Herramientas preactivas de defensa y su incidencia en la ciberseguridad

Edward Enrique Arévalo Ríos

Trabajo de grado para optar al título profesional:
Maestría en Ciberseguridad y Ciberdefensa

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

2020

Ministerio de Defensa Nacional

Comando General de las Fuerzas Militares

Escuela Superior de Guerra

Maestría en Ciberseguridad y Ciberdefensa

HERRAMIENTAS PREACTIVAS DE DEFENSA Y SU INCIDENCIA EN LA CIBERSEGURIDAD

MY. Edward Enrique Arévalo Ríos

Director

Pedro A. Buitrago Rincón

Maestría en Ciberseguridad y Ciberdefensa Trabajo de grado

Bogotá – Colombia 2020

Tabla de Contenido

Lista de Tablas

Lista de Ilustraciones

RESUMEN

El concepto de seguridad presenta muchas definiciones como ámbitos de aplicación, se pueden encontrar nociones en la seguridad de personas, de documentos, de instalaciones, seguridad en las comunicaciones y muchas otras tipologías, no obstante, en el presente documento se tomará el concepto de seguridad como aquel que representa un estado deseado por una sociedad, en el cual, esta pueda desarrollarse y prosperar libre de amenazas, también acuñado al mismo se podría citar el siguiente concepto: seguridad nacional es cuando el estado asume la responsabilidad de proteger a sus ciudadanos y demanda su lealtad. Así, la seguridad de los ciudadanos de un país está garantizada cuando la propia seguridad del estado también lo está. Según G. Kennan (1948) la seguridad nacional es "la capacidad continuada de un país para proseguir el desarrollo de su vida interna sin interferencia seria, o amenaza de interferencia de potencias extranjeras" (Laborie, 2011), sea cualquiera el origen y el entorno de las amenazas, como para los efectos correspondientes en el presente documento es el constituido por el ciberespacio.

Por consiguiente, el abordaje integral de la ciberseguridad en la esfera nacional requiere de mecanismos de defensa efectivos que permitan aclarar sus niveles de eficacia, esta última debe comprender todos los aspectos civiles y militares tendientes a conseguir o garantizar aquella condición en la que los intereses y activos estratégicos de un Estado se encuentran salvaguardados de cualquier vector de amenaza o riesgo. Esto conlleva a pensar que en los países lo que se defiende básicamente es el territorio que un Estado considera como propio, este territorio compuesto por sus formas reconocidas mundialmente como: la *tierra, el mar, el aire y el espacio.* Pero en los últimos años a estos espacios se le ha agregado

uno más, el *ciberespacio, por* consiguiente es menester identificar el *ciberespacio* y sus componentes esenciales.

Ahora bien, consciente de los elementos que deben ser considerados por los Estados como herramienta para la consolidación y consecución de las sus intereses nacionales, surge la necesidad de establecer modelos de análisis y producción de información, lo anterior como mecanismo para la materialización de dichos fines, en lo que a la identificación y mitigación de riesgos y amenazas se refiere, en consideración a los rasgos propios del siglo XXI, las nuevas tecnologías, y lo que estos representan para la configuración y amoldamiento de las estructuras institucionales de orden estatal en sus diferentes niveles.

En consecuencia, el documento aquí presentado busca aportar herramientas de análisis que permitan dilucidar y caracterizar las condiciones en las que se desarrollan los procesos de análisis y mitigación de riesgos y amenazas que afectan las condiciones de seguridad y resiliencia de los Estados y el planteamiento de una perspectiva prospectiva de análisis que pueda representar una herramienta adicional al momento de establecer las estrategias de Ciberdefensa en el marco de una Estrategia Nacional. Para dichos efectos se plantea una investigación cualitativa de corte descriptivo-deductivo, a partir de la apropiación y análisis de perspectivas teóricas y conceptuales, por medio de la revisión de fuentes secundarias, aspecto que implicó la consulta de artículos académicos, documentos de política pública y literatura especializada.

En un primer momento se desarrollará una conceptualización sobre las características derivadas

del ciberespacio y su incidencia en la consolidación de mecanismos para contrarrestar riesgos y amenazas. El segundo segmento de la investigación tomará en consideración algunos referentes internacionales para la determinación de los cursos de acción empleados en otros contextos para la mitigación de riesgos, así como un examen a la capacidad de las herramientas empleadas. Finalmente se plantearán los componentes integradores de una perspectiva prospectiva de análisis y producción de información, que constituya una herramienta útil para la toma de decisiones bien a nivel operacional y estratégico en relación con la mitigación de riesgos y amenazas.

PALABRAS CLAVE

CIBERSEGURIDAD, CIBERDEFENSA, RESILIENCIA, RIESGOS, AMENAZAS, MODELO DE ANÁLISIS PROSPECTIVO EN DEFENSA

ABSTRACT

The concept of security presents many definitions as areas of application, we can find the security of people, security of documents, security of facilities, security in communications and many other aspects, but in this work we will take the concept of security as that which represents a state desired by a society, in which it can develop and thrive free of threats, also coined to the same could be cited the following concept: national security is when the state assumes the responsibility to protect its citizens and demand their loyalty . Thus, the security of the citizens of a country is guaranteed when the state's own security is also guaranteed. According to G. Kennan (1948), national security is "the continued ability of a country to continue the development of its internal life without serious interference, or threat of interference from foreign powers" (Laborie, 2011).

Therefore, the comprehensive approach to security in the national sphere requires effective defense mechanisms to clarify its levels of effectiveness, the latter must include all civil and military aspects aimed at achieving or guaranteeing that condition in which the interests and Strategic assets of a State are safeguarded from any threat or risk vector. This leads to think that in the countries what is defended basically is the territory that a State considers as its own, this territory composed of its forms recognized worldwide as: land, sea, air and space. But in recent years these spaces have been added one more, cyberspace, therefore it is necessary to identify cyberspace and its essential components.

However, aware of the elements that should be considered by the States as a tool for the consolidation and achievement of their national interests, intelligence and readaptation of

the cycle of collection, classification and production of information, as a mechanism to materialize said purposes, in terms of the identification and mitigation of risks and threats, in consideration of the characteristics of the 21st century and the new technologies, and what these represent for the configuration and adaptation of the institutional structures of state order in their different levels. Consequently, the document presented here seeks to provide analytical tools that allow elucidating and characterizing the conditions in which the processes of analysis and mitigation of risks and threats that affect the security and resilience conditions of the countries are developed. For such effects, a qualitative research of a descriptive-deductive nature is proposed, based on the appropriation and analysis of theoretical and conceptual perspectives.

At first, a conceptualization will be developed on the characteristics derived from cyberspace and its incidence in the consolidation of mechanisms to counteract risks and threats. The second segment of the research will take into consideration some international references for the determination of courses of action used in other contexts for risk mitigation, as well as an examination of the capacity of the tools used. Finally, the conditions of the complex intelligence cycle and its advantages will be established in relation to the needs of gathering, analyzing and producing information that is relevant to decision makers in the mitigation of risks and threats.

KEY WORDS

CYBERSECURITY, CYBERDEFENSE, RESILIENCE, RISKS, THREATS, PROSPECTIVE DEFENSE ANALYSIS MODEL

OBJETIVO GENERAL Y OBJETIVOS ESPECÍFICOS

La presente investigación presenta como objetivo general aportar herramientas de análisis que permita dilucidar y caracterizar las condiciones en las que se desarrollan los procesos de evaluación y mitigación de riesgos y amenazas que afectan las condiciones de seguridad y resiliencia de los Estados en relación con el ciberespacio.

OBJETIVOS ESPECÍFICOS

- Conceptualizar las características derivadas del ciberespacio y su incidencia en la consolidación de mecanismos para contrarrestar riesgos y amenazas.
- Determinar los cursos de acción empleados en otros contextos para la mitigación de riesgos.
- Plantear los componentes integradores de una perspectiva prospectiva de análisis y producción de información, que constituya una herramienta útil para la toma de decisiones bien a nivel operacional y estratégico en relación con la mitigación de riesgos y amenazas.

INTRODUCCIÓN

Con el descubrimiento del procesador nacen las computadoras y las redes de telecomunicaciones que asienten a que la tecnología militar combine esta última innovación con las armas existentes haciéndolas más automáticas, eficientes y efectivas para atacar o defenderse de un adversario con una carrera armamentística tecnológica en los ejércitos de los Estados potencia y emergentes, por lo que las sociedades entran en una nueva era globalizada, como lo afirma la Unión Internacional de Telecomunicaciones.

La transformación de las sociedades en sociedades de la información, gracias a la integración de nuevas tecnologías en todas sus actividades e infraestructuras, aumenta la dependencia de los individuos, de las organizaciones y de los Estados, de los sistemas de información y de las redes (Touré, 2007, pág. 6).

En pleno siglo XXI, la anterior evolución armamentista desarrollada durante la existencia de la humanidad da origen a un nuevo escenario de guerra que no emplea las armas bélicas como medio de defensa o ataque, este escenario es el ciberespacio con el cual se desarrolla el concepto de ciberguerra y para prevenir esta forma de guerra se da origen a la ciberseguridad, constituyéndose en un nuevo reto para los países en desarrollo y en cabeza del sector defensa. Para el caso de Colombia, bajo el liderazgo del Ministerio de Defensa por intermedio del Comando General de la Fuerzas Militares (FF.MM.) se crearon los organismos que hacen la gestión de ciberseguridad y Ciberdefensa, por lo que nació el grupo de respuesta a emergencias cibernéticas de Colombia (ColCERT), Centro Cibernético Policial – (CCP) y el

Comando Conjunto Cibernético – (CCOC) (Conpes 3701, 2011, pág. 21), los anteriores organismos dentro de los nuevos escenarios se alinean con lo argumentado por Unión Internacional de Telecomunicaciones, donde "Las infraestructuras de telecomunicaciones y los servicios y actividades que éstas permiten desarrollar y generar, deben plantearse, concebirse, instalarse y administrarse en términos de seguridad" (UIT, 2007).

Basado en lo expuesto anteriormente durante el desarrollo de la presente tesis se presentará como primera parte una introducción con el planteamiento del problema de las FF.MM y la importancia de la ciberseguridad en la misma, seguido se presentará la justificación y los objetivos pertinentes al objeto de la investigación.

Por lo tanto, el problema de investigación radica en que las Fuerzas Militares de Colombia cuentan con una Red Integrada de Comunicaciones Militares (SICM) (MDN, 2014, pág. 8) para garantizar el comando, control y comunicación con el objeto de proporcionar a los comandantes la información y los medios del planeamiento, administración y conducción de las operaciones mediante la gestión de los recursos humanos, terrestres, marítimos y aéreos, incorporando diferentes sistemas de información y comunicación tales como: la red de campaña VHF, red de UHF, redes informáticas, segmento y nodos de comunicación satelital, red digital, internet, intranet y los sistemas de información que contienen las bases de datos de vital importancia para el funcionamiento de las Fuerzas Militares, pero expuestas a los ataques cibernéticos (Ejército Nacional, 2009).

Mencionadas redes al ser atacadas desde el ciberespacio y de lograrse una efectividad en el ataque, los sistemas y la información de la institución se verían gravemente afectados, con consecuencias que irían desde la pérdida de información administrativa, operacional, técnica de inteligencia e informática, hasta incluso el colapsando de la misión institucional de las

FF.MM., retrocediendo de esta manera en campos considerados plenamente consolidados en el tema de seguridad.

Ahora bien, de cara a la consecución de los elementos aquí planteados se ha diseñado una investigación principalmente cualitativa, basada en la revisión de literatura técnica, documentos de política pública y de manera general todas aquellas fuentes secundarias que permitan establecer el alcance del modelo de seguridad planteado por el Estado colombiano para la defensa de sus activos estratégicos.

1. CIBERESPACIO: EL QUINTO DOMINIO DE LA INTERACCIÓN HUMANA

1.1 El ciberespacio como un interés de orden global y estratégico

Las guerras han sido un factor inherente a la historia de la humanidad, lo que ha significado que su evolución implique procesos de adaptación ante las diferentes herramientas y estrategias tanto en los campos tradicionales de batalla como en otros.

En este sentido, los conflictos han evolucionado hasta llegar a las denominadas *guerras híbridas*, caracterizadas por el empleo de estrategias militares no convencionales, como el despliegue de militares sin identificación en un territorio, las acciones de inteligencia, la *ciberguerra* se ha consolidado como un ambiente cotidiano donde diferentes actores como personas, organizaciones y gobiernos interactúan, con el fin de comunicarse y realizar ‘‘transacciones económicas e inclusive gestionar diversas actividades grupales a nivel nacional e internacional” (Sancho, 2016, p.41).

En este sentido, Clarke y Knake (2011) lo definen de la siguiente manera: “El ciberespacio lo conforman todas las redes informáticas del mundo y todo lo que ellas conectan y controlan. No se trata solo de Internet. Es importante dejar claro la diferencia. Internet es una red de redes abierta. Desde cualquier red de Internet podemos comunicarnos con cualquier ordenador conectado y con cualquiera otra de las redes de Internet. El ciberespacio es Internet más montones de otras redes de ordenadores a las que, se supone, no es posible acceder desde Internet. Algunas de esas redes privadas son muy semejantes a Internet, pero, al menos teóricamente, se encuentran separadas de ella. (p. 104)”

En la actualidad, las características del ciberespacio han conducido a catalogarlo como un

"bien público mundial", y la importancia que ocupa en la actual agenda internacional es innegable teniendo en cuenta los riesgos que diariamente lo amenazan. En este sentido, este ámbito virtual representa un factor de vital importancia para la Seguridad Nacional de los Estados, pues un ataque cibernético podría afectar tanto a los clientes de un banco, como a los habitantes de una ciudad, y dependiendo del caso, la estabilidad entera de todo un país, siendo así un escenario no tradicional en el cual convergen intereses tanto estatales como de naturaleza disímil.

Por lo anterior, Llongueras (2013) realiza un análisis sobre lo que el ciberespacio representa para la Seguridad Nacional de un Estado: "El ciberespacio es un elemento de poder dentro la Seguridad Nacional, es a través de este nuevo y artificial dominio que se ejerce una innovadora influencia estratégica en el siglo XXI; en este mundo virtual hasta los actores más modestos pueden ser una amenaza para las grandes potencias, forjándose y desarrollándose el concepto de las operaciones militares centradas en redes (p.19)"

En este contexto, surgen dos conceptos claves para referirse a las acciones del Sector Defensa y Seguridad, así como a la actuación de los actores del Sistema Internacional en el ciberespacio, siendo estos, la *ciberdefensa* y la *ciberseguridad*. Estos dos conceptos se han convertido en pilares fundamentales de la Seguridad Nacional de los Estados, y aunque muchas veces son utilizados como sinónimos, es importante diferenciarles. En este sentido, mientras la ciberseguridad tiene una connotación eminentemente de protección, la ciberdefensa engloba otras acciones más allá de las puramente defensivas; entre ellas, la denominada ciberdefensa activa, la ciberinteligencia, y todo un abanico de acciones ofensivas: la intrusión, la infección, la denegación de servicios o la alteración de la información, que puede llevar aparejada incluso la destrucción física. (Cubeiro, 2016, p.45).

A partir de lo anterior, se considera la existencia de una relación de complementariedad entre los dos conceptos, por lo cual su aprehensión por parte de los gobiernos nacionales al momento de realizar la planificación de las políticas de Defensa y Seguridad cibernética es determinante. Así como la ciberseguridad se encuentra vinculada estrechamente a la Estrategia de Seguridad Nacional, la ciberdefensa no puede ser un caso aislado, por el contrario, debe estar incluida en la Defensa Nacional, en la Defensa Militar y en la Defensa Civil. También en temas como, la protección de *infraestructuras críticas* y la lucha contra organizaciones criminales y terroristas (Feliu, 2012).

En este sentido, existen países como Estados Unidos que han decidido privilegiar con vehemencia la consolidación de una política de ciberdefensa seria y agresiva. Según Laqueur (2015), el Pentágono "dispone de una lista de armas cibernéticas destinadas al espionaje y sabotaje propios de la ciberguerra. En todas las principales operaciones ofensivas tales como la de introducir un virus en las redes de países extranjeros, se precisa la aprobación del presidente" (p.13). Respecto a lo anterior, Kissinger (2016) plantea que el mundo debe comenzar a preguntarse si la "tecnología de Internet ha superado la estrategia y la doctrina, al menos por ahora, [particularmente cuando es] más fácil emprender ciberataques que defenderse de ellos, lo que posiblemente estimulará una propensión ofensiva en la construcción de nuevas capacidades" (p.345).

Ahora bien, respecto a la infraestructura crítica, ésta se puede definir en el ámbito de la cibernética como "instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción pueden tener una repercusión importante en la

salud, la seguridad, el bienestar económico de los ciudadanos o en el eficaz funcionamiento de los gobiernos" (Torres, 2011, p.347). De este modo, la protección de este tipo de infraestructura es una tarea fundamental para la ciberdefensa y la ciberseguridad de todo país, pues aunque en un principio, por ejemplo, se consideraba que un *malware* solo tenía capacidad de generar daños en los "archivos" de un equipo, en la actualidad es posible que pueda llegar a destruir su *hardware*.

Por lo anterior, se destaca otra caracterización de la infraestructura crítica tomada de las disposiciones para la *Estrategia Digital Nacional en Materia de Tecnologías de la Información y Comunicaciones de México*, en donde se define como aquellas "infraestructuras de información esenciales consideradas estratégicas, por estar relacionadas con la provisión de bienes y prestación de servicios públicos esenciales, y cuya afectación pudiera comprometer la Seguridad Nacional" (Vásquez, 2016, párr.4). En este punto, una realidad que se debe tener en cuenta es que los logros de la ciberdelincuencia y el ciberespionaje combatidos mediante la ley y la contrainteligencia, han encontrado pocos obstáculos en este tipo de estrategias, lo que indica, que es cuestión de tiempo para que ciberataques cada vez mayores comiencen a atentar contra las infraestructuras críticas y de manera más eficaz (Bejarano, 2011).

Así, la estrategia de Defensa y Seguridad de todo Estado deberá ser implacable en la prevención de posibles ataques, en la protección para disminuir la vulnerabilidad y, en caso de crisis, en minimizar daños y acelerar el período de recuperación. Las amenazas a la infraestructura crítica siempre han existido en tiempos de guerra o conflicto, pero en la actualidad los escenarios de amenaza incluyen también ataques en tiempos de paz por medio de ciberataques (Feliu, 2012).

Adicionalmente, y como lo plantea Lewis (2002), si se tiene en cuenta que un ciberataque resulta más fácil y barato que uno físico (así los niveles y duración de los primeros sean comparativamente menores), se hace fundamental proteger este tipo de infraestructura mediante las siguientes recomendaciones: (…) servicios y organizaciones estratégicas, lo cual obliga a convocar a actores de diversa naturaleza, provenientes de la administración civil del Estado y a las Fuerzas Armadas y de Orden y Seguridad, junto a variados estamentos dentro de la sociedad civil, quienes deben garantizar que esa información cumpla con las siguientes características: disponibilidad, integridad, oportunidad, confiabilidad, interoperabilidad, seguridad. (Sancho, 2016, págs.57-58)

Por lo anterior, este concepto toma gran relevancia en la presente investigación, pues todo ataque contra el ciberespacio se perpetrará contra la infraestructura crítica, lo que pondría en juego la estabilidad de un determinado Estado, así como la confianza de la ciudadanía en tal territorio para enfrentarse a estas amenazas. En este orden de ideas, se debe realizar otra diferenciación conceptual entre dos nociones que se usan indistintamente en el ámbito de la defensa y la seguridad cibernética: el *cibercrimen* y la *ciberamenaza*. Los anteriores términos no pueden catalogarse como categorías equivalentes, pues existen ciberdelitos que no constituyen amenazas a la Seguridad Nacional, ni todas las amenazas a la Seguridad Nacional nacen de la criminalidad cibernética. Ahora bien, en los supuestos de terrorismo y criminalidad organizada, determinadas formas de cibercriminalidad sí representan verdaderas amenazas a la Seguridad Nacional (Feliu, 2012). Para efectos de la investigación, se tendrá en cuenta esta categorización a la hora de utilizar un término u otro.

Con la evolución de los conflictos armados fue mutando el concepto de seguridad tradicional

"para dar paso a una nueva función del Estado que es la defensa de su soberanía en el espacio digital y la protección de los derechos de sus ciberciudadanos frente a las amenazas emergentes en el escenario de una vida más digital y gobernada por la información" (Sánchez, 2011). De allí, y como se analizará más adelante, la importancia que tiene la consolidación de estrategias contundentes y multidimensionales para prevenir y combatir los ataques al ciberespacio, comprendido como un bien público mundial, y orientadas, por ende, a garantizar la Seguridad Nacional de los actores internacionales.

Como pudo examinarse en este primer apartado, los conceptos de Defensa y Seguridad han evolucionado en atención a la aparición de nuevas y cada vez más sofisticadas amenazas a los Estados.

1.2 Entornos cibernéticos seguros: El nuevo paradigma de la Seguridad Estatal

Las organizaciones políticas humanas, desde la antigüedad, han sufrido serios desafíos a su Defensa y Seguridad, pues de forma continua las estrategias de guerra y las amenazas a estas variables han cambiado y generado nuevos retos, pasado así por en un principio a las tribus, luego a los imperios, más tarde a las naciones y posteriormente a los Estados modernos (Cancelado, 2010, p.92). En este sentido, tras el final de la Guerra Fría y los atentados del 11 de septiembre de 2001 (11-S), el Orden Mundial se redefinió especialmente en materia de seguridad, configurando nuevas prioridades en la agenda política de los diferentes actores del Sistema Internacional.

Las fronteras territoriales empezaron a perder poder, al igual que el dominio militar del

espacio y el tiempo. El uso de aviones civiles en un atentado terrorista demostró que todo podía llegar a convertirse en un arma, en cualquier momento, por tanto nada comenzó a parecer imposible o impensable en el reinventado Orden Mundial del siglo XXI (Theiler, 2011).

Como se explicó en el anterior apartado, con la evolución de Internet y la llegada de las nuevas Tecnologías de la Información y las Comunicaciones (TIC) se dio origen a un nuevo espacio para el desarrollo de las actividades humanas: el ciberespacio. Éste se constituyó, de acuerdo con la revista *The Economist*, en el *quinto dominio de interacción humana*, luego del terrestre, el marítimo, el aéreo y el espacial (Camps, 2016). De este modo, el ciberespacio comenzó a posicionarse progresivamente como un campo que debía ser atendido desde la perspectiva de Seguridad de los Estados.

En un comienzo el ciberespacio parecía ser el escenario virtual e ideal para facilitar la vida de millones de personas alrededor del mundo, poniendo a su disposición información, nuevas posibilidades y servicios para los usuarios, convirtiéndose en un instrumento estratégico para la industria, la administración y las Fuerzas Militares. Sin embargo, a partir del 11-S, esta herramienta comenzaría a convertirse en un serio riesgo para todo el Sistema Internacional, mutando en un campo fértil para amenazas de diversa índole en un mundo globalizado y, por ende, cada vez más interconectado.

Así, las amenazas tradicionales transformaron su forma y ámbito de actuación, pasando ahora a accionar en este ciberespacio, dando lugar a la aparición de términos como ciberdelito, cibercrimen, ciberactivismo, ciberterrorismo, ciberespionaje, ciberataque, ciberseguridad, los

cuales se constituyeron como nuevos riesgos en el ámbito cibernético. A partir del surgimiento de este tipo de amenazas (ciberamenazas), los Estados empezarían a dirigir sus esfuerzos hacia la creación de infraestructuras institucionales y normativas para contener cualquier ataque cibernético, pues la salvaguarda de la soberanía y la integridad del espacio geográfico ya no podía asegurarse únicamente por medio de la defensa militar, dada la complejidad de un nuevo tipo de amenazas que comenzarían a exigir una visión mucho más amplia e integral de los gobiernos durante la planificación de su Defensa y Seguridad (Camps, 2016).

La importancia de un ciberespacio seguro y blindado es innegable en un mundo cada vez más interconectado, pues cada día se hace más extenso, alberga más información y aumenta su oferta de servicios para los usuarios. El denominado quinto dominio de la interacción humana es susceptible a amenazas que pueden ocasionar daños complejos para las víctimas y otorgar grandes réditos a los victimarios, quienes muchas veces, incluso, no pueden ser identificados. En este medio, los ataques pueden ser patrocinados por Estados o empresas privadas, pueden venir de grupos organizados con fines terroristas o activistas, de organizaciones delictivas o de simples individuos, así como pueden ser dirigidos o genéricos y atacar blancos gubernamentales, empresariales o particulares con objetivos dispares según el caso (Camps, 2016).

En este sentido, salvaguardar el ciberespacio se ha posicionado como un elemento central en la planificación de la Defensa y Seguridad de los Estados, pues debido a los riesgos y amenazas que lo pueden vulnerar, se hace necesario garantizar una serie de estándares mínimos de seguridad en su uso, lo cual implica enfrentar desafíos importantes a nivel nacional e internacional. De esta manera, Sancho (2016) destaca algunos de los derroteros que deben tener en cuenta los Estados al momento de diseñar y estructurar su estrategia para prevenir actividades

ilícitas en el ciberespacio: En el nivel nacional, la formulación de una política pública de ciberseguridad que contemple e integre los diferentes aspectos involucrados en este tema con la finalidad de evitar que un ciberincidente ponga en riesgo la vida de las personas, su patrimonio y/o la seguridad nacional. A nivel internacional cobra relevancia la necesidad de participar en instancias de diálogo multilaterales, donde sean abordados temas como: la gobernanza en internet; estándares mínimos de seguridad en el ciberespacio y la participación en convenios o resoluciones internacionales sobre situaciones que afectan la ciberseguridad y que involucran a diferentes países del mundo. (p.49).

A partir de lo anterior, se evidencia cómo la búsqueda de un ciberespacio seguro demanda la sinergia de esfuerzos entre diferentes actores estatales y transnacionales con miras a prevenir y combatir las diversas amenazas que se pueden llegar a gestar en este ámbito virtual, las cuales pueden traer consigo efectos devastadores. Al respecto, el *Informe de Riesgos Mundiales* (*2013*), elaborado por el Foro Económico Mundial (FEM), advirtió sobre el peligro de los "incendios digitales en un mundo hiperconectado". Con ello, se refería a las consecuencias sociales e inclusive políticas que puede generar la información falsa difundida en Internet, resultado de un error humano o una acción deliberada, siendo esta última la que genera mayores desafíos desde la perspectiva de la seguridad de la información en el ciberespacio (Sancho, 2016).

Como se analizó en este apartado, el ciberespacio, además de representar las ventajas de la evolución informática y digital, como la economía en las comunicaciones y demás, se ha convertido en un bien público de carácter global constantemente amenazado por actividades ilícitas que se pueden perpetrar en él con inconmensurables secuelas para sus víctimas. En consecuencia, cada vez son más los Estados que han asumido dentro de sus prioridades en

materia de Defensa y Seguridad la vinculación de una nueva necesidad: "la defensa del quinto dominio".

Para alcanzar este objetivo, se ha hecho necesario comprender que esta defensa debe realizarse desde diversos ámbitos y a partir de una asociación de esfuerzos entre actores estatales y no estatales, alineándose con los estándares internacionales en esta materia, con el fin de proteger la vida de las personas, la integridad, la estabilidad, el *statu quo* y funcionamiento de los Estados, así como su estabilidad económica. De este modo, es fundamental que los gobiernos implementen buenas prácticas en materia de ciberdefensa y ciberseguridad para evitar el cibercrimen, el ciberespionaje, el ciberhacktivismo, e incluso, la ciberguerra y, en caso de producirse alguno de ellos, contar con un plan de contingencia que contemple acciones de prevención, respuesta, mitigación y resiliencia, con la finalidad de enfrentar de la mejor forma posible el ciberincidente manifestado (Sancho, 2016).

Con base en lo argumentado, es claro cómo la evolución de las tecnologías de la información y las comunicaciones no solo se ha puesto a disposición de millones de personas un ámbito virtual que facilita sus vidas de distintas maneras, sino además, un reto a la Seguridad Nacional de los actores que conforman el Sistema Internacional. El anterior desafío, sin duda alguna, representa un nuevo paradigma en la planificación de la Defensa y Seguridad de los Estados que es la búsqueda de un ciberespacio seguro.

1.3 La Defensa y Seguridad de Colombia en un mundo digital

Colombia ha presentado una tendencia creciente en los niveles digitales desde hace varios

años, lo cual ha traído grandes oportunidades y amenazas para el país. El número de suscriptores a Internet (fijo dedicado y móvil) en Colombia pasó de 687.637 en el 2005 a casi 11'000.000 en el primer trimestre del 2015 (Consejo, 2016, p.27; Colombia, 2015, p.9). Asimismo, el sector que más se vio favorecido con el aumento de los niveles de conectividad en los últimos años ha sido el financiero, toda vez que el número de operaciones monetarias usando Internet como canal pasó de 31.66% en el 2012 a 42.62% en el 2015, lo cual significó un 35% más de transacciones (Superintendencia Financiera de Colombia, 2015).

Los altos niveles de conectividad incrementan la dependencia de los diferentes actores (individuos, empresas, instituciones públicas y privadas, etc.) a las Tecnologías de la Información y las Comunicaciones, lo que significa mayor riesgo proveniente de las amenazas que rondan en el ambiente digital (Sánchez & Jones, 2016). Teniendo en cuenta los acontecimientos de los últimos años en el mundo generados por ataques al ciberespacio, Colombia se ha volcado, cada vez más, a fortalecer sus capacidades en materia de ciberdefensa y ciberseguridad para contrarrestar eventuales riesgos.

En 2011, el país realizó un primer gran esfuerzo desplegando su primera política pública en la materia mediante la formulación del "CONPES 3701: *Lineamientos de Política para ciberdefensa y ciberseguridad*", documento desarrollado por el Consejo Nacional de Política Económica y Social, siendo un hito que permitió al país iniciar un camino con grandes logros operativos, legislativos, estratégicos y diplomático (Sánchez & Jones, 2016, p.81).

Como se ha analizado hasta aquí, "no es un misterio que las Tecnologías de la Información y Comunicación, al igual que los mayores niveles de conectividad, traen grandes beneficios y

oportunidades para los diferentes usuarios" (Baker, 2014, págs.122- 123), de lo anterior que Colombia ha dirigido sus esfuerzos en materia de Defensa y Seguridad al mantenimiento de un ciberespacio seguro y que le permitiera potenciar las capacidades económicas y sociales del país con la ayuda de este ámbito virtual.

Además de las experiencias negativas de los últimos veinte años en el mundo vale la pena mencionar algunos incidentes cibernéticos que tuvieron lugar, no hace mucho tiempo, en la región y en el país. Dichos eventos, también impulsarían la consolidación del CONPES 3701, ya que a partir de éstos quedaron expuestas algunas debilidades de Colombia en materia cibernética: El 23 de diciembre de 2009 se desmanteló, en una operación conjunta entre Panda Security, FBI y la Guardia Civil Española, una de las más grandes Botnets para cyberscamming y DDoS conocidas hasta la fecha: Botnet "Mariposa". En la cuenta de afectación de Mariposa- 13 millones de computadores, 190 países y 31.901 ciudades – Colombia se encontró en la quinta posición con 4.94% de las infecciones, dos de sus ciudades principales también lograron la lista de mayor número de IP comprometidas (i.e. Bogotá, D.C, 2.68% y Medellín 0.65%). Ese mismo año, McAfee Labs ya había identificado a Colombia como el origen de 1.9% del Spam mundial, por encima de países con mayor nivel de conectividad y población como Rusia. (Sánchez & Jones, 2016, p.82)

En esta misma línea, durante el año 2009 se presentaron una gran cantidad de delitos informáticos que tuvieron lugar en Colombia. Mención aparte se debe hacer a las filtraciones de los cables secretos de los Estados Unidos publicados por *WikiLeaks* entre 2010-2011, las cuales tuvieron un impacto importante en las relaciones diplomáticas entre Colombia y sus vecinos, particularmente con Venezuela y Ecuador (Sánchez & Jones, 2016).

Por otra parte, el 15 de abril del año 2011, las páginas web de Presidencia, Senado, Ministerio del Interior y la plataforma de trámites "Gobierno en Línea", fueron víctimas de ataques DDoS que las inhabilitaron por varias horas. Estos ataques fueron atribuidos al grupo hacktivista *Anonymous*, y se replicarían el 20 de julio del mismo año en el marco de lo que este grupo denominó "Operación Independencia", continuando hasta 2012 mediante una arremetida exacerbada por la presentación de una nueva versión de la Ley Lleras (Ley 201 de 2012) y la Cumbre de las Américas (Sánchez y Jones, 2016).

Adicionalmente, según el *McAfee Threats Report*, Colombia presentó en el año 2011 un aumento significativo de computadores *Zombie* utilizados como remitentes de Malware para la creación de botnets, superando a países como Japón, España, Australia, Portugal, Reino Unido y Venezuela (McAfee Labs, 2011, p. 11-13). Vale la pena mencionar, que esta estadística negativa que ostentaba el país fue decreciendo con la implementación del CONPES 3701.

Hechos como los expuestos, serían el punto de partida para incentivar la creación del referenciado documento, el cual establecería los derroteros del país para contener este tipo de amenazas en el ciberespacio. En este sentido, esta política fue explícita en su introducción: "El Gobierno Nacional requiere conocer y actuar de forma integral frente amenazas informáticas (…) que puedan comprometer información, afectar infraestructura crítica del país y poner en riesgo la seguridad y defensa del Estado" (Departamento Nacional de Planeación, 2014).

Para alcanzar el anterior objetivo, dentro del documento se establecieron tres ejes estratégicos: Desarrollo de capacidades de ciberseguridad y ciberdefensa, fortalecimiento del cuerpo normativo, y capacitación especializada. Adicionalmente, para apoyar el objetivo de esta

política se constituyeron cuatro instancias: Comisión Intersectorial[10], Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT), Comando Conjunto Cibernético de las Fuerzas Militares (CCOC), Centro Cibernético Policial (CCP).

Los resultados del CONPES 3701 fueron más que satisfactorios para Colombia, pues al año 2015 se había cumplido en un 90% lo planteado por el Consejo Nacional. Los logros más representativos con la implementación del CCOC, por ejemplo, serían: "La creación de un comité de ciberdefensa de las Fuerzas Militares; adquisición de la plataforma de entrenamiento y ciberdefensa; cooperación internacional con Estados Unidos, OEA, y España; 38 cursos de capacitación y 340 servidores entrenados; adquisición de plataformas operacionales en ciberdefensa; identificación de infraestructuras críticas cibernéticas nacionales; elaboración del manual de ciberdefensa conjunta" (Sánchez & Jones, 2016, p.86). De igual forma, con la implementación del CONPES 3701 se atendieron muchos más incidentes digitales en Colombia. "El CCP agenció 2.652 incidentes en el año 2013, mientras que para el año 2015 el CCP y CSIRT de la Policía Nacional atendieron 6.366 incidentes, incrementando la cobertura de capacidades operativas en un 140%" (Sánchez & Jones, 2016, p.86).

En materia de infraestructura normativa para la ciberdefensa y la ciberseguridad, el Consejo determinó una falencia dentro del Ordenamiento Jurídico colombiano al respecto. Por esta razón, se recomendó fortalecer el cuerpo legal y la *cooperación internacional* en asuntos cibernéticos. "Desde julio del año 2011, Colombia desarrolló 11 herramientas jurídicas (4 leyes y 7 decretos) en materia cibernética; algunas para seguridad y defensa, otras para regular servicios electrónicos" (Sánchez & Jones, 2016, p.86). De esta forma, el Estado colombiano logró robustecer la regulación y legislación en el ámbito cibernético para blindar el ciberespacio,

también, desde el ámbito normativo.

En 2015, con la creación de un nuevo borrador de CONPES en materia cibernética y en el marco del Plan Nacional de Desarrollo (2014-2018) "Todos unidos por un nuevo país", se delineó la "Política Nacional de Seguridad Digital en Colombia", a partir de ahora CONPES 3854 de 2016. En concordancia con lo argumentado hasta aquí, dentro del PND (en sus bases) se estableció que el respeto de la soberanía nacional y la protección de los intereses nacionales implicaría un reconocimiento del dominio ciberespacial -también conocido como quinto dominio, lo que involucra, además, que el país debe desarrollar sus capacidades de neutralización y reacción frente amenazas que atenten contra la crítica digital (DNP, 2014). En las bases del DNP, también quedó claro cómo la estrategia nacional de ciberseguridad debe cumplir algunas iniciativas precisas.

Se debe señalar que, a partir de la aprobación del CONPES 3854 el 11 de abril de 2016, se proyectarían algunas novedades en materia cibernética al introducir un nuevo enfoque para la seguridad digital: *la gestión del riesgo en Colombia.* "Esta transversalidad implica que los actores sufren los impactos provenientes de los riesgos digitales y, en consecuencia, se requiere de un esfuerzo cooperativo para gestionarlos" (Organisation for Economic Cooperation and Development, 2015, p.4). De esta forma, se evidencia cómo los retos de Colombia en el ciberespacio se plantean dentro el nuevo documento a la luz de las recomendaciones de organismos internacionales como la Organización Económica para la Cooperación y Desarrollo (OECD) y la Organización de Estados Americanos (OEA).

En este sentido, vale la pena destacar cómo Colombia se convirtió en el primer país de

Latinoamérica, y uno de los primeros en el mundo en incorporar plenamente las recomendaciones y las mejores prácticas internacionales en gestión de riesgos de seguridad digital emitidas por la OECD. Según este organismo internacional, en la medida que se cuente con una aproximación basada en la administración del riesgo, y siempre que se mantenga un enfoque económico y social, los riesgos digitales pueden aproximarse como riesgos económicos. Adicionalmente, aseguran que una aproximación diferencial de la seguridad digital genera una respuesta excluyente que contraviene la naturaleza transversal del ámbito digital (Sánchez & Jones, 2016, p.91).

Para generar este nivel de confianza, la "Política Nacional de Seguridad Digital en Colombia" dispone de cinco dimensiones y objetivos estratégicos, todos soportados en cuatro principios fundamentales. El primero de estos principios es salvaguardar los derechos humanos y valores fundamentales de los individuos, lo cual gira en torno a temáticas tan complejas como garantizar la libertad de expresión, confidencialidad, y protección de la intimidad (Departamento Nacional de Planeación, 2014, p.71). El segundo principio es la adopción de un enfoque influyente y colaborativo que involucre a los actores que hacen uso del entorno digital. El tercer principio se refiere a la corresponsabilidad de estos actores para proteger el entorno, mientras que el último principio enfatiza la necesidad de contar con un enfoque basado en la gestión de riesgos (Sánchez & Jones, 2016, p.92). Las cinco dimensiones estratégicas que encaminan la formulación de los objetivos son: fortalecimiento del marco legal y regulatorio, gobernanza, gestión sistémica del riesgo, cultura ciudadana, y capacidades para la gestión del riesgo (Departamento Nacional de Planeación, 2014, págs.71-72).

Así, el CONPES 3854 otorga una visión estratégica a Colombia que le permite vincular integralmente las partes interesadas para gestionar los riesgos de la seguridad digital, maximizar las oportunidades en el desarrollo de actividades socioeconómicas, desarrollar las capacidades de ciberdefensa y ciberseguridad necesarias y fortalecer los esfuerzos de cooperación y colaboración nacional e internacional (Consejo, 2016, págs.47-65). Las anteriores líneas estratégicas se consolidarían dentro de la nueva política a partir de aportes realizados por los representantes del sector privado, del Gobierno, de la sociedad civil, de la industria TI y de la Academia (Portafolio, 2017, párr.13).

Adicionalmente, y bajo la misma lógica de la OECD, el CONPES 3854 parte de la premisa que mayor confianza en el entorno digital significará mayor prosperidad económica, política y social, y que esta puede construirse mitigando el riesgo proveniente de vulnerabilidad y amenazas a niveles aceptables (Consejo Nacional de Política Económica y Social, 2016, págs.10-55). Lo anterior, implica que las medidas de seguridad que se tomen deben tener un entendimiento holístico de las necesidades de todos los actores, y que no deberían ser tan férreas que impidan el uso del ambiente digital abierto requerido para generar capital. Este nuevo enfoque de política para Colombia es más entendible cuando se conocen las cifras nacionales, pues los sectores más afectados en Colombia por los incidentes digitales para el año 2015, fueron también los que más aportaron al Producto Interno Bruto (PIB) (Sánchez & Jones, 2016, p.91).

Para finalizar, se debe aducir que el tema de cooperación en materia de defensa del ciberespacio, eje fundamental del CONPES 3854, se abordará en los siguientes capítulos de la investigación.

1.4 La ciberseguridad y la Ciberdefensa

Con la evolución del hombre se presentan paralelamente formas de enfrentamiento entre los seres humanos, que buscan imponer la voluntad de unos sobre otros, de manera voluntaria o violenta, pasando por la utilización de medios físicos como herramientas que reciben el nombre de -armas- para lograr ganar la ventaja que le proporcionará la victoria sobre su contraparte. Los escenarios que se emplean para dichas interacciones son físicos (tierra, mar, aire y espacio) pero en las últimas décadas se ha configurado un quinto escenario que tiene que ver con todos los anteriores *ciberespacio,* en todos ellos también están presentes las guerras asimétricas que nos muestran que una contienda entre dos actores con capacidades diametralmente diferentes, se puede presentar y no necesariamente dar la victoria a quien tenga más capacidad bélica, sino a quien sepa utilizar a su favor las ventajas que le ofrece el campo de batalla; para este caso el *ciberespacio* es un escenario donde un actor con una mínima capacidad (basta con tener a su disposición un ordenador y el conocimiento necesario) puede afectar de manera significativa a su oponente. En el ciberespacio a una colección de actores que buscan controlarlo, como son: Estados, Organizaciones, Grupos, Individuos.

En el ciberespacio se presentan características diferenciales a comparación de los demás espacios:

a) El ciberespacio es un ambiente único, sin fronteras geográficas. El atacante puede estar en cualquier parte del globo y es difícil localizarlo
b) La defensa se complica por la intervención de los diferentes actores, no solo estatales sino también privados.
c) La confrontación en el ciberespacio presenta las características de la guerra asimétrica, el atacante puede ser muy inferior al atacado en medios técnicos y con relativamente pocos

medios y baratos pueden causarse perjuicios significativos.

d) Es una actividad clandestina y anónima, lo que atrae a terroristas y criminales.

e) La utilización del ciberespacio permite obtener información sobre objetivos sin necesidad de destruir ni amenazar ningún sistema, a veces sin necesidad de delatarse.

f) Sus usos están en el ámbito militar, político o industrial.

g) Se puede utilizar para realizar chantaje o para la disuasión

h) Su evolución está determinada por la tecnología.

Los conceptos de seguridad y defensa se han ampliado como consecuencia de la aparición de nuevas vulnerabilidades, entre ellas la dependencia creciente a las tecnologías de comunicaciones e información, hoy es casi imposible realizar alguna actividad sin utilizar este tipo de tecnologías y tampoco funcionar bajo sistemas aislados o cerrados. La Ciberseguridad debe formularse proactivamente como un proceso continuo de análisis y gestión de los riesgos asociados en el ciberespacio.

Las vulnerabilidades de las infraestructuras críticas se dan por descontado, al prever que estas pueden fallar, se fabrican para poder reiniciarse, entonces más que intentar una protección total, se debe prever una buena gestión de riesgo. La inteligencia juega un papel protagónico en la detección de amenazas y riesgos contra la seguridad, pero con más énfasis en la previsión.

Las potencias coinciden en: Se debe definir con claridad las amenazas y los riesgos existentes para la Ciberseguridad y como consecuencia de estos, los objetivos a alcanzar, las medidas a tomar, y las acciones a ejecutar; de la misma forma el adiestramiento para el personal implicado y las actividades en el campo de Inteligencia, Investigación y Desarrollo (I+I+D).

Para Colombia, la Estrategia Nacional de Seguridad (La Ciberseguridad es el componente más importante de la Seguridad Nacional, que pretende lograr un estado deseado por una sociedad en el que pueda ésta desarrollarse y prosperar libre de amenazas), debe contemplar las diferentes estrategias de defensa para los diferentes espacios, como son terrestre, aéreo, marítimo, espacial y para completar los escenarios se debe contemplar el ciberespacio; este último al igual que los convencionales, se muestra ante los diferentes actores como un espacio de interés para ser dominando y aprovechado a fin de utilizarlo a favor para imponer la voluntad propia sobre la del oponente. La estrategia de Seguridad Nacional debe definir la forma de proteger el territorio, la infraestructura crítica y a los propios ciudadanos, los objetivos estratégicos a alcanzar, los órganos competentes y sus responsabilidades, la contribución de las instituciones al país, el nivel tecnológico a alcanzar (I+I+D).

De la misma manera, se debe impulsar una estrategia y una entidad que actué como un director general al más alto nivel, para que asuma el valor estratégico que la Ciberseguridad tiene para nuestro país y que con la autoridad necesaria reúna a todos los organismos tanto privados como militares y los enfoque en un solo esfuerzo bajo una clara política nacional.

Se requiere mejorar la seguridad en el ciberespacio, con un ajuste previo de la legislación, reforzando la capacidad de resistencia y recuperación de los sistemas de gestión y comunicación de las infraestructuras y los servicios críticos, lo anterior acompañado de la colaboración de las entidades privadas, ya que estas se ven involucradas de la misma forma que las entidades gubernamentales.

En España el Ejército de tierra, siguiendo las políticas de la OTAN ha desarrollado un proyecto denominado "Ejército de tierra CERT ", para cubrir la necesidad de hacer frente a ataques sobre redes clasificadas del Ejército de tierra, inicialmente en el ámbito de Mando y Control. Este Ejército se enfoca en la detección-respuesta ante incidentes de seguridad; además, este Ejército se compone de sondas desplegadas en cada nodo de un sistema, tanto en territorio nacional como en zona de operaciones, las sondas informan a un servidor central de cualquier evento que se produzca en su nodo. El servidor central contiene un motor de inteligencia artificial capaz de correlacionar enormes cantidades de eventos, ordenarlos, deducir patrones de ataque, dar un punto de situación sobre los sistemas afectados y proponer las situaciones oportunas o incluso, ejecutarlas automáticamente, todo ello en tiempo real.

En el caso de Europa, los programas y órganos para hacer frente a los distintos riesgos y amenazas cibernéticas se han desarrollado adecuadamente, como por ejemplo, la creación de la ENISA en el año 2004, esta agencia asesora a la comisión y a los estados miembros en lo relacionado con la Ciberseguridad, el programa para la protección de la infraestructura crítica y la presentación en el año 2010 de una "Agenda Digital para Europa" que constituye un compendio de los problemas y oportunidades actuales y previsibles, todo esto acompañado de iniciativas legislativas.

Aunado a lo anterior, se han realizado ejercicios prácticos de simulación deciberataques, como el Cyber Europe 2010, que tenía por objeto obtener enseñanzas sobre cómo mejorar la seguridad comunitaria y de los países. El 04 de noviembre de 2010 se desarrolló este ejercicio, primer simulacro de ciberataque a nivel paneuropeo en el que se efectuó una situación en la que se

presentaban dificultades para acceder a servicios esenciales de Internet, este ejercicio se desarrolló por ENISA en coordinación con los estados miembros y con la participación de Estados miembros de la Unión Europea como Islandia, Noruega y Suiza.

ENISA (European Network and Information Security Agency) fue creada en marzo de 2004, en Bruselas, dentro de sus objetivos está: mejorar la capacidad de la Unión Europea para la seguridad en la información y de las redes, desarrollar un alto conocimiento en la materia, promover la colaboración entre actores de los sectores público y privado. Esta comisión ha desarrollado un plan de acción para enfrentarse al crimen organizado, donde se fija como objetivo "Aumentar los niveles de seguridad de los ciudadanos y las empresas en el ciberespacio" (UIT, 2007).

También se aprobó en diciembre de 2002 la "Estrategia Europea de Seguridad ", en ella se contemplaba la seguridad ante la situación mundial como consecuencia de la apertura de las fronteras, el desarrollo tecnológico que incrementa la dependencia de Europa a una infraestructura interconectada en ámbitos como el transporte, la energía o la información, generando a la vez vulnerabilidades. En el año 2010 se aprobó la "Estrategia de Seguridad Interior" de la unión europea, que busca hacerles frente a las amenazas graves entre las que se incluye la ciberdelincuencia.

La tendencia mundial apunta a la advertencia y consecuente preparación de todos los Estados hacia una amenaza en el ciberespacio, que atenta contra la seguridad de sus naciones, sino se atiende de manera oportuna.

El Ciberataque de la primavera de 2007 a Estonia fue el que representó un hito y un reto histórico para la OTAN ya que fue la primera vez que un estado miembro solicitó apoyo a la OTAN por un ataque a la infraestructura crítica de su país, la OTAN no tenía un plan de acción en caso de un ciberataque a un estado miembro, puesto que hasta el momento solo se tenían antecedentes de ataques de índole nacional como el caso de los EE.UU. sin que esto exigiera la intervención de la OTAN.

Posteriormente, en el año 2008, año en el que se celebró la cumbre de Bucarest, se llegó a un acuerdo que quedó escrito en la declaración de la cumbre: "La OTAN se mantiene comprometida en el fortalecimiento de los sistemas de información crítica de la alianza contra ciberataques. Hemos adoptado recientemente la política de Ciberdefensa y estamos desarrollando las estructuras y autoridades para llevarla a cabo nuestra política en materia de Ciberdefensa" (OTAN,2008).

Subraya la necesidad de la OTAN y de las naciones miembros de proteger los sistemas de información crítica conforme con sus respectivas responsabilidades, compartir las mejores prácticas y establecer una capacidad de apoyo a las naciones, (bajo petición), para contrarrestar un ciberataque "(OTAN, 2008).

Otros casos de ataques como el de Estonia se describen a continuación y representaron un caso de reflexión para la OTAN, como por ejemplo el ciberataque a Lituania en julio de 2008, el ciberataque a Georgia en julio de 2008 y el ciberataque a Kirguistán en enero de 2009.
Es imposible hacer una contabilidad de los sucesos de ataques (de baja intensidad) consistentes en robos de datos, denegaciones de servicio, publicación dolosa de informaciones personales que

se han sucedido en los últimos meses en lugares como: Sony, Honda, Citigroup, Apple, Facebook, Fondo Monetario Internacional, CIA, Movistar, etc. En el año 2007 y 2008, un informe del Congreso de los EE. UU., expone los indicios que señalan que dese China se tuvo acceso a dos satélites de la NASA, a través de un centro de control terrestre ubicado en Noruega, sin consecuencias prácticas, pero si demuestra la capacidad de intrusión en misiones de alto valor estratégico

En noviembre de 2011 se presentó un ciberataque contra la infraestructura industrial civil de los EE. UU., un servicio de distribución de aguas en Illinois, usando claves robadas de una empresa que desarrolla software para los sistemas de control SCADA, para acceder remotamente e inhabilitar una (o más) bombas de agua, demostrando la posibilidad de intervenir remotamente la infraestructura crítica de un país.

Ciberataque sufridos por GEORGIA durante el conflicto con RUSIA en Osetia del sur y Abjasia, estos ataques sobre Georgia se organizaron desde seis *botnets* distintos (redes de ordenadores actuando bajo un mismo control) que implicaban terminales en todo el mundo; los combates físicos se originaron con ocasión de una serie de disturbios en las regiones independentistas de Osetia del Sur y Abjasia y dentro del contexto general de la expansión hacia las antiguas repúblicas soviéticas tanto de la alianza Atlántica como de la Unión Europea. En cuestión de horas, fuerzas rusas y georgianas tomaron posiciones convergiendo sobre la capital de Osetia del sur. Durante las agresiones llegó a anularse el dominio *.ge* perteneciente a la república de Georgia; las webs de distintos ministerios de la República caucásica estuvieron colapsadas permanentemente, paralización de la actividad económica y mediática en Tiblisi;

todo esto creo un vacío informativo para Georgia ante su incapacidad de comunicarse con el exterior.

La Revisión del concepto estratégico de 1999 también considera a la Ciberseguridad como un nuevo reto respecto al concepto estratégico de la OTAN, el nuevo concepto aprobado en Lisboa en noviembre de 2010 aclara: "…la defensa y seguridad común… continuará siendo efectiva en un mundo cambiante… incluidas las nuevas amenazas, los ciberataques están siendo más frecuentes, más organizados y costosos en el daño que infringen en todos los factores, estos pueden alcanzar un nivel de amenaza a la seguridad y estabilidad nacional ". (Gaitán, 2016).

Toda esta experiencia llama la atención para el caso colombiano, es por eso que ante este panorama, la OTAN dio los siguientes pasos para atender esta amenaza:

1. Adquirir la capacidad NCIRC (NATO Computer Incident Response Capability)
2. Atender los objetivos concretos en un centro técnico.
3. Aprobar el soporte jurídico, en el 2008 el concepto y política de Ciberdefensa, creando la Autoridad de Gestión de la Ciberdefensa CDMA (Cyber Defense Management Authority).
4. Diseño de la estructura y organización de apoyo

ENISA, en busca de su objetivo de "Aumentar los niveles de seguridad de los ciudadanos y las empresas en el ciberespacio "; se impone las siguientes acciones:

1. Reforzar la capacidad judicial y policial necesaria para la lucha contra el cibercriminal.
2. Trabajar con la industria para proteger a los ciudadanos mediante la formación y concientización acerca de la protección a la privacidad en la red; detección y denuncia de actividades de acoso a menores, suplantación de identidad y sitios web falsos.

Instalación de antivirus y cortafuegos, nombres de usuario y contraseñas.

3. Mejorar la capacidad para hacer frente a los ciberataques, para este propósito es necesario que los estados miembros tengan en correcto funcionamiento los CERT, posteriormente que estos centros estén interconectados.

La estrategia de Seguridad Nacional deberá tener en cuenta la Ciberseguridad y la consecuente Defensa Nacional deberá incluir planteamientos nuevos e imaginativos, acompañados de cambios de mentalidad para darle más atención a la Ciberdefensa y la Ciberseguridad, para lo cual se deben precisar los objetivos estratégicos a alcanzar, los órganos competentes y sus funciones, su contribución a las distintas instituciones del país, el nivel tecnológico a alcanzar y las metas en I+D.

En Colombia no se ha definido una legislación específica y completa en materia de seguridad, por eso las responsabilidades en el ciberespacio no están del todo claras, entendiéndose el no establecimiento de un organismo o entidad oficial que dirija la estrategia de seguridad en el ciberespacio, consecuentemente los objetivos no se observan, con lo cual se genera preocupación al advertir que no se le da la importancia necesaria al tema de la seguridad en el ciberespacio.

Es importante que exista una autoridad nacional que defina una estrategia nacional de Ciberseguridad y establezca la Ciberdefensa coordinando las distintas instituciones (Estatales, Armadas y Privadas), medidas a tomar y acciones a realizar.

1.5 Estructura del ciberespacio y ciberactividades

El Ciberespacio (como campo de operaciones) está dividido en tres capas: la sintáctica, la semántica y la física, entonces, todo lo que conocemos como programas, información que reposa en los servidores y discos conforman la capa semántica; ahora, los protocolos, sistemas operativos, lenguajes de programación, constituyen la capa sintáctica, esta es la más utilizada por los hackers e intrusos, ya sea explotando una imperfección en el diseño o una puerta trasera dejada con intención por el programador para hacer correcciones posteriores. Por último, está la capa física, formada por discos duros, monitores, teclados, servidores (ubicados a nivel mundial), cables submarinos y hasta satélites por donde pasa mucha información (Gaitán, 2016).

En el ciberespacio se presenta un reequilibrio de fuerzas, en este mundo virtual, las fuerzas de cada país están mucho más cerca del equilibrio que en elmundo físico, por esta razón los Estados que han mantenido la hegemonía en el mundo contemporáneo, están más cerca de perder ese poder por las características que presenta el ciberespacio, donde una persona con los conocimientos necesarios y valiéndose de unas máquinas adecuadas (sin que esto implique altos costos) puede llegar a afectar la normal convivencia de los habitantes de una nación específica.

Si definimos un ciberataque como toda acción intencionada que se inicia en un equipo informático, con el objetivo de comprometer la confidencialidad, disponibilidad o integridad del equipo, red o sitio web atacado y de la información contenida o transmitida a través de ellos, podremos estar hablando tanto de ataques DoS (denegación de servicio), infecciones por *malware*, *phishing*, robo de credenciales o robo de información, en definitiva, de incidentes de seguridad que usan medios digitales para lograr un fin ilícito.

Por tanto, un ciberincidente o la brecha de seguridad es el resultado de un ciberataque que puede afectar a los sistemas militares, corporativos o a los sistemas industriales en infraestructuras civiles. Junto con la evaluación y gestión de riesgos dinámica, una práctica de operación eficaz pasa por identificar los posibles escenarios de ataque (análisis de escenarios excluyentes).

En los ochenta y los noventa, los cibercriminales actuaban compelidos por el deseo de superar desafíos tecnológicos. Creaban un virus y su objetivo era lograr afectar el mayor número de máquinas posibles. Los ataques representaban, ante todo, incomodidad y pérdida de tiempo. Estos individuos solían actuar en soledad. Sin embargo, con la masificación de la tecnología sobrevino una revolución social. Ahora, la mayoría de las instancias de la vida de los individuos se encuentran influenciadas por un avance tecnológico. La evolución de esta arista de la ciencia se ha visto acompañada de la evolución del crimen en las lides virtuales

El cibercriminal ya no actúa en solitario y sus ataques han adquirido un matiz diferente, sus motivaciones son, sobre todo, económicas (robar dinero o información). El cibercriminal se ha convertido en una actividad con la complejidad propia de una empresa. La expansión del crimen virtual se ve soportada por las cifras. Según la firma de seguridad informática Symantec, en el 2009 se detectaron 2'361.414 programas maliciosos. En cuestión de seis años se vio un crecimiento superior al 20.000 por ciento. En el 2015 se detectaron 430,5 millones. En otras palabras, se crean 1'179.000 amenazas por día. El carácter "profesional" del cibercrimen ha conllevado a que se configure un nuevo perfil para el individuo encargado de perseguir a los ladrones de la red. El nuevo perfil del profesional en seguridad informática

representa la tecnificación de la labor criminal en el entorno tecnológico, obliga a la formación de profesionales de la seguridad informática con un mayor grado de especialización e interdisciplinaridad. "Debe contar con un fundamento tecnológico, por supuesto. Estamos hablando de alguien que va a proteger tecnología. Debe saber programación, bases de datos, redes, aplicaciones; debe entender sobre criptografía, cortafuegos, técnicas de protección contra intrusos, contra programa malicioso. Pero, además debe ser un profesional con entendimiento en otras áreas: debe saber sobre legislación, para concebir castigos acordes y apropiados para los crímenes cometidos en el ámbito virtual e incluso, debe estar preparado para atender a las víctimas del cibercrimen desde la perspectiva psicológica.

Dada la complejidad del universo del cibercrimen, se hace cada vez más necesario que este profesional desarrolle estrategias para comunicar las amenazas con claridad. Si este profesional trabaja en un hospital, es menester que conozca sobre medicina. Si forma parte de un grupo mediático, debe entender sobre comunicación y temas relacionados. Es un oficio que debe alimentarse de otras ramas de la ciencia, porque la tecnología ahora impacta todas las aristas de la vida, debe caracterizarse por contar con una metodología clara en su proceder y una ética intachable.

Son organizaciones "empresariales", porque el cibercrimen se ve cada vez más como una fuente de dinero. Como cualquier empresa, estos individuos quieren tener cada vez más "clientes"; por ende, extienden su cartera de servicios y disponen de una estructura conformada por áreas dedicadas a los recursos humanos, al manejo financiero, a la planeación estratégica, a la investigación y a las ventas.

Las personas dedicadas a este oficio tienen altos conocimiento en programación, sistemas, bases de datos redes y estándares de la industria. Regularmente son autodidactas y tienden a crear sus propias comunidades. Otro aspecto que caracteriza a estas organizaciones es su carácter global, disponen de integrantes en todo el mundo (Gaitán, 2016). En Colombia, la Fiscalía General de la Nación, cada hora recibe más de 27.000 ataques cibernéticos desde computadores ubicados en todo el mundo que buscan desestabilizar los sistemas de seguridad del ente acusador, robar o dañar información o, simplemente, que un 'hacker' gane reputación penetrando los dispositivos de control establecidos en el organismo. Para enfrentar esas constantes amenazas, la Fiscalía ubicó en el búnker de Bogotá el Centro de Operaciones de Seguridad (SOC, por sus siglas en inglés), en donde desde el 2013 un grupo de ingenieros monitorea y pone en marcha en tiempo real maniobras para rechazar ataques desde servidores en el exterior o, incluso, intentos de saboteo originados en computadores de la misma entidad.

En el lugar, un grupo de analistas vigila 24 horas al día, los siete días a la semana, los sistemas de la Fiscalía, desde la página web de la entidad hasta el sistema penal oral acusatorio (SPOA), que es uno de los blancos más sensibles, pues allí está en línea la información de las personas que tienen o han tenido procesos penales, la etapa del proceso, la existencia de orden de captura y otros datos de las investigaciones.

Una de las tareas de los analistas es evitar que la información del SPOA sea robada o modificada. De hecho, técnicos confirmaron que tras la captura del 'hacker' Andrés Fernando Sepúlveda y las versiones de que él había logrado ingresar al sistema, se puso en marcha un plan de contingencias y rastreo que terminó determinando que las barreras de seguridad no habían

sido rotas.

Los expertos han logrado establecer que cada año hay más de 6.000 millones de eventos en los que alguien ha intentado ingresar a la plataforma de la Fiscalía, ya sea mediante gusanos, ataques masivos, 'phishing' u otras modalidades. Los ataques pueden ser directos por la red o por descuido de funcionarios que descargan de internet información en sus computadores o que han usado memorias con virus. De esos eventos, en el último año, 242 millones fueron considerados amenazas y 6.863, hechos críticos en los que había una clara intención de intentar dañar o robar información. Los ataques provienen especialmente de servidores ubicados en China, Estados Unidos, Rusia, Israel, Francia, Brasil, Honduras, Venezuela, México y Colombia.

En las pantallas de la central de seguridad, los analistas observan en tiempo real cómo empiezan a ingresar mensajes sospechosos a la Fiscalía y el sistema los empieza a clasificar según el nivel de riesgo; si no es alto, el mismo sistema les cierra la puerta a los mensajes, pero, en los casos de mayor alerta, los técnicos lo hacen manualmente estableciendo códigos de bloqueo, según la modalidad de ataque. Luego de que el visitante no autorizado es neutralizado, se reporta internacionalmente su información y entra a una lista negra que pone en alerta a los sistemas de seguridad del mundo.

En ese centro se observa cómo otros países son objeto de ataques masivos y se siguen los mecanismos puestos en marcha por esas naciones para combatir a los 'hackers', lo que permite a los técnicos colombianos tener información sobre cómo enfrentar un ataque de esas características.

La externalización, si bien está demostrando que sirve para ahorrar costos y generar un tejido empresarial alrededor de los organismos gubernamentales, también está afectando la seguridad por los sistemas y la información que emplean. Más del 80% de los sistemas críticos para una nación están en manos privadas y su protección es solo parcialmente responsabilidad de los gobiernos (Jordán & Torres, 2007).

El Ciberespacio es un escenario físico, único y diferenciado. El Ciberespacio es un entorno físico incluso de mayor extensión que los tradicionales. Aunque popularmente se le viene denominando "espacio virtual", pero de eso tiene muy poco, ya que está compuesto por una tela de araña de equipos informáticos y de comunicaciones interconectados.

El Ciberespacio exige de las autoridades principalmente innovación y constante seguimiento a los desarrollos, modificaciones y adaptación a entornos cambiantes y volátiles, dadas las repercusiones prácticas que para la mitigación consecuencial tiene el retardo tecnológico. EN consecuencia, el equipamiento para este tipo de amenazas requiere no solo altas capacidades técnicas y tecnológicas, también exige de los encargados de mitigación un proceso constante de capacitación y sofisticación de capacidades, de lo contrario no sería dable pensar en responder de manera adecuada a dichos desafíos. requiere la utilización de medios específicos para moverse, desenvolverse y combatir en él. La lucha en el ciberespacio requiere de elementos especiales muy diferentes a los utilizados en las guerras convencionales, por lo consiguiente los elementos que tenemos en nuestros hogares para conectarnos a internet no pueden ser los que servirían para desenvolver la guerra en el ciberespacio, estos deberán estar especialmente diseñados para combatir en el nuevo escenario, como cortafuegos, sistemas de detección de intrusos, sistema de previsión de intrusos, equipos de correlación y gestión de eventos de seguridad de información, acompañados de hardware robustecidos, con sistemas operativos y aplicaciones especialmente

diseñados y codificados, con configuraciones reforzadas y con redundancia que les permita tener una alta disponibilidad para asegurarse la supervivencia en caso de ataques contra ellos mismos.

Las operaciones en el ciberespacio se complementan a las de los dominios convencionales, disponen de un objetivo estratégico, operacional y/o táctico, requiere de la acción ofensiva para lograr la iniciativa, concentración de fuerzas con distribución de recursos eficiente, maniobrar con seguridad mediante acciones de ciberespionaje para obtener posiciones ventajosas; todo lo anterior dirigido por un único mando del más alto nivel, circunstancia que posibilitaría el anclaje estratégico bajo el cual debe pensarse en la gestión de los procesos de ciberseguridad, dado que resulta imprescindible esclarecer que no se está actuando frente a una amenaza residual o asistemática, es un imperativo encauzar la naturaleza precisa del fenómeno que se está estudiando, no solo en cuanto a su capacidad, sino también en relación con su poder potencial para generar afectaciones graves a la infraestructura crítica nacional.

En el ciberespacio también existen armas defensivas y ofensivas, pero con otra índole, para ser más precisos, las armas defensivas están compuestas por dispositivos de análisis y control de tráfico de *red*, hardware y software de seguridad, configuraciones correctas, procedimientos y protocolos de usuarios; y las armas ofensivas se construirán conbase en la investigación, generación de código, conocimientos adecuados y adecuados procedimientos. En este escenario, la información es el objetivo y artículo más apreciado, en la acción defensiva se tiene que proteger y en la ofensiva se ha de negar, alterar o sustraeral enemigo. Es importante determinar la calidad de la información, ya que esta cualidad es más importante que la cantidad. De la misma manera como en la guerra convencional se buscaba atacar los centros de abastecimiento y objetivos económicos de la nación atacada, en este espacio el

campo de combate está en todos los rincones de la nación, puede entrar en cada uno de los lugares de interés de los estados en conflicto y de interrumpir los suministros necesarios para la supervivencia.

2.ESTRATEGIAS PARA EL CONTROL DEL CIBERESPACIO

Entender la manera como los Estados han venido desarrollando su infraestructura, tanto para responder a las condiciones volátiles de los entornos, como para adaptarse a los retos representados por un Sistema Internacional cada vez más hostil, entendiendo que se advierten usos indiscriminados de las herramientas de orden tecnológico, a partir de las cuales se pueden desarrollar ejercicios *pseudo militares*, y que en consecuencia pueden representar afectaciones graves a los intereses de índole nacional de cualquier Estado.

Dicho entorno ha posibilitado la destinación ingente, tanto de recursos como de personal, a la mitigación de nuevos escenarios que resultan problemáticos para los Estados, entendiendo y manteniendo como premisa que cualquier falta de actuación, genera condiciones graves de riesgo que deberán ser o bien, asumidas o desplazadas. Este nuevo escenario de actuación representa un desafío para todos los Estados, no existen actores más o menos afectados por las amenazas cibernéticas, la diferencia está dada por la existencia de procesos de preparación frente a las condiciones de mitigación o respuesta que puedan presentarse.

En dicho escenario, resulta importante resaltar algunos esfuerzos, tal como el desarrollado por Estados Unidos, quien de manera temprana advirtió la necesidad de entender el potencial del ciberespacio como un entorno estratégico que requiere generar las condiciones para garantizar un control de pleno espectro. En consecuencia, EE. UU. Ha desarrollado estrategias para el control del Ciberespacio, para lo cual crearon el USCYBERCOM. Con la creación del USCYBERCOM Estados Unidos ha militarizado la *red* al considerar esta como el quinto espacio de batalla, la doble función de su comandante muestra la importancia que tiene la ciberseguridad para la administración, además del hecho de que se haya desplazado el centro de gravedad hacia el ciberespacio.

Desplazar el centro de gravedad no consistió solo en la destinación de personal en relación con la generación de nuevas capacidades, sino que incluyó todo un proceso de transformación institucional que estuvo mediada por la investigación, participación de la comunidad académica y redes de expertos que propendieron por dotar al conductor político de herramientas suficientes para entender y asimilar la naturaleza etérea del ciberespacio como el principal activo a explotar, en relación con los intereses nacionales.

Ahora bien, en cuanto a Rusia, país a menudo señalado como origen de graves ciberataques del estilo de los sufridos por Estonia en el año 2007 y Georgia en el año 2008, ha logrado sancionar la nueva doctrina militar en la que prevé la utilización de operaciones en la *red* en apoyo de las operaciones militares, así como la utilización de las tecnologías de la información para valorar y predecir situaciones y relaciones político-militares, con el objetivo de prevenir y disuadir el desencadenamiento de conflictos militares; así, las capacidades de la ciberguerra rusa estarían repartidas ente su servicio de inteligencia, el Estado Mayor Conjunto y la Guardia Federal (encargada de las TIC) (Gaitán, 2016).

En el ciberespacio, la principal herramienta es la información, a diferencia de los otros espacios en la guerra convencional (tierra, mar, aire, espacio) donde lo principal además del ser humano son los medios materiales.

El ciberespacio fue declarado por como el quinto dominio después de la tierra, el mar, el aire y el espacio. Lo que ha generado procesos de alistamiento por parte de los Estados potencia, circunstancia que puede advertirse por ejemplo en el caso de Estados Unidos, quien está preparándose para la Ciberguerra, así como las correspondientes declaratorias frente a la

infraestructura crítica digital de América como «un activo estratégico nacional».

The Economist, plantea que los datos actuales se envían por numerosas rutas, pero la infraestructura digital global todavía es muy frágil. Más de las nueve décimas partes del tráfico de Internet viaja por cables de fibra óptica debajo del mar y éstos pueden ser saboteados alrededor de Nueva York, el Mar Rojo o el estrecho de Luzón en las islas Filipinas.

El tráfico de Internet está dirigido por 13 *clústers* de servidores de nombres de dominio, potencialmente vulnerables. Otros peligros pueden darse en las conexiones de cables de fibra óptica a través de países de África o de Asia. La masiva penetración del internet móvil está creando nuevos medios de ataques.

De igual forma, a manera de ejemplo, es importante observar la organización desarrollada para la Alianza Atlántica su NCIRC (OTAN, 2015), que constituye un elemento clave de la política de Ciberdefensa aliada, tal y como se indica en la declaración de los jefes de Estado y de Gobierno que se produce tras la cumbre de Lisboa celebrada a finales del año 2010, en la que se comprometen a acelerar su implementación y despliegue hasta alcanzar la capacidad plena operativa de la NCIRC durante el año 2012. Analizando con un poco más al detalle la NCIRC, nos sirve como referencia de su capacidad, puesta en ejecución en los entornos de Defensa.

La NCIRC se diseña para ser capaz de dar una serie de servicios de apoyo técnico y legal, que puedan responder a incidentes de seguridad informática dentro de la OTAN, implantando de forma centralizada tres grupos de medidas, así:

1. *Medias preventivas o preactivas:* que incluía, entre otros, la publicación de boletines de

seguridad, la distribución de actualizaciones de *software*, la disponibilidad de equipos de análisis de vulnerabilidades, etc.

2. *Medidas reactivas*: que incluía el soporte y la respuesta ante incidencias o intentos de intrusión.

3. *Asesoramiento legal:* que incluía el análisis forense, la investigación y la actualización normativa.

El diseño de la NCIRC debía responder a los siguientes requerimientos:

– Capacidad para coordinar la respuesta global de la OTAN durante un incidente.

– Base de conocimiento centralizada en apoyo de los administradores de sistemas locales.

– Centralizar los servicios en línea y los *in situ.*

– Centralizar los acuerdos de apoyo forense y también de asesoramiento legal.

– Optimización de recursos.

– Servir de punto de contacto de la OTAN con otros CERT externos.

Finalmente, el catálogo de servicios de la NCIRC incluía los siguientes:

– Gestión de incidentes.

– Información de vulnerabilidades y amenazas.

– Análisis de vulnerabilidades *(onlinein situ).*

– Servicios de consultoría (tecnológica y forense).

– Recopilación y monitorización de información de diversas fuentes: IDS, antivirus, cortafuegos, etc.

– Soporte en línea de actualizaciones automáticas, descargas *software* o procedimientos operativos estándar.

– Análisis de incidente y pruebas de seguridad.

Podemos concluir que la Ciberdefensa militar no es la Defensa Militar del ciberespacio de interés para la seguridad nacional, sino la defensa del ciberespacio de interés militar. En el campo de la Ciberdefensa Militar se debe elaborar la doctrina conjunta emanada por el departamento de Inteligencia (D-2) de las FF.MM. En las operaciones militares los ciberataques deben considerarse como una amenaza, ya que los sistemas de mando y control son objetivo primordial para las fuerzas enemigas, por ende para asegurar la libertad de acción en la conducción de operaciones es necesario garantizar el uso seguro de los canales de comunicación.

2.2 NACIONAL

Teniendo en cuenta las tendencias globales sobre el tema de la ciberseguridad, y el modelo de coordinación en Colombia emanado del CONPES 3701/2011, se estudia la organización presentada, a la cual se harán las posteriores referencias.

2.2.1 MODELO DE COORDINACIÓN EN COLOMBIA

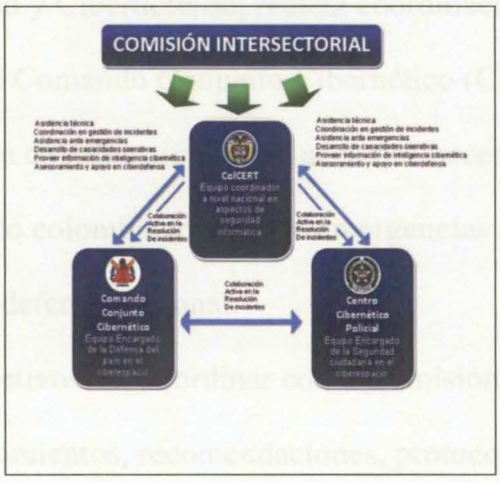

Ilustración 1 Modelo de Cooordinacion Nacional

(Conpes 3701 de 2011, 2011)

2.2.1.1 Comisión Intersectorial

La Comisión Intersectorial fue creada con la visión de convertirse en un organismo encargado de fijar la visión estratégica de la gestión de la información, así como de establecer los lineamientos de política respecto de la gestión de la infraestructura tecnológica (hardware, software y comunicaciones), información pública, ciberseguridad y Ciberdefensa. Esta Comisión estaría encabezada por el presidente de la República e integrada como mínimo por el Alto Asesor para la Seguridad Nacional, el Ministro de Defensa Nacional, el Ministro de Tecnologías de Información y Comunicaciones, el Director de la Agencia Nacional de Seguridad o quien haga sus veces, el Director de Planeación Nacional y el Coordinador del colCERT.

a. ColCERT

Por cuenta del mismo planteamiento fue creado el Grupo de Respuestas a Emergencias Cibernéticas perteneciente al Ministerio de Defensa Nacional, es un organismo coordinador a nivel nacional de ciberseguridad y Ciberdefensa; realiza coordinaciones y apoyo al Centro Cibernético Policial (CCP) y al Comando Conjunto Cibernético (CCOC).

La misión del ColCERT es la coordinación de las acciones necesarias para la protección de la infraestructura crítica del Estado colombiano frente a emergencias de ciberseguridad que atenten o comprometan la seguridad y defensa nacional.

El ColCERT tiene como objetivos: a. Coordinar con la comisión intersectorial el desarrollo y promoción de políticas, procedimientos, recomendaciones, protocolos y guías de ciberseguridad y Ciberdefensa, en conjunto con los agentes correspondientes y velar por su implementación y cumplimiento. B. Promover el desarrollo de capacidades locales/sectoriales así como la creación de CSIRTs sectoriales para la gestión operativa de los incidentes de ciberseguridad en la

infraestructura crítica nacional, el sector privado y la sociedad civil. C. Coordinar y asesorar a CSIRTs y entidades tanto del nivel público, privado y de la sociedad civil en la respuesta a incidentes informáticos (Ministerio de Defensa, 2017). Ofrecer servicios de prevención ante amenazas informáticas, respuesta frente a incidentes informáticos, así como aquellos de información, sensibilización y formación en materia de seguridad informática a todas las entidades que así lo requieran. D. Coordinar la ejecución de políticas e iniciativas público-privadas de sensibilización y formación de talento humano especializado, relativa a la ciberseguridad y Ciberdefensa. E. Apoyar a los organismos de seguridad e investigación del Estado en la prevención e investigación de delitos donde medien las tecnologías de la información y las comunicaciones. F. Fomentar un sistema de gestión de conocimiento relativo a la ciberseguridad y Ciberdefensa, orientado a la mejora de los servicios prestados por el colCERT. G. Proveer al CCP y al CCOC la información de inteligencia informática que sea requerida. H. Actuar como punto de contacto internacional con sus homólogos en otros países, así como con organismos internacionales involucrados en esta temática.

b. CCOC

El Comando Conjunto Cibernético de las Fuerzas Militares, organismo encabezado por el Comando General de las Fuerzas Militares, quien podrá delegar sus funciones dentro de las Fuerzas militares dependiendo de las especialidades existentes en el sector. Deberá prevenir y contrarrestar toda amenaza o ataque de naturaleza cibernética que afecte los valores e intereses nacionales. El CCOC deberá seguir los lineamientos nacionales y trabajará de manera coordinada con el ColCERT.

El CCOC tiene como funciones: a. Fortalecer las capacidades técnicas y operativas del país que permitan afrontar las amenazas informáticas y los ataques cibernéticos, a través de la

ejecución de medidas de defensa a nivel de hardware y/o software y la implementación de protocolos de Ciberdefensa. B. Defender la infraestructura crítica y minimizar los riesgos informáticos asociados con la información estratégica del país, así como reforzar la protección de los sistemas informáticos de la Fuerza Pública de Colombia. C. Desarrollar capacidades de neutralización y reacción ante incidentes informáticos, que atenten contra la Seguridad y Defensa Nacional.

C. CCP

Finalmente, en el marco de dicha estructura se puede encontrar el Centro Cibernético Policial, el cual estará encargado de la ciberseguridad del territorio colombiano, ofrece información, apoyo y protección ante los delitos cibernéticos. Desarrolla labores de prevención, atención, investigación y judicialización de los delitos informáticos en el país; informa en su página web sobre vulnerabilidades cibernéticas. Recibe y atiende los lineamientos nacionales en ciberseguridad y trabajará de forma coordinada con el colCERT.

Dentro de las funciones principales del CCP se encuentran: A. Proteger a la ciudadanía de las amenazas y/o delitos cibernéticos. B. Responder operativamente ante los delitos cibernéticos, con labores coordinadas de prevención, atención, investigación y de apoyo a la judicialización de los delitos informáticos en el país. C. Dar asesoría sobre vulnerabilidades y amenazas en sistemas informáticos. D. Divulgar información a la ciudadanía, que permita prevenir lo concerniente a pérdida de disponibilidad, integridad y/o confidencialidad de la información. E. Apoyar e investigar en coordinación con el colCERT las vulnerabilidades, amenazas e incidentes informáticos que afecten la seguridad de la infraestructura informática crítica de la Nación. F. Fomentar la concientización de políticas de seguridad cibernética en coordinación con los actores involucrados.

3. HERRAMIENTAS PREACTIVAS DE DEFENSA. UNA PERSPECTIVA INTEGRAL DE ANÁLISIS EN DEFENSA.

En el desarrollo de los conflictos, la ciberguerra está presente en todas las fases, desde los comienzos se emplea como ciberespionaje, luego como ciberataque dependerá de las tácticas que se adopten en el planeamiento conjunto de las operaciones, esta puede ser anterior o durante el mismo conflicto. De todos modos, los conflictos a lo largo de la historia han tenido el mismo propósito, subsanar necesidades económicas, territoriales, religiosas, étnicas, de unos grupos de personas agrupadas en una organización denominada Estado; lo que ha cambiado es el escenario de confrontación.

Los Estados utilizan los instrumentos de poder para influir o presionar a otros Estados a que cumplan con sus intereses u objetivos, estos "instrumentos de poder" se pueden encerrar entre los siguientes cuatro grades conjuntos:

1) Diplomático
2) Información
3) Militar
4) Económico

De estos instrumentos de poder, solo el militar permanece en el espacio físico de manera obligatoria, los demás presentan una característica física y otra cognitiva. Por lo anterior, el ciberespacio mantiene una influencia importante en los tres espacios restantes, ya que es en él donde se mantiene toda la información referente a acuerdos diplomáticos, embargos económicos o noticias. Así, el ciberespacio es un escenario estratégico, operacional y táctico. Todas las acciones que se puedan ejecutar en el ciberespacio han de tener una consecuencia en

el espacio físico y real, cualquiera que sea su propósito, por lo cual, la utilización de este teatro carecería de interés si no produce efectos en el plano físico, es decir en los escenarios terrestre, marítimo, espacial y aéreo.

La capacidad de las naciones para defender sus redes y sistemas siempre quedará por detrás de la habilidad del enemigo para aprovecharse de sus puntos débiles. Siempre existirán vulnerabilidades susceptibles de ser descubiertas por los expertos y siempre se superarán las medidas de seguridad que se impongan para intentar evitar intrusiones. Es por esto que una acción meramente defensiva no puede garantizar un empleo seguro o mayormente seguro para la navegación por el ciberespacio.

La capacidad de ciberespionaje y ciberataque es exclusivamente militar y a la vez políticamente delicada por lo cual es menester que se empiecen a desarrollar las acciones tendientes a cumplir con estas tareas, lo anterior se debe poner en práctica con el personal que se destine al ColCERT, logrando incluir dentro de otras funciones las siguientes: Especialización, Dedicación, Formación, Economía, Doctrina, Organización, Operación e Imagen.
Especialización: Técnicas defensivas necesarias para asegurar la confidencialidad, integridad y disponibilidad de los sistemas, así como garantizar la autenticidad de los usuarios y la trazabilidad de sus acciones. Igualmente requería conocimiento de técnicas ofensivas, análisis y explotación de vulnerabilidades, penetración en sistemas, descifrado, codificación de exploits y aprendizaje de técnicas de stealth de evasión y de borrado de huellas, etc.
Dedicación: personal que durante toda la carrera tenga exclusividad en el combate del ciberespacio.

Formación: unificada, serviría para estandarizar criterios, economizar recursos. Economía: una sola organización permite disminuir gastos.

Doctrina: Disponer, complementar y actualizar la doctrina que sirva de base para el desarrollo de las tareas en todos los ámbitos.

Ahora bien de cara a las necesidades estratégicas, operacionales Las clases de defensa se determinan en tres tipos:

- **Defensa preactivas**: son las que se ejecutan antes de que se produzca el ataque enemigo. Entre ellas están la concientización y formación de usuarios y técnicos, la definición de normas y procedimientos, la instalación y la configuración correcta de hardware y software, y las acciones de disuasión.
- **Defensas proactivas**: son las que se ejecutan en el momento que se detecta el posible ataque enemigo. Estarán basadas principalmente en normas de procedimiento (análisis de eventos, determinación de atribuciones, desconexión de sistemas, lanzamiento de contraataques, etc.) dentro de las defensas proactivas se puede distinguir tres tipos:
  - Reacción pasiva: solo se ponen defensas
  - Reacción semiactiva: defensas con pequeñas acciones no agresivas
  - Reacción activa: contraataques contra agresores
- **Defensas reactivas**: son las que se deben ejecutar una vez se haya producido el ataque enemigo, sin importar si esta ha tenido éxito o no. Son las acciones encaminadas a la recuperación y aumento de la disponibilidad de los sistemas o a averiguar en qué sistemas se ha producido el daño o robo de la información e inmediatamente poner los medios para evitar su repetición (Gaitán, 2016).

Las capacidades necesarias para la Ciberdefensa, con base en la doctrina de la NC3A, las

podemos establecer para la presente propuesta, de la siguiente manera:

1) **Detección de actividad maliciosa**: recopilando información con una gama de sensores, desarrollando los controles de la siguiente manera:
   - Recopilación de datos: detección de intrusos, escáneres de vulnerabilidad, informes de registros de eventos.
   - Evaluación con otras agencias: comparar ataques recibidos por otras entidades
   - Correlación de datos: recibidos por los diferentes sensores
   - Asignación de capacidades a las agencias: con base en las tareas que se requieran y a las funciones que cada agencia esté en capacidad de desarrollar
   - Evaluación de la situación: mediante la correlación de agencias, localización de la fuente técnica del ataque, interpretación de la actividad, interpretación del contexto y visualización para hacer análisis.
2) **Prevención, mitigación y terminación de ataques; mediante:**
   - Reconfiguración de la estructura de los sistemas de información, comunicaciones, su interconexión y la configuración de cualquiera de los módulos (reubicación de los servicios de información asociados a las TIC; compartimentación de sistemas; cierre de componentes y servicios; revocación de credenciales; actualización de Software).
   - Control del flujo de tráfico: terminar o limitar el flujo de datos.
   - Decepción: crear áreas del sistema TIC para que el ataque no genere impacto
   - Defensa activa: únicamente para parar o mitigar un ataque.
   - Coordinación de la respuesta externa: con terceros (proveedores)
3) **Análisis dinámico de riesgos, ataques y daños**: se desarrolla mediante la valoración de

activos, que refiere a los servicios que proporciona el sistema para la organización; Evaluación de la amenaza; Análisis de vulnerabilidades; Estructura del sistema; Valoración de ataques; Evaluación de daños (análisis del malware, identificación de sistemas afectados, verificación del estado de la información, diagnóstico de la disponibilidad del servicio).

4) **Recuperación de los ciberataques**: mediante la restauración del sistema y la información a su estado original y a sus propiedades de seguridad, logrando:
   - Restaurar totalmente el sistema: puede ser necesaria una reinstalación de este
   - Restauración de la información
   - Registro de la información comprometida: para que las partes interesadas tomas las medidas pertinentes
5) **Toma de decisiones**: de manera oportuna, teniendo como referencia la cantidad de acciones que se presentan en el ciberespacio, esto se lleva a cabo mediante:
   - Identificación de opciones
   - Coordinación con las partes implicadas
   - Comunicación de la decisión a los interesados e implicados
6) **Gestión del riesgo**: recopilar información para realizar un sondeo de la capacidad del atacante y compartirla con los colaboradores y agencias a fines, para tener una mejor evaluación del riesgo e implementar las medidas preventivas, buscando reunir y compartir información vital, garantizada e histórica, para apoyar futuras acciones.

"La ventana de Johari se trata de un modelo que intenta explicar el flujo de información desde dos ópticas o puntos de vista; el primero la exposición (cuanto se muestra a los demás) y el

segundo la retroalimentación (cuanto se acepta de los demás), mostrando de esta manera la interacción entre dos fuentes de emisión; los demás y el yo". (Fritzen, Silvino José, 2002).

Si bies cierto que este modelo fue diseñado inicialmente para mejorar la comunicación entre grupos a nivel de relaciones interpersonales que permitiera a los miembros de estos recibir un feedback acerca de lo como los perciben los demás. Este modelo permite de una u otra forma reinterpretarse para dar paso a realizar diferentes aplicaciones así como hasta hoy en día se ha hecho, si bien es cierto que este inicialmente fue aplicado a procesos de psicología cognitiva hoy en día ya se puede aplicar en procesos educativos y laborales, en el mundo de las estrategias de marketing así como en talleres orientados al desarrollo personal.

La importancia del modelo de la ventana de Johari va a permitir observarnos desde el exterior, incuso desde el exterior cercano de nuestra organizaciones, de esta forma este modelo permite reinterpretarse y ser aplicado a escenarios ajustado a la ciberseguridad y particularmente a los riesgos que se alinean con esta, permitiendo de esta forma poder convertirla en una herramienta preactiva prospectiva en donde por mantener la una identificación de los riesgos de tipo lineal pueden dejarse de observar aspectos, los cuales no estrictamente están relacionados con el exterior como u todo de la organización sino que aquellos también que confluyen fuera de las áreas de ciberseguridad y de las áreas de la seguridad informática.

"En la gestión empresarial, un aspecto interesante es que podemos repetir ese mismo ejercicio con diferentes grupos. Ese "nosotros" puede ser la dirección de la empresa, la de un departamento o cualquier conjunto de personas que formen parte de la organización. Y "los demás" puede ser un panel de expertos, personas que trabajan en otros departamentos, consumidores" (García, 2018). Como anteriormente se menciona la ventana de Johari puede ser aplicado en cualquier área de la organización, de esta forma al realizar una reinterpretación

orientada a que se convierta en una herramienta preactiva que nos permita conocer que aspectos en materia de riesgos no estamos identificando o no observamos por razones que pueden ir desde el desconocimiento de las funciones especificas de otras áreas hasta por el simple hecho de que nos limitamos a establecer los riesgos que son comunes o a los cuales siempre la organización sabe como realizar los planes de mitigación, es decir esa primera parte del modelo que es lo publico, a lo que todos los años tras años realizan, esos planes de mitigación que están orientados a lo que los directivos quieren escuchar que la organización es capaz de mitigar, una de las cuatro partes que la organización esta cómoda frente a esos riesgos y amenazas.

La áreas que comprenden el modelo de Johari: Abierta, oculta, ciega y desconocida aportan para que se realice un reinterpretación aplicada a la ciberseguridad en donde tal y como sucede en el modelo base no solo mejore los procesos de comunicación organizacionales sino que también permita identificar riesgos y amenazas que si bien pueden conocerse o tener indicios de su existencia no son contemplados en ningún plan de manejo de riesgos y/o estrategia de la organización que permitan anticiparse a la forma afrontarlos en caso de que se materialice alguno de ellos.

"El análisis del modelo esta hecho sobre el individuo, Yo (uno mismo) y su relación con los demás. Pero cambiando la palabra Yo (uno mismo) por "equipo" o "grupo", el modelo también permite un acercamiento a la dinámica de grupos o equipos y su entorno. Así es que a medida que se va ampliando el área Abierta gracias a una mayor comunicación, su evolución hace que se reduzcan las restantes áreas. Y lo ideal es que la mencionada área Abierta vaya precisamente ampliando su radio de acción, de forma que se reduzca al mínimo el resto de las áreas desconocidas, tanto de los demás como de nosotros mismos." (Fritzen, Silvino José, 2002).

Este modelo plantea como la reducción del tamaño de las otras áreas permite que el área al que

normalmente las organizaciones están limitadas es decir a una de las cuatro partes, la cual es esa área publica que en el modelo se ha reinterpretado como las amenazas conocidas incremente su tamaño y de esta manera poder contar con el diseño de planes de mitigación o de la reorientación de una estrategia en materia de ciberseguridad en una organización.

"Avanzar en la gestión de la seguridad de la información, es conquistar nuestro temor natural por la inseguridad, por la materialización de los riesgos. Mientras un riesgo no sea una oportunidad para desaprender del entorno y repensar nuestras medidas de seguridad, la inseguridad de la información será un escenario desconocido donde la industria, las vulnerabilidades y el individuo se matizan y se esconden al lente del responsable de la seguridad". (Cano, 2009).

La reinterpretación de los cuadrantes se afirma con lo referenciado anteriormente en el sentido que los riesgos no solo deben ser considerados en ciberseguridad en los escenarios conocidos sino que deben contemplarse todas aquellas situaciones que no se contemplan usualmente que conlleve a repensar como la organización mitiga los mismos o como aun no contempla un plan para afrontarlos.

"La buena gestión del riesgo significa prepararse para lo inesperado. Favorecer profundamente los activos para los que se espera un mejor desempeño mientras que se evitan aquellos que históricamente tienen un desempeño inferior puede parecer intuitivo, pero esta técnica no protege a las carteras. Eso significa tener una visión a largo plazo al elegir las inversiones y siempre considerar la potencialidad de que ocurra un evento y la probabilidad de que se produzca el evento, así como también el impacto que tendría en una cartera" (Cardona, 2007).

Hace años los expertos han ido concluido concordantemente con los nuevos y desconocidos escenarios que la gestión de los riesgos debe repensarse, sin importar el área a la que estos estén asociados toda vez que sin bien es cierto el impacto de estos pueden verse reflejados en costos

elevados para la organización en otros la imagen institucional puede verse afectada, lo anterior depende del foco sectorial en la cual se desempeñe la misma.

Así mismo en el informe realizado por Asobancaria y la OEA en octubre de 2019 refiere que "De acuerdo con la visión general del estado de la seguridad cibernética en Colombia, para ese momento el país cuenta con una estrategia de seguridad cibernética nacional y un programa de seguridad cibernética coordinado vinculados a los riesgos, prioridades y objetivos nacionales. Así mismo, asegura que se han identificado amenazas especificas a la seguridad nacional en el ciberespacio, pero aún no se cuenta con una estrategia de respuesta coherente. En materia de coordinación destaca que existen acuerdos entre los sectores público y privado en materia de defensa cibernética y que agencias lideres del Estado, así como empresas líderes del sector privado han comenzado a darle prioridad a la seguridad cibernética mediante la identificación de riesgos, amenazas y prácticas de alto riesgo." (Castaño 2019), en donde claramente el país ha realizado esfuerzos para mitigar los riesgos de ciberseguridad pero también resalta que aun se presentan brechas de preparación y de gestión frente a estos, con lo cual se hace necesario continuar trabajando en este aspectos de tal forma que aporta con herramientas orientadas a mejorar el entorno en que se gestionan los riesgos resultan un aporte positivo sumando esta también a contribuir no solo a la identificación de riesgos sino también a la toma de decisiones y al mejoramiento de la cultura organizacional.

3.1 PERSPECTIVA PROSPECTIVA DE ANÁLISIS EN DEFENSA

"En Colombia existe una claridad creciente acerca de la importancia de los estudios del futuro y que hay un interés interinstitucional en camino por aprender de las experiencias

nacionales e internacionales, lo cual será sin duda fundamental para el futuro del Sistema Nacional de Ciencia y Tecnología, y para las políticas industrial, de comercio exterior, educación superior, medio ambiente y desarrollo regional, entre otras. Quizás esta coincidencia o sin cronicidad signifique una mayor conciencia acerca de que los grandes problemas del país requieren tratamientos estructurales y de largo aliento". (Henao, Jaramillo. 2015). Como se puede advertir, la generación de perspectivas de análisis a partir de las cuales puedan efectuarse valoraciones acertadas respecto a los retos de la Ciberseguridad y la Ciberdefensa resulta un imperativo misional para las diferentes entidades cuyas responsabilidades recaigan en la generación de entornos seguros o carentes de vulnerabilidades excesivas. Con dicha finalidad este documento busca poner a consideración categorías de análisis y una perspectiva integradora por medio de la cual pueda procesarse la información relativa a riesgos o amenazas y en consecuencia pueda emplearse como herramienta al momento de determinar cuál es el curso causal adecuado de cara a las necesidades de anulación, mitigación o morigeración fenomenológica.

Como se ha establecido previamente, en el campo de la Ciberseguridad y Ciberdefensa el manejo y disponibilidad de la información constituye el principal activo, razón por la cual resulta imprescindible contar con herramientas técnicas que faciliten la producción de documentos que faciliten la toma de decisiones en lo que corresponde al planeamiento de la defensa o la formulación de políticas de Ciberdefensa que permitan a las organizaciones correspondiente, la aplicación de protocolos de alta calidad, que incidan directamente en la gestión, incidentes y/o amenazas.

Las diferentes categorías que deben ser identificadas y/o consideradas al momento de iniciar cualquier análisis prospectivo de defensa se catalogan en dos subgrupos relacionados de información; a. Información sistémica reconocida; y, b. Información sistémica desconocida, a partir de las cuales se desarrolla un ejercicio transversal relativo a la información de riesgos y amenazas distinguidos en varias tipologías a saber: i. conocidos, latentes, focalizados y emergentes.

Una vez pueda distribuirse la información sistémica disponible, de cara al reconocimiento de cada una de las tipologías establecidas por el modelo para la identificación de amenazas o riesgos latentes o emergentes, inicia el proceso de indización y análisis de cada una de las variables identificadas, ejercicio del cual necesariamente debe desprenderse el curso de acción más pertinente en lo que refiere a la formulación de una estrategia que permita contrarrestar o mitigar un fenómeno o incidente.

Ahora bien, el delineamiento de instrumentos de análisis pasa necesariamente por la determinación de las estructuras existentes, la capacidad en términos de pertinencia, conducencia y la eficacia relativa a la identificación de las posibilidades reales de incidir en la gestión de incidentes, riesgos o amenazas. En dicho escenario, la elección de modelo debe atender a especificidad relativa a los intereses nacionales, la infraestructura crítica y las necesidades estratégicas referidas al proceso específico.

"La estrategia debe instar a las entidades a dar prioridad a sus inversiones en ciberseguridad y a gestionar los riesgos de forma proactiva. Dependiendo del nivel de riesgo que la entidad desee asumir, se debe mantener un equilibrio entre las medidas de seguridad y los beneficios

potenciales, teniendo en cuenta la naturaleza dinámica del entorno digital. La estrategia también debe reconocer la necesidad de gestionar continuamente los riesgos y facilitar un planteamiento coherente entre entidades interdependientes" (Guía para la elaboración de una estrategia nacional de ciberseguridad). Esta guía para la elaboración de una estrategia nacional de ciberseguridad es conducente a que los riesgos sean gestionados proactivamente que contribuyan a la resiliencia de un estado, de esta forma también puede aplicar estos aspectos a una organización con lo cual una herramienta como el modelo propuesto contribuye a que los riesgos y las amenazas puedan ser gestionados de forma positiva y diferencial con un enfoque prospectivo que permita las toma de decisiones frente a riesgos y amenazas no identificadas o por lo contrario sin que cuenten con un plan de mitigación.

3.1.1 DELIMITACIÓN DE LAS CATEGORIAS DE ANÁLISIS DE INFORMACION

A. LATENCIA

Entendida como la condición en la cual una organización o Estado cuenta con información respecto a un riesgo o amenaza, pero no cuenta con planes o estrategias de respuesta para su mitigación. Esta categoría implica un amplio conocimiento de las capacidades, pero un bajo conocimiento del entorno o vectores de amenaza.

B. RIESGOS O AMENAZAS CONOCIDAS

Condición o categoría de análisis deseada, se cuenta con amplia y verificable información sobre el riesgo o amenaza, también se cuentan con planes o estrategias de mitigación. Respecto al conocimiento de las capacidades y los componentes del vector de amenaza existe una adecuada correlación.

C. RIESGOS O AMENAZAS FOCALES

Esta categoría implica la determinación y materialización del riesgo o amenaza en determinado sector o campo de acción del Estado, implica un estudio fenomenológico relativo a las consecuencias evidenciadas de la amenaza. Esta categoría está definida por la existencia de planes marco de respuesta, pero presenta importantes carencias en lo que refiere a componentes específicos de estrategia que permitan su mitigación. Implica la materialización de la tipología relacionada con la reactividad defensiva.

D. RIESGO O AMENAZA EMERGENTE

Categoría determinada por la existencia de riesgos o amenazas que constituyen el grado máximo de incertidumbre, representan el más alto grado de desconocimiento fenomenológico, tanto frente a sus causas como aquellas referidas a sus consecuencias. Esta categoría conlleva el ejercicio factico de llana reacción, toda vez que presenta características que no han podido ser anticipadas por los analistas o expertos técnicos.

El acumulado de las características mencionadas, efectuado el corte transversal en relación con el entorno tanto conocido como desconocido representa el principal reto que se tiene al momento de evaluar los incidentes que cuenten con el potencial de representar un riesgo para los intereses nacionales, o bien para la infraestructura crítica, circunstancia que requiere un riguroso análisis por cuenta de los operadores de información.

Con el propósito de eliminar grados inaceptables de incertidumbre, resulta imprescindible aplicar modelos técnicos de análisis de la información, tal como el que es presentado, toda vez que la adecuada atención tanto a las categorías de análisis, que proporcionan mecanismos

objetivos de análisis, como la integración en los espectros referidos a la disponibilidad de información relativa a los entornos, permiten a los tomadores de decisión o formuladores de política pública, la generación de diagnósticos que respondan en mayor medida a las necesidades estratégicas, las capacidades a desarrollar, los componentes mínimos de una estrategia que responda satisfactoriamente a los riesgos o amenazas que se presenten y la articulación de planes que desde el nivel estratégico también cuenten con la capacidad de hacer descender los requerimientos en lo operacional y lo táctico, de manera que se pueda proporcionar una visión integradora en la respuesta a incidentes de ciberseguridad o Ciberdefensa en relación con la protección de los intereses nacionales o la infraestructura física.

Tabla 1 Modelo de Análisis Prospectiva en Defensa

Primer nivel de análisis	Información Conocida	Información desconocida
Entorno conocido	**Riesgo o amenaza conocida**	**Riesgo o amenaza en latencia**
Entorno desconocido	**Riesgo o amenaza focalizado**	**Riesgo o amenaza emergente**

Segundo nivel de análisis

	DIAGNÓSTICO INICIAL	DIAGNÓSTICO INTERMEDIO	DIAGNÓSTICO FINAL
Relación con el entorno	**Riesgo o amenaza en latencia analizada**	**Capacidad nociva del riesgo o amenaza emergente**	**Riesgo o amenaza focalizada**
Capacidades propias	**Identificación de planes de manejo o estrategia de mitigación**	**Riesgo o amenaza conocida contrarrestada**	**Inventario de daños o consecuencias del incidente**

Fuente Elaboracion Propia basado en (Cano, 2014)

Ahora bien, filtrada la información disponible referida al incidente, las causas y consecuencia

de este, las capacidades de respuesta y las posibilidades reales de mitigación, corresponde la generación de cursos causales de acción que permitan elaborar respuestas con base en elementos objetivos de análisis, despojados de grados intolerables de incertidumbre. No obstante, frente a las posibilidades de generar análisis *ex post facto* el principal aporte perseguido a lo largo de la investigación, corresponde a evidenciar la necesidad de desarrollar constantes ejercicios de prospectiva, mediante el abordaje hipotético de diferentes tipologías y modalidades, aun pese a lo inverosímiles que pudiesen considerarse, tal como es planteado por (Clarke & Knake, 2011).

Un ejercicio analítico riguroso mediante la adecuada apropiación teórico-conceptual en los dos niveles presentados constituye una herramienta practica para la cabal valoración de las capacidades actuales y potenciales, circunstancia que resulta imperativa en el marco de delimitar las necesidades estratégicas y operativas en el marco de la ciberseguridad y la defensa, toda vez que sigue haciendo énfasis en la premisa bajo la cual debe partir el planeamiento o delineamiento de políticas en ciberseguridad y Ciberdefensa, consistente en la imperativa necesidad de anticipar en la mayor medida posible la aparición de cualquier riesgo o amenaza, aun pese a las dificultades propias de las lagunas de información en relación con el entorno.

Ante la aplicación abstracta de la perspectiva de análisis prospectivo, efectuando las respectivas reseñas de cara a la identificación de las categorías requeridas, pueden advertirse los siguientes componentes a considerar de cara el delineamiento, formulación y evaluación de políticas de gestión de la seguridad que incidan efectivamente en la gestión fenomenológica de riesgos y/o amenazas.

Ahora bien, las categorías analizadas frente a la determinación del grado de inminencia frente a la clasificación de riesgo, peligro o amenaza, constituye el elemento que permite determinar cuáles con los mecanismos que deban ser considerados al momento de filtrar las condiciones objetivas que tengan incidencia en el tipo de mecanismos a elegir para la gestión de incidentes o amenazas.

Existen dos niveles claramente definidos a partir de los cuales pueden incluirse datos que faciliten la toma de decisión frente a los insumos que deben ser incluidos en el modelo. El primero está caracterizado por las condiciones externas de la fuente originadora de riesgo, aspectos que necesariamente pasan por la determinación del tipo de actor, sus posibles motivaciones y/o intereses, aspecto que en términos estratégicos clásicos podría determinarse como la manifestación de la estrategia del adversario y el entorno.

Una vez se agote la inclusión de datos en este primer nivel, debe incluirse un segundo momento de evaluación, que necesariamente incluye un proceso de autoevaluación de capacidades, como mecanismo que permitan ponderar adecuadamente un balance de capacidades frente al fenómeno o incidente enfrentado, atendiendo a sus características inherentes a las manifestaciones de poder real y potencial. La valoración de estos niveles responde a la ponderación de elementos que definen taxativamente la posibilidad que tienen los Estados para gestionar sus procesos de planeamiento y respuesta ante incidentes.

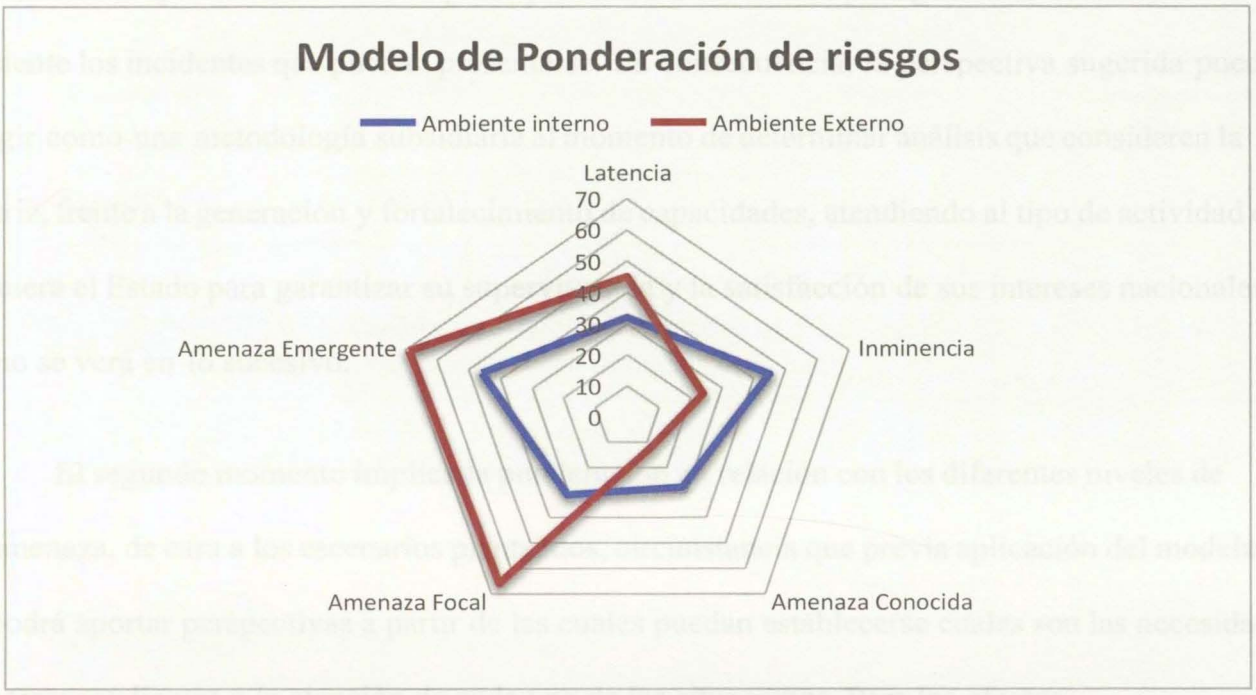

Ilustración 2 Modelo de Ponderación de riesgos

Fuente: Elaboración propia con fundamento en (Cano, 2014)

Resultado de la aplicación del mecanismo de análisis con fundamento en los diferentes niveles de riesgo, peligro o amenaza, surgen posibilidades de elección frente al catálogo de acciones ofensivas o defensivas que deben ser desplegadas por los Estados con la finalidad de garantizar la situación en la cual los intereses se encuentran a salvaguarda de cualquier amenaza interna o externa. Considerando que el modelo propuesto puede surgir como un instrumento de evaluación que atendiendo a categorías objetivas pueda aportar información que influya en las decisiones respecto a los procedimientos de planeamiento de las condiciones de ciberseguridad y Ciberdefensa del Estado, resulta relevante a la hora de formular diagnósticos que tengan como finalidad la elección de las herramientas que puedan incidir en la protección de los intereses nacionales, las cuales necesariamente deben atender a las capacidades que previamente han sido desarrolladas, pero aún más importante, puede ofrecer como resultado la identificación de

aquellas otras que aún no se tienen pero que resultan necesarias para gestionar de manera eficiente los incidentes que puedan presentarse. En consecuencia, la perspectiva sugerida puede fungir como una metodología subsidiaria al momento de determinar análisis que consideren la matriz, frente a la generación y fortalecimiento de capacidades, atendiendo al tipo de actividad que requiera el Estado para garantizar su supervivencia y la satisfacción de sus intereses nacionales, como se verá en lo sucesivo.

El segundo momento implica la ponderación en relación con los diferentes niveles de amenaza, de cara a los escenarios planteados, circunstancia que previa aplicación del modela podrá aportar perspectivas a partir de las cuales puedan establecerse cuales son las necesidades correspondientes a la atención de cada una de las situaciones. Para los efectos correspondientes fue empleado un instrumento de recolección de información cerrado aplicado a una población de 50 expertos en ciberseguridad, técnicos en ciberseguridad y miembros de la comunidad académica, para lo cual fue explicado de manera previa tanto el alcance del modelo como la finalidad de la aplicación correspondiente.

3.2 ALCANCE Y APLICACIÓN DEL INSTRUMENTO DE INVESTIGACION

El diagnóstico inicial se adelantó con 20 personas de diferentes sectores entre expertos temas de seguridad informática, directivos, así como de personal no afín a las mismas que se desempeña en cualquier otra área de la organización. El instrumento de medición definido fue la encuesta, y se formuló un cuestionario con 12 preguntas (ANEXOS). A continuación, la tabla, enseña las dimensiones y los respectivos objetivos de las preguntas del cuestionario diseñado.

Tabla 2 Dimensiones y objetivos

Dimensiones	Objetivos Dimensión	Número Preguntas Realizadas	A qué preguntas corresponde en el cuestionario
Organización	Conocer el tipo de organización actual al que pertenecen las personas encuestadas	2	1,3
Conocimiento sobres riesgo y amenazas de ciberseguridad	Conocer el grado de conocimiento de los diferentes perfiles en cuento a riesgos y amenazas cibernéticas	5	2,5,6,10,12
Procedimientos para identificar riesgos o amenazas de ciberseguridad.	Conocer la forma en que realizan la identificación de los riesgos y amenazas.	5	4,7,8,9,11

3.2.1 Trabajo de Campo: diagnóstico.

Una vez definida la muestra, se realizó el diseño del instrumento de recolección de la información (Anexo 1), el cual permitió realizar una caracterización de las personas y del sector que hicieron parte del trabajo de campo, su conocimiento, así como de sus procedimientos generales en la identificación de riesgos y amenazas de ciberseguridad punto de referencia para la evaluación del modelo propuesto.

Las ilustraciones 3 y 4 detallan los principales atributos y particularidades de las 20 personas que participaron en esta investigación, en donde se obtuvo que la encuesta fue realizada en un 70% por personal que tiene la responsabilidad directa en la gestión e identificación de riesgos y amenazas de ciberseguridad (alta dirección, líderes técnicos y jefes de departamento) y en el restante 30% se contó con la participación de miembros de los equipos de trabajo de las diferentes áreas.

Por otra parte, característica de esta población de muestra es que los dos más importantes sectores hacia donde están orientados sus servicios son el sector financiero (45%) y el sector de la seguridad del país. (25%).

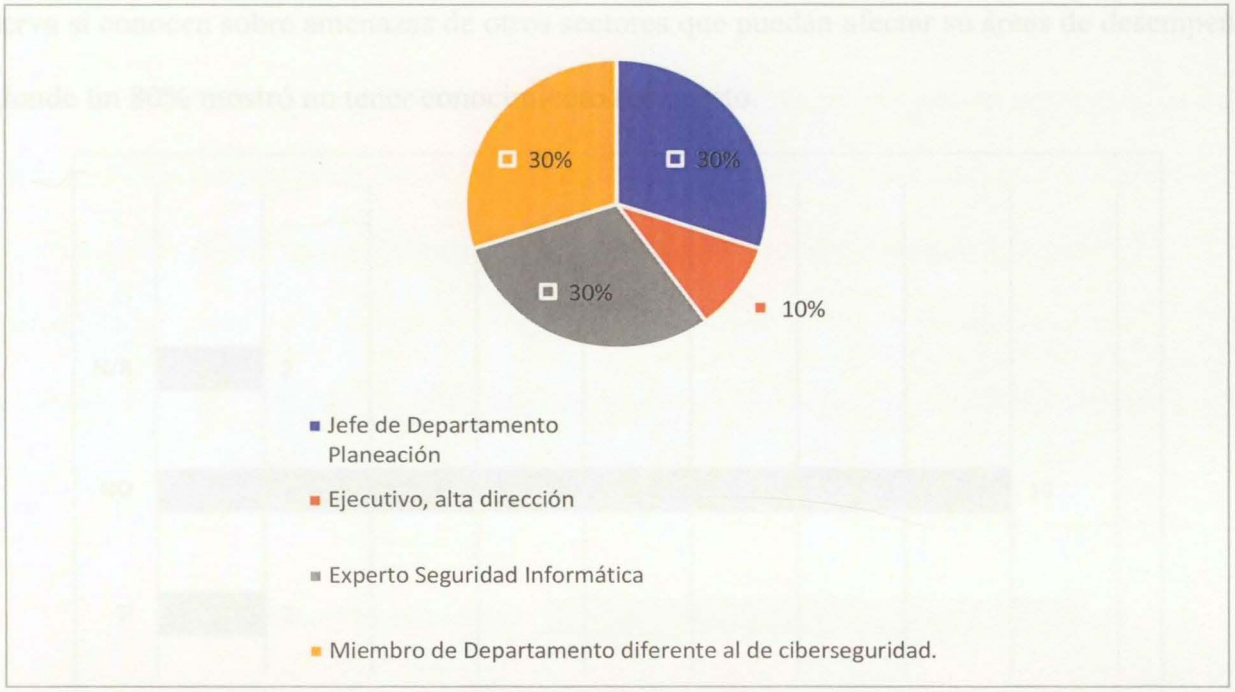

Ilustración 3 Perfil población de muestra

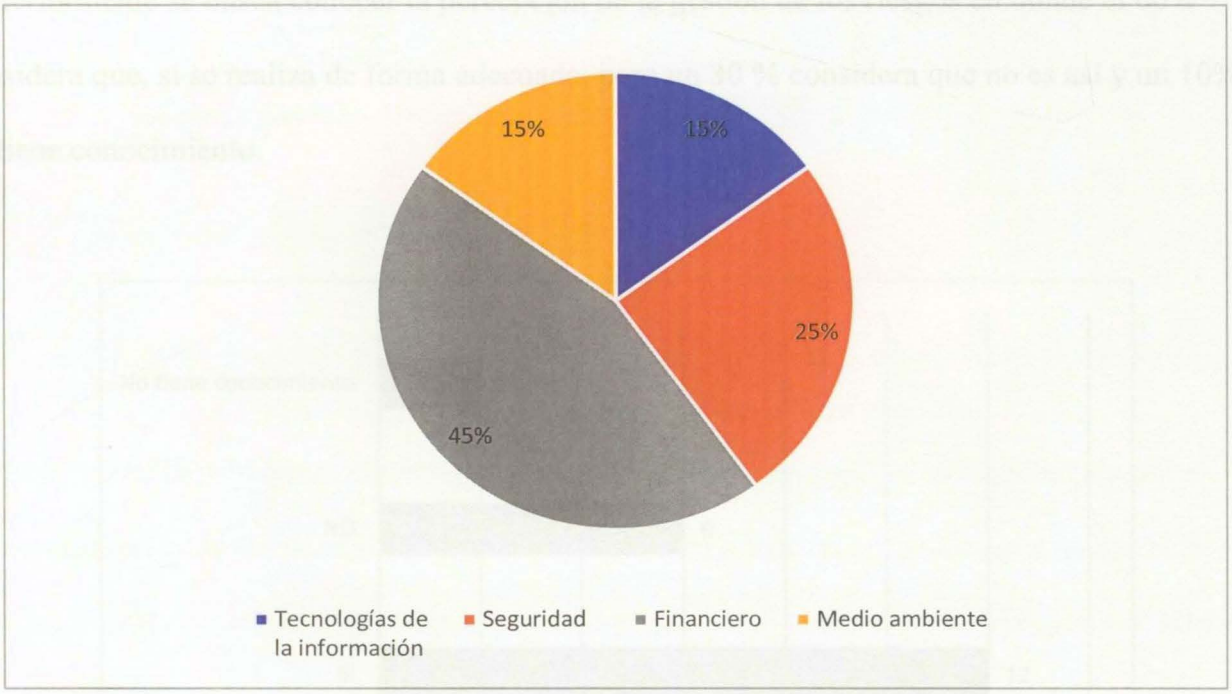

Ilustración 4 Sector al que pertenecen

A continuación, en las siguientes ilustraciones se muestra como los diferentes encuestados dan muestra de los conocimientos sobre los riesgos y amenazas en ciberseguridad, en donde se

observa si conocen sobre amenazas de otros sectores que puedan afectar su áreas de desempeño en donde un 80% mostró no tener conocimiento sobre esto.

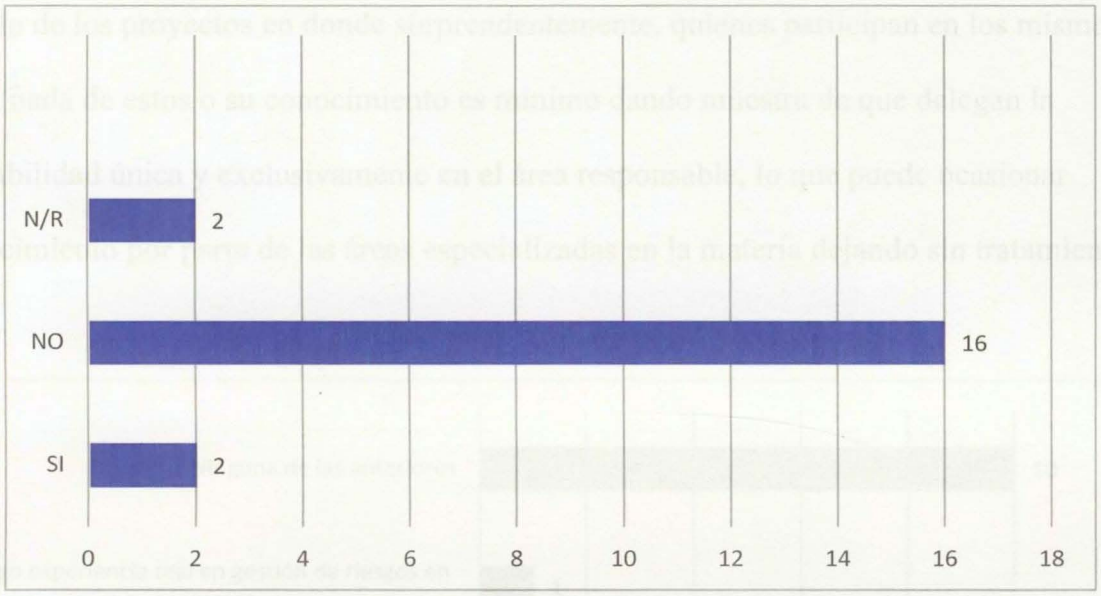

Ilustración 5 Conocimientos Amenazas en otros sectores

Posteriormente se busca conocer la percepción de la gestión de los riesgos en donde el 60% considera que, si se realiza de forma adecuada, pero un 30 % considera que no es así y un 10% no tiene conocimiento.

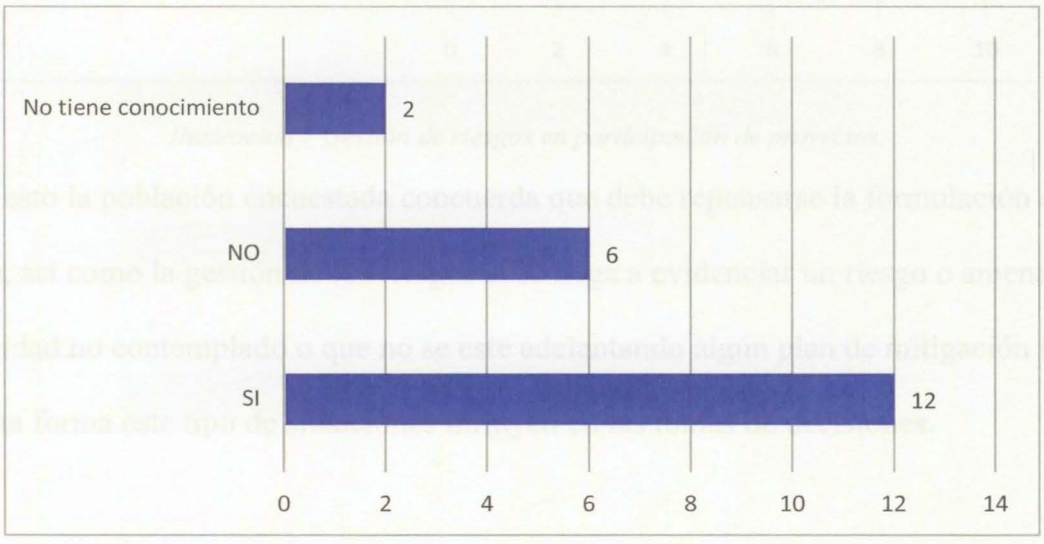

Ilustración 6 Percepción gestión de riesgos

Luego se busca conocer la importancia de la gestión de los riesgos durante la participación del desarrollo de los proyectos en donde sorprendentemente, quienes participan en los mismos o no conocen nada de estos o su conocimiento es mínimo dando muestra de que delegan la responsabilidad única y exclusivamente en el área responsable, lo que puede ocasionar desconocimiento por parte de las áreas especializadas en la materia dejando sin tratamiento los mismos.

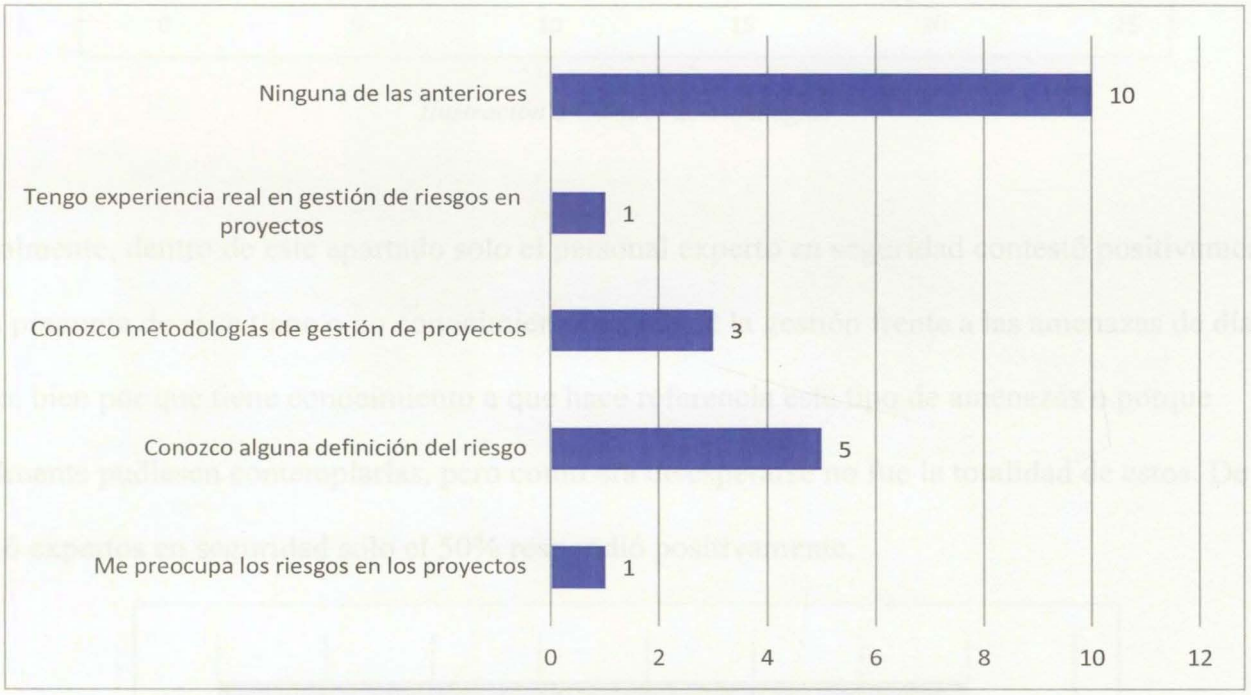

Ilustración 7 Gestión de riesgos en participación de proyectos

Seguido a esto la población encuestada concuerda que debe repensarse la formulación de las estrategias, así como la gestión de los riesgos si se llega a evidenciar un riesgo o amenaza de ciberseguridad no contemplado o que no se este adelantando algún plan de mitigación frente a este, de esta forma este tipo de situaciones influyen en las tomas de decisiones.

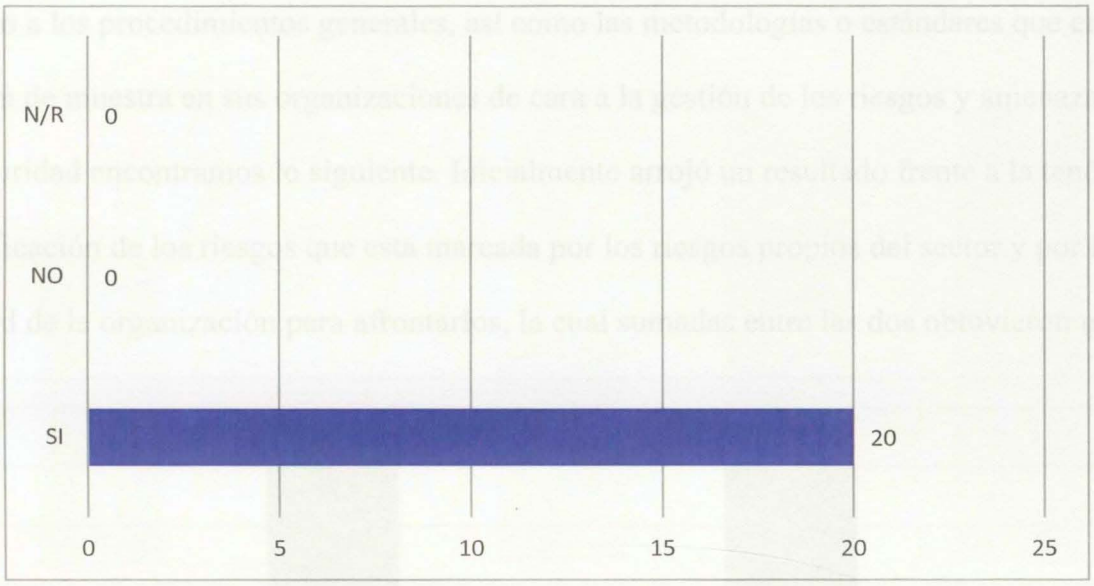

Ilustración 8 Cambio de estrategias

Finalmente, dentro de este apartado solo el personal experto en seguridad contestó positivamente a la pregunta de si se tiene o no conocimiento acerca de la gestión frente a las amenazas de día cero, bien por que tiene conocimiento a que hace referencia este tipo de amenazas o porque realmente pudiesen contemplarlas, pero como era de esperarse no fue la totalidad de estos. De los 6 expertos en seguridad solo el 50% respondió positivamente.

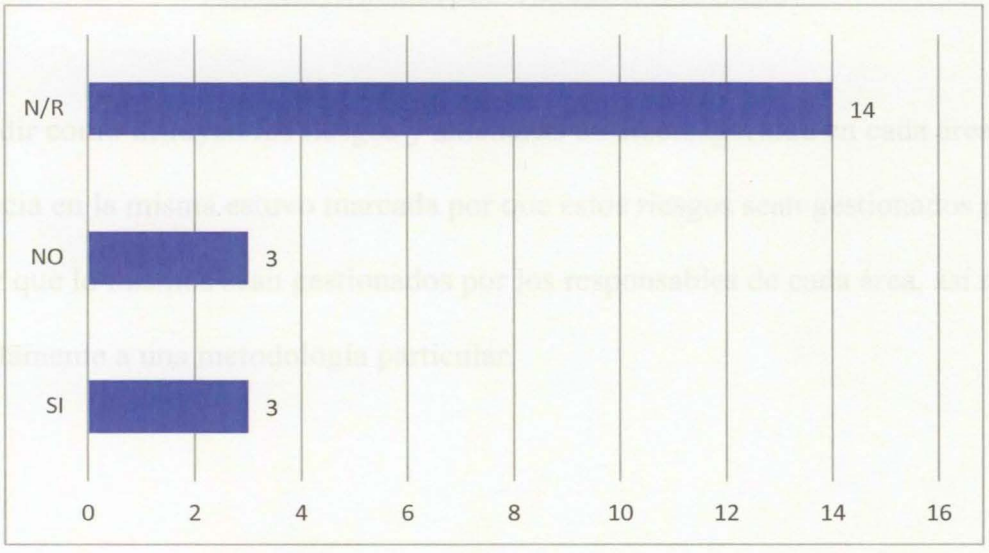

Ilustración 9 Gestión Amenazas Día Cero

En cuanto a los procedimientos generales, así como las metodologías o estándares que emplea la población de muestra en sus organizaciones de cara a la gestión de los riesgos y amenazas de ciberseguridad encontramos lo siguiente. Inicialmente arrojó un resultado frente a la tendencia a la identificación de los riesgos que esta marcada por los riesgos propios del sector y por la capacidad de la organización para afrontarlos, la cual sumadas entre las dos obtuvieron un 80 %.

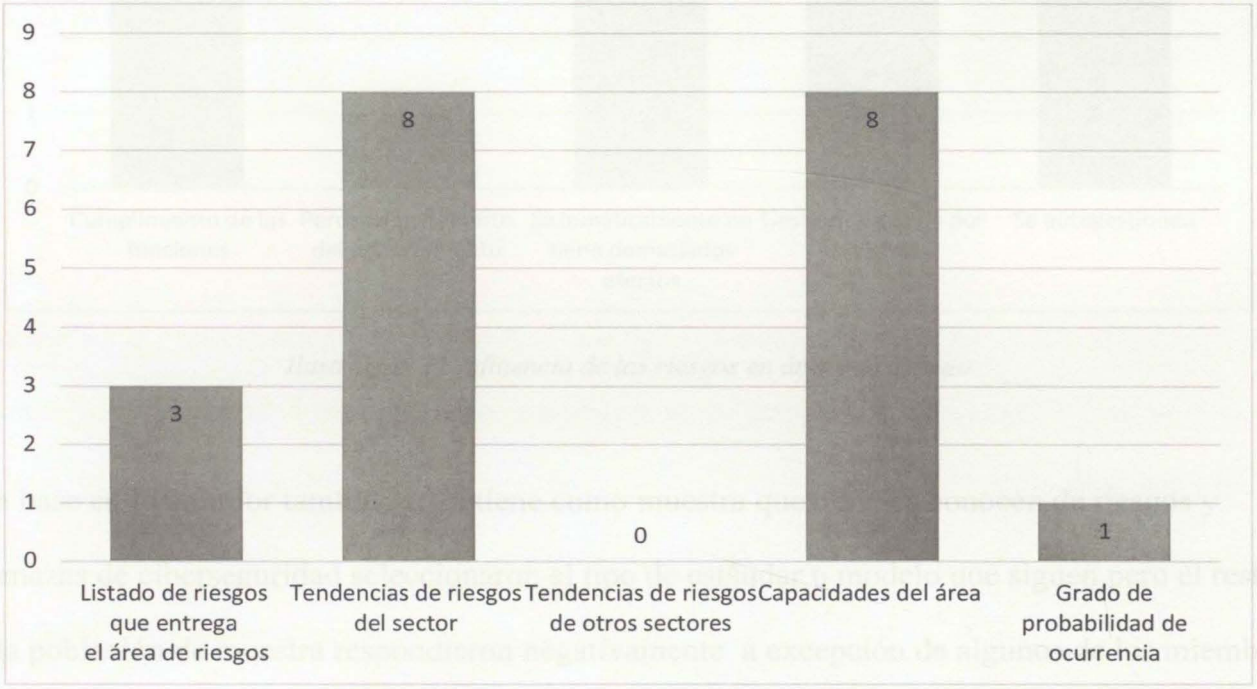

Ilustración 10. Insumos para la identificación de riesgos

Luego al medir como influyen los riesgos y amenazas de ciberseguridad en cada área de acuerdo a la experiencia en la misma estuvo marcada por que estos riesgos sean gestionados por terceros así como por que lo mismos sean gestionados por los responsables de cada área, así no estén atados estrictamente a una metodología particular.

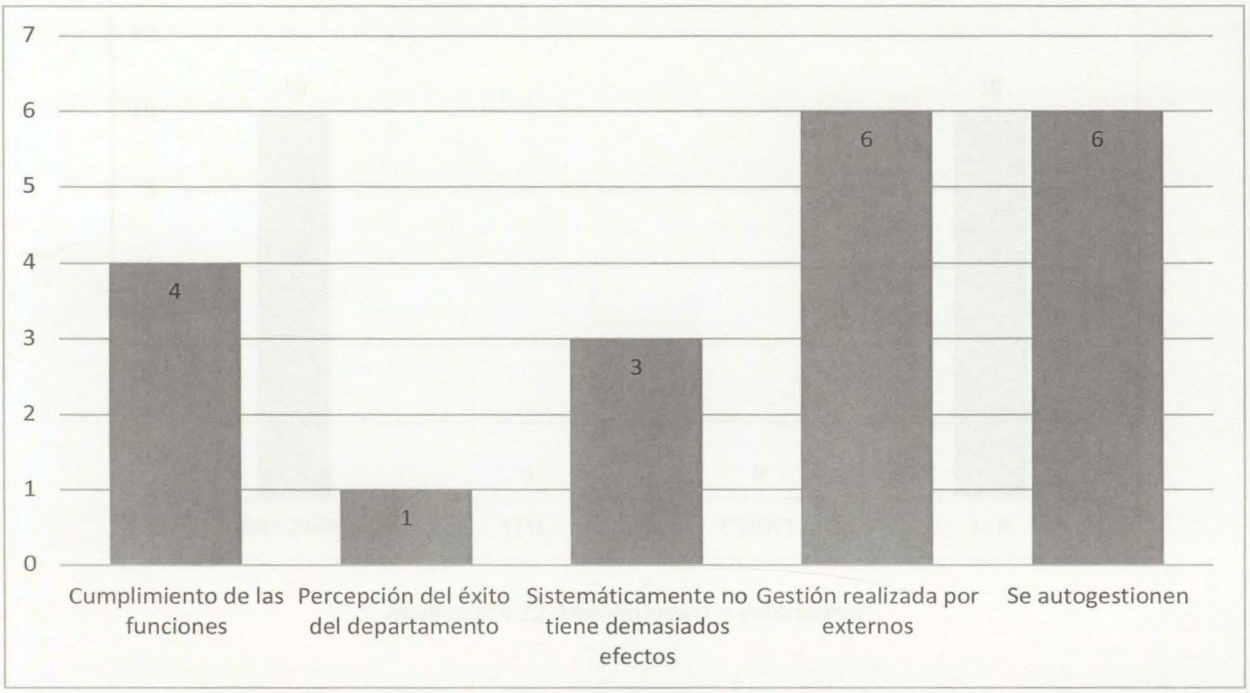

Ilustración 11 Influencia de los riesgos en áreas de trabajo

Con base en lo anterior también se obtiene como muestra que quienes conocen de riesgos y amenazas de ciberseguridad seleccionaron el tipo de estándar o modelo que siguen pero el resto de la población de muestra respondieron negativamente a excepción de algunos de los miembros del departamento de planeación , dejando como resultado un 50 % para la Iso 270005 y el restante no sabe o no responde.

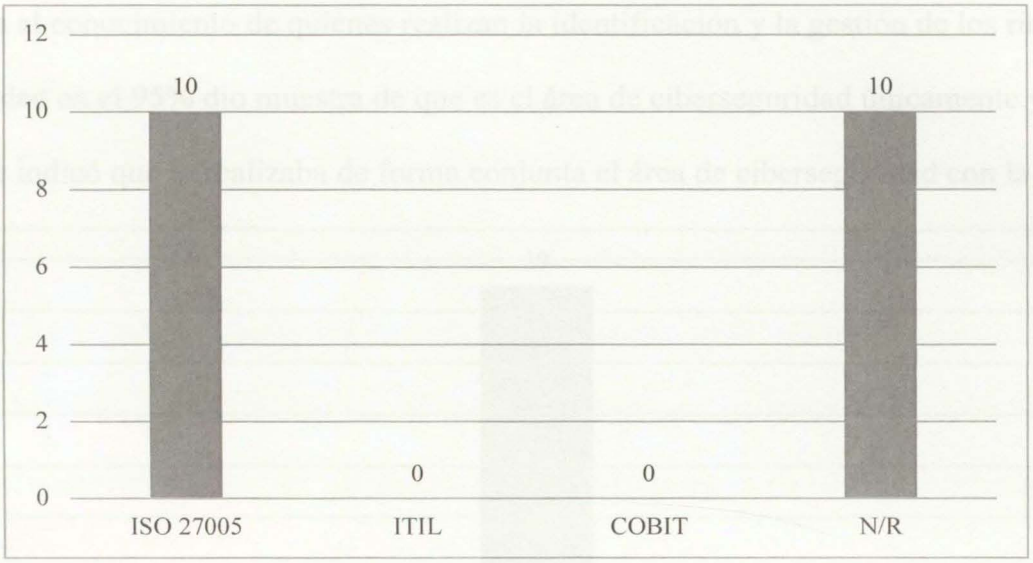

Ilustración 12 Metodologías o estándares

En cuanto a la participación en la identificación de los riesgos y amenazas de ciberseguridad solo los expertos en seguridad respondieron positivamente es decir el 30% de la población de muestra, de las personas diferentes al área de seguridad solo el 10 % participa ocasionalmente y el 20% restante no participa, personal de planeación el 20 % participa, el otro 10% ocasional y finalmente los directivos encuestados no participan.

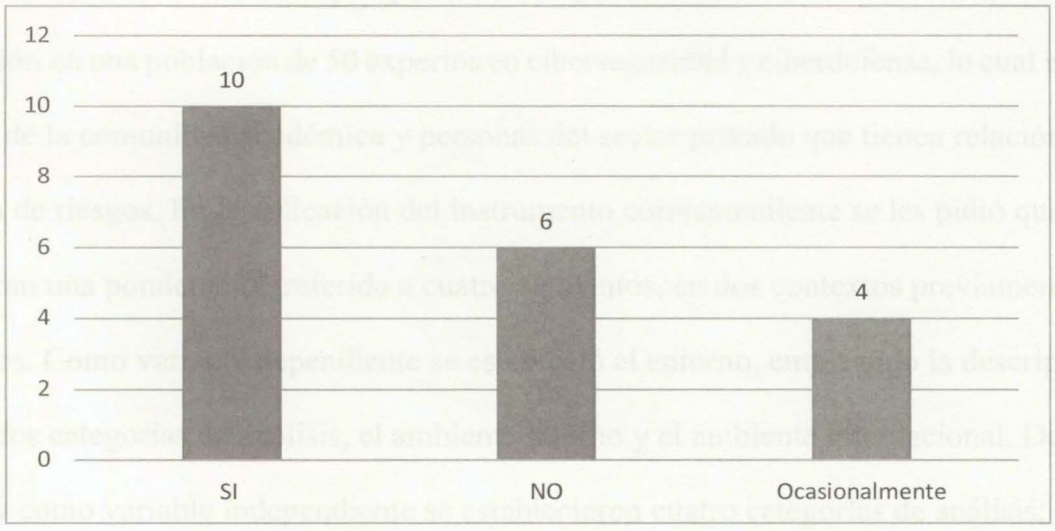

Ilustración 13 Participación identificación riesgos y amenazas ciberseguridad

En cuanto a al conocimiento de quienes realizan la identificación y la gestión de los riesgos de ciberseguridad en el 95% dio muestra de que es el área de ciberseguridad únicamente y solo el 5% restante indicó que lo realizaba de forma conjunta el área de ciberseguridad con la funcional.

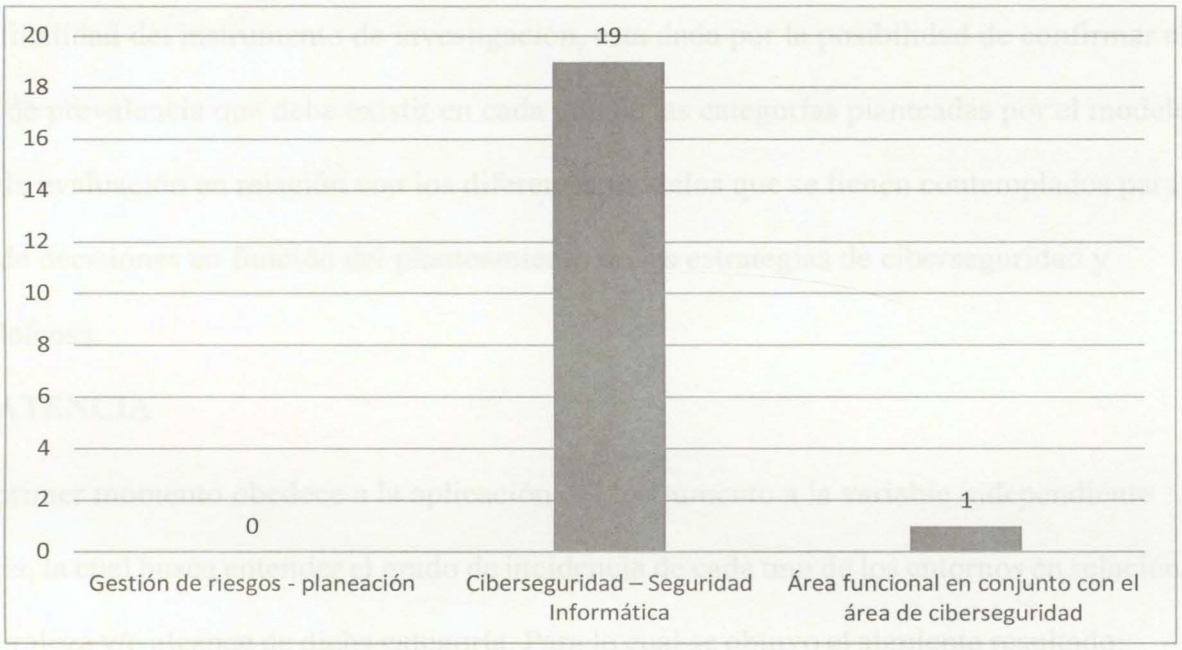

Ilustración 14 Área que realiza la gestión de riesgos y amenazas de la ciberseguridad

Con la finalidad de proporcionar mayores elementos que permitan establecer el alcance de la ponderación del modelo de diseño prospectivo, fue aplicado también un instrumento de investigación en una población de 50 expertos en ciberseguridad y ciberdefensa, lo cual incluyó a miembros de la comunidad académica y personas del sector privado que tienen relación con la mitigación de riesgos. En la aplicación del instrumento correspondiente se les pidió que establecieran una ponderación referida a cuatro elementos, en dos contextos previamente establecidos. Como variable dependiente se estableció el entorno, empleando la descripción mediante dos categorías de análisis, el ambiente interno y el ambiente internacional. De manera adicional y como variable independiente se establecieron cuatro categorías de análisis; a. latencia, b. riesgo o amenaza conocida, c. Riesgo o amenaza focal y d. riesgo o amenaza emergente. Como mecanismo cuantificador se les pidió a los participantes otorgar una valoración

numérica entre 01 y 100, donde 100 obedecía al nivel más alto de preocupación, en función de los mecanismos existentes para la gestión o mitigación de riesgos.

La finalidad del instrumento de investigación, esta dada por la posibilidad de confirmar el orden de prevalencia que debe existir en cada una de las categorías planteadas por el modelo, así como la evaluación en relación con los diferentes modelos que se tienen contemplados para la toma de decisiones en función del planteamiento de las estrategias de ciberseguridad y ciberdefensa.

A. LATENCIA

El primer momento obedece a la aplicación del instrumento a la variable independiente latencia, la cual busca entender el grado de incidencia de cada uno de los entornos en relación con la naturaleza y/o alcance de dicha categoría. Para lo cual se obtuvo el siguiente resultado:

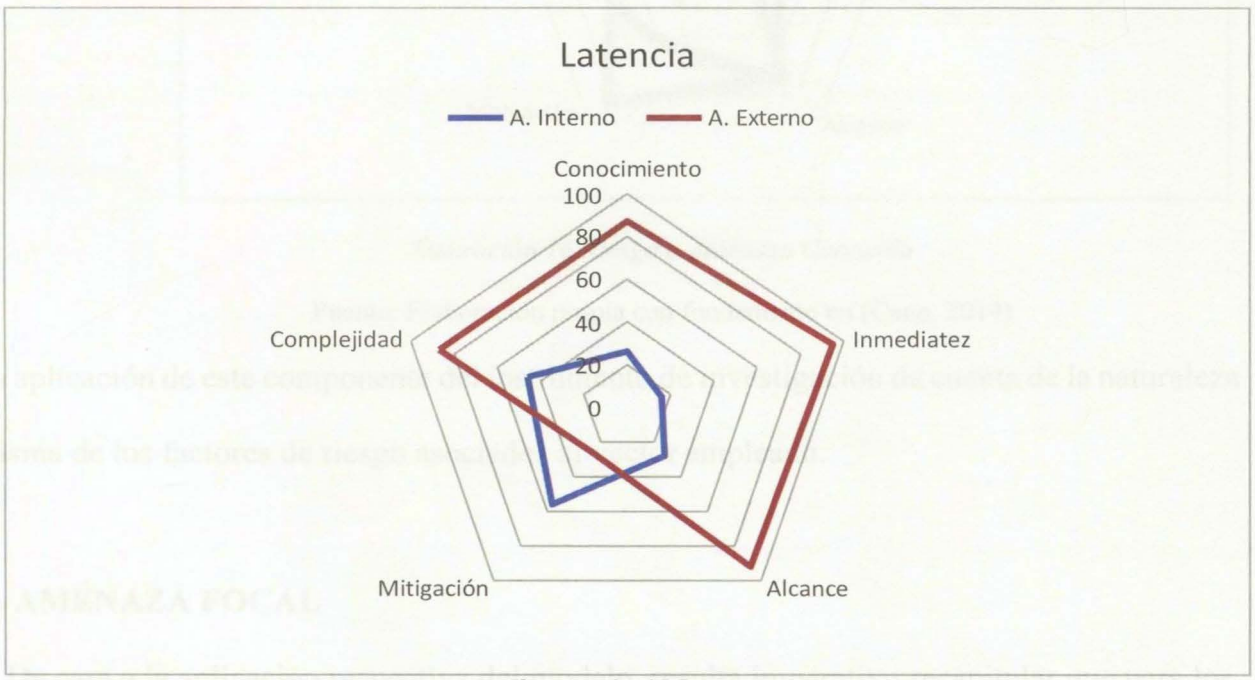

Ilustración 15 Latencia

Fuente: Elaboración propia con fundamento en (Cano, 2014)

B. AMENAZA CONOCIDA

En relación con dicha categoría también fueron aplicados los mismos elementos de ponderación, conocimiento, complejidad, inmediatez, mitigación y alcance, para lo cual fueron adoptados algunos mecanismos de control cualitativos para garantizar la idoneidad del personal seleccionado para la aplicación de la prueba.

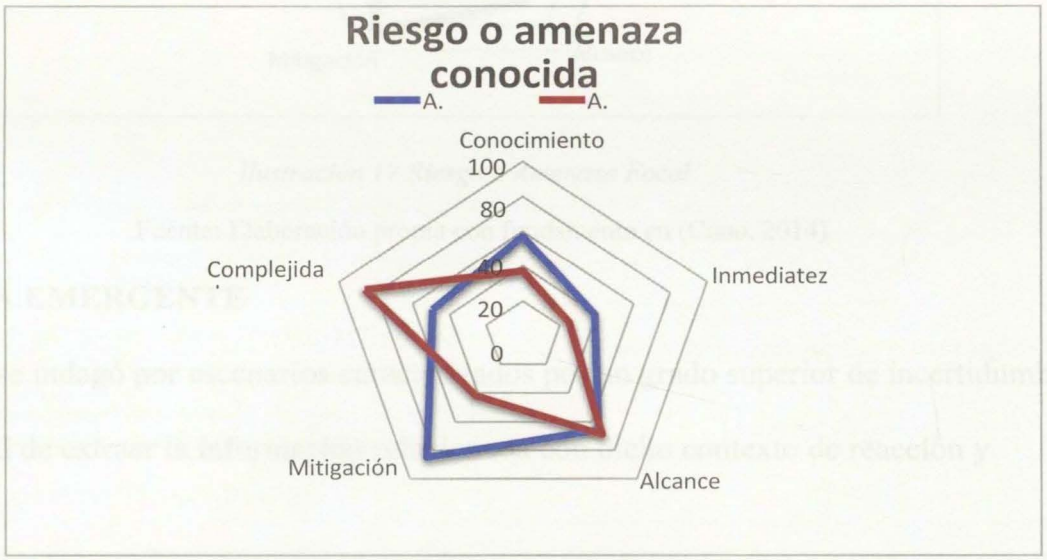

Ilustración 16 Riesgo o Amenaza Conocida

Fuente: Elaboración propia con fundamento en (Cano, 2014)

La aplicación de este componente del instrumento de investigación da cuenta de la naturaleza misma de los factores de riesgo asociados al vector empleado.

C. AMENAZA FOCAL

De cara a la aplicación respectiva del modelo, resulta imperativo recapitular que para los efectos planteados en el modelo de análisis, por amenaza focal se entiende aquella de la que se

tiene información siquiera sumaria, pero que tiene la capacidad de afectar o bien la infraestructura crítica o bien los intereses estratégicamente tutelados. Fueron utilizadas las mismas variables y preguntas para determinar su impacto.

Ilustración 17 Riesgo o Amenaza Focal

Fuente: Elaboración propia con fundamento en (Cano, 2014)

D. AMENAZA EMERGENTE

Finalmente se indagó por escenarios caracterizados por un grado superior de incertidumbre, con la finalidad de extraer la información relacionada con dicho contexto de reacción y mitigación.

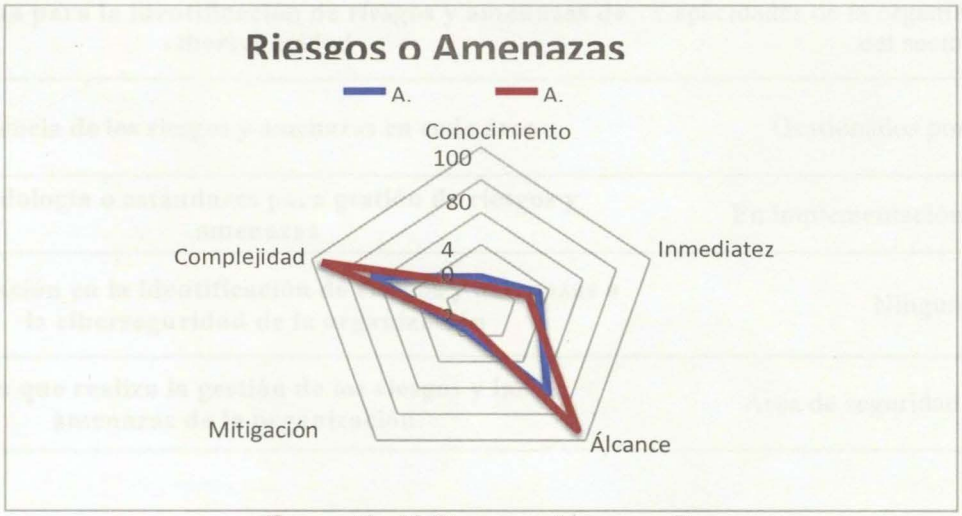

Ilustración 18 Riesgos o Amenazas Emergentes

Fuente: Elaboración propia con fundamento en (Cano, 2014)

3.3 APLICACIÓN DEL MODELO

A continuación, se presenta la primera aplicación del modelo propuesto. Esta aplicación se dio con uno de los directivos de las empresas del sector financiero definidas en la muestra la cual hace parte de las pymes del país y que permite al modelo propuesto una posterior implementación, comprobación y maduración en un segmento amplio de organizaciones. Por practicidad, se hará referencia a la empresa en estudio como D1. Se elabora la ficha de caracterización de la organización de acuerdo con la siguiente tabla.

Tabla 3. Caracterización y estado

Aspecto	Descripción
Antigüedad en la Empresa	Mas 2 años e inferior a 5 años.
Mercado	Financiero.
Conocimiento en riesgos y amenazas en ciberseguridad	NO.
Percepción de la gestión de riesgos y amenazas en ciberseguridad.	Positiva
Gestión de riesgos y amenazas de ciberseguridad en los proyectos	Delegado al área de Seguridad Informática.
Postura frente a identificación de riesgos y amenazas no identificados de forma lineal.	Tomador de decisiones
Gestión y conocimiento de amenazas de Día cero	Ninguno
Tendencia para la identificación de riesgos y amenazas de ciberseguridad	Capacidades de la organización y tendencias del sector.
Influencia de los riesgos y amenazas en cada área	Gestionados por terceros
Metodología o estándares para gestión de riesgos y amenazas	En implementación ISO 270005
Participación en la identificación de riesgos y amenazas a la ciberseguridad de la organización	Ninguna
Área que realiza la gestión de los riesgos y las amenazas de la organización.	Área de seguridad informática

3.3.1 Aplicación del modelo en campo

En la figura a continuación se muestra el plan adelantado para la aplicación del modelo en D1, el cual contemplo las siguientes fases:

1. Apoyado en el diagnóstico a través de la encuesta, se identificaron las brechas existentes en la identificación de los riesgos y amenazas de ciberseguridad entre el área planeación, el área de ciberseguridad y las demás áreas de la organización.
2. Se socializó y contextualizó al equipo de trabajo en D1 a través de video conferencia sobre el alcance del modelo propuesto y el detalle de los diferentes componentes integrales del mismo.
3. Se seleccionaron dos áreas de la organización para que realizaran la aplicación del modelo diligenciando cada uno de los componentes de este.
4. Socialización del modelo diligenciado
5. Aprendizajes

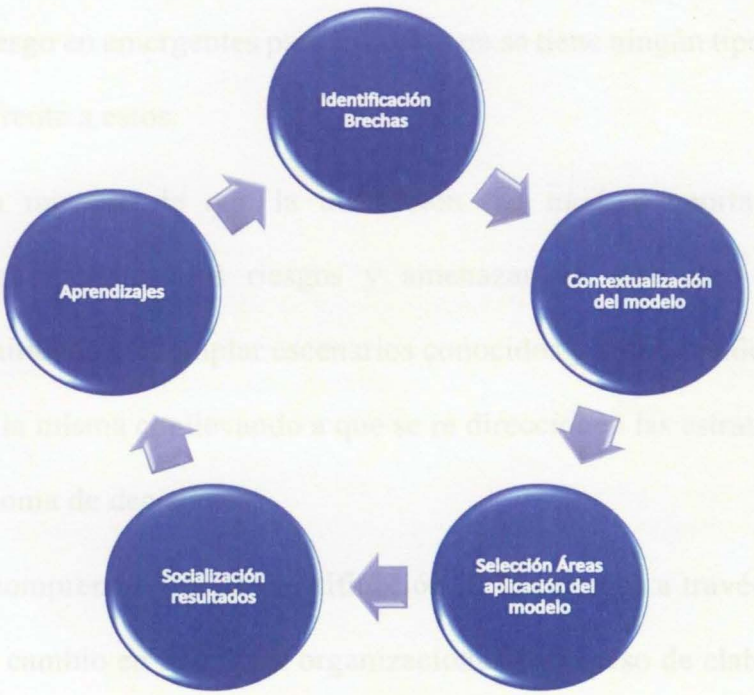

Ilustración 19. Plan Implementación

3.3.1.1 Captura y análisis de los datos de salida del modelo aplicado

En referencia a la información registrada durante el periodo de implementación del modelo en sus diferentes componentes se obtuvo lo siguiente:

En la matriz de riesgos de la entidad realizada a comienzo del año en cuanto a riesgos y amenazas en ciberseguridad, se logro identificar que gran parte de estos se encuentra en el campo de los conocidos, es decir aquellos para los cuales la organización cuenta con un plan o al menos tareas especificas orientadas al control de la no materialización de estos.

Se identificaron 3 riesgos en el campo de los focalizados bajo los cuales D1, conoce de estos porque se presentan en su sector y tiene planes de mitigación mas no controles, pero es posible que el entorno no los conozca ya que se presentan específicamente de acuerdo al nicho de la organización. Sin embargo, esta organización da muestra que no contaba con planes de mitigación para 1 de estos.

Se identificaron 3 riesgo en emergentes para lo cuales no se tiene ningún tipo de plan de mitigación o de acción alguna frente a estos.

Los resultados dan muestra de que la utilización del modelo aporta adecuadamente a la planificación y seguimiento a los riesgos y amenazas en este caso con respecto a al a ciberseguridad permitiendo contemplar escenarios conocidos y desconocidos por parte de algunos de los miembros de la misma conllevando a que se re direccionen las estrategias o hayan cambios en el proceso de la toma de decisiones.

El personal de D1 comprendió que la identificación de los riesgos a través del modelo de forma preactiva genera un cambio en la cultura organizacional el proceso de elaboración de estos así la generación de un pensamiento fuera de la línea común en la que se desarrolla.

El modelo es un documento dinámico que debe ser actualizado y gestionado periódicamente para que este proceso deje de realizarse de forma estática.

También este ejercicio de aplicación permitió la observación que durante la identificación de los riesgos hay deficiencias en los miembros de D1 para la definición apropiada de un riesgo y se confundían con causas o con consecuencias.

La aplicación de modelo permitió al directivo de esta organización en conjunto con el área de planeación a redireccionar y replantear su matriz de riesgos. Así mismo en la video conferencia del aprendizaje manifestó que la situación de la pandemia lo ha llevado a que gran parte de su equipo de trabajo desarrolle sus funciones desde casa, de esta manera están accediendo desde sus computadores y equipos móviles en donde como amenaza emergente se identificó malware en estos últimos, de esta manera planteo la posibilidad de realizar inversión para la adquisición de antivirus para que se sean distribuidos a sus empleados y de esta forma dar inicio a acciones frente a este tipo de amenazas.

Primer nivel de análisis	Información Conocida	Información desconocida
Entorno conocido	• Errores de los usuarios • Intrusión de software malicioso • Ataques de virus • Ataques al sitio web • Acceso no autorizado	• Ciber Terrorismo • Denegación de servicios • Cryptomalware (IA). • Ataques de día Zero
Entorno desconocido	• Phishing dirigido • Ataques Coordinado • **USB Driverby**	• **Malware Móviles** • **Inteligencia Artificial** • **IOT**

3.3.2 APRECIACIONES APLICACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN

Pudo advertirse de cara a los resultados obtenidos por cuenta de la aplicación del instrumento de investigación correspondiente a viabilizar las categorías de análisis del modelo de análisis planteado, que existe una relación de variabilidad independiente en relación con el nivel de conocimiento, tanto de la amenaza o riesgo, como de los mecanismos disponibles de mitigación. En general, existe un mayor de riesgo asociados al entorno externo en relación tanto con la inmediatez, el alcance y las posibilidades de mitigación, circunstancia que toma una dirección distinta al momento de evaluar el entorno o contexto interno en función de los riesgos o amenazas disponibles bajo cada una de las categorías -Latencia, amenaza conocida, amenaza focal o amenaza emergente-. En dicho orden de ideas, es pertinente destacar la coherencia de las variables independientes seleccionadas, tanto para el instrumento de investigación, como al momento de delimitar las variables respectivas al modelo de análisis. Así las cosas, resulta imperativo que pueda integrarse el modelo planteado, como complemento al modelo racional en la toma de decisiones estratégicas para la mitigación de riesgos o amenazas derivadas del ciberespacio, pues solo así se podrá establecer en un sentido técnico, cuales son las herramientas más eficientes al momento de establecer escenarios de respuesta a incidentes y que las mismas no correspondan a versiones integristas o reduccionistas que se basen en criterios de ponderación de corte subjetivo.

La tecnología y sus diferentes manifestaciones tienen el potencial de igualar las capacidades de actores no estatales en su intento por generar afectaciones graves a la infraestructura de los Estados o afectar el cumplimiento de los objetivos o intereses nacionales, circunstancia que implica la obligación para los Estados y sus cuerpos de seguridad, en relación con el incremento de las capacidades de prevención, detención, investigación y respuesta a las amenazas o riesgos

que puedan provenir del ciberespacio.

Debido a esta especial característica del marco de riesgos y amenazas en los cuales se ven inmersos los Estados en su relación con el ciberespacio, resulta deseable la generación de procesos de anticipación estratégica por medio de las metodologías planteadas, que al facilitar los procesos de recopilación de la información disponible, así la generación de escenarios de respuesta, permitan la consolidación de estrategias de ciberseguridad que tengan capacidad de contrarrestar o mitigar eficazmente cualquier de los fenómenos reseñados.

En dicho orden de ideas, la apropiación de la metodología presentada para la elección de herramientas preactivas de defensa, corresponde a un insumo a considerar al momento de plantear estrategias nacionales de seguridad nacional, manteniendo siempre a la vista que las mismas corresponden tan solo a uno de los elementos (Medios) en el marco general de la ecuación estratégica $[E = F + M + m + EA + e]$[1], pero que sin lugar a dudas deben armonizarse para el adecuado cumplimiento de los objetivos.

[1] Estrategia = Fines + Medios + Modos + Estrategia del Adversario + Entorno

CONCLUSIONES

Una tarea inherente de las Fuerzas Militares es desarrollar un sistema de defensa que mantenga la seguridad nacional, que ofrezca a los ciudadanos bienestar y una mejor calidad de vida, esta seguridad debe estar presente en todos los campos, terrestre, aéreo, marítimo y espacial, aunado a los anteriores ahora corresponde velar por la seguridad en el ciberespacio. Colombia debe prepararse en conjunto con los sectores civiles y armados para atender una amenaza latente denominada *ciberguerra,* de lo contrario no solo seremos testigos, sino también víctimas del uso de las TIC bajo el concepto de *ciberataques* debilitando las instituciones y las empresas que movilizan la economía nacional.

Entendiendo que el ciberespacio corresponde a un bien público de carácter universal, que ofrece un sinfín de posibilidades de interconexión, de simplificación de procedimientos y en general, que redunda en impactos positivos para los Estados, se puede entender la constante transición que se ha efectuado en las últimas décadas en términos de depositar mayores activos estratégicos en su esfera de influencia, lo que inherentemente obliga a que los Estados y sus fuerzas de seguridad, aborden y apropien nuevas manera de diseñar las estratégicas de seguridad, lo anterior partiendo de la premisa de entender el ciberespacio como un activo/recurso que desarrolla los intereses nacionales y, en consecuencia, susceptible de ser protegido con todas las capacidades institucionales.

En los conflictos actuales los enfrentamientos se presentan en escenarios poco habituales, con contendores asimétricos que emplean espacios, medios y técnicas no convencionales, viéndose esto con más frecuencia en los procedimientos empleados por los

terroristas, dentro de ese extenso abanico de escenarios está el *ciberespacio* lugar donde interactúan infinidad de organizaciones y de instituciones como los Estados, convirtiendo este escenario en el campo de batalla del futuro inmediato.

En consideración a lo anterior, resulta imprescindible establecer y adoptar mecanismos de análisis que faciliten la anticipación estratégica de cara a la constante interacción de riesgos y amenazas en relación con la infraestructura crítica, así como de aquellos activos estratégicos que deban ser resguardados por parte de los cuerpos de seguridad del Estado.

La ciberseguridad debe abordarse de manera tal que involucre a las diferentes agencias de seguridad e inteligencia del Estado, los centros de investigación públicos y privados y al sector empresarial. La ciberseguridad no debe limitarse a acciones preventivas y pasivas sino también a acciones ofensivas, razón por la cual es necesario generar doctrina orientada en el tema de la ciberseguridad, que procure la defensa de la Nación en el ciberespacio ante una amenaza cada vez más capaz y peligrosa, posteriormente alcanzar la operatividad necesaria, teniendo claro que las Fuerzas Armadas, tarde o temprano incursionaran en el ámbito del ciberespacio para desarrollar sus operaciones.

El concepto de seguridad es base fundamental para el desarrollo de un país, aportando la estabilidad necesaria para que el sistema económico sea productivo, por lo tanto en el escenario de la economía digital se aplica de la misma manera este fundamento, todos los procedimientos y movimientos que se lleven a cabo en la red, requieren la seguridad necesaria para que los usuarios puedan desenvolverse con tranquilidad. La política de Ciberseguridad y Ciberdefensa

adoptada por Colombia debe ser complementada para responder adecuadamente a los nuevos tipos de incertidumbres e incidentes digitales, los cuales son el resultado de un entorno digital creciente y dinámico. Incidentes que pueden afectar a cualquier sector de la economía o ciudadano, y no solo al Estado; y que, según diversos estudios, deben ser abordados desde un enfoque de riesgos en el que se involucren a todas las partes, lo cual implica, en consonancia con lo que ha sido presentado por el presente documento, la asunción de la heterocomposición del concepto de seguridad, así como sus estrategias construcción de capacidades de mitigación.

No se contempla a cabalidad el ciberespacio como un quinto teatro de operaciones de las Fuerzas Militares, que permita planear, prever y contrarrestar los ataques que son de naturaleza cibernética, limitándose a considerar únicamente las amenazas delincuenciales de grupos armados al margen de la ley, en su capacidad de armas tradicionales que buscan afectar el cumplimiento de la misión constitucional de las Fuerzas Militares para lo cual dentro de su organización interna cuenta con unidades operativas, tácticas y fundamentales que deben considerar dentro de los teatros de operaciones el ciberespacio.

Ahora bien, la falta de conciencia de los funcionarios de las FF.MM. frente a la existencia y evolución de los métodos de ataque en ciberseguridad, dejando dicha responsabilidad únicamente a los que intervienen directamente en la administración de los recursos informáticos y de comunicaciones, representa uno de los primeros desafíos al momento de planear las condiciones de seguridad y respuesta frente a incidentes. Esto conlleva a que no solo se deban aplicar nuevos modelos de análisis al momento de determinar las mejores rutas de actuación, también implica la incorporación de mecanismos que estén encaminados a desarrollar cambios

culturales en las organizaciones, en relación con la administración de los riesgos en el ciberespacio.

No debe perderse de vista que los vectores de ataque son mutantes en el tiempo y requieren de estudios permanentes con personal especializado que permitan crear estrategias para contrarrestar con mejores prácticas la amenaza de estos. Como conclusión general de la presente tesis se puede establecer que los objetivos estratégicos de las FF.MM. de Colombia están constantemente amenazados por múltiples vectores que son la entrada de diferentes formas de ataque a la infraestructura crítica digital, poniendo en riesgo la capacidad de defensa y seguridad Nacional del Estado Colombiano, pasando de tener una actitud preventiva y reactiva a una ciberseguridad operacional y estratégica que emplee herramientas de defensa preactivas que puedan contrarrestarlas cabalmente.

En consecuencia, y en relación con la posibilidad de generar procesos de anticipación estratégica, debe estudiarse la posibilidad de involucrar el modelo de análisis desarrollado, con la finalidad de construir capacidades en función de las herramientas preactivas de defensa, de forma tal que tanto la infraestructura crítica como los activos estratégicos del Estado colombiano puedan encontrarse a salvaguarda de cualquier riesgo y/o amenaza interna o externa.

De manera adicional, y fruto de los evidenciado en desarrollo de la presente investigación, resulta fundamental que las modificaciones orgánicas, doctrinales y procedimentales se lleven a cabo de manera sistemática, toda vez que existe cierta percepción de tranquilidad en relación con el nivel de seguridad de la infraestructura crítica digital del Estado colombiano, ya que si bien es cierto que a la fecha no se han presentado incidentes masivos que constituyan una afectación grave a los recursos estratégicos digitales, no se debe constituir esta situación en óbice para el abandono frente al planeamiento o simulación de situaciones de crisis de manera constante.

En dicho orden de ideas, la ponderación frente a la información disponible de cara a la naturaleza de los riesgos, el nivel de la amenaza, las posibilidades de terminar en procesos de convergencia con otros fenómenos, y el poder potencial de la misma, constituye una tarea permanente que debe ser desarrollada por personal altamente cualificado, que pueda generar la capacidad de esbozar lecturas frente al entorno y frente a las condiciones de seguridad, para la adecuada mitigación de los riesgos. La aplicación del modelo de prospectiva preactiva en defensa, mas que limitarse al cumplimiento de una lista de verificación, tiene la capacidad de modificar la cultural organizacional al interior de las FF.MM. y otros organismos de seguridad del Estado, privilegiando los procesos de anticipación estratégica, en función de la generación de múltiples escenarios situacionales que garanticen el dominio de pleno espectro.

No obstante, se abre la puerta a que futuros desarrollos puedan incluir nuevas variables o niveles de análisis que puedan ser considerados en los procesos de análisis de los riesgos o amenazas y sus posibilidades de mitigación, lo anterior partiendo de la premisa que ha sido desarrollada a lo largo de la investigación y que toma mayor auge con cada día que pasa y que consiste en la celeridad, imprevisibilidad, contundencia y aleatoriedad que desarrollan las amenazas que tienen como objetivo socavar las condiciones de seguridad en el ciberespacio.

El Estado Final Deseado -EFD- debe consistir en un modelo integral que pueda responder a cualquier tipo de amenaza a la infraestructura crítica digital del Estado colombiano.

REFERENCIAS

Baker, E. (2014). "A model for the impact of cybersecurity infrastructure on economic development in emerging economies: evaluating the contrasting cases of India and Pakistan. Information Technology for Development". [S.l], v. 20, n. 2, págs. 122- 139.

Bejarano, M. (2011). Alcance y ámbito de la seguridad nacional en el ciberespacio". En: Cuaderno de Estrategia, No. 149, IEEE, febrero de 2011.

Camps, P. (2016). "Ciberdefensa y ciberseguridad: Nuevas amenazas a la Seguridad Nacional, estructuras nacionales de ciberdefensa, estrategias de ciberseguridad y cooperación interagencias en este ámbito". Consulta realizada el 25 de mayo de 2017. Disponible en: www.calen.gub.uy/pdf/investigacion/2016-1-Ciberseguridad- Camps.pdf

Cancelado, H. (2010). "La seguridad internacional frente a las amenazas globales contemporáneas". En: Análisis Político, Nº 68, Bogotá, enero-abril, 2010, págs. 91-100.

Cano, J. (2014). La ventana de AREM. Una herramienta estratégica y táctica para visualizar la incertidumbre. RECSI.

Clarke, R. & Knake, R. (2011). Guerra en la red, los nuevos campos de batalla. Barcelona: Editorial Planeta.

Cerezuela Gil, José, General de Brigada. (1992). Ejército de España. Military Review. Guerra Electrónica.

Chifofsky, E. J y Cross, E. (1990). ii, Reverse Engineering and Desing Recovery: A

Taxonomy, IEEE Software. Pag. 13-17

CITEC (2010) Historia CITEC. Documento archivo sección operaciones CITEC.

Consejo Nacional de Política Económica y Social. (2011). "POLÍTICA NACIONAL DE SEGURIDAD DIGITAL". Consejo Nacional de Política Económica y Social N° 2854. Bogotá.

Consejo Nacional de Política Económica y Social. (2016). "POLÍTICA NACIONAL DE SEGURIDAD DIGITAL". Consejo Nacional de Política Económica y Social. Bogotá.

Cubeiro, E. (2016). "Ciberdefensa". En: Díaz, A. (Ed.). Conceptos fundamentales de inteligencia. Valencia: Tirant lo Blanch.

Departamento de Defensa -DoD -. Estados Unidos FM 34-1 (1994). Manual de operaciones de inteligencia y guerra electrónica, inteligencia de señales.

Departamento Nacional de Planeación. (2011) Lineamientos de Política para Ciberseguridad y Ciberdefensa. Consejo Nacional de Política Económica y Social. N° 3701. Bogotá D.C., 14 de julio de 2011.

Departamento Nacional de Planeación (2014). "Bases del Plan Nacional de Desarrollo 2014-2018: todos por un nuevo país". Bogotá, D.C., 2014. Consulta realizada en febrero de 2016. Disponible en: https://colaboracion.dnp.gov.co

Department of the army. FM 3-36-1. (2012). Electronic Warfare. Recuperado de http://hosted.ap.org/specials/interactives/_documents/electronic_warfare.pdf

Ejército Nacional de Colombia. (2007). Manual de inteligencia técnica en operaciones militares. EJC, 2. 19.

Ejército Nacional de Colombia. (2010). Manual de inteligencia técnica en operaciones militares irregulares. Sin publicar.

Escuela Superior de Ingenieros de Telecomunicaciones. (2013). "Seguridad Nacional y Ciberdefensa aproximación conceptual: ciberseguridad y Ciberdefensa". Conferencia en la UPM- Escuela Superior de Ingenieros de Telecomunicaciones. Madrid.

Feliu, L. (2012). "La ciberdefensa y la ciberseguridad". En: Ministerio de Defensa de España. El Ciberespacio. Nuevo escenario de confrontación. España: Imprenta del Ministerio de Defensa.

Gaitán, A. (2016). "La ciberguerra y sus generaciones: un enfoque para comprender la incidencia de las TICS en la guerra regular. ESDEGUE LIBROS. Bogotá D.C.

Gordon, R. Sullivan y Michael V. Harper. (2009). La esperanza no es un método. Bogotá, D. C.: Editorial Norma.

Instituto Español de Estudios Estratégicos. (2010). "Ciberseguridad, retos y amenazas a la seguridad nacional en el ciberespacio". Instituto Español de Estudios Estratégicos, cuaderno de estrategia N° 149, Madrid.

Jordan, M. & Torres, M. (2007). "Internet y actividades terroristas: El caso del 11-M. En "El profesional de la información; Vol 16, Núm. 2.

Kissinger, H. (2016). "Orden mundial: Reflexiones sobre el carácter de las naciones y el curso de la historia". [S.l.]: Debate. 2016

Laborie, M. (2013). "La estrategia de Seguridad Nacional". Instituto Español de Estudios

Estratégicos – IEEE-. Documento de Análisis No. 034/2013.

Laqueur, W. (2015). "La guerra cibernética". Vanguardia Dossier, [S.l.], No. 54.

Lewis, J. (2002). "Assessing the risks of cyber terrorism, cyber war and other cyber threats". Center for Strategic and International Studies, diciembre de 2002.

Llongueras, A. (2013). La guerra inexistente, la ciberguerra. Madrid: Eae Editorial Acad MIA Espa Ola.

McAfee Labs (2011). "McAfee threats report: fourth quarter 2011". Santa Clara, CA, 2012. Consulta realizada en marzo de 2016. Disponible en: http://www.intel.com

Ministerio de Defensa Español. (2009) La guerra electrónica en España. Instituto Español de Estudios Estratégicos – IEEE-.

Ministerio de Defensa Nacional. (2011). POLÍTICA INTEGRAL DE SEGURIDAD Y DEFENSA PARA LA PROSPERIDAD, PISDP Ministerio de Defensa Nacional República de Colombia. Bogotá.

Organisation for Economic Co-operation and Development (2015). "Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document". Paris: OECD. Consulta realizada el 24 de mayo de 2016. Disponible en: http://www.oecd.org/sti/ieconomy/digital-security-riskmanagement.pdf

OTAN – Organización para el Tratado del Atlantico Norte-. (2008). "NATO Review – Cumbre de Bucarest". En NATO.

Portafolio, (2016). "Para el país, la seguridad digital es una política nacional". En:

Portafolio.com. Consulta realizada en julio de 2017. Disponible en: http://www.portafolio.co/economia/gobierno/conpes-aprobo-nueva-politica- seguridad-digital-colombia-494057

Sánchez, M. & Jones, S. (2016). "Lineamientos de Política en ciberseguridad y ciberdefensa: Logrando la Seguridad y Defensa de Colombia en un Mundo Digital". En: J. Rodrigues (Ed.), Ciberdefesa e Cibersegurança: Novas Ameaças à Segurança Nacional (págs. 81-94). Rio de Janerio: ESG.

Sancho, C. (2016). "Ciberespacio bien público mundial en tiempos de globalización: Política Pública de ciberseguridad una necesidad imperiosa y la ciberdefensa como desafío del siglo XXI". En: J. Rodrigues (Ed.), Ciberdefesa e Cibersegurança: Novas Ameaças à Segurança Nacional (págs. 42-74). Rio de Janerio: ESG.

Servitja Roca, Xavier. (2013) Ciberseguridad, Contrainteligencia y Operaciones Encubiertas en el Programa Nuclear de Irán: de la neutralización selectiva de objetivos al "Cuerpo Ciber" IRANÍ. Recuperado de http://www.ieee.es/Galerias/fichero/docs_opinion/2013/DIEEEO42-2013_Inteligencia_Iran_XSertvija.pdf

Superintendencia Financiera de Colombia (2015). "Informe de operaciones: Primer semestre de 2015". [S.l.]. Consulta realizada el 25 de abril de 2017. Disponible en: https://www.superfinanciera.gov.co

Touré, H. (2013). ITU Global Security Agenda (GCA). A framework for international cooperation in Cybersecurity. International Telecommunication Union.

Theiler, O. (2011). "Nuevas amenazas: el ciberespacio". Revista de la OTAN (edición digital). Consulta realizada el 27 de julio de 2017. Disponible en: http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/ES/index.htm

Torres, A. (2011). Cooperación Policial en la Unión Europea: la necesidad de un modelo de inteligencia criminal eficiente. [S.l.]: Editorial Dikinson.

-UIT- Union Internacional de Telecomunicaciones. (2007). "El escenario de la ciberseguridad y los procesos de corresponsabilidad". UIT.

Vargas, E. (2014). Ciberseguridad y Ciberdefensa: ¿Qué implicaciones tienen para la Seguridad Nacional? (Tesis de pregrado). Universidad Militar Nueva Granada. Bogotá.

Vásquez. E. (2016). "Proteger la infraestructura crítica, una tarea fundamental en ciberseguridad nacional". Consulta realizada el 21 de julio de 2017. Disponible en: https://securingtomorrow.mcafee.com

García, G (2018). "La ventana de Johari: cómo conocer tu negocio para mejorarlo"

Cardona, O (2018) La necesidad de repensar de manera holística los conceptos de vulnerabilidad y riesgo. Universidad de los Andes

Castaño , J (2019) Ciberseguridad: una oportunidad de crecimiento que nos desafía hacia una adecuada gestión del riesgo.

Henao, Jaramillo (2015) LA PROSPECTIVA EN COLOMBIA, un relato de esperanza-acción con altibajos.

ANEXOS

Tabulación instrumento de ponderación de variables – Modelo de Análisis Prospectivo

INSTRUMENTO DE PONDERACIÓN

TITULO	**Herramientas preactivas de defensa y su incidencia en la ciberseguridad**
Tamaño de la muestra	**50 personas**
Método de selección	**Aleatorio por especialidad**
Modo de aplicación	**Virtual mediante SharePoint**

1. Entendiendo que la latencia es una condición en la cual una organización o Estado cuenta con información respecto a un riesgo o amenaza, pero no cuenta con planes o estrategias de respuesta para su mitigación. Esta categoría implica un amplio conocimiento de las capacidades pero un bajo conocimiento del entorno o vectores de amenaza. Establezca una ponderación numérica en un rango entre 01 y 100 a los siguientes indicadores:
    - **a.** Conocimiento
    - **b.** Complejidad
    - **c.** Inmediatez
    - **d.** Mitigación
    - **e.** Alcance
2. Entendiendo las amenazas conocidas como aquella condición o categoría de análisis deseada, se cuenta con amplia y verificable información sobre el riesgo o amenaza, también se cuentan con planes o estrategias de mitigación. Respecto al conocimiento de las capacidades y los componentes del vector de amenaza existe una adecuada correlación. Establezca una ponderación numérica en un rango entre 01 y 100 a los siguientes indicadores:
    - **a.** Conocimiento
    - **b.** Complejidad
    - **c.** Inmediatez
    - **d.** Mitigación
    - **e.** Alcance
3. Entendiendo las amenazas focales como la determinación y materialización del riesgo o amenaza en determinado sector o campo de acción del Estado, implica un estudio fenomenológico relativo a las consecuencias evidenciadas de la amenaza. Esta categoría está definida por la existencia de planes marco de respuesta, pero presenta importantes carencias en lo que refiere a componentes específicos de estrategia que permitan su mitigación. Implica la materialización de la tipología relacionada con la reactividad defensiva. Establezca una ponderación numérica en

un rango entre 01 y 100 a los siguientes indicadores:

a. Conocimiento
b. Complejidad
c. Inmediatez

   d. Mitigación
   e. Alcance

4. Entendiendo las amenazas emergentes como aquella categoría determinada por la existencia de riesgos o amenazas que constituyen el grado máximo de incertidumbre, representan el más alto grado de desconocimiento fenomenológico, tanto frente a sus causas como aquellas referidas a sus consecuencias. Esta categoría conlleva el ejercicio factico de llana reacción, toda vez que presenta características que no han podido ser anticipadas por los analistas o expertos técnicos. Establezca una ponderación numérica en un rango entre 01 y 100 a los siguientes indicadores:
   a. Conocimiento
   b. Complejidad
   c. Inmediatez
   d. Mitigación
   e. Alcance

Id. Participante	PREGUNTAS																			
	P.1	P.2	P.3	P.4	P.5	P.6	P.7	P.8	P.9	P.10	P.11	P.12	P.13	P.14	P.15	P.16	P.17	P.18	P.19	P.20
ESG01	76	64	98	45	17	54	43	87	14	29	27	65	45	87	44	12	55	16	9	25
ESG02	25	37	43	87	34	54	26	87	29	54	33	88	23	98	25	65	15	26	44	27
ESG03	54	26	87	29	54	33	88	23	98	25	65	15	64	98	45	17	54	43	87	14
ESG04	25	43	27	87	23	98	25	65	15	27	55	25	98	25	24	65	45	25	54	27
ESG05	76	34	23	98	45	45	26	87	23	33	87	23	98	25	23	43	45	45	45	43
ESG06	44	65	29	43	56	15	33	88	23	98	25	23	54	43	23	23	15	56	45	23
ESG07	23	23	65	67	23	23	43	65	23	32	98	65	23	98	25	65	15	23	2	98
ESG08	45	56	23	54	33	29	23	98	12	65	15	54	23	78	77	54	29	29	64	77
ESG09	56	43	98	46	65	65	54	12	98	23	29	12	88	87	98	12	65	65	23	23
ESG10	23	23	65	33	88	23	98	25	25	43	29	76	77	87	56	12	23	25	65	29
ESG11	29	32	65	25	43	45	43	65	43	23	65	67	54	43	65	23	32	98	65	65
ESG12	65	54	25	43	23	45	23	25	23	32	23	98	87	65	54	25	54	23	43	23
ESG13	25	12	43	23	56	54	32	43	98	54	43	33	88	23	98	25	54	56	23	45
ESG14	43	15	23	98	77	54	54	23	23	98	25	65	15	25	45	23	45	77	98	23
ESG15	23	25	98	77	54	56	12	98	43	15	56	33	87	23	98	25	23	54	77	54
ESG16	56	43	77	23	87	77	45	77	98	25	23	43	45	23	56	23	15	87	43	12
ESG17	77	23	54	29	54	12	98	23	29	43	54	43	56	98	77	54	23	54	23	15
ESG18	54	98	29	65	33	87	23	98	25	23	15	23	77	77	54	67	29	76	32	25
ESG19	87	77	73	23	43	67	23	98	25	65	15	32	54	77	87	76	65	67	54	43
ESG20	34	76	23	45	23	23	23	43	65	23	32	98	65	54	17	54	23	87	12	12
ESG21	54	23	23	45	32	29	56	76	25	56	33	88	23	98	25	23	98	25	65	15
ESG22	64	34	29	15	54	65	77	17	43	43	87	15	29	23	33	87	23	98	25	23
ESG23	38	25	65	23	12	23	54	54	23	23	98	25	23	43	45	29	45	43	12	23
ESG24	27	43	23	29	45	17	87	43	98	43	65	23	32	98	65	65	45	65	15	23
ESG25	34	23	87	65	54	43	54	23	77	23	25	23	56	56	43	23	15	25	25	29
ESG26	67	98	32	23	33	87	23	98	25	23	25	98	77	17	23	43	23	43	43	65
ESG27	76	77	64	98	45	17	54	43	87	65	23	13	54	29	32	34	29	23	23	23
ESG28	54	29	43	23	98	25	65	15	56	23	98	54	12	98	23	29	65	98	98	43
ESG29	34	65	43	43	24	25	65	23	33	87	23	98	25	23	12	43	23	77	45	23
ESG30	87	23	23	23	45	43	54	43	87	54	12	98	23	29	23	23	87	65	76	54
ESG31	23	34	87	32	33	87	23	98	25	23	56	25	43	23	29	32	23	54	25	65
ESG32	35	45	54	54	45	98	35	25	33	88	23	98	25	88	65	54	25	65	15	15
ESG33	65	45	34	12	65	77	43	43	24	45	23	98	25	65	15	12	65	23	43	25
ESG34	26	45	34	65	25	23	98	25	65	15	34	98	77	54	43	15	45	25	23	43
ESG35	67	15	29	54	43	88	32	98	25	15	15	77	43	65	23	32	98	65	29	54
ESG36	23	23	65	23	23	12	54	77	65	23	25	98	25	23	43	45	15	65	65	12
ESG37	98	29	25	29	98	54	12	98	54	29	43	23	98	25	65	15	23	45	23	65
ESG38	36	65	43	65	77	25	15	87	65	65	23	64	77	23	32	98	29	87	12	54
ESG39	74	23	23	23	65	43	25	65	23	23	98	25	54	32	54	23	65	23	32	65
ESG40	23	54	98	45	54	23	43	35	25	12	77	43	87	54	12	98	23	29	43	23
ESG41	15	34	77	56	65	98	23	64	65	45	17	23	43	12	23	77	43	65	23	25
ESG42	35	23	23	23	23	12	98	23	29	43	65	23	32	98	65	54	12	98	23	29
ESG43	65	65	87	29	25	23	65	43	43	64	98	77	17	25	43	87	22	43	54	54
ESG44	34	25	43	65	25	29	54	23	23	98	25	65	15	43	65	65	23	23	12	12
ESG45	33	43	23	54	43	65	65	32	98	65	15	54	23	23	25	54	29	56	15	65
ESG46	66	23	32	43	23	23	23	54	77	54	43	87	29	98	43	65	65	77	25	54
ESG47	57	98	54	23	98	23	25	12	23	98	25	98	25	23	43	23	23	54	43	65
ESG48	89	77	12	56	77	24	23	98	25	65	15	43	65	23	32	25	65	87	23	23
ESG49	43	52	34	77	54	12	98	23	29	33	88	23	98	25	77	15	34	46	98	25
ESG50	32	23	65	54	65	98	25	23	43	45	43	54	12	98	23	29	23	43	45	23
MEDIA	48	43	49	46	48	45	46	54	45	44	43	54	50	53	45	42	39	53	40	36

ENCUESTA

Nombre:

Fecha:

1. Seleccione el rol o perfil que desempeña dentro de la organizacion:

( ) Jefe de Departamento Planeación

( ) Miembro del Departamento diferente al de ciberseguridad.

( ) Ejecutivo, alta dirección

( ) Experto Seguridad Informática

( ) Educador o formador

( ) Vendedor o Contratista

( ) Otro, ¿cuál?_____

2. Conoce riesgos o amenazas en ciberseguridad de otros sectores que pueda afectar sus funciones:

( ) Si

( ) No

( ) N/R

3. Seleccione el foco de servicios o producción en el mercado a los que presta servicios su organización

( ) Tecnologías de la información:

( ) Financiero

( ) Servicios

( ) Energía

( ) Gobierno

( ) Salud

( ) Manufactura

( ) Telecomunicaciones

( ) Construcción

( ) Consultoría

( ) Educación

( ) Transporte/Logística/Distribución ( ) Alimentos

( ) Minería

( ) Legal

( ) Otro, ¿cuál?_____

4. Como selecciona los riesgos y amenazas en ciberseguridad en su área de trabajo.

( ) De acuerdo al listado de riesgos que entrega el área de riesgos – planeación

( ) De acuerdo a las tendencias de riesgos del sector de la organización.

( ) De acuerdo a las tendencias de riesgos de otros sectores diferentes a la organización.

( ) De acuerdo a las capacidades del área para afrontar los mismos.

( ) De acuerdo a las situaciones que tengan cierto grado de probabilidad de ocurrencia.

5. Considera que los riesgos y amenazas en ciberseguridad son identificados y gestionados apropiadamente.

( ) Si

( ) No

( ) No tiene conocimiento

6. Qué importancia le da a la gestión de riesgos dentro de los proyectos en los que participa (seleccione máximo 2):

( ) Me preocupa los riesgos en los proyectos

( ) Conozco alguna definición del riesgo

( ) Conozco metodologías de gestión de proyectos

( ) Tengo experiencia real en gestión de riesgos en proyectos

( ) Ninguna de las anteriores

7. De acuerdo con su experiencia, que influencia tiene la identificación de riesgos y amenazas de ciberseguridad en la organización o en su área (seleccione máximo 2):

( ) Tiene una influencia objetiva en el cumplimiento de las funciones

( ) Tiene una influencia objetiva en la percepción del éxito del departamento por sus miembros

( ) Identificar los riesgos es positivo, medir los riesgos y abordarlos sistemáticamente no tiene demasiados efectos.

( ) Es mejor una gestión realizada por externos que una gestión realizada por los miembros del área.

( ) Es mejor que los miembros del área hablen de riesgos y se autogestionen, aunque sus prácticas no sean del todo metodológicas.

8. Seleccione la metodología, norma o modelo que se utiliza en la gestión de riesgos en su organización:

( ) Project Risk Management

( ) COBIT

( )ISO 27005

( ) ISO 31010

( ) ITIL

( ) MAGERIT

( ) N/R

9. Participa activamente en la identificación de riesgos y amenazas en ciberseguridad de su área de desempeño.

( ) Si

( ) No

( ) Ocasionalmente

10. Considera que las decisiones o estrategias de la organización o del área deben repensarse si se identifican riesgos o amenazas en ciberseguridad después de que ya existe un plan de mitigación de riesgos de la organización.

( ) Si

( ) No

( ) N/R

11. Quienes realizan el proceso de gestión de riesgos y amenazas de ciberseguridad en la organización.

( ) Área de gestión de riesgos - planeación

( ) Área de Ciberseguridad – Seguridad Informática

( ) Cada área funcional en conjunto con el área de ciberseguridad .

12. Conoce si las amenazas de día cero cuentan con planes de gestión o mitigación en su organización.

( ) Si

( ) No

( ) N/R