Escuela Superior de Guerra

“General Rafael Reyes Prieto”

Maestría en Ciberseguridad y Ciberdefensa

PROPUESTA ESTRATÉGICA PARA MEJORAR EL PROTOCOLO DE PROTECCIÓN DE INFRAESTRUCTURA CRÍTICA CIBERNÉTICA DE LA NACIÓN

DIEGO ALFONSO ESPINOSA BERMUDEZ

Director de trabajo de grado

LUCAS GIRALDO RIOS MBA, MSc, PhD (c)

Bogotá DC, Colombia; 12 de Octubre de 2022.

Dedicatoria

Dedico este trabajo a Dios, a mi familia, a mis hijos y a todos aquellos que me han ayudado a lo largo de mi carrera militar.

Agradecimientos

Agradezco a Dios, a mis hijos, mis padres, mis docentes y al Ejército Nacional por permitirme dar un paso más en esta, la carrera de las armas.

Tabla de contenido

Abreviaturas

Microsoft Azure – Software empleado para concertar bases de datos digitales.

Resumen

Proteger la infraestructura crítica cibernética de la nación se convirtió en un objetivo relevante para los estamentos de seguridad cibernética involucrados; especialmente desde que se emitió el CONPES 3701 de 2011. Una de esas preocupaciones y a la vez objetivo, es el fortalecimiento del Plan Sectorial para la Protección del Medio Ambiente, pues su actualización reciente data de 2018, y deja a un lado nuevas tendencias de contexto como la migración digital de bases de datos a la nube o la incorporación de plataformas tecnológicas que conduzcan a procesos de anticipación y predicción de ataques. Es dicha desactualización sistemática en el plan, la que condujo a esta investigación a formular un objetivo general: proponer lineamientos estratégicos para el fortalecimiento del esquema de Ciberdefensa que compete a la protección de la infraestructura crítica del sector ambiental en Colombia frente al surgimiento de nuevas ciber amenazas. Para tal fin, se seleccionó un método de investigación dividido en tres partes: diagnóstico de la situación actual (AS IS), análisis de tendencias contextuales y estructuración final de una propuesta conformada por cuatro lineamentos: la migración de bases de datos por intermedio de Microsoft Azure, la adopción de una plataforma Warden para prevenir y anticipar ataques, la sistematización de los sistemas de información y capacitación totalizada del capital humano en temas tendencia.

Palabras clave: estrategia, ciberdefensa, medio ambiente, infraestructura, crítica, cibernética.

Abstract

Protecting the nation's critical cyber infrastructure became a relevant objective for the cyber security establishments involved; especially since CONPES 3701 of 2011 was issued. One of those concerns, and at the same time an objective, is the strengthening of the Sectoral Plan for the Protection of the Environment, since its recent update dates from 2018, and leaves aside new context trends. such as the digital migration of databases to the cloud or the incorporation of technological platforms that lead to processes of anticipation and prediction of attacks. It is this systematic obsolescence in the plan, which led this research to formulate a general objective: to propose strategic guidelines for the strengthening of the Cyber defense scheme that is responsible for the protection of the critical infrastructure of the environmental sector in Colombia against the emergence of new cyber threats. For this purpose, a research method divided into three parts was selected: diagnosis of the current situation (AS IS), analysis of contextual trends and final structuring of a proposal made up of four guidelines: the migration of databases through Microsoft Azure, the adoption of a Warden platform to prevent and anticipate attacks, the systematization of information systems and comprehensive training of human capital on trending topics.

Keywords: strategy, cyberdefense, environment, infrastructure, criticism, cybernetics.

Introducción

La infraestructura crítica cibernética de la nación que coexiste en el sector de medio ambiente es una prioridad estratégica para el Estado colombiano. Así queda demostrado en la estructuración del Plan Sectorial para la Protección del Medio Ambiente, único en su clase.

De acuerdo con la Organización de los Estados Americanos (2018), Colombia afronta de tiempo atrás dos desafíos en materia ciber: concientización del capital humano y la transversalidad de los procesos de ciberdefensa en todos los campos del desarrollo. Precisamente, debatir uno de esos dos desafíos se vuele la proposición primaria de este trabajo de investigación, el cual se centra en el resguardo y protección de infraestructura crítica cibernética para el sector medio-ambiental.

Realizar un estado del arte conformado por 25 autores permitió entender que la estrategia actual en Colombia depende ejercicios orientados a la determinación de riesgos que de hecho radican en su mayoría sobre una entidad adscrita al Ministerio de Medio Ambiente y Desarrollo Sostenible: el IDEAM.

Así mismo, con el ejercicio de construcción de antecedentes se hallaron tres factores problemáticos. Por un lado, la estrategia para proteger la ICCN-MA[1], si bien obedeció a un plan estratégico, está desactualizada y eso se comprobó con el análisis cualitativo realizado en este trabajo de investigación. También se hallaron problemáticas relacionadas con la desactualización y ralentización de los sistemas de ciberdefensa y protección, ya que no hay estudios asociados al concepto "estructuración de soluciones" conexas al contexto. Por el otro, la estrategia actual no se alinea a las necesidades

[1] Infraestructura crítica cibernética de la Nación – Sector Medio Ambiente

tecnológicas del contexto; por ejemplo, ciberamenazas con características complejas y genealogías con tipologías híbridas.

Por la anterior razón, esta investigación propuso como punto de inicio un interrogante exploratorio: ¿Cuáles son los elementos a fortalecer en el esquema de Ciberdefensa de la infraestructura crítica del sector ambiental en Colombia frente al surgimiento de nuevas Ciber amenazas?

Pues bien, formular una respuesta implicó el diseño y ejecución de un proceso de investigación divido en tres fases. En la primera fase se llevó a cabo un análisis diagnóstico de la estrategia de protección y ciberdefensa actual utilizado para el sector de medio ambiente. En la segunda se realizó un estudio de tendencias contextuales que condujo a la identificación de acciones ciber estratégicas utilizadas en contextos y problemáticas afines. En la tercera se identificaron los factores de intervención y las líneas estratégicas por implementar.

No fue hasta la tercera parte de la investigación hasta cuando se determinó que los elementos por fortalecer son: primero, las bases de datos como principal activo estratégico de información; segundo, la anticipación y predicción de ciber ataques con tipologías complejas y desconocidas; tercero, la tecnificación generalizada y vertical de los subsistemas de información y cuarto, la capacitación micro-especializada para el capital humano.

CAPÍTULO I
Planteamiento de la Investigación

El esquema de ciberdefensa colombiano resulta de múltiples esfuerzos institucionales. Hablar de ciberdefensa en Colombia es establecer parámetros de acción y análisis en los que ingresan diferentes términos a la ecuación. Uno de esos términos corresponde al proceso funcional ligado al resguardo y protección de infraestructura crítica y cibernética de la nación centrada en el concepto *medio ambiente*.

Para el resguardo de esta ICCN, se diseñó el Plan Sectorial de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia Sector Ambiente y RRNN (Ministerio de Medio Ambiente y Desarrollo Sostenible, 2018). El plan busca dar cumplimiento a un objetivo: anticipar cualquier tipo de ciber-ataque mediante la concertación de líneas estratégicas cuyo rol es desarticular riesgos conocidos, latentes y emergentes.

Sin embargo, la estrategia de protección se centra en un núcleo de acción cuya concepción yace en la anticipación de ciberataques a través de factores procedimentales como el marco AREM.

Por esa razón, resulta necesario analizar las fallas y/o vacíos de función que posee el plan estructurado, toda vez que es necesario comprender cómo y bajo qué parámetros se puede mejor u optimizar el proceso estructural y funcional utilizado para prevenir ciber ataques de tipología compleja sobre la ICCN; esta última, necesaria para el funcionamiento del sector medio ambiental.

Dar esta explicación demanda el planteamiento de tres argumentos clave. Primero, mejorar sistemas ciber o subsistemas de información con volúmenes de datos altos, demanda concertar o idear centros de recepción de data en los que exista un código fuente para ciber protección a partir de la variable *diferenciación de firewalls*.

En este sentido, es imperativo reconocer que una de las estrategias diseñadas por el Ministerio de Medio Ambiente y Desarrollo Sostenible es la combinación de elementos digitales sujetos a: integración tecnológica de sistemas en contra de Malware, Botnets y Ransonmware (PSPMA, 2018, p. 38).

Si bien hay una postura tecnológica fuerte, hay otros elementos – vacíos de función- no incluidos en el esquema de protección. Esos elementos son: tecnologías de predicción basadas en minería de datos, interconexión de factores procedimentales con machine learning e integración de IA[2] al marco estratégico.

Un segundo argumento tiene relación con el planteamiento *riesgos emergentes*. Para comprender esta parte es necesario analizar el fragmento consiguiente:

> La intrusión del continuo digital en todas las áreas de actividad humana, así como los niveles sin precedentes de innovación e interdependencia tecnológicas, han hecho que sea imposible tratar la ciberseguridad de forma aislada, como un asunto técnico o un área de políticas independiente. En los últimos años, la ciberseguridad ha roto la barrera de los silos técnicos y se encuentra en la intersección de múltiples disciplinas y áreas de políticas: acceso digital y conectividad, resiliencia, justicia penal, diplomacia, seguridad y defensa internacional, y economía digital y comercio, así como las nuevas tecnologías (USECIM, 2021, p. 2).

Como se puede observar, la amenaza digital está en constante evolución. Ello significa que el esquema digital de protección planteado en el 2018 por el plan, si bien está vigente, no está actualizado. Siendo así, uno de los problemas relevantes para el

[2] Inteligencia artificial

sistema de protección de ICCN medio ambiental sería la desactualización de sus elementos de función digital.

El tercer argumento que suma a esta discusión es la capacitación del recurso humano. Mírese la tabla 1 para proseguir con esta explicación.

Tabla 1 Línea estratégica de prevención

CONOCIDOS	CONTROLES
Malware	• Instalación Antivirus • Sensibilizaciones contra la ingeniería social, Phishing, etc. • La segregación de red impide que el malware se mueva en la organización. • Parchar vulnerabilidades / Actualizaciones del SO y herramientas. • Monitoreo
Fuga de Información	• Conocer la información que gestiona la organización • Clasificación de los activos de información. • Determinar el grado de seguridad. • Cifrar la información confidencial corporativa. • Acuerdos de confidencialidad
Botnets	• Solución especializada de Seguridad. • Actualizaciones del SO y herramientas. • Monitoreo

Fuente: Fuente: información recuperada de PSPMA (2018)

Como se puede observar, en la primera línea de contención, el Malware, hay un fundamento necesario para comprender que la capacitación del capital humano juega un rol primario en el proceso de ciber protección. Ese fundamento es la s*ensibilización* del RRHH (Burov, 2016). Ello quiere decir que no todos los elementos orientados a ciber-protección pertenecen a la categoría t*ecnologías* o *componentes digitales complejos*.

Los tres argumentos expuestos terminan en una conclusión primaria. El sistema de protección del ICCN para el sector medio ambiental, si bien es procedente y posee formas estructurales apropiadas, necesita intervención y optimización categórica, no solo para su mejoramiento, sino también para una optimización de naturaleza inter sector que

permita dar cumplimiento al objetivo central: proteger y garantizar el funcionamiento de infraestructura crítica cibernética de la nación.

Estado del Arte

La protección de infraestructura crítica cibernética (de ahora en adelante ICC) es una misión constitucional para las Fuerzas Militares de Colombia. Los avances tecnológicos y la rápida expansión del internet han generado fenómenos y alteridades contextuales; algunas de ellas encajarían en la categoría de guerra cibernética (Bravo, 2019).

El rol de las Fuerzas Militares frente al proceso de protección de infraestructura crítica es un indicador preponderante para establecer la importancia de las políticas de seguridad y defensa digital. También, saber cuan necesario es que las políticas se extiendan al sector privado para garantizar el normal funcionamiento de sistemas y subsistemas tecnológicos sujetos al marco de gobernanza digital.

En la investigación que titula Importancia de la Ciberdefensa en la Infraestructura Crítica Financiera colombiana frente a las Nuevas Crecientes Amenazas Cibernéticas, Benavidez (2020) realiza un estudio de los valores agregados, representativos en el modelo de ciberdefensa colombiano actual. Una de sus conclusiones sostiene lo siguiente:

> se encontró que primero, hay una creciente preocupación internacional respecto a los temas de ciberseguridad y ciberdefensa, que abarcan tanto los Estados en primera medida, pero también los privados en ciertos sectores particulares como los financieros, esto se presenta como resultado de que hay actores con capacidades de atacar las redes y los sistemas con el riesgo de afectar de forma grave el funcionamiento incluso de una

> nación, así que esto posiciona al tema de ciberseguridad y ciberdefensa en las primeras posiciones de la agenda (Benavidez, 2020, p.50).

Otra investigación con la que también se puede analizar la importancia de proteger la infraestructura crítica cibernética se halla en la publicación Ciberseguridad en la Infraestructura Crítica mediante el Sistema SCADA en Planta de Tratamiento de Agua en Lima. En el documento, Machado (2017) estudia diferentes modelos de ciberseguridad y ciberdefensa utilizados en la protección de recursos acuíferos. Con la investigación el autor deduce que los ciberataques son amenazas latentes con posibilidad de cambio, evolución y/o transmutación.

Como Machado (2017), Díaz y Mendoza (2019) entran al debate conceptual para explicar que ataque cibernético a infraestructura críticas no solo afectaría al Estado como actor representativo, pues junto al ataque vendría una serie de consecuencias socioeconómicas sobre el actor poblacional. Mírese lo que afirman los autores para continuar con la explicación:

> En Colombia se han sucedido un gran número de actos mal intencionados contra las infraestructuras críticas, entre ellos; los oleoductos, estaciones petroleras, infraestructuras de telecomunicaciones, torres de trasmisión de energía, subestaciones eléctricas entre otras de pleno conocimiento de la sociedad, por parte de grupos al margen de la ley, entre ellos el extinto grupo de las FARC, el ELN, el EPL y algunas disidencias que en ocasiones llevan al país a situaciones de desastre y emergencia (Díaz y Mendoza, 2019, p. 73).

Los autores realizan una comparación de la afectación en medios cibernéticos con las afectaciones a la infraestructura cometidas por otros actores delictivos tradicionales.

Los impactos a la infraestructura crítica cibernética de la nación son una preocupación constante para el organismo de seguridad y defensa nacional. Mírese que en la investigación de Leyva (2021) se plantea una propuesta estratégica, cuyo objetivo es mejorar la seguridad cibernética de infraestructuras críticas, necesarias para la subsistencia dl actor poblacional.

De acuerdo con Leyva (2021), la digitalización de sistemas de información ha puesto en riesgo no solo la seguridad de las infraestructuras críticas y cibernéticas de la nación, sino también la integridad misma del actor poblacional. Para el investigador, las nuevas estrategias de ciberseguridad y ciberdefensa tienen que enfocarse sobre la protección de activos estratégicos, planes de desarrollo y otros componentes digitales necesarios para el funcionamiento de las infraestructuras.

Otra investigación que también se aproxima al objeto de este trabajo es planteada por Villar (2021). De acuerdo con el investigador, es necesario que al proceso de securitización y protección de infraestructura crítica cibernética se anexen tecnologías de disrupción; lo anterior teniendo en cuenta el parámetro integral cibernético que contrae el internet de las cosas. El punto objeto en la investigación de Villar (2021) es el que el Estado debe aumentar sus esfuerzos a partir de integraciones conceptuales e interinstitucionales, pues el estado final deseado es proteger infraestructuras críticas cibernéticas que generan beneficios de naturaleza colectiva.

Una postura similar a la de Villar (2021) es la de López, Cárdenas y Triana (2019). En su investigación, los autores se enfocan sobre un punto objeto: la responsabilidad que el Estado posee frente a la protección de infraestructura crítica cibernética por la naturaleza misma de los derechos fundamentales del actor poblacional. En ese sentido, el afán por proteger este tipo de infraestructuras no recaería en el factor “control estatal”, sino más bien en el factor *protección poblacional*.

Por otro lado, y con una óptica que se acerca más a la investigación científica, López, Ruete y Gatica (2021) entran a la construcción teórica para estructurar propuestas que, a través de procesos de integración, protejan de forma integral infraestructuras cibernéticas necesarias para promulgar el desarrollo en sociedades, actores poblacionales e instituciones públicas.

Finalmente, se integra en este estado del arte el resultado investigativo obtenido por Tellechea (2019). La investigación desarrollada titula Infraestructura Crítica, Usuarios y Contenido ¿Qué se busca proteger en el ciberespacio? Allí, la autora realiza un análisis multimodal de los asuntos de ciber seguridad encaminados a la protección de ICC, llegando a determinar que: primero, las estrategias de protección tienen que alinearse con el planteamiento de las políticas públicas; segundo, es necesario que se adopten tecnologías de prevención y anticipación, cuyo enfoque tecnológico sea superior al de las amenazas emergentes.

Formulación del problema

¿Cuáles son los elementos a fortalecer en el esquema de Ciberdefensa de la infraestructura crítica del sector ambiental en Colombia frente a las Ciber amenazas?

Objetivos de la investigación

Objetivo general

Proponer lineamientos que permiten el fortalecimiento del esquema de Ciberdefensa para la protección de la infraestructura crítica del sector ambiental en Colombia frente a las Ciber amenazas.

Objetivos específicos

- Identificar el esquema de Ciberdefensa establecido por Colombia para la protección de las infraestructuras criticas frente a Ciber amenazas.
- Realizar un diagnóstico del esquema de ciberdefensa del sector ambiental para la protección de su infraestructura crítica.
- Desarrollar lineamientos para el fortalecimiento del esquema de Ciberdefensa del sector ambiental en Colombia frente a las Ciber amenazas.

Metodología

Esta investigación es mixta y su realización implica el uso de herramientas cualitativas y cuantitativas. El diseño metodológico seleccionado obedecerá al siguiente esquema:

Tabla 2 Explicación del diseño metodológico

Proceso de investigación	**Descripción**	**Método**	**Resultado esperado**
Conceptualización de teorías	En este punto se llevará a cabo el estudio teórico de la investigación	Método de esquematización conceptual por categorías principales y secundarias	Análisis teórico completo de la investigación
Análisis del modelo de protección de ICCN actual	Identificación de falencias, fallas y vacíos funcionales que pongan en riesgo procesos estructurales sujetos al funcionamiento de la ICCN	Aplicación de herramientas del pensamiento estratégico.	Extracción de fallas, problemáticas y protocolos poco funcionales

Proceso de investigación	Descripción	Método	Resultado esperado
Análisis de la percepción del personal de expertos en materias de ciber defensa; específicamente centrada en infraestructura crítica cibernética de la nación	Recolección de datos cualitativos a un personal de expertos en ciber defensa sobre infraestructura crítica y cibernética de la nación	Aplicación de entrevistas generales con preguntas estructuradas	Análisis de datos cualitativos y proposición de debate y disertación de hallazgos.
Protocolos de mejoramiento	Desarrollar los protocolos de mejoramiento de la protección de infraestructura crítica mediante la aplicación de los planteamientos metodológicos contraídos por la norma ISO 27032 – estándares de ciber defensa y ciberseguridad	Metodología ISO 27032	Portafolio de procesos de mejoramiento para optimizar la protección de ICCN

Fuente: elaboración propia

CAPÍTULO II
Marco de Referencia

Marco teórico

1. Ciberespacio

1.1. Definición

La palabra ciberespacio nace de la unión del término "cibernao", la cual proviene del griego antiguo que significa timonel, gobernador, piloto, (el cual "*gobierna*" la embarcación, “pilotea una nave”) y el vocablo “espacio” dando así la idea de estar piloteando o navegando sobre un mundo virtual. (Wikipedia, 2017)

El término Ciberespacio fue utilizado por primera vez como una palabra artificial en una novela de ciencia ficción llamada Neuromante (Neuromancer en inglés) escrita por William Gibson y publicada en 1984, el escritor norteamericano la utilizó para para describir una red de computadoras ficticia donde el actor principal utiliza electrodos para conectarse a una computadora, que generan un mundo paralelo, la “Matriz” que corresponde a la realidad en su percepción. y que contenía enormes cantidades de información que podría explotarse con el fin de adquirir riquezas y poder.

El prefijo Ciber, en la actualidad tiene muchos usos, como muestra de esto se utiliza para referirnos a cualquier cosa que ocurriese a través de Internet como, por ejemplo, ciberamenazas, ciberriesgos, ciberdefensa, ciberespionaje, ciberacoso, ciberespacio, cibercultura, cibercafés, cibernautas; entre otras muchas más y su utilización se desarrolla para hacer referencia al mundo digital en general.

Se conoce como Cibernautas a los individuos que pueden interactuar, intercambiar ideas, compartir información, proporcionar apoyo social, crear medios artísticos, jugar juegos, participar en la discusión política y otras múltiples actividades, a través del uso de una red interconectada, que por lo general es de carácter global, es decir,

que los usuarios que navegan por el ciberespacio se llaman cibernautas y generalmente, pasan varias horas al día, en la realidad virtual que se encuentra dentro de los ordenadores y redes del mundo, que se llama ciberespacio.

El término Ciberespacio suele confundirse con el de Internet, sin embargo, la expresión Ciberespacio se refiere generalmente a los objetos y recursos que coexisten en la misma red informática, es decir, que los fenómenos que ocurren dentro de Internet, ocurren en el ciberespacio, y no en el espacio geográfico donde los cibernautas o sus servidores se encuentran físicamente; por lo tanto, llamamos ciberespacio a un mundo no físico, el cual no tiene límites y donde cualquier persona puede estar interconectada únicamente con una conexión a la red de tal manera que pueda interactuar con el mundo entero sin barreras. (Facultad de Informática de la Universidad Complutense de Madrid, 2017)

De acuerdo con el artículo del Real Instituto Elcano "Ciberseguridad en España: una propuesta para su gestión" publicado por el ingeniero superior en informática, Enrique Fojón Chamorro y el ingeniero de telecomunicación Ángel F. Sanz Villalba, el Ciberespacio se refiere al conjunto de medios físicos y lógicos que conforman las infraestructuras de los sistemas de comunicaciones e informáticos. (Fojón Chamorro & Sanz Villalba, 2010, pág. 1)

En la V Conferencia Internacional sobre Guerra de la Información y Seguridad realizada en la ciudad de Dayton, Estado Ohio, Estados Unidos entre el 8 y 9 de abril de 2010.en la cual con el título de “Ciberespacio: definición e implicaciones” los autores exponen que el ciberespacio es un conjunto dependiente del tiempo de sistemas de información interconectados y los usuarios humanos que interactúan con estos sistemas. (Ottis & Peeter, 2010, pág. 267)

La Guía de ciberseguridad para los países en desarrollo refiere que el término ciberespacio se usa para describir sistemas y servicios conectados directamente o indirectamente a Internet, las telecomunicaciones y las redes informáticas. (International Telecommunication Union - ITU, 2011, pág. 5)

Dada la constante evolución tecnológica que ha desarrollado la humanidad se ha creado un ambiente artificial denominado ciberespacio y que está plenamente integrado en las actividades humanas y ha trascendido de forma transversal a los espacios físicos y naturales ya existentes en los que la humanidad se había desarrollado naturalmente como lo son el terrestre, marítimo, aéreo y espacial; el nuevo ambiente o espacio, no reconoce fronteras físicas ni estados naciones, permite la evolución de las operaciones en términos de interoperabilidad de los sistemas en los distintos ambientes naturales. (Gastón Sack & Ierache, 2015, pág. 1)

Otro punto de vista que vale la pena mencionar es el concepto de ciberespacio entregado en septiembre de 2006, por los Jefes de Estado Mayor de los Estados Unidos el cual lo definieron como "dominio caracterizado por el uso de electrónica y espectro electromagnético para el almacenamiento, modificación e intercambio de información vía sistemas en red e infraestructuras físicas asociadas"; en otras palabras, abarca todo lo que fluya a través del espectro electromagnético (como celulares, Internet, etc.); y si emite o transmite, a través de propagación de energía, usa el ciberespacio. (Gastón Sack & Ierache, 2015, pág. 2)

En la siguiente tabla se realiza una recopilación de las diferentes definiciones del Ciberespacio, la cual es elaborada teniendo en cuenta el documento "Controles de Seguridad Propuesta inicial de un Framework en el contexto de la Ciberdefensa". (Gastón Sack & Ierache, 2015, págs. 3-4).

Tabla 3
Definiciones de Ciberespacio

Organismo o País	Definición
Real Academia Española.	Ámbito artificial creado por medios informáticos. Esto quiere decir que para implementar el ciberespacio se necesita de una infraestructura física de computadoras y líneas de comunicaciones que las mantengan interconectadas.
National Institute of Standards and Technology (NIST).	Dominio global dentro del entorno de la información que consta de redes interdependientes de infraestructuras de sistemas de información que incluyen: internet, redes de telecomunicaciones, sistemas informáticos, procesadores y controladores.
Unión Europea.	Espacio virtual por donde circulan los datos electrónicos de los ordenadores del mundo.
Unión Internacional de Telecomunicaciones.	Lugar creado a través de la interconexión de sistemas de ordenador mediante Internet.
España.	Conjunto de medios físicos y lógicos que conforman las infraestructuras de los sistemas de comunicaciones e informáticos.
Estados Unidos (DoD).	Dominio global dentro del entorno de la información, consistente en la red interdependiente de las infraestructuras de tecnología de la información incluida la Internet, redes de telecomunicaciones, sistemas informáticos, los procesadores y controladores.
Estados Unidos (National Military Strategy for Cyberspace Operations).	Dominio que se caracteriza por el uso de la electrónica y el espectro electromagnético para almacenar, modificar e intercambiar datos a través de sistemas de redes e infraestructuras físicas asociadas
Alemania.	Espacio virtual de todos los sistemas informáticos vinculados a nivel de datos a escala global. La base para el ciberespacio es el Internet como una red de conexión y transporte universal y accesible al público que puede ser complementada y más expandido en cualquier número de redes de datos adicionales. Sistemas de informáticos en un espacio virtual aislado no son parte del ciberespacio
Reino Unido.	Todas las formas de actividades en redes digitales; esto incluye el contenido y acciones realizadas a través de redes digitales.

Nota: Adaptado del documento "Controles de Seguridad Propuesta inicial de un Framework en el contexto de la Ciberdefensa". (Gastón Sack & Ierache, 2015, págs. 3-4)

Como una visión particular se puede definir que el ciberespacio es el ambiente virtual, que depende del tiempo generado por los cibernautas o usuarios que interactúan con los sistemas de información y que utilizan un conjunto de elementos físicos (hardware) y lógicos (software) que conforman las infraestructuras de los sistemas comunicación e información y los cuales se encuentran interconectados de forma global produciendo transferencia de datos entre individuos particulares o comunidades virtuales.

1.2. Características del Ciberespacio

Entre las características más representativas con las que cuenta el ciberespacio se pueden clasificar de acuerdo con la siguiente tabla:

Tabla 4
Características del Ciberespacio.

Característica.	Descripción.
Conectividad de Redes de Equipos de Cómputo	Una característica física del ciberespacio es la creación de redes de equipos de cómputo y su interconexión como base para su existencia; con un grado cada vez mayor de redes, se obtiene en cada caso un valor de utilidad superior para el usuario individual y los costos disminuyen a medida que aumenta el número de usuarios y redes conectadas. Las tasas de crecimiento de redes actuales se identifican por la red de computadoras totalmente interconectadas tal como lo vemos en la actualidad a través de dispositivos móviles, automóviles o electrodomésticos y cualquiera sea el aspecto del futuro del ciberespacio, este se conectará a través de una red de equipos de cómputo.
Ambiente virtual	Esta característica es uno de los principales rasgos del ciberespacio porque no es un elemento físico. El Ciberespacio es la dimensión generada durante el tiempo de interconexión e interoperabilidad de redes, sistemas, equipos y personal, en el cual personas y ordenadores coexisten con los sistemas informáticos cualesquiera que sean estos y las telecomunicaciones que los vinculan En cuanto al termino tan utilizado de “realidad virtual" se trata de la creación de un mundo virtual a través de dispositivos de entrada y salida adecuados, toda sensación y percepción está mediada por aparatos: pantallas cascos

Característica.	Descripción.
	digitales para ver, altavoces para oír, guantes de datos para sentir tacto, etc. a los que los usuarios están conectados. A través de la simulación de impresiones realistas ("virtuales"), tiene más o menos la sensación de estar en un espacio real, que en realidad existe solo en forma de datos dentro de una computadora. Sin embargo, en este lugar imaginario y virtual, es posible crear una sensación de presencia a pesar de la ausencia física.
Accesibilidad	Dado el carácter del lenguaje y de su forma de acceder y participar activamente, el ciberespacio es un entorno conceptualmente accesible y manipulable donde existen muchas formas de participación.
Igualdad	En el Ciberespacio todos tenemos la misma oportunidad de acceder, participar y trasferir información y/o comunicarse. En el Ciberespacio solo se transmiten las señales lingüísticas puramente relacionadas con el contenido. Se eliminan las características sociales como la edad, el estado y la vestimenta que en el mundo real normalmente podría afectar la comunicación, adicional a esto no existen signos no verbales, por lo que la atención debe concentrarse en el contenido del mensaje. Algunos llaman a esto Democracia Net.
Económica	El Ciberespacio es una dimensión que tiene una accesibilidad más económica que otros canales de difusión e información de utilidad comparable; esto se hace visible con el crecimiento exponencial de los usuarios.
Canal de distribución de información	El Ciberespacio funciona satisfactoriamente como canal de distribución de información o de ofertas comerciales, las redes interconectadas vinculan millones de computadoras en todo el mundo proporcionando datos de ida y vuelta que pueden ser textos, fotos, videos, música. Tenemos a nuestro alcance casi toda la información sin importar el punto geográfico; variada; histórica y también de actualidad.
Sin límites espaciales	La comunicación o el intercambio de información en el Ciberespacio no está vinculada espacialmente, las distancias geográficas no limitan para poder comunicarse, emitir, recibir o transferir información. Los usuarios de intercambio de información o los participantes de las comunicaciones pueden estar en diferentes ubicaciones geográficas y reunirse en el espacio virtual para intercambiar ideas. Por lo tanto, es posible comunicarse en el mundo real y virtual al mismo tiempo.

Característica.	Descripción.
Atemporal	La comunicación y la trasferencia de información en el Ciberespacio no está vinculada al tiempo, todo está inmediatamente a nuestro alcance, no gastamos tiempo en desplazarnos, la restricción de tiempo puede cancelarse porque en la comunicación asincrónica es posible enviar y recibir un mensaje en diferentes momentos. En la comunicación sincrónica, el intercambio está vinculado a la presencia simultánea de los participantes, sin embargo, el contenido de las llamadas puede almacenarse y recuperarse, y rastrearse en función del tiempo. Debido a esta característica, los socios de comunicación no tienen que estar físicamente presentes.
Sin identidad	A diferencia de la comunicación cara a cara, en el cual se identifica claramente al interlocutor. Esta característica da como resultado la posibilidad de anonimato, utilizar un seudónimo, se puede tener una identidad imaginaria o falsa. incluso podemos ofrecer una imagen diferente a los demás creando un "avatar" o simplemente con nuestra página web
La digitalización de la información	Esta característica, es fundamental porque cada comunicación en línea e intercambio de información en el Ciberespacio se basa en procesos digitalizados. El resultado de la digitalización de la información es la capacidad de almacenar y documentar toda la información digital, lo que a su vez permite un procesamiento más sencillo. El Ciberespacio sería impensable sobre una base análoga. Solo pudo surgir a través de la disponibilidad digital de la información. Cada texto, cada información de sonido y cada imagen se pueden codificar en sus Dominios digitales y hacer que esa información sea accesible para el ciberespacio. La digitalización en sí misma significa un acercamiento con la realidad, reduce esta información a la parte perceptible por el ser humano, que buscan filtrar la información más allá de nuestro umbral de percepción a favor de una transmisión más rápida. Los datos digitales, por su parte, se pueden transformar fácilmente en estados magnéticos, como lo es un disco duro; en corrientes eléctricas como por ejemplo en una línea de datos, es decir, que los bits de información pueden ser extraídos del medio físico al medio digital y viceversa sin grandes gastos de energía y ser compartidos sin mayor esfuerzo con todos los usuarios que lo requieren.

Nota: (Obtenido de: Del Rio, José Luis et al (s.f.). Las Redes y la documentación. Profesor de Documentación de la UCM. [En Línea] https://webs.ucm.es/info/multidoc/multidoc/revista/num8/jldelrio.html)

1.3. Importancia del Ciberespacio

En las últimas dos décadas, el ciberespacio ha tenido un tremendo impacto en todos los sectores de la sociedad. Nuestra vida diaria, los derechos fundamentales, las interacciones sociales; y, las economías dependen de que la tecnología de la información y la comunicación funcione a la perfección. Un ciberespacio abierto y libre ha promovido la inclusión política y social en todo el mundo; ha derribado barreras entre países, comunidades y ciudadanos, permitiendo la interacción y el intercambio de información e ideas en todo el mundo; ha proporcionado un foro para la libertad de expresión y el ejercicio de los derechos fundamentales, y ha empoderado a las personas en su búsqueda de sociedades democráticas y más justas. La tecnología de la información y las comunicaciones se ha convertido en la columna vertebral de nuestro crecimiento económico y es un recurso crítico en el que todos los sectores económicos confían y para algunos de ellos, sus complejos sistemas de intercambio de información se han convertido en la base de su funcionamiento, en sectores clave como las finanzas, la salud, la energía, el transporte y en muchos modelos comerciales. (European Commission, 2013)

La importancia del Ciberespacio es que ha creado un ambiente donde la información se comporta libremente, siendo accesible a un número bastante mayor de personas y donde existen múltiples canales de comunicación con distintos puntos de vista.

En el presente siglo, dada la evolución que han alcanzado las tecnologías de la información, el Ciberespacio se ha convertido en una herramienta que ha generado una formidable productividad desde el punto de vista económico, y una oportunidad para generar Investigación, Desarrollo e innovación – I+D+i, como parte de un compromiso para mejorar el futuro a servicio de la humanidad, tanto es así que hoy en día es posible trabajar de forma virtual con toda la información necesaria al instante, a un costo bajo y sin tener que hacer presencia física en un punto geográfico especifico.

Otro de los factores por los cuales esté mundo virtual, llamado Ciberespacio, ha tomado una importancia relevante y ha cambiado el mundo real es porque suele ser un lugar donde se ejecutan acciones hostiles que pueden enmarcarse en los conceptos de cibercrimen, ciberterrorismo o ciberguerra.

Esto platea un escenario con múltiples problemas para la seguridad y defensa del Estado-Nación, esta modalidad de ataques a las infraestructuras críticas de los estados se comenzó a regularse después de los ataques sufridos por Estonia en el 2007, pues la Organización del Tratado del Atlántico Norte (OTAN) tomó medidas para la creación de un centro de Ciberdefensa. El centro se inauguró en 2008, a apenas unos cuantos kilómetros del lugar donde originalmente se encontraba el soldado de bronce, cuyo traslado origino el ciberataque.

Esta preocupación tiene prácticamente un carácter global y la ocurrencia frecuente de atentados en la red, así como la aparición de amenazas, conllevó que muchos de los gobiernos de los países tomaran este asunto como una prioridad y comenzaran a desarrollar estrategias y sistemas de defensa contra los ataques cibernéticos. De esta manera, el gobierno de los Estados Unidos reconoce la tecnología de información interconectada y la red interdependiente de infraestructuras de tecnología de la información que operan en este medio como parte de la infraestructura crítica nacional de los EE. UU. y para el Departamento de Defensa de los Estados Unidos, el ciberespacio se convirtió en un campo de operaciones, similar a los que se han presentado en la tierra, el mar, el aire o el espacio y por tanto, un lugar susceptible para llevar a cabo maniobras defensivas y ofensivas, que pueden incluir ataques preventivos o represalias (López de Turiso y Sánchez, 2012, pág. 134).

De ahí, que le haya concedido un carácter de escenario estratégico, operacional y táctico (Centro Superior de Estudios de la Defensa , 2013, pág. 6). Khuel por ejemplo, se

refiere al ciberespacio como un “espacio operacional donde los humanos y sus organizaciones hacen uso de las tecnologías necesarias para actuar o crear efectos, los cuales pueden ser en el mismo ciberespacio o sobre otros dominios operaciones o elementos del poder” (Kuhel, 2009, pág. 29).

Khuel plantea que, en ese sentido, el ciberespacio es similar a los otros cuatro dominios que existen (tierra, mar, aire y espacio), en la medida en que es un dominio operacional y un elemento del poder dentro del cual opera la seguridad nacional.

Contrario a esta opinión. Gómez Agreda (2013) plantea, que quienes se han acercado al concepto de ciberespacio lo han hecho desde una perspectiva parcial que los ha llevado a categorizarlo como un entorno donde los seres humanos operan y se comunican, sin la adecuada comprensión que requiere el término. El autor explica que, si éste se entendiera como una zona difusa utilizada para el tránsito de bienes, personas o ideas, efectivamente podría ser similar al resto de dominios, pero lo que los distingue es precisamente su carácter artificial que le confiere unas características diferentes, además de su inmaterialidad y, sobre todo, de la capacidad que tiene para producir alteraciones en los otros dominios.

Aunque la discusión sobre si el ciberespacio es un dominio, es mucho más extensa y debe dársele un tratamiento cuidadoso, que ayude a tomar una posición frente al concepto, lo que es innegable es que como señala Lynn, “los ataques cibernéticos serán un Dominio significativo de cualquier conflicto futuro, ya sea que involucre naciones principales, estados paria o grupos terroristas” (Máquez, 2011). También es cierto que el Ciberespacio, representa una permanente agresión, en el que todos los usuarios, independiente de su nivel, son vulnerables a los ataques aun cuando cuente con algún tipo de seguridad.

1.4. Crecimiento del Uso del Ciberespacio

El crecimiento del ciberespacio está relacionado con el uso de las comunicaciones a través de internet, las cuales están presentes durante las 24 horas del día, los 7 días de la semana, este uso se ha convertido en una actividad tan común como comer, trabajar o dormir; toda vez, que para realizar actividades diversas como enviar correos electrónicos, enviar mensajes de texto, compartir o buscar información, trabajar en red, investigaciones académicas, actividades de esparcimiento o laborales es usual estar conectados a una red y ahora más con el boyante "Internet de las cosas" donde los dispositivos tales como refrigeradores, marcapasos o automóviles interactúan en línea de forma independiente.

El crecimiento del uso del Ciberespacio se evidencia en temas tan complejos como en operaciones quirúrgicas de corazón abierto, operaciones de socorro humanitario y hasta agricultores que usan aplicaciones móviles para acceder a datos en tiempo real.

Teniendo en cuenta el crecimiento del Ciberespacio, los gobiernos han visto todas estas tecnologías como como la fórmula para el empoderamiento y el desarrollo social. Han invertido en infraestructura para llevar la información hasta comunidades en las áreas más aisladas, bajo la premisa que el acceso al conocimiento y la creación de redes son las claves del crecimiento económico. Tanto es así que como resultado de la expansión del ciberespacio y la creciente dependencia de diversas actividades de la sociedad, el ciberespacio es reconocido por los Estados como uno de los bienes comunes globales.

El uso de la Internet a nivel mundial ha estado en crecimiento y América Latina y el Caribe no se apartan de esta tendencia En el siguiente cuadro se realiza un comparativo del uso de la Internet entre América Latina y el Caribe y América del Norte:

Tabla 5
Comparativo del Uso de la Internet entre ALC y América del Norte.

	América del Norte			América Latina y el Caribe		
Año	**Población total**	**Población con uso de Internet**	**Porcentaje**	**Población total**	**Población con uso de Internet**	**Porcentaje**
2000	312.993.944	137.339.784	43,88%	524.829.248	20.487.828	3,90%
2001	316.113.359	158.568.850	50,16%	532.173.135	30.071.793	5,65%
2002	319.050.105	188.422.049	59,06%	539.373.531	47.936.013	8,89%
2003	321.847.258	199.351.358	61,94%	546.480.559	61.682.098	11,29%
2004	324.864.038	210.753.099	64,87%	553.565.401	79.726.632	14,40%
2005	327.892.753	224.042.150	68,33%	560.677.294	93.239.456	16,63%
2006	331.014.940	229.295.551	69,27%	567.825.874	117.838.826	20,75%
2007	334.184.023	250.048.534	74,82%	574.999.132	136.291.671	23,70%
2008	337.405.012	250.578.903	74,27%	582.185.012	154.281.817	26,50%
2009	340.465.736	244.851.540	71,92%	589.352.524	182.901.455	31,03%
2010	343.418.591	249.117.507	72,54%	596.477.846	207.035.206	34,71%
2011	346.070.702	245.857.450	71,04%	603.534.610	237.469.567	39,35%
2012	348.813.722	263.436.622	75,52%	610.545.003	263.657.864	43,18%
2013	351.425.360	255.944.102	72,83%	617.492.351	285.663.588	46,26%
2014	354.173.159	263.521.885	74,40%	624.331.830	304.481.631	48,77%
2015	356.810.463	270.965.561	75,94%	631.058.524	342.536.881	54,28%
2016	359.479.269	278.741.700	77,54%	637.664.490	359.471.327	56,37%

Nota: La información se soporta con datos suministrados por los Indicadores del Desarrollo Mundial del Banco Mundial

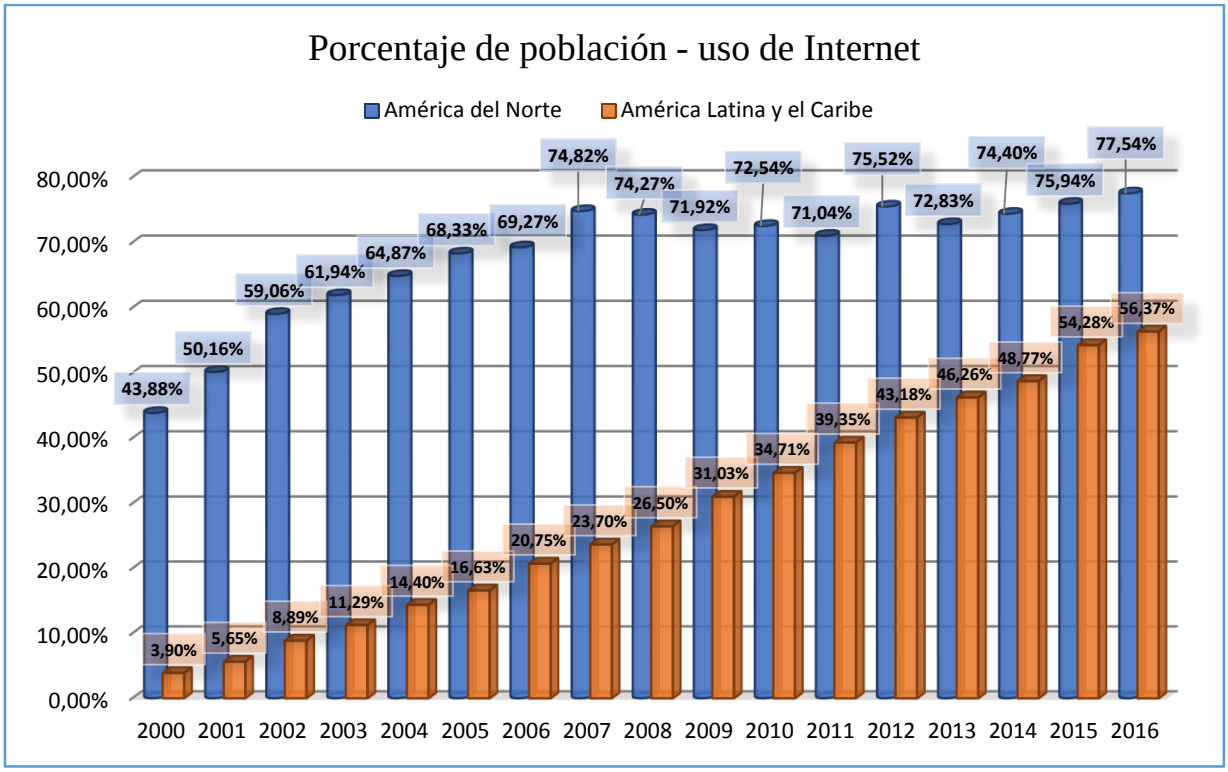


Figura 1 Comparativo del Uso de la Internet entre ALC y América del Norte
Fuente: La información se soporta con datos suministrados por los Indicadores del Desarrollo Mundial del Banco Mundial

Analizando la información de la figura anterior se puede establecer que el crecimiento del uso de la Internet durante este milenio en América Latina y el Caribe ha estado en un constante crecimiento, y el número de usuarios de Internet siguió creciendo a una tasa anual cercana al 10% (International Telecomunication Union - ITU., 2016), es importante entender que los usuarios de Internet son las personas que lo han usado desde cualquier ubicación. Internet se puede utilizar a través de una computadora, un teléfono móvil, un asistente digital personal, una máquina de juegos, un televisor digital, etc., sin embargo, este crecimiento del uso de la Internet de la totalidad de los países latinoamericanos y del caribe, no se iguala con el porcentaje de utilización de América del Norte.

Es evidente que el ciberespacio se ha convertido en una parte integral de la vida humana, no obstante su importancia no radica en la tecnología en sí, sino en el hecho que permite el acceso al conocimiento, la información y las comunicaciones; elementos cada vez más transcendentales en la interacción económica y social de la civilización actual, situación que se ve reflejada en el crecimiento y expansión mundial de los dispositivos de tecnologías de la información y comunicaciones, como computadoras y teléfonos móviles.

Y como una perspectiva particular se puede concluir que el ciberespacio es un ambiente donde la información se comporta libremente, que su uso tiene un crecimiento exponencial en cuanto al número de personas que lo utilizan y se ha convertido en una herramienta para mejorar la calidad de vida de los seres humanos, sin embargo, en esté mundo virtual, se ejecutan acciones hostiles, que afectan la que pueden enmarcarse en los conceptos de cibercrimen, ciberterrorismo o ciberguerra, con lo que es necesario proporcionar un mejor tratamiento y entendimiento de sus características e implicaciones, que una vez estructurado y formalizado este conocimiento permitirán un mayor desarrollo de las capacidades defensivas en este ámbito para lo cual los Estados han desarrollado estrategias de Ciberseguridad y Ciberdefensa para combatir este flagelo que afecta a la sociedad en todos sus niveles.

2. Ciberseguridad y Ciberdefensa

2.1. Definición

De acuerdo con la definición entregada por el doctor Jeimy J. Cano, Ph.D., miembro investigador del Grupo de Estudios en Comercio Electrónico, Telecomunicaciones e Informática (GECTI) de la Facultad de Derecho y Profesor de la misma Facultad de la Universidad de los Andes, Colombia y miembro del Subcomité de Publicaciones de ISACA, la seguridad informática es:

> La disciplina se encargaría de las implementaciones técnicas de la protección de la información, el despliegue de las tecnologías antivirus, firewalls, detección de intrusos, detección de anomalías, correlación de eventos, atención de incidentes, entre otros elementos, que—articulados con prácticas de gobierno de tecnología de información—establecen la forma de actuar y asegurar las situaciones de fallas parciales o totales, cuando la información es el activo que se encuentra en riesgo. (Cano, 2011)

Lo anterior, conlleva a la importancia de buscar diferentes medios como estrategia de protección ante las amenazas que se generan por la dependencia de la sociedad en el uso del ciberespacio.

De otra parte, la seguridad de un Estado-Nación ya no está limitada a la defensa de su soberanía y sus fronteras, sino que también debe responder por el bienestar de su sociedad frente a los nuevos riesgos y las amenazas transnacionales que la globalización provoca entre las cuales se destaca la ciberdelincuencia. Los ataques tienen motivaciones heterogéneas y dificulta la atribución de responsabilidad y reduciendo la capacidad de respuesta de los Estados víctimas de estas agresiones.

Las agresiones originadas en el Ciberespacio no tienen una consecuencia física sobre quienes son infringidas, estas tienen otro tipo de efectos sobre la vida de las personas y sobre las organizaciones. Debe tenerse en cuenta, que el ciberespacio representa, igualmente, un lugar donde puede acudir infinidad de agresores potenciales, los cuales son poco vulnerables a las medidas disuasorias, debido a que en dicho universo es más difícil el seguimiento de los delitos y la identificación de los autores, por lo que se hace posible que escapen a cualquier represalia. (Gómez de Agreda, 2012, pág. 180)

Esta preocupación es la misma que tiene la mayoría de los estados, por esta razón se observa que el gobierno estadunidense por medio del Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST) ha actualizado el marco para mejorar las infraestructuras críticas Ciberseguridad también conocido como el Marco de Ciberseguridad. El cual está enfocado a la gestión de los riesgos de la cadena de suministro cibernético, aclarando términos claves e introduciendo métodos de medición para la seguridad cibernética, y tiene como objetivo seguir desarrollando la orientación voluntaria del NIST a las organizaciones para reducir los riesgos de ciberseguridad. (NIST - National Standard Institute of Technology, 2017, pág. 1).

Lo anterior lleva a plantear que indiscutiblemente, el ciberespacio posibilita la expansión de conflictos y de amenazas a la seguridad del Estado-Nación, con lo que es necesario incurrir en mayores investigaciones que ayuden no sólo a unificar el concepto de este, sino a proporcionar un mejor tratamiento y entendimiento del mismo. De tal suerte que, con mayores conocimientos asimilados será mucho más fácil comprender sus características e implicaciones, que una vez formalizadas permitirán un mayor desarrollo de las capacidades defensivas en este ámbito.

La ciberseguridad ya no es un problema de seguridad puramente informática, es un asunto de política nacional porque el uso ilícito del ciberespacio podría obstaculizar

las actividades económicas, de salud pública, de seguridad ciudadana y de seguridad nacional y dado que los gobiernos existen principalmente para mantener el orden social, proteger las vidas y las propiedades de sus ciudadanos y permitir el comercio, por lo tanto, deben utilizar todos los instrumentos de poder nacional para reducir adecuadamente los riesgos cibernéticos. En particular, elaborando una estrategia de seguridad cibernética y fomentar la cooperación intersectorial local, nacional e internacional. (International Telecommunication Union - ITU, 2011, pág. 5)

La vida moderna depende del desempeño oportuno, adecuado y confidencial del ciberespacio. Por lo tanto, la ciberseguridad es importante para todos los Estados porque se esfuerza por asegurar que el ciberespacio siga funcionando cuando y como se espera incluso bajo ataque. (International Telecommunication Union - ITU, 2011, pág. 5)

Se puede entender que la ciberseguridad es un proceso que tiene la capacidad para minimizar el nivel de riesgo al que está expuesta la información ante amenazas o incidentes de naturaleza cibernética, cuenta con un conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger la infraestructura computacional y los activos de la información digital contenida o circulante en los sistemas interconectados.

La Globalización ha sido agente catalizador donde las Tecnologías de la información y las Comunicaciones comenzarían a definir el curso, el progreso y la dependencia de los Estados y los ciudadanos a la Internet generado un ambiente virtual sobre el cual se ha impuesto una multiplicidad de prácticas, actividades, procesos y hábitos de la sociedad, conllevando a que las herramientas que apoyan su subsistencia se interconecten y se sincronicen en un ambiente instituido sobre un código binario.

Así mismo, la configuración del ciberespacio ha proporcionado un nuevo escenario para acciones que ponen en peligro a la sociedad y al Estado, pues el empleo de ordenadores y aplicaciones informáticas para transformar, almacenar, gestionar, difundir y localizar datos necesarios para cualquier actividad humana ha hecho que se convierta en una amenaza, producto de los ataques de grupos al margen de la ley o como resultado de acciones de un actor en el marco de un conflicto regular.

La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos y de los usuarios contra los riesgos de seguridad correspondientes en el ciberespacio, para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información, que permite la prevención, detección, reacción o respuesta, e incluye elementos de aprendizaje para la mejora continua del propio proceso.

La ciberseguridad surge ante el creciente uso del ciberespacio y se constituye en un elemento esencial para permitir que todas las partes interesadas de una sociedad, como lo son los ciudadanos, las organizaciones e instituciones puedan beneficiarse del uso del ciberespacio explotando las interacciones sociales de forma rápida y económica, resultado de la revolución de la tecnología de la información y comunicación, lo cual ha acelerado el proceso de globalización.

2.2. Riesgos, Amenazas y Vulnerabilidades de la Seguridad Digital

Es claro que la revolución tecnológica es clave para la transformación de las sociedades y modos de vida, sin embargo, el desarrollo tecnológico está asociado a una mayor exposición a nuevas amenazas en el ciberespacio, las cuales agudizan varias de las vulnerabilidades del sistema de seguridad de un Estado-Nación, lo que conlleva a la exigencia de una mejor protección de las redes y sistemas, así como de la privacidad y

los derechos digitales de los diferentes actores de la sociedad. Esta realidad no es ajena a los países Latinoamericanos y del Caribe, por esta razón los Estados deben adaptarse a esta transformación permanente del mundo digital y la hiperconectividad actual, para lo cual es necesario realizar evaluaciones a los controles implementados para mitigar los riesgos cibernéticos y con el fin de garantizar la seguridad de las partes interesadas que convergen en la sociedad.

Es importante mencionar, que la administración de los riesgos asociados a las tecnologías de la información es muy compleja, toda vez que la amenaza cibernética tiene múltiples aspectos y sin lugar a duda potencialmente peligrosas. Sobre esto, Gastón (Gastón Sack & Ierache, 2015, págs. 1-3) llama la atención sobre las características asimétricas que tiene el espacio y que lo convierten en algo más complejo de definir y de defender, mencionando: 1) La inteligencia y el engaño son aspectos críticos en el ciberespacio; 2) el ciberespacio es extenso y fácil esconderse en el mismo; 3) los efectos que producen los ataques son desproporcionados de cara a las herramientas que se utilizan para producirlos.

En este contexto, la prestigiosa revista británica The Economist, tituló la portada "Cyberwar. The thread from the Internet", en el primer número del mes de julio de 2010, destacando que era el momento para que los países comenzaran a dialogar sobre el control de las armas cibernéticas en Internet, en uno de sus artículos titulado "Ciberguerra: Guerra en el quinto dominio" (The Economist, 2010), analiza más detenidamente el ratón y el teclado de una computadora como las posibles "armas cibernéticas" del mundo en que vivimos, sus amenazas y los riesgos que conllevan.

Los espacios comunes globales como el ciberespacio, caracterizado por su fácil acceso, débil regulación; y, de difícil control se encuentran innumerables riesgos y amenazas entre los que se cuentan estados extranjeros, conflictos, amenazas internas,

sabotaje, individuos aislados, organizaciones terroristas, delincuencia, hacktivistas, crimen organizado, espionaje, fenómenos naturales, terrorismo, hacking, entre otros que se deben controlar y evaluar para mitigar las consecuencias de su impacto en dado caso que se materialice el riesgo.

2.2.1. Riesgos de la seguridad digital.

A pesar de la creciente inversión en seguridad de tecnologías de la información, las amenazas de ataques de origen cibernético continúan creciendo, a consecuencia que la sociedad, en todos sus niveles y sectores, subestiman los riesgos de origen cibernético y continúan ejecutando medidas de control para defenderse de las ciber amenazas del pasado, en cambio los ciber delincuentes usan las últimas tecnologías y están enfocados en innovar, desarrollar, investigar, estudiar, y aprovechar las vulnerabilidades del futuro.

Los riesgos de seguridad digital están estrechamente relacionados con el uso de las tecnologías de la información y comunicaciones enfocada a los activos digitales, las operaciones y la información.

De acuerdo con lo publicado en el documento "Ciberseguridad una guía de Supervisión" del Instituto de Auditores Internos de España, los principales riesgos cibernéticos a los que se exponen todos los usuarios del ciberespacio se pueden clasificar de la siguiente manera: (Instituto de Auditores Internos de España, 2016, pág. 9 y 10)

Tabla 6
Riesgos de la Seguridad Digital.

Riesgo Cibernético	Descripción
Fraude Financiero	Las instituciones y entidades financieras son uno de los principales objetivos de los ciber delincuentes. El robo económico representa una de las principales motivaciones de la gran mayoría de ciber atacantes.
Robo de información	La información de carácter personal o documentos clasificados son algunos de los principales activos de información que deben ser

Riesgo Cibernético	Descripción
	especialmente protegidos. La filtración pública o pérdida de la información confidencial es un riesgo elevado, cuyos impactos o pérdidas pueden resultar especialmente significativos.
Indisponibilidad de servicios	Es la interrupción puntual o prolongada de los servicios ofrecidos en línea como por ejemplo correos, pagos financieros, cobro de impuestos, registros públicos, entre otros.
Sabotaje de infraestructuras	Son los ataques contra los servicios o infraestructuras críticas de un país o estado, provocando desabastecimientos, o interrupciones de comunicaciones, etc. con el objetivo de provocar una paralización puntual o prolongada de los mismos.
Pérdida de reputación	Es una de las principales consecuencias de las agresiones cibernéticas y el objetivo de gran parte de los ciberataques, cuyos efectos pueden resultar altamente significativos.

Nota: Adaptado del documento "Ciberseguridad una guía de Supervisión" del Instituto de Auditores Internos de España (Instituto de Auditores Internos de España, 2016, pág. 9 y 10)

2.2.2. Amenazas de la seguridad digital.

A través de los últimos años las amenazas cibernéticas han estado en constante evolución de pasar a ser una molestia para los usuarios como lo son los virus, gusanos, troyanos, entre otros a convertirse en herramientas potencialmente dañinas, han evolucionado hacia ataques de denegación de servicios DDoS y sofisticados softwares maliciosos -malware hasta llegar a las amenazas persistentes avanzadas APTs o ataques dirigidos, que combinan múltiples técnicas de ataque y explotación de diferentes tipos de vulnerabilidades, incluyendo el uso de técnicas de ingeniería social por ejemplo spear-phishing, así como una fase previa de estudio y recolección de información del objetivo que los hace mucho más eficaces, dañinos y ampliando considerablemente el abanico de víctimas. (Instituto de Auditores Internos de España, 2016)

Las ciber amenazas se pueden clasificar en dos, contra la información y contra la infraestructura TIC (Instituto de Auditores Internos de España, 2016, pág. 10 y 11)

Tabla 7
Clasificación de Ciberamenazas

Amenaza	Descripción	Ejemplos
Contra la información	Las materializaciones de estas ciber amenazas provocan una pérdida, manipulación, publicación o uso inadecuado de la información.	• Espionaje, desde el ámbito del espionaje de Estado al espionaje industrial. • Robo y publicación de información clasificada o sensible (datos personales, datos bancarios). • Robo de identidad digital. • Fraude.
Contra la infraestructura de Tecnologías de la Información y Comunicaciones	Son aquellas cuya materialización pueden provocar la interrupción temporal, parcial o total de determinados servicios o sistemas	• Ataques contra infraestructuras críticas. • Ataques contra las redes y sistemas. • Ataques contra servicios de Internet. • Ataques contra sistemas de control y redes industriales. • Infecciones con malware. • Ataques contra redes, sistemas o servicios a través de terceros.

Nota: Adaptado del documento "Ciberseguridad una guía de Supervisión" del Instituto de Auditores Internos de España (Instituto de Auditores Internos de España, 2016, pág. 10 y 11)

2.2.3. Principales técnicas de ataque y vulnerabilidades de la seguridad digital.

Las principales técnicas de ataque están enfocadas y en las que cuentan con mayores esfuerzos para contrarrestarlas de la ciberseguridad, se pueden clasificar en las siguientes tres:

1. El ciber crimen, que incluye actores individuales o grupos que dirigen ataques a sistemas para obtener ganancias financieras.
2. La ciberguerra, que a menudo involucra recopilación de información con motivaciones políticas.
3. El ciber terrorismo, cuyo propósito es comprometer los sistemas electrónicos y causar pánico o temor.

Partiendo de lo anterior se puede clasificar que los principales ciberataques se encuentran clasificados en diferentes formas así:

1. Ataques a plataformas propias en forma de DDoS, hacking o de explotación de vulnerabilidades en el hardware y software corporativo.
2. Ataques fuera del perímetro, como los dirigidos a clientes utilizando phishing, malware, credenciales robadas.
3. Ataques a activos intangibles, tales como la reputación de la marca o de los directivos.
4. Ataques a activos físicos o infraestructuras críticas.
5. Ataques basados en el fraude económico y en la fuga de información confidencial tales como filtraciones, robos o perdidas de dispositivos.

En la siguiente tabla se presenta las principales técnicas y vulnerabilidades de la seguridad Digital, la cual fue construida con base en la información suministrada en las buenas prácticas de gestión de riesgos del Instituto de Auditores Internos de España en el documento denominado "Ciberseguridad una guía de Supervisión": (Instituto de Auditores Internos de España, 2016)

Tabla 8
Técnicas de Ataque y Vulnerabilidades

Técnicas de Ataque y Vulnerabilidades	**Descripción**
Ingeniería Social	Técnicas y habilidades sociales o psicológicas para obtener información confidencial a través de la manipulación de las personas o usuarios.

Técnicas de Ataque y Vulnerabilidades	**Descripción**
Fingerprinting	Búsqueda y recolección de todo tipo de información del objetivo, principalmente en Internet, y realizada de manera pasiva, que pueda ser utilizada en la perpetración de un ataque. Puede incluir tanto la recolección de información de fuentes públicas (OSINT: Open-Source Intelligence), como de fuentes privadas o de pago.
Enumeración y Escaneo	Identificación de sistemas, equipos y dispositivos existentes en la red. Obtención de nombres de equipos, usuarios, recursos compartidos, etc. También incluye habitualmente la identificación de posibles vulnerabilidades.
Ataques de días cero (0-day)	Ataques contra aplicaciones o sistemas que aprovechan nuevas vulnerabilidades, desconocidas por los fabricantes del producto y/o software, y para los que no se han desarrollado aún "parches" o soluciones que las corrijan Estos ataques pueden tener un grave impacto, y el código para explotar dichas vulnerabilidades se vende a menudo por elevadas cantidades de dinero en el denominado mercado negro de los exploits.
Spam y Phishing	Ataques a través del servicio de correo electrónico, ya sea buscando la indisponibilidad del mismo o la suplantación de identidad para obtener información confidencial de los usuarios. Durante los últimos años las técnicas de phishing han evolucionado enormemente dada su simplicidad y alta efectividad, y es habitual hablar de ataques concretos de smishing, vishing, spear phishing, etc.
Hijacking	Técnicas ilegales utilizadas por los atacantes para adueñarse o tomar el control de diferentes recursos: navegador, credenciales de sesión, conexiones TCP/IP, páginas web, etc.
DDos (Denegación de servicios)	Ataques de desbordamiento con el objetivo de provocar la parada o interrupción de un servicio crítico, típicamente realizados a través de una inundación de peticiones a páginas web.
SQL Injection	Técnica de ataque sobre páginas web que a través de la ejecución de comandos SQL, permite la obtención y/o manipulación de información de la base de datos del servidor.

Técnicas de Ataque y Vulnerabilidades	Descripción
Cross-Site Scripting (XSS):	Técnicas de inyección de código (principalmente Javascript y PHP) que, aprovechando errores de programación en las páginas web, provocan un comportamiento anormal del sistema a pudiendo afectar a la integridad del mismo
Virus, malware, gusanos y troyanos	Software o código malicioso que tiene como objetivo infiltrarse o dañar un sistema o equipo, estando además normalmente diseñados para su rápida propagación en una red de ordenadores. Especialmente extendido se encuentra el uso de troyanos, cuya apariencia simula la de un programa benigno o inocuo que, tras ser ejecutado por el usuario, ocultan y liberan el virus contenido en él.
Botnet (redes zombis)	Conjunto de ordenadores (conectados a Internet) infectados que se ejecutan y controlan de manera autónoma y automática. Estas redes son usadas principalmente para aumentar la capacidad de procesamiento necesaria para perpetrar un ataque, así como para ocultar el origen y autoría del mismo.
Rootkits	Herramientas y programas usados para esconder la presencia del intruso, obteniendo privilegios de administración que permitirán la manipulación futura del sistema.
APT (Amenaza persistente avanzada)	Ataques especialmente diseñados y dirigidos contra una organización o entidad concreta. Por lo general requieren de un elevado tiempo de preparación y combinan diferentes técnicas y vulnerabilidades de entre las ya comentadas anteriormente.

Nota: Adaptado del documento "Ciberseguridad una guía de Supervisión" del Instituto de Auditores Internos de España (Instituto de Auditores Internos de España, 2016, pág. 13 a 15)

Es importante precisar que el éxito de estas técnicas se basa en la detección y existencia de errores en la configuración de seguridad de los sistemas, obsolescencia o falta de modernización de las infraestructuras tecnológicas, y fallos de programación o diseño en las arquitecturas de seguridad y comunicaciones, cuya identificación y mitigación debe considerarse una prioridad por las entidades y organizaciones. (Instituto de Auditores Internos de España, 2016, pág. 15)

Otro aspecto para tener en cuenta, es la poca conciencia, culturización y educación que se tiene en cuanto a la seguridad digital; toda vez que un gran participación de los ciberataques podrían prevenirse al ejecutarse una serie de medidas sencillas de buenas prácticas en redes y equipos, ya que el mayor porcentaje tienen su origen en vulnerabilidades ya conocidas y para las que se dispone de soluciones y medidas de detección y mitigación que suelen incluir el uso de contraseñas seguras, configuraciones de seguridad adecuadas, correcta gestión del control de accesos a aplicaciones y datos, y un apropiado nivel de actualización de los sistemas. (Instituto de Auditores Internos de España, 2016, pág. 15 y 16)

Por los anteriores aspectos es por lo que organismos internacionales como la OTAN, la ONU y la OEA han estado en el proceso de la construcción de modelos de Ciberdefensa y Ciberseguridad con el fin de salvaguardar los activos de información, infraestructura critica, la economía y las personas en el ciberespacio.

Para adelantar dichos esfuerzos e iniciativas se han adelantado convenios internacionales como el adoptado el 23 de noviembre de 2001 en Budapest, llamado "Convenio Sobre la Ciberdelincuencia", en la cual los estados miembros han fortalecido la seguridad digital y han creado políticas de cooperación, colaboración y asistencia a otros países de diferentes regiones y del sector privado, fortaleciendo la ciberseguridad a nivel global. Dichos países se han unido en contra de la ciber criminalidad fortaleciendo las regulaciones en materia procesal y penal.

2.3. Tipología de los Ciber delitos

Considerando el aumento en la última década de dispositivos, sistemas redes y los servicios tecnológicos mundiales, de igual manera las ciber amenazas se encuentran en constante crecimiento, razón por la cual se debe evaluar los requisitos de las bases

jurídicas solidas de la ciberseguridad con el fin de tipificar aquellas conductas que violentan y afectan la seguridad de los sistemas informáticos y de sus usuarios.

Los ciberataques se llevan a cabo con fines tales como robo y/o manipulación de información o para detener y/o causar el mal funcionamiento de los sistemas. Los métodos para el ataque cibernético son diversos. Los ejemplos incluyen la introducción de malware, el envío de grandes cantidades de datos para sobrecargar un sistema o el acceso ilegal a los sistemas.

El ciber crimen es una industria en crecimiento, para los ciber delincuentes los retornos son excelentes y los riesgos son bajos, esta afirmación se puede ratificar con los datos extraídos del estudio realizado en el 2011 por Symantec Internet Security Threat Report - The Norton Cybercrime Report (Informe de Ciber crimen de Norton 2011), en el cual se calcula que cada segundo catorce adultos se convierten en víctimas del delito cibernético, lo que da como resultado que diariamente más de un millón doscientos mil personas a nivel mundial son víctimas de los ciber delincuentes; adicionalmente el estudio de Norton calcula que las pérdidas globales sufridas por actos de ciberdelincuencia ascienden a más de $ 114 mil millones de dólares anuales. (Symantec Internet Security , 2011).

Lo anterior, es decir, la utilización de la tecnología como una herramienta con fines delictivos, conllevo que los principales organismos internacionales hayan recomendado a los Estados acondicionar las legislaciones nacionales para adaptarlas a los nuevos retos que plantea el entorno digital, con el fin de hacerle frente a las diferentes tipologías de los ciber delitos.

En la siguiente tabla se realiza una aproximación a la tipología el ciber delito, la cual podría ser de ayuda para reglamentar la legislación ante las nuevas amenazas de

seguridad que contempla la siguiente clasificación: (Unión Internacional de Telecomunicaciones - UIT, 2014, p. 12).

Tabla 9
Tipología de los Ciberdelitos.

Tipología de los Ciberdelitos	Actividades que violentan y afectan la seguridad de los sistemas informáticos y de sus usuarios
Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.	•Acceso ilícito: piratería de sistemas y programas. •Espionaje de datos. • Intervención ilícita. •Manipulación de datos •Ataques contra la integridad del sistema
Delitos relacionados con el contenido.	•Material erótico o pornográfico (excluida la pornografía infantil). •Pornografía infantil •Juegos ilegales y juegos en línea •Difamación e información falsa •Correo basura y amenazas conexas •Otras formas de contenido ilícito
Delitos en materia de derechos de autor y de marcas.	•Delitos en materia de derechos de autor. •Delitos en materia de marcas. •Delitos informáticos •Fraude y fraude informático. •Falsificación informática. •Robo de identidad. •Utilización indebida de dispositivos.
Combinación de delitos.	•Ciberterrorismo. •Guerra informática. •Ciberblanqueo de dinero. •Phishing.

Nota: Adaptado del documento Comprensión del Ciberdelito: Fenómenos, dificultades y respuesta jurídica (Unión Internacional de Telecomunicaciones - UIT, 2014, pág. 12)

La anterior clasificación es bastante general, sin embargo, es acorde a las categorías descritas en el Convenio sobre la Ciberdelincuencia de Budapest y resultan

útiles para la necesaria reacción jurídica, la cual se convierte para la jurisprudencia en un constante desafío a vencer a razón de la permanente evolución tecnológica, así como la variedad, multiplicidad y complejidad de los métodos que se emplean los ciber delincuentes para cometer los ciber delitos.

En este capítulo se puede concluir que la ciberseguridad es un proceso que tiene la capacidad para minimizar el nivel de riesgo al que está expuesta la información ante las amenazas o incidentes de origen cibernético; que los riesgos, las amenazas y las vulnerabilidades a las que se enfrenta son complejas, para lo cual los Estados se han enfocado en desarrollar estrategias de seguridad digital que incorporan la cooperación, colaboración y asistencia mutua internacional y han empezado a adaptar su legislación ante las nuevas amenazas cibernéticas y la clasificación de las diferentes tipologías de ciber delitos, con el fin de realizar su aplicación a los ciber delincuentes.

Ciberdefensa, factores de contextuales

La ciberdefensa es un concepto que ha venido en evolución constante. Su naturaleza yace en la rápida transmutación de las amenazas que afronta. Para Cubajante Bahamón, Prieto y Quiroga (2020), quien cita a Singer y Friedman (2014), la ciberdefensa es el resultado de procesos tecnológicos cambiantes, en estructura y sistema funcional.

Al hablar de ciberdefensa también se hablaría de protección en el ciber-espacio. Para Cujabante et al. (2020):

> El dominio del ciberespacio fue una carrera iniciada por las grandes potencias como Rusia, Estados Unidos y China, que por ello son un punto de referencia para la creación de instrumentos que salvaguarden la seguridad y la defensa nacional en el ciberespacio (p. 1).

Tanto ciber-defensa como ciberespacio son dos conceptos correlacionados e inter-dependientes. El tema ciber se centra principalmente en la protección de sistemas de información e infraestructuras cibernéticas estatales. Esto quiere decir, que la función de la ciber defensa nacional es anticipar y prevenir cualquier tipo de ataque cibernético que afecte a la estructura de seguridad y defensa nacional.

La rapidez del mundo ciber centrado en internet, interacciones digitales y otro tipo de acciones conexas al mundo digital, trajeron consigo el surgimiento de nuevos fenómenos criminales; ciber-amenazas y ciber-delitos para el caso (Cubajante, et al., 2020).

La ciber-defensa como contraposición para el ciber terrorismo halla en la concertación de estrategias de anticipación e intervención, ventajas estratégicas de naturaleza digital. Concepto ciber en la óptica de lo estatal proteccionista entre en el campo de las ciencias militares y demás acciones diseñadas para resguardar al Estado.

Una postura interesante, y de facto la que se utilizará para delimitar los resultados es la que presenta (Díaz, 2010). Para este autor hay elementos que son indispensables, y su importancia sobresale entre otros. La detección en tiempo real y la aplicación de ciber-inteligencia al tema de ciberdefensa, son indispensables.

Desde su perspectiva, la estrategia de ciberdefensa debe establecer en pro de los últimos acontecimientos de contexto, toda vez que esos componentes son los impulsan el continuo desarrollo tecnológico.

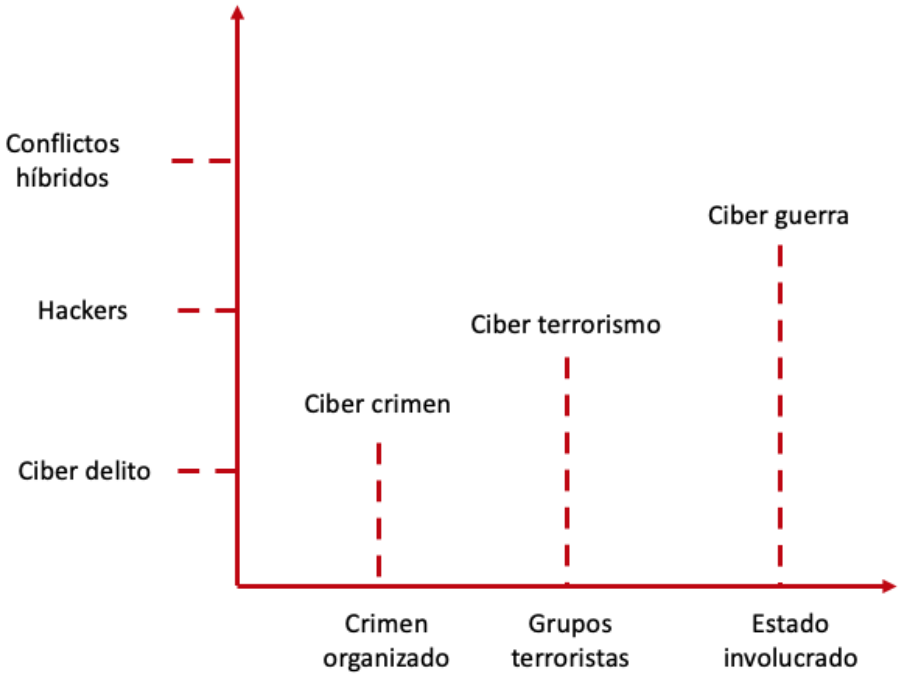
De la misma forma, Díaz (2010) explica que los ciberataques no solo tienen motivaciones intelectuales o económicas, también son políticas, y por eso su evolución depende de los intereses que otros actores delictivos han demostrado. Llama la atención que Díaz (2010) confirma esa relación que existe entre el crecimiento de los ciber ataques, y el aumento del número de usuarios conectados a la red.

Ese hecho convierte a la categoría “ciber amenazas”, en un fenómeno delictivo que en muchas ocasiones se asocia al ciber-terrorismo, y por ende al campo de la guerra híbrida (Danyk, Maliarchuk, & Briggs, 2017). La percepción que Díaz (2010) sostiene acerca de las ciber-amenazas, es que estas se van entrelazando con aspectos básicos del contexto cotidiano. Por ejemplo, con sistemas de información financieros, culturales, políticos y económicos.

Tanto ciber-defensa como ciber-terrorismo dependen del grado de conocimiento que los actores tienen. El conocimiento en materia cibernética es fundamental para estructurar procesos a favor o en contra de la estructura de seguridad y defensa nacional. No obstante, la mayoría de actuaciones internacionales vigentes se han expuesto fenómeno cibernéticos delictivos con gran capacidad expansiva, pero sobre todo, por su característica primaria: la transformación frecuente de sus formas de impacto.

El cambio constante presentado por las ciber amenazas, así como la formación de nuevas estructuras delictivas, creó las condiciones necesarias para reconocer que factores hostiles como el ciber terrorismo, en efecto, podrían crear escenarios que se adaptan al concepto “ciberguerra”. Para continuar con esta explicación es conveniente analizar la siguiente figura:

Figura 2 Elementos criminales tipo ciber



Fuente: elaboración propia con información recuperada de Díaz (2010)

Antes de pasar a la etapa ciberguerra, el ciberterrorismo presenta manifestaciones asociadas a la organización de grupos criminales y otro tipo de delincuentes independientes. Surgen en el contexto amenazas cibernéticas complejas, las cuales evolucionaron a la par de los sistemas de información y tendencias digitales.

En la investigación que se titula *Concientización de la situación de Ciber defensa*, publicada por Barford (2010), hay puntos de vista con los que se llega a comprender que el tema de ciber empieza con la concientización de usuarios o unidades digitales.

Dicha concientización encaja en el término compuesto *aceptación cultural*. Es decir, al depender directamente de sistemas tecnológicos, la ciber defensa hallaría en la conducta preventiva del usuario digital un factor aventajado ausenta en la estrategia de los ciber-atacantes.

La cultura del usuario digital es fundamental entonces para anticipar afectaciones no solo a una infraestructura crítica cibernética, sino al usuario mismo; y resulta menester poner en consideración que, en el caso colombiano, el principio constitucional de los entes

encargados de la defensa nacional es resguardar y proteger instituciones y personas parte del territorio.

Una misma postura es compartida por Denning (2014). Para este autor, la ciber defensa es el resultado de cuatro pasos o procesos, los cuales integran un espacio multidimensional en el que se debe identificar: el alcance de los efectos internos y externos, el nivel de cooperación que poseen las amenazas y los aliados estratégicos, el tipo de efecto y la naturaleza desagregada de la automatización (Denning, 2014, p. 10).

En tanto, la ciber defensa como modelo de protección debe contar con principios básicos que faciliten la erogación de estrategias tecnológicas, pero también protocolares y procedimentales.

La ciber-defensa vista como un interés geo-estratégico del Estado es otra de las discusiones presentes para comprender este tema. La ciber defensa se convierte en un interés del Estado cuando el espacio cibernético empieza a generar algún tipo de afectación al sistema estatal público o población *per se*. Mírese la siguiente afirmación para comprender esta postura:

> La ciberseguridad es un aspecto cada vez más importante para el correcto funcionamiento de las empresas, los gobiernos y las sociedades en general. Sin embargo, junto a los avances tecnológicos de la Cuarta Revolución Industrial se incrementa el número y la forma de amenazas en el ciberespacio. Una de esas amenazas es la que provienen de otros Estados, o de Estados coludidos con actores no estatales para vulnerar alguna capacidad de un tercer Estado. Al tratarse de intereses y capacidades estatales en juego, el concepto de ciberseguridad evoluciona al concepto de ciberdefensa (Rossi, 2021, p. 12).

La interpretación de Rossi (2021) amplía el espectro de entendimiento, pues la autora extiende la necesidad ciber-proteccionista a otros actores como el gobierno y la sociedad. Significa esto que el proceso de defensa digital depende de la capacidad que posea el Estado para resguardar sus sistemas críticos de información, pero también para proteger su población civil.

Tal necesidad, protección a la población civil, no solo se limita a la seguridad sobre los sistemas funcionales digitales independientes, sino también a todos aquellos sistema y estructuras necesarias para las garantías de vida y subsistencia del actor poblacional: hospitales por ejemplo o centros de abastecimiento.

Cualquier tipo de afectación a este tipo de infraestructuras es, o podría considerarse ciberterrorismo (Harries & Yellowlees, 2013). Entonces, hay que aceptar cuan dependiente es el desarrollo social actual de los sistemas digitales o sistemas de información.

Por ejemplo, para (Lee, Choi, Shandler, & Kayser, 2021), el ciber terrorismo, como factor de afectación a sistemas de información es disperso, pero posee redes de intercomunicación que se encargan de desarticular, analizar e identificar blanco abiertos con un alto nivel de afectación.

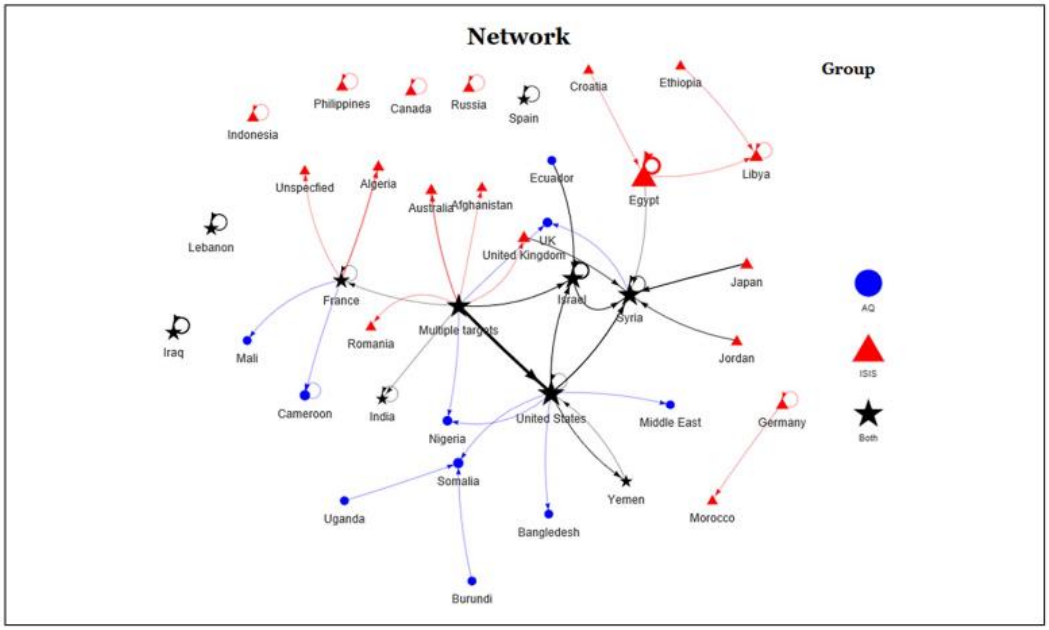
Para Lee *et al* (2021), el surgimiento del ciberterrorismo como fenómeno delictivo no solo tuvo lugar en la concentración de acciones tecnológicas definidas desde el interés de lo político o económico, pues su naturaleza es flexible y depende de los intereses presentados actor amenazante. En el caso que presentan Lee et al (2021), el ciber-terrorismo emerge como una herramienta para la dispersión del miedo (factor de cohesión) y como un instrumento con fines geoestratégicos utilizadas por el Estado Islámico y por Aqueda.

El ciber-terrorismo estructurado por ISIS o Alqueda no está en el orden de los ataques con medios y fines tecnológicos. Todo lo contrario, se encuentra en una categoría compleja en la que el concepto tecnológico pasa a ser una técnica de hipermediatización de informaciones visuales o auditivas, pero no un instrumento que afecte de forma directa a sistemas de información y otros escenarios virtuales de interés para uno o varios Estados.

El estudio presentado por Lee *et al* (2021) confirma que la estimación de acciones o la configuración de medidas de prevención no depende exclusivamente de lo tecnológico especializado, dando así razón a las ideas presentadas por Díaz (2010) y Denning (2014), con las que se entiende al ciberterrorismo como acción predeterminada que depende de factores humanos. Para el contexto, el fin de estos grupos terroristas fue crear redes de retransmisión de mensajes por las que viajaron grandes volúmenes de información, cuya caracterización primaria fue la recreación de escenas visuales, generando algún tipo de transgresión a los derechos humanos o derecho internacional humanitario.

Un resumen gráfico de esta afirmación se puede evidenciar en la figura 2.

Figura 3 Redes de Alqaeda y ISIS en las que se presentaron casos de ciber terrorismo.



Fuente: información recuperada de Lee et al (2010)

Si el ciber terrorismo ha evolucionado en aspectos ajenos al campo de lo tecnológico, la ciberdefensa también. El término ciber-defensa no refiere *strictu sensum* a esa conformación de estrategias en las que el concepto tecnológico sistemático ocupa un puesto fundamental. Si bien es importante, otras técnicas de prevención que regulan el tema ciber salen a la luz. Una de esas técnicas es lo que (Zhang & Vrizlynn, 2021) llama *el engaño*.

Para estos autores, la ciberdefensa desde los años 80 ha basado parte del sistema funcional en protección autónoma o desarrollo de técnicas para la desviación del blanco. La contribución de Zhang y Vrizlynn (2021) cobra sentido cuando se empieza a comprender que una estrategia ciber se basa en el estudio de experiencias pasadas y en la concertación de hipótesis de futuro, las cuales, poco obedecen a la realidad de los escenarios por venir.

Una muestra que respalda esta afirmación es que anualmente el número de ciber ataques aumenta. Para el año 2021, se registró un incremento en Estados Unidos[3] del

[3] Se propone como referencia a Estados Unidos, ya que su Agencia de Seguridad y Ciber seguridad para la Infraestructura crítica es un referente.

167% (Sánchez, 2016). Uno de los datos preocupantes es que la Agencia para la Seguridad y Ciberseguridad de Infraestructura Crítica Americana (2021) explicó que gran proporción de esos ciber ataques se dirigía hacia infraestructura necesaria para la subsistencia del actor poblacional. En tanto, cualquier tipo de afectación configuraría un ataque terrorista de tipología premeditada.

Los métodos de afectación son varios, y acá el factor humano, aunque importante pasa a un segundo plano. Según la CISA (2021), las tendencias relativas a un ciberataque oscilan entre el acceso a nuevas redes de información a través de métodos tradicionales como el Pishing o el robo de credenciales, al uso de métodos tecnológicos que buscan extraer información de escenarios digitales atados a la nube o mediante ataques a sectores industriales con importancias macro-económicas.

Hasta este punto se desarrolló un análisis somero de los diferentes aspectos funcionales, estructurales y conceptuales que rodean los términos ciber defensa y ciber-terrorismo. Numerosas conclusiones salieron de este análisis; quizá la más importante una caracterización actual del comportamiento de las ciber amenazas que conducen al ciber-terrorismo.

El ciber terrorismo como escenario previo a la ciberguerra ha cambiado. Es decir, tratar acerca de la estrategia de ciber defensa o estudiar las amenazas cibernéticas de años anteriores resultaría poco útil, pues su estructura tecnológica y su forma funcional transmutan a la par, no del tiempo, sino de nuevas invenciones tecnológicas que tengan relación o interacción con un usuario digital.

Sin embargo, entender al ciber terrorismo como un hecho tangible, y no como un instrumento o medio de coerción, deja de lado experiencias pasadas conexas a la utilización de un sistema digital como un método de dispersión y rápida difusión de información con fines terroristas.

Por lo tanto, hay que comprender que por ciber terrorismo debe entenderse a toda acción que busca generar afectación o impacto a la infraestructura crítica cibernética de la nación, mientras que ciber defensa una contraposición procedimental y tecnológica cuyo objetivo es anticipar o prevenir afectación macro a los sistemas públicos – digitales de un Estado.

Análisis conceptual de la infraestructura crítica cibernética de la nación.

Para entender qué es infraestructura crítica cibernética de la nación es necesario poner en consideración dos aspectos. Primero, por infraestructura cibernética debe entenderse a todo aquel sistema de información que tenga relación con la administración de formas y/o componentes tecnológicos sujetos al procesamiento datos de interés nacional con tipología estratégica. Segundo, la administración del sistema de información cibernético debe darse en pro del control, resguardo y anticipación de acciones que pongan en riesgo el correcto proceder de portafolios tecnológicos o de procesos integrados en los que interactúe el ser humano con un dispositivo tecnológico que cumple roles y misiones de interés nacional.

Así los términos, podría decirse que la infraestructura crítica cibernética de la nación, de ahora en adelante ICC, es objetivo nacional que busca dar continuidad a procedimientos de naturaleza estatal cuyos fines son sociales y gubernamentales. Una definición concreta a este tema, dada desde el argot de la institucionalidad colombiana es la siguiente:

> (…) infraestructura crítica cibernética de nacional es aquella soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado. Su afectación, suspensión o destrucción puede generar

> consecuencias negativas en el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las organizaciones e instituciones, así como de la administración pública (Ministerio de Tecnologías de la Información y las Comunicaciones, 2020, p. 12).

La descripción dada por el MINTIC (2020) explica que la ICC se basa groso modo en el funcionamiento de sistemas cibernéticos que tienen un objetivo: asegurar el funcionamiento de redes digitales con las cuales controlar o supervisar un proceso gubernamental y estatal *per se*. Una postura similar, pero que se enfoca más hacia la explicación de ICC como estrategia de anticipación y no de reacción es la que ofrecen Realpe y Cano (2020).

Para estos autores, la estrategia de seguridad para una ICC debe partir con un antecedente: establecer cuáles son las posibles vulnerabilidad y vacíos funcionales o GAPS que surgen del flujo de información actual y de sus medidas de control y prevención.

La perspectiva que manejan Realpe y Cano (2020), expone entonces una prioridad circunstancial: comprender que el ciber espacio es un escenario aún no comprendido por muchos actores, entre los cuales están incluidos los organismos de seguridad y defensa nacional. Significa esto que el desarrollo de medidas para la protección puede ralentizarse por la cantidad de cambios y actualizaciones constantes que afecten el sistema de seguridad para el resguardo de datos e informaciones compuestas.

De ahí surge esa necesidad primaria: conocer qué o cuáles son los presupuestos estratégicos y analizar en sectores o sobre que procesos el sistema no es fuerte, útil o tecnológicamente adecuado para detener el avance de los ciber ataques.

Al respecto, Realpe y Cano (2020) realizan un ejercicio muy importante en cuanto al estudio de antecedentes e identificación de posibles necesidades. En su artículo titulado

Amenazas Cibernéticas a la Seguridad Nacional, Reflexiones y Perspectivas, los autores correlacionaron los objetivos planteados en el CONPES 3701 de 2011 con el análisis DOMPILEM que trae la doctrina estandarizada. Los resultados adquiridos se evidencian en la siguiente tabla:

Tabla 10 Análisis DOMPILEM

OBJ.	***D Doctrina***	***O Organización***	***M Material***	***P Personal***	***I Instalaciones***	***L Liderazgo***	***E Entrenamiento***	***M Mantenimiento***
OE1	Manuales conjuntos y por Fuerza	Un nuevo componente militar	Hardware Software	Militar y Civil	Oficinas Laboratorios Salas	Estrategas Expertos Especialistas Técnicos	Persistente	Plataformas Cibernéticas
OE2	Planes de Protección	Equipos interdisciplinarios	Plataformas compartidas	Militar y Civil	Propias y de terceros	Expertos en activos estratégicos sectoriales	Sistemas Control Industrial TI TO	Sistemas de Defensa Cibernética
OE3	Manual Operaciones Cibernéticas	Equipos de Batalla	Equipo de combate cibernético	Comandos Cibernéticos	Sala Mando y Control cibernético	Plan de Carrera Cibernética	Simulación Olimpiadas Cibernéticas	Plataformas de Operaciones Cibernéticas
OE4	Manual de Apoyo Cibernético	Conformación Ligas	Especializado Alto Nivel	Sector Público y Privado	Salas de Intercambio Cibernético	Expertos Cibernéticos	Entrenamiento Interinstitucional	Sistemas de Apoyo
OE5	Acuerdos, convenios	Nacionales Internacionales	Especializado Alto Nivel	Nacional e Internacional	Propia y de Terceros	Internacionalistas	Cursos Internacionales	Sistemas de Intercambio

Fuente: elaboración propia

Se observan 40 hallazgos. Los más significativos para el objeto de esta investigación son el desarrollo de planes de protección, la adquisición de equipo especializado y el entrenamiento y capacidad para el recurso humano. Esos tres hallazgos representan una línea de vacíos funcionales que ponen riesgo el marco estructural desarrollado para proteger la ICC.

Así como Realpe y Cano (2020) exploran iniciativas para el mejoramiento de la estrategia concretada a través de los tres CONPES subsecuentes, Anbalón y Donders (2014) entran al debate para explicar dos puntos de vista con los que se realiza una revisión del concepto ciberdefensa a partir de la categoría *infraestructura crítica*.

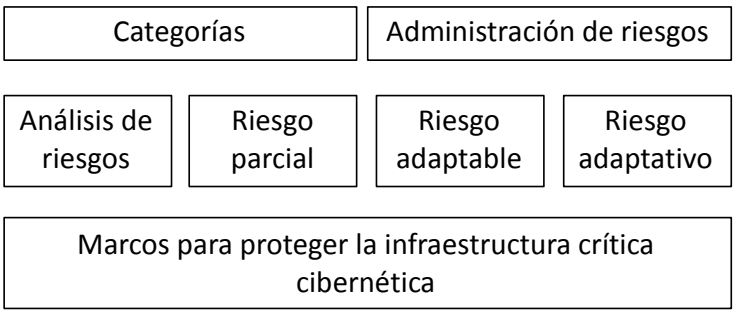
En un primer momento, Anbalón y Donder arguyen cuán importantes es entender que la ICC posee conexiones directas con agendas gubernamentales, cuyos objetivos son

la satisfacción de necesidades básicas poblacionales y concertación de objetivos estatales; hecho este que los convierte a su vez en intereses nacionales.

En un segundo momento, los autores explican que las amenazas extrínsecas al proceso de seguridad y defensa nacional son cambiantes, transmutan rápido y ello pone en desventaja a los sistemas estatales cuya actualización no depende en muchas ocasiones de la existencia de recursos, sino de protocolos públicos – legales que obstaculizan tanto actualización como cambio de sistemas proteccionistas. Anbalón y Donder no se enfocan únicamente en esa disertación de acciones complejas que traigan consigo la adopción y adecuación de nuevas tecnologías.

Todo lo contrario, estos investigadores se concentran en lo existente y funcional. Por eso con su ótica recomiendan a los estamentos de seguridad y defensa nacional cibernéticos adoptar estrategias con marco cibernético que aborde el análisis de riesgos, prospección de ciber ataques, identificación de vulnerabilidad intangibles y tangibles y articulación de procesos sistemáticos en un solo core para el control. Un ejemplo de este modelo puede analizarse en la figura 3.

Figura 4 Vulnerabilidades intangibles



Fuente: información recuperada de CCI (2018)

CAPÍTULO III

Análisis cualitativo del sistema de seguridad y defensa para infraestructura crítica cibernética[4] diseñada para resguardar al sector ambiental.

La realización de esta primera parte de la investigación se divide en dos partes: el análisis cualitativo y la aplicación de dos herramientas de análisis estratégico, matriz DOFA y matriz de impactos externos e internos.

Para comprender cómo funciona el esquema de protección y ciberdefensa de la ICCM hay que establecer, primeramente, que su estructura s el resultado del desarrollo funcional que plantean los pilares del CONPES 3701 DE 2011 Y 3854 DE 2016 (IDEAM, 2018). Esta estrategia de protección depende de múltiples factores y elementos conceptuales. Es decir, los procedimientos efectuados para este tipo de protección no provienen únicamente de los CONPES diseñados, pues hay otras fuentes de información como los protocolos nacionales de ciberseguridad o lineamientos institucionales internos con los cuales se prioriza la importancia que posee cada una de las partes que conforman el sistema *a quo*.

Un primer aspecto para tener en cuenta es que el sistema para proteger la ICCM tiene como alcance la definición, protección y restricción de cualquier tipo de impacto que ponga riesgo al medio ambiente. Ello significa que la proposición de estrategias de mejoramiento o acciones de optimización resulta ser benéfica no solo para mejorar el estándar estratégico planteado para la ICCM, sino también para definir nuevos alcances con los cuales prevenir, pero al mismo tiempo anticipar posibles afectaciones.

La estrategia para la protección de ICCM puede hallarse en el documento Plan Sectorial de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia – Sector Ambiente y RRNN. El documento es a su vez una guía direccional, la cual trae a colación una hipótesis: el sector medio ambiental, a diferencia de otros campos de injerencia, incluye a su

[4] De ahora en adelante ICCM

sistema de protección posibles ciber afectaciones que rezagan en el marco de lo ciber delictivo, pero también de lo ciber terrorista. Siendo así, la defensa de la ICCM puede darse desde lo policial operativo o desde lo estratégico enmarcado en el esquema de seguridad y defensa nacional.

Un ejemplo claro para discernir y aceptar que el plan posee una estrategia híbrida es que reconoce las afectaciones producidas por un malware, así como también las desencadenada por una APT (Amenaza Avanzada Persistente).

El desarrollo de esta estrategia halla su genealogía en la necesidad proteccionista del Estado. Aunque el marco legal con el que funciona posee una estrategia que acude a lineamientos jurídicos y procesos estatales, su naturaleza es distinta y se aproxima más a la preservación de la ICCM como forma de garantizar el goce del derecho a un medio ambiente sano o a gozar de recursos naturales estratégicos imperativos para la subsistencia de la especie.

El plan como documento rector se enfoca en el sector ambiental. Este es un punto favorable pues micro-segmenta la necesidad que afronta el campo cibernético de lo ambiental. Dicho campo, aunque no ha llegado a consagrar ausencia por parte de los organismos del Estado, es quizá el más sensible, pues a diferencia de otros segmentos, el funcionamiento de sistemas de información para la administración del medio ambiente y recursos naturales se basa en una supuesta priorización de componentes sensibles.

En otros términos, el plan rector no solo busca resguardar sistemas de información, pues sabe de antemano que lo protocolar y humano también es importante. Por esa razón es que uno de los frentes a intervenir, resguardar y proteger es el recurso humano que interactúa u opera la directriz tecnológica de la ICCN.

Para comprender como funciona esta estrategia actual resulta conveniente analizar dos puntos: la identificación de posibles amenazas, la cual parte con el reconocimiento de las amenazas hasta la caracterización de sus componentes funciones y la concertación de las

acciones estratégicas conexas a 2022. Para comprender el tema de las amenazas es necesario que se tenga en cuenta la siguiente afirmación:

Un riesgo cibernético para el sector ambiente y recursos naturales corresponde a la probabilidad que una amenaza se materialice sobre una vulnerabilidad de un servicio esencial como el servicio de información hidrometereológica, provocando situaciones que pueden incluir la pérdida de equipos, el robo de datos, la intrusión no autorizada para manipular datos y acciones que tengan como resultado la afectación de uno o más componentes de los servicios. Los riesgos cibernéticos del sector se deben gestionar porque existe un alto grado de afectación de muchos otros sectores usuarios de la información que genera el sector de ambiente y recursos naturales, especialmente en los relacionados con información hidrometereológica y sus alertas meteorológicas que son insumos para los sectores transporte, industria, comercio y turismo, agricultura, etc. (IDEAM, 2016).

Según el IDEAM (2016), los riesgos cibernéticos que pudieren materializarse en contra de la ICCM no son solo tecnológicos; también son procedimentales, y de ahí que sea necesario conocer qué amenazas u acciones entreven posibles ciber afectaciones, ya sea en el protocolo operativo o en el sistema de información *per se*.

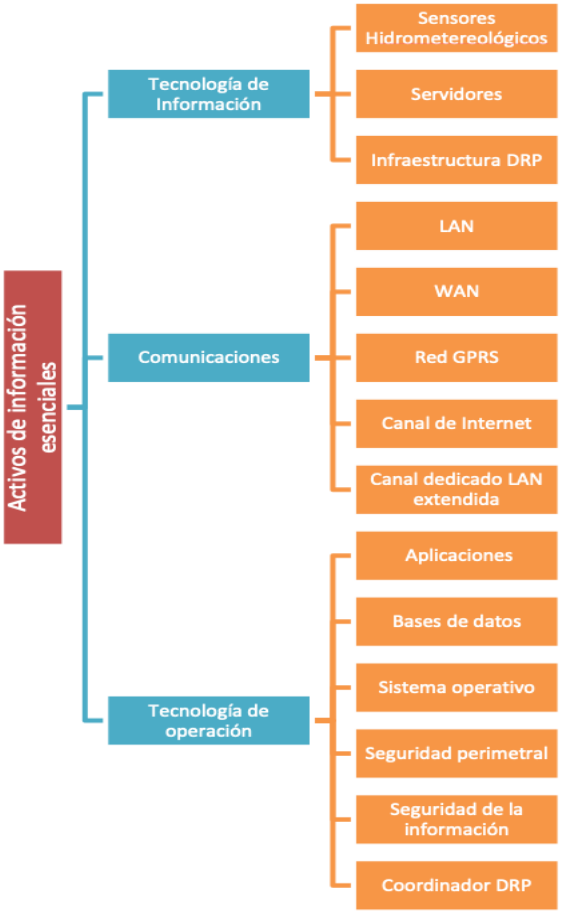
Para comprender el tema de las amenazas hay que establecer cuáles son los campos cibernéticos del sector medio ambiental que más afectación reciben. Según el Plan Sectorial, los servicios de información hidrometereológica, meteorología aeronáutica y otros sistemas de información correlacionados a la administración de recursos naturales como agua e hidro electricidad son los que mayor concurrencia en cuanto a ciber ataques presentan.

El ataque a este tipo de sistemas trae consigo una hipótesis. Esta hipótesis puede interpretarse de igual manera en el libro titulado Ciber seguridad para la Infraestructura Crítica del Agua, publicado por (Fedulova & Pivovarov, 2019). De acuerdo con ambos autores, un ataque dirigido hacia la infraestructura crítica y cibernética de la nación que presente relación

con el medio ambiente o sistemas de información, pone en riesgo a dos actores: el Estado y el actor poblacional. Por esta razón, una ciber afectación causaría impactos ambientales de tipología estructural, pero también de naturaleza socio-humanística.

Así los términos, en el Plan Intersectorial, de acuerdo a su registro de amenazas, que como ya se dijo no solo yacen en ciber seguridad, sino también en ciber defensa, hay una distinción categorial de diferentes amenazas, las cuales abarcan TIC, comunicaciones y tecnología de operación. (Ver figura 4)

Figura 5 Activos de Información Esenciales



Fuente: información recuperada de IDEAM (2016)

CAPÍTULO IV

Diagnóstico del esquema de ciber defensa del sector ambiental

Para llevar a cabo este ejercicio se emplearon dos métodos diagnósticos: una matriz DOFA y matriz de análisis de factores externos e internos. El objetivo en esta parte de la investigación es establecer de facto, cuáles son las fallas y vacíos funcionales que posee el proceso de gestión para garantizar el concepto de defensa y seguridad cibernética en el sector medio ambiental.

El propósito de esa identificación de hallazgos es conocer directamente el número o cantidad aproximada de problemáticas a partir de ejercicios cualitativos configurados bajo el parámetro de pensamiento estratégico gerencial.

Esta parte del proceso de investigación contó con la asesoría de expertos en materia ciber y medio ambiental. La descripción del perfil del panel de expertos es la siguiente:

- Ingeniero de sistemas con especialización en seguridad digital y maestría en ciber defensa. El experto invitado posee amplia experiencia en investigación científica e hizo parte de la línea de asesores externos que ayudó a estructurar y configurar el CONPES 3918 de 2018.
- Politólogo con maestría en proyectos de desarrollo sostenible. Experiencia investigativa en temas asociados con el medio ambiente, análisis de datos ambientales y construcción de modelos de supervisión y monitoreo eco sistémico.

Los dos expertos invitados al proceso de investigación y el autor primario plantearon como objetivo desarrollar y configurar la matriz DOFA a través de una metodología dividida en tres puntos: identificación y definición de las variables, ponderación de variables por importancia y gobernabilidad y concertación final de deducción y conclusiones del ejercicio realizado.

La primera parte del ejercicio fue la configuración de las variables DOFA. El resultado en este punto fue el siguiente:

Tabla 11 Variables DOFA - descripción

Variable		Descripción	Imp.	Gob.	Pro.
D1	Estrategia unificada	El sector medio ambiental no cuenta con una estrategia unificada, toda vez que el proceso de intervención y protección de ICCC-MA depende de los lineamientos e iniciativas desplegadas por parte de la estrategia general que posee el CCOCI	4,8	4,9	4,85
D2	Infraestructura tecnológica	Actualmente, el sector medio ambiente no cuenta con toda la infraestructura tecnológica que se requiere para desarrollar un proceso de intervención apropiado y bien estructurado	3	2	2,5
D3	Conocimiento	Una de las falencias o vacíos de función con mayor capacidad de afectación es la ausencia de capital humano altamente especializado en materia de protección cibernética de tipología medio ambiental	4,6	4,3	4,45
D4	Articulación	El proceso de articulación con otras entidades del Estado es débil, y debe reforzarse con parámetros como: cooperación en tiempo real y estructuración de estrategias conjuntas	2,5	3,3	2,9
D5	Cooperación internacional	Actualmente, el sector medio ambiental no posee procesos de cooperación y colaboración en materia de investigación científica, cuyo fin es estructurar estrategias de intervención y prevención de ciber ataques en materia medio ambiental	2,8	3,2	3
O1	Optimizar	Optimizar el proceso de gestión para estructuración de líneas estratégicas enfocadas en materia ambiental- Esa optimización se debe dar bajo el precepto "configuración de elementos estratégicos para anticipar y prevenir"	3,1	3,2	3,15
O2	Potenciar	Potenciar el proceso de intervención para la reducción de ciber ataques orientados a la ICCN- MA. Para ello es	4,1	3,9	4

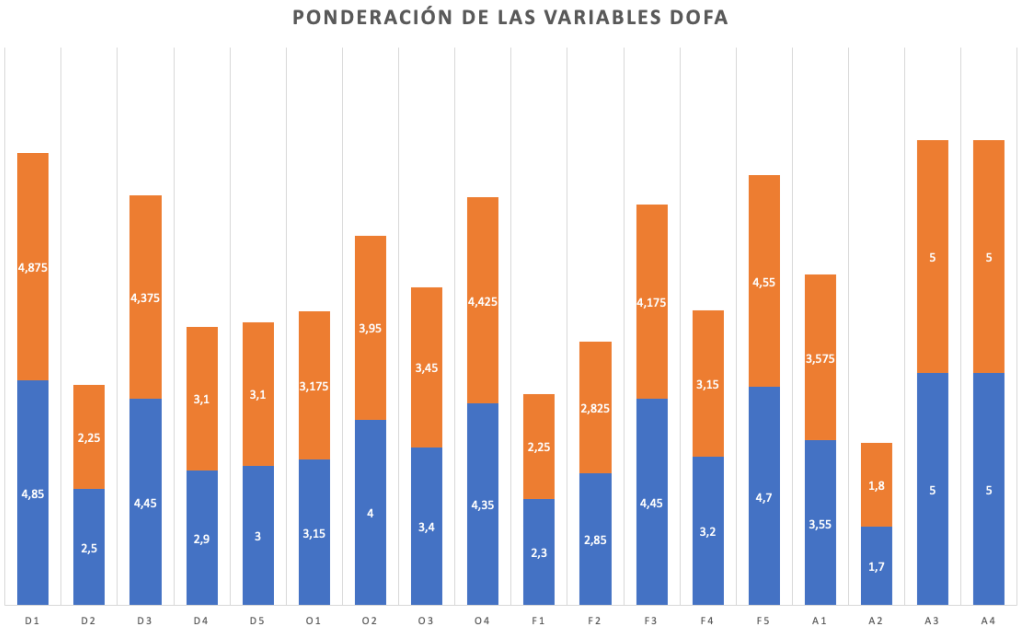
Variable		Descripción	Imp.	Gob.	Pro.
		necesario: investigar, detectar falencias y formular y ejecutar proyectos de inversión para mejorar múltiples espectros de afectación			
O3	Incorporar	Incorporar nuevas gestiones tecnológicas para conformar y construir una estrategia de anticipación y prevención de ataques	3,3	3,5	3,4
O4	Mejorar	Mejorar los estándares de gestión con miras a la protección de ICCN-MA por adoptar y en surgimiento.	4,2	4,5	4,35
F1	Estructura	Actualmente, el sector medio ambiental posee una estructura de gestión integrada, competente y con parámetros de funcionamiento claros y objetivos	2,4	2,2	2,3
F2	Recursos	Actualmente, el gobierno nacional cuenta con recursos suficientes para establecer, formular y desarrollar proyectos de optimización con miras a la actualización de sistemas de defensa cibernética para el sector medio ambiental	2,9	2,8	2,85
F3	Respaldo gubernamental	El sector medio ambiental cuenta con un CONPES direccional, ceñido al tema de "seguridad y defensa digital", por lo cual permite conceptualizar elementos estratégicos para mejorar que no requieren inversión	5	3,9	4,45
F4	Monitoreo	El sector medio ambiental posee un sistema de supervisión y monitoreo constante, el cual permite analizar, explorar y estudiar la naturaleza y procedencia del ciber ataques (especulativo)	3,3	3,1	3,2
F5	Estrategia	Actualmente, el sector medio ambiental posee una estrategia de intervención estructurada, con recursos asignados y metas planteadas, las cuales son flexibles y están prestas a cualquier tipo de cambio para: mejorar, optimizar y volver más eficiente	5	4,4	4,7
A1	Disrupción	Disrupción de procesos estratégicos de prevención y anticipación, hecho este que genera ataques no esperados	3,5	3,6	3,55

Variable		Descripción	Imp.	Gob.	Pro.
A2	Fluctuación	Aumento y disminución continua de ciber ataques que cada vez son más complejos y con mayor nivel y alcance de afectación	1,5	1,9	1,7
A3	Daño - infraestructura	Ciber ataques continuos con capacidad para generar daños estructurales irreparables, de gran costo y sin procesos de gestión direccionados hacia la reducción o desarticulación de impactos	5	5	5
A4	Desactualización estratégica	Ralentización de elementos estratégicos que no permiten mejorar o aumentar la eficiencia y eficacia de los procesos de para reducir la variable "posibilidad de daño".	5	5	5

Fuente: elaboración propia

Los resultados gráficos obtenidos son los siguientes:

Figura 6 Ponderación de las variables DOFA



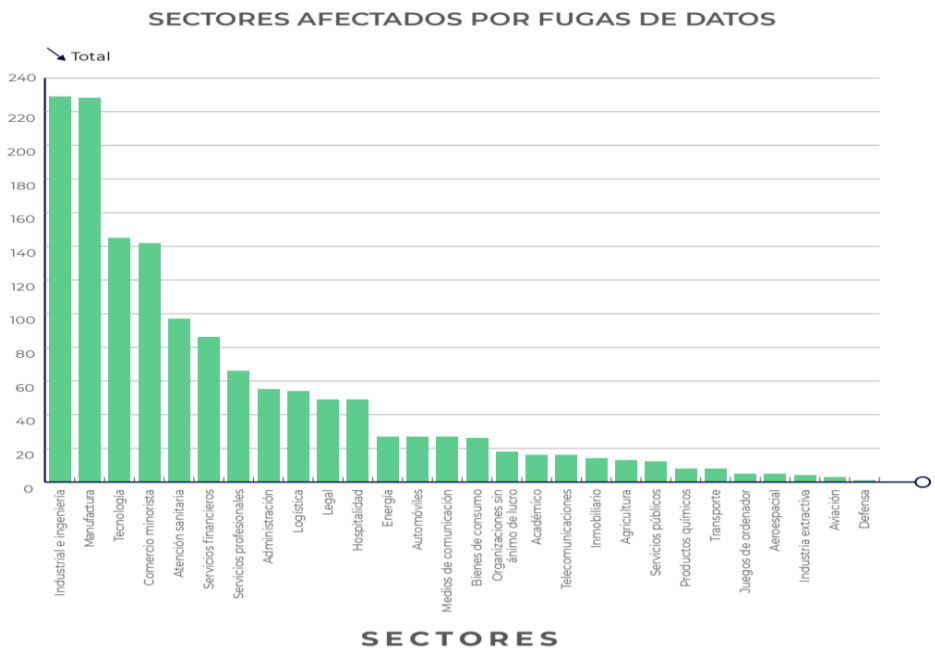
Fuente: elaboración propia

CAPÍTULO V
Situación de ciberataques en Colombia

Los tiempos modernos han suscitado una serie de cambios, que evocan amenazas cambiantes y afectan la estabilidad del orden mundial, Colombia no ha sido excepción en términos de seguridad; de hecho, es una realidad latente observar cómo los crímenes cibernéticos han desencadenado inestabilidad para las personas e incluso para el gobierno (Villanueva, 2015).

En consecuencia, muchas empresas y personas naturales se han visto afectadas por una serie de ataques maliciosos con propósitos múltiples pero con una particularidad, el crimen cibernético; al observar como la tasa de crímenes cibernéticos incrementa surgen una variedad de preguntas, de hecho para el año 2019 fueron registrados 30.410 casos donde se reportaba posibles ataques cibernéticos (CCIT, 2021); estos ataques denotan como es imperativo aplicar estrategias defensivas que puedan contrarrestar efectivamente las amenazas digitales.

Figura 7 Sectores Afectados Por fugas de datos



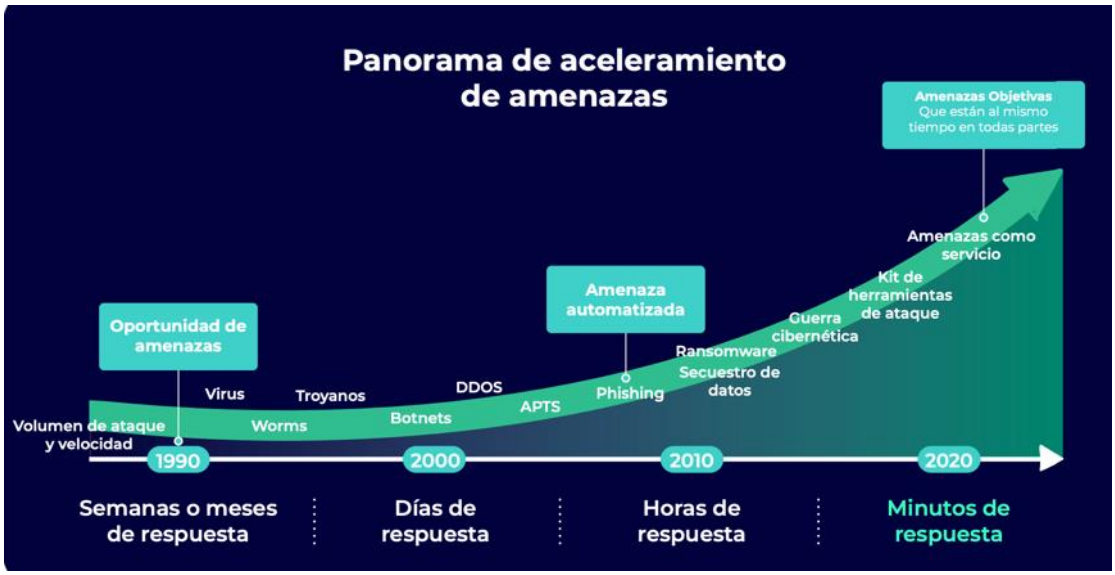
Fuente: recuperado de Informe SAFE (2021).

De acuerdo con la figura 6, los sectores de la economía más afectados han sido el de industria e ingeniería, seguido de la manufactura y el área de tecnología, es importante destacar que estos sectores aporten de sobremanera al desarrollo integral de estrategias corporativas del país, los ataques para robar datos demuestran que los intereses pueden ir más allá del dinero, de hecho representa la divulgación de estrategias para alcanzar posicionamiento o para establecer conductas de consumidores (Ospina y Sanabria, 2020).

Los ciberataques en Colombia se han vuelto más comunes a través del tiempo; de facto, muchos de estos se han visto direccionados a afectar a personas y entidades para la obtención ilegal de dinero o para el robo de cuentas bancarias, estas modalidades afectan la seguridad de las personas, debido a que en muchas ocasiones se observan como las herramientas de suplantación representan una de las principales tendencias criminalísticas que son usadas para cometer robos; más de 31.058 casos bajo la modalidad de "hurto por medios informáticos" demuestran que el interés principal de los ladrones cibernéticos es a través de suplantaciones o métodos como softwares malignos ingresar y extraer la información de personas que no tienen la suficiente seguridad sobre sus plataformas digitales (CCIT, 2021).

Ahora bien, Colombia es un territorio en el que el uso del internet suscitó un avance notorio en los crímenes cibernéticos, y es que la seguridad de la red implica unas medidas cautelosas de protección de los datos y la información debido a que sin estas, no se puede estimar la cantidad de afectaciones que se pueden presentar sobre los valores informativos de las personas, desafortunadamente la cultura de seguridad aun no es imperante entre la incredulidad de las personas (Martínez, 2021); no obstante, las estrategias conjuntas de múltiples empresas han buscado reducir los efectos negativos que son ocasionados por la fuga de información y por el robo de datos.

Figura 8 Panorama de Aceleramiento de Amenazas en Colombia



Fuente: recuperado de Informe SAFE (2021).

Las amenazas cibernéticas han tenido un ritmo de crecimiento exponencial a través de los años, esto puede ser explicado en la figura 2, donde se denota como el internet y el aumento de crímenes cibernéticos tienen una correlación directa debido a que básicamente son interdependientes. Si bien es cierto, hace unos años las amenazas cibernéticas tenían una demora en la respuesta que podría tardar semanas e incluso meses para ser resuelta, el auge de la tecnología; así como el uso de herramientas modernas que periten el autoaprendizaje garantiza que muchas de las nuevas amenazas sean resueltas en minutos aumentando la capacidad de protección de los sistemas de información (Aziz y Dowling, 2019).

El aumento de los ataques cibernéticos es una clara muestra de la falta de protección de datos que existe en los sistemas electrónicos; si bien es cierto existen una amplia cantidad de variables que pueden determinar el alcance y la cantidad de daño sobre un servidor, también es una realidad que las herramientas de software perjudicial, afectan en sobre manera la información que está en la red, cuando no se calculan los efectos negativos que puede presentarse sobre servidores y bases de datos, la cantidad de información que se puede fugar trasciende los límites y se convierten en un riesgo para la protección de os datos (CCIT, 2021).

El efecto de la pandemia trajo consigo un periodo crítico, este evocó una realidad que nadie quería aceptar pero que significaba un notorio problema; las redes y la internet tomaron fuerza a medida que se acrecentaban los casos de coronavirus; las empresas tuvieron que recurrir a modelos remotos y a la digitalización de la información para poder mantener el ritmo de trabajo de las mismas; ahora bien, la incursión de sistemas de trabajo remoto le dieron apertura a un sin número de ataques a la red de datos e información que vulneran la seguridad del internet para finales del año 2021 en Colombia se habían reportado a través de los sistemas de denuncia de la Fiscalía General de la Nación 46.527 denuncias en contra de los delitos cibernéticos es decir que comparado con el año 2019 se presentó un crecimiento de más del 107% en amenazas y vulneraciones a la seguridad (Informe SAFE, 2021), sin lugar a dudas un escenario que se convierte en inestable a medida que pasa el tiempo.

Del mismo modo, la pérdida de información que se ha llevado a lo largo del tiempo en plataformas donde se resguardan una gran cantidad de datos e información, es una de las principales modalidades y tendencias que se deben afrontar en los tiempos modernos (CCIT, 2021). Los criminales cibernéticos aprovechan el desconocimiento de los usuarios para vulnerar la información y apoderarse de la misma, además, en una época donde la híper-mediatización existe a través de todas las plataformas que conectan al mundo, los sistemas de defensa de la información debe ser garantes de la organización y de la protección de los datos, para lograr una mejora constante en la calidad de la misma y la eficiente protección frente a amenazas externas (Chauvel, 2020).

La protección de los datos se convierte en una prioridad imperativa, debido a la relevancia de los mismos para el descubrimiento de tendencias y de gustos de las personas en un mundo globalizado (Chauvel, 2020); es por ello que una contraseña e incluso estados bancarios pueden ser blancos de aquellos que quieren usarlos para suplantar y hurtar el dinero de las personas; los ataques cibernéticos no discriminan blanco y están orientados a ocasionar

inestabilidad en todos los sectores de un territorio es decir a entidades públicas y privadas por igual.

Dentro de las principales tendencias que han amenazado el área de ciberseguridad en Colombia se encuentra la suplantación de identidad, el enmascaramiento de correos, la infección de sitios web y el uso de correos fraudulentos personalizados, estas amenazas en conjunto han representado millonarias pérdidas de dinero para las empresas quienes deben enfrentarse a diferentes modalidades organizadas que suplantan desde los clientes hasta incluso el CEO de la organización todo para adquirir dinero y poder afectar la economía de la empresa (CCIT, 2021).

Para lograr salvaguardar la información de forma efectiva, se requiere de sistemas modernos equipados con tecnologías vanguardistas como la inteligencia artificial y el Machine Learning; que permiten realizar un análisis de las amenazas de igual modo garantizan que los sistemas de información estén en protección constante y les permite aprender sobre los Ransomware y otras amenazas latentes en los sistemas para poder brindar una protección detallada a los datos y la información de las organizaciones (Aziz & Dowling, 2019).

La situación actual sobre los delitos cibernéticos en el país también ha mostrado como las amenazas cibernéticas aumentan a través de la mejora del comercio y la economía nacional, sin lugar a dudas el e-commerce ha sido una de las nuevas tendencias para la adquisición de productos y servicios desafortunadamente a través de esta herramienta también se ha presentado un gran aumento de los crímenes cibernéticos que muestran una vez más como los bandidos aprovechan el desconocimiento de los usuarios y terminan afectando el “bolsillo de los colombianos” (CCIT, 2021).

Durante el periodo 2018-2022 se llevó a cabo una estrategia de recolección y recuperación económica conocida como el día sin IVA, sin lugar a dudas un método acertado para mejorar el flujo de caja de las empresas e inyectar con capital al sistema económico

nacional, desafortunadamente los criminales cibernéticos también aprovecharon estas jornadas para perpetrar ataques, de hecho en cada uno de estos eventos se presentaban cerca de 5.000 amenazas a empresas y clientes a través de uso de plataformas de pago alternas, o casos de suplantación (Informe SAFE, 2021).

Las consecuencias que un ciberataque trae a la economía colombiana son bastante relevantes, debido a que gran parte de las fuentes de empleo que existen en Colombia provienen de las PYMES (pequeñas y medianas empresas), estas empresas de una u otra forma aportan al crecimiento del mercado colombiano y brindan una fuente de empleo a los sectores más vulnerables del país (Meléndez *et al.*, 2017); desafortunadamente de acuerdo al informe CCIT:

> "El 60% de las pequeñas y medianas empresas, no pueden sostener sus negocios más de seis meses luego de sufrir un ciberataque importante. Esto demuestra que los factores en torno a los Ciberataques a PYMES en Colombia comprometen seriamente los activos económicos e impactan asuntos estrictamente legales y de cumplimiento de las compañías. (2021)"

Esto demuestra como la seguridad empresarial no está salvaguardada y como las empresas que están en auge sufren daños irreversibles que terminan ocasionando el cierre de las mismas lo que afecta notablemente el crecimiento económico de la sociedad perjudicando al país y a los ciudadanos.

En conclusión, la situación actual de los ataques cibernéticos en Colombia implican un análisis detallado por parte del gobierno, para propender por estrategias lideradas en el área del ministerio de las TICS, en donde se pueda coordinar herramientas que ayuden a mejorar el uso y el cuidado de la protección de la información, es importante resaltar que en un ambiente incierto y cambiante como la realidad actual, esta información es considerada un activo

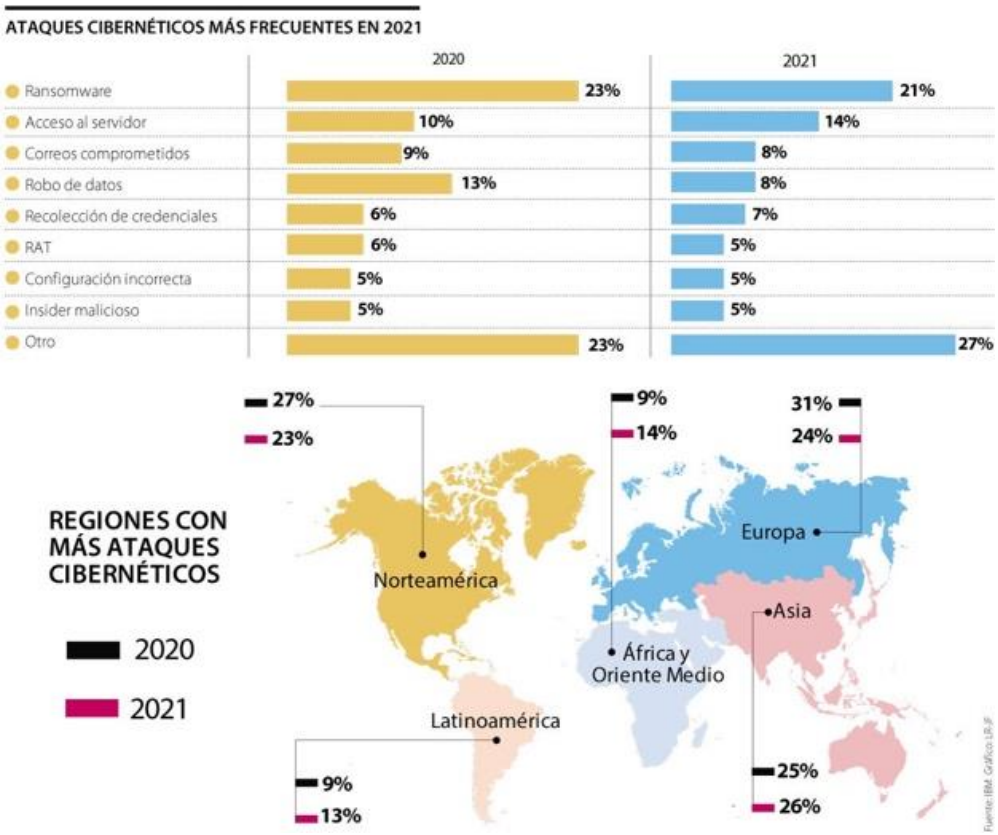
estratégico para cualquier nación y por ende debe ser considerada como un activo estratégico nacional, del cuidado de estos datos así como de la educación digital depende que se mitiguen las amenazas y que se pueda mejorar de sobremanera la forma en la que se difunde la información, y se aplican tendencias del mundo moderno como el e-commerce que fomentan la economía nacional y por ende logran direccionar el estado hacia el crecimiento integral.

La protección de la información y los datos es garante de la seguridad de las instituciones, visto desde el punto de inflexión en el que los blancos de estas vulneraciones, no son solo las personas naturales sino a su vez entidades públicas y privadas lo que representa que cualquier vulneración a la seguridad se convierte en una debilidad en potencia que puede repercutir en aspectos relevantes como la estabilidad nacional e incluso en la propiedad intelectual para el desarrollo de estrategias que ayuden al desarrollo del territorio colombiano.

Al analizar la cantidad de ataques cibernéticos que se han presentado en el contexto internacional, es importante analizar como el impacto de los mismo ha ocasionado inestabilidad y de igual manera un sin número de afectaciones a los países, el aumento de los mismos implica medidas que han sido tomadas de forma activa por los diferentes países quienes a través del uso adecuado de herramientas modernas buscan mitigar los efectos negativos de los ciberataques (Carlini, 2016)

La realidad actual demuestra como el aumento indiscriminado de estos ataques vulnera a todos los sectores de los gobiernos, la figura 8 demuestra como en los últimos años, el aumento de ataques cibernéticos ha crecido de manera exponencial dejando en evidencia como esta modalidad de robo se ha vuelto más común con el tiempo.

Figura 9 Ataques cibernéticos más frecuentes



Fuente: recuperado de La República (2022)

Las regiones más afectadas sin lugar a dudas han sido Asia, Europa y Norteamérica con 26%, 24% y 23% de ataques respectivamente lo que se podría traducir como una forma de afectar las principales potencias que gobiernan el orden mundial (Morán, 2015), sin embargo, es importante destacar que estas potencias como se les conoce poseen a su vez amplios conocimientos para la detección y mitigación de amenazas cibernéticas.

La relevancia de la protección sobre estos asaltos cibernéticos, radica en la vulnerabilidad e importancia de la información, en muchos casos la información que se busca guardar posee datos sobre entidades públicas y privadas e incluso sensibles para los gobiernos por lo que el cuidado de los mismos se convierte en una política de estado que debe propender por garantizar que no sean filtrados o “robados” para ser usados con fines delictivos o extorsivos (Sánchez, 2020).

Los ataques cibernéticos más comunes en la actualidad incluyen el uso de inteligencia artificial combinada con los famosos “malware” que afectan los sistemas operativos de los equipos y contrarrestan antivirus y otras fuentes de protección, estas amenazas se nutren a partir de los conocimientos que adquieren del objetivo que van a atacar y extraen información y datos en tiempos récord lo que obstaculiza y ralentiza los tiempos de respuesta (Informe SAFE, 2021); del mismo modo el uso de perfiles falsos en redes sociales para la captación ilícita de dineros se ha disparado, vulnerando así a miles de personas que desconocen este tipi de accionar delictivo.

Otros métodos que aplican los delincuentes cibernéticos incluyen el uso de mercados ilegales en la “dark-web” y métodos a través de correos extorsivos que incluyen algunos tipos de “ransomware” diseñados para robar los datos de los usuarios y la información bancaria de los mismos (Informe SAFE, 2021); así como estos ataques, existen de igual manera múltiples ataques perpetrados por organizaciones a gran escala, los objetivos de estas no es otro diferente a generar inestabilidad en los gobiernos y someterlos a peticiones ilógicas a cambio de acuerdos para la no revelación de información estratégica que vulnere los secretos de estado (Ludlow, 2010).

El mundo ha sufrido varios ejemplos de ataques encaminados a la revelación de información sensible un claro ejemplo de esto fueron las revelaciones de WikiLeaks en donde el mundo se enteraría de atrocidades que revelaban las operaciones secretas del gobierno de los Estados Unidos (Corneil, 2010); de igual manera, el grupo autodenominado como “Anonymous” también ha sido una piedra en el zapato para muchos gobiernos, sus apariciones y sus revelaciones han puesto de manifiesto que la seguridad de la información es un asunto de interés nacional y que este puede marcar la diferencia entre la estabilidad de los estados (Deseriis, 2013).

Ahora bien, todos estos ataques demuestran como el mundo está siendo afectado por las denominadas guerras de quinta generación, conflictos que implican el uso de medios cibernéticos como herramientas para desestabilizar las naciones y que se aplican bajo el precepto de guerras sin contacto y silenciosa (Abbott, 2010); visto de otra manera, estos conflictos ocasionan que las naciones preparen sistemas integrados de defensa que garanticen la protección de la información y del mismo modo garanticen medidas efectivas de respuesta frente a cualquier posible amenaza.

La tecnología es cambiante y gracias al auge de la misma, existen diferentes métodos que se encargan de la protección efectiva de esos datos, el diseño de sistemas de protección existen desde el mismo comienzo del internet, a través de herramientas como los sistemas antivirus que cuidaban a través de "firewalls" los sistemas operativos de los computadores, sin embargo muchas organizaciones criminales poseen mentes brillantes aprovechando al máximo las debilidades de las plataformas defensivas por ello, muchos de los métodos para mitigar las amenazas incluyen el uso de todas las herramientas del estado un ejemplo de esto es el gobierno Norte americano quienes a través de la CIA, han capturado a muchos criminales cibernéticos y mediante acuerdos con ellos han desarrollado nuevas formas de defensa que mitiguen las amenazas de hackers o ciber-terroristas (Samoriski, 2020).

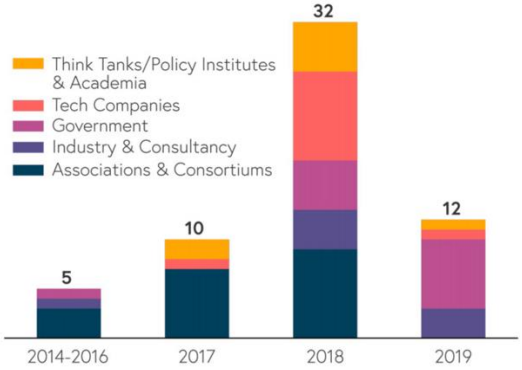
Del mismo modo agencias como la KGB en Rusia e incluso China se ha potencializado el uso de ex criminales cibernéticos para mejorar sus defensas y poder hacer frente a nuevas amenazas que puedan alterar el poder de sus estados (Buchanan, 2020). Sin embargo, las formas de protección no se limitan únicamente a la capacidad de utilizar estos medios de defensa, también se han implementado métodos como el desarrollo de nuevos softwares de protección, la seguridad es una realdad latente por ende se debe buscar el cuidado de la información a todo costo (Gordon y Ford, 2002).

Dentro de los sistemas modernos de cuidado que han sido desarrollados a través del tiempo, se destaca la implementación del Machine Learning, una característica esencial del mundo moderno en la que a través del autoconocimiento de las amenazas los sistemas integrados de computación pueden hacer frente, aprender y mejorar la protección mediante barreras de seguridad en la información (Buchanan, 2020).

La inteligencia artificial juega un rol muy importante debido a que, a través de algoritmos de protección y detección, esta puede aplicar modelos predictivos que garanticen respuestas eficaces a las amenazas (Buchanan, 2020); es así, como en conjunto los sistemas predictivos pueden garantizar la mitigación de amenazas a través de una programación orientada a la solución de problemas durante la ejecución de tareas propias

Por otra parte, los gobiernos también han recurrido a métodos de detección de amenazas o de vulneraciones a sus redes, a través de las agencias de seguridad nacional se busca identificar las fuentes donde surgen los posibles ataques a las redes, y mediante la respuesta eficaz de los mismos a las amenazas pueden contrarrestar cualquier tipo de actividad perjudicial que atente contra la seguridad de la información.

Figura 10 Numero de sistemas de Inteligencia Artificial producidos por entidades



Fuente: recuperado de INDEX reporte mundial (Garcia, 2019)

Como se puede observar en la figura 2, para el año 2019 las entidades que mayor número de Software tipo Inteligencia artificial desarrollaron fueron los gobiernos, esto debido a la cantidad de ataques cibernéticos que se venían suscitando para la época, los retos y los desafíos de estas entidades se convertirá entonces en la búsqueda de herramientas efectivas que garantizaran la protección de los datos de los sectores públicos y privados para mitigar conflictos ocasionados por la pérdida de la información o la vulneración de los secretos estatales.

En conclusión, las amenazas cibernéticas han tenido un gran aumento a través de los años, dicho de otro modo, los problemas económicos mundiales, la pandemia y los conflictos internacionales como el que se vive actualmente entre Rusia y Ucrania, suscitan una serie de eventos que vulneran el orden de las naciones, estos espacios de conmoción y caos, ocasionan el crecimiento de fenómenos que atentan y vulneran la sociedad, las organizaciones ilícitas que se autoproclaman no gubernamentales e independientes amenazan a través de sus plataformas a todo aquel que se oponga ocasionando caos en los organismos de control de los estados.

Para mitigar estas amenazas, los estados han optado por utilizar herramientas que abarcan todas las dimensiones del conflicto mediante el uso de sistemas que garanticen la detección y localización de las amenazas, de igual modo la utilización de softwares y herramientas que con el uso del Machine Learning y la Inteligencia Artificial logren mitigar y disminuir al máximo la cantidad de vulneraciones a la seguridad que se pueda presentar; finalmente, la conjunción de estas actividades, así, como las sanciones internacionales a todos los criminales que vulneren la protección de los datos busca garantizar que todos los organismos del estado estén preparados y listos para actuar pero que de igual manera estén tranquilos pues la información se mantendrá segura y a salvo de manos criminales que busquen atentar contra la estabilidad.

CAPÍTULO VI
Estructuración de la propuesta estratégica

Hasta esta parte de la investigación se realizó un análisis diagnóstico de los diferentes componentes que conforman el precepto “seguridad y defensa digital” para la infraestructura crítica cibernética de la nación. Un hallazgo fundamental que de hecho se pudo observar en la aplicación de la matriz DOFA es que la entidad del sector medio ambiental que mayor riesgo corre es el IDEAM. De facto, los riesgos identificados en el documento Plan Sectorial de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia sector Ambiente y RRNN, tienen plena relación con el IDEAM como actor con mayor vulnerabilidad. (Ver tabla 5).

Tabla 12 Riesgos identificados en el IDEAM

Nro RIESGO	ACTIVO/ SERVICIO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VULNERABILIDAD	AMENAZA	TIPO AMENAZA	PROBABILIDAD	IMPACTO	NIVEL DE RIESGO
R1	Pronóstico Meteorológico y Alertas	BAJO	ALTO	ALTO	Deficiencia en protección antivirus	Malware	Conocidos	2- Improbable	4- Crítico	Alto
R2	Pronóstico Meteorológico y Alertas	BAJO	ALTO	ALTO	Deficiencia en las claves de acceso	Fuga de información	Conocidos	1- Raro	3- Moderado	Medio
R3	Pronóstico Meteorológico y Alertas	BAJO	ALTO	ALTO	Deficiencia en los equipos de seguridad (IDS e IPS)	DDoS	Latente	2- Improbable	5- Muy Crítico	Crítico
R4	Pronóstico Meteorológico y Alertas	BAJO	ALTO	ALTO	Deficiencia en la configuración del aplicativo	Defacement	Conocidos	2- Improbable	4- Crítico	Alto
R5	Pronóstico Meteorológico y Alertas	BAJO	ALTO	ALTO	Deficiencia en protección antivirus (host y perimetral)	Ransomware (Pcs o Servidores)	Conocidos	1- Raro	5- Muy Crítico	Alto
R6	Pronóstico Meteorológico y Alertas	BAJO	ALTO	ALTO	Deficiencia en el análisis de eventos y logs	Ataques coordinados	Focales	1- Raro	4- Crítico	Alto
R7	Pronóstico Meteorológico y Alertas	BAJO	ALTO	ALTO	Deficiencia en protección antivirus (host y perimetral)	Cryptomalware	Conocidos	2- Improbable	3- Moderado	Medio
R8	Pronóstico Meteorológico y Alertas	BAJO	ALTO	ALTO	Actualización en infraestructura de Seguridad	Computación en la niebla (Fog Computing)	Emergentes	3- Posible	5- Muy Crítico	Crítico

Fuente: información recuperada de MADS (2018)

Significa esto que el proceso de gestión estratégica por desarrollar debe estructurarse en pro y a favor del IDEAM como actor con mayor grado de vulnerabilidad, pero también de las entidades adscritas al ministerio como son la Autoridad Nacional de Licencias Ambientales (ANLA), Parques Nacionales (PPN), Instituto de Investigaciones Ambientales del Pacífico, Instituto Amazónico de Investigaciones Científicas (SINCHI), Instituto de investigación de

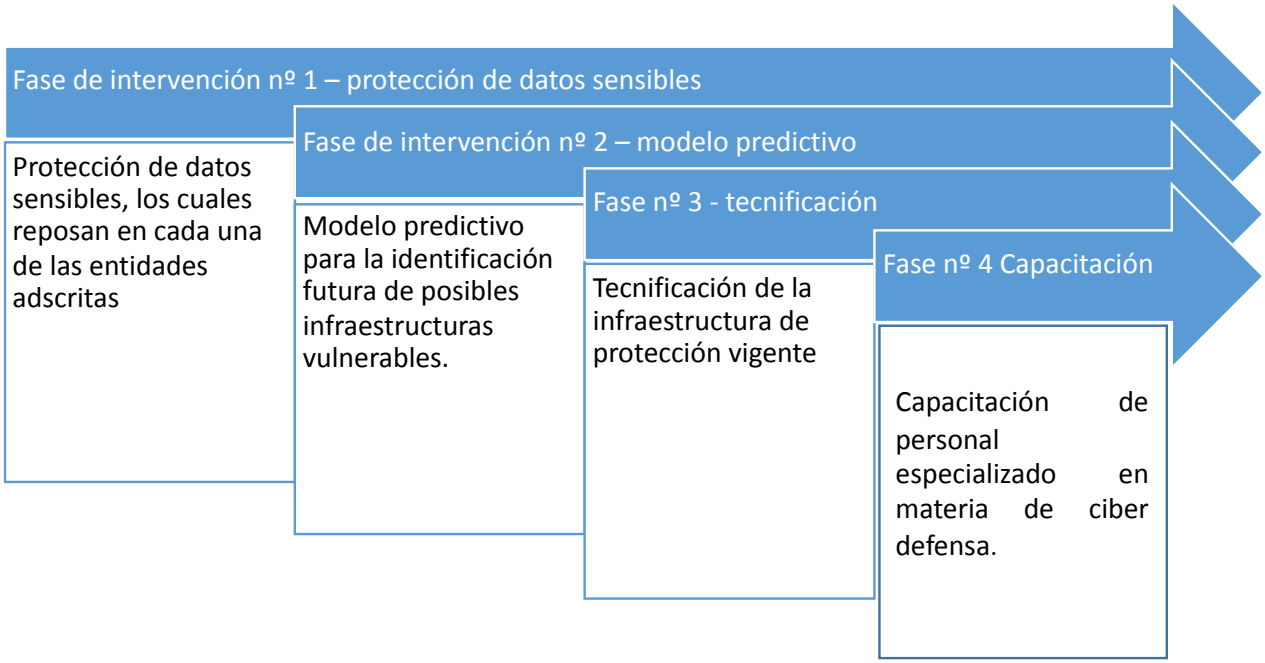
recursos biológicos Alexander Von Humboldt y el Instituto de Investigaciones Marino – Costeras (IVEMAR).

Ahora bien, para estructurar las líneas estratégicas que fortalecerán el plan vigente, la investigación centra el proceso de atención e intervención en tres aspectos principales; estos surgen del análisis cualitativo que se desarrolló en los capítulos cuatro y cinco. En total son tres factores de atención e intervención, y su descripción es la siguiente:

- Factor de intervención Nº 1 – protección de datos sensibles.
- Factor de intervención Nº 2 – modelo predictivo para la identificación futura de posibles infraestructuras vulnerables.
- Factor de intervención Nº 3 – tecnificación de la infraestructura de protección vigente.
- Factor de intervención Nº 4 – capacitación de personal especializado en materia de ciber defensa.

Los focos de intervención, resumidos gráficamente, son los siguientes:

Figura 11 Factores de intervención



Fuente: elaboración propia

Teniendo claridad acerca de los factores de intervención, se da paso a la explicación metodológica de las líneas estratégicas a estructurar. Cada factor de intervención tendrá una línea conformada por:

- Primero, descripción de situación
- Segundo, planteamiento del objetivo de intervención.
- Tercero, creación de actividades.
- Cuarto, proposición de necesidades.
- Quinto, indicadores de gestión

Una vez finalizada el ejercicio de estructuración de líneas, se dará paso al capítulo de triangulación de hallazgos, conclusiones y deducciones.

Estructura estratégica para el factor de intervención Nº 1 - protección de datos sensibles.

Descripción de la situación

Se pudo evidenciar en el análisis cualitativo, que el almacenamiento y protección constante de datos en las entidades que son parte del MADS ocupa un puesto prioritario en el proceso de aseguramiento y protección de ICCN-MA[5]. Actualmente, las bases de datos cuentan con sistemas de protección cuya actualización se da cada 24/ 48 horas**. Sin embargo,** tienen un problema: las bases de datos son públicas, y la modificación de los lenguajes de programación depende de validadores y expertos terceros, hecho este que pone en riesgo el concepto "protección autónoma".

Objetivo de la línea estratégica Nº 1

Implementar una metodología de resguardo, protección y compatibilidad de datos conjuntos entre las entidades adscritas al MADS a través de la adecuación de una nube

[5] Infraestructura crítica cibernética de la nación – medio ambiente.

simplifica y única, cuya licencia sea responsabilidad directa del MADS y cuya administración y utilización dependa de siete usuarios exclusivos[6]. Para unificar la base de datos, el personal de expertos sugiere al MADS adoptar el software Microsoft Azure.

Creación de actividades

Las actividades necesarias para implementar esta línea estratégica son las siguientes:

Tabla 13 Actividades requeridas

Actividad	Descripción	Objetivo
Diagnóstico	Diagnóstico micro-especializado para conocer la vulnerabilidad que poseen las bases datos de las entidades adscritas; centrarse específicamente en el periodo de actualización de los instrumentos digitales necesarios para el resguardo de los data warehouses	Implementar un diagnóstico de situación para establecer la situación real en cuanto vulnerabilidad y riesgo de las bases de datos que poseen las entidades adscritas.
Migración	Migración del sistema de database digital al sistema de data base en la nube a través de la adopción de una cuenta protegida y única en Microsoft Azure	Realizar el proceso de migración de bases de datos a la cuenta única de Microsoft Azure, toda vez que el interés primario es dar acceso único DE funcionarios de las entidades que, mediante IA, administren la database,

[6] Siete equivale al número de entidades adscritas al Ministerio de Medio Ambiente y Desarrollo Sostenible.

Actividad	Descripción	Objetivo
		restringiendo el acceso a consultores externos.
Protección	Protección de database SDK que trae Microsoft Azure para resguardar los data warehouses a partir de un código único diseñado para el MADS y sus entidades	Implementar el programa de database SDK que trae Microsoft Azure para resguardar los data warehouses a partir de un código único diseñado para el MADS y sus entidades
Retroalimentación	Retroalimentación del sistema de defensa digital que trae Microsoft Azure a través de un proceso de integración por retroalimentación (migración de IA)	Conformación de sistema con IA para retroalimentar Microsoft Azure con los hechos digitales criminales registrados en años anteriores

Fuente: elaboración propia

Proposición de necesidades

Para implementar esta línea se requieren las necesidades consiguientes:

Tabla 14 Necesidades para la línea estratégica

Necesidad	Descripción
Diagnóstico con consultoría especializada	Realizar un diagnóstico conjunto entre el MADS y sus entidades adscritas a través de una consultoría especializada en protección de bases de datos.

Necesidad	Descripción
Adquisición de licencia Microsoft Azure	Estructurar el proyecto de inversión institucional para la adquisición global de las licencias de Microsoft Azure y sistema de protección SDK
Preparación del capital humano	Capacitación del capital humano designado para el control y administración de las bases de datos una vez dada la migración.

Fuente: elaboración propia

Indicadores de gestión

Los indicadores de gestión para la línea Nº 1 son los siguientes:

Tabla 15 Indicadores de gestión y evaluación

Indicador de gestión	Indicador de evaluación
Reducción de riesgo de pérdida de información por ataque externo en un 80%	Reducción de riesgo por ataque externo en mínimo aceptable de 60%
Migración de bases de datos a Microsoft Azure en un 80% para tercer trimestre de 2023	Migración mínima del 40% a Microsoft Azure para el último trimestre de 2023
Migración de bases de datos a Microsoft Azure en un 80% para tercer trimestre de 2023	Migración de bases de datos a Microsoft Azure en un 30% para tercer trimestre de 2023
Capacitación del 100% de capital humano que tendrá por responsabilidad la base de datos (2023)	Capacitación del 50% de capital humano que tendrá por responsabilidad la base de datos (2023)

Fuente: elaboración propia

Estructura estratégica para el factor de intervención Nº 2 – modelo predictivo.

Descripción de la situación

Actualmente, el MADS y sus entidades adscritas no poseen un modelo de ciber defensa predictivo o de anticipación. De hecho, ninguna entidad del Estado colombiano ha adaptado a sus mecanismos de defensa el planteamiento "predicción", dejando así un vacío de función poco explorado: el de los medios de defensa anticipada bajo la adaptación de un modelo predictivo.

Objetivo de la línea estratégica Nº 2

Implementar un modelo predictivo bajo la figura estratégica de la plataforma Warden, a fin de anticipar posibles riesgos y vulnerabilidades generadoras de impacto cibernético con fines terroristas.

Creación de actividades

Las actividades necesarias para esta línea estratégica son las siguientes:

Tabla 16 Actividades y descripción

Actividad	Descripción	Objetivo
Proyecto de inversión	Proyecto de inversión para la adquisición de la plataforma de predicción y anticipación de ataques bajo la metodología WARDEN	Estructurar el proyecto de inversión para la adquisición de la plataforma predictiva
Adaptación	Adecuación de la plataforma WARDEN al modelo de administración de base de datos de Microsoft Azure	Adaptación del modelo predictivo al componente tecnológico de y de protección de Microsoft Azure
Capacitación	Capacitación del capital humano que se encarga de los procesos de gestión y	Implementar un programa de capacitación para actualizar y alinear cognitivamente al

Actividad	Descripción	Objetivo
	defensa cibernética de ICCN en el tema específico de plataforma Warden	personal encargado con las funciones y propiedades digitales de la plataforma Warden

Fuente: elaboración propia

Proposición de necesidades

Las necesidades para implementar la línea estratégica Nº 2 son las siguientes:

Tabla 17 Proposición de necesidades

Necesidad	Descripción
Adquisición de plataforma Warden	Proyecto de inversión para la adquisición de la plataforma Warden
Capacitación de capital humano	Preparación del capital humano frente al tema de manejo y administración de la plataforma WARDEN.

Fuente: elaboración propia

Indicadores de gestión

Los indicadores de gestión son los siguientes:

Tabla 18 Indicadores de gestión y evaluación

Indicador de gestión	Indicador de evaluación
Ejecución del proyecto de adquisición en un 100% para el primer trimestre del 2024	Ejecución del proyecto de adquisición en un 100% para el primer trimestre del 2024

Indicador de gestión	Indicador de evaluación
Poner en funcionamiento la plataforma WARDEN en un 80% para primer semestre de 2024	Poner en funcionamiento la plataforma Warden en un 70% para el último trimestre de 2024
Capacitación del 100% del capital humano antes del último trimestre del 2024.	Capacitación del 50% del capital humano antes del último trimestre del 2024.

Fuente: elaboración propia

Estructura estratégica para el factor de intervención Nº 4 – capacitación

Descripción de la situación

Se pudo evidenciar al desarrollar la matriz DOFA, que una de las debilidades concernientes es la falta de conocimiento de capital humano frente a procesos de estructuración conexos a la implementación de medidas de ciber seguridad y ciber defensa. Por esa razón, esta línea de gestión impone como variable clave: capacitar al capital humano encargado del concepto de seguridad y defensa cibernética; específicamente en dos áreas: administración de la base de datos con Microsoft Azure y utilización de la plataforma WARDEN (modelo predictivo).

Objetivo de la línea estratégica Nº 4

Capacitar al capital humano del MADS y sus entidades adscritas cuya responsabilidad es proteger los sistemas de información cibernéticos centrados en ICCN-MA.

Creación de actividades

Las activades para esta línea estratégica son las siguientes:

Tabla 19 Actividades y descripción para la línea estratégica Nº 4

Actividad	Descripción	Objetivo
Preparación de RR.HH.	Preparación del capital humano para dominar conocimientos asociados a la administración de bases de datos con Microsoft Azure	Llevar a cabo el desarrollo de procesos de preparación para el capital humano que tendrá como función administrativa gerenciar y proteger las bases de datos que se implementen con Microsoft Azure.
Adquisición de RR.HH.	Contratación de recursos humano especializado para la administración y operatividad de la plataforma WARDEN.	Contratar el recurso humano indispensable para utilizar la plataforma WARDEN de acuerdo a las fluctuaciones del contexto.

Fuente: elaboración propia

Conclusiones

La infraestructura crítica cibernética de la nación centrada en el sector de medio ambiente es un campo de estudio naciente. Como se pudo observar en la construcción teórica, este es un sector poco estudiado debido a la complejidad técnica que yace en la genealogía "protección cibernética del medio ambiente".

Uno de los puntos relevantes encontrados en esta investigación es que, para el caso colombiano, ya hay un plan sectorial cuya labor fue analizar los riesgos prominentes al sistema, así como también advertir acerca de posibles hechos de impacto. Entre esos hechos están los ataques directos a la infraestructura crítica del MADS, así como a la infraestructura de sus entidades adscritas; el IDEAM específicamente.

Precisamente, con el análisis cualitativo se identificó un patrón de entorno: es el IDEAM la entidad más atacada y la que mayor cantidad de riesgos y vulnerabilidades presenta. Siendo así, y con base en el diagnóstico que se desarrolló durante la implementación del primer objetivo de investigación, se determinó que el núcleo de posibles amenazas cibernéticas, así como de sus acciones disruptivas, yace en cuatro debilidades conexas: la necesidad irrestrictita que contrae mejorar la protección de bases de datos, la ausencia de un modelo predictivo, las necesidades asociadas a la tecnificación generalizada del sistema digital y la capacitación técnica y micro-focalizada para el capital humano que hace parte del sistema.

Estos cuatro puntos o factores de intervención llevaron a la proposición de cuatro líneas de gestión con las cuales constituir una propuesta estratégica que apunte a: primero, acelerar la migración de datos que reposa en las *database* hacia un sistema de administración digital con mayor capacidad y efectividad tecnológica. Para el caso, y gracias a la asesoría de los expertos, se determinó como herramienta predilecta al software Microsoft Azure.

Segundo, adecuar un modelo predictivo que permita analizar el entorno a partir de una perspectiva micro-segmentada. De ahí que surgiera como una necesidad formal la

implementación de la plataforma de *forecasting* y *foresigth* conocida como Warden Software. En efecto, la implementación de la plataforma es un componente innovador que conduce a la proposición de un tercer factor para solucionar la problemática: tecnificar el subsistema de protección macro-digital que emplea el MADS y sus entidades adscritas. Cuarto, iniciar una campaña de capacitación y actualización para potenciar el dominio y capacidad cognoscitiva que posee el capital humano del sector de medio ambiente.

Para finalizar, la respuesta a la pregunta de investigación determinaría entonces que los elementos, campos y/o componentes por fortalecer con el esquema de ciberdefensa de la infraestructura crítica del sector ambiental son: primero, las bases de datos como principal activo estratégico de información; segundo, la anticipación y predicción de ciber ataques con tipologías complejas y desconocidas; tercero, la tecnificación generalizada y vertical de los subsistemas de información y la capacitación micro-especializada para el capital humano.

Referencias

Abbott, D. (2010). The Handbook of Fifth-Generation Warfare.

Anabalón, J., & Donders, E. (2014). Una revisión de ciberdefensa de infraestructura crítica. *Estudios Seguridad y Defensa*, 3-9.

Aziz, S., & Dowling, M. (2019). Machine learning and AI for risk management. In Disrupting finance. *Palgrave Pivot, Cham.*, (pp. 33-50).

Barford, P., Dacier, M., Dietterich, T. G., Fredrikson, M., Giffin, J., Jajodia, S. y Yen, J. (2010). Cyber SA: Situational awareness for cyber defense. *Cyber situational* awareness, 3-13.

Buchanan, B. (2020). The hacker and the state: Cyber attacks and the new normal of geopolitics. Harvard University Press.

Burov, O. Y. (2016). Educational networking: human view to cyber defense. *Інформаційні технології і засоби навчання*, 144-156.

Carlini, A. (2016). Carlini, A. (2016). Ciberseguridad: un nuevo desafío para la comunidad internacional. *Bie3: Boletín IEEE, (2).* 950-966.

CCIT. (2021). *Tendencias Cibercrimen Colombia 2019-2020.* Investigativo, CCIT, Departamento de amenzas ciberneticas, cibercrimen y ciberseguridad, Bogotá D.C.

Chauvel, L. E. (2020). El pueblo de la Web. Consecuencias de la mediatización y transformación de la esfera política. The Web's people. Digital enunciation and transformation of the political sphere. 135.

CISA. (12 de enero de 2021). *nación, Agencia de seguridad y ciber seguridad para la infraestructura crítica de la*. Obtenido de 2021 Trends Show Increased Globalized Threat of Ransomware: https://www.cisa.gov/uscert/sites/default/files/publications/AA22-040A_2021_Trends_Show_Increased_Globalized_Threat_of_Ransomware_508.pdf

Corneil, D. (2010). Harboring Wikileaks: Comparing Swedish and American press freedom in the Internet age. . *Cal. W. Int'l LJ,* , 41, 477.

Cujabante, X. A., Bahamón, M. L., Prieto, J. C., & Quiroga, J. A. (2020). Ciberseguridad y ciberdefensa en Colombia: un posible modelo a seguir en las relaciones cívico-militares. *Revista Científica General José María Córdova*, 1-12.

Denning, D. (2014). Framework and principles for active cyber defense. *Computers & Security*, 108-113.

Deseriis, M. (2013). Is Anonymous a new form of Luddism? A comparative analysis of industrial machine breaking, computer hacking, and related rhetorical strategies. . *Radical History Review, 2013*, (117), 33-48.

Díaz, J. (2010). LA CIBERSEGURIDAD EN EL ÁMBITO MILITAR. En *Ciberseguridad, Retos, Amenazas a la Seguridad Nacional en el Ciber-espacio* (págs. 217-256). Madrid: Ministerio de Defensa - Cuadernos de Estrategia.

Fedulova, S., & Pivovarov, O. A. (2019). *Global Water Security in the Critical Infrastructure Management: Physical, Cybernetic and Human Aspects.* Boston: Universidad Estatal de Ucrania.

Garcia, J. (2019). *Este es el estado actual de la inteligencia artificial a nivel mundial, según el AI Index Report 2019.* Obtenido de Artificial Intelligence Index Report 2019: https://www.xataka.com/inteligencia-artificial/este-estado-actual-inteligencia-artificial-a-nivel-mundial-ai-index-report-2019

Gordon, S., & Ford, R. (2002). Cyberterrorism?. *Computers & Security, , 21*(7), 636-647.

Harries, D., & Yellowlees, P. (2013). Cyberterrorism: Is the US healthcare system safe?. *Telemedicine and e-Health*, 61-66.

Informe SAFE. (2021). *Tendencias del Cibercrimen 2021-2022 "Nuevas Amenazas al Comercio Electronico".* Informes de Ciber seguridad atendiendo las necesidades del e-commerce. Bogota: TIC TAC.

LA REPUBLICA. (2022 de Marzo de 19). Cantidad de ciberataques aumentaron 4% en América Latina durante el año pasado. *La República* (1).

Lee, C. S., Choi, K., Shandler, R., & Kayser, C. (2021). Mapping global cyberterror networks: an empirical study of al-Qaeda and ISIS cyberterrorism events., 333-355. *Journal of Contemporary Criminal Justice*, 333-355.

Ludlow, P. (2010). Wikileaks and hacktivist culture. . *The Nation,*, 4, 25-26.

Martinez Lopez, L. P. (2021). El Cibercrimen en Colombia. *CCIT*, 15.

Meléndez, A. M., Taboada, D. M., & J. E. (2017). Competitividad en pymes familiares: aportes al desarrollo económico en Colombia Competitiveness in family pymes: contributions to economic development in Colombia. . *LIBRO DE MEMORIAS, ,* 349.

Ministerio de Medio Ambiente y Desarrollo Sostenible. (2018). *Plan Sectorial de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia Sector Ambiente y RRNN PSPICCN V 1.0.* Bogotá D.C.: Publicaciones del MADS.

Ministerio de Tecnologías de la Información y las Comunicaciones. (2020). *Modelo Nacional de Gestión de Riesgos - Seguridad Digital.* Bogotá D.C.: Publicación MINTIC.

Morán, D. R. (2015). La visión internacional de la ciberseguridad. . *Pre-bie3, (2), 15.*

Organización de Estados Americanos. (4 de junio de 2002). *Declaración de Bridgetown*. Obtenido de http://www.oas.org/xxxiiga/espanol/documentos/docs_esp/agcgdoc15_02.htm

Ospina Díaz, M. R., & Sanabria Rangel, P. E. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. *Revista Criminalidad, 62*(2), 199-217.

Pastor, O., Pérez, J., Arnáiz, D., & Taboso, P. (2009). Seguridad Nacional y Ciberdefensa. *Cuadernos Catedra,* 12-24.

Realpe, M., & Cano, J. (2020). Amenazas Cibernéticas a la Seguridad y Defensa Nacional. *Reflexiones y perspectivas en Colombia*, 1.12.

Rossi, G. (12 de enero de 2021). MAESTRÍA EN DIPLOMACIA Y RELACIONES INTERNACIONALES. *TESIS PARA OBTENER EL GRADO DE MAESTRO EN DIPLOMACIA Y RELACIONES INTERNACIONALES*. Lima, Perú: Repositorio de la Academia de Diplomacia y Relaciones Internacionales del Perú.

Samoriski, J. H. (2020). Encryption and Hacking: Cyphers, Hacks and Attacks on the Digital Frontier. In Reimagining Communication: Action . *Routledge.*, (pp. 89-106). .

Sánchez, C. M. (2020). Dos ejemplos de transparencia claudicante: La protección de datos y los secretos de Estado. . *Revista española de la transparencia, ,* (10), 129-150.

Villanueva Méndez, J. C. (2015). *La ciberdefensa en Colombia.* (Bachelor's thesis, Universidad Piloto de Colombia).

Zhang, L., & Vrizlynn, T. (2021). Three decades of deception techniques in active cyber defense - Retrospect and outlook. *Computers & Security*, 1-10.

Lista de Tablas

Lista de Figuras