional.

Con el fin de lograr una mayor integración y alineación estratégica en el país, se deberá promover por intermedio de los Ministerios de Defensa Nacional y del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, mesas de trabajo que integren actividades de seguridad y defensa, que permitan el desarrollo e implantación de industrias dedicadas a la ciberseguridad, y por intermedio de estas, integrar herramientas con protocolos de seguridad que permitan aumentar la capacidad de respuesta para la protección de nuestros objetivos estratégicos, al igual, que se pueda contribuir al desarrollo en nuestro país de la industria digital en forma dual (militar – privada).

2.3.1.1. Misión

Con la intención de buscar una estrategia nacional en Ciberdefensa y Ciberseguridad, Colombia deberá a través de sus instituciones privadas y del Estado, bajo el liderazgo del gobierno nacional, velar por la protección de su propia infraestructura, de su información, así como, de garantizar la seguridad nacional y protección de los activos estratégicos de la Nación.

De igual forma, será responsabilidad de todas las instituciones Públicas y Privadas, dar cumplimiento a las Políticas Públicas y a los planes intersectoriales para el control y prevención de ciberataques y el ciberdelito, siendo su principal responsabilidad, la de elaborar y mantener actualizados los planes de seguridad y defensa, para poder garantizar la Ciberseguridad y Ciberdefensa de la Nación.

2.3.1.2. Propósito

La Estrategia Nacional de Ciberseguridad y Ciberdefensa, tendrá como propósito, diseñar una acertada política de Estado, con la visión de establecer el derrotero del país en el mediano y largo plazo, con el fin de orientar los esfuerzos e incrementar la protección de nuestros objetivos estratégicos, así como, la respuesta ante cualquier riesgo cibernético al interior de la Nación, además, en forma paralela, deberá trazarse como objetivo el desarrollo de la industria digital nacional y de gobernanza del internet, con un límite no superior al año 2024.

2.3.2. Marco Jurídico

El Derecho de la Ciberseguridad y la Ciberdefensa, está compuesto por las más diversas normas y cuyos orígenes han sido los más desemejantes; algunos con el más sincero deseo de acertar y otros donde sus intenciones distan mucho de lo que desean alcanzar. La normativa jurídica ha recorrido un camino tan complejo como el desarrollo de la misma Internet desde su génesis, maduración y su evolución, hasta lo que hoy en día conocemos. De por si, se ha podido demostrar que las reglamentaciones de cada país son tan diferentes unas de otras, que ha sido muy difícil lograr una unificación conceptual y jurídica de todo lo que puede suceder en la red y lo que se pretende regular, (Gobernanza), ya que ha sido casi imposible lograr un consenso jurídico en cualquier tema que implique Internet y el ciberespacio.

Uno de los grandes retos que se avecinan desde la perspectiva jurídica es la aplicación eficaz, eficiente y efectiva jurídico-procesal-probatoria, de las normas del marco jurídico del llamado Derecho de la Guerra a la ciberdefensa, a la ciberseguridad y a los escenarios y operaciones de ciberguerra. Bajo este criterio Victor Luke, afirma que "subsumir normas que fueron creadas para aplicarse a acciones y objetos con existencia corpórea, a una realidad compuesta de cosas inmateriales genera problemas que la interpretación analógica no siempre logra resolver. Las armas informáticas solo consisten en información, en pulsos eléctricos organizados bajo códigos lógicos que expresados en un lenguaje matemático pueden traducirse en órdenes ejecutables por un computador". (Luke, 2012)

Sin duda alguna, la detección y manejo de ataques e incidentes cibernéticos, el dinamismo con el cual los ciberataques han sido perpetrados, amerita la formulación

y actualización de estrategias y/o políticas relacionadas con la seguridad digital, para blindar a los ciudadanos y a las organizaciones un entorno seguro y confiable. Estas realidades disruptivas o nuevos encuentros en un entorno no tangible como el ciberespacio, han transformado las relaciones, los negocios, el entorno social, político y económico en el mundo, dejando en evidencia que en ellos se desvanecen las fronteras terrestres y las barreras entre el entorno privado y el ámbito público.

Así las cosas, se han generado nuevos escenarios; donde los teatros de operaciones como lo son tierra, aire, mar, no son los únicos que hay que intervenir y proteger, ahora el ciberespacio es nuestro reto, es el otro teatro de operaciones de las nuevas expresiones del crimen organizado transnacional, que amenazan la Seguridad y Defensa Nacional en muchos países.

Los retos de seguridad principales del ciberespacio, tienen que ver con condiciones habilitantes para la innovación digital, los incidentes cibernéticos, la confianza digital de los ciudadanos y empresas, la ciberdefensa y la seguridad nacional, con la protección de un marco jurídico integral que dé a las autoridades o agentes del Estado, el campo de acción para mitigar esa inseguridad en el ciber. En este sentido, nos exige invertir más en seguridad digital y en ampliar nuestros tipos penales y adecuarlos a las nuevas exigencias.

Por consiguiente, no se puede descartar la materialización de escenarios potencialmente catastróficos como la colisión de aeronaves, la emisión de sustancias tóxicas desde plantas químicas, o la perturbación de la infraestructura y los servicios vitales como las redes eléctricas o de abastecimiento de agua. Las principales víctimas de esas operaciones serían, con toda probabilidad las personas civiles. (Droege, 2011). Este escenario es viable y materializable cuando somos los atacantes, pero cuando somos los atacados debemos preguntarnos: ¿Tenemos las facilidades probatorias y procesales para hacer valer las leyes sustanciales de los Delitos Cibernéticos vigentes en nuestro país? ¿Contamos con las herramientas necesarias para combatir, prevenir e investigar estas conductas?

Entre otros delitos que se evidencian por la utilización del ciberespacio tenemos "La sustracción de datos de carácter personal, la suplantación de la identidad, el fraude, la extorsión, el acoso a través de la red, los delitos contra menores y los daños a terminales y equipos personales que debilitan la confianza digital depositada por los individuos en la sociedad de la información," (Lecuit, 2017), es acá donde es válido preguntarnos. ¿Debemos incorporar nuevos tipos penales y replantear las instituciones judiciales?

Es así como, estas cualidades y aptitudes, se describen en el marco de trabajo conceptual establecido por la Unión Internacional de Telecomunicaciones - UIT en el Global Cybersecurity Index 2018, que se enfoca en 5 pilares que describen los aspectos habilitadores que deben tenerse en cuenta al momento de pensar en una cultura nacional de ciberseguridad que permita abordar la 4RI y el futuro digital. (Unión Internacional de Telecomunicaciones (UIT), 2018).

Estas se integran en:

a. 

Capacidad Legal: se refiere a la existencia de instituciones y marcos normativos y regulatorios que permiten el manejo de situaciones relacionadas con ciberseguridad, cibercrimen y ciberdefensa. También incluye lo relacionado con los mecanismos de investigación y judicialización de crímenes y la imposición de sanciones por incumplimiento de la ley. El objetivo de esta capacidad es contar con la legislación suficiente y necesaria que simplifique el combate nacional e internacional contra el cibercrimen.

b. 

Capacidad Técnica: se refiere a la existencia de instituciones y estándares técnicos que permitan abordar y entender las situaciones de ciberseguridad. Esto incluye las competencias y mecanismos técnicos para detectar y responder a las amenazas y ataques cibernéticos. El objetivo de esta capacidad es contar con un mínimo de condiciones técnicas aplicables de confianza y seguridad, que evite y minimice las vulnerabilidades en seguridad digital.

c. 

Capacidad Organizacional: se refiere a la existencia de instituciones que coordinen las políticas, así como las estrategias para el desarrollo de la ciberseguridad a nivel nacional. Igualmente se refiere a las medidas organizacionales que son indispensables para la implementación de una iniciativa nacional en seguridad de la información. El objetivo de esta capacidad es contar con una estrategia nacional, un modelo de gobernanza e instituciones que supervisen los esfuerzos en los diferentes sectores, evitando los conflictos en las acciones y generando una armonización efectiva entre las múltiples partes interesadas.

d. 

Construcción de nuevas capacidades: se refiere a la existencia de investigación y desarrollo, educación y programas de entrenamiento, profesionales certificados y entidades del sector público o privado que concienticen, informen, capaciten o formen en materia de seguridad digital. Este conocimiento se genera en relación con los tres pilares anteriores. Esto incluye también el desarrollo social, económico, político y humano implícito en la ciberseguridad. El objetivo de esta capacidad es la construcción de conocimiento y conciencia, así como lograr disponer de los profesionales cualificados en materia de seguridad digital.

e. **Capacidad de Cooperación:** se refiere a la existencia de alianzas, trabajo cooperativo y compartición de información en el ámbito nacional e internacional. Dado que el cibercrimen es de naturaleza transfronteriza, se requiere del concurso de múltiples partes interesadas en el ámbito nacional e internacional. El objetivo de esta capacidad es fortalecer la ciberseguridad nacional a través del establecimiento de acuerdos bilaterales y multilaterales y la participación en espacios internacionales de cooperación en la materia. Esto en pro de aunar esfuerzos para detectar y responder a amenazas y ataques.
(UIT, 2018).

Entre las que abordaremos en el marco de este numeral, son las legales, que nos permitirán visualizar de hecho aquellas que se han desarrollado a nivel mundial, no obstante, todo se fundamenta en la prevención para que el delito no se configure, y esta tarea viene de plantear líneas estratégicas, acciones y métricas que engranadas permitan que los planes y políticas, sean eficaces y eficientes para la Seguridad y Defensa en esta autopista como lo es el ciberespacio.

2.3.2.1. Marco Jurídico Internacional

Los riesgos digitales a la Infraestructura Critica nacional (ICN) traspasan fronteras, se desdibujo la soberanía de los Estados en la mayoría de veces, tanto la infraestructura física como sus datos se ubican y son enviados a diversas partes del mundo. Por lo anterior, es necesario contar con socios internacionales en un trabajo de protección conjunto, en donde las acciones de cooperación, ayuda mutua, intercambio de capacidades técnicas y jurídicas, vayan encaminadas a la identificación de los riesgos y vulnerabilidades de la cadena logística que va integrada desde la seguridad que brindan los fabricantes de tecnología, operadores ISP, y aquellas que debe tener el ciudadano del común al utilizarlas, así como las entidades públicas y privadas.

Es importante agregar que, se ha hecho necesario fijar marcos multilaterales, efectuar acuerdos de cooperación, documentos de orientación, declaraciones, capacitaciones, destinadas a fortalecer las organizaciones tanto a nivel nacional como internacional, fomentar normas que permitan dar el instrumento forzoso para proteger los derechos, soberanía, derechos fundamentales de las personas y otros, generar pautas, regulaciones, directivas permitiendo tanto al formulador de políticas incentivar el uso y apropiación de nuevas tecnologías, procurando garantizar la neutralidad tecnológica, sin que se afecte la seguridad y confianza en

las mismas, pero imponiendo reglas de juego que garanticen la protección de los derechos de cada una de las personas en el entorno digital.

Es así como, el cibercrimen, delitos cibernéticos o delitos de alta tecnología, entre otros términos, hicieron que los diferentes países comenzaran a modernizar su legislación de acuerdo con estas nuevas modalidades ilícitas de tres maneras:

Ante las diferentes actuaciones que han tenido los Estados en este nuevo escenario legislativo y normativo, entre otros ejemplos, tenemos a países como Estados Unidos, el cual creó el Ciber Comando (United States Cyber Command – USCYBERCOM), cuyo objetivo es el de salvaguardar la tecnología vital para esa nación. De igual manera, observamos que otras comunidades han creado uniones para combatir las ciberamenazas y crear formas de ayuda y cooperación mutua como, por ejemplo, la Unión Africana, que se creó para identificar las prioridades de la Política de ciberseguridad para África y que dentro de su legislación creó la Convención de la Unión Africana sobre Seguridad Cibernética y Protección de Datos Personales (Convención de Malabo).

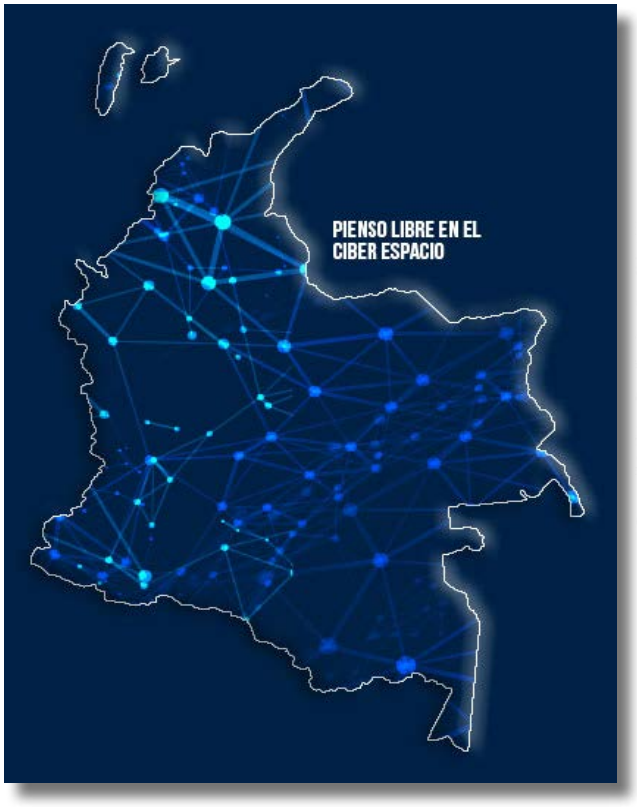
Por otro lado, tenemos la Comunidad del Caribe (Caribbean Community – CARICOM) cuyos países se encuentran en vía de desarrollo, la Unión Europea (UE), que cuenta actualmente con 27 países, los cuales formularon la Ley de Ciberseguridad, para la lucha contra el fraude y la falsificación de pagos electrónicos, de igual forma, la Directiva sobre seguridad de redes y sistemas de información (Directiva NIS), el Reglamento UE 2016/679, la Directiva UE 2016/680 y la Directiva 2013/40, entre otras.

De igual forma, podemos Observar la Unión Internacional de Telecomunicaciones (UIT) la cual cuenta con 193 Estados, incluido Colombia como países miembros. Dicha organización, elaboró una Guía de Estrategia Nacional de Ciberseguridad y una Agenda Global como marco de cooperación internacional; también, cabe mencionar, a la OTAN, organización que constas de 30 Estados miembros, generando como estrategia la Política de Defensa Cibernética mejorada y la Declaración de la Cumbre de Bruselas de 2018.

A nivel global, encontramos otras organizaciones con similitud de objetivos, como, la (Association of Southeast Asian Nations – ASEAN), el Grupo de los Siete (G7), la (Organisation of Islamic Cooperation – OIC) y la ONU, entre otras.

Como consecuencia de lo anterior, y dentro de los planes y políticas de los Estados, se han creado diferentes regulaciones, siendo las más importantes en el Derecho Internacional:

La Declaración Universal de los Derechos Humanos (DH), catalogada como el cimiento de toda regulación internacional, la cual ha sido llevada a un punto, donde mucho de lo que hay en internet afecta directa o indirectamente estos derechos, llegando hablar hoy día, de la cuarta generación de los DH, todos relacionados con la tecnología y el ciberespacio.



Libertad de Expresión en la Red, como uno de los Derechos Humanos en el Ciberespacio

Robert B. Gelman

Un avance importante en este punto fue la llamada Declaración del Milenio, (ONU, 2000), donde se ratificó la estrecha relación entre seguridad, fomento y protección de los Derechos Humanos con el desarrollo sostenible y las TIC; por otro lado, Robert B. Gelman redacto la Declaración Universal de Derechos Humanos del Ciberespacio basándose en la Declaración Universal de los Derechos Fundamentales, expedidos el 10 de diciembre de 1948 por la ONU, dichos derechos, regulan los comportamientos en el uso de las nuevas tecnologías, haciendo hincapié en la protección y respeto del individuo en su integridad personal. (Galarza, 2014).

Por otra parte, se tiene el Manual de las Naciones Unidas sobre Prevención y Control de Delitos Informáticos: este documento presentado en 1994 por un grupo de expertos de la ONU presentó por primera vez una amplia y futurista visión sobre lo que sería la ciberdelincuencia hoy en día, evidenciando las grandes problemáticas de la actualidad de la cibercriminalidad y visualizó un alcance transnacional de las conductas delictivas desplegadas en el ciberespacio.

Del mismo modo LA UNESCO Y LA SOCIEDAD DE LA INFORMACION PARA TODOS, asentado sobre los mandatos de la Asamblea General de la ONU la UNESCO expone un interesante proyecto educativo, científico y cultural donde la base principal son las tecnologías de la información y de la comunicación y cuyo norte es la inclusión de toda la población en el mismo; la CARTA SOBRE DERECHOS DE INTERNET: La APC (Asociación Para El Progreso De Las Comunicaciones) (APC) es una red internacional de organizaciones de la sociedad civil fundada en 1990 para proporcionar infraestructura de comunicaciones, incluyendo aplicaciones de internet, a grupos e individuos que trabajan por la paz, los derechos humanos, la protección del ambiente y la sustentabilidad;

Del mismo el Centro de Excelencia para la Ciberdefensa Cooperativa de la OTAN (Cooperative Cyber Defence Centre of Excellence – CCDCOE), publicó el Manual de Tallín el cual ya va en su versión 2.0 y lo define como una "Guía No Vinculante" para la aplicación de las leyes internacionales en los eventuales conflictos en el ciberespacio. Cubre tópicos como la soberanía, la responsabilidad de los Estados, el "Jus Ad Bellum", el "Jus In Bello", el Derecho Humanitario Internacional y la ley de neutralidad, entre otros. (OTAN, 2017).

En efecto, varios Estados, entre ellos Alemania, España, Francia y el Reino Unido han revisado desde 2015 los instrumentos legales a disposición de las autoridades judiciales y fuerzas de seguridad en la lucha contra el crimen organizado y el terrorismo en la red, incorporando, entre otras medidas, nuevas y controvertidas obligaciones a los operadores para la interceptación individual y masiva de comunicaciones en redes de telefonía e Internet así como el registro remoto de equipos informáticos. (Bueno de Mata, 2016).

A propósito, nos referiremos al **Convenio Budapest, el cual fue firmado en Hungría en el año 2001, en el seno del Consejo de Europa, con el fin de "prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos…"** El Convenio establece diferentes tipologías del delito en el ámbito de la cibercriminalidad como modelo legislativo, tanto en el ámbito de derecho penal como procesal penal; principios generales de cooperación entre los diferentes países en materia judicial y procedimientos vinculados a la investigación criminal. (de Europa, 2001).

Finalmente, en España, el Consejo de Seguridad Nacional aprobó en diciembre de 2013, la Estrategia de Ciberseguridad Nacional concretada en seis objetivos, entre ellos, "garantizar un uso seguro de las redes y los sistemas de información a través del fortalecimiento de capacidades de prevención, defensa, detección, análisis, investigación, recuperación y respuesta a los ciberataques". Para su consecución se establecieron ocho líneas de acción y 45 medidas concretas. (de España, 2013). En octubre de 2014 el mismo Consejo aprobó el Plan Nacional de Ciberseguridad que identifica de manera más exhaustiva los riesgos y amenazas para el desarrollo de las líneas de acción.

En resumen, todos los Estados para garantizar su seguridad en el entorno digital, se han volcado a generar estrategias que a groso modo, permitan concebir un espacio de seguridad y confianza que garantice los derechos y la privacidad de todas las personas naturales y jurídicas, la actuación y cooperación de países en un delito transnacional, el trabajo en la revisión e implantación de marcos legales para adecuarlos a las crecientes exigencias en materia de Ciberseguridad y Ciberdefensa y la constante investigación y capacitación de los Gobiernos y sus componentes para hacer frente a esta nueva era.

2.3.2.2. Marco Jurídico Nacional

Colombia un País de retos y desafíos en temas de Ciberseguridad y Ciberdefensa, es así como, las empresas diseñan sus políticas de ciberseguridad en función de las oportunidades y amenazas que pueden favorecer o perjudicar su competitividad. Desde la perspectiva corporativa, la gestión del riesgo adopta en ocasiones criterios que priorizan el impacto económico y de reputación de sus negocios, frente al impacto en la seguridad de terceros.

También, es de vital importancia resaltar que, **se debe aplicar de manera armónica e integral los principios constitucionales, tratados internacionales y demás actuaciones que se realicen en materia de seguridad digital**, de la protección y defensa del Estado, a través del ciberespacio concatenándose de manera coordinada a las múltiples partes interesadas, para garantizar la armonía en el ejercicio de sus funciones y el logro de los objetivos.

Para comenzar a desglosar las diferentes actividades y lineamientos tomados en el País en materia de Ciberseguridad y Ciberdefensa, debemos partir desde la Constitución Política de Colombia que en su artículo 1° establece como principio "(...) Colombia es un Estado Social de derecho organizado en forma de República unitaria, descentralizada, con autonomía de sus entidades territoriales, democrática, participativa y pluralista, fundada en el respeto de la dignidad humana, en el trabajo y la solidaridad de las personas que la integran y en la prevalencia del interés general (...)". (de Colombia, 1991).

Conforme a lo anterior y como se ha venido explicando, el Gobierno a través de sus instituciones y la empresa privada, trabajan de la mano para garantizar la protección de las redes, las infraestructuras críticas, los servicios esenciales y los sistemas de información en el ciberespacio Colombiano, formulando y ejecutando articuladamente las políticas, principios, objetivos y estrategias dirigidas al fortalecimiento de la seguridad digital, al cuidado de las infraestructuras críticas, y los activos.

Inicialmente las políticas del país en este tema, han evolucionado de acuerdo con la capacidad del Estado en brindar soluciones que se adapten al entorno y los cambios tecnológicos. En una primera instancia (2000 – 2006) se formularon documentos Conpes que tuvieron como prioridad ampliar el acceso comunitario a servicios básicos de voz e Internet y dotar de computadores a sedes educativas públicas. En una segunda etapa (2006 – 2010) se buscó fortalecer la provisión de accesos de banda ancha y de procesos de apropiación de las TIC en el ámbito educativo, incluso en sedes educativas públicas, buscando involucrar al sector productivo, especialmente a las micro, pequeñas y medianas empresas – Mipymes, y a las regiones como forma de incentivar el uso y aprovechamiento de las TIC.

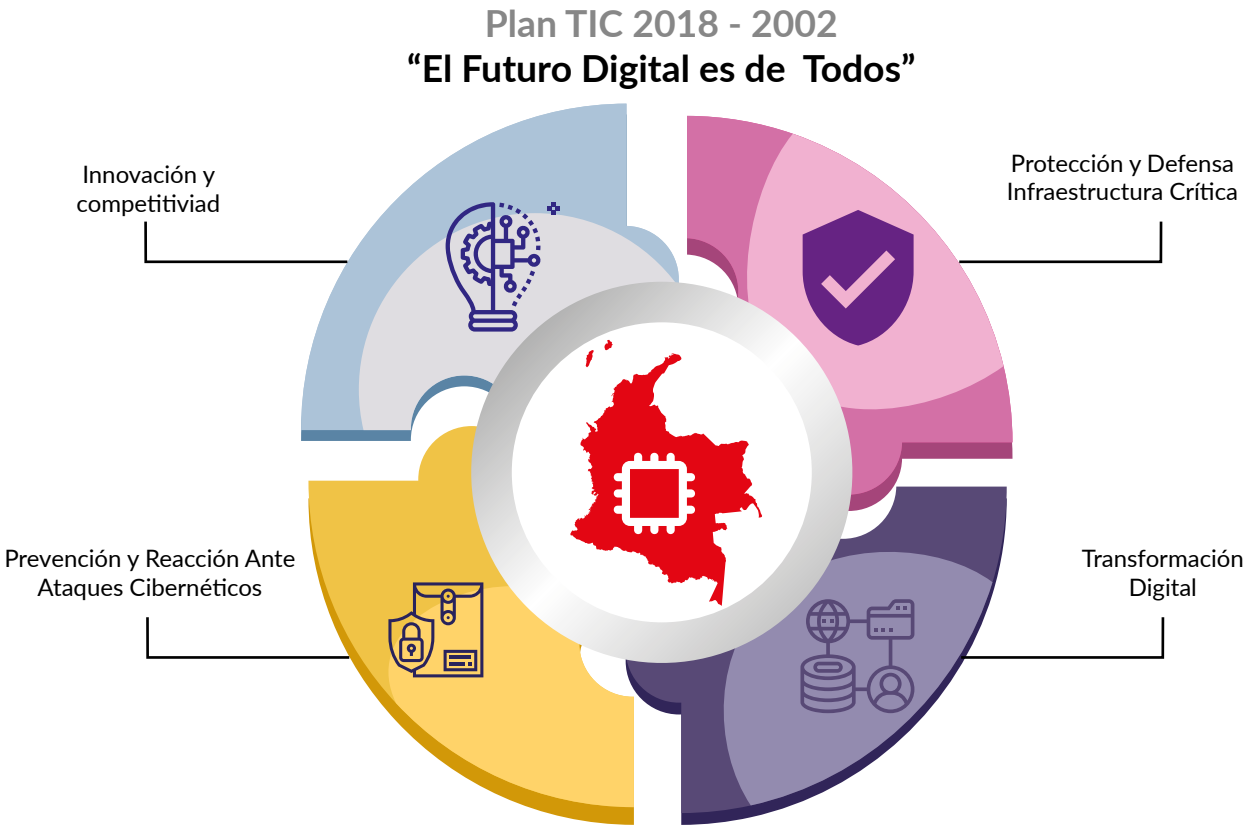
Al respecto, tendremos los lineamientos jurídicos y técnicos en su evolución cronológica, así: En primer lugar, tenemos los documentos de lineamientos de política pública que tienen como objeto dar lineamientos para el desarrollo de competencias en el ciberespacio, establecidas en los diferentes Consejos Nacionales de Política Económica y Social (CONPES), en especial, el CONPES 3701 de 2011 para la Ciberseguridad y Ciberdefensa, el cual estuvo a cargo del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), el Ministerio de Defensa, el Departamento Nacional de Planeación y otras instituciones nacionales, las cuales fueron claves, para determinar las estrategias, para enfrentar las amenazas que atentan contra la seguridad y defensa del Estado, en relación con la Ciberseguridad y la Ciberdefensa, creando el Grupo de Respuesta a Emergencias Cibernéticas de Colombia - ColCERT, el Centro Cibernético Policial, CCP y el Comando Conjunto Cibernético – CCOC. (Arango, 2014).

Con el fin de establecer un derrotero, brindar herramientas a nivel tecnológico y sobre todo crear normatividad, se deberá dar cumplimiento a los CONPES 3854 del 2016, el cual establece la adecuación del marco legal y regulatorio, con un enfoque de gestión de riesgos, así como, la capacitación para comportamientos responsables en el entorno digital. Del mismo modo, al CONPES 3988 de 2020, con el fin de impulsar la innovación en las prácticas educativas a través de las tecnologías digitales. A su vez, el CONPES 3975 de 2019, en el cual se establece la Política Nacional para la transformación digital e inteligencia artificial, que tiene como objetivo potenciar la generación de valor social y económico en el país a través del uso estratégico de tecnologías digitales en el sector público y del sector privado.

Finalmente, tenemos el CONPES 3995 del 2020 se está adelantando un proyecto de CONPES, el cual establecerá la Política Nacional de Confianza y Seguridad Digital, además, del marco de Gobernanza en esta materia, cuyo documento, también establece los marcos de trabajo de todas las entidades privadas y del Estado, en la adopción de modelos para la seguridad digital, con énfasis en las nuevas tecnologías.

De igual manera se aprobó la "Política de Defensa y Seguridad PDS para la legalidad, el emprendimiento y la equidad de Colombia", formulada por el Ministerio de Defensa Nacional, la Consejería de Seguridad Nacional y las Fuerzas Armadas en el año 2019, que busca generar una transformación estratégica y condiciones de seguridad y convivencia que preserven y potencialicen los intereses nacionales, la independencia, soberanía e integridad del Estado, en el marco de la línea de política "Disuasión y Diplomacia para la Defensa y la Seguridad" se establecen acciones y estrategias para fortalecer las capacidades militares de defensa para la disuasión, en especial aquellas capacidades en el ciberespacio y para liderar la lucha contra el delito transnacional, en áreas como la ciberseguridad y protección de infraestructura crítica. (Ministerio de Defensa, 2019).

Para que todas las iniciativas tengan un marco y un derrotero, que permita la modernización, innovación y le de altos estándares de competitividad al País, se generaron diferentes planes y programas, como el Plan TIC 2018-2022 "El Futuro Digital es de Todos", documento que presenta los proyectos e iniciativas del sector TIC que están relacionados con seguridad y la transformación digital del Estado, de igual forma, se desarrolló el Plan Nacional de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia, en el cual se definen los lineamientos generales que deben adoptar los diversos actores dueños y operadores de las infraestructuras críticas cibernéticas en Colombia, con el fin de prevenir y reaccionar ante la presencia de ataques cibernéticos que pongan en riesgo la continuidad y disponibilidad de los servicios críticos para el país.



Como herramientas que han permitido el avance normativo tenemos la Ley 1266 de 2008 (Habeas Data), la cual desarrolla una regulación integral del derecho fundamental de las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. Es una de los principales acercamientos para la protección al usuario garantizando que la información compartida sea veraz, completa, exacta, actualizada y comprobable; La Ley 1273 de 2009 o "Ley de Delitos Informáticos", nace con el objeto primordial de proteger la información y los datos, norma que crea o tipifica dentro del ámbito penal los delitos informáticos.

A su vez, la Ley 1341 de 2009**,** define los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones TIC, norma que dio línea y avance en el desarrollo de las Tecnologías de la Información en el país. Posteriormente, se expide la Ley 1437 de

2011 que faculta al Gobierno Nacional a definir estándares y protocolos, dando gran relevancia a la utilización e implementación de los medios tecnológicos dentro del procedimiento contencioso administrativo.

De la misma forma, vemos la expedición de normas como la Ley 1474 de 2011 orientada a robustecer la utilización de medios tecnológicos en los trámites y procedimientos judiciales; Ley 1581 de 2012 (Habeas Data) para la protección de datos personales registrados en cualquier base de datos que permite realizar operaciones por parte de entidades de naturaleza pública y privada; Ley 1680 de 2013 que garantiza el acceso autónomo e independiente de las personas ciegas y con baja visión, a la información, a las comunicaciones, al conocimiento, y a las tecnologías de la información y las comunicaciones, para hacer efectiva su inclusión y plena participación en la sociedad y la Ley 1735 de 2014, esta norma creó las sociedades especializadas de depósitos y pagos electrónicos (Sedpes), entidades destinadas a promover la inclusión financiera a través de productos transaccionales.

Se observa que, se va incrementando la necesidad de reglamentar todas las actuaciones, uso y apropiación de las Tecnologías de la Información y las Comunicaciones por medio de normas sustanciales y procedimentales para garantizar la navegabilidad en el ciberespacio, entre otras normas, tenemos, la ley 1712 de 2014 de Transparencia y del Derecho de Acceso a la Información Pública Nacional donde el Gobierno Nacional coloca a disposición de los ciudadanos como un derecho de acceso a la información, y como avance en la imperiosa necesidad de crear tipos penales que permitan de igual manera hacer frente a las nuevas realidades, una política penal común encaminada a proteger a la sociedad frente a los ciberdelincuentes.

La más receinte normativa en Colombia es la Ley 1928 de 2018, donde nuestro País se adhiere al convenio sobre ciberdelincuencia de Budapest.

CONVENIO DE BUDAPEST

El Convenio sobre la Ciberdelincuencia se presenta como un instrumento internacional cuyo objetivo es intensificar la cooperación entre los Estados Parte del mismo, mediante la materialización de una política criminal común en contra de la comisión de delitos cibernéticos.

Para el Ministerio de Justicia y del Derecho, desde un punto de vista material, el Convenio sobre la Ciberdelincuencia defiende fines constitucionalmente válidos y su ratificación busca materializar los lineamientos de política pública relacionados con la ciberseguridad, la ciberdefensa y la prevención de la cibercriminalidad, adoptadas a través de los documentos CONPES 301 de 2011 y 3854 de 2016, en los que se precisa la necesidad de contar con estrategias complementarias, procedimentales y de cooperación internacional, entre otras, dirigidas a articular esfuerzos y consolidar una política de protección común en temas de escala y afectación global. (Corte Constitucional, 2019).

La Ley 1955 de 2019 establece el documento denominado Bases del Plan Nacional de Desarrollo 2018-2022: Pacto por Colombia, pacto por la equidad", el pacto VII "por la transformación digital de Colombia: Gobierno, empresas y hogares conectados con la era del conocimiento", se incorpora como objetivo la promoción de la digitalización y automatización masiva de trámites a través de implementación e integración de servicios ciudadanos digitales, esto en el marco de generar la confianza y la seguridad digital.

Por último tenemos el proyecto de ley de Ciberdefensa, que ha teniendo como base la Ley 1341 del 30 de julio de 2009, proyecto que principalmente define los fundamentos, principios, responsabilidad, roles, la articulación y coordinación de acciones y operaciones para la seguridad digital, la protección de las redes, las infraestructuras críticas, los servicios esenciales y los sistemas de información en el ciberespacio, con la finalidad de defender y proteger la soberanía, los intereses nacionales, los activos críticos nacionales y recursos claves para mantener las capacidades nacionales frente a amenazas o ataques en y mediante el ciberespacio, cuando estos afecten la seguridad nacional.

En tal sentido, estas leyes han tenido sus Decretos reglamentarios que a groso modo se enumeran a continuación, con el fin de evidenciar los avances en la organización y la importancia que representan, para generar confianza y seguridad digital.

Es así como, se han expedido Decretos 1727 de 2009 (Habeas Data); Decreto 1704 de 2012 (Interceptación legal de comunicaciones), Decreto 2573 de 2014 (lineamientos generales de la estrategia de Gobierno en Línea), Decreto 1078 de 2015 (Decreto único reglamentario del Sector de las Tecnologías de la información y las Telecomunicaciones), el Decreto 1008 de 2018 (lineamientos generales de la política de Gobierno Digital), Decreto 1974 de 2019 (Asociaciones Público Privadas en materia de Tecnologías de la Información y las Comunicaciones), Decreto 620

del 2 de mayo del 2020 (estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales).

Es por todo lo anterior y basados en las leyes existentes a nivel nacional e internacional, que **se requiere una estrategia para una Ciberdefensa y Ciberseguridad, estructurada y sólida, innovadora, creativa y actualizada, con personal capacitado** que adquiera nuevas competencias, no solo para prevenir ataques informáticos contra instituciones estatales, si no, de una estructura activa que permita garantizar la defensa y seguridad Nacional.

Cada vez más observamos como con el estudio, capacitación y análisis de las tendencias nacionales e internacionales, se ha hecho inminente adoptar medidas de corrección y adición por medio de normatividad, que regule el uso y masificación de las tecnologías, pero de igual forma proteja al usuario proveyéndolo de seguridad y confianza en la utilización de las herramientas digitales.

No obstante, Colombia no se ha quedado atrás en su evolución tanto tecnológica como normativa, se aplaude el constante trabajo efectuado por las diferentes partes interesadas, pero a pesar de esta ardua labor, se recomienda una urgente revisión y actualización de normas penales y de procedimiento, para equiparar y dar las herramientas necesarias al Juez con el fin de imponer sanciones penales ejemplares y acordes a la problemática que se vive en el ciberespacio.

Si bien es cierto que hay proyectos con otros planes, normas y modelos para apropiar, se debe elaborar un marco legal más robusto y menos disperso, que logrará que la automatización de procesos, la digitalización de servicios, la optimización de sistemas de gestión pública y todas aquellas formas de modernización a través de las TIC, uso y apropiación de ellas, se haga más seguro y confiable.

Por otro lado, **es necesario efectuar un análisis de las fortalezas y debilidades de la legislación colombiana, que permita identificar las dificultades que al momento se presentan para mitigar los daños y riesgos en la red,** y exigir a los proveedores de redes y servicios, dar esa confianza y seguridad que requiere la comunidad que usa las redes del ciberespacio, con un instrumento legal más cercano a la realidad y la mitigación de la problemática planteada, a través de la articulación eficaz y eficiente de todas las ramas del poder público y de la voluntad política, para avanzar en la creación y tipificación de los delitos, lo cual, en este momento se presenta como un desafío.

Como se mencionó anteriormente, el Gobierno nacional tiene un compromiso adquirido al adoptar el convenio de Budapest, siendo perentorio dar el paso a la creación de tipos penales que se adecuen al mismo, para de esta manera, brindar a todas las instituciones privadas y del Estado, las herramientas jurídicas para combatir la ciberdelincuencia.

Finalmente, es preciso incluir en la actual legislación, una estructura que permita tener un modelo más proactivo que haga frente al delito en término de horas con su respectivo componente jurídico, de tal manera, que se agilicen los procedimientos para intervenir al cibercriminal. Dicha legislación, permitiría obtener la orden del Juez de Garantías con capacidad de reacción inmediata, ya que, con las herramientas jurídicas propicias, se permitirá neutralizar los daños en la comisión de un delito.

Por lo anterior, es necesario promover los cambios en las diferentes estructuras, con un equipo de respuesta inmediato, conformado por fiscales y jueces de control de garantías, actuando de forma ágil, oportuna, coordinada y eficiente con el ColCERT y los diferentes CSIRT, que permitan neutralizar o suspender inmediatamente las URL o redes sociales según el caso, desde donde se estén llevando a cabo dichos delitos, haciendo que las medidas tomadas para minimizar los riesgos en el ciberespacio, sean eficaces y permitan en corto tiempo penalizar a los infractores.

2.3.3. Protección a Centros de poder (político, económico, social y militar)

El concepto de la globalización actual se encuentra en un proceso de cambio continuo, debido a factores como la evolución constante de los centros de poder, nuevas potencias en ascenso, la consolidación de nuevos actores internacionales, la mayor capacidad de influencia adquirida por parte de la población, los cambios demográficos, por el incremento en la competencia por los recursos energéticos, alimenticios y económicos, así como, por el papel preponderante de las tecnologías en el desarrollo de la sociedad del conocimiento, de igual forma, por una mayor interdependencia económica, política y jurídica.

Los centros de poder son el eje del Estado y la sociedad, y es sobre estos, que se tejen las instituciones y las relaciones público- privadas, que le dan sustento a un país e identidad a una sociedad, en nuestro caso, materializados en amenazas de tipo cibernético que afectan la Seguridad Nacional, siendo necesario:

Identificar, priorizar y catalogar los Centros de Poder.

01

Establecer las Amenazas y sus riesgos cibernéticos.

02

Por tal razón, se han generado nuevos riesgos y amenazas para afrontar, las cuales, junto a las amenazas tradicionales tales como los conflictos armados, representan un alcance de tipo esencialmente transnacional, que al retroalimentarse e interactuar, potencian su peligrosidad y la vulnerabilidad del entorno. Otros elementos que suman complejidad a los riesgos y amenazas del contexto estratégico actual, son su impacto transversal en distintas estructuras y actores del Estado y de la sociedad, además, de la difícil identificación de su origen y a la ausencia de un centro de gravedad único, elementos que, por ejemplo, se materializan en las amenazas de tipo cibernético.

De tal forma, que la respuesta a los riesgos y amenazas que comprometen la seguridad en nuestros días, requieren de la cooperación tanto en el plano nacional de las entidades públicas y privadas, al igual, que en el plano general multilateral que permitan una respuesta eficiente. Es por eso, que las respuestas unilaterales y aisladas no son eficaces, por su carácter incompleto y parcial, frente a unos retos que exigen un enfoque multidisciplinar y una acción conjunta.

Por ejemplo, tal vez una de las más relevantes amenazas que podemos encontrar, son los ataques que buscan desinformar a la población, por otro lado, aquellas que buscan deslegitimar algún centro de poder, por esa razón, efectúan sus ataques vía noticias falsas o en la desinformación, mostrando al Estado como incompetente y corrupto.

Dichas campañas, también buscan hacer ver al sector privado, como un enemigo de la igualdad y la justicia social, de igual forma, se valen de ataques frontales a la idoneidad y el respeto de las Fuerzas Armadas y de afectaciones en contra de los derechos humanos, todos ellos, son ejemplos claros de lo que hoy en día se puede hacer desde el ciberespacio, para atacar la legitimidad y porque no decirlo, a determinado centro de poder o actor social.

2.3.3.1. Identificación, priorización y catalogación de los Centros de Poder

Una de las principales características para determinar los centros de poder y su criticidad, seria evaluando su nivel de afectación, de exposición y la capacidad de cada uno para sobreponerse (resiliencia), ante un posible ciberataque.

Por consiguiente, realizar un proceso a nivel nacional que conlleve a identificar, priorizar y catalogar los centros del poder o centros de gravedad, estaría de cierta

forma obligando a los sectores que los conforman, a realizar una autoevaluación en materia de ciberseguridad, generando conciencia ante las potenciales amenazas y frente a las acciones encaminadas a la protección de los datos y la privacidad de las personas, organizaciones y entidades del Estado.

Es fundamental, complementar los diseños de varios programas de ciberseguridad basados en el riesgo, al igual que, establecer e identificar los estándares para infraestructuras críticas. Así mismo, se deben perfeccionar las estrategias de política pública, robustecer las leyes y la normatividad en la materia, mejorando así el entorno de ciberseguridad de todos los sectores productivos del país; realizando las inversiones y buscando el apoyo desde todas las entidades tanto privadas como públicas.

Por lo tanto, la priorización y categorización de los centros de poder, se debe elaborar a través de un sistema de cascada, el cual debe partir en los organismos de primer orden estratégico, seguidos, por aquellos que cumplen funciones operativas o tácticas. Es así que, en este planteamiento, el criterio de priorización debe estar dictado sobre la protección prioritaria de los centros de poder vitales para el correcto funcionamiento del Estado, la democracia y los principios y preceptos contemplados a nivel constitucional.

2.3.3.2. Amenazas y riesgos cibernéticos de los Centros de Poder

La constante evolución de las tecnologías de la información y de las comunicaciones, brindan un ambiente propicio para el desarrollo de actividades al margen de la ley, así como, nuevas oportunidades para cometer delitos mediante las mismas, en consecuencia, tenemos una nueva amenaza para la seguridad nacional, en donde el Internet se convierte en un lugar accesible, fácil de usar y eficaz, del que cada vez se depende en mayor medida para llevar a cabo un sinnúmero de actividades de nuestra vida cotidiana.

Estas características, hacen precisamente del ciberespacio, un lugar propicio para que los delincuentes salgan impunes, considerando las dificultades para rastrearlos a través de la red, localizarlos y atribuirles la autoría de los delitos cometidos; por consiguiente, **las principales modalidades de ataques a los que se ven en riesgo los centros de poder nacional, se conocen como: Ciberterrorismo, Ciberdelito, Ciberespionaje y el hacktivismo.** Algunos ejemplos de delitos cometidos a través del ciberespacio, son la captación y reclutamiento de personal para una organización terrorista y la inutilización de medios informáticos de instituciones públicas, el robo

de datos personales mediante "phishing" y la intrusión de troyanos en los sistemas de información. Todos estos, representan un reto para las Fuerzas Militares y para los organismos de seguridad del Estado, así como, para las instituciones públicas y privadas que conforman los centros de poder nacional.

Por otra parte, las nuevas tecnologías han permitido desarrollar una nueva metodología de espionaje, las cuales, sumadas a los métodos tradicionales, generan una gran vulnerabilidad en los archivos confidenciales almacenados en dispositivos electrónicos y en la web. Por consiguiente, se hace preciso extremar la protección de los sistemas de información y sus repositorios frente a cualquier agresión externa que persiga la extracción de la información, que, de llegar a materializarse, conllevaría a la exposición de información estratégica, relacionada con los planes a nivel nacional en varios sectores, al igual, que vulneraría información vital de los centros de poder.

2.3.4. Protección activos estratégicos de la Nación

Comando Conjunto Cibernético (CCOCI) desde el año 2014, ha realizado un proceso metodológico que involucra a todos los sectores productivos del país, brindando la autonomía para que cada empresa, cuente con un plan de protección y defensa para su infraestructura crítica. Este proceso metodológico, ha incluido los nombramientos de equipos sectoriales, guías para la identificación, priorización y catalogación de la infraestructura crítica, además, de los planes nacionales y sectoriales de protección y defensa.

2.3.4.1. Identificación de los activos estratégicos de la Nación

La identificación de la infraestructura crítica, es la operación que permite determinar aquellas instalaciones, medios, hardware, software, comunicaciones y tecnologías de información que soportan el funcionamiento del sector, así como, su interacción con los otros sectores productivos de la Nación. Para este proceso, se diseñó en el año 2015 por parte del Comando Conjunto Cibernético (CCOCI) la guía para la identificación de la infraestructura crítica cibernética (ICC) de Colombia, que brinda un estándar a nivel nacional, el cual, puede ser aplicado por todos los sectores.

2.3.4.2. Priorización de los activos estratégicos de la Nación

Una vez se hayan identificado los activos estratégicos, es necesario contar con un marco metodológico que permita priorizarlos, con el fin de optimizar los recursos de las empresas destinados a la protección de sus activos. Con respecto a lo anterior, a nivel internacional, existen varios marcos normativos como: el NIST, ISACA y COBIT, que brindan las herramientas necesarias, permitiendo priorizar las infraestructuras, y de este modo, realizar los respectivos planes de gestión de riesgos.

Guía para la identificación de Infraestructura Crítica (ICC) de Colombia

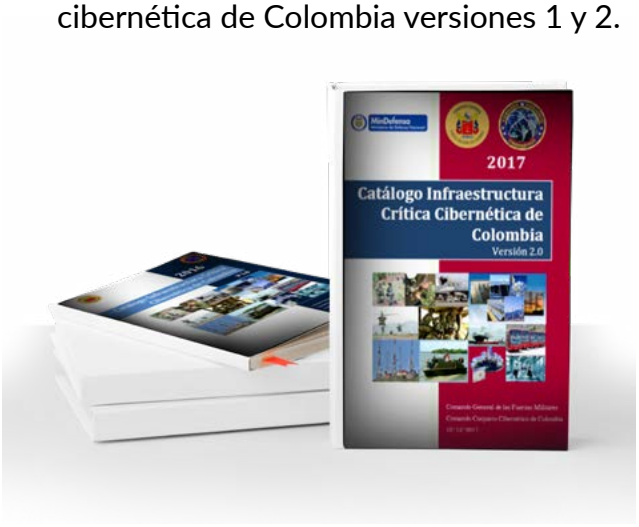
Sin embargo a nivel nacional, el CCOCI desarrolló en el año 2016 la cartilla "Sectores estratégicos de la República de Colombia desde la óptica cibernética", la cual, tiene como base, la metodología de la ventana de AREM, siendo esta, un ejercicio de construcción conjunto de significados, alrededor de situaciones poco conocidas, como quiera que los participantes de distintas áreas en una empresa, pueden establecer una lectura complementaria de los riesgos, que naturalmente, sigue estándares disponibles en nuestro país a la fecha. (Cano, 2014).

Sectores estratégicos de la República de Colombia desde la óptica Cibernética.

2.3.4.3. Catalogación de los activos estratégicos de la Nación

Una vez se hayan realizado las labores de identificación y priorización de las infraestructuras críticas, se hace necesario catalogarlas, para ello el CCOCI ha desarrollado dos versiones de acuerdo con los procesos metodológicos desarrollados.

Catálogos de infraestructura crítica cibernética de Colombia versiones 1 y 2.



Después de la identificación y priorización de los activos críticos de la nación, de acuerdo con la Guía de la Infraestructura Crítica Cibernética Para Colombia, se pueden identificar trece (13) sectores, realizando una identificación de los activos críticos, los cuales, se enumeran en su orden: Gobierno, Seguridad y Defensa, TIC, Electricidad, Financiero, Educación, Minero – Energético, Industria – Comercio – Turismo, Ambiental, Salud y Protección Social, Agua, Transporte y finalmente, de Agricultura y Alimentación.

En cada uno de los sectores estratégicos, se aplicarán los criterios de identificación de activos estratégicos, se priorizan los activos críticos, se establecerán los riesgos y actividades mitigadoras, para realizar las verificaciones de los planes de cada sector.

En cada Sector se han identificado las unidades de ciberseguridad y los mecanismos de colaboración entre los organismos del Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT), Comando Conjunto Cibernético (CCOC) y el Comando Cibernético de la Policía Nacional.

Por ejemplo, para el sector financiero, se ha implementado el CSIRT, unidad que aglutina entidades financieras y se encarga de fortalecer los mecanismos defensivos en materia de ciberseguridad, aportando también, una serie de alianzas internacionales que permiten colaborar con mayor precisión en materia de ciberdefensa.

Por consiguiente, se debe también efectuar la catalogación de activos críticos y, sobre todo, de los lineamientos sobre las acciones de ciberdefensa que aplicaran las fuerzas militares en caso de un ataque cibernético.

2.3.5. Gobernanza de la Ciberseguridad y Ciberdefensa Nacional

Nadie es ajeno al avance de las tecnologías de información en el mundo moderno. Desde la creación de las computadoras personales y el internet en los años 70, se han desarrollado avances sin precedentes en el manejo de información

y el uso de la misma para gestionar activos empresariales y del orden nacional, siendo difícil hoy día, encontrar alguna actividad productiva que no esté fuertemente asociada al uso de la tecnología.

Es así que, con el crecimiento del uso de las tecnologías de información, han surgido nuevos problemas para las personas, las organizaciones y los Estados, debiéndonos hacer, la gran pregunta de ¿Cómo proteger los sistemas de información y los activos asociados a ellos?, por esa razón, miles de expertos en tecnología alrededor del mundo dedican su tiempo a hackear los sistemas de información, para obtener datos relevantes y de control sobre activos estratégicos de las organizaciones y los Estados. De igual forma, las guerras que enfrenta el mundo, se trasladan al campo virtual para obtener ventajas competitivas sobre los otros a velocidades alarmantes, es hoy por hoy, cualquier aparato electrónico vulnerable y se hace necesario un actuar conjunto para responder al desafío que enfrentamos.

En este contexto los organismos internacionales han dado pasos importantes en la definición de guías o acuerdos que ayuden a los sectores públicos y privados en el cumplimiento de estándares y procesos que den respuesta a sus amenazas. Algunos organismos han publicado varios documentos o estándares, como la Guía de la ciberseguridad para los países en desarrollo (ITU 2007) o el National Cybersecurity Strategy Guide (ITU 2011). De igual forma, organismos de estandarización como la Organización Internacional de Estandarización (ISO) han creado guías contenidas en sus Sistemas de Seguridad de la Información contenidas en el ISO/IEC 27000, buscando dar pautas sobre seguridad de la información a distintas instituciones.

Acudiendo a los mecanismos de cooperación internacional los Estados han buscado acudir a organismos internacionales para lograr acuerdos que les permitan de manera conjunta protegerse de las distintas amenazas que surgen del ciberespacio. En este punto es importante destacar la Resolución AG /RES 2004 (XXXIV-O/04), de la Asamblea General de la Organización de Estados Americanos (OEA), a partir de la cual se consagra una estrategia multidimensional para conjurar los retos a la seguridad cibernética (OEA, 2004).

Asimismo, cabe mencionar la Declaración de la Cumbre de Gales, de la Organización del Tratado del Atlántico Norte (OTAN), suscrita en 2014, (Ruiz, 2014), y la Declaración sobre la Protección de Infraestructura Critica ante las Amenazas Emergentes, aprobada en la V Sesión Plenaria de la OEA, el 20 de marzo de 2015 (OEA, 2015).

Por lo anterior, es imprescindible para Colombia contar con un modelo de gobernanza de la Ciberseguridad y la Ciberdefensa Nacional, la cual debe al menos, desempeñar las funciones que se identifican como esenciales, y que no están siendo abordadas o se ejecuten de manera descoordinada en el país, por lo cual se propone la creación de una institucionalidad que asuma dichas funciones.

El modelo de gobernanza y la estructura organizacional moderna, acorde a las necesidades del ciberespacio y del desarrollo digital del país, deben garantizar las herramientas al Comité de Seguridad Digital, de tal forma que se creen las condiciones que permita a las diferentes instituciones la gestión del riesgo digital y se genere la confianza de su uso, creando un alto grado de madurez conforme a la resiliencia con que cuentan las diferentes organizaciones del Estado, tanto a nivel Público como Privado.

2.3.5.1. Gobernanza de la Ciberseguridad Nacional

Las funciones identificadas como esenciales, deberán ser ejercidas temporalmente por algunas de las instituciones que forman parte de la actual estructura del Gobierno, por ejemplo, en materia técnica para la gestión de los incidentes que se generen en la Red de Conectividad e infraestructura tecnológica

del Estado, se le puede asignar este rol a ColCERT, mientras que a nivel político, las seguirá desarrollando el Comité de Seguridad Digital, con funciones de comunicación, coordinación y seguimiento de las medidas presentadas en la presente Estrategia Nacional de Ciberseguridad y Ciberdefensa.

Es importante recalcar que el sector privado juega un papel relevante, toda vez que, en su gran mayoría, ellos son los gestores y propietarios de la infraestructura tecnológica con que cuenta nuestro país, por tal razón, se hace necesario contar con su apoyo, así como, con la promoción y la inversión en ciberseguridad para generar mayor competitividad y crecimiento económico que brinde entornos digitales mucho más seguros.

Por otra parte, se hace necesario que el país genere una autonomía tecnológica mediante el fomento de la industria en materia de ciberseguridad, a través de la Investigación, el desarrollo e Innovación (I+D+i), así como, con la gestión del talento tecnológico; lo cual permitirá contar con capacidades propias y autónomas que sean estratégicas para la Seguridad y Defensa de la Nación, haciéndose necesario, desarrollar un modelo criptológico nacional, que pueda ser usado a futuro en comunicaciones de voz y datos.

2.3.5.2. Gobernanza de la Ciberdefensa Nacional

Dado que las capacidades de la Defensa Nacional pueden colaborar en la formación de un ciberespacio libre, abierto, seguro y resiliente para el país, y considerando que las redes y sistemas de información constituyen una infraestructura crítica para la seguridad exterior y el ejercicio de la Soberanía de la Nación, razón por la cual, la Ciberdefensa del Estado debe continuar en cabeza del Ministerio de la Defensa Nacional, sin embargo, se hace necesario integrar a las demás instituciones en temas de ciberseguridad, la cual, es fundamental y complementaria a las actividades de protección de la infraestructura crítica de la nación, por tal razón, son actividades que se pueden realizar de manera coordinada e interagencial.

Si bien es cierto que la ciberseguridad se enmarca dentro de los modelos de carácter defensivo y preventivo, la ciberdefensa, debe considerarse dentro de los elementos que brinden al Estado una mayor fuerza disuasiva, la cual obedece a un contexto global de mayor campo de acción geopolítico.

Finalmente, se debe considerar que la rápida evolución de las ciberamenazas, debe contar con un aporte proactivo de la ciberinteligencia, integrándose en un esquema conjunto con la Ciberseguridad y la Ciberdefensa, consolidándose como

un elemento clave para el conocimiento de la situación y la anticipación, ante potenciales adversarios a través de la identificación de sus capacidades técnicas, tácticas e intenciones a desarrollar.

2.3.6. La preparación, una respuesta a nuevos desafíos

Claramente la cibernética es uno de los frentes más dinámicos de la actualidad y requiere del país entero una preparación para la defensa de los intereses nacionales, de las organizaciones y de los ciudadanos. Esta preparación debería iniciarse desde la creación de campañas de sensibilización, concientización y educación de la población en el mundo digital y de las necesidades de informática y defensa que nos lleven a la creación de una cultura nacional para la Ciberdefensa y la Ciberseguridad. Bajo el entendido de que los ataques no solo afectan a la información en medios digitales, sino a la tergiversación de la realidad a través de las famosas noticias falsas, para lo que debería cada persona estar preparada para validar la veracidad de la información y la validez de las fuentes.

Consideramos de vital importancia el diseño de programas específicos y el plan de carrera del talento dedicado en el país a este tema, lo mismo que determinar las necesidades de capacitación de las Fuerzas Militares, de la Policía Nacional y en general de las organizaciones privadas y estatales.

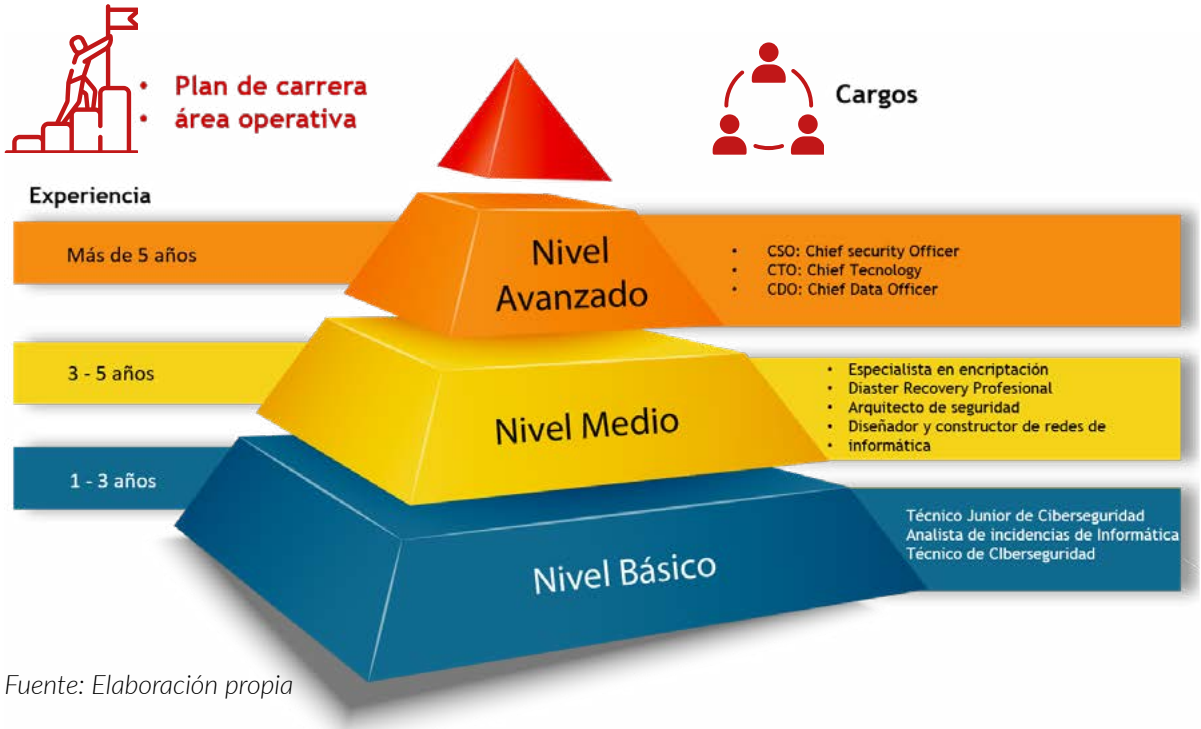
En la actualidad todas las organizaciones se encuentran en la obligación de constituir comités en seguridad industrial y salud ocupacional. Así mismo, se hace necesario que se tome en cuenta la obligatoriedad de tener líderes idóneos en seguridad y defensa de la información.

Consecuente con el establecimiento de planes de carrera y programas de capacitación, cobra relevancia, la retención y estabilidad del talento humano en las áreas dedicadas a la Ciberseguridad y Ciberdefensa como agentes multiplicadores del cambio hacia una cultura de transformación y seguridad en el mundo digital.

2.3.6.1. Plan de Carrera de Profesionales en Ciberseguridad y Ciberdefensa

En adición a lo comentado anteriormente sobre la formación de los profesionales de la Ciberseguridad y Ciberdefensa del país, se requiere un importante número de años de experiencia y ejercicio profesional en el campo, así como, de la creación de un escalafón de cargos y funciones en las que las personas puedan moverse con claridad, el cual, requiere ser implementado por niveles y áreas, que permitan promover al personal de profesionales y técnicos especialistas del sector, con un adecuado plan de carrera.

Plan de carrera – área operativa



Fuente: Elaboración propia

a. Plan de Carrea del Área Operativa

1. Primera fase o Nivel Básico – Área de Gestión y Administración:

Para esta fase se esperan profesionales entre 1 y 3 años de experiencia, los cuales pueden optar por los siguientes cargos:

- Técnico Junior de Ciberseguridad
- Analista de incidencias de Informática
- Técnico de Ciberseguridad
- Hacker Ético Junior

2. Segunda Fase o Nivel Medio – Área de Gestión y Administración:

Se requiere entre 3 y 5 años de ejercicio profesional y la oferta de posiciones puede ser del siguiente orden o sus equivalentes

- Especialista en encriptación.
- Disaster Recovery Professional (Profesional en planes de recuperación de desastres).
- Arquitecto de seguridad.
- Diseñador y constructor de redes de informática.

3. Tercera Fase o Nivel Avanzado – Área de Gestión y Administración:

Para ocupar una posición en este nivel que es el más alto del área técnica en la pirámide organizacional, se requiere un mínimo de 5 años de experiencia y puede optar por una de las siguientes posiciones o denominaciones de cargo:

- CSO: Chief Security Officer.
- CTO: Chief Technology (or Tecnical) Officer.
- CDO: Chief Data Officer.

Plan de carrera – área Gestión y Administración

Fuente: Elaboración propia

b. Plan de Carrera del Área de Gestión y Administración

1. Primera fase o Nivel Básico

Se necesitan profesionales y tecnólogos con experiencia entre 1 y 3 años, los cuales pueden aspirar a los siguientes cargos:

- Analista Junior de Ciberseguridad.
- Analista de Datos de Seguridad.
- Analista de ataques de Ciberseguridad.

2. Segunda Fase o Nivel Medio

Es indispensable contar con experiencia profesional entre 3 y 5 años para optar por alguna de las siguientes posiciones:

- Analista Senior de Ciberseguridad.
- Analista detector de Seguridades Técnicas.
- Data Protection Officer (con conocimientos jurídicos).

3. Tercera Fase o Nivel Avanzado

Se considera la cabeza de la administración de ciberseguridad de las organizaciones y puede llegar a ser asumida incluso por el presidente o jefe de toda la organización.

Este cargo para el que se requiere mínimo 5 años de ejercicio profesional puede tener alguna de las siguientes denominaciones:

- CIO: Chief Information Office.
- CISO: Chief Information Security Office.

2.3.6.2. Oferta académica de Ciberseguridad y Ciberdefensa

Actualmente, las diferentes instituciones del Estado y del sector privado, juegan un rol especial en el objetivo de elevar su nivel de respuesta y capacitación ante cualquier amenaza cibernética, cuyo impacto, requiere como requisito adelantar los diferentes programas de capacitación, teniendo como base al personal formado en carreras profesionales como ingeniería en sistemas, ingeniería electrónica o afines, al igual que, profesionales en sicología, sociología, ciencias políticas y derecho, quienes se desempeñarán en el área de gestión y administración. De igual forma, se hace necesario personal técnico y tecnológico con formación en sistemas, quienes integrarán el área operativa de cada organización.

En efecto, la permanencia en la organización en cualquiera de las dos áreas, depende de una línea de carrera que les permita no solo la promoción, si no, la medición de su desempeño, logrando identificar el personal clave para los intereses y defensa de la nación por parte del Estado, así como, del personal idóneo para cada una de las entidades del sector privado, motivo por el cual, cada Institución debe definir los requisitos mínimos del Plan de Carrera, tomando como referencia la presente Estrategia y la capacitación mínima que se requiere para este fin.

Por consiguiente, es necesario establecer la certificación básica y capacitación mínima requerida por cada una de las instituciones del Estado y del sector privado, la cual,

debe estar orientada tanto a los funcionarios del Área de Gestión y Administración, así como, del Área Operativa, debiendo estar enfocada dicha formación en tres fases o niveles de capacitación, así:

a. Primera Fase o Nivel Básico

Esta primera fase, se puede adelantar conjuntamente entre el personal del área operativa y del área de gestión y administración, quienes, al finalizar esta fase, contarán con la capacidad para realizar la prevención de incidentes cibernéticos.

b. Segunda Fase o Nivel Medio

1. **Área Operativa:** El personal técnico y profesional al culminar esta fase de capacitación, contará con la capacidad de resolver inconvenientes de mediana y alta complejidad, así como, la de gestionar una adecuada arquitectura para la defensa de ciberataques.

2. **Área de Gestión y Administración:** Al culminar la presente fase, el personal de esta área, deberá contar con la capacidad de determinar eventos cibernéticos, mediante el monitoreo, detección y análisis de las diferentes amenazas, de igual forma, gestionar los incidentes cibernéticos con la capacidad de forense digital.

c. Tercera Fase o Nivel Avanzado

1. **Área Operativa:** El personal técnico y tecnólogo al culminar la presente fase, deberá contar con la capacidad necesaria para realizar pruebas de penetración (Pentester Avanzado), tanto a los sistemas de información como de operación.

2. **Área de Gestión y Administración:** Para este nivel, que es el más alto de la pirámide organizacional, los profesionales deberán contar con la capacidad de gestionar la corrección a las vulnerabilidades que se detecten en los sistemas de información, al igual que, generar programas que eleven la conciencia situacional y la transferencia de conocimiento para las diferentes entidades. Por otro lado, el personal profesional tendrá la capacidad de hacer parte de los equipos de "Cyberhunting", los cuales, son equipos preventivos del más alto nivel, ante cualquier amenaza cibernética.

Finalmente, las diferentes entidades del Estado y del sector privado, podrán aplicar la propuesta de capacitación mínima requerida en cada una de las fases o niveles

establecidos, la cual se encuentra determinada en el Anexo "A" de la presente estrategia.

2.4. Intereses Nacionales (Ciberdefensa)

Los continuos avances y la dependencia tecnológica a nivel mundial han dado paso al surgimiento de múltiples y complejas amenazas contra las infraestructuras interconectadas, dichas infraestructuras, se han convertido en blanco de ataques y objetivos de interés estratégico; que en caso de ser atacadas pueden afectar los intereses nacionales, el orden constitucional, la soberanía, la independencia, la integridad territorial, la seguridad, la defensa nacional y el orden económico.

Las amenazas cibernéticas a la Seguridad y Defensa Nacional tienen connotaciones sustancialmente diferentes a las de otro tipo de amenazas, dado que éstas, pueden ser realizadas por actores como los Grupos Armados Organizados (GAO), Grupos Delictivos Organizados (GDO) e incluso por parte de amenazas actuales y potenciales cibernéticas internas o externas con diferentes objetivos; con bajos costos y difícil trazabilidad, siendo en algunos casos, casi imposible determinar la atribución de los hechos.

El creciente aumento de los medios electrónicos y la elevada dependencia del internet en la operación de las infraestructuras críticas nacionales, han definido un notable incremento de ataques, incidentes y delitos contra la seguridad y defensa cibernética, lo que permite evidenciar el elevado nivel de vulnerabilidad del país ante este tipo de amenazas, tales como el uso de dichas plataformas con fines terroristas, el sabotaje de servicios a entidades y gobiernos, el ciberespionaje, el robo de información clasificada y el hurto por medios electrónicos, entre otros.

Lo descrito anteriormente, tiene como principales efectos el incremento de la delincuencia cibernética, el riesgo de acceso indebido a la información, la afectación de las infraestructuras críticas tecnológicas cibernéticas, cuya perturbación o destrucción, tendría repercusiones importantes, con consecuencias posiblemente transfronterizas e intersectoriales, que impedirían una normal operación y gobernabilidad del país.

Más allá que recursos como el dinero, la información es la materia fundamental que puede cambiar el curso de cualquier situación, y gracias a internet, se logró tener acceso a información de todas partes y de todo tipo. Al comprender dicha concepción, se generó una problemática mundial en la que se aprovecharon las bondades y

vulnerabilidades del sistema para acceder a información privilegiada, clasificada y concerniente a tan solo unas pocas entidades específicas o gubernamentales.

A medida que se van sofisticando los ataques cibernéticos y con el presente internet de las cosas (Internet of Things - IoT), que le ha dado un mayor alcance al ya extensivo internet, se convierte en una necesidad inmediata el adoptar medidas que permitan contrarrestar y proteger las entidades del Estado. Dicha problemática, es una preocupación común en todos los países; razón por la cual, se han generado acuerdos y convenios internacionales tanto de concienciación, como de capacitación, incluyendo intercambio de información con el objetivo de poder hacer frente a esta creciente amenaza, que en la actualidad es perfectamente tangible y medible en todos los continentes.

"La Política del Sector Defensa y Seguridad busca una transformación estratégica que permita retomar la iniciativa y dar el salto decisivo para garantizar la primacía de la dignidad humana, la protección de la población y el territorio, la vigencia de las instituciones del Estado, promover el bienestar y asegurar el imperio del orden jurídico y la democracia en el país y en el hemisferio, para lo cual, desarticular y neutralizar definitivamente las amenazas internas, externas, tradicionales y contemporáneas será objetivo principal."

La política del sector defensa y seguridad, conlleva a una transformación estratégica del sector en cinco ejes: agua, biodiversidad y medio ambiente; seguridad cooperativa; disrupción del delito; del control militar al control institucional del territorio; e innovación, ciencia y tecnología.

Ejes de Transformación Estratégica del Sector Defensa y Seguridad

Fuente:Política de Defensa y Seguridad (PDS) 2019

Los anteriores antecedentes, son fácilmente ubicables en los escenarios regulares de la guerra regular, como son la tierra, el aire, el mar y los ríos, teniendo límites fáciles de identificar por fronteras, naturaleza o definiciones políticas.

Hoy para algunos países según sus capacidades tecnológicas, se tienen establecidas capacidades para atender un cuarto dominio en el espacio, donde se comienzan a generar capacidades de exploración y defensa, existiendo este dominio dentro de un marco que se puede explicar desde ciencias cómo la física.

Desde la segunda guerra mundial, se vinieron dando las bases y elementos para definir un quinto dominio de la guerra.

Las guerras conllevan el manejo de información confidencial que conlleva planes de combate, desarrollo de estrategias, desarrollo de armas, diseño de mecanismos de defensa, información de combatientes y mucha más información, que siempre va a ser objeto de interés del enemigo, interés, que desarrolló el mundo del espionaje

y la necesidad de proteger un activo que con el desarrollo de la tecnología se fue volviendo cada vez más virtual, la información.

La información se identifica como un activo estratégico que debe ser asegurado en su ubicación, contenido, transporte, transformación o actualización, lo anterior hizo que desde la segunda guerra mundial se trabajara en técnicas de encriptación que protegieran de desconocidos, el conocimiento de los datos y actuar en contra del propietario de la información. Creada la encriptación, se da la necesidad de espiar los medios donde se transporta la información y desencriptar los datos para obtener una ventaja en el desarrollo de las estrategias militares que permita lograr una victoria parcial o total en la guerra.

La evolución de la tecnología permite el análisis de señales donde se transporta la información, táctica que permitió el espionaje de secretos militares en todos los sentidos de las grandes potencias durante la guerra fría y fue evolucionando en herramientas, velocidad y capacidades, de la mano de la evolución de la tecnología.

La aparición de internet, originada en un proyecto de investigación militar, ha traído a la humanidad una velocidad de cambio sin precedente, con grandes beneficios en el desarrollo del conocimiento, el intercambio social, la evolución de los negocios, el intercambio de bienes y servicios, etc. Esto desarrolló un mundo virtual en el que se conectan diferentes dispositivos de comunicaciones, almacenamiento, presentación de información y que hoy conecta a más de 4.500 millones de usuarios, 5.160 millones de teléfonos móviles, 3.800 millones de personas activas en redes sociales, con un consumo promedio de servicios de internet de más de seis horas.

Este mundo virtual ha sido denominado el ciberespacio y está teniendo un nuevo componente en su desarrollo y es el incremento geométrico de dispositivos inteligentes conectados a internet, como televisores, electrodomésticos, controles y monitores caseros, controles y monitores industriales que van camino de ser billones en el mundo, conjunto de dispositivos agrupados en el concepto de IoT o internet de las cosas.

Este mundo virtual es el nuevo dominio de la guerra, el quinto, donde no existen reglas claras, donde las fronteras de los países no se pueden determinar con facilidad, donde elementos legales no están totalmente acordados entre naciones.

En el quinto dominio, en el ciberespacio, es común hablar de internet como el medio de encuentro para organizaciones, individuos, redes sociales, etc., pero también existe una red menos conocida, la dark web, la red oscura donde las reglas realmente no existen y allí se comercian toda clase de ilícitos o herramientas para cometerlos. La comunidad hacker tiene como lugar de encuentro la dark web,

donde son indetectables y aprovechando el nacimiento de las monedas digitales, cuyos orígenes y movimientos no son identificables, comerciar desde herramientas básicas, armas sofisticadas y cualquier clase de delincuencia.

Hoy con la denominada revolución industrial 4.0, el desarrollo de las infraestructuras críticas se ha acelerado, interconectado y expuesto al ciberespacio de diversas maneras. Las naciones han entendido esto y en las grandes potencias mundiales se ha venido dando el desarrollo de capacidades de ciberdefensa y ciber ataque, creando diversidad unidades donde las fuerzas militares son protagonistas con baluarte del sostenimiento de las leyes, la soberanía y la protección de la población.

Países como Estados Unidos, Rusia, Irán, China, Israel y aliados de estos, han intercambiado diferentes ciber ataques sobre diferentes activos críticos como plantas nucleares, plantas de tratamiento de agua, entidades gubernamentales, sistema financiero, industrias relevantes a la nación atacada, etc. Ante el ciber ataque la ciberdefensa toma relevancia, pero resulta compleja, demanda recursos especializados y constante colaboración entre las diferentes unidades de ciber protección creadas en cada país.

2.4.1. Hipótesis de ataques cibernéticos a los activos estratégicos

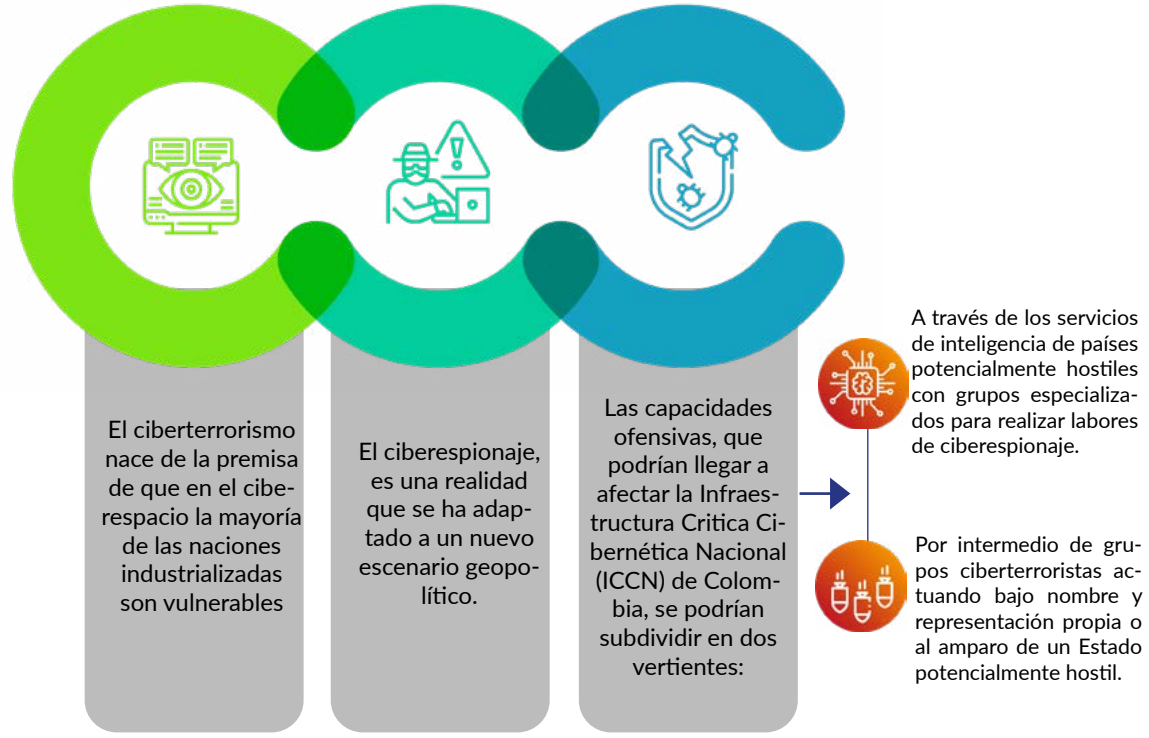
El ciberterrorismo nace de la premisa de que en el ciberespacio la mayoría de las naciones industrializadas son vulnerables, realidad, que ha sido develada en los últimos años y está siendo utilizada para trascender a terrenos políticos, sociales y económicos. Los principales lugares en los cuales se han evidenciado los estragos de ataques ciberterroristas son Europa y Estados Unidos, allí, mediante el uso de las tecnologías de la información van dejando a su paso afecciones en los principales objetivos, es decir la infraestructura crítica de un país.

El ciberespionaje, es una realidad que se ha adaptado a un nuevo escenario geopolítico, caracterizado por una creciente competitividad económica y tecnológica. Las posibilidades y campos para la obtención ilícita de créditos de tipo político, económico y tecnológico, por parte de personas, grupos y Estados, se han multiplicado con las ventajas que ofrecen los constantes avances tecnológicos. De igual modo, las oportunidades para los actores de ejercer acciones que puedan tener una afectación directa sobre el bienestar de los ciudadanos, el sistema económico, las comunicaciones, así como, infraestructuras e instituciones, se han incrementado.

Es de público conocimiento, que diversas organizaciones terroristas alrededor del mundo, utilizan sus recursos económicos para financiar, contratar o subvertir jóvenes promesas con grandes conocimientos técnicos para llevar a cabo este tipo

de ataques a través del ciberespacio, lo cual, constituye una amenaza latente y creciente, ante la falta de cultura en materia de ciberseguridad en la gran mayoría de la población mundial y específicamente en la población colombiana.

Es posible evidenciar a través de los ejemplos relacionados con anterioridad, la manera en que diferentes conflictos entre países y al interior de las naciones, han migrado al ámbito ciberespacial. Colombia no es ajena a dicha situación, cada vez son más frecuentes las alertas que se generan por ciberterrorismo en América Latina, a su vez, se proyecta que diferentes tensiones diplomáticas con países de la región, puedan repercutir en protestas y ataques desde el ciberespacio.



En efecto, los ataques cibernéticos buscan información privilegiada, conocimiento de estrategias nacionales, información de personas distinguidas, acceso a servicios esenciales tales como la energía y el agua, en el cual, tienen por objetivo, afectar su disponibilidad y, por ende, afectar a la población.

Por otro lado, podemos observar que:

Los ataques cibernéticos sobre cualquier infraestructura, son de fácil implementación.

El ataque involucra la creación de armas virtuales o digitales, con un escenario para el combate, mecanismos de respuesta y planes de recuperación.

El origen de un ataque puede venir de cualquier lugar del mundo y en muchos casos no se puede precisar.

2.4.2. Plan de Ciberdefensa de activos estratégicos

Este plan se debe realizar en coordinación del Consejo Superior de Seguridad Digital, Protección y Defensa del Ciberespacio. En materia de ciberdefensa se seguirá el Plan de Guerra vigente por parte del Comando General de las Fuerzas Militares, el cual a través del Comando Conjunto Cibernético (CCOCI), es el encargado de la defensa de los activos estratégicos del país.

Se pondrá particular atención, al impacto que pueda tener un incidente de seguridad de la información en infraestructuras físicas controladas o monitoreadas desde el ciberespacio, en especial, en la seguridad de los sensores y dispositivos de control industrial que habilitan dichas acciones. Para ello, se debe contar con equipos de respuesta cibernéticos que puedan contener los ataques que se presenten.

Por otro lado, se debe prestar especial atención al CONPES 3854, el cual, presenta un enfoque de gestión, basado en riesgos de seguridad digital, fortaleciendo la cooperación sectorial y el desarrollo de vínculos internacionales en esta materia.

Es de esta manera, que los enfoques de ciberdefensa requieren mayor coordinación intersectorial, basado en leyes más fuertes que aseguren no solo la cooperación, si no, el poder compartir información pertinente a la protección cibernética. De igual forma, es necesario el desarrollo y entrenamiento del talento humano, como parte fundamental de los elementos a fortalecer, lo que conllevará a una estrategia de consolidación en las Fuerzas y sobre todo, el lograr continuidad y experiencia en el personal, mejorando la misión institucional.

2.4.3. Resiliencia Cibernética

Para contar con resiliencia cibernética, se debe contar con un plan de recuperación de desastres y continuidad del negocio, cuyo objetivo, es garantizar que se pueda gestionar una efectiva defensa ante un ataque cibernético, mientras se continúa operando el negocio de manera efectiva, para ello, se deben considerar los siguientes puntos:

a. Identificar activos críticos

El primer paso es detectar datos críticos, saber dónde se guardan, qué flujo siguen dentro de la compañía y qué personas tienen acceso a ellos, al identificarlos, es posible tomar las medidas necesarias para protegerlos de forma adecuada.

b. Evaluar todos los riesgos

Desde las prácticas comerciales, pasando por la tecnología de la información, los usuarios de TI, la gobernanza de la seguridad y hasta la seguridad física de los activos de información, requieren una revisión al interior de las organizaciones, donde se puedan evidenciar las deficiencias y vulnerabilidades de la seguridad cibernética en todas las áreas empresariales clave. Es también importante, tener en cuenta el posible impacto que un ataque cibernético podrá tener sobre la reputación de marca o la imagen institucional.

c. Involucrar a toda la organización

Identificados y evaluados los riesgos, es indispensable educar a los empleados y líderes en todos los niveles de la organización e implementar planes provisionales de crisis que llevarán a construir una organización verdaderamente ciber resiliente.

d. Mantener las alarmas encendidas

Las acciones que se tomen, deben mantenerse activas en todo momento, y ser sometidas a pruebas aleatorias, que permitan garantizar su efectividad permanente y, sobre todo, su capacidad de respuesta en caso de ser requeridas.

CAPÍTULO
TRES

RIESGOS, AMENAZAS Y DESAFÍOS

Riesgos, amenazas y desafíos

Este capítulo se desarrolla de acuerdo con la apreciación y el concepto del Comando Conjunto Cibernético del Comando General de las Fuerzas Militares y la Unidad de Ciberseguridad de la Policía Nacional.

En Colombia, aunque se advierte que el vertiginoso crecimiento de las Tecnologías de la Información y las Comunicaciones (TIC) y su correspondiente aporte a la globalización, ha servido de plataforma a las amenazas contra la seguridad a través del ciberespacio, no se reconocen los efectos catastróficos que podrían causar los ataques generados por esta clase de amenazas sobre la infraestructura crítica cibernética pública y privada, ya que "estas amenazas se materializan principalmente en conductas delictivas dirigidas a afectar el patrimonio económico y la intimidad de las personas" (Ministerio de Defensa Nacional, 2015).

El desarrollo de los sistemas tecnológicos avanza a grandes velocidades al igual que las amenazas y los riesgos que atentan contra sistemas informáticos de los activos estratégicos y la infraestructura crítica de los sectores públicos y privados.

El desarrollo de los sistemas tecnológicos avanza a grandes velocidades al igual que las amenazas y los riesgos que atentan contra sistemas informáticos de los activos estratégicos y la infraestructura crítica de los sectores públicos y privados. Las armas cibernéticas nacionales e internacionales inteligentes como robots programados para desarrollar operaciones cibernéticas dirigidas, impresión de armas en 3D, el despliegue de avatares, y otras tecnologías disruptivas constituyen un riesgo inminente para la Seguridad y Defensa nacional.

El ciberterrorismo se ha puesto de manifiesto en las Guerras de Quinta Generación, caracterizadas por su declaración no formal, usando recursos de múltiple naturaleza incluyendo las nuevas tecnologías, pudiéndose entender más fácilmente al estudiar

los casos de ataques a infraestructuras críticas cibernéticas, como el caso del virus Stuxnet y más recientemente el ***malware*** WannaCry, este último descrito por Kaspersky (2017) como: El ataque mundial de ransomware que ocupó los titulares de todo el mundo, infectando más de 200.000 sistemas en 150 países. Hoy en día están surgiendo informes de una nueva cepa del ataque tipo gusano que Europol ha descrito como "a un nivel sin precedentes".

Por lo anterior, la formulación de la Estrategia en Ciberdefensa analiza los riesgos, las amenazas y desafíos que el uso de la deep web, dark web y otras redes clandestinas representan para el Estado colombiano.

Las capacidades en materia de ciberdefensa y ciberseguridad en las Fuerzas Militares y Policía Nacional no son suficientes para responder ante las amenazas y ataques cibernéticos actuales y futuros; adicionalmente se presentan grandes debilidades normativas que soporten las actuaciones de las autoridades sobre lo adverso en el ciberespacio.

Las principales debilidades se observan en la falta de coordinación entre las entidades para la atención integral para la atención, mitigación, gestión y judicialización, para la atención del incidente informático. Por lo tanto, se hace necesaria una mayor cooperación y un mejor intercambio de

datos entre las entidades del Estado, los equipos de respuesta a incidentes de seguridad informática, el sector privado y la academia.

A lo anterior se suma la falta de protocolos, el desarrollo de modelos estandarizados de buenas prácticas e infraestructura para enfrentar la materialización de riesgos cibernéticos, sistemas y procedimientos de resiliencia.

Las nuevas tecnologías conllevan a la innovación criminal. Esto demanda personal capacitado y en proceso de aprendizaje y mejora continua para enfrentar emergencias cibernéticas, toda vez que el cibercrimen es un fenómeno que evoluciona junto a las tecnologías, creando ataques emergentes y ventanas de oportunidad para los ciberdelincuentes.

Frente a la seguridad digital, el Estado debe tener una visión integral de la seguridad física y financiera, lo que demanda una respuesta coordinada entre la Fuerza Pública, el aparato judicial, las entidades públicas y privadas. Mejorar el acceso transfronterizo a la evidencia electrónica y la efectividad de la cooperación público-privada a través del intercambio de información. Desarrollar acuerdos bilaterales de intercambio de información y de evidencia digital para la cooperación internacional, cumpliendo con los protocolos judiciales necesarios de delitos trasnacionales.

Esto se puede lograr optimizando recursos y esfuerzos en la mitigación de amenazas, fortalecimiento de capacidades en seguridad digital, incremento de la confianza digital y desarrollando técnicas de investigación, que permitan afrontar los desafíos de anonimidad y volatilidad de la información.

3.1. Riesgos

La disrupción de las nuevas tecnologías que está directamente relacionado con el crecimiento exponencial de las amenazas cibernéticas, constituyen una preocupación para Colombia dado el alto impacto que pueden tener a la seguridad y defensa nacional y por ende a la prosperidad económica y social del país. En lo que refiere al componente Militar, es evidente que a medida que los sistemas de navegación, armamentísticos, transporte, información y de comunicaciones de las Fuerzas Militares dependan cada vez más de las plataformas tecnológicas, mayor será el riesgo de ser víctimas de ciberataques y más amplia será la gama de posibles escenarios.

Frente a este panorama el Estado enfrenta riesgos que sepueden clasificar así:

a

Ciberataques a la infraestructura financiera. Están catalogados como uno de los de mayor impacto dado que sobre éste sector se sostiene el desarrollo de la nación, y a través de él se puede afectar una gran parte de la población, especialmente ante el fenómeno actual de las monedas virtuales.

b

La composición del enemigo en el ciberespacio no se puede determinar, teniendo en cuenta la gran variedad y cantidad de posibles atacantes que pueden existir a través del mismo, los cuales van desde personas con poco conocimiento en informática, quienes pueden planear y ejecutar pequeños ataques, hasta hackers expertos quienes tienen la capacidad de planear y ejecutar ataques a gran escala en referencia a temas de Estado y sectores de la población, empleando redes sociales y sitios web clandestinos para el planeamiento de sus ataques cibernéticos.

c

Movimientos hacktivistas con capacidad de realizar ataques a entidades del Estado y el sector privado.

d

El anonimato con que gozan los cibercriminales son un factor negativo en contra de las agencias de Ley que persiguen estas organizaciones delincuenciales a nivel mundial, considerando que se incrementa el nivel de dificultad para identificar e individualizar a los cibercriminales introduce la posibilidad de que los responsables internos o gobiernos hostiles planeen y ejecuten ataques fácilmente negables sin que se pueda determinar exactamente el origen, por tal razón, su ubicación exacta dentro de un territorio específico puede llegar a ser remoto.

e

El escaso presupuesto para ciberseguridad y ciberdefensa, sumado a los recortes presupuestales, limita la capacidad de respuesta frente al crecimiento exponencial de nuevas tecnologías del cibercrimen que demandan permanente desarrollo, lo que incide en el fortalecimiento y sofisticación de las capacidades de las instancias responsables en Colombia.

f

En la sociedad digital actual, el acelerado cambio tecnológico revoluciona la forma de hacer la guerra (***warfare***), crea nuevos dominios en el espacio exterior, el ciberespacio, el espectro electromagnético, lo que obliga a replantear los conceptos operativos, jurídicos, técnicos, y diplomáticos, entre otros.

g

La ausencia de una estrategia coordinada e interagencial dificulta la acción y coordinación de las capacidades hacia un objetivo común frente al cibercrimen.

h

La revolución tecnológica ha cambiado el ambiente operacional, el carácter de los conflictos contemporáneos y el enfoque de la guerra híbrida ha creado nuevos actores que amenazan la defensa y seguridad nacional.

i

La evolución de las amenazas por las armas cibernéticas generan un escenario permanente de ataque inminente contra los Estados y sus individuos.

Por su parte, los riesgos en seguridad digital son los siguientes:

Creciente participación de ciudadanos en el entorno digital

Alta dependencia de la infraestructura digital.

Aumento en el uso y adopción de nuevas Tecnologías de la Información y las Comunicaciones (TIC).

Aumento del comercio electrónico.Comunicaciones (TIC).

Uso de infraestructuras digitales, como modelos de negocio globales altamente rentables.

Amenazas emergentes de las nuevas tecnologías; tecnologías emergentes de anonimización, cifrado, inteligencia artificial, así como la evolución de patrones criminales como servicios, tráfico de datos, y ataques hechos a la medida, haciendo que cada día los ataques sean más costosos y sofisticados. Por lo anterior, el impacto trasciende a la continuidad del negocio, el riesgo reputacional, la satisfacción del cliente y la moral de los empleados.

Las vulnerabilidades en los procesos y tecnologías establecidas.

La facilidad de renovación de amenazas cibernéticas longevas tras la persistencia de muchos modus operandi establecidos.

Los riesgos pueden ser originados por:

3.2. Amenazas

Las amenazas cibernéticas son múltiples y muy variadas, que mutan sus vectores de operación en cuestión de segundos, y se soportan en la masificación de las tecnologías disruptivas, entre ellas: Computación generalizada, redes inalámbricas, biotecnología, impresión 3D, aprendizaje de máquina, nanotecnología, robótica y otras, que ofrecen un escenario complejo y dinámico que pueden impactar la defensa y seguridad en Colombia. El crecimiento exponencial del internet, la convergencia tecnológica, la automatización, la globalización, las tecnologías disruptivas, la densidad digital de los productos y servicios digitalmente modificados y en términos generales, la llamada cuarta revolución industrial o revolución digital

genera las condiciones propicias para un ataque cibernético a gran escala que desestabilice la gobernabilidad, la economía, el sistema financiero, la prestación de servicios esenciales de cualquier país del mundo.

Las amenazas cibernéticas desconocen las fronteras nacionales y los límites organizacionales, toda vez que un ataque cibernético puede ser lanzado desde dentro de una organización por usuarios de confianza o desde lugares remotos, empleando desde un acceso no autorizado hasta un dispositivo de control o una red a través de una vía de comunicación de datos.

Las amenazas consideradas son las siguientes:

a. Difusión de mensajes a través de páginas Web para reclutar nuevos miembros.

b. Utilización de Internet para comunicarse incluyendo comunicación encriptada para coordinar actos terroristas.

c. Realizar transacciones financieras, lavado de dinero, extorción a cambio de información secuestrada y estafas a través de Internet.

d. Ataques Distribuidos de Denegación de Servicio (DDoS); es una forma relativamente sencilla y efectiva de hacer caer una Web. Las acciones se pueden realizar de forma voluntaria siguiendo las instrucciones dadas para iniciar el ataque a una hora señalada en una convocatoria mediante foros en una red, o utilizando redes de ordenadores previamente infectados por virus.

e. Los Botnets o robots de la red, son redes de ordenadores zombies que se emplean para realizar ataques, envíos masivos de correos basura y espionaje contra empresas. Un botnet se crea infectando ordenadores sin que sus dueños lo sepan. Cada máquina reclutada se pone en contacto con el ciber criminal a la espera de órdenes. Los ciber delincuentes de modo aislado o en una organización, construyen sus botnets y los venden o alquilan a empresas que desean mandar correo basura, bombardear o espiar a otras empresas, o robar datos bancarios. El virus puede enviarse por correo electrónico, aunque lo habitual es ponerlo en páginas Web que tengan muchas visitas. Una vez dentro del ordenador, el virus descargará un programa y lo instalará, es el bot, el lazo entre el ordenador infectado y el net, la red que permite su control remoto.

f

Utilización de virus para sistemas de control industrial: caso Stuxnet que es un programa de software dañino (malicioso) del tipo troyano muy avanzado, que aprovechó la vulnerabilidad MS10-0466 de los sistemas operativos Windows, empleados en los sistemas de adquisición de datos y control de supervisión (SCADA 14) fabricados por Siemens y que se utiliza en infraestructuras críticas tales como el control de oleoductos, plataformas petroleras, centrales eléctricas, centrales nucleares y otras instalaciones industriales con el objetivo de sabotearlos. Se piensa que una vez dentro de una planta podría reprogramar las centrifugadoras para hacerlas fallar sin que se detectara. Stuxnet es un virus muy sofisticado que utiliza técnicas de rootkit para instalarse en el sistema operativo. El troyano queda camuflado y latente en el equipo infectado hasta que su autor decide activarlo.

g

Ataques destructivos DDos a IoT. El potencial destructivo a nivel masivo de los ataques DDoS fruto de la inseguridad de los dispositivos IoT (Internet de Cosas). Se espera que los cibercriminales encuentren fácilmente la manera de ampliar su alcance debido al gran número de dispositivos IoT que contienen un código obsoleto basado en sistemas operativos mal mantenidos y aplicaciones con vulnerabilidades conocidas, ya que estos fueron elaborados para funcionar mas no para tener seguridad.

h

Sustitución de exploits por ataques sociales dirigidos. Los ataques cada vez son más sofisticados y convincentes e intentan confundir a los usuarios para que comprometan su propia seguridad. Un ejemplo, es común ver un correo electrónico que se dirige al destinatario por su nombre y afirma que tiene una deuda pendiente que el remitente ha sido autorizado a cobrar. La sorpresa, el miedo o la recaudación de impuestos por parte de autoridades son tácticas comunes y eficaces. El email los dirige a un enlace malicioso donde si los usuarios hacen clic quedan expuestos al ataque. Estos ataques de phishing ya no se pueden considerar como simples equivocaciones del usuario.

i

El uso del phishing. Estos ataques utilizan información detallada sobre los ejecutivos de la empresa para engañar a los empleados y que paguen por fraudes o comprometan cuentas. Ataques infraestructuras financieras críticas.

j

Explotación de la infraestructura intrínsecamente insegura de Internet. Todos los usuarios de Internet están a merced de antiguos protocolos que datan de su creación y su ubicuidad los hace casi imposibles de renovar o reemplazar. Estos protocolos arcaicos que han sido durante mucho tiempo la columna vertebral de Internet y las redes empresariales están a veces, sorprendentemente, sujetos a graves fallos.

k

Incremento en la complejidad de los ataques. Los ataques agrupan, cada vez más, múltiples elementos técnicos y sociales, y reflejan un examen cuidadoso y continuado de la red de la empresa que será víctima. Los atacantes comprometen varios servidores y endpoints mucho antes de que empiecen a robar los datos o actúen de forma agresiva. Controlados por expertos, estos ataques son estratégicos, no tácticos, y pueden causar mucho más daño.

l

Ataques con lenguajes y herramientas de administración integradas. Exploits basados en PowerShell, el lenguaje de Microsoft para automatizar las tareas administrativas. Como lenguaje de scripting, PowerShell evade las contramedidas centradas en ejecutables. También se ven más ataques que utilizan técnicas de penetración y otras herramientas administrativas que ya existen en la red de la víctima, sin necesidad de infiltrarse y no levantando sospechas.

m

Evolución del ransomware. A medida que más usuarios reconocen los riesgos del ataque de ransomware por correo electrónico, los cibercriminales están explorando otros métodos. Algunos están experimentando con un malware que vuelve a infectar más tarde, mucho después de que se pague por rescatar los datos, y algunos están empezando a usar herramientas integradas y sin malware ejecutable en absoluto, para evitar la detección por código de protección endpoint que se centra en los archivos ejecutables.

n

Aparición de ataques de IoT personales. Los usuarios de dispositivos IoT en casa pueden no notar ni incluso advertir que sus monitores son secuestrados para atacar la web de otra persona. Pero, una vez que los atacantes se hacen con un dispositivo en una red doméstica, pueden comprometer otros dispositivos, como ordenadores portátiles que contienen datos personales importantes. Se prevé que esto suceda más veces, así como más ataques que utilicen cámaras y micrófonos para espiar los hogares de las personas.

o

Crecimiento de malvertising y corrupción de ecosistemas de publicidad online: el malvertising, que propaga el malware a través de redes de anuncios online y páginas web, ha existido desde hace años. Estos ataques ponen de relieve mayores problemas en todo el ecosistema publicitario, como el fraude de clics, que genera clics de pago que no se corresponden con un interés real de clientes. El malvertising ha generado fraudes de clics, ha comprometido a los usuarios y robado a los anunciantes, todo al mismo tiempo.

p

La desventaja del cifrado. A medida que el cifrado se vuelve omnipresente, se ha vuelto mucho más difícil para los productos de seguridad inspeccionar el tráfico, haciendo que para los cibercriminales sea más fácil pasar de forma furtiva a través de las detecciones. Como era de esperar, los ciberdelincuentes utilizan el cifrado de manera creativa. Los productos de seguridad tendrán que integrar estrechamente las capacidades de red y de cliente, para reconocer rápidamente los incidentes de seguridad después de que el código se descifre en el punto final.

q

Aumento del enfoque en exploits contra sistemas virtualizados y cloud. Los ataques contra hardware físico (por ejemplo, Rowhammer) plantean la posibilidad de nuevas explotaciones peligrosas contra los sistemas cloud virtualizados. Los atacantes pueden abusar del host u otras máquinas virtualizadas que se estén ejecutando en un host compartido, atacar los privilegios y posiblemente acceder a los datos de otros. Por otro lado, a medida que Docker y todo el ecosistema de contenedores (o "sin servidor") se vuelvan más populares, los atacantes buscarán cada vez más descubrir y explotar sus vulnerabilidades de esta relativamente nueva tendencia informática. Es de esperar que se den intentos activos para hacer operativos tales ataques.

r

Ataques técnicos contra estados y sociedades. Los ataques tecnológicos se han vuelto cada vez más un tema político. Hoy en día, las sociedades se enfrentan cada vez más a la desinformación, como son las noticias falsas y sistemas de votación comprometidos en su seguridad. Se ha demostrado que los ciberataques podrían permitir a un mismo votante repetir el proceso de votación varias veces de manera fraudulenta, sin ser descubierto. Incluso, si los estados no están involucrados en los ataques contras sus adversarios en las elecciones, la percepción de esta capacidad de vulnerar el sistema democrático es en sí mismo un arma poderosa

Las amenazas deliberadas se clasifican en concordancia con la Declaración para el Registro del Comité Económico Conjunto, de Lawrence K Gershwin, oficial de Inteligencia Nacional de Ciencia y Tecnología de la Agencia Central de Inteligencia.

A **Gobiernos hostiles:** Su objetivo es debilitar, alterar o destruir un país. Sus objetivos secundarios incluyen el espionaje con fines de ataque, el espionaje de avance de la tecnología, la interrupción de la infraestructura para atacar a la economía de un país.

B **Terroristas:** Su objetivo es sembrar el terror entre la población civil. Sus objetivos secundarios son: ataques para debilitar la economía del país.

C **Espías industriales y grupos de crimen organizado:** Sus objetivos se basan en la consecución lucrativa. Sus objetivos secundarios incluyen ataques a la infraestructura para el beneficio de los competidores o de otros grupos antes mencionados, el robo de secretos comerciales, y obtener acceso y el chantaje a la industria afectada, con posible exposición pública como una amenaza.

D **Hacktivistas:** Su objetivo es apoyar su agenda política. Sus objetivos secundarios son la propaganda y causar daños al alcanzar notoriedad por su causa.

E **Hackers:** Son una amenaza insignificante generalizada, daño de larga duración a las infraestructuras a nivel nacional. Sin embargo, la gran población mundial de hackers representa una proporción relativamente alta amenaza de una interrupción aislada o breve causando graves daños. A medida que la población de los piratas cibernéticos crece, también lo hace la probabilidad de que un hacker excepcionalmente hábil y malicioso intentar y tener éxito en este tipo de ataque.

De igual forma, es importante considerar que gobiernos que han abordado el tema de la Ciberdefensa como uno de sus puntos de política interna más importante, realizaron una clasificación de la amenaza en el ciberespacio teniendo en cuenta su finalidad y origen, enmarcándolas en las siguientes:

1 **Estado Nación:** esta amenaza es potencialmente peligrosa debido al acceso a recursos, personal y tiempo que pueden no estar disponibles para otros actores. Los países pueden utilizar el ciberespacio para atacar y realizar espionaje contra cualquier país. Las amenazas estado-nación implican adversarios tradicionales y, a veces, en el caso de espionaje, incluso aliados tradicionales. Los estados-nación pueden

realizar operaciones directamente o pueden subcontratar a terceros para lograr sus objetivos.

2 **Actores Transnacionales:** son organizaciones formales e informales que no están vinculadas por las fronteras nacionales con el estado objetivo. Estos actores utilizan el ciberespacio para recaudar fondos, comunicarse con los públicos objetivos y entre ellos reclutar, realizar coordinaciones y ejecutar operaciones de ataque o desestabilizar la confianza en los gobiernos y llevar a cabo acciones terroristas.

3 **Crimen Organizado:** las organizaciones criminales pueden ser de carácter nacional o transnacional en función de cómo se organizan. Las organizaciones criminales roban información para su propio uso o la venden para obtener beneficios económicos.

4 **Las principales actividades que realiza el crimen organizado** suelen estar relacionadas con el robo de información de tarjetas de crédito o de los certificados digitales asociados, con el fraude telemático, con operaciones bancarias o con cualquier transacción desde internet, con el blanqueo de dinero y con el robo de identidades asociado a inmigración ilegal.

5 **Individual o de grupos pequeños:** Los individuos o pequeños grupos de personas pueden interrumpir o tener acceso a una red o sistema informático; estas personas son más conocidos como "hackers". Las intenciones de los piratas informáticos varían. Algunos son pacíficos y hackean sistemas para descubrir vulnerabilidades, a veces comparten la información con los propietarios. Otros hackers tienen motivaciones políticas y utilizan el ciberespacio para difundir su mensaje a los destinatarios. Por otro lado, existen hackers que desean fama o estatus y la obtienen irrumpiendo en sistemas de seguridad o creando malware que origina caos en sistemas comerciales o gubernamentales. Los hackers también pueden ser utilizados por otras amenazas del ciberespacio, como las organizaciones delictivas, con el fin de realizar operaciones encubiertas contra objetivos específicos, mientras que preservan su identidad o crean una negación plausible.

6 **Amenaza Tradicional:** Las amenazas tradicionales normalmente surgen de los estados que emplean las capacidades y fuerzas militares reconocidas en formas bien definidas de conflicto militar. En el ciberespacio, estas amenazas pueden ser menos entendidas debido a la continua evolución de las tecnologías y métodos. Estas amenazas

se centran generalmente en contra de las capacidades ciberespaciales que permiten a una fuerza militar el desarrollo de sus operaciones a nivel terrestre, marítimo o aéreo e intentan negar la libertad de acción militar y el uso del ciberespacio. Pueden ser un vector de amenaza crítico sobre todo en tiempo de crisis o conflicto. Muchas naciones disponen de esta capacidad sólo en los servicios de inteligencia, aunque en otras, las Fuerzas Armadas disponen de unidades que tienen asignadas misiones de ataque a los sistemas de información de los adversarios. Estas unidades son la evolución de las capacidades de inteligencia de señales (SIGINT) disponibles en un sinnúmero de países y pueden estar catalogadas, así:

7 **Servicios de Inteligencia:** Se considera el principal vector de amenaza contra la información sensible o clasificada manejada por los sistemas de información gubernamentales y de empresas nacionales de sectores estratégicos (y especialmente aquellas relacionadas con defensa). Disponen de medios y recursos técnicos y una gran capacidad de acción. Sus actividades son muy prolongadas en el tiempo y el tipo de herramientas que utilizan normalmente muestran unos niveles muy bajos de detección en los sistemas de seguridad de los sistemas objetivos.

8 **Ciberespionaje:** Los ciberataques más sofisticados se esperan de los servicios de inteligencia y las agencias de operaciones de información militares extranjeras. En la mayoría de los casos, estos atacantes disponen de muchos recursos, tienen la paciencia necesaria para encontrar la debilidad del sistema y durante la explotación del ataque intentan lograr la mayor persistencia en el mismo, para ello instalan puertas traseras en previsión de una posible detección del ataque.

9 **Espionaje industrial:** Son compañías o gobiernos que tienen interés en disponer de información crítica de desarrollos tecnológicos e industriales de industrias de la competencia.

10 **Amenaza irregular:** Las amenazas irregulares pueden utilizar el ciberespacio como un medio no convencional para hacer frente a las ventajas tradicionales. Estas amenazas pueden también manifestarse a través de la focalización de las capacidades ciberespaciales y de infraestructura selectiva de un adversario. Por ejemplo, los terroristas

podrían usar el ciberespacio para llevar a cabo operaciones contra los sectores financiero e industrial, así como el lanzamiento de otros ataques físicos. Los terroristas también utilizan el ciberespacio para comunicarse anónimamente, de forma asíncrona y sin estar atados a configurar ubicaciones físicas. Tratan de protegerse de la aplicación de la ley, la inteligencia y las operaciones militares a través del uso de productos de seguridad y servicios comerciales fácilmente disponibles en el ciberespacio. Las amenazas irregulares de elementos criminales y los defensores de las agendas políticas radicales tratan de utilizar el ciberespacio para sus propios fines de impugnar el gobierno, las empresas o los intereses sociales.

11 **Amenaza catastrófica:** Las amenazas catastróficas involucran la adquisición, posesión y uso de armas de destrucción masiva o los métodos que producen efectos similares a armas de destrucción masiva. Estos eventos físicos (cinética), pueden tener profundos efectos en el dominio cibernético, claves para degradar o destruir infraestructuras vitales, como los sistemas SCADA. Los ataques bien planeados en los nodos claves de la infraestructura del ciberespacio tienen el potencial de producir el colapso de la red y generar efectos en cascada que pueden afectar gravemente las infraestructuras críticas a nivel local, nacional o incluso mundial. Por ejemplo, un pulso electromagnético podría causar daños a los segmentos del dominio ciberespacio en el que deben confluir las capacidades operacionales.

12 **Amenaza Destructiva:** Son tecnologías innovadoras que puedan negar o reducir las actuales ventajas de un estado en los dominios bélicos. La investigación global, la inversión, el desarrollo y los procesos industriales proporcionan un ambiente propicio para la creación de los avances tecnológicos. Se debe estar preparado para la posibilidad de un aumento de los avances de los adversarios debido a la continua difusión de las tecnologías del ciberespacio.

13 **Amenaza Natural:** Las amenazas naturales que pueden dañar e interrumpir el ciberespacio incluyen eventos como inundaciones, huracanes, erupciones solares, rayos y tornados. Este tipo de eventos suelen producir efectos muy destructivos. Se debe estar bien preparado con elementos de respaldo para mantener o restablecer sistemas claves. Estos eventos también proporcionan a la amenaza la oportunidad de sacar provecho de la degradación de la infraestructura

y el desvío de la atención y los recursos.

14 **Amenaza accidental:** Las amenazas accidentales son impredecibles y pueden tomar muchas formas. Desde una retroexcavadora que corte un cable de fibra óptica de un nodo clave del ciberespacio, hasta la introducción involuntaria de virus son amenazas accidentales que, sin ninguna intención, pueden interrumpir el funcionamiento del ciberespacio. Sin embargo, las investigaciones posteriores a los accidentes muestran que la gran mayoría de los accidentes se pueden prevenir y que se pueden adoptar medidas para reducir los accidentes.

15 **Amenaza interna**: La amenaza interna se refiere a los actos perjudiciales que miembros internos con cierto nivel de confianza pueden llevar a cabo algo para causar daño a la organización, o para realizar un acto no autorizado que beneficia al individuo. La "información privilegiada" en manos de un individuo, puede convertirse en uno de los blancos más rentables para la amenaza, ya que este puede acceder al sistema de una organización para extraer información o puede incluso afectar el normal funcionamiento de la red y sus servicios.

Hacking Político/Patriótico: Este tipo de actividad es el reflejo de un conflicto regional, étnico, religioso o cultural en el ciberespacio. Así, son frecuentes los ataques de denegación de servicio entre China y Japón; Azerbaiyán y Turquía; India y Pakistán, chiitas y sunitas o en el conflicto entre árabes e israelíes. Normalmente no tiene un gran impacto en los sistemas de información del país o área que recibe el ataque pues la actividad normalmente se limita a ataques realizados contra servicios web y no alcanza los sistemas internos.

16 **Terrorismo:** Los grupos terroristas emplean el ciberespacio como una herramienta más para realizar sus actividades delictivas. Normalmente lo emplean para establecer comunicaciones entre sus células y grupos de apoyo, para obtener información de posibles objetivos, para realizar acciones de propaganda o para obtener financiación a sus actividades. La posibilidad de combinar ataques físicos a infraestructuras de internet con ataques cibernéticos complejos es poco probable por el nivel tecnológico del ciberterrorismo, pero el empleo de internet para actividades de propaganda, reclutamiento y comunicaciones se ha incrementado por los nuevos servicios que están a disposición como las redes sociales.

Virtualmente todo grupo terrorista ha establecido su presencia en internet, porque las posibilidades que ofrece son diversas:

1. Permite un medio de divulgación amplio y económico, ya que los públicos a los que llega internet son muy diversos:
2. En primer lugar, está la opinión pública internacional, a la que ofrecen su mensaje simultáneamente en los principales idiomas del planeta (inglés, castellano, alemán, francés, etc.).
3. Buscan dirigirse a los que les ayudan y sobre todo a los que pueden ayudarlos en un despliegue de ventas (camisetas, bolsas, banderas, vídeos), para aumentar su base de simpatizantes.
4. Como uno de sus objetivos es causar miedo, los terroristas incluyen no sólo a los gobiernos sino también a los ciudadanos, con el objetivo de desmoralizarlos, amedrentarlos y presionarlos para cambiar su conducta. No se puede separar el ciberterrorismo de la guerra psicológica. Uno de los mejores ejemplos fue la publicación en internet de los asesinatos de civiles occidentales en la guerra de Irak.

17 **Minería y extracción de datos (Footprinting):** Es la capacidad de obtener información sobre objetivos sin necesidad de romper ningún sistema. Por ejemplo, Google Earth permite a cualquier persona con una conexión normal obtener fotos de satélite de las principales ciudades del mundo y en unos pocos segundos, obtener las coordenadas exactas de instalaciones químicas o de reactores nucleares.

18 **Comunicaciones seguras mediante la utilización de programas gratuitos o comerciales**, e inclusive redes específicas de ocultamiento y VPN's que permiten la clandestinidad y obstruyen las posibilidades de trazabilidad y seguimiento de los actores de los hechos delictivos.

En materia de ciberseguridad las amenazas son:

a. El ransomware como la forma de ciberataque más extendida y dañina financieramente.

b. Ataques más específicos y rentables a objetivos más grandes que causen mayor afectación económica.

c. El fraude de tarjeta no presente (CNP) como la principal amenaza financiera al ciudadano.

d. Defraudaciones al comercio electrónico.

e. Explotación a niños, niñas y adolescentes, vulnerables en todo el mundo.

f. Nuevas tecnologías como medio transversal para la criminalidad convencional como criptomonedas o la web oscura.

g. Recopilación de datos de las malas prácticas de seguridad de datos y la ingeniería social.

h. Compromiso comercial por correo electrónico (BEC), aprovechando las estructuras corporativas segregadas y las brechas internas en los procesos.

i. Denegación de servicios y ataques a la continuidad del negocio

j. Técnicas como malware e intrusión en la red.

k. Flexibilidad en la variación de ataques de acuerdo a volúmenes, objetivos y nivel de sofisticación.

l. Vulnerabilidades conocidas en las tecnologías existentes y nuevas tecnologías.

m. Los datos siguen siendo el elemento clave, en la perspectiva del delito. (la seguridad de los datos con respecto a las organizaciones y la falta de conciencia de los consumidores).

n. Ataques a la cadena de suministro, ejemplo: servicios tercerizados en la nube.

ñ. La facilidad de uso, la variedad de mercado existente y la base de clientes (red oscura).

o. Explotación de plataformas emergentes para el terrorismo, en pro de sus estrategias de comunicación.

3.3. Desafíos

En este sentido, Colombia al igual que todos los países que vienen adoptando las tecnologías de información y las tecnologías de operación para optimizar el desarrollo de sus procesos productivos, económicos, sociales, políticos e incluso de seguridad y defensa nacional, se encuentran frente a un escenario de cambios revolucionarios a los cuales se hace necesario adaptarse y prepararse para evitar que pueda ocasionar daños de alto impacto en las infraestructuras críticas cibernéticas del país que afecten directamente la prestación de los servicios básicos a la población y por consiguiente afecte la prosperidad económica y social del país.

La dinámica del futuro presenta un escenario de conflictos o ciberguerras basados en plataformas tecnológicas en una lucha sin tregua por la información, por inhabilitar un sistema crítico o quizás por denegar un servicio esencial a una nación, todo esto, desde el componente cibernético.

Es por esto, que los focos de atención en materia de ciberseguridad y ciberdefensa se deben concentrar en desarrollar capacidades activas, pasivas y ofensivas altamente especializadas, a fin de obtener la superioridad en el ciberespacio. Dicho componente

cibernético puede fortalecerse basando sus capacidades en tecnologías, el recurso humano en cantidad, educación y entrenamiento; investigación, innovación y desarrollo en materia cibernética, así será posible desarrollar capacidades diferenciales y estratégicas al momento de enfrentar las ciberamenazas.

Considerando que las amenazas cibernéticas crecen a ritmos y velocidades desconcertantes, la ciberseguridad y ciberdefensa cobran un papel trascendental en el quinto dominio de la guerra: el ciberespacio. De acuerdo con estudios realizados por el Foro Económico Mundial, en el Informe Global Risk Report 2018, se presentan los riesgos más significativos a nivel global, teniendo mayor relevancia las amenazas cibernéticas y los ciberataques o ataques cibernéticos a gran escala por el grado de probabilidad de ocurrencia.

En ese orden, los desafíos se clasifican en gobernanza, capacitación, operaciones cibernéticas, legislación, doctrina, cooperación, recurso humano, infraestructura, investigación, innovación y desarrollo, así:

1. Promover Leyes de Seguridad y Defensa Nacional que incluyan la Ciberseguridad y Ciberdefensa, la protección a la infraestructura crítica y los activos estratégicos como marco jurídico de las acciones y operaciones del Estado en el ciberespacio.

2. Fortalecimiento y articulación de las capacidades entre todas las instancias responsables de la seguridad digital.

3. Contar con el Centro Nacional para protección de las Infraestructuras críticas cibernéticas nacionales para centralizar las capacidades del gobierno en materia de prevención, análisis, protección, investigación, judicialización y defensa cibernética.

4. Contar con el Centro Nacional de Excelencia en Ciberdefensa para la capacitación, investigación, innovación, desarrollo, observatorio cibernético y laboratorios especializados en materia cibernética. (Incluye una Escuela de Ciberdefensa para la Fuerzas Pública).

5

Fortalecer la ciberseguridad y ciberdefensa a través del liderazgo de la Fuerza Pública como un componente estratégico nacional. En este sentido considerar la ciberseguridad y ciberdefensa en las políticas de seguridad y defensa como un factor transversal que garantice ventajas estratégicas ante potenciales amenazas internas y externas.

6

Diseñar y documentar una Estrategia Nacional de Ciberdefensa.

7

Contar con Unidades móviles de Ciberdefensa en las Fuerzas Militares con capacidad para desarrollar operaciones cibernéticas de acuerdo con su misión.

8

Incrementar y mantener la capacitación y entrenamiento de los especialistas en materia cibernética a fin de prevenir, detectar, neutralizar o dar respuesta a las nuevas amenazas y ataques cibernéticos. Al mismo tiempo desarrollar programas de prevención y sensibilización en ciberseguridad y ciberdefensa a nivel sectorial y de infraestructuras críticas cibernéticas que permitan generar una cultura cibernética nacional.

9

Comprender las intenciones y capacidades estratégicas de la amenaza en materia cibernética y sus implicaciones a la seguridad y defensa nacional, para detectar y alertar oportunamente los planes y ataque en el ciberespacio.

10

Aplicar medidas para detectar e impedir la materialización de ataques cibernéticos, así como identificar las fuentes que los originan para ejercer la respuesta oportuna, legítima y proporcional.

11

Planear y conducir operaciones cibernéticas en tiempos de paz y en tiempos de guerra en apoyo a las operaciones de la Fuerza Pública.

12

Incrementar las operaciones cibernéticas estratégicas y tácticas de las Fuerzas Militares para la Defensa y Seguridad Nacional.

13

Implementar las medidas necesarias para la resistencia y recuperación ante un ataque cibernético (resiliencia cibernética), procurando el sostenimiento de las operaciones y el respaldo de la información crítica de la Fuerza Pública.

14

Brindar asesoría en materia de ciberseguridad y ciberdefensa para el desarrollo de normas, políticas nacionales y Leyes que determinen las reglas de enfrentamiento en el ciberespacio bajo los principios de legalidad y protección del Estado.

15

Fortalecer el trabajo y la doctrina conjunta y coordinada en materia cibernética y actualizarla conforme a los cambios del entorno cibernético y las amenazas cibernéticas emergentes.

16

Promover y articular la cooperación nacional e internacional como una estrategia entre las entidades responsables de ciberdefensa y ciberseguridad, promoviendo el intercambio de información de amenazas y alertas tempranas; así como gestionar la adhesión a organismos internacionales en materia cibernética, que permitan obtener información anticipada de las amenazas trasnacionales.

17

Desarrollar y fortalecer las relaciones interinstitucionales en materia de ciberdefensa y ciberseguridad teniendo en cuenta los constantes cambios y el desarrollo acelerado del dominio cibernético.

18

Establecer en coordinación con las Fuerzas el plan de carrera que integre la capacitación, el entrenamiento y la proyección del personal en ciberseguridad y ciberdefensa a fin de garantizar el fortalecimiento del componente cibernético en las Fuerzas Militares.

19

Mantener y fortalecer las habilidades del personal en materia de ciberdefensa y ciberseguridad garantizando su continuidad para el desarrollo de operaciones en el ciberespacio.

20

Desarrollar la infraestructura física adecuada, toda vez que esta capacidad requiere de sitios especializados para garantizar el desarrollo eficiente de las acciones y operaciones cibernéticas estratégicas..

21

Implementar y fortalecer la infraestructura tecnológica en materia de ciberdefensa y ciberseguridad, teniendo en cuenta que el componente cibernético basa su accionar en personas, sistemas tecnológicos y medios de trasmisión.

22

Garantizar el desarrollo de operaciones cibernéticas integradas a las operaciones de la Fuerza Pública, con la finalidad de defender los intereses nacionales en el ámbito cibernético, infraestructura crítica cibernética y afectar o deshabilitar sistemas enemigos en o a través del ciberespacio.

23

Derrotar las amenazas cibernéticas mediante el empleo de las operaciones cibernéticas.

24

Identificar y advertir con anticipación la presencia de amenazas cibernéticas contra la seguridad y defensa nacional.

25

Participar en eventos internacionales, foros, ciberolimpiadas, ejercicios cibernéticos o cualquier otro que permitan la actualización de los avances en guerra cibernética.

26

Analizar y evaluar las capacidades de la amenaza interna y externa para proponer las respuestas adecuadas.

27

Planear y realizar ejercicios de entrenamiento cibernético nacional e internacional.

28

Desarrollar la industria militar cibernética con el propósito de contar con plataformas y herramientas propias de ciberdefensa a través de un programa de investigación, desarrollo e innovación consolidando e integrando los grupos de investigación de la Fuerza Pública, la academia y la empresa pública y privada.

29

Estructurar del plan de carrera de ciberdefensa con la implementación de la Especialidad de Ciberdefensa.

30

Crear la Escuela de Ciberseguridad y Ciberdefensa, para la instrucción y entrenamiento del personal.

31

Implementar los programas de capacitación y sensibilización a fin de ampliar la cobertura en materia cibernética en las Escuelas de formación, las empresas públicas y privadas.

32

Fortalecer la capacitación en idiomas al personal de ciberseguridad y ciberdefensa para el aprovechamiento de cursos internacionales, intercambio de información y entendimiento de los lenguajes de programación especialmente inglés, ruso y mandarín.

33

Incrementar el pie de Fuerza del Comando Conjunto Cibernético mediante la incorporación de personal especialista o capacitación de inmersión total en materia cibernética.

34

Realizar la estructuración de un cuerpo de reserva cibernética, conformada por expertos nacionales para la actuación en un proceso de movilización.

35

Fortalecer la doctrina, la estandarización de procesos misionales operacionales y la estandarización de protocolos de enlace de plataformas informáticas.

36

Crear los manuales de ciberdefensa, de operaciones cibernéticas y de funcionamiento de los Centros Cibernéticos; de acuerdo a los lineamientos de interoperabilidad con organismos y Estados aliados.

37

Sostener la vigilancia tecnológica para nuevos desarrollos de software, hardware y técnicas de asistencia online, a través del monitoreo de red e inteligencia de amenazas.

38

Mejorar la protección de los datos institucionales a través de mecanismos propios como la computación en la nube privada estatal con herramientas de vigilancia, red de datos restringida y red de telefonía celular cifrada.

Compartir información en tiempo real, a través de canales seguros de comunicación que permitirá:

- a. Garantizar la preservación de información volátil.
- b. Generar una taxonomía común.
- c. Compartir buenas prácticas contra la cibercriminalidad.
- d.Fomentar la innovación tecnológica.
- e. Construcción de protocolos de prevención y actuación policial.
- f. Fomentar las capacitaciones y la inversión en tecnología escalable con altos estándares de calidad y seguridad.

Desarrollar el uso de plataformas para la cooperación con el fin de:

- a. Intercambiar conocimiento en el sector público, privado y agencias del Estado.
- b. Identificar nuevas modalidades y vectores de ataque.
- c. Obtener resultados y contextualización del fenómeno.
- d. Identificar vulnerabilidades.
- e. Desarrollar el grupo de trabajo conjunto, coordinado e interagencial.

Establecer la cooperación, a través de:

- a. Desarrollo de programas de actualidad.
- b. Protección de la imagen institucional.
- c. Capacitación.
- d. Formación de Policías, Fiscales y Jueces.

Fortalecimiento legislativo.

- a. Regulación sector privado-público.
- b. Cooperación y suministro de datos.
- c. Tratados de Asistencia Legal Mutua (MLAT).

CAPÍTULO
CUATRO

OBJETIVOS Y LÍNEAS DE ACCIÓN ESTRATÉGICAS

Objetivos

4.1. Objetivo General

Garantizar y proteger la utilización segura del ciberespacio por parte de los ciudadanos y de la Nación, mediante el despliegue de las capacidades de defensa y seguridad del Estado, que permita mitigar los riesgos y amenazas mediante un trabajo coordinado y de cooperación, que contribuya al crecimiento económico y social del país.

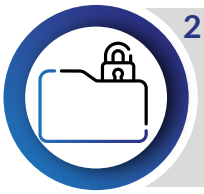
4.2. Objetivos Específicos

Objetivo 1

Fortalecer la confianza y la seguridad digital de los individuos y de la Nación, a través de la anticipación y prevención, de los riesgos identificados en el ciberespacio, generando la cultura ciberseguridad.

Líneas de Acción

1 Identificar los riesgos existentes en el ciberespacio nacional y global, que permitan generar un mecanismo de respuesta efectiva.



2 Promover la ciberseguridad, para responder a la necesidad de privacidad y protección de información personal, dentro del marco constitucional de los derechos fundamentales.

3 Definir las buenas prácticas para garantizar la resiliencia frente a las amenazas materializadas en los riesgos identificados contra la ciberseguridad del Estado Colombiano.

4 Revisión y ajuste de la normatividad penal y administrativa vigente, de los delitos acaecidos en el entorno digital, así mismo los comportamientos contrarios a la convivencia.

5 Desplegar en el ecosistema digital una campaña masiva de prevención, divulgando las modalidades de criminalidad en el entorno digital que emplean los ciberdelincuentes, con el fin de lograr una disrupción al comportamiento de este fenómeno.

6 Estructurar un componente estratégico de capacidades tácticas y operacionales, de respuesta oportuna, encargados de garantizar la seguridad del ciberespacio, y desarrollar las actuaciones judiciales en contra de los ciberdelincuentes.

Líneas de Acción

1. Fortalecer las capacidades de las agencias de la ley encargadas de prevenir, anticipar e investigar los comportamientos que afecten la ciberseguridad de Colombia.

2. Crear programas de apoyo a la persecución penal y prevención de conductas que afecten la seguridad ciudadana, mediante canales oficiales de denuncia como un tanque de concentración y veeduría ciudadana que tenga participación de todos los sectores garantes de derechos y libertades en internet.

3. Aumentar las capacidades en investigación criminal, para generar una respuesta oportuna en la identificación, individualización y persecución penal de los ciberdelincuentes

Objetivo 2

Fortalecer la legislación, la respuesta oportuna y las capacidades operacionales de investigación y judicialización de la cibercriminalidad, desde un enfoque de seguridad pública (ciudadana), garantizando los derechos fundamentales en el espacio digital.

Objetivo 3

Protección y seguridad de activos estratégicos y críticos del país, incluidos los ciberactivos.

Líneas de Acción

1. Implementar procesos permanentes de identificación de las amenazas y análisis de las vulnerabilidades, los impactos y la probabilidad de ocurrencia de los ataques cibernéticos a la Infraestructura Crítica y Cibernética nacional para determinar los niveles de seguridad y los criterios de activación de las acciones asociadas para su respuesta

2. Establecer una estructura intersectorial que permita dirigir y coordinar las actuaciones necesarias para proteger las infraestructuras críticas cibernéticas, con el fin, de movilizar y articular las capacidades logísticas, operativas y técnicas para la toma de decisiones y respuesta ante eventos e incidentes cibernéticos

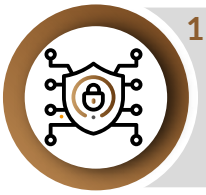
3. Garantizar la protección y prestación de servicios esenciales ante ciberataques.

4. Desarrollar una normativa que garantice la protección de infraestructura crética tanto de propiedad pública como privada.

Objetivo 4

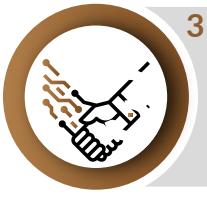
Promover la cooperación interinstitucional y de los sectores público y privado para la protección del ciberespacio.

Líneas de Acción



1. Proteger de manera transversal los ecosistemas privados y públicos a nivel de personas naturales, empresas e instituciones públicas.

2. Promover el intercambio de mejores prácticas de ciberseguridad entre sectores público y privado y entre instituciones de diferente índole.



3. Gestionar de manera compartida entre diferentes actores involucrados, la seguridad y defensa del ciberespacio priorizando procesos críticos para el país.

4. Monitorear de manera permanente e integral la seguridad de los diferentes procesos que se lleven cabo o se canalicen a través del ciberespacio.

5. Promover el uso seguro del ciberespacio internacional y la cooperación entre países para judicialización ante uso ilícito o malicioso del mismo.

Líneas de Acción

1. Promover el intercambio de mejores prácticas de ciberseguridad entre países.
2. Adoptar estándares internacionales de seguridad y defensa del ciberespacio que garanticen el mantenimiento de relaciones confiables y fluidas con otros países.
3. Garantizar la seguridad de procesos críticos que involucren la intervención de entidades internacionales
4. Protección multilateral de ciberespacios compartidos entre diferentes países.

Objetivo 5

Promover la cooperación internacional y adhesión de Colombia a iniciativas de ciberseguridad y ciberdefensa.

Objetivo 6

Sensibilizar, concientizar, promover la educación y la cultura de ciberseguridad.

Líneas de Acción

1. Fomentar el conocimiento de riesgos y amenazas existentes en el ciberespacio y de las medidas para su mitigación

2. Promover el sentido de responsabilidad compartida por parte de personas y entidades usuarias del ciberespacio.

3. Crear espacios y medios para comunicar mejores prácticas en términos de ciberseguridad.

4. Diseñar programas específicos y el plan de carrera a aplicar para el talento humano dedicado a la ciberseguridad y ciberdefensa.

4.3. Consideraciones Finales

Es importante, que las diferentes entidades del Estado, así como las privadas, socialicen en todo momento los riesgos que conlleva el uso masificado de la tecnología, tales como las comunicaciones y de la información, en contra de la Ciberdefensa y Ciberseguridad nacional, factores, que inciden en la preservación de nuestros intereses nacionales, de la infraestructura critica del país, de las entidades gubernamentales y privadas, llegando afectar nuestra Seguridad Nacional.

Es por lo anterior, que la Ciberseguridad y Ciberdefensa, son un objetivo prioritario para el Estado Colombiano, de tal manera, que se pueda participar activamente y de forma segura en el ciberespacio, facilitando elementos de entendimiento y confianza mutua, con unas relaciones sólidas en el ámbito de la Seguridad y Ciberdefensa.

El objetivo general que busca la Estrategia Nacional de Ciberseguridad y Ciberdefensa, es la de garantizar la seguridad y defensa de la nación a través del aseguramiento y direccionamiento estratégico del gobierno nacional, el cual debe asignar roles y funciones, así como, los criterios técnicos necesarios para una adecuada respuesta, ante cualquier ciberataque, espionaje, sabotaje o fraude, proveniente de otro país, grupo organizado o particulares, entre otros.

Es de este modo, que Colombia no se ha quedado atrás en su evolución tanto tecnológica como normativa, donde se aplaude el constante trabajo efectuado por las diferentes partes interesadas, pero a pesar de esta ardua labor, aún se requiere de una urgente revisión y actualización de normas penales y de procedimiento, a través de un marco legal robusto e integrado con la automatización de servicios y de los sistemas de la gestión pública, al igual, de la modernización de sus procesos a través de las TIC, en forma segura y confiable, logrando con esto, equiparar y dar las herramientas al Estado y al sector privado, que le permitan contrarrestar las amenazas a la Ciberseguridad y Ciberdefensa, que a diario enfrenta el país.

Como se mencionó anteriormente, se debe realizar a nivel nacional, un proceso de identificación, autoevaluación y categorización de nuestros centros de gravedad, que generen conciencia ante las potenciales amenazas en Ciberseguridad y Ciberdefensa, encaminadas a proteger la privacidad de la población, la protección de los datos, organizaciones privadas y gubernamentales, pero lo más importante, hacia la gestión de la protección de los centros de poder de la Nación.

CAPÍTULO
CINCO

ANEXOS

Anexos

Anexo A

5 Plan de Capacitación Mínima Para el Personal de Profesionales de la Ciberseguridad y Ciberdefensa.

El presente anexo, tiene por finalidad establecer la capacitación mínima que debe adoptar cada una de las Instituciones del Estado y del Sector Privado, las cuales, son necesarias para promover en el personal de profesionales y personal técnico, una adecuada oferta académica, que le permita al personal afrontar los diferentes desafíos que presenta la ciberseguridad y ciberdefensa, proporcionando las herramientas para la defensa y seguridad de Colombia, difundir una cultura del uso seguro del ciberespacio, así como, estimular a partir de la capacitación, un Plan de Carrera acorde a las necesidades de la nación.

5.1.Oferta académica y Experiencia Mínima propuesta en Ciberseguridad y Ciberdefensa

Basados en una apropiada oferta académica, nos prepararemos adecuadamente para un ciberataque o ciberdelito, los cuales, pueden ser ejecutados al interior del país o desde el exterior, ya sea por un organismo estatal, privado, grupo organizado, delincuencia transnacional, terrorismo o persona en forma individual, entre otras; siendo ideal, contar con una respuesta multisectorial con las instituciones del Estado y del sector privado.

En consecuencia, es necesario que cada una de las instituciones, establezca la certificación básica y capacitación mínima requerida, la cual, debe estar orientada tanto a los funcionarios del Área de Gestión y Administración; así como, del Área Operativa, enfocando dicha formación en tres fases o niveles de capacitación, basada en sus propias necesidades.

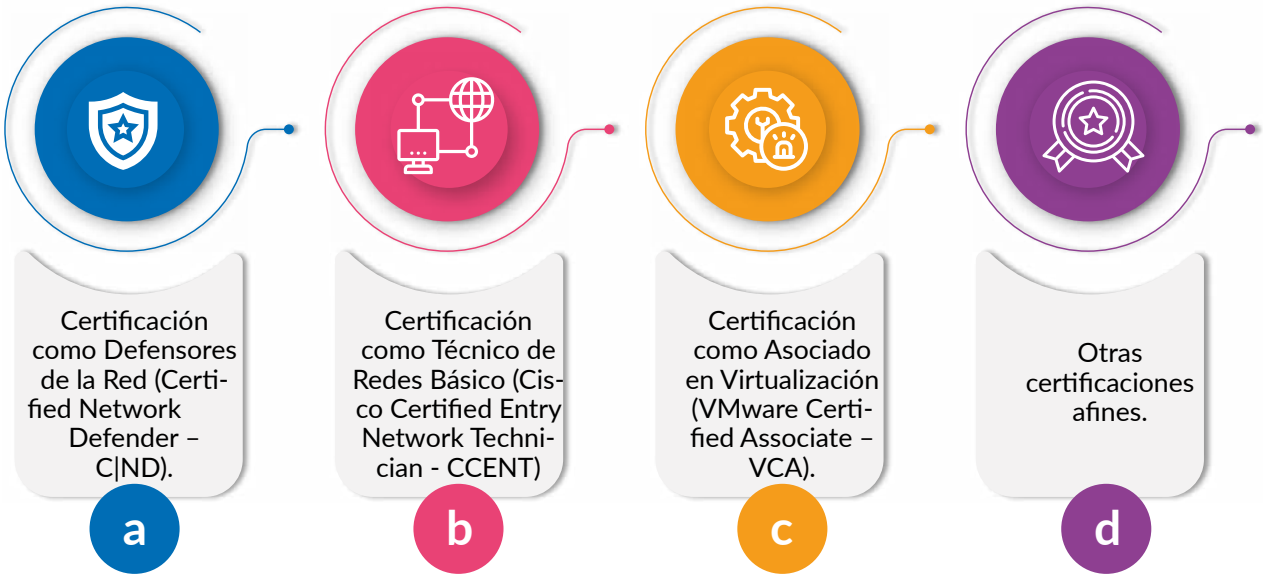
La siguiente, es la Propuesta Mínima de Capacitación que se recomienda para cada fase o nivel, la cual, se encuentra alineada con el Plan de Carrera de la presente estrategia

5.1.1 Primera Fase o Nivel Básico - Área Operativa y Área de Gestión y Administración

Durante la primera fase se debe brindar capacitación y certificación básica, tanto a los funcionarios del Área Operativa, como al personal del Área de Gestión y Administración, que les permita contar con las capacidades para realizar procesos de seguridad en el nivel básico.

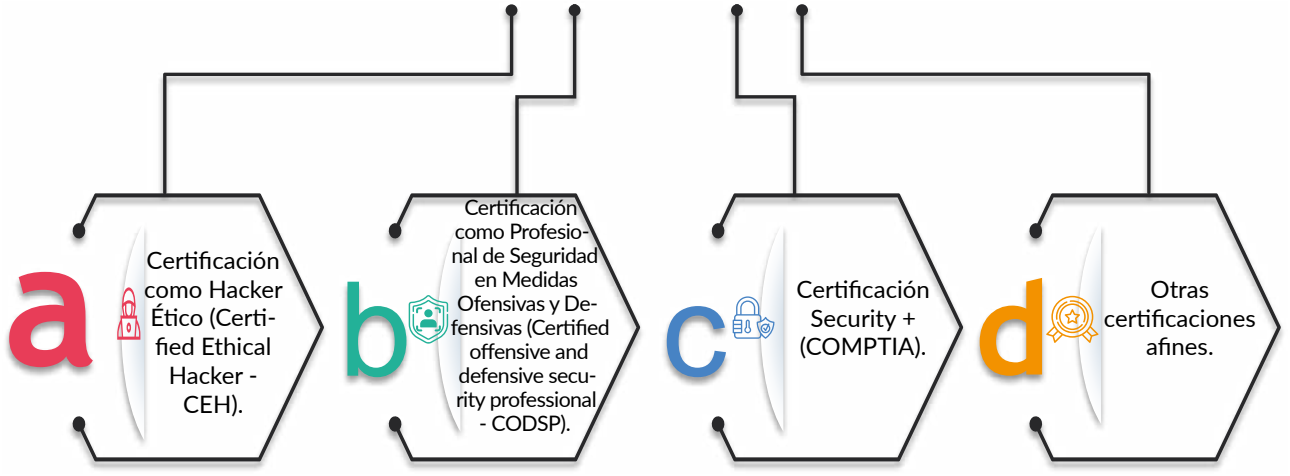
Dicha capacitación, le permitirá proteger, detectar y responder, ante cualquier incidente cibernético de primer nivel.

Algunas de las certificaciones que se pueden alcanzar en esta primera Fase, son:



Posteriormente, es necesario certificar al personal que labora en las áreas de Ciberdefensa y Ciberseguridad, para la realización de pruebas de penetración (pentesting), permitiendo entender, inspeccionar y valorar, la infraestructura de red con el consentimiento institucional, con el fin de encontrar las vulnerabilidades en cuanto a seguridad, que los hackers informáticos podrían afectar y atacar.

Para ello, el personal deberá contar como mínimo con las siguientes certificaciones:



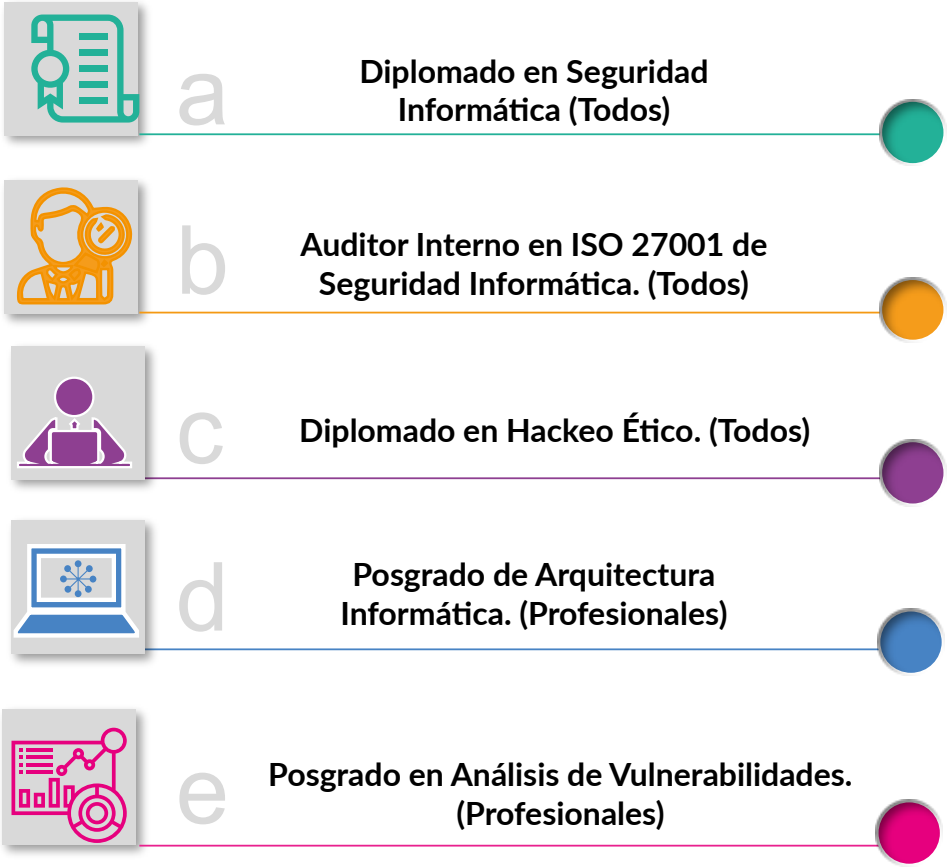
Entre las normas internacionales por las cuales se pueden regir las organizaciones del Estado y del Sector Privado, que permitirán al personal de esta área, desarrollar competencias para lograr el aseguramiento, la confidencialidad e integración de los datos, así como mitigar o eliminar el riesgo, se encuentran:

El personal capacitado en Ciberdefensa y Ciberseguridad, al concluir la primera fase de su Plan de Carrera, deberá desempeñar y aplicar su capacitación por un periodo mínimo de dos años, lo que le permitirá incrementar su experiencia y aplicarla en beneficio de las diferentes instituciones del Estado y del sector privado que así lo consideren, siendo posteriormente promovidos a la segunda fase de entrenamiento.

5.1.2. Segunda Fase o Nivel Medio

5.1.2.1. Área Operativa

En esta fase se requiere de Profesionales en Ingeniería de Sistemas, Ingeniería Electrónica, así como, de Técnicos y Tecnólogos del sector, en los cuales se aplican los siguientes niveles de capacitación:



En esta fase o nivel, los profesionales y el personal técnico, estarán en condiciones de atender problemas de mediana y alta complejidad.

El personal de profesionales, estará en la capacidad de diseñar programas y redes, cuya arquitectura esté provista de defensas para ciberataques.

Finalmente, también podrán, diseñar y utilizar herramientas para detectar, bloquear y solucionar ataques de segundo grado.

5.1.2.2. Área de Gestión Administración

En esta fase se requieren profesionales en Ingeniería de Sistemas, Ingeniería Industrial, Administración de Empresas, Sicología, Sociología, Economía, Derecho y Ciencias Políticas, siempre y cuando esta formación de pregrado este acompañada de programas formales de Posgrado y Especialización o sus equivalentes en el campo de la informática y de seguridad de la información.

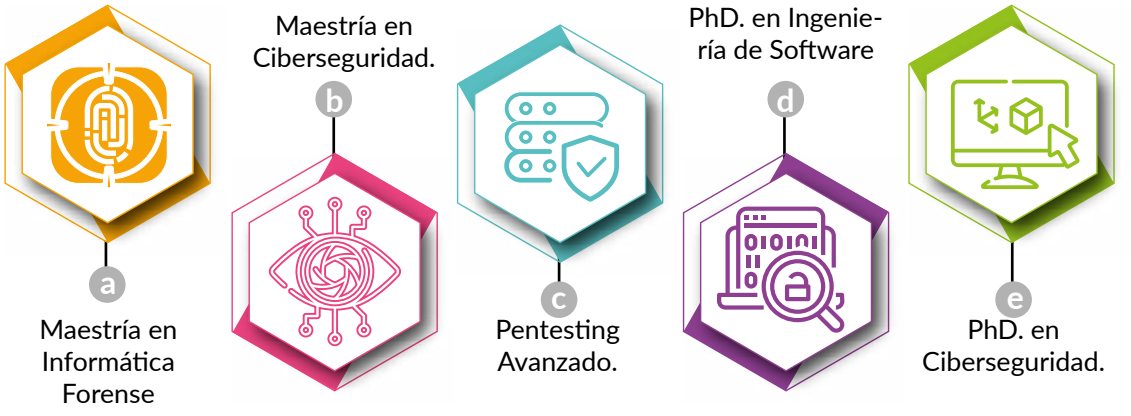
El personal de profesionales descrito en el punto anterior, debe acceder a la siguiente capacitación.

En este campo, el Ministerio de Tecnologías de la Información y Comunicaciones, dispone de certificaciones y diplomados, en su Oferta Académica Gestión TI y Seguridad de la Información.

5.1.3.Tercera Fase o Nivel Avanzado

5.1.3.1. Área Operativa

En esta fase se espera que encontremos personal con aprobación de los más altos estándares de profundidad y una hoja de vida con un recorrido académico que incluya los siguientes programas o sus equivalentes en contenido, duración e intensidad:



Capacidades adquiridas en Ciber, por fases o nivel de capacitación, para el persona Operativo

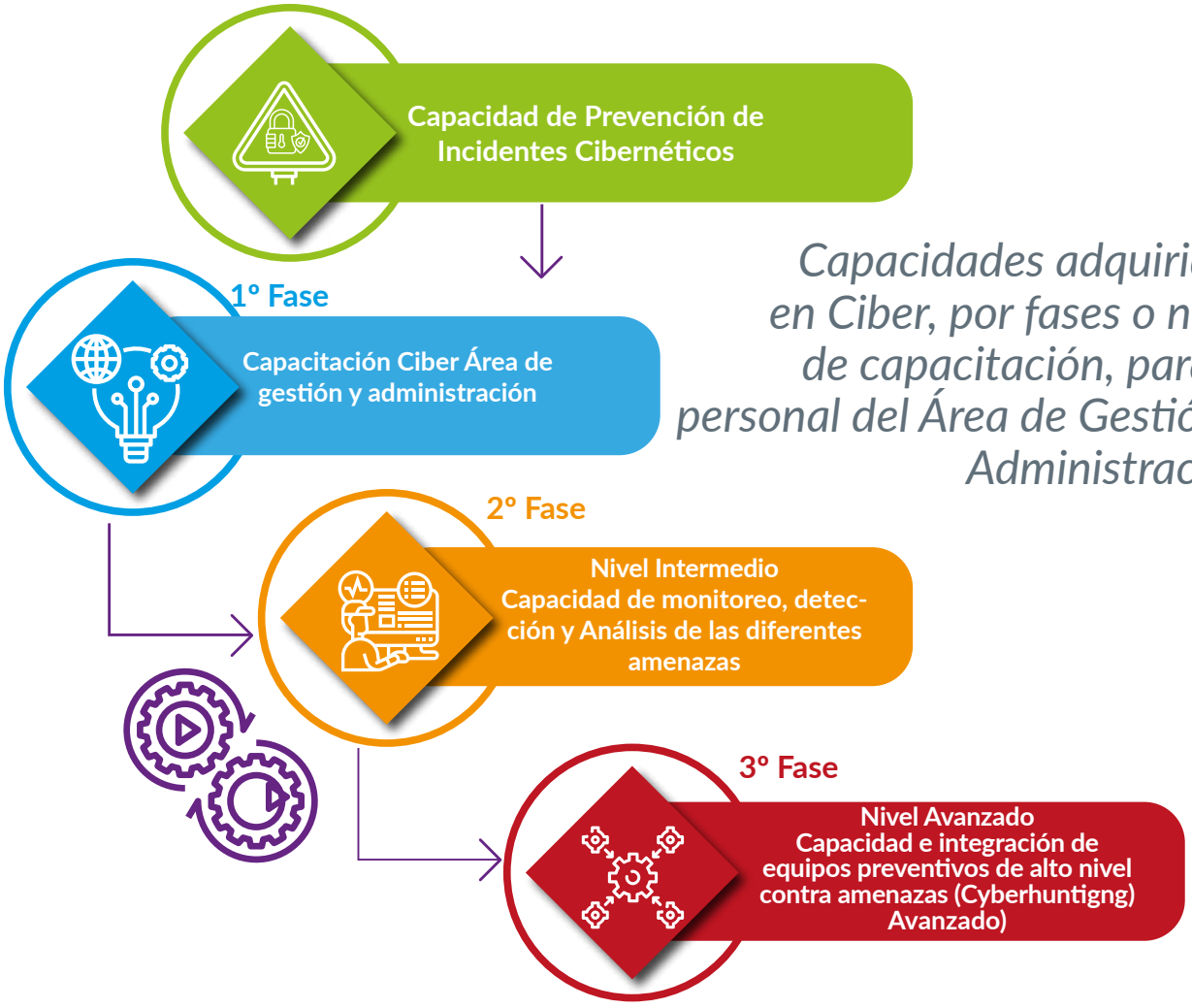
5.1.3.2. Área de Gestión y Administración

Para este nivel, que es el más alto de la pirámide organizacional, los profesionales deben poseer aparte de la experiencia de los niveles anteriores, una formación académica basada en los siguientes programas o su equivalente en intensidad, profundidad y duración.

a. Maestría en Gestión de Seguridad Informática

b. PhD. en Ciencias de la Computación

c. Maestría en Ciberseguridad.



Capacidades adquiridas en Ciber, por fases o nivel de capacitación, para el personal del Área de Gestión y Administración

Por lo anterior, es necesario que cada una de las entidades, promueva la creación de un escalafón de cargos y funciones en el Área Operativa, al igual que, en el Área de Gestión y Administración, debiendo definir tres niveles (básico, medio y avanzado), los cuales, estarán directamente relacionados con los niveles de formación académica.

Referencias:

Arango García, J. M. (2014). Conpes 3701 (Bachelor's thesis, Universidad Piloto de Colombia).http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2971/00001323.pdf?sequence=1

Arteaga, F. (10 de septiembre de 2019). Capacidades ofensivas, disuasión y ciberdefensa. Real Instituto Elcano. Madrid, España. http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari92-2019-arteaga-capacidades-ofensivas-disuasion-y-ciberdefensa

Asamblea General de las Naciones Unidas - AGNU. (24 de junio de 2019). Los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional. Informe del Secretario General A/74/120. Nueva York, Estado Unidos. https://undocs.org/pdf?symbol=es/A/74/120

Banco Interamericano de Desarrollo - BID, Organización de los Estados Americanos-OEA, & Centro Global de Capacitación de Seguridad Cibernética- GCSCC. (2016). Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? Informe de Ciberseguridad 2016. Washington, D.C., Estados Unidos. https://publications.iadb.org/publications/spanish/document/Ciberseguridad-%C2%BFEstamos-preparados-en-Am%C3%A9rica-Latina-y-el-Caribe.pdf

Bonilla, J. (11 de febrero de 2019). defensa.com. https://www.defensa.com/cyberseguridad/ejercito-brasileno-inaugura-escuela-defensa-cibernetica-ano

Bueno de Mata, F. (2016). Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. https://gredos.usal.es/bitstream/handle/10366/130070/Ley_Organica_13_2015,_de_5_de_octubre,_d.pdf?sequence=1 https://bibliotecadigital.ccb.org.co/bitstream/handle/11520/24627/CONSTITUCION%20POLITICA%201991.pdf?sequence=1

Colombia, C. P. (1991). Constitución política de Colombia. Bogotá, Colombia: Leyer. Cano, M., & Jeimy, J. (2014). La ventana de AREM. Una herramienta estratégica y táctica para visualizar la incertidumbre.

Colombia, C. P. (1991). Constitución política de Colombia. Bogotá, Colombia: Leyer.

Cano, M., & Jeimy, J. (2014). La ventana de AREM. Una herramienta estratégica y táctica para visualizar la incertidumbre. https://bibliotecadigital.ccb.org.co/bitstream/handle/11520/24627/CONSTITUCION%20POLITICA%201991.pdf?sequence=1

Comisión Económica para América Latina y el Caribe - CEPAL. (7 de agosto de 2015). Agenda Digital para América Latina y el Caribe (eLAC2018). Quinta Conferencia Ministerial sobre la Sociedad de la Información de América Latina y el Caribe. Ciudad de México, México. https://repositorio.cepal.org/bitstream/handle/11362/38886/S1500758_es.pdf?sequence=1&isAllowed=y

Comité Interministerial sobre Ciberseguridad. (2017). Política Nacional de Ciberseguridad 2017-2022. Santiago, Chile. https://www.ciberseguridad.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf

CONPES. (2016). CONPES 3854, Política Nacional de Seguridad Digital. https://www.mintic.gov.co/portal/604/articles-14481_recurso_1.pdf

Departamento de Defensa de los EE.UU. (septiembre de 2018). Cyber Strategy (summary) [Estrategia Cibernética (resumen)]. Washington, D.C., Estados Unidos. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

Droege C. (2011) No hay lagunas jurídicas en el ciberespacio. CICR Entrevista. https://www.icrc.org/es/doc/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm

Edwards, J. (9 de mayo de 2019). Todo lo que necesitas saber sobre la nueva ley de ciberseguridad en China. Ipswitch. Bedford, Massachusetts, Estados Unidos. https://blog.ipswitch.com/es/todo-lo-que-necesitas-saber-sobre-la-nueva-ley-de-ciberseguridad-en-china

Escuela Superior de Guerra General Rafael Reyes Prieto. (2019). Estrategia Multidimensional de Seguridad Nacional Propuesta 2018-2028. Bogotá.

Escuela Superior de Guerra General Rafael Reyes Prieto. (2020). Apreciación Político Estratégico Nacional (APEN 2018-2022). Bogotá.

España, G. (2013). Estrategia de Ciberseguridad Nacional, 2013. http://www.dsn.gob.es/es/sistema-seguridad-nacional/qu%C3%A9-sseguridadnacional/%C3%A1mbitos-seguridad-nacional/ciberseguridad.

Europa, C. (2001). Convenio sobre la ciberdelincuencia [Convenio de Budapest]. http://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Foro de la Cumbre Mundial de la Sociedad de la Información - CMSI. (2019). Foro de la CMSI de 2019. Ginebra, Suiza. https://www.itu.int/net4/wsis/forum/2019/es

Geopolitica.ru. (28 de Diciembre de 2016). China publica programas sobre ciberseguridad y espacio exterior. Geopolitica.ru. Moscú, Distrito Federal Central, Rusia. https://www.golovinfond.ru/es/news/china-publica-programas-sobre-ciberseguridad-y-espacio-exterior

Galarza, A. C. (2014). Ciberespacio amenazado: necesidad de leyes de protección a la privacidad. Universidad de la Salle. de la Unión Europea.

Gonzales, S. L., & Portela, L. S. (2018). A geopolítica do espaço cibernético Sul-americano: (in) conformação de políticas de segurança e defesa cibernética? Austral: Revista Brasileira de Estratégia e Relações Internacionais. https://seer.ufrgs.br/austral/article/view/87994/50497

International Telecommunication Union - ITU. (2019). Global Cybersecurity Index 2018. Gineva, Suiza. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

International Telecommunications Union- ITU. (2020). Global Cybersecurity Index [Índice Global de Ciberseguridad]. Ginebra, Suiza. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

Internet Governance Forum - IGF. (2019). IGF 2019. Internet Governance Forum. Ginebra, Suiza. http://www.intgovforum.org/multilingual/content/igf-2019

Leiva, E. A. (20 de octubre de 2015). Estrategias nacionales de ciberseguridad: estudio comparativo basado en enfoque top-down desde una visión global a una visión local. Revista Latinoamericana de Ingeniería de Software, III(4), 161-176. http://revistas.unla.edu.ar/software/article/view/775

Ministerio de Defensa Nacional. (2019). Política de Defensa y Seguridad PDS para la legalidad, el emprendimiento y la equidad. https://www.mindefensa.gov.co/irj/go/km/docs/Mindefensa/Documentos/descargas/Prensa/Documentos/politica_defensa_deguridad2019.pdf.

Ministerio de Defensa - MD. (2012). Libro Blanco de Defensa Nacional. Brasília, DF, Brasil.

Morán, D. R. (4 de enero de 2017). Ciberseguridad en China. Documento Informativo(1), págs. 8-15. http://www.ieee.es/Galerias/fichero/docs_informativos/2017/DIEEEI01-2017_CyberChina_DRM.pdf

Lecuit, J. (2017). Ciberseguridad: marco jurídico y operativo. Real Institute El Cano. http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari51-2017-alonsolecuit-ciberseguridad-marco-juridico-perativo

Luke, V. (2012). Seguridad Informática y Derecho Internacional Público en el siglo XXI: desafíos jurídicos frente a la protección de infraestructuras informáticas. Revista de Derecho Público. https://revistas.uchile.cl/index.php/RDPU/article/view/30935

OEA. (2015). Declaración protección de infraestructura crítica ante las amenazas emergentes. Décimo Quinto Período ordinario de sesiones. Washington DC, Estados Unidos de América.https://www.oas.org/en/sms/cicte/documents/sessions/2015/CICTE%20DOC%201%20DECLARACION%20CICTE00955S04.pdf

Organización de los Estados Americanos - OEA. (2020). Comité Interamericano contra el Terrorismo: ¿Qué hacemos? Washington, D.C., Estados Unidos. https://www.oas.org/es/sms/cicte/default.asp

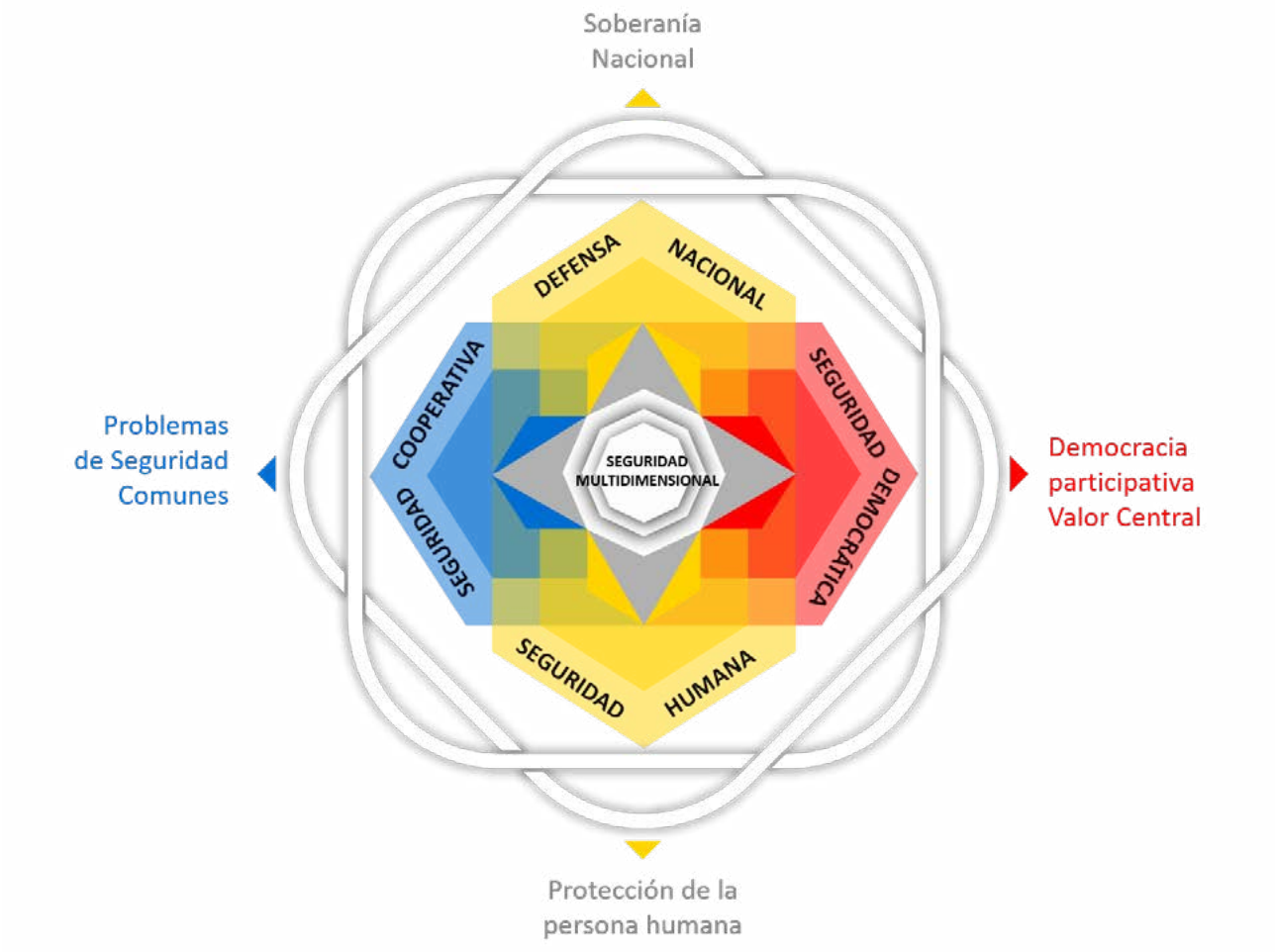
Organización de los Estados Americanos - OEA, Banco Interamericano de Desarrollo- BID, & Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia- MINTIC. (2017). Impacto de los incidentes de seguridad digital en Colombia 2017. Informe. Bogotá, D.C., Colombia. https://publications.iadb.org/publications/spanish/document/Impacto-de-los-incidentes-de-seguridad-digital-en-Colombia-2017.pdf

Organización de Naciones Unidas. (2000). Asamblea General. Declaración del Milenio. A/RES/55/2.2000.III.20 https://www.un.org/spanish/milenio/ares552.pdf

Organización para la Cooperación y Desarrollo Económicos - OCDE. (23 de junio de 2016). Declaración ministerial sobre la economía digital: innovación, crecimiento y prosperidad social. Cancún, México. http://www.oecd.org/centrodemexico/medios/declaracion-ministerial-sbore-la-economia-digital.htm

Organización para la Cooperación y Desarrollo Económicos - OCDE, & Banco Interamericano de Desarrollo- BID. (2016). Políticas de banda ancha para América Latina y el Caribe: un manual para la economía digital. Publicación OCDE.

https://www.oecd-ilibrary.org/docserver/9789264259027es.pdf?expires=1591134221&id=id&accname=guest&checksum=F59883E63F26BCECCA03BFC93AB7E36B


Soberanía
Nacional
DEFENSA
NACIONAL
SEGURIDAD
DEMOCRÁTICA
SEGURIDAD
HUMANA
SEGURIDAD
COOPERATIVA
SEGURIDAD
MULTIDIMENSIONAL
Problemas
de Seguridad
Comunes
Democracia
participativa
Valor Central
Protección de la
persona humana

Estrategia Nacional de **Ciberdefensa y Ciberseguridad**

- ECDCS -

2020-2030

El futuro es de todos

MinDefensa

LA VICTORIA ES DE TODOS

FUERZAS MILITARES DE COLOMBIA

ESCUELA SUPERIOR DE GUERRA

"General Rafael Reyes Prieto"

Colombia