Proyecto organizacional para la optimización del sistema de ciberseguridad del centro de educación militar

José Vicente Aranda Gómez
Jairo Andrés Becerra

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

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

2020

PROYECTO ORGANIZACIONAL PARA LA OPTIMIZACIÓN DEL SISTEMA DE CIBERSEGURIDAD DEL CENTRO DE EDUCACIÓN MILITAR

(2018 – 2020)

JOSÉ VICENTE ARANDA GÓMEZ

MAESTRÍA EN CIBERSEGURIDAD Y CIBERDEFENSA

ESCUELA SUPERIOR DE GUERRA

COMANDO GENERAL DE LAS FUERZAS MILITARES

BOGOTÁ, DC.

OCTUBRE 2020

PROYECTO ORGANIZACIONAL PARA LA OPTIMIZACIÓN DEL SISTEMA DE CIBERSEGURIDAD DEL CENTRO DE EDUCACIÓN MILITAR

Autor:

JOSÉ VICENTE ARANDA GÓMEZ

Director:

JAIRO ANDRÉS BECERRA

ESCUELA SUPERIOR DE GUERRA

2020

Tabla Contenido

Índice de tablas

Índice de figuras

Resumen

Este trabajo de investigación se desarrolló en el Centro de Educación Militar bajo los lineamientos conceptuales adquiridos desde la ejecución de cada uno de los saberes que hacen parte de la Maestría en ciberseguridad y ciber-defensa de la Escuela Superior de Guerra; como objetivo general se planteó estructurar un proyecto organizacional para la optimización del sub-sistema de ciber-seguridad del Centro de Educación Militar, con el fin de prevenir traumatismos inter-sistémicos derivados del impacto multidimensional generados por actores endógenos (unidad) y exógenos (ciber-delictivos).

Para lograr su desarrollo se plantearon cuatro fases intermedias, en la primera se realizó un diagnóstico empleando una matriz DOFA y una matriz MEFE- MEFI; en ese estudio se identificaron los vacíos inter-sistémicos primarios. Para el caso, es necesario destacar que las fallas poseían dos espectros, unos técnicos y otros de categoría socio-humanística.

Seguido al diagnóstico, el lector encontrará un estudio de tipología micro-etnográfico. Ese estudio es determinante para comprender tres factores de interés; primero, la inmersión de tipologías y virologías complejas es un suceso de ocurrencias comunes, factor que transformado a esta fenomenología en un vector que hace parte de la cotidianidad de los funcionarios del CEMIL (interacción usuario y sistemas de información).

Segundo, concomitancia de errores básicos como el intercambio de equipos, el uso de dispositivos de extracción de información externos, y el empleo multi-actor de los sistemas de información. Tercero, violación de códigos de seguridad correlacionados con la protección del data-warehouse y de la blackboard (activo estratégico primario del Centro de Educación Militar).

El diagnóstico y el estudio micro etnográfico coadyuvaron con la construcción de las fallas, necesidades y posibles soluciones. Una tercera parte compete a la formulación y estructuración del proyecto de intervención mediante metodología Marco Lógico; para el

desarrollo de toda la investigación se utilizó un enfoque de tipología mixta, cuyo diseño de investigación, subdividido en cinco fases, correspondió a la categoría transeccional.

Palabras clave: Ciberdefensa, CEMIL, Ciberseguridad, Stakeholders, ColCERT, Data Warehouses, Ciberamenazas, OVA´s, DOFA, Método Delphi, Método Mic Mac.

Abstract

This research work was developed at the Military Education Center under the conceptual guidelines acquired from the execution of each of the knowledge that is part of the Master's Degree in cyber-security and cyber-defense of the ESDEGUE; As a general objective, it was proposed to structure an organizational project for the optimization of the cyber-security sub-system of the Military Education Center, in order to prevent inter-systemic trauma derived from the multidimensional impact generated by endogenous (unit) and exogenous (cyber) actors. -criminal).

To achieve its development, four intermediate phases were proposed, in the first a diagnosis was made using a SWOT matrix and a MEFE-MEFI matrix; in that study, primary intersystemic gaps were identified. In this case, it is necessary to highlight that the faults had two spectra, some technical and others of a socio-humanistic category.

Following the diagnosis, the reader will find a micro-ethnographic typology study. This study is essential to understand three factors of interest; First, the immersion of complex typologies and virologies is an event of common occurrences, a factor that transformed this phenomenology into a vector that is part of the daily life of CEMIL officials (user interaction and information systems).

Second, the concomitance of basic errors such as the exchange of equipment, the use of external information extraction devices, and the multi-actor use of information systems. Third, violation of security codes correlated with the protection of the data-warehouse and the blackboard (primary strategic asset of the Center for Military Education).

The diagnosis and the micro-ethnographic study contributed to the construction of the failures, needs and possible solutions. A third part competes in the formulation and structuring of the intervention project using the Logical Framework methodology; For the development of all research, a mixed typology approach was used, whose research design, subdivided into five phases, corresponded to the transectional category.

Key Words: Cyberdefense, CEMIL, Cybersecurity, Stakeholders, ColCERT, Data Warehouses, Cyber threats, OVA's, SWOT, Delphi Method, Mic Mac Method.

Glosario

Ciberseguridad. Desarrollo de acciones que se orientan a la prevención de riesgos concernientes al campo de la virtualidad. Esos riesgos son: animadversión, alteración o disrupción del orden digital.

Riesgos en ciberseguridad. Estos riesgos hacen alusión a acciones o factores de contexto que pudieren afectar el marco natural de orden digital, procesos IT y otros elementos que dependen de un proceso digital ya preestablecido.

Estrategia de ciberseguridad. Este término compuesto explica que la importancia que subyace en la conformación de acciones preventivas, dirigidas a la reducción de riesgos digitales que pudieren poner en peligro a un núcleo de acción o de función coligado a escenarios o estructuras digitales.

Prospectiva. Es la disciplina que se encarga de estudiar escenarios a futuro, sean ellos posibles, probables o remotos.

Mic Mac. Software empleado para desarrollar análisis estructurales simples o complejos.

Mactor. Software que se encarga de desarrollar un análisis multimodal que emerge de la postura conceptual que poseen diferentes expertos en temáticas comunes o individuales.

MEFE. Este término hace alusión a una de las herramientas que se emplea en el análisis inter-objetivo y estratégico del entorno. MEFE significa Matriz para el Análisis de Factores Externos.

MEFI. Este término aduce a una de las herramientas empleadas durante el análisis inter-objetivo y estratégico del entorno. MEFI significa Matriz para el Análisis de Factores Internos.

Introducción

Este trabajo de investigación se desarrolló en el Centro de Educación Militar bajo los lineamientos conceptuales adquiridos desde la ejecución de cada uno de los saberes que hacen parte de la Maestría en ciberseguridad y ciber-defensa de la Escuela Superior de Guerra. Este trabajo de investigación contó con un objetivo general, el cual buscaba estructurar un proyecto organizacional para la optimización del sub-sistema de ciber-seguridad del Centro de Educación Militar, con el fin de prevenir traumatismos inter-sistémicos derivados del impacto multidimensional generado por actores endógenos (unidad) y exógenos (ciber-delictivos).

Para dar completitud a este objetivo general, fueron planteadas cuatro fases intermedias (objetivos específicos). El primero de ellos compete a la realización de un método diagnóstico mediante el empleo aplicativo de una matriz DOFA y una matriz MEFE-MEFI. En ese estudio se identificaron los vacíos inter-sistémicos primarios. Para el caso, es necesario destacar que las fallas poseían dos espectros, unos técnicos y otros de categoría socio-humanística.

Seguido al diagnóstico, el lector encontrará un estudio de tipología micro-etnográfico. Ese estudio es determinante para comprender tres factores de interés. Primero, la inmersión de tipologías y virologías complejas es un suceso de ocurrencias comunes, factor que transformado a esta fenomenología en un vector que hace parte de la cotidianidad de los funcionarios del CEMIL (interacción usuario y sistemas de información).

Segundo, concomitancia de errores básicos como el intercambio de equipos, el uso de dispositivos de extracción de información externos, y el empleo multi-actor de los sistemas de información. Tercero, violación de códigos de seguridad correlacionados con la protección del data-warehouse y de la blackboard (activo estratégico primario del Centro de Educación Militar).

El diagnóstico y el estudio micro etnográfico coadyuvaron con la construcción de las fallas, necesidades y posibles soluciones. Una tercera parte compete a la formulación y estructuración del proyecto de intervención mediante metodología Marco Lógico. Para el desarrollo de toda la investigación se utilizó un enfoque de tipología mixta, cuyo diseño de investigación, subdividido en cinco fases, correspondió a la categoría transeccional.

Capítulo 1
Descripción del problema

El Centro de Educación Militar hace parte del Comando de Educación y Doctrina. Sobre el CEMIL reposan múltiples responsabilidades, todas ellas asociadas con el paradigma "educación". A pesar de poseer una carga con múltiples responsabilidades, el CEMIL aún depende de los subsistemas de ciber-seguridad que proceden desde el Centro de Seguridad Informática del Ejercito Nacional, siendo este una sub-sección diseñada para estructurar y proponer paradigmas estratégicos correlacionados con la variante "ciber-seguridad interna". En el año 2017, fue realizada una inspección a los subsistemas diseñados para garantizar el concepto de ciber-seguridad en el CEMIL (Centro de Educación Militar , 2017), los resultados obtenidos permitieron detectar tres falencias o vacíos inter-sistémicos.

El primero de estos vacíos yace en la caracterización de las problemáticas comunes en materias de seguridad, en especial de aquellas que requieren del diseño de un subsistema especializado en sistemas de protección para la categoría "educación virtual". Esta problemática puede ser estudiada a partir de la construcción de entornos descriptivos de los que provendrían hipótesis o planteamientos para el mejoramiento. Por tanto, no es en sí un problema de naturaleza funcional, sino más bien sistémico.

El segundo hallazgo hizo alusión a la estructura y arquitectura de sistemas internos. De forma directa, la crítica planteaba que el sistema de ciber-seguridad del CEMIL no era apto para la necesidad constante que implicaba la carga laboral y estudiantil distribuida a través de los diferentes subsistemas para la enseñanza de oficiales y suboficiales. Este hallazgo, al igual que el primero, propuso el desarrollo de un sistema de ciber-seguridad apropiado; sin embargo, la concretización de ese proyecto se imposibilitaba, pues no existían estudios o investigaciones coligadas a la detección de fallas y demás preceptos de función procedentes del sistema de ciber-seguridad empleado.

El tercer hallazgo radicaba en el desconocimiento de los procedimientos y protocolos diseñados para la materialización, en detalle, de la política de ciberseguridad propuesta para el CEMIL. Este hallazgo permitió identificar que el recurso humano es el factor que presentó el mayor número de debilidades, toda vez que el grupo laboral del CEMIL carece de conocimiento en temáticas interconectadas con ciberseguridad y protección de los subsistemas, lo que desestima todo precepto coligado a la construcción de políticas de "auto-protección".

Los tres hallazgos deducen que el CEMIL presenta un problema en general en temas que se asocian al marco – objeto de la seguridad digital. Esta problemática es el resultado que procede por la convergencia de las tres causales consiguientes:

i. Primero, el sistema de ciber-seguridad del CEMIL no posee un concepto categórico micro-focalizado en la categoría "educación virtual".

ii. Segundo, insistencia de investigaciones o exploraciones investigativas que permitan la estructuración de un proyecto de gestión para dar optimización sistema de ciber-seguridad actual.

iii. Tercero, el recurso humano del CEMIL es uno de los dinamizantes primarios en la generación de traumatismos inter-sistémicos conexos al concepto organizacional de "ciberseguridad".

Ahora bien, la exposición de las causales que conducen a la concepción de una problemática más general, lleva a esta parte de la investigación a señalar que, de no solucionar factores que conciernan a la seguridad digital de la estructura educacional del CEMIL o incluso, al fortalecimiento de la estrategia o modelo de ciberseguridad actual, el Centro de Educación Militar deberá afrontar problemas extensivos, de tipología compleja, caracterizados por ciber-ataques a la infraestructura crítica digital que regula y administra las

diferentes plataforma de enseñanza, secuestro y extracción de información clasificada y disrupción de los indicadores básicos que garantizan el concepto de ciberseguridad en el CEMIL.

Pregunta de investigación

¿Cómo optimizar el modelo de ciberseguridad organizacional que posee el Centro de Educación Militar a fin de prevenir traumatismos inter-sistémicos derivados del impacto multidimensional generado por actores endógenos (unidad) y exógenos (ciber-delictivos)?

Justificación

El desarrollo de la investigación es justificable en pro de cuatro hechos o escenarios. El primer factor subyace en la perspectiva organizacional. Este factor busca demostrar que, en efecto, el sistema de ciberseguridad que posee el CEMIL no es el adecuado para la función que le fue asignada. Es decir, la generalidad del modelo de ciberseguridad que regula al CEMIL desestima constantes necesarias para la protección de fuentes de información interconectadas con las plataformas de enseñanza y aprendizaje, los sistemas administrativos y los sistemas confidenciales y clasificados, empleados en el desarrollo de ejercicios de simulación y entrenamiento especializado.

El segundo factor es alusivo a la perspectiva disciplinar. La perspectiva disciplinar sirve para justificar el proyecto, toda vez que no existen investigaciones previas que demuestren con claridad cuáles son las dificultades, falencias y vacíos funcionales que posee el sistema de ciber-seguridad del Centro de Educación Militar. Al no existir un precepto investigativo anticipado, no existirá modelo de mejoramiento alguno que facilite a la institución desarrollar proyectos de optimización o mejoramiento del sistema en mención.

El tercer factor para justificar esta investigación corresponde al marco de la seguridad institucional. Este elemento hace parte del tercer eje del Plan Bicentenario y demanda el robustecimiento de sistemas y subsistemas internos, necesarios en el desarrollo de capacidades diferenciales. Mírese que este aparte es objetivo y micro-focalizado. Es decir, exige la construcción de elementos organizacionales para la protección de todo sistema o subsistema de gestión, inteligencia, información o entrenamiento, siendo el CEMIL un allegado de la última variable.

El cuarto factor de justificación surge de la realización de una investigación de tipología mixta que pueda entregar a la comunidad científico-militar un constructo o producto innovador, caracterizado por la creación de un modelo ciberseguridad estandarizado para los sectores organizacionales concernientes a la función educativa, preparatoria o instruccional.

Objetivos

Objetivo general

- **Estructurar** un proyecto organizacional para la optimización del Sistema de ciber-seguridad del Centro de Educación Militar **con el fin** de prevenir traumatismos inter-sistémicos derivados del impacto multidimensional generado por actores endógenos (unidad) y exógenos (ciber-delictivos).

Objetivos específicos

- **Realizar** un análisis situacional del modelo de gestión de ciber-seguridad del Centro de Educación Militar **a través** de un método de correlación y comparación de subsistemas.
- **Desarrollar** un estudio micro-etnográfico de la cultura en ciber seguridad de los funcionarios que hacen parte del CEMIL **con el propósito** de identificar las fallas desde el marco del recurso humano.
- **Estructurar** un estudio en prospectiva que permita la identificación de tendencias asociadas a la generación de modelo de gestión de ciber-seguridad para el Centro de Educación Militar.
- **Plantear** requerimientos, protocolos y actividades necesarias para la estructuración de un proyecto organizacional de optimización del modelo de ciberseguridad que posee el Centro de Educación Militar

Marco metodológico

La investigación a desarrollar se llevará a cabo a través de cinco fases. Cada una de las fases busca dar completitud a los objetivos de investigación planteados. Ahora, el lineamiento metodológico de la investigación estará basado en los aportes de Hernández, Fernández y Baptista (2006), por tanto, para materializar procesos metodológicos claros, la investigación contará con los siguientes acápites:

i. Tipo y enfoque de la investigación
ii. Alcances de la investigación
iii. Diseño investigativo
iv. Correlación metodológica

Tipo y enfoque de la investigación

El tipo de investigación es de clasificación "compleja" y el enfoque de naturaleza mixta. Este tipo de investigación permitirá el empleo de herramientas de análisis y recolección de datos cualitativos y cuantitativos. Por tanto, plantear hipótesis o escenarios de optimización implicará una revisión de la literatura, la construcción de marcos teóricos y conceptuales y el análisis de datos a través de encuestas de percepción.

Alcances de la investigación

Los alcances de esta investigación son de tipo correlacional y exploratorio. Desde la tipología correlacional, la investigación busca realizar análisis modélicos a partir de la transección de datos teóricos, estadísticos y métodos descriptivos e intermodales. Tal vez es por esto que el método de búsqueda de información obedecerá a la categoría triangular.

El alcance exploratorio planteará un límite metodológico al cual llegarán los instrumentos para la recolección de datos, que para el caso de esta investigación obedecerán a una tipología de características prospectivas (análisis y construcción de escenarios).

Diseño de la investigación

El diseño de la investigación es de tipo transeccional. Este diseño facilita la interconexión de datos, teorías y métodos. (Ver figura 1).

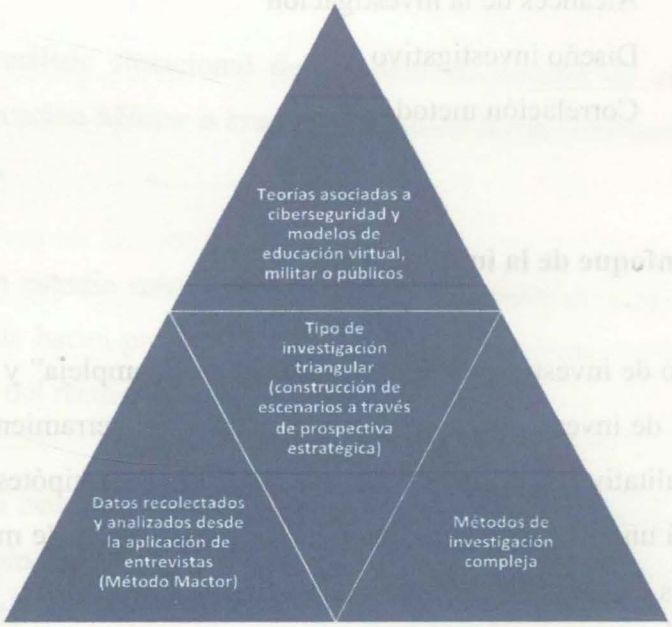

Figura 1 Modelo triangular
Fuente: elaboración propia con información
Interpretada de Hernández et al. (2006)

El tipo transeccional admite el empleo de un concepto de correlación metodológica. La correlación en este caso advierte el uso de cinco fases. Cada una de las fases posee relación e interdependencia. El análisis del diseño de la investigación es funcional. El diseño se explica mediante la construcción de una hoja de ruta sujeta a la correlación del método de investigación por materializar.

Correlación metodológica

Como se explicó con anterioridad, la investigación está subdividida en seis fases. La explicación de las fases es la siguiente:

- **Primera fase.** En esta fase de la investigación, el autor construye una relación causal entre antecedentes investigativos, proposiciones teoréticas y disposiciones conceptuales. El marco de referencia en este caso hace alusión a la comprensión de distintas posiciones académicas asociadas con las categorías: ciber-seguridad y optimización. Para tal fin, el autor da una respuesta rápida a la pregunta de investigación mediante la identificación de una ruptura epistémica. La teoría, los conceptos y los antecedentes coadyuvan a delimitar y re direccionar el objetivo general de la investigación.

- **Segunda fase.** En esta fase de la investigación se desarrolla un estudio de características micro-etnográficas. La identificación del número muestral, y la caracterización de la población llevan a esta fase a desarrollar un ejercicio de recolección de datos. El instrumento de recolección corresponde a una encuesta general de pregunta estructurada. Su explicación depende de un análisis por porcentajes y promedios de respuesta. Ambas variables, la concepción teórica y la construcción de hipótesis basadas en el análisis de percepciones cualitativas y cuantitativas (datos de encuesta) facilitan la realización de un nuevo proceso, el estudio en prospectiva.

- **Tercera fase.** El estudio en prospectiva, diseñado a partir de las hipótesis trazadas durante la segunda fase de la investigación, busca construir tres escenarios en los que la intervención o solución de la problemática del CEMIL terminaría siendo un obstáculo para el desarrollo de procesos educacionales ligados a seguridad y defensa nacional y conocimientos aledaños al factor "ciencias militares". El estudio

complementará ambas. A través de la contribución de cuatro expertos en materias de ciberseguridad, el estudio entregará una construcción hipotética de escenarios. De ahí, que la estrategia por esbozar posea insumos suficientes para diseñar líneas de acción, intervención y prevención en temáticas de ciberseguridad y seguridad informática en el Centro de Educación Militar.

- **Cuarta fase.** La cuarta fase trata de la estructuración de un proyecto de inversión organizacional en el que las líneas de acción tendrían que ser la actualización del subsistema de ciberseguridad del CEMIL, creación de una oficina de seguridad informática y la capacitación del recurso humano, siendo la anterior un factor vital para el funcionamiento de la estrategia a desarrollar. Para llegar a este punto deben diseñarse, un árbol de problemas y objetivos. Seguido, serían propuestas las gestiones de control y ejecución, estas son: stakeholders, riesgos, costos y adquisiciones.

- **Quinta fase.** La última fase comprende el diseño de los protocolos que no están sujetos a ninguna clase de adquisición estructural o material, sino más bien a toda acción sujeta al concepto estratégico de lo funcional. En esta fase estarán los protocolos de intervención ligados a la supervisión de procesos y procedimientos, junto a la anexión de la oficina de contrainteligencia al marco base de ciberseguridad para el CEMIL.

Capítulo 2
Marco de referencia

Tal y como se planteó en el diseño de la investigación, el desarrollo del marco de referencia busca interpretar antecedentes investigativos, a fin de hallar rupturas epistémicas, la identificación de teorías apropiadas para analizar, delimitar y orientar el interés objetivo del proyecto y definir conceptos interconectados a las tres categorías de la investigación: ciberseguridad, ciber-prevención y optimización para subsistemas de información.

En la primera parte del marco de referencia, estado del arte, el investigador entrega un estudio de los antecedentes. El estudio está compuesto por posturas diversas. Cada una de las posturas comprende líneas de contribución, comprensión e interpretación de nuevos aportes a la ciencia computacional. Cabe recordar que, para el caso de esta investigación, la disciplina única de estudio es "ciberseguridad". En el estado del arte, los lectores encontrarán una discusión acerca de la importancia de un modelo de ciberseguridad en que exista dependencia entre: actores de interacción (capital humano - endógenos) y elementos tecnológicos (exógenos).

En la segunda parte se hace una explicación descriptiva de tres teorías, la teoría de los juegos, la teoría del conflicto y la teoría de la ciberdefensa. Con la teoría de los juegos, el investigador indaga acerca del rol que desempañan los actores que están inmersos en la problemática. Mediante los juegos y haciendo énfasis en el equilibrio de Nash, el investigador da a conocer la importancia que nace de la relación causal entre ciberseguridad internacional y estrategias de prevención y anticipación a nivel organizacional.

Otro acápite teorético comprende al estudio observacional de la teoría del conflicto. Esta parte de la investigación da al lector una idea clara de la construcción social (humanista, económica o tecnológica) u escenario cotidiano del que surgen múltiples factores o situaciones conflictuales. En esta parte del sustento teórico, el lector construirá una hipótesis propia a partir de la importancia que poseen los protocolos de ciberseguridad (tecnología) y componentes instruccionales orientados a la preparación del capital humano.

En la tercera fase se incluye un análisis explicativo de la teoría de la ciberdefensa. Dicho análisis sustenta cuán importante es el diseño de modelos únicos de ciberseguridad. De la defensa tipo ciber se desprende el concepto de seguridad clase "ciber". De allí, que la relación entre ambas categorías sea proteger, prevenir y anticipar cualquier ataque de naturaleza digital.

La parte final del marco de referencia data de la conceptualización de categorías que fueron propuestas en los objetivos específicos y en la pregunta de investigación. Con la teoría, el estudio de investigaciones previas y definición de diferentes conceptos, se traza una respuesta inicial de la pregunta de investigación. Esta ha de definirse o configurar durante el desarrollo de los resultados (capítulo 4).

Estado del arte

Diferentes aportes relevantes para el desarrollo de esta investigación radican en ciclos exploratorios como los de Borja (2016). De acuerdo con Borja (2016): "(...) la ciberseguridad es una propuesta de reacción en materias de defensa nacional. Su alcance aborda distintas aproximaciones, pues no puede centrar su direccionamiento funcional en la constante securitista únicamente" (p. 83). Esto quiere decir que la ciberseguridad es la repuesta a una eventualidad poco conocida hasta el año 2000. Tal vez es por esto que una de las críticas más llegadas al concepto de seguridad procede de su naturaleza de reacción, poco alineada con las funciones de prevención y anticipación.

Para Borja (2016), la relación entre seguridad y espectro ciber, replantea el concepto mismo de defensa nacional, pues para el caso, el diseño de sistemas para la seguridad de los Estados debe estar atado al lineamiento de los intereses nacionales, siendo estos de tipología ciber. Por ejemplo, Estados como Suiza y Suecia poseen sistemas de gobierno altamente dependiente a la dinámica de las Tecnologías de Información y las Comunicaciones, facto por el cual construyen fuertes subsistemas de ciberseguridad,

por el cual construyen fuertes subsistemas de ciberseguridad, coligados con el paradigma nacional, pero desagregados en pro de cada uno de los sectores de posibles impactos.

Así las cosas, Suiza y Suecia cuentan con modelos de ciberseguridad en los que existe inter-dependencia entre objetivos estratégicos, objetivos estatales e interés nacionales. Algo que llama la atención en el contexto del Estado suizo es que el sistema de ciberseguridad está orientado a la protección de sistemas alternos, no solo a los preceptos básicos de seguridad antiaérea o seguridad naval. Según Ramírez (2017), sectores financieros, de salud y de educación son los espectros prioritarios para la protección por parte de Suiza.

En tanto, la ciberseguridad de estos Estados es multidimensional e intersectorial. En este caso, Borja (2016) hace énfasis en la construcción de cibersistemas en los que el objetivo sea múltiple, pues no podría existir prelación o preferencia, toda vez que los intereses del Estado son diversos, y no recaen únicamente en la variable "seguridad y defensa nacional". Ahora, aunque su objetividad es múltiple, su naturaleza es exclusiva, y depende de la capacidad de análisis en prospectiva que puedan llegar a desarrollar los actores involucrados.

Mírese que en este acápite se realiza un realce conceptual allegado a los actores involucrados. De ahí, que la objetividad se pluralista, pues cada uno de los sectores del gobierno, liderado por un actor primario, debe velar para que existan parámetros de protección, por parte de un ciber-modelo y de un esquema tradicionalista.

Sin embargo, y este uno de los hallazgos de Borja (2016), las bases culturales del trabajo en seguridad y defensa, analizadas desde la concepción "ciber" , dejan entrever una serie de elementos y constantes asociadas con el paradigma "reacción-prevención". El factor de reacción-prevención ha servido como hoja de ruta en la estructuración de ciber-sistemas para la protección de las instituciones del Estado. En tanto, la ciberseguridad desde el hallazgo de Borja (2016) carece de visos funcionales, necesarios para la construcción de escenarios a futuro.

Al igual que Borja (2016), Ramírez (2017) es enfático al demarcar que un modelo de ciberseguridad debe obedecer condicionamientos múltiples, es decir, no solo sujetarse a la línea de seguridad y defensa nacional, pues de ella parten los principios, pero de esta también derivan múltiples obligaciones, en gran mayoría correlacionadas al concepto de seguridad integral. Es este tipo de seguridad la que demanda una construcción multimodal de las facetas de defensa, siendo el caso de la ciberseguridad, una repuesta misma a la necesidad de los contextos.

Frente a esta nueva constante, el contexto, Ramírez (2017) describe que: "(…) muchas opiniones han servido para debatir temáticas impuestas por el desafío que subyace en el surgimiento de nuevas amenazas a la seguridad de los Estados, el ciber terrorismo es una de ellas" (p. 84). Por ende, el debate de la ciberseguridad no podría estudiarse a partir de la proposición de ideas o sistemas pasados, pues el ciberterrorismo, mutación del cibercrimen, es frecuente, y en su esencia yace un vector dinámico que sobrevalora la capacidad del cibersistema nacional de seguridad.

Un ejemplo de ello surge de ciberataques como los que fueron presenciados en Lituania para el año 2007. El ciberataque llamado "Windows hell" logró desestabilizar el sistema de saneamiento de aguas residuales en la parte norte del país. Este daño generó el cese del trabajo funcional de la planta Eschvestein por seis días, produciendo un efecto dominó que se reflejó en la pérdida de 93 millones de dólares (costos de reparación) y el desabastecimiento del recurso hídrico por tres días para los habitantes de la ciudad de Kaunas.

El ejemplo de Lituania sirve para comprender cómo el concepto intersectorial del cibercrimen finiquita quebrantando esquemas básicos del sistema de seguridad y defensa nacional. Obsérvese que sus impactos no son del todo una acumulación de intenciones y objetivos apuntados al aparato militar; todo lo contrario, el ciberterrorismo apunta a

La contribución de Ramírez (2017) posee propiedades funcionalistas. Para el autor, la ciberseguridad es una función del Estado. Tal función recae en el concepto de seguridad, pero analizando el mismo en pro de la estructuración de tres conceptos: el objetivo del Estado, la estrategia del Estado y los intereses nacionales por proteger.

El objetivo del Estado hace alusión a la línea de acciones y tareas por completar. En cuanto al objetivo estatal, el investigador es reiterativo al confirmar que la función del Statu Quo no es otra diferente a la reguardar la integridad física e intangible de los sistemas colectivos (actores poblacionales). A ello, que cualquier tipo de afección, material o inmaterial, pasaría a ser responsabilidad inmediata del Estado, pues es este el garante del respeto hacia derechos básicos (Vida, Educación, Saludad, Protección Social, etc.).

El segundo concepto, el de la estrategia del Estado, está más aproximado al sistema de seguridad y defensa. La estrategia del Estado para el caso en desarrollo, es aquella que se encarga de estructurar parámetros, visiones, misiones y actores asociados, orientados a la prevención de todo factor de riesgo que pueda poner en peligro al modelo de seguridad nacional, seguridad pública y seguridad ciudadana. Entonces, para hacerle frente a una amenaza de tipología ciber, el Estado debe reconfigurar toda base inter-sistémica que no esté conectada al sistema de ciberseguridad.

El tercer concepto emerge de los intereses nacionales por proteger. Los intereses nacionales, sean estos públicos o estratégicos, hacen parte de un segmento estatocéntrico, del que proceden diferentes elementos de intervención. Varios de estos elementos influyen en la conexión que existe entre bienestar colectivista y seguridad integral. Aunque los intereses nacionales son parámetros imprescindibles para conocer cuál es el objetivo geopolítico y geoestratégico del Estado, estos podrían carecer de alineación interinstitucional, puesto que, por un lado, el objeto del Estado y los métodos de protección no están acordes con la fluctuación de los contextos.

interinstitucional, puesto que, por un lado, el objeto del Estado y los métodos de protección no están acordes con la fluctuación de los contextos.

Al igual que Ramírez (2017), Castelbondo (2017) trae a colación una postura conceptual que procede del resultado de una investigación multimodal. Para el autor, la ciberseguridad es una línea más del aparato de seguridad y defensa nacional. Ahora, su efectividad no está comprobada, ya que si se observaran las estadísticas transeccionales que realiza el conteo de la cantidad de ciberataques por parte de la Secretaría de Seguridad Multidimensional de la OEA se llegarían a distinguir cuatro trazos característicos a nivel Latinoamérica. Estos son:

i. Primero, el 40% de los ciberataques posee una naturaleza compleja; es decir, frente al concepto de seguridad y defensa nacional, si se realizara una comparación entre el momento de reacción, neutralización y reducción de impactos, se obtendría un número porcentual no mayor a 39,2% frete a la variable "efectividad".

ii. El 62% de los ciberataques está dirigido al sector financiero, mientras que el sector educativo, el sector de salud pública y el sector defensa ocupan otro 38%.

iii. En Sur América, Perú, Argentina y Colombia son los países que mayores niveles de infección inter-sistémica poseen. Para el caso de Perú y Colombia, los sectores más atacados serían los concernientes a "finanzas" y "seguridad y defensa". (Ver tabla 1)

iv. El 54,1% de los ciberataques proviene de países como: Rusia, Brasil, China, Estonia, Ucrania y Latvia.

Rango superior	País	Tasa de infección
1	China	53,85%
2	Taiwán	39,57%
3	Turquía	37,50%
4	Polonia	36,65%
5	Perú	35,63%
6	Rusia	34,55%
7	Argentina	34,42%
8	Canadá	34,31%
9	Colombia	33,33%
10	Brasil	32,25%

Rango superior	País	Tasa de infección
45	Suecia	16,18%
44	Reino Unido	18,18%
43	Portugal	18,55%
42	Suiza	19,23%
41	Alemania	20,69%
40	Francia	21,02%
39	Países Bajos	21,07%
38	Venezuela	23,13%
37	Estados Unidos	23,85%
36	España	26,82%

Fuente: información recuperada de OEA (2018)

Los resultados investigativos obtenidos por Salazar (2017) permiten el pre establecimiento de hipótesis socio-científicas en las que el concepto de ciberseguridad pasaría a ser la repuesta a una fenomenología criminal creciente. De ahí, que la versión de Posada (2017), otro investigador del campo de las ciencias jurídicas, enfocado al marco de la tipicidad del delito mediante factos de hecho como los cibercrimenes, llegar a discernir que, a la luz del derecho internacional, la ciberseguridad vendría a ser una especie de paradoja que surge debido a la evolución constante de amenazas de tipología transnacional e híbridas.

Mírese que la afirmación de Posada (2017) va de la mano de la inclusión de una nueva forma de observación: la categorización del ciber crimen. Para Posada (2017):

> (…) parece necesario y relevante complementar las categorías tradicionales del delito en la tipicidad, con una perspectiva digital que, por cierto, ya no es la excepción a la regla, sino que comienza a ser la regla general en la criminalidad moderna. Esto, incluso en ámbitos hasta ahora reservados a la criminalidad física, como la criminalidad organizada y transnacional, que comienza a actuar mediante organizaciones virtuales transnacionales (OVT) que dificultan aún más combatir este tipo de delincuencia sin fronteras. (p. 107)

Por ende, la creación de organizaciones virtuales transnacionales, producto transmutativo de la acción ciber-terrorista de amenazas computacionales básicas, es el siguiente paso en la esfera del cibercrimen organizado; así las cosas, los modelos estatales diseñados para garantizar los conceptos básicos de seguridad integral deben estar sujetos a la realidad

Por ende, la creación de organizaciones virtuales transnacionales, producto transmutativo de la acción ciber-terrorista de amenazas computacionales básicas, es el siguiente paso en la esfera del cibercrimen organizado; así las cosas, los modelos estatales diseñados para garantizar los conceptos básicos de seguridad integral deben estar sujetos a la realidad fluctuante de los contextos, pues tal y como es argumentado por Posada (2017), existe una tendencia evolutiva hacia la aparición de ciberamenazas poco contempladas por el sistema internacional de la OEA que se encarga de temáticas coligadas a ciberseguridad, ciberdefensa y estudio de los patrones del ciberterrorismo.

Por otro lado, realizando una aproximación nacional a la problemática en cuestión, es conveniente analizar el núcleo de antecedentes investigativos a partir de la relación tácita que existe entre ciberseguridad y sistemas de seguridad y defensa nacional colombianos. Esta afirmación trae a colación una hipótesis de interés, en la que es necesaria la descripción analítica de los efectos y consecuencias del cibercrimen y ciberterrorismo en el Estado colombiano.

Una de los planteamientos más apropiados para explicar cómo surge el modelo criminal en Colombia procede de las investigaciones de Castillo (2017). Según Castillo (2017) "(...) para entender el surgimiento del cibercrimen en Colombia, teniendo en cuenta que este representa una tipología delincuencial poco estudiada, es necesaria la explicación de la política de seguridad digital" (p. 73)

La afirmación del investigador, adjudica entonces una responsabilidad circunstancial a la Política Digital que posee el país. No obstante, el autor es crítico en describir también que tal política es obsoleta, pues entre el 2016 y el 2018 Colombia recibió más 242 millones de ciberataques.

De esta cantidad, el 65,2% estaba dirigido el sector ciudadanía, siendo en este contexto el ciber delito una variante apropiada para explicar la conexión que hay entre vulnerabilidad, desconocimiento y poca acción interviniente por parte de las autoridades pertinentes. El sector gobierno ocupa el 23,9%. De este segmento provienen los ataques

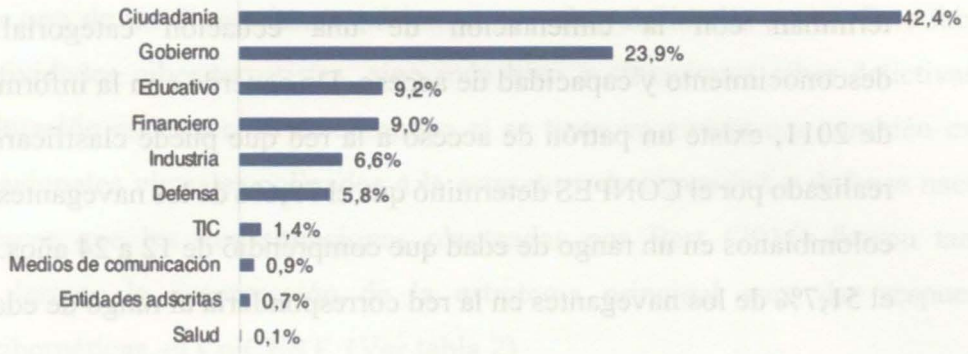

Figura 2 Histograma con datos de sectores ciber-atacados
Fuente: información recuperada de CONPES 3854

Para el caso colombiano, la ciudadanía es el sector más afectado. Estos impactos son explicables a partir de dos hipótesis que poseen naturalezas correlacionales. La primera hipótesis subyace en el aumento de las conexiones a banda ancha. Según MINTIC (2017), durante los últimos 10 años (2008-2018), el incremento de los usuarios con acceso a internet se elevó en un 27,2%. Esto quiere decir que en la actualidad 17,2 millones de colombianos poseen amplio acceso a la red. Frente a esto, el MINTIC (2017) explica que el aumento más notable empezó en el año 2014. El aumento en este caso posee una relación directa entre la cantidad de usuarios que pueden acceder y la cantidad de usuarios que no poseen el conocimiento básico para navegar. (Ver figura 3)

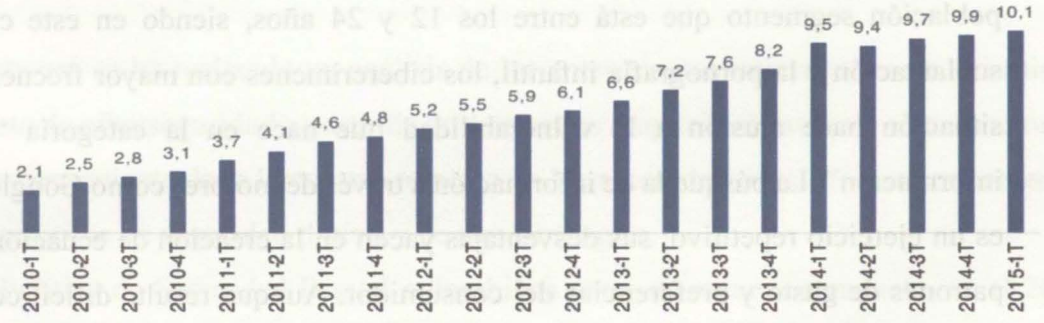

Figura 3 Histograma personas con acceso a internet
Fuente: información recuperada de CONPES 3854

El rango de edades es un segmento de metadatos que coadyuva a entender cómo los términos "inmigrantes digitales" y "nativos digitales", propuestos por Prensky (2001),

terminan con la cimentación de una ecuación categorial: vulnerabilidad, edad, desconocimiento y capacidad de acceso. De acuerdo con la información del CONPES 3701 de 2011, existe un patrón de acceso a la red que puede clasificarse por edades. El estudio realizado por el CONPES determinó que el 79,6% de los navegantes, para el año 2014, fueron colombianos en un rango de edad que comprendió de 12 a 24 años. Asimismo, para el 2013, el 51,7% de los navegantes en la red correspondería al rango de edad 5 a 11 años.

Esto quiere decir que el aumento es evolutivo. Es decir, la relación entre el número de vulnerabilidades, el número de usuarios y su capacidad de acceso (nativos digitales) es paralela. En tanto, la segunda parte de la hipótesis encontraría un sentido en la variable "desconocimiento". Para sustentar esta afirmación, se incluye en la investigación la contribución praxeológica de Bert (2016).

Durante el desarrollo de una investigación de tipología aplicada, Bert (2016) halla en el desconocimiento de los usuarios una vulnerabilidad de riesgos propensos. Es decir, el desconocimiento que los usuarios poseen frente al uso de la red, pone en peligro su integridad. Para esto, Bert (2016) ejemplifica tres situaciones clásicas. La primera de ellas estima que el acceso masivo a datos por parte de las redes sociales es en sí un gap sistémico poco intervenido por los actores de seguridad y defensa nacional.

Este hallazgo toma relevancia una vez que se identifica como blanco objetivo a la población segmento que está entre los 12 y 24 años, siendo en este caso la estafa, la suplantación y la pornografía infantil, los cibercrimenes con mayor frecuencia. La segunda situación hace alusión a la vulnerabilidad que nace en la categoría "búsqueda de la información". La búsqueda de información a través de motores como Google, Yahoo! o Bing es un ejercicio repetitivo; sus desventajas yacen en la creación de ecuaciones de búsqueda, patrones de gusto y preferencias del consumidor. Aunque resulte difícil comprender, estos vectores permiten al ciber-delincuente o ciber-terrorista establecer un perfil de ataque, colectivo, no individual, que pueda llegar a generar un impacto de tipología masiva.

La tercera situación, de gran interés para el desarrollo de la presente investigación, corresponde al acceso a plataforma de educación y aprendizaje. En Colombia, el sistema

educacional es uno de las dimensiones que mayores vulnerabilidades posee. Este facto no compete a actividades ciber-terroristas, sino más bien a situaciones ciber-delictivas. No obstante, la situación en este caso se complica si se tiene en cuenta que también existen sistemas educacionales virtuales coligados a la estructura de seguridad y defensa nacional. Cabe de destacar que las tres situaciones planteadas por Bert (2016) fueron también consideradas durante la construcción de la estrategia principal para dar respuesta a emergencias cibernéticas, el ColCERT. (Ver tabla 2)

Tabla 2

Actividades con mayor frecuencia de acción en red

Actividad en línea	2014	2015	2016	2017	2018	2019
Redes sociales	63,2	65,1	67,6	67,1	69,6	68,3
Obtenet información	61,7	63,4	65,1	66,9	71,1	69,5
Correo y mensajería	57,6	59,8	63,3	65,5	68	68,9
Educación y aprendizaje	36,7	42,2	52,4	54	57	58
Actividades de entrenamiento	28,7	34,3	43,1	46,2	49,2	53,3
Consulta de medios de comunicación	9,9	11,1	17,7	19,8	22,3	25

Fuente: información recuperada de CONPES 3854 de 2011, 3701 de 2016 e Informe de Gestión Ciber-seguridad Digital (2019)

Hasta acá se ha realizado un análisis de los antecedentes investigativos concernientes al concepto de ciberseguridad a partir de dos espectros amplios, el nacional e internacional. Por ello, es conveniente dar a lector una relación de los antecedentes investigativos haciendo uso de las políticas de seguridad digital y de sus estrategias.

La Política de Seguridad Digital colombiana nace, de manera compacta, en el 2011. La política de seguridad propuso en ese tiempo la creación del Grupo de Respuesta a Emergencias Cibernéticas, de ahora en adelante ColCERT. El ColCERT posee una función primaria, reaccionar ante cualquier eventualidad, y, por intermedio de los actores

La Política de Seguridad Digital colombiana nace, de manera compacta, en el 2011. La política de seguridad propuso en ese tiempo la creación del Grupo de Respuesta a Emergencias Cibernéticas, de ahora en adelante ColCERT. El ColCERT posee una función primaria, reaccionar ante cualquier eventualidad, y, por intermedio de los actores institucionales involucrados, construir una repuesta apropiada para decrecer el nivel de impacto.

Obsérvese que la prioridad del ColCERT en este caso es preventiva; tal y como se discutió al principio, no hay una relación prospectiva entre las variables seguridad, intervención temprana y desarticulación anticipada de Organizaciones Virtuales Transnacionales. Si se estudiaran las herramientas que posee el ColCERT para hacerle frente a la aparición de nuevas emergencias[1], se distinguiría que: primero, hay una notable interdependencia entre las bases de datos internacionales (CVSS[2]) y la construcción de estrategias nacionales; segundo, no hay claridad en cuanto al número de ciberataques presentados por año, o por sector, lo que imposibilita conocer el objeto básico del ciber-atacante y sus métodos de interdicción.

La primera política de seguridad digital, que como se aclara comienza con el ColCERT, coadyuva al sistema general de seguridad y defensa nacional para co-crear estrategias de seguridad y defensa nacional, encabezadas por el MEN y el MINTIC, y direccionadas hacia el establecimiento de políticas de protección y reacción frente a posibles ciberataques o cibercrimenes. En tanto, como respuesta al creciente hecho de ciberataques que Colombia presenció entre el 2005 y 2010, es creada la Estrategia Intersectorial.

La estrategia intersectorial está conformada por tres organizaciones militares: el Comando Conjunto y Cibernético de las Fuerzas Militares, el Centro Cibernético Policial y el ColCERT. La función de cada uno de estos entes yace en la prevención y reacción ante la inminente posibilidad de ciberataques, sean estos criminales o terroristas.

[1] Acciones cibercriminales o ciber-terroristas

[2] Esta sigla se remite al Sistema para el análisis de vulnerabilidades, o por su definición en inglés Common Vulnerability Scoring System.

la nación respondería a 198 millones de ciberataques, siendo en este caso el quinto Estado más atacado.

Tabla 3
Posición de Colombia en la escala de ciberataques resumen (2014-2018)

Nº	País	%
1	Estados Unidos	19,14
2	India	12,54
3	México	11,8
4	Brasil	9,5
5	Corea	8,21
6	Rusia	5,8
7	Egipto	5,4
8	Colombia	3,1
10	Malasia	2,9
11	Ucrania	2,9
12	Pakistan	2,7
13	Perú	2,5
14	Irán	2,3
15	Arabia Saudi	2,1

Fuente: información recuperada de CONPES 3854 de 2011, 3701 de 2016 e Informe de Gestión Ciber-seguridad Digital (2019)

Las cifras reflejadas traen a colación un cuestionamiento base ¿por qué Colombia es un país blanco para los ciber-atacantes? Aunque no hay repuesta investigativa a la pregunta estipulada, si hay hipótesis conceptuales que ayudarían a construir una repuesta base. Quizá la contribución de Lynn (2016) sea la más adecuada para responder. Según Lynn (2016): "la visión geopolítica y geoestratégica del Estado colombiano, en relación con los nexos estratégicos que sostiene con Estados Unidos, es una de las aseveraciones necesarias a la hora de distinguir al Estado como blanco base de los ciber-delincuentes" (p. 83)

Se podría debatir la afirmación de Lynn (2016) al suponer que existen vulnerabilidades y riesgos propensos debido al desconocimiento de los usuarios. No obstante, el mismo ColCERT es enfático al afirmar que el 67,2% de los ciberataques registrados para el 2018,

Se podría debatir la afirmación de Lynn (2016) al suponer que existen vulnerabilidades y riesgos propensos debido al desconocimiento de los usuarios. No obstante, el mismo ColCERT es enfático al afirmar que el 67,2% de los ciberataques registrados para el 2018, por ejemplo, proviene de naciones extranjeras, en tanto, la problemática no es de naturaleza nacional.

La segunda versión de la política digital proviene del CONPES 3854 de 2011. Este documento es reiterativo en cuatro bases conceptuales, necesarias para entender la problemática. A partir de este CONPES, la política de seguridad transmuta y empieza a ser considerada una política allegada al precepto de seguridad y defensa nacional. De ahí que el documento persista en que:

> El creciente uso del entorno digital en Colombia para desarrollar actividades económicas y sociales, acarrea incertidumbres y riesgos inherentes de seguridad digital que deben ser gestionados permanentemente. No hacerlo, puede resultar en la materialización de amenazas o ataques cibernéticos, generando efectos no deseados de tipo económico o social para el país, y afectando la integridad de los ciudadanos en este entorno. (CONPES 3854, 2011, p. 03)

Entonces, el carácter figurativo de la política va de la mano de la capacidad de intervención que el Estado o que las instituciones públicas puedan proferir en pro de la construcción de sistemas de defensa que estén caracterizados por la presencia de factores prospectivos y anticipativos. Para dar con tal fin, el CONPES 3854 busca analizar, primeramente, una línea de obstáculos y de desavenencias organizacionales, poco favorables para dar completitud a una política real.

El primer obstáculo surge de la desarticulación de sistemas de protección que existe entre en las instituciones públicas y los métodos de resguardo planteados por el aparato de seguridad y defensa nacional. La desarticulación en este caso, se refiere a la poca eficiencia inter-sistémica que poseen los métodos de protección; véase que en el caso colombiano no existe un sistema único de prevención anticipación; es más, el 78,2% del concepto de ciberseguridad es administrado por compañías privadas Hernández (2017).

El tercer obstáculo, procede de la complejidad tipológica que coexiste en la naturaleza de los ciber ataques. Véase que a pesar de que desde el 2011 hay una estrategia de características intersectoriales, la reducción de ciberataques ha sido de -12,1%, ahora, la eficiencia es más notable cuando son analizadas las estadísticas no de reducción, sino de disminución de impactos. (Ver figura 4)

Figura 4 Histograma de ciberataques más comunes
Fuente: información recuperada de CONPES 3854 de 2011, 3701 de 2016 e Informe de Gestión Ciber-seguridad Digital (2019)

Un último obstáculo surge de la insuficiencia de esfuerzos de cooperación internacional. Es decir, en Colombia no había asociatividad de intenciones y objetivos, esto es tal vez lo producía el diseño de estrategias de ciberseguridad desalineadas con el ordenamiento operacional y jurídico internacional. Frente a esto, Hernández (2017) argumenta que:

> En Colombia, se evidencia que existen esfuerzos aislados de cooperación nacional e internacional por parte de los responsables de la seguridad digital, por lo que se presentan dificultades en el intercambio de conocimiento, experiencias, investigación, desarrollo de nuevas tecnologías, e información relacionada con los incidentes digitales. Los esfuerzos en materia de cooperación, colaboración y asistencia internacional en seguridad digital, no son suficientes ni responden a una estrategia permanente que maximice su aprovechamiento. (p. 82)

En el análisis subsecuente de los antecedentes investigativos hay convergencia de tres patrones de interés. El primero de ellos corresponde a una estrategia de ciberseguridad

> asistencia internacional en seguridad digital, no son suficientes ni responden a una estrategia permanente que maximice su aprovechamiento. (p. 82)

En el análisis subsecuente de los antecedentes investigativos hay convergencia de tres patrones de interés. El primero de ellos corresponde a una estrategia de ciberseguridad generalizada, lo que ralentiza la construcción de micro estrategias de intervención o anticipación en un nivel focalizado.

El segundo, el sector educación, para el contexto "educación virtual militar", es uno de los espectros en el que se presenta un gran número de ciber ataques; no obstante, para el sector público, en el que no hay contratación de actores de protección privados, especializados en el tema ciber, es difícil esbozar estrategias de anticipación o reacción temprana, por ende, sobre ese sub-sistema, habría un gap de tipología funcional y estructural.

El tercero, el sector gobierno, en cabeza de sus ministerios e instituciones, posee un elemento estratégico de intervención que no está basado núcleos de acción intermodal. Es decir, la naturaleza de la defensa para el caso del sistema de ciberseguridad colombiano no está orientada al micro segmentación de variables estratégicas.

Hasta acá se han planteado posturas investigativas internacionales detalladas y nacionales generales. Es conveniente en tanto analizar la problemática a partir de una revisión de antecedentes investigativos provenientes del análisis de artículos de investigación, resoluciones del comando cibernético de la policía y documentos adjunto, derivados de investigaciones nacionales previas.

Una consideración primaria proviene de las investigaciones de De Ocampo (2019). En su tesis de maestría titulada "Modelo de Ciberseguridad para la Protección del Banco de Datos de la Universidad Junín" De Ocampo (2019) empieza por la configuración de un modelo desagregado, es decir, biparticionado en diferentes fases y etapas. Cada una de las fases buscaba identificar actores y vectores tecnológicos.

Es así, como De Ocampo (2019) entra a discutir la importancia de modelos de ciberseguridad en los que el personal de funcionarios es un actor de prevención o de causalidades. Por un lado, el autor es enfático al discernir que el modelo de ciber-seguridad a imponer debe venir acompañado de campañas instruccionales en las que el capital humano atraviese una fase cultural, caracterizada por la concientización. Por otro, es imperativo que el capital humano entienda la responsabilidad que trae el acceso continuo a sistemas de información institucionales, expuestos al secuestro o robo de información frecuente.

Diferente a la proposición de De Ocampo (2019), y acudiendo a la Circular 2354 de 2019, publicada por el Comando Cibernético de la Policía Nacional (2019), Castillo (2019) allega a esta investigación un aporte significativo interconectado con la construcción de modelos de ciberseguridad a partir de la protección primaria de datos y metadatos. En su investigación, el autor logra descubrir tres vacíos principales.

El primer vacío concierne a la transmutación constante de virologías y ciberamenazas. El autor difiere de los modelos de ciber-seguridad actuales, mucho más de aquellos que pertenecen a entidades públicas, pues la actualización depende de tramitologías y aspectos económicos. Ello imposibilita actualizar esquemas de ciber-protección, a tiempo y realidad de contextos en los que hay amplia interacción.

Poniendo como ejemplo problemas e inconvenientes técnicos derivados de procesos de actualización del modelo de ciberseguridad del Banco de la República, Castillo (2019) discierne que: "(…) el sistema de actualización en materias de ciberseguridad no puede depender de procesos o fases contractuales. La ralentización de los procesos imposibilita generar cobertura totalizada de esquemas y sistemas de función e información" (p. 83).

La contribución de Castillo (2019) pone en duda la efectividad de los ciber-sistemas de protección, pues el modelo ciber depende de actualizaciones constantes, factor que dificulta protección total en entidades que no poseen un proceso de contratación privado. Similar a

Castillo (2019), pero refiriéndose nuevamente al capital humano, Castillo (2019), discute que:

> (…) un modelo de ciberseguridad debe enfocarse en tres facciones: humanísticas, tecnológicas e inter-sistémicas. Los tres poseen naturaleza inter-dependiente. No hay, por ende, argumentación distinta. Un argumento clave para conocer falencias y problemas yace en la distinción individual de los vacíos. (…) el 80% de la ciber-responsabilidad recae en el personal de inter-nautas.

Al igual que Castillo (2019), pero estribado el tema a un micro-segmento que identifica al problema de la ciber-seguridad como concepto propio de actualización, y no como elemento exógeno (ciberamenazas), Carreño (2019) entra a debatir que la ciberseguridad en Colombia es una acción sujeta a la fluctuación de múltiples tendencias. Sin embargo, discute el investigador, ninguna de ellas trata de agrupar las líneas de ciber protección y ciber-prevención, bajo un mismo esquema; ello ha generado división de esfuerzos cibernéticos.

Para ambientar sus resultados, Carreño (2019) aplica un instrumento de recolección de datos a la empresa ANSAS SAS (Aserradero del Norte). La recolección de datos fue de tipo transeccional. Eso indica que el análisis de los datos se desarrolló en tres perspectivas. En la primera perspectiva, la técnica, el investigador determinó que actualizar el sistema no es suficiente; deben unirse a él técnicas de monitoreo y protección preventiva (seguridad digital). En la segunda, la inter-sistémica, el autor dispuso de dos técnicas de prevención, protección de data *warehouses* y protección de *clouds*. En la tercera, el investigador aduce que el entrenamiento del capital humano es fundamental. Por ello, existe una necesidad, alinear sistemas, protocolos, gestiones y comportamientos preventivos.

Quizá, llame la atención que en la afirmación de Carreño (2019) existe especial cuidado por el capital humano. Por ello, es conveniente aunar a la construcción de los antecedentes resultados investigativos como los de Bolaños (2019). Para Bolaños (2019), quien basa su investigación en la norma ISO 2732, la preponderancia, es decir, importancia *ad hoc* de un

sistema de ciber-seguridad radica en el diseño de políticas de prevención que pongan en consideración la importancia del rol del capital humano.

Para explicar la idea de Bolaños (2019) es necesario analizar que:

i. La ciberseguridad es un principio de protección para la estructura organizacional.

ii. La ciberseguridad es una estructura construida en pro de: tecnología y factor socio-humanista.

iii. La ciberseguridad es una variable múltiple. Es decir, se necesitan diferentes perspectivas para contrarrestar cualquier tipo de ciber-delito. Por consiguiente, el ciber-sistema debe ser: transversal a toda función, vertical ante todo proceso e intersectorial (gestiones y áreas de función).

Diferente a la idea de Bolaños (2019), también sujeto a la concepción de la ISO 2732, Ramírez (2020) interviene para diseñar un modelo de ciberseguridad basado en los principios de flexibilidad, análisis de contexto, prevención de posibles ciber-acciones y profundidad investigativa al momento de diseñar modelos de ciber-prevención, en los que el capital humano es un actor de interés prioritario.

En sus investigaciones aplicativas, Ramírez (2020) entra a discutir que el capital humano es el acelerante principal de los factores generadores de riesgo. Por consiguiente, desarticulación de programas de prevención en ciber-seguridad es sinónimo de animadversión y propensión a riesgo. Ahora, la visión objetiva de Ramírez (2020) es integral; aun así, permite dividir acciones, factores y posibles estrategias, gran parte ellas direccionadas al mejoramiento de las técnicas de prevención y anticipación para el capital humano.

Otra fuente para analizar el precepto de ciber-seguridad haciendo uso de las perspectivas base, capital humano y concepto técnico, proviene de investigaciones como las de Cala (2019). Para este autor existen diferentes modelos de ciberseguridad. El 80% de los modelos

desarticulación de programas de prevención en ciber-seguridad es sinónimo de animadversión y propensión a riesgo. Ahora, la visión objetiva de Ramírez (2020) es integral; aun así, permite dividir acciones, factores y posibles estrategias, gran parte ellas direccionadas al mejoramiento de las técnicas de prevención y anticipación para el capital humano.

Otra fuente para analizar el precepto de ciber-seguridad haciendo uso de las perspectivas base, capital humano y concepto técnico, proviene de investigaciones como las de Cala (2019). Para este autor existen diferentes modelos de ciberseguridad. El 80% de los modelos se diseña en pro de dos características: optimización de conocimiento del capital humano que interactúa con los sistemas de información y construcción de códigos de seguridad.

La afirmación de Cala (2019) da a entender que, si bien es necesario actualizar sistemas y todo aquel aspecto que esté asociado con tecnología de protección o intervención, es también indispensable actualizar conocimientos que se dependan del manejo de redes y escenarios virtuales por parte del personal de funcionarios, públicos o de sector privado.

Al igual que Cala (2019), Chesney (2020) entra a rebatir ciertas posturas. Para Chesney (2020) un modelo de ciberseguridad actual debe enfocarse sobre la perspectiva tecnológica. Es decir, la preparación del capital humano es importante. Sin embargo, cada software de ciber-protección debe codificarse a partir del principio de prevención automática. De ahí, que el desconocimiento o insuficiencia digital cultural de los actores se asuma como factor de riesgo, propenso, pero solucionable.

Una de las particularidades de la investigación de Chesney (2020) yace en la conceptualización de los modelos de ciberseguridad por tipo, orden y categoría organizacional. Según el autor, cada corporación, de acuerdo con el orden de gestiones y objetividad *per se*, amerita el diseño único de modelo de ciber-seguridad. Por ende, aunque los patrones, acciones, códigos y programas de prevención son repetitivos, los sistemas de

Por tal razón, la ruptura epistémica que da origen a la pregunta de investigación del proyecto en desarrollo, radica en conocer cómo optimizar el sistema de ciberseguridad de una plataforma virtual de aprendizaje en temáticas de seguridad y defensa nacional; para este caso es seleccionado un elemento muestral específico, el Centro de Educación Militar.

Marco teórico

Desarrollar el marco teórico para el constructo investigativo en proceso, requiere la inclusión de diferentes posturas académicas. Esto implica interpretar ciberseguridad y ciberdefensa desde debates conceptuales en los que hay divergencia de términos, puesto que ambos pueden encajar en la misma posición teórica pero no en una misma definición de roles y funciones. La conceptualización lleva a esta investigación a proponer tres líneas teóricas altamente asociadas con el concepto de ciberseguridad. Estas líneas son:

i. La teoría de los juegos, una perspectiva del concepto de ciberseguridad.

ii. La teoría del conflicto, un análisis desde la multidimensionalidad que abarca el concepto de ciberseguridad.

iii. La teoría de la ciberdefensa, una interpretación desde la obligación intersectorial del Estado.

Teoría de los juegos, una perspectiva desde el concepto de la ciberseguridad

El equilibrio de Nash, desde el que es interpretable la relación ganar-ganar a partir de una visión por-estratégica, puede servir como base referencial para explicar cuál es la importancia que nace en la construcción de escenarios en los que sería inminente un ataque de naturaleza ciber, y cómo, a partir de las herramientas del Estado, resultaría conveniente estructurar propuestas estratégicas, no de prevención, sino de anticipación. Para esta explicación son

iii. La teoría de la ciberdefensa, una interpretación desde la obligación intersectorial del Estado.

Teoría de los juegos, una perspectiva desde el concepto de la ciberseguridad

El equilibrio de Nash, desde el que es interpretable la relación ganar-ganar a partir de una visión por-estratégica, puede servir como base referencial para explicar cuál es la importancia que nace en la construcción de escenarios en los que sería inminente un ataque de naturaleza ciber, y cómo, a partir de las herramientas del Estado, resultaría conveniente estructurar propuestas estratégicas, no de prevención, sino de anticipación. Para esta explicación son utilizadas las posturas investigativas de Roy, y otros (2010), Fraile (2018) y Do, y otros (2017).

En la posición de Roy et al. (2010), el Equilibrio de Nash solo se consigue cuando las partes involucradas llegan a un acuerdo conveniente. Sin embargo, no todos los actores tendrían que estar alineados a la determinación final, pues en este caso, la mayoría representa una animadversión de la conceptualización de "colectividad estratégica". Ahora, en cuanto a la seguridad y versión de "colectividad estratégica" cabría destacar la importancia que el precepto de seguridad intangible significa para dar continuidad a los intereses nacionales.

Al mencionar seguridad intangible (ciberseguridad) y colectividad estratégica se haría necesaria la conclusión del vector inter-sistémico que reposa en los intereses nacionales. Estas categorías conforman un núcleo de acción, cuyos objetivos hacen parte del ya conocido equilibrio de Nash. Es decir, para un Estado es conveniente conocer naciones o gobiernos alternos que coadyuven a alcanzar sus interese nacionales; pues bien, para el caso en cuestión, la cooperación estaría enlazada con el marco de la ciberseguridad.

No obstante, y aunque poco conveniente para todos, tal y como discute Roy et al. (2010), conformar alianzas traería consigo un cúmulo de intereses encontrados, a lo que se llamaría "intereses contrarios".

fría, no tendría que poseer una característica estructural contemporánea, en límites, conexiones marítimas o actores militares terrestres.

En tanto, el desbalance en el equilibrio de Nash produciría la creación de alianzas estratégicas en un espectro electromagnético, poco conocido, dominado y explorado por parte de los actores en conflicto. Mírese que incluso el concepto de alianzas cambia; es decir, no es necesaria la intervención de actores mediante la reproducción de acciones conjuntas y tangibles, puesto que la conexión de redes facilita la coordinación de acciones, objetivos y planteamientos inter-objetivos.

Otro de los aportes de interés provenientes de la concepción teórica de Roy et al. (2010) surge de la caracterización del equilibrio que se expone a través de la descripción del término "cooperación". En este contexto, la cooperación hace parte de los planteamientos inter-objetivos. Es decir, no existiría cooperación de no existir fundamentos básicos como la asociación intereses inter-estatales.

Esto lleva a analizar la línea de patrones mediante la caracterización de los beneficios multi-actor. Los beneficios multi-actor comprueban que, en efecto, el equilibrio de Nash se sostiene, siempre y cuando exista una proposición de favorabilidad para dos o tres actores, siendo un último actor en desacuerdo el que pudiere llegar a plantear los intereses contrarios. Por ello es que la comprobación de la las alianzas planteadas debe sellarse a través de pactos de cooperación.

La cooperación en materias de ciberseguridad, debe establecerse a partir de la relación causal beneficio, estrategia y fin prospectivo. A ello, que Roy et al. (2010) sugiera el diseño de propuestas estratégicas sujetas a la concepción de proposiciones de intervención y anticipación. Para Roy et al. (2010) el equilibrio de Nash, en el caso de la ciberseguridad, es parcial, no es total, toda vez que el mismo está regulado por las proposiciones de intereses nacionales, compatibles o inconvenientes.

Otro de los aportes significativos en este caso procede de Frayle (2018). Para Fraile (2018):

contrarios. Por ello es que la comprobación de la las alianzas planteadas debe sellarse a través de pactos de cooperación.

La cooperación en materias de ciberseguridad, debe establecerse a partir de la relación causal beneficio, estrategia y fin prospectivo. A ello, que Roy et al. (2010) sugiera el diseño de propuestas estratégicas sujetas a la concepción de proposiciones de intervención y anticipación. Para Roy et al. (2010) el equilibrio de Nash, en el caso de la ciberseguridad, es parcial, no es total, toda vez que el mismo está regulado por las proposiciones de intereses nacionales, compatibles o inconvenientes.

Otro de los aportes significativos en este caso procede de Frayle (2018). Para Fraile (2018):

> La teoría de juegos es una teoría famosa para detectar las amenazas y prevenir las amenazas. En el análisis, se pueden considerar diversas estrategias de ataque, como inflación, deflación y oscilación. La teoría de juegos proporciona el entrenamiento básico y la conciencia de los principios algorítmicos clave y las lecciones aprendidas. En teoría de juegos, las estrategias de defensa son detección de valores atípicos y selección de Umbral adaptativo. Utilizando la teoría de juegos, el usuario puede detectar fácilmente a los intrusos y proporcionar la solución a los problemas paso a paso. (p. 27)

La versión de Frayle (2018) está más allegada a una proposición técnica. Es decir, el análisis de la vectorialidad en esa ocasión debería hacerse a través de las descripciones que subyacen en la categorización: ciberseguridad y ciber-canales. Los ciber-canales, de acuerdo con las interpretaciones de Frayle (2018), son los sectores en los que debería existir una relación formal entre actividad y estrategia especializada. Para dar más claridad a esta afirmación es diseñada la figura 5.

La figura 5, facilita comprender la estructura de métodos de intervención planteados por Frayle (2018). Los tres métodos hacen parte de un lineamiento en ciberseguridad, no obstante, sus estrategias cambian; no son las mismas para el caso del sector privado o del sector público. Por ende, desde la concepción de Frayle (2018), los métodos de intervención son todas aquellas figuras o formas que se utilizan para detener o generar disuasión ante posibles factos ciber-delictivos.

Otra de los aportes de Frayle (2018) radica en la consecución del equilibrio de Nash. Para el investigador, en el caso de la ciberseguridad, el equilibrio no se consigue a través de la prelación de favorabilidades que pueda emanar de dos o tres actores diferentes. Contrario a esto, el equilibrio de Nash, en cuanto a las dimensiones de la ciberseguridad, puede conseguirse a partir de la favorabilidad mayor del actor central. Es decir, un solo actor puede llegar a preestablecer un sistema de coacción, obligando a los demás actos a adherirse a la política de ciberseguridad planteada.

Entonces, mírese que al igual que en otras alianzas, la capacidad hegemónica juega un rol vital en la preponderancia de las normas por establecer. Similar a la posición de Frayle (2018), pero haciendo uso de la perspectiva de los actores, Do et al. (2017) describe que:

> (…) en un juego de conveniencias, el actor primario puede beneficiar a los actores secundarios. Por ello, no es necesario conseguir un equilibrio colectivo. En economía, el equilibrio de Nash beneficia a unos cuantos, en ciberseguridad, el equilibrio de Nash los beneficia a todos por igual, pues la complejidad y rapidez de las ciberamenazas con el nivel de impacto generado, no es individual, es colectivo. (p. 291)

La concepción de Do et al. (2017) categoriza toda forma de animadversión. Es decir, en este caso, la ciberseguridad es en sí una forma de defensa interestatal, pues se ha comprobado que un ciberataque solo sigue los principios de la distinción de blancos. Por esta razón, la estructuración de posibles estrategias de intervención debe practicarse desde la razón lógica de los actores que posean un alto nivel de experiencias, conocimientos y métodos de protección, prevención y anticipación.

Entonces, mírese que al igual que en otras alianzas, la capacidad hegemónica juega un rol vital en la preponderancia de las normas por establecer. Similar a la posición de Frayle (2018), pero haciendo uso de la perspectiva de los actores, Do et al. (2017) describe que:

> (…) en un juego de conveniencias, el actor primario puede beneficiar a los actores secundarios. Por ello, no es necesario conseguir un equilibrio colectivo. En economía, el equilibrio de Nash beneficia a unos cuantos, en ciberseguridad, el equilibrio de Nash los beneficia a todos por igual, pues la complejidad y rapidez de las ciberamenazas con el nivel de impacto generado, no es individual, es colectivo. (p. 291)

La concepción de Do et al. (2017) categoriza toda forma de animadversión. Es decir, en este caso, la ciberseguridad es en sí una forma de defensa interestatal, pues se ha comprobado que un ciberataque solo sigue los principios de la distinción de blancos. Por esta razón, la estructuración de posibles estrategias de intervención debe practicarse desde la razón lógica de los actores que posean un alto nivel de experiencias, conocimientos y métodos de protección, prevención y anticipación.

Para el caso Americano, el Estado líder en materias de ciberseguridad es Estados Unidos. Otros países como Chile y México también han desarrollado campañas de intervención y métodos de ciberdefensa, conscientes de la realidad contextual. Uno de estos métodos, el Programa de Ciberseguridad Hemisférico estructurado por la OEA asimila al equilibrio de Nash como a un elemento de favorabilidades múltiples.

Es decir, la construcción de un programa colectivo de sensibilización y protección encuentra en el recurso humano (el usuario) uno de los focos primarios para el desarrollo de ciber-estrategias que puedan producir efectos "reductivos", no preventivos. Esta clase de efectos, son los que el actor más fuerte ofrece; otros como el tecnicismo o lógica estratégica del método planteado son valores agregados que pertenece únicamente a su sistema de ciberseguridad.

es conveniente realizar un análisis primario del conflicto interno; es decir, cuáles son los impactos o efectos que desencadenan ciberataques objetivados hacia la estructura básica de los conglomerados sociales.

Los conflictos internos, generados por la interacción de ciberataques y ciberamenazas a la seguridad pública, se cualifican por la relación constante entre conflictividad social y dinamismo de vectores. Los vectores en esta ocasión representan un avivamiento del conflicto de tipología social, debido a la irrupción de factores cotidianos asociados con las NBI. Así, por ejemplo, un ciberataque al sistema de tratamiento de aguas potables puede llegar a detener el funcionamiento básico de necesidades esenciales, todas ellas de naturaleza poblacional.

Uno de los teóricos más acertados para discutir esta temática es Dewell (2015). De acuerdo con Dewell (2015): "la teoría de los conflictos cubre la aparición de factos conflictuales, modernos y tradicionales" (p. 98). Del interior de la categoría moderna provendrían diferentes elementos, actores u acciones, siendo en el contexto de esta investigación el cibercrimen o el ciberterrorismo fenomenologías complejas, capaces de producir conflictividad social.

En tanto, es la conflictividad social, el hecho principal para la aparición de conflictos de interés internos. Frente a esta afirmación, Klein (2017) procede a realizar una investigación multimodal, de la que saldrían a colación tres hipótesis descriptivas.

La primera hipótesis demanda que, ante la complejidad de los ciber-ataques, la ciber defensa sería entonces una repuesta estatal, apropiada para disminuir el nivel de conflictividad. De ahí, que su naturaleza básica – ciberseguridad- sea reactiva, coligada con la intervención pos-facto.

La segunda hipótesis va de la mano de la evolución constante de las ciberamenazas. Frente a esto, el autor propone que, de cierta forma, la creación de amenazas ciber es paralela al avance de la tecnología, esta afirmación propone un interrogante clave para entender la

conflictuales, modernos y tradicionales" (p. 98). Del interior de la categoría moderna provendrían diferentes elementos, actores u acciones, siendo en el contexto de esta investigación el cibercrimen o el ciberterrorismo fenomenologías complejas, capaces de producir conflictividad social.

En tanto, es la conflictividad social, el hecho principal para la aparición de conflictos de interés internos. Frente a esta afirmación, Klein (2017) procede a realizar una investigación multimodal, de la que saldrían a colación tres hipótesis descriptivas.

La primera hipótesis demanda que, ante la complejidad de los ciber-ataques, la ciber defensa sería entonces una repuesta estatal, apropiada para disminuir el nivel de conflictividad. De ahí, que su naturaleza básica – ciberseguridad- sea reactiva, coligada con la intervención pos-facto.

La segunda hipótesis va de la mano de la evolución constante de las ciberamenazas. Frente a esto, el autor propone que, de cierta forma, la creación de amenazas ciber es paralela al avance de la tecnología, esta afirmación propone un interrogante clave para entender la capacidad de protección que posean los Estados: ¿Tiene el Estado la capacidad tecnológica para evolucionar a la par del cibercrimen?

La tercera hipótesis, preponderante y sobresaliente en pro del interrogante que plantea la segunda hipótesis, es necesaria para distinguir que el concepto de ciberseguridad debe poseer un elemento prospectivo. Por ello, que sus análisis, dese de la teoría de los conflictos, debe empezar con la relación e identificación de posibles causales. Esta identificación facilitaría a los Estados la construcción de escenarios de intervención y acción. El ejemplo gráfico de la tercera hipótesis puede analizarse en la figura 6.

través de la categorización de medios o el estudio de afecciones posibles, probables o inminentes.

La teoría de la ciberdefensa, una interpretación desde la obligación intersectorial del Estado

La ciberdefensa, diferente a ciberseguridad, es un campo de acción con propiedades amplias. En la ciberdefensa, la visión objetiva de los sistemas está encaminada a la creación de elementos de protección que garanticen el funcionamiento base de factores sociológicos, indispensables para garantizar el paradigma "subsistencial".

Autores como Goodman (2010) y Donahue (2017), convergen al discutir que la ciberdefensa es en sí una responsabilidad del Estado. Su diferencia con la ciberseguridad yace en la magnitud y alcance de sus acciones. Mientras que la ciberseguridad está en nivel alterno, la ciberdefensa se encarga de regular toda política de acción que busque hacerles frente a amenazas de tipología cibernéticas, que interactúan en escenarios volátiles, inciertos, complejos y ambiguos (VICA).

Ahora, para Donahue (2017), la responsabilidad de la ciberdefensa es compartida; es decir, son todas las instituciones militares del Estado las encargadas del diseño de una aproximación estratégica que sea útil a la hora de proteger organismos e instituciones públicas, estas últimas necesarias en la satisfacción de necesidades esenciales.

En cuanto al término de ciberdefensa el autor denota que el mismo está compuesto, a diferencia de ciberseguridad, por dos actores claves: los físicos y los intangibles. Los físicos por un lado son todos aquellos usuarios que hacen uso de la red, mientras que los intangibles son los actores o subsistemas virtuales. Ambos, juegan un rol vital en la construcción de escenarios a futuro. Es decir, los dos actores hacen parte de la estructura de protección.

Así las cosas, podrían ser deducidos planteamientos:

de elementos de protección que garanticen el funcionamiento base de factores sociológicos, indispensables para garantizar el paradigma "subsistencial".

Autores como Goodman (2010) y Donahue (2017), convergen al discutir que la ciberdefensa es en sí una responsabilidad del Estado. Su diferencia con la ciberseguridad yace en la magnitud y alcance de sus acciones. Mientras que la ciberseguridad está en nivel alterno, la ciberdefensa se encarga de regular toda política de acción que busque hacerles frente a amenazas de tipología cibernéticas, que interactúan en escenarios volátiles, inciertos, complejos y ambiguos (VICA).

Ahora, para Donahue (2017), la responsabilidad de la ciberdefensa es compartida; es decir, son todas las instituciones militares del Estado las encargadas del diseño de una aproximación estratégica que sea útil a la hora de proteger organismos e instituciones públicas, estas últimas necesarias en la satisfacción de necesidades esenciales.

En cuanto al término de ciberdefensa el autor denota que el mismo está compuesto, a diferencia de ciberseguridad, por dos actores claves: los físicos y los intangibles. Los físicos por un lado son todos aquellos usuarios que hacen uso de la red, mientras que los intangibles son los actores o subsistemas virtuales. Ambos, juegan un rol vital en la construcción de escenarios a futuro. Es decir, los dos actores hacen parte de la estructura de protección.

Así las cosas, podrían ser deducidos planteamientos:

i. Primero, en pro de la teoría de la ciberdefensa, cabría redefinir su concepto ante la materialización de un sistema de protección allegado a la seguridad pública, pero administrado desde la dimensión de la seguridad nacional. Dicho en otras palabras, aunque la ciberdefensa posee un objetivo macro, su obligación es segmental, alineada a la seguridad integral de los actores poblacionales.

La lógica estratégica que encabezan ambos factores -disuasión y prevención- sirve para distinguir funciones asociadas con ciberseguridad. Desde la lógica estratégica, la ciberseguridad representaría un elemento de disuasión, que emplea a la intervención y a la anticipación como a una forma de interacción que sirve para desarticular y reducir la multidimensionalidad de los impactos que generan los ciberataques.

El segundo concepto es aquel que se asocia con seguridad multidimensional. La ciberseguridad es, en definitiva, una de las derivaciones del sistema de seguridad multidimensional, que para el caso americano está ligado con la OEA. La ciberseguridad, vista desde una relación multidimensional de espectros, está encargada de velar por la seguridad de los estamentos, instituciones y actores poblacionales. Su ventaja radica en la micro-segmentación de focos de intervención. Es decir, los espacios o sectores por proteger.

El tercer concepto es ciberdefensa. Este se define como:

> La evolución de las tecnologías de la información y las comunicaciones ha provocado un cambio de paradigmas que exige la adopción de procedimientos especializados para neutralizar y controlar las amenazas cibernéticas. La Ciberdefensa, además de prevenir los ataques como hace la Ciberseguridad, da respuesta a los mismos con nuevos ataques con fin de salvaguardar la seguridad. (I.B.S.-Next, 2017, p. 01)

Por ello, la ciberdefensa es una herramienta de carácter interestatal. Mientras que la ciberseguridad se ocupa de las fenomenologías cibercriminales internas, la ciberdefensa plantea modelos de protección que puedan prevenir y contraatacar en caso de que existan ciber-ofensas por parte de otro actor internacional.

El cuarto concepto emerge de la estrategia interna de los sistemas y subsistemas de seguridad y defensa, en especial de los que están ligados con aspectos básicos como la educación. Tal y como se observó durante el desarrollo del estado del arte, Colombia es una de las naciones con mayor presencia de ciberataques. El 27,2% de las acciones

vista desde una relación multidimensional de espectros, está encargada de velar por la seguridad de los estamentos, instituciones y actores poblacionales. Su ventaja radica en la micro-segmentación de focos de intervención. Es decir, los espacios o sectores por proteger.

El tercer concepto es ciberdefensa. Este se define como:

> La evolución de las tecnologías de la información y las comunicaciones ha provocado un cambio de paradigmas que exige la adopción de procedimientos especializados para neutralizar y controlar las amenazas cibernéticas. La Ciberdefensa, además de prevenir los ataques como hace la Ciberseguridad, da respuesta a los mismos con nuevos ataques con fin de salvaguardar la seguridad. (I.B.S.-Next, 2017, p. 01)

Por ello, la ciberdefensa es una herramienta de carácter interestatal. Mientras que la ciberseguridad se ocupa de las fenomenologías cibercriminales internas, la ciberdefensa plantea modelos de protección que puedan prevenir y contraatacar en caso de que existan ciber-ofensas por parte de otro actor internacional.

El cuarto concepto emerge de la estrategia interna de los sistemas y subsistemas de seguridad y defensa, en especial de los que están ligados con aspectos básicos como la educación. Tal y como se observó durante el desarrollo del estado del arte, Colombia es una de las naciones con mayor presencia de ciberataques. El 27,2% de las acciones cibercriminales está direccionada a la desestabilización de los sistemas de educación nacional, en especial de los que poseen un carácter público.

Por ende, la estrategia interna debe definirse a partir de un planteamiento en el que se hacen explícitas sus funciones, estas son: detección temprana de ciberataques, regulación de impactos, intervención de posibles escenarios cibercriminales, diseño de campañas de concientización y planteamiento de modelos pedagógicos que sirvan para reducir el riesgo prominente.

El CONPES 3854 de 2016 demanda la realización de una estrategia intersectorial. En el documento se pueden hallar direccionamientos y políticas regulatorias, aptas para adaptar la estrategia a cualquier tipo de sistema o subsistema de información, público o privado. Para dar al lector una relación de los lineamientos planteados es diseñada la tabla 4.

Tabla 4
Marco jurídico para la investigación

Acto jurídico	Descripción del acto jurídico	Interpretación a fin para la investigación
CONPES 3854 de 2016	El CONPES ofrece una relación completa de la estrategia estatal orientada a la optimización de los subsistemas de ciberseguridad y ciberdefensa	CONPES alineado con la interpretación de la investigación, allegada a la optimización de las estrategias intersectoriales. (micro focalización de áreas de intervención)
Ley 1150 de 2007	Habeas data, y seguridad de datos informáticos	Esta ley regula el comportamiento de las instituciones financieras, comerciales o de cualquier índole que posean acceso total a datos personales
Ley 1341 de 2009	Tecnologías de la información y aplicación de la seguridad	Esta ley enfatiza toda regulación circunstancial enfocada al empleo de herramientas TIC para la protección privada o pública de los sistemas personales, naturales o jurídicos
Ley 1437 de 2011	Procedimiento administrativo y aplicación de criterios de seguridad	Ley encaminada a la construcción de criterios de administración de sistemas y subsistemas digitales
Ley 1581 de 2012	Ley estatutaria de protección de datos personales	Ley direccionada a la protección de datos y elementos personales que queden registrados en la red. Para esto son empleados

Tabla 4
Marco jurídico para la investigación

Acto jurídico	Descripción del acto jurídico	Interpretación a fin para la investigación
CONPES 3854 de 2016	El CONPES ofrece una relación completa de la estrategia estatal orientada a la optimización de los subsistemas de ciberseguridad y ciberdefensa	CONPES alineado con la interpretación de la investigación, allegada a la optimización de las estrategias intersectoriales. (micro focalización de áreas de intervención)
Ley 1150 de 2007	Habeas data, y seguridad de datos informáticos	Esta ley regula el comportamiento de las instituciones financieras, comerciales o de cualquier índole que posean acceso total a datos personales
Ley 1341 de 2009	Tecnologías de la información y aplicación de la seguridad	Esta ley enfatiza toda regulación circunstancial enfocada al empleo de herramientas TIC para la protección privada o pública de los sistemas personales, naturales o jurídicos
Ley 1437 de 2011	Procedimiento administrativo y aplicación de criterios de seguridad	Ley encaminada a la construcción de criterios de administración de sistemas y subsistemas digitales
Ley 1581 de 2012	Ley estatutaria de protección de datos personales	Ley direccionada a la protección de datos y elementos personales que queden registrados en la red. Para esto son empleados métodos de conservación autorizados por los estamentos de seguridad y defensa nacional. Sin embargo, estos métodos no pueden alejarse de la regulación demandada en la Ley de Habeas Dara

Fuente: elaboración propia con información recuperada de MINTIC (2013)

Capítulo 4
Resultados de la investigación

Los resultados de la investigación serán descritos en orden. Es decir, su explicación irá de la mano del desarrollo de cada uno de los objetivos específicos que fueron planteados. El primer objetivo corresponde al desarrollo de un diagnóstico circunstancial del sistema de ciberseguridad que en la actualidad posee el CEMIL. Una vez finiquitado este punto procede el desarrollo de un análisis micro focalizado de la cultura en ciberseguridad que poseen los funcionarios que hacen parte del Centro de Educación Militar. El tercer resultado compete a la realización de un estudio en prospectiva; mientras que el cuarto corresponde al planteamiento de requerimientos, protocolos y demás gestiones necesarias para la formulación de un proyecto de inversión organizacional que pueda llegar a solventar vacíos institucionales coligados con la insuficiencia de formas de intervención y prevención de posibles ciberataques al sistema que ostenta el Centro de Educación Militar (CEMIL).

Cada uno de los resultados obtenidos es descrito a través de la concepción de tres categorías interconectadas: carencia de sistemas de ciberseguridad orientados específicamente hacia el concepto de seguridad virtual para la educación militar; cultura organizacional poco allegada a la regulación de un sistema de seguridad virtual por parte de los funcionarios públicos y, falta de proyectos de inversión organizacional a raíz de la no estructuración de planteamientos bases.

Análisis situacional del modelo de gestión de ciber-seguridad del Centro de Educación Militar

El modelo de gestión de ciberseguridad que posee el sistema general del Centro de Educación militar se caracteriza por una regulación subdividida en tres segmentos: sistemas tecnológicos, sistemas educacionales y capital humano. Los sistemas tecnológicos hacen alusión al concepto de arquitectura organizacional que yace en la inclusión de un sistema de ciberseguridad diseñado para proteger estándares imprescindibles como información, bases de datos y conceptos funcionales derivados de la plataforma de educación virtual, empleada

en la capacitación de oficiales y suboficiales. Este segmento también compete a todo el subsistema de datos de información, programación, códigos y herramientas de función que son empleadas en la construcción de aulas virtuales, asignaturas y estándares de ciberseguridad.

Los sistemas educacionales, segundo segmento, son administrados a través de un servicio pedagógico especializado, administrado por Blackboard y por el software que ofrece Google Class. Para el contexto, los sistemas educacionales son el objetivo principal del concepto de ciberseguridad en el CEMIL; de este sistema dependen factores necesarios para el funcionamiento del sistema educativo tales como: notas, información de los estudiantes, OVA´s, módulos de enseñanza, herramientas TIC y aulas virtuales.

El último segmento, el capital humano, corresponde al personal de funcionarios públicos que laboran en el CEMIL. Esta parte del sistema de ciberseguridad concierne a la concientización de usuarios, pues como bien se ha analizado, son ellos el factor que mayores riesgos y vulnerabilidades generan.

Con base en la anterior información, convendría aclarar que la primera herramienta de análisis para el modelo de gestión de ciberseguridad que posee el CEMIL corresponde a una matriz DOFA de correlación y ponderación de variables. Esta matriz coadyuva a crear una línea de estrategias e hipótesis, las cuales se evalúan y analizan en profundidad. Para el desarrollo de la matriz son expuestas las variables de análisis en la Tabla 2; una vez identificadas las variables, se procede con el desarrollo de la matriz. (Tabla 3), y, por último, a la evaluación y ponderación de posibles estrategias procedentes del ejercicio de transección de amenazas, oportunidades, debilidades y fortalezas (Tabla 5).

Ahora bien, en la matriz de exposición de las variables DOFA (Tabla 5), hay cuatro casillas descriptivas. En la primera se expone el componente como tal (variable); en la segunda se asigna un porcentaje de ponderación que corresponde a la constante "nivel de importancia" que posee la variable; en la tercera está el nivel de impacto que la variable causa sobre el objetivo funcional de un modelo clásico o moderno de ciberseguridad,

cuando está diseñado para servir a guarniciones o instituciones militares. Al final hay una casilla en la que se refleja el resultado próximo de las ponderaciones.

Tabla 5
Variables DOFA

DOFA				
Factor Interno **Debilidades**	**Componente**	**Pond.**	**Nivel de Impacto**	**Calificación Ponderada**
D1	El CEMIL no posee un sistema de ciber-seguridad especializado en temas de educación militar	4%	5	0,2
D2	El sistema de ciber-seguridad del CEMIL no posee un componente técnico especializado, orientado hacia el factor de prevención	2%	4	0,08
D3	La estrategia de prevención que posee el CEMIL recae sobre el capital humano	4%	3	0,12
D4	El sistema de ciber-seguridad del CEMIL funciona en pro de una red externa, lo que resta control de función y supervisión a los funcionarios encargados del concepto de ciber-seguridad	3%	4	0,12
D5	El sistema de ciber-seguridad del CEMIL no está acorde a la necesidad que demandan los contextos. De ahí que la ciber-seguridad no sea una prioridad organizacional	3%	5	0,15
D6	El sistema de ciber-seguridad del CEMIL posee una naturaleza generalizada, es decir, no hay una micro-segmentación de los vectores de función (educación militar)	3%	2	0,06
D7	El sistema de ciber-seguridad no está encaminado al establecimiento de objetivos como: confidencialidad, integridad y seguridad especializada	3%	5	0,15

	seguridad especializada			
D8	No hay un proceso continuo de análisis, monitoreo y predicción de posibles ciberataques al sistema de educación virtual del CEMIL	3%	4	0,12
TOTAL		**25%**	**32**	**1**
Factor Interno **Fortalezas**	**Componente**	**Pond.**	**Nivel de Impacto**	**Calificación Ponderada**
F1	El CEMIL posee un concepto estructural consolidado, es decir, la infraestructura facilita cualquier tipo de cambio en pro de la optimización de los sistemas de ciber-seguridad	8%	5	0,4
F2	El CEMIL posee un número de funcionarios públicos suficiente para conformar campañas de monitoreo y control	4%	3	0,12
F3	El CEMIL posee sistemas de ciber-seguridad que pueden reemplazarse u optimizarse en pro de la disminución de riesgos organizacionales	8%	5	0,4
F4	El CEMIL posee unidades subalternas, especializadas en temas de ciber-seguridad. Esta facultad puede llegar a generar investigación científica que coadyuve al centro de educación militar a mejorar los sistemas y culturas de ciber-seguridad sin exceder costos anuales	5%	5	0,25
	TOTAL	**25%**	**18**	**1,17**
Factor Externo **Oportunidades**	**Componente**	**Ponderación**	**Nivel de Impacto**	**Calificación Ponderada**
O1	Mejorar el sistema de ciber-seguridad mediante la estructuración de un proyecto de inversión organizacional	9%	5	0,45
O2	Optimización del sistema de ciber-seguridad actual, el cual procede de	6%	5	0,3

	tipología organizacional, focalizada en ciber-seguridad "generalizada"			
O3	Mejorar el sistema de ciber-seguridad mediante la proposición de tres objetivos claves: supervisión, concientización y diminución de riesgos	5%	5	0,25
O4	Reconfigurar el sistema de ciber-seguridad del CEMIL, y convertirlo en un modelo organizacional. Esto facilitará la consecución de recursos públicos que sirvan durante la fase de intervención y micro focalización del sistema hacia el concepto de ciber-seguridad para el sistema de educación virtual militar	5%	5	0,25
TOTAL		**25%**	**20**	**1,25**
Factor Externo Amenazas	**Componente**	**Pond.**	**Nivel de Impacto**	**Calificación Ponderada**
A1	Aumento de ciberataques al sistema de educación virtual del CEMIL	5%	5	0,25
A2	Aumento de las vulnerabilidades inter-sistémicas	8%	5	0,4
A3	Aumento de las vulnerabilidades que están relacionadas con el capital humano	5%	5	0,25
A4	Violación masiva de sistemas de información, necesarios para garantizar la educación militar virtual de oficiales y suboficiales	4%	4	0,16
A5	Incremento de riesgos derivados de la sustracción y captación ilegal de datos de interés, correlacionados con el marco de "educación para la defensa"	3%	3	0,09
Total		**25%**	**22**	**1,15**

Tabla 6
Matriz de variables DOFA

MATRIZ DOFA	**INTERNAS**			
	FORTALEZAS		**DEBILIDADES**	
	F1	El CEMIL posee un concepto estructural consolidado, es decir, la infraestructura facilita cualquier tipo de cambio en pro de la optimización de los sistemas de ciber-seguridad El CEMIL posee un número de funcionarios públicos suficiente para conformar campañas de monitoreo y control	**D1**	El CEMIL no posee un sistema de ciber-seguridad especializado en temas de educación militar
			D2	El sistema de ciber-seguridad del CEMIL no posee un componente técnico especializado, orientado hacia el factor de prevención
	F2	El CEMIL posee sistemas de ciber-seguridad que pueden reemplazarse u optimizarse en pro de la disminución de riesgos organizacionales	**D3**	La estrategia de prevención que posee el CEMIL recae sobre el capital humano
			D4	El sistema de ciber-seguridad del CEMIL funciona en pro de una red externa, lo que resta control de función y supervisión a los funcionarios encargados del concepto de ciber-seguridad
	F3	El CEMIL posee un concepto estructural consolidado, es decir, la infraestructura facilita cualquier tipo de cambio en pro de la optimización de los sistemas de ciber-seguridad El CEMIL posee un número de funcionarios públicos suficiente	**D5**	El sistema de ciber-seguridad del CEMIL no está acorde a la necesidad que demandan los contextos. De ahí que la ciber-seguridad no sea una prioridad organizacional
			D6	El sistema de ciber-seguridad del CEMIL posee una naturaleza generalizada, es decir, no hay una

			para conformar campañas de monitoreo y control		micro-segmentación de los vectores de función (educación militar)
		F4	El CEMIL posee sistemas de ciber-seguridad que pueden reemplazarse u optimizarse en pro de la disminución de riesgos organizacionales	D7	El sistema de ciber-seguridad no está encaminado al establecimiento de objetivos como: confidencialidad, integridad y seguridad especializada
				D8	No hay un proceso continuo de análisis, monitoreo y predicción de posibles ciberataques al sistema de educación virtual del CEMIL
EXTERNAS	**OPORTUNIDADES**		**ESTRATEGIAS FO**		**ESTRATEGIAS DO**
	O1	Mejorar el sistema de ciber-seguridad mediante la estructuración de un proyecto de inversión organizacional	Estructuración de un proyecto de inversión organizacional que pueda mejorar el sistema de ciber-seguridad a través de la micro-focalización de acciones		Diseño de una propuesta de intervención para el capital humano. Esta propuesta debe mejorar el uso de los sistemas ciber por parte de los funcionarios públicos del CEMIL. (Forma de reducción del riesgo)
	O2	Optimización del sistema de ciber-seguridad actual, el cual procede de una arquitectura general, de tipología organizacional, focalizada en ciber-seguridad "generalizada"			Proponer el diseño de un sistema de ciber-seguridad del que se desprendan factores tecnológicos coligados a la protección del subsistema de seguridad para la educación militar
	O3	Mejorar el sistema de ciber-seguridad mediante la proposición de tres objetivos claves: supervisión, concientización y diminución de riesgos	Plantear una estrategia de intervención en el CEMIL que identifique riesgos, evalúe estrategias e implemente acciones, tecnológicas y socio-humanísticas		Plantear una estrategia de intervención en el CEMIL que identifique riesgos, evalúe estrategias e implemente acciones, tecnológicas y socio-humanísticas

		ciber-seguridad del CEMIL, y convertirlo en un modelo organizacional. Esto facilitará la consecución de recursos públicos que sirvan durante la fase de intervención y micro focalización del sistema hacia el concepto de ciber-seguridad para el sistema de educación virtual militar		sistema de ciber-seguridad del CEMIL, con el fin de identificar fallas, vacíos sistémicos y demás gaps interconectados con el grupo de vulnerabilidades técnicas.
	AMENAZAS		**ESTRATEGIAS FA**	**ESTRATEGIAS DA**
	A1	Aumento de ciberataques al sistema de educación virtual del CEMIL	Identificar fallas en el sistema de ciber-seguridad, a partir de la realización de un estudio técnico y de observación directa. El estudio técnico coadyuvara a la investigación identificar fallas en el sistema. El estudio de observación directa facilitará la identificación de fallas humanas.	Mejorar el sistema de ciber-seguridad a través del despliegue de una campaña pedagógica en temáticas de prevención y anticipación de riegos para el personal de funcionarios del CEMIL
	A2	Aumento de las vulnerabilidades inter-sistémicas	Hallar fallas de gestión que estén asociadas con el sistema de supervisión; esto permitirá conocer cuál es la naturaleza de las falencias que generan estándares de ciber-seguridad poco útiles	
	A3	Aumento de las vulnerabilidades que están relacionadas con el capital humano		
	A4	Violación masiva de sistemas de información,		Mejorar el rendimiento del sistema de ciber-seguridad del CEMIL, mediante la

		necesarios para garantizar la educación militar virtual de oficiales y suboficiales		optimización de variables básicas, coligadas a la supervisión, control y monitoreo
	A5	Incremento de riesgos derivados de la sustracción y captación ilegal de datos de interés, correlacionados con el marco de "educación para la defensa"	Plantear un proyecto organizacional para cambiar el sistema de ciber-seguridad a nivel Centro de Educación y Doctrina	

Fuente: elaboración propia

Tabla 7
Matriz de evaluación de estrategias

Estrategias	Variables combinadas	Total
Estructuración de un proyecto de inversión organizacional que pueda mejorar el sistema de ciber-seguridad a través de la micro-focalización de acciones	(F1+F2+F3+F4) * (O1+O2)	0,8785
Diseño de una propuesta de intervención para el capital humano. Esta propuesta debe mejorar el uso de los sistemas ciber por parte de los funcionarios públicos del CEMIL. (Forma de reducción del riesgo)	(F3+F4) * (A2+A3+A4)	0,5265
Proponer el diseño de un sistema de ciber-seguridad del que se desprendan factores tecnológicos coligados a la protección del subsistema de seguridad para la educación militar	(F3+F4) * (O3+O4)	0,325
Plantear una estrategia de intervención en el CEMIL que identifique riesgos, evalúe estrategias e implemente acciones, tecnológicas y socio-humanísticas	(D1+D2+D5) * (O1+O2)	0,3235
Realizar una evaluación formal del sistema de ciber-seguridad del CEMIL, con el fin de identificar fallas, vacíos sistémicos y demás gaps interconectados con el grupo de vulnerabilidades técnicas.	(D3+D4+D6) * (A1+A2+A3)	0,27
Identificar fallas en el sistema de ciber-seguridad, a partir de la realización de un estudio técnico y de observación directa. El estudio técnico coadyuvara a la investigación identificar fallas en el sistema. El estudio de observación directa facilitará la identificación de fallas humanas.	(F1+F3+F4) * (A1)	0,2625
Mejorar el sistema de ciber-seguridad a través del despliegue de una campaña pedagógica en temáticas de prevención y anticipación de riegos para el personal de funcionarios del CEMIL	(D3+D4+D6) * (O1+O3)	0,21
Mejorar el rendimiento del sistema de ciber-seguridad del CEMIL, mediante la optimización de variables básicas, coligadas a la supervisión, control y monitoreo	(D1+D4+D5+D6) * (A4+A5)	0,1325
Hallar fallas de gestión que estén asociadas con el sistema de supervisión; esto permitirá conocer cuál es la naturaleza de las falencias que generan un estándar de ciber-seguridad poco útiles	(D7) * (O1+O2)	0,1125
Plantear un proyecto organizacional para cambiar el sistema de ciber-seguridad a nivel Centro de Educación y Doctrina	(D8) * (O1+O2)	0,09

El desarrollo de la matriz DOFA sirvió para llevar a cabo un ejercicio de análisis micro-segmentado. Es decir, las variables acá relacionadas fueron ponderadas de acuerdo con su nivel de influencia, interés e importancia para el cumplimiento de los objetivos misionales, organizacionales y estratégicos asignados al CEMIL. Durante el desarrollo de la matriz se identificaron dos debilidades principales. La primera de ellas correspondía a un sistema de ciber-seguridad poco acorde con la necesidad que demandan los contextos. De ahí que la ciber-seguridad no sea una prioridad organizacional. La segunda, el sistema de ciber-seguridad no está encaminado al establecimiento de objetivos como: confidencialidad, integridad y seguridad especializada.

Las debilidades expuestas materializan dos amenazas. Estas amenazas poseen un alto nivel de impacto desfavorable para el cumplimiento de los objetivos organizacionales y educacionales asignados al CEMIL. La amenaza más significativa en este caso compete al aumento de las vulnerabilidades que están relacionadas con el capital humano. El capital humano hace parte del núcleo de amenazas vigentes, debido a la insuficiencia de campañas pedagógicas y de concientización.

Ahora bien, de las oportunidades demarcadas, saldrían a colación el mejoramiento del sistema de ciber-seguridad mediante la estructuración de un proyecto de inversión organizacional, y la optimización del sistema de ciberseguridad mediante la proposición de tres objetivos concretos: supervisión, concientización y disminución de riesgos.

El resultado final del desarrollo de esta matriz corresponde a la proposición de diez estrategias. No obstante, una vez elaborado el ejercicio de ponderación fueron planteadas dos estrategias de implementación y aplicación. Las estrategias por considerar son:

i. Estructuración de un proyecto de inversión organizacional que pueda mejorar el sistema de ciber-seguridad a través de la micro-focalización de acciones.

ii. Diseño de una propuesta de intervención para el capital humano. Esta propuesta debe mejorar el uso de los sistemas ciber por parte de los funcionarios públicos del CEMIL. (Forma de reducción del riesgo).

Las dos estrategias seleccionadas corresponden a una ponderación de 0,01 a 1,0. El gráfico final de la matriz de ponderación y evaluación de estrategias es la siguiente:

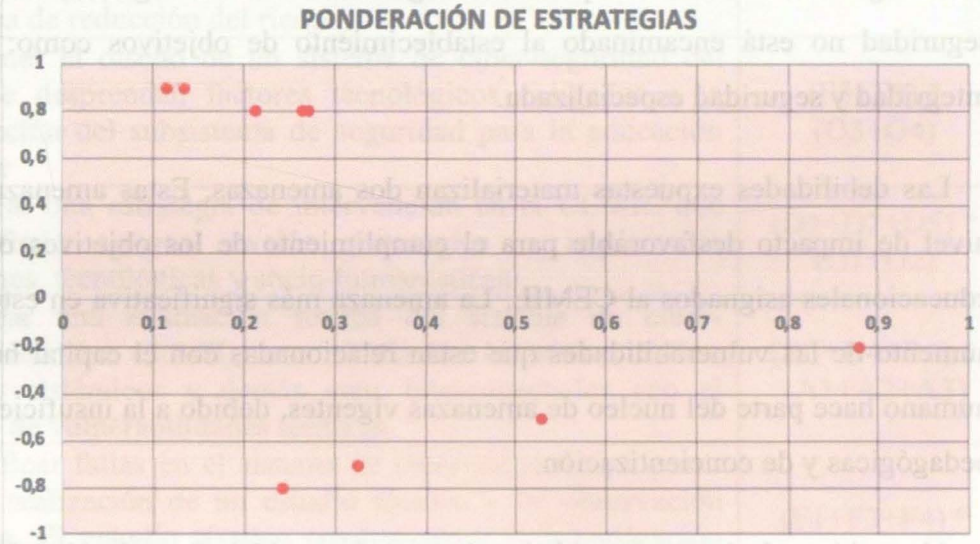

Figura 7 Ponderación de estrategias
Fuente: elaboración propia

La matriz DOFA sirve para para realizar una extracción de variables de ponderación, concernientes a la multiplicación de impactos sobre el objetivo, internos y externos. Para realizar un análisis más profundo del modelo de gestión en ciberseguridad, perteneciente al Centro de Educación Militar, es propuesto el desarrollo de una matriz de análisis de factores de convergencia externos e internos. Esta matriz coadyuvará al investigador a plantear hipótesis que puedan surgir ideas o iniciativas claves durante el proceso de diseño y estructuración de propuestas de solución para la problemática.

Tabla 8
Matriz FE-FI

Descripción del factor	Análisis del factor	Ponderación del impacto sobre el objetivo misional del CEMIL	Ponderación de impacto sobre el propósito estratégico del CEMIL	Ponderación de impacto / capacidad de desarticulación
Factor interno				
Vulnerabilidades provocadas por falta de una cultura organizacional "Cyber"	**Vulnerabilidad interna - alta**	8	9	8,5
Insuficiencia de sistemas internos micro-focalizados al concepto de ciberseguridad para la educación militar	**Vulnerabilidad interna - media**	8	9	8,5
Sistema de ciberseguridad poco asociado a la necesidad contextual que posee el CEMIL	**Vulnerabilidad interna - alta**	7	7	7
Sistema de ciberseguridad generalizado, poco distintivo en cuanto a la prevención de ciber-ataques direccionados al sistema de ciberseguridad	**Vulnerabilidad interna - media**	7	7	7
Sistema de ciberseguridad sin actualizaciones recientes	**Vulnerabilidad interna - media**	6	5	5,5
Vulnerabilidades producidas por la insuficiencia de campañas	**Vulnerabilidad interna - media**	7	5	6

pedagógicas de concientización				
Sistema de ciberseguridad que no está micro segmentado. Esto disminuye la efectividad de acciones coligadas con prevención y anticipación	**Vulnerabilidad interna - media**	7	7	7
Sistema de ciberseguridad que posee gran vulnerabilidad debido a la relación capital humano-usuario-subsistema	**Vulnerabilidad interna - alta**	8	6	7
Factor externo				
No hay estructuración de proyectos de inversión organizacional correlacionados al concepto de "ciberseguridad para la seguridad"	**Vulnerabilidad interna - media**	9	8	8,5
Presencia de ciberataques complejos al sistema de educación virtual	**Vulnerabilidad interna - media**	7	6	6,5
No hay personal especializado suficiente para desarrollar campañas de sistematización y ciberdefensa en temáticas educacionales virtuales	**Vulnerabilidad interna - media**	7	6	6,5

No hay estrategias de intervención, prevención y anticipación de ciberataques al sistema de educación virtual	**Vulnerabilidad interna - media**	6	7	6,5
No hay estrategias inter-sistémicas, direccionadas a la protección de bases de datos, datos de función e información necesaria para la construcción de escenarios educacionales virtuales	**Vulnerabilidad interna - media**	7	8	7,5

Fuente: elaboración propia

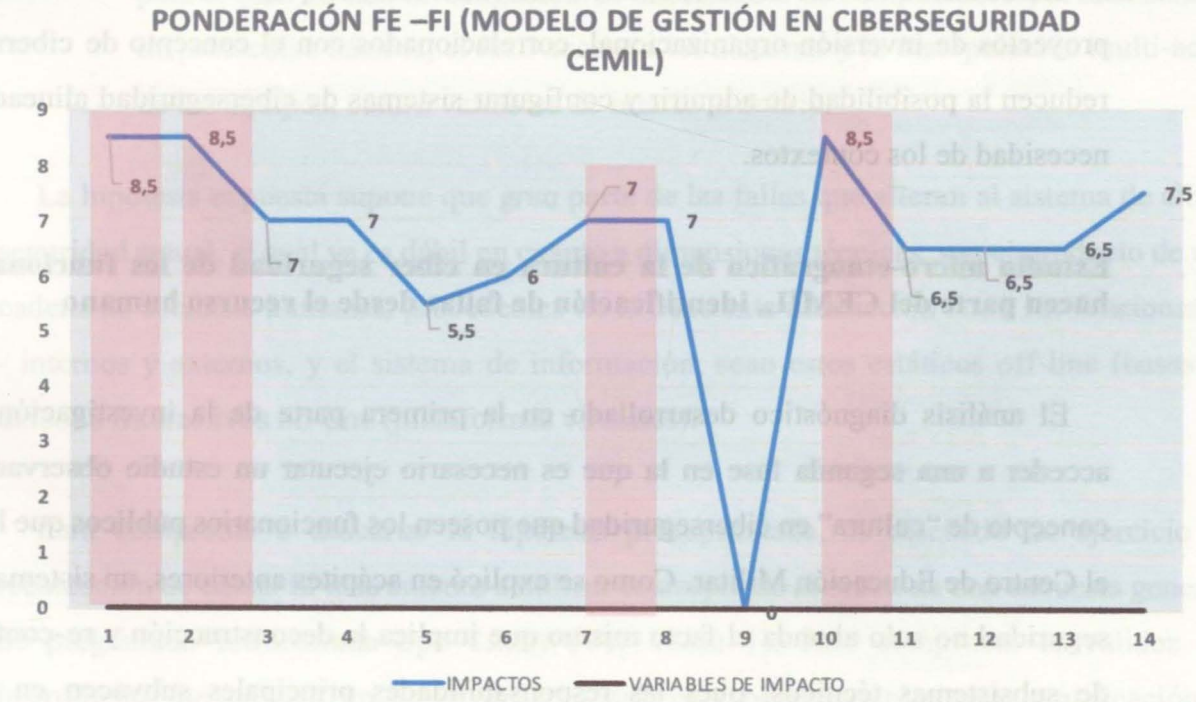

Figura 8 Ponderación FE-FI modelo de gestión en ciberseguridad CEMIL

Fuente: elaboración propia

La matriz FE-FI realiza tres aportes principales a esta investigación. El primero de ellos corresponde a la identificación de un factor interno de ponderación mayor; este factor hace alusión a vulnerabilidades provocadas por la falta de una cultura organizacional "Cyber" que, para el caso, es administrada y empleada por funcionarios públicos que pertenecen al Centro de Educación Militar.

El segundo factor interno corresponde a la existencia de un sistema de ciberseguridad que posee gran vulnerabilidad debido a la relación capital humano-usuario-subsistema. Ambos factores convergen en el mismo punto: capital humano. A ello, que la construcción de estrategias vaya de la mano de la proposición de campañas pedagógicas que sirvan para generar concientización en los usuarios.

En cuanto a los factores externos, conviene subrayar que la falta de estructuración de proyectos de inversión organizacional, correlacionados con el concepto de ciberseguridad, reducen la posibilidad de adquirir y configurar sistemas de ciberseguridad alineados con la necesidad de los contextos.

Estudio micro-etnográfico de la cultura en ciber seguridad de los funcionarios que hacen parte del CEMIL, identificación de fallas desde el recurso humano

El análisis diagnóstico desarrollado en la primera parte de la investigación, permite acceder a una segunda fase en la que es necesario ejecutar un estudio observacional del concepto de "cultura" en ciberseguridad que poseen los funcionarios públicos que laboran en el Centro de Educación Militar. Como se explicó en acápites anteriores, un sistema de ciberseguridad no solo ahonda el facto mismo que implica la deconstrucción y re-configuración de subsistemas técnicos, pues las responsabilidades principales subyacen en el capital humano.

De este modo, resulta conveniente realizar un análisis inter-modal de la cultura en ciber seguridad que poseen los funcionarios que hacen parte del Centro de educación militar. El estudio, de naturaleza cuantitativa, posee dos objetivos y desarrolla en pro de una hipótesis. Los objetivos son:

i. Identificar el nivel de riesgo que genera el uso de sistemas de información, mediante metodología computacional (redes, clústeres, etc.), por parte de los funcionarios públicos del Centro de Educación Militar.

ii. Realizar una disertación micro-sistémica de los riesgos aproximados.

Ahora, la hipótesis de la que parte este estudio es la siguiente:

i. El 80% de los riesgos funcionales asociados al ciber-sistema del Centro de Educación Militar del Ejército Nacional provienen de acciones humanas, siendo para el caso de esta investigación: el intercambio de computadores, la inexistencia de protocolos básicos, el fácil acceso a los sistemas y la manipulación multi-actor de los equipos, cuatro variables de interés primario.

La hipótesis expuesta supone que gran parte de las fallas que alteran al sistema de ciber-seguridad actual, el cual ya es débil en cuanto a dimensiones técnicas, son el producto de una cadena de acciones humanas, procedentes de la constante interacción entre los funcionarios - internos y externos, y el sistema de información, sean estos estáticos off-line (bases de datos) o interactivos on-line (plataformas virtuales).

Para comprobar o descartar la hipótesis presupuestada, es diseñado un ejercicio de recolección de datos. El instrumento a utilizar corresponde al orden de una encuesta general, de preguntada estructurada tipo Likert (Ver Tabla 1). Para comprobar la validez del instrumento fue utilizado un Alpha de Crombach, cuyo objeto era el estudio y ratificación de

fluctuaciones conducentes (patrones de alteridad), producto de la viabilidad objetiva y subjetiva de las preguntas (Ver tabla 2).

El ejercicio de recolección de datos se divide en tres fases. La primera fase, data de la relación, descripción y explicación que caracteriza al elemento muestral. La segunda fase corresponde a la aplicación del instrumento de recolección de datos. El tercero yace en la correlación afirmativa o negativa de la hipótesis a partir de las deducciones observacionales que derivan del proceso de recolección.

Primera fase, caracterización de la muestra

La identificación numérica de la población para la recolección de datos implica el uso de una ecuación muestral. La ecuación y su desarrollo se refleja en la tabla 1.

Tabla 9
Caracterización de la muestra

Ecuación	$n= \frac{k^{2}*p*q*N}{(e^{2}*(N-1))+k^{2}*p*q}$
N (Población total)	149
K (Valor promedial)	2
E (Valor promedial 2)	5
P (Nivel de riesgo)	0.5
Q (Factor)	1
N (Número de muestra obtenida)	133
Tipo de muestra	Probabilística – multivarial

Variable de medición	Escala de elección – tipo Likert
Descripción de la muestra	La muestra debe estar compuesta por: • Oficiales y suboficiales que trabajen en el sector administrativo del CEMIL. • Personal de instructores de planta o por OPS. • Personal de trabajadores de OPS • Soldados regulares o profesionales que tengan contacto con los sistemas o subsistemas online y offline de CEMIL. • Personal ajunto al CEMIL.

Fuente: elaboración propia

El número muestral es de 133 integrantes. Sumado a ello, cabe destacar que la caracterización obedece a la lista de condicionamientos interpuestos en la Tabla 1. En necesario discutir en esta parte que, la muestra, posee una cualificación de naturaleza objetiva. A ello, que la misma se organice de la siguiente forma: clasificación por segmentos y por escolaridad. Los resultados son los siguientes:

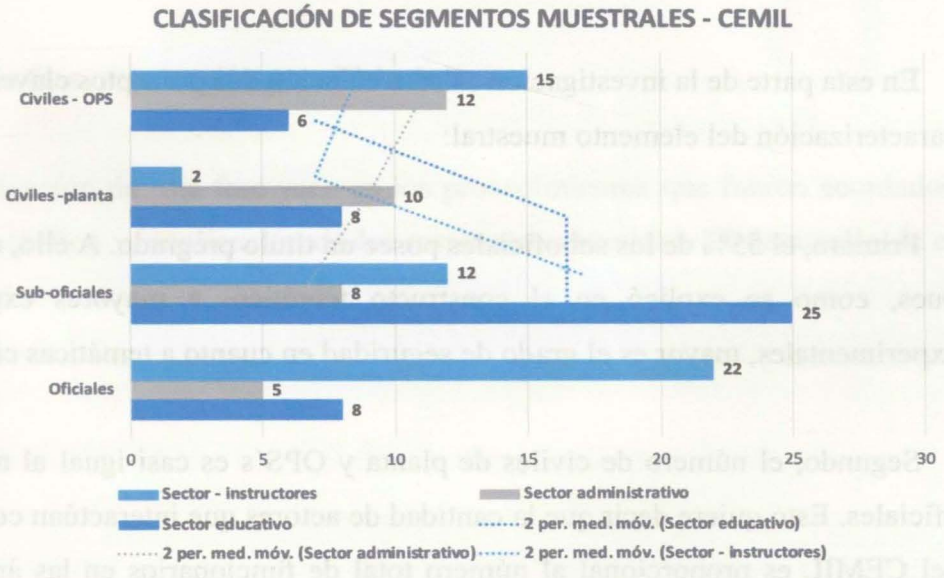

Figura 9 Clasificación de segmentos
Fuente: elaboración propia

La prueba está conformada por cuatro segmentos: oficiales, suboficiales, civiles de planta y OPS´s. El número total muestral es de 133 funcionarios, de los cuales 35 son oficiales, 45 suboficiales, 20 civiles de planta y 33 civiles que trabajan con la institución mediante metodología OPS.

Los cuatro segmentos hacen parte de un clúster objetivo, el cual interactúa de manera directa con el sistema y subsistemas generales del CEMIL, sean estos online u offline.

Cabe destacar que la población muestral también posee una subdivisión en la que hay tres variables de cualificación: bachilleres – técnicos, tecnólogos y profesionales.

La división es importante y ayuda a comprender que la diversificación de actitudes y aptitudes profesionales es finiquitante a la hora de evaluar paradigmas funcionales bases como el comportamiento que los actores demuestran frente al uso de sistemas y subsistemas de tipología online y offline.

En esta parte de la investigación salen a colación dos preceptos claves para el ejercicio de caracterización del elemento muestral:

Primero, el 55% de los suboficiales posee un título pregrado. A ello, que el grado importe pues, como se explicó en el constructo teorético, a mayores experiencias laborales experimentales, mayor es el grado de seguridad en cuanto a temáticas ciber.

Segundo, el número de civiles de planta y OPS´s es casi igual al número total de sub-oficiales. Esto quiere decir que la cantidad de actores que interactúan con los ciber-sistemas del CEMIL es proporcional al número total de funcionarios en las áreas administrativas, educaciones y de instrucción *per se* (Ver figura 10).

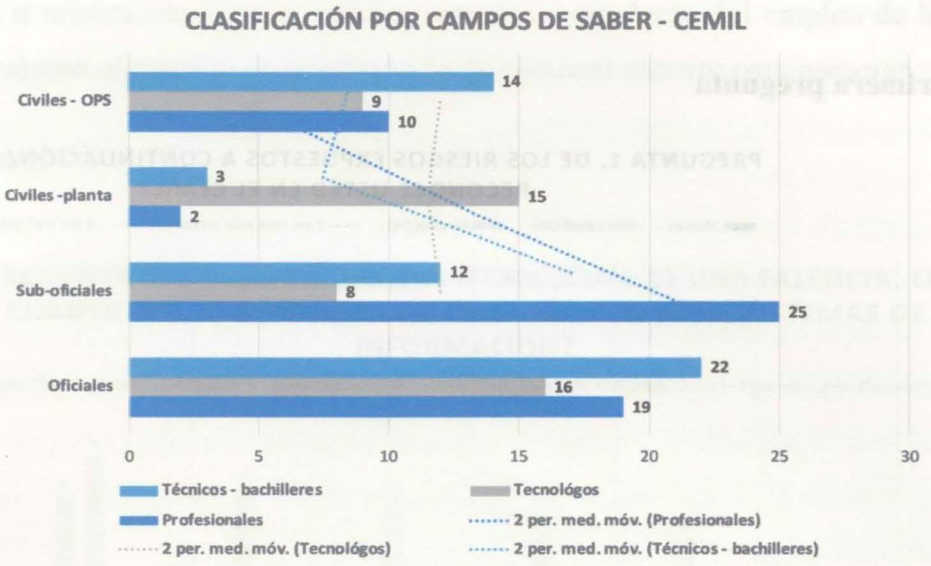

Figura 10 Clasificación por campos del saber
Fuente: elaboración propia

Las dos figuras, 12 y 13, otorgan a esta investigación una delimitación muestral, lo que permite a este ciclo investigativo desarrollar la fase aplicativa del instrumento de recolección de datos.

Segunda fase, recolección y análisis de datos

La explicación de esta fase yace en los procedimientos que fueron acordados. Primero, diseño del gráfico y, explicación de las respuestas obtenidas. El desarrollo de esta fase se ejecuta así:

Primera pregunta

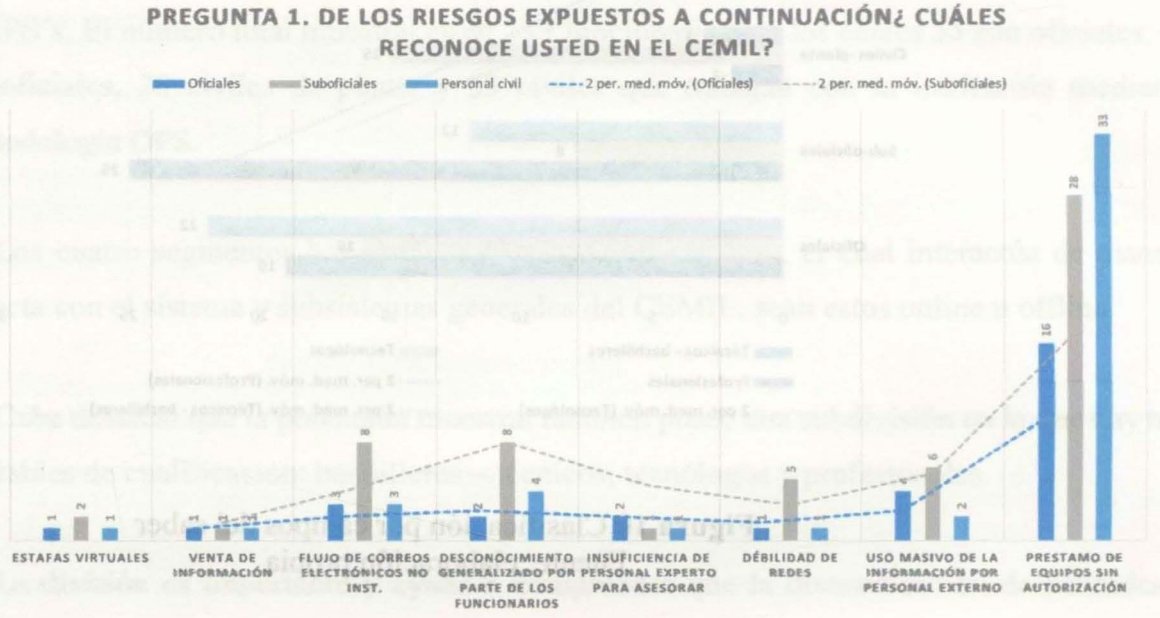

Figura 11 Respuesta pregunta 1
Fuente: elaboración propia

En este interrogante, el 68,2% de los encuestados acordó que el factor de simultaneidad más allegado a la presunción de la variable "riesgos" corresponde a la constante "préstamo de equipos sin autorización". Un 18,3% de los participantes concluyó que el desconocimiento para el uso de los subsistemas corresponde a una variable de categoría "impacto". Es decir, el desconocimiento que el personal posee, asociados con ciber-seguridad, es una de las causales de robo, extracción o secuestro de información, más frecuente.

Otros riegos coligados que fueron identificados en este interrogante subyacen en el flujo de correos electrónicos civiles (no institucionales). El dato demarca a claridad que los subsistemas off-line y online están siendo empleados en actividades ajenas a que se encuentran coligadas con el servicio.

Adicional a ello, es indispensable calcular que hay otros riesgos como la venta de información (denuncias no vigentes), debilidad en redes, uso masivo de la información sin

supervisión u orientación alguna, estafas virtuales – producto del empleo de las redes en actividades ajenas al servicio- e insuficiencia de personal experto para asesorar.

Segunda pregunta

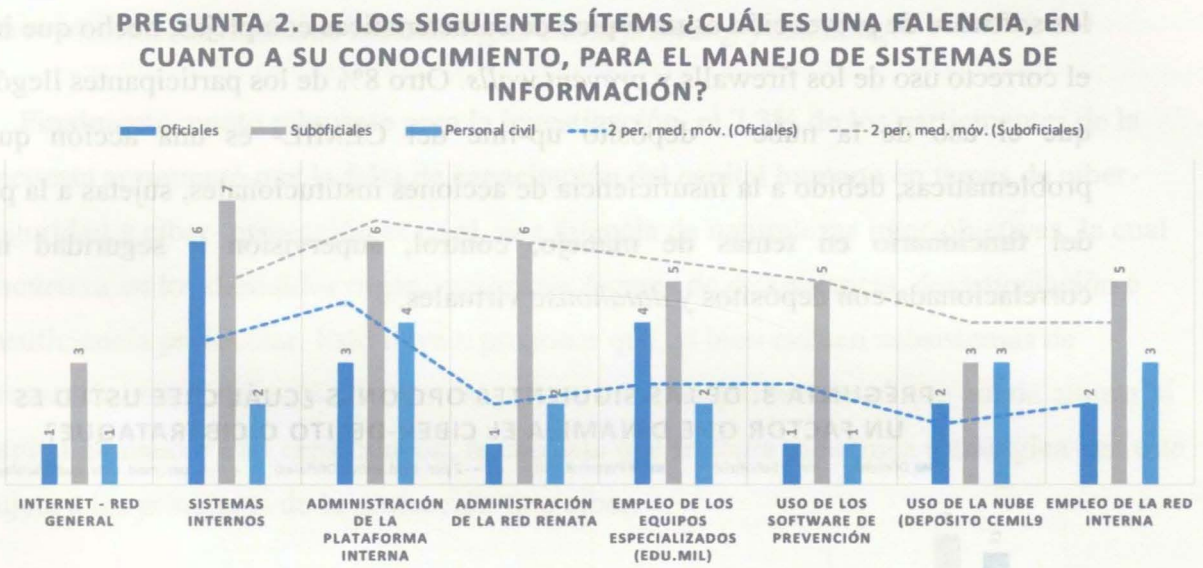

Figura 12 Respuesta pregunta 2
Fuente: elaboración propia

Este interrogante es importante para el desarrollo de la investigación. Con este, el autor busca conocer cuáles son las falencias o vacíos cognoscitivos que poseen los funcionarios que hacen parte del CEMIL. En esta pregunta, el 33,1% de los funcionarios encuestados contestaron que algunos elementos funcionales de tipología interna hacen parte de los subsistemas de información. El desconocimiento acerca de los sistemas de información que yacen en la configuración de acciones matutinas como la transferencia de datos, metadatos o la migración de elementos inter-sistémicos.

Otra respuesta particular, procede de la categoría "Empleo de la Red Interna". El empleo de la red interna, hecho constante, representa para el elemento muestral una perspectiva de animadversión, la cual convierte al manejo diario de las redes de información, en una acción de naturalezas complejas. En tanto, la poca comprensión de las funciones, propiedades y

demás variables, es considerado un hecho que dinamiza el riesgo, siendo el mismo un peligro inminente que se asocia a las rupturas del procedimiento o protocolo de ciber-seguridad.

Seguido a esto, vienen otros ítems. Por ejemplo, para el 16% de los encuestados, el uso de los software de prevención es un tópico de características complejas, hecho que imposibilita el correcto uso de los firewalls y *prevent walls*. Otro 8% de los participantes llegó a concluir que el uso de la nube – depósito up-line del CEMIL- es una acción que produce problemáticas, debido a la insuficiencia de acciones institucionales, sujetas a la preparación del funcionario en temas de manejo, control, supervisión y seguridad informática correlacionada con depósitos y *datahouse* virtuales.

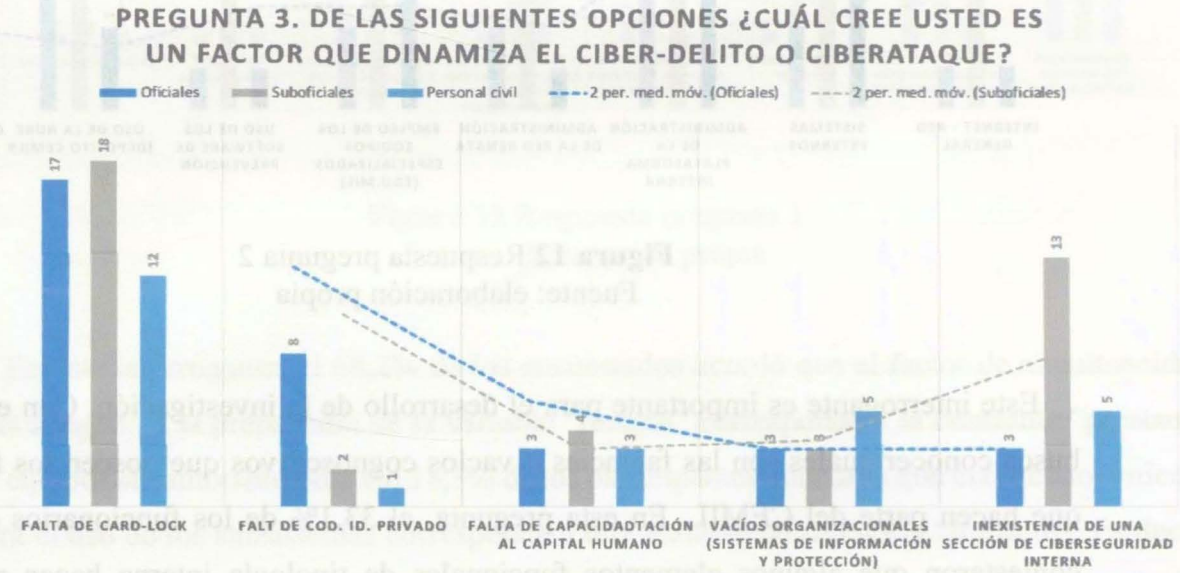

Figura 13 Respuesta pregunta 3
Fuente: elaboración propia

En este interrogante, el 67,2% de los encuestados confirmó que una de las opciones claves para hacerle frente a la problemática del ciber-delito o cualquier otro tipo de ciber ataques que pueda poner en riesgo a los sistemas y subsistemas off y online del CEMIL, corresponde a la variable "adquisición de una Card-Lock".

El Card – lock hace parte del segmento de medidas preventivas. Otro 22% de los encuestados acordó que, al no existir una sección en ciberseguridad interna, habría amplias oportunidades para la ocurrencia de sucesos allegados a la desorientación, descontextualización, insuficiencias cognoscitivas frente al uso de los SII (Sistemas internos de información), robo, secuestros y extracción de información y usurpación de ciber-identidades mediante metodologías como *phishing* y *smishing*.

Finalmente, punto relevante para la investigación, el 7,3% de los participantes de la encuesta argumentó que la falta de capacitación del capital humano en temas de ciber-seguridad y ciber- protección es en sí, una falencia de naturalezas inter-objetivas, la cual encuentra en los descuidos organizacionales fuentes de discordancia, desarticulación e insuficiencia protocolar. Esto lleva a proponer que, si bien existen subsistemas de protección, estos no están acordes, no poseen un concepto funcional que pueda alinear al capital humano y a su capacitación, hecho este que fractura toda línea estratégica que esté sujeta a los principios de la protección tipo ciber.

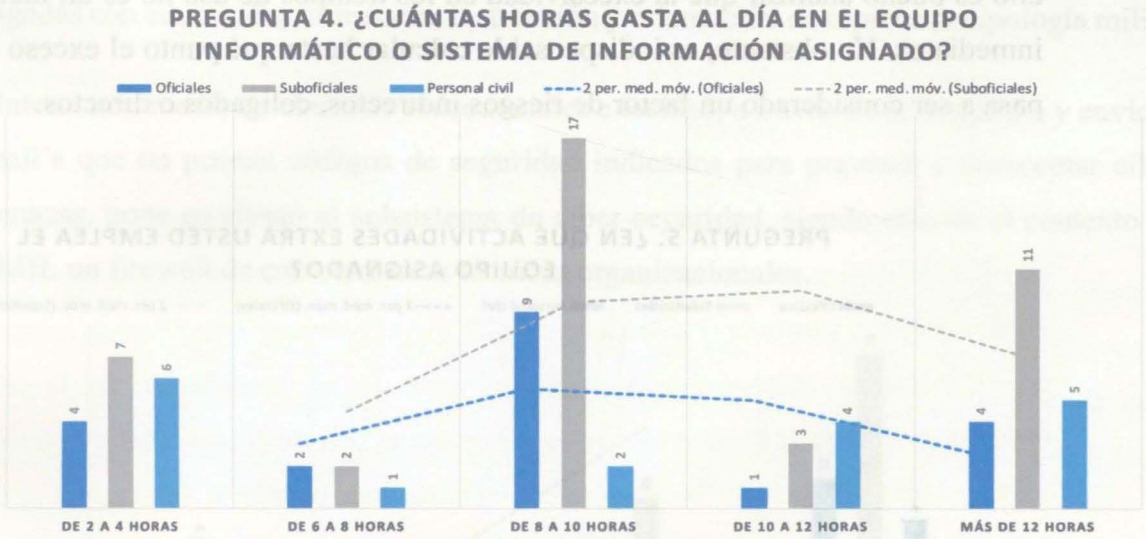

Figura 14 Respuesta pregunta 4
Fuente: elaboración propia

Esta es una de las preguntas que conforma al segmento de "seguridad informática". De acuerdo con el 54,2% de los encuestados, el uso de elementos online y off-line (equipos cómputos, etc.) es de 8 a 10 horas. En esta respuesta, el personal de oficiales y suboficiales

hace parte de la mayoría conceptual, pues es necesario comprender que los funcionarios militares poseen extensas jornadas laborales, en las que sostienen un nivel de interacción constante.

En cuanto al personal civil, resulta lógico analizar que el uso de los elementos va de 2 a 6 horas, pues su horario laboral no sobrepasa un número total de 8. Sin embargo, y en relación con el horario de trabajo, es necesario focalizar en este punto que el riesgo es inminente, toda vez que el personal civil no está capacitado y sus vacíos conceptuales son notables.

No se puede afirmar en este caso que existe una relación u ecuación categorial que disponga que, a mayor tiempo de empleo, mayor representatividad posee el riesgo, pues, como se ha visto, el riesgo no depende de los tiempos de uso, sino de las acciones de desprotección, desarticulación o quebrantamiento de protocolos que fueron sugeridos.

De acuerdo con las respuestas otorgadas, hay un segmento de la población muestral que emplea equipos (off-line y online) en tiempos prolongados, mayores a 12 horas. En cuanto a ello es bueno analizar que la excesividad en los tiempos de uso no es un factor de alcances inmediatos. No obstante, es indispensable calcular hasta qué punto el exceso de los tiempos pasa a ser considerado un factor de riesgos indirectos, coligados o directos.

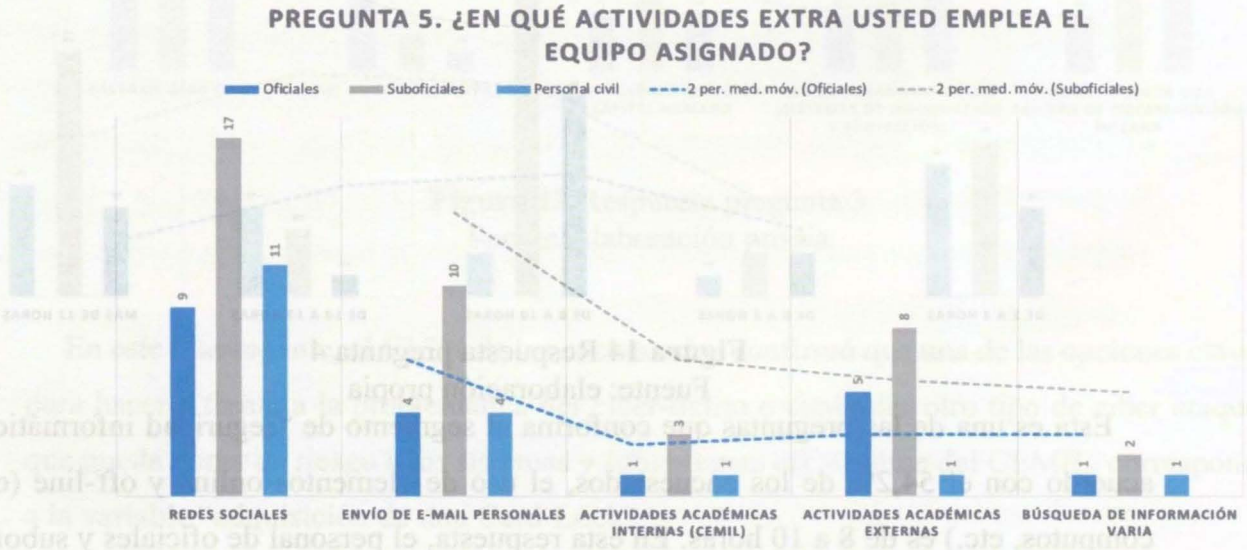

Figura 15 Respuesta pregunta 5
Fuente: elaboración propia

En el interrogante nº 5, orden descriptivo-investigativo, los participantes de la encuesta subrayaron que la opción "redes sociales" posee un alto número de confluencias. El segmento que mayores inclinaciones presenta frente a esta respuesta corresponde al de los sub-oficiales y civiles. Otras actividades como el envío de e-mail personales y actividades académicas externas hacen parte de la lista de factores de disrupción para la ciberseguridad informática del Centro de Educación Militar.

Este interrogante es primordial. Su importancia nace de la identificación de actividades ajenas a la función del uso de los equipos. Obsérvese que el riesgo prominente no proviene de los tiempos de uso, sino de las acciones efectuadas frente al uso off-línea u on-line de los equipos. El análisis de este interrogante nace en la interpretación de las causales de uso, toda vez que el condicionamiento del CEMIL es claro y no permite el acceso a redes o sistema de información cuyas licencias y objetivos sean contrarios a los del precepto natural de acciones coligadas con educación, formación, instrucción y orientación de tópicos de tipología militar.

Interactuar mediante el uso de redes sociales e incluso, a través de la recepción y envío de e-mail´s que no posean códigos de seguridad indicados para prevenir e interceptar ciber-amenazas, pone en riesgo al subsistema de ciber-seguridad, siendo este en el contexto del CEMIL un firewall de características técnicas organizacionales.

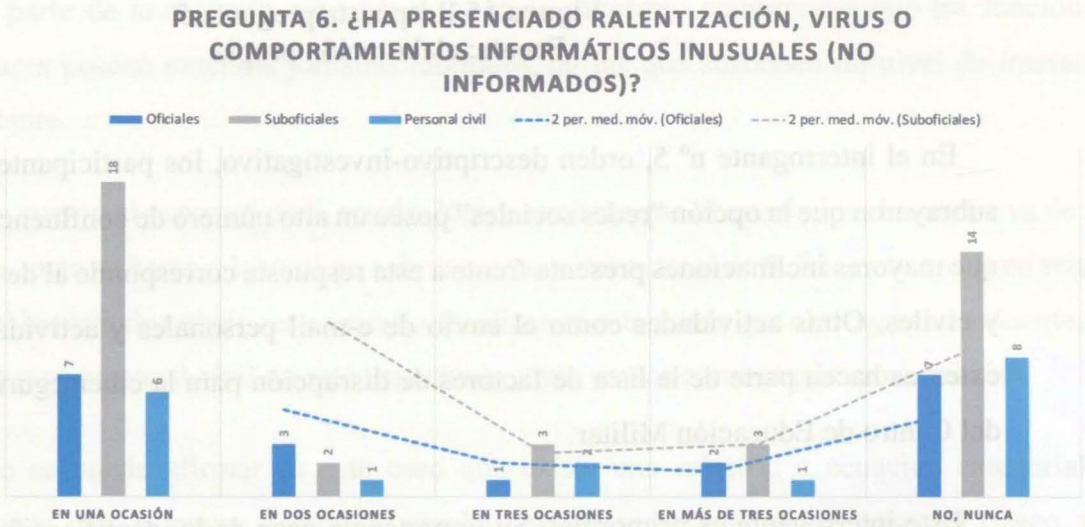

Figura 16 Respuesta pregunta 6
Fuente: elaboración propia

La pregunta nº 6 indica que, en efecto, el 57,2% de los encuestados respondió que en una ocasión detectó patrones y comportamientos cibernético alterativos. Un 33,2% contestó que nunca, y el restante argumentó que en más de dos o tres ocasiones. Esta parte de la encuesta da a conocer que los problemas como infección con virus o sistematización de impactos son hechos normales, de ahí, que las soluciones sean intervenir, reorientar y robustecer protocolos de protección y prevención.

El interrogante es conveniente para denotar que la infección con virus y fenomenologías de animadversión cibernética se ha convertido en hecho común, natural e inherente al empleo de dispositivos externos (Flash Driver o CD´s). Al haber un componente cultural en el que la coexistencia de ciber-acciones y ciber-riesgos no es considerado un factor de alcances contextuales, sino más bien un hecho inherente al uso de equipos off y online, es irracional exponer que el ciber-delito y las ciber-ofensas han pasado a fusionarse con los entornos laborales, contextuales y educacionales.

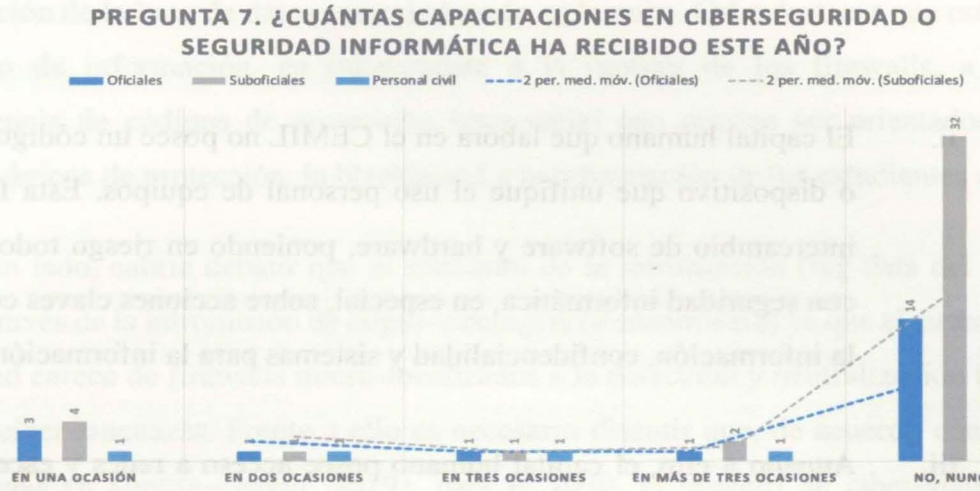

Figura 17 Respuesta pregunta 7
Fuente: elaboración propia

En el interrogante nº 7, el 78,3% del personal que está adscrito al CEMIL manifestó que nunca ha hecho parte de una conferencia, capacitación, curso o seminario en el que se expliquen temáticas directamente asociadas con ciber-seguridad y seguridad digital en el trabajo. El hecho imposibilita el uso y articulación de protocolos y variables que sirvan para prevenir u anticipar cualquier tipología de hecho, acción o alteración inter-sistémica que proceda de ciber-acciones delincuenciales.

Tercera fase, análisis de los datos que fueron recolectados

Los datos recolectados durante el desarrollo del ejercicio anterior sirvieron para reconocer los vacíos co-sustanciales que posee el capital humano que hace parte del Centro de Educación Militar en cuanto a temáticas como ciber-seguridad y seguridad digital en sistemas de información. El ejercicio de recolección de datos coadyuvó a esta parte de la investigación a deducir que:

i. Es indispensable conocer que el capital humano manifiesta "no poseer" conocimiento alguno que esté interconectado con ciber-seguridad y prevención de afectaciones cibernéticas.

ii. El capital humano que labora en el CEMIL no posee un código de identificación o dispositivo que unifique el uso personal de equipos. Esta falencia facilita el intercambio de software y hardware, poniendo en riesgo todo aspecto alineado con seguridad informática, en especial, sobre acciones claves como el manejo de la información, confidencialidad y sistemas para la información clasificados.

iii. Aunado a ello, el capital humano posee acceso a redes y escenarios online, no permitidos por el código de conducta digital que regula al subsistema de prevención y protección del Ejército Nacional. Esta acción aumenta el riesgo, siendo en el contexto una puerta que da entrada a acciones y demás variables consecuentes, productos de la intervención de actores exógenos, delictivos o de naturalezas contrarias al *statu quo* (Objetivo institucional).

iv. El subsistema de protección y prevención de ciber ataques del CEMIL es desconocido para el 80% de los funcionarios que hacen parte de los tres segmentos, administrativos, educacionales o instruccionales *per se*. El desconocimiento subyace en el talante objeto, es decir, principios de protección que se necesitan para anticipar, desarticular y detener toda acción adversa. Esto pone en evidencia que, primero, no hay capacitación para los funcionarios; segundo, no hay elementos de difusión; tercero, el sub-sistema de ciber-seguridad es débil; cuarto existen múltiples falencias, gran parte de ellas coligadas con la parte socio-humanística y organizacional – tecnológica.

v. El ciber-delito y la ciber-acción (infecciones – Phishing -Smishing) se han vuelto elementos de poca alteridad para los contextos organizacionales. El personal del CEMIL se ha adaptado al constante daño que producen los ciberataques. Esto da a entender que el problema no solo es técnico, también es cultural, organizacional y, de cierta forma, inter-seccional.

información de la base de datos central ubicada en la nube. Cabe destacar que está acción, el secuestro de información, es subsecuente a la ruptura de los firewalls, a raíz de la insuficiencia de códigos de protección inter-varial que puedan ser orientados hacia dos factores únicos de protección: la blackboard y la información de los estudiantes militares.

Por un lado, cabría debatir que el secuestro de la información (big data del CEMIL) se daría a través de la intromisión de cripto-virologías (Ransomware) ya que el sistema de ciber-seguridad carece de firewalls micro-focalizados a la detección y neutralización total de este tipo de ciber-amenazas. Frente a ello es necesario discutir que, de acuerdo con las fuentes consultadas en (Impre-system, 2019), para el 2020, el número de ciber-ataques a nivel mundial llegará a incrementarse en un 34,3%.

Hipótesis B

La desinformación y poco conocimiento que poseen los funcionarios del CEMIL se convertirá en el factor organizacional de mayores afectaciones. Es decir, aunque es necesario reconocer que el sistema de ciber-seguridad que posee el CEMIL es débil, no se puede señalar al mismo como a un participe primario de las causas de afectación e impacto, pues el capital humano sí es parte del problema. Subsecuente, la insuficiencia de medidas preventivas e incluso, de estrategias de intervención y capacitación, generan al sistema de ciberseguridad CEMIL, una serie de incongruencias tácitas, producto de la relación causal que yace entre el acceso continuo y el desconocimiento de las medidas de seguridad. Sumado, es indispensable conocer que el capital humano no posee conocimiento técnico frente a factores bases como la suplantación a través de Phising, el robo de información con Ransomware o la observación de paradigmas y patrones mediante la inserción de virologías como *spyware bet*.

Hipótesis C

El CEMIL presenta cuatro problemas frente a temáticas que están ligadas a la ciber-seguridad. La primera problemática, la insuficiencia de sistemas y conceptos técnicos que dinamicen y fortalezcan a los sistemas de ciberseguridad, corrobora, en efecto, que el CEMIL requiere el cambio o transmutación circunstancial de los elementos que conforman al

subsistema de ciberseguridad. El segundo problema está asociado con el capital humano. Este, insiste en demarcar que el personal de funcionarios, responsables principales del proceso, accede al sistema de información sin conocimiento alguno de consecuencias o posibles factos derivados (impactos). El tercero, consecuente con la insuficiencia de propuestas estratégicas de intervención y optimización, lleva a cuestionar la eficacia y eficiencia del sistema como condición *sine qua non* para el funcionamiento de los subsistemas de información y almacenamiento de data (Warehouses del CEMIL). El cuarto y último supone una convergencia de problemáticas alternas, sujetas a una línea intermodal de estudio, ya sean de naturaleza organizacional o técnica.

Segunda parte: desarrollo de los ejercicios de prospectivos

Ahora, con base en las hipótesis, el autor procede a aplicar las herramientas prospectivas mediante el uso de dos métodos, Mic Mac y Delphi. Ambas herramientas buscan conocer:

i. Cuál es la hipótesis probable
ii. Cuál es la hipótesis posible
iii. Cuáles son los escenarios más fluctuantes

Para el desarrollo del primer método, el Delphi, fueron incluidas las observaciones, proposiciones y opiniones de cuatro expertos en las materias de ciber-seguridad y ciber-defensa. Las contribuciones que fueron otorgadas estarán planteadas en cuatro acápites diversos. Cada una ellas se confrontarán con las variables de evaluación, para, posteriormente, analizar una sola perspectiva en general. Los actores involucrados en esta parte de la investigación son los siguientes:

i. **Doctor Edgar Enrique Peña**, consultor particular de la empresa Ciber-Secuirity Colombia SAS. Mencionado es profesional en Ciencias de la Dirección de la Universidad Central de Cataluña. Sus énfasis son: ciber seguridad, redes

Hasta este segmento de la investigación se han realizado dos análisis subsecuentes y consecuentes. En un primer análisis se desarrolló el diagnóstico modal del subsistema técnico que comprende al modelo base de "ciberseguridad para el CEMIL". En el primer análisis se pudo concluir que: i) el sistema de ciber-seguridad que posee el CEMIL es débil, poco objetivo y no posee micro-segmentación de variables de acción alguna; ii) el subsistema de ciber-seguridad del CEMIL no posee una función objetivada hacia la prevención, tampoco enfocada en "ciber-seguridad" para la educación.

Ahora bien, con el fin de marcar un hito investigativo hasta esta parte del proceso en desarrollo, es diseñado el plano de arquitectura organizacional que se refleja a continuación:

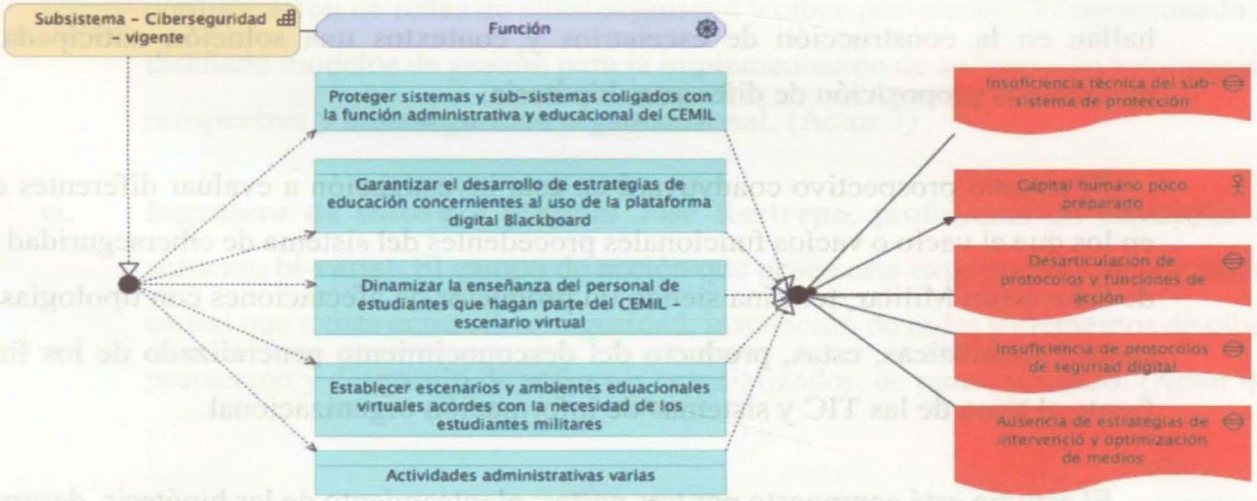

Figura 18 Hallazgos identificados
Fuente: elaboración propia

Análisis en prospectiva, identificación de tendencias asociadas con la generación de modelo de gestión de ciber-seguridad para el Centro de Educación Militar

El trabajo de investigación en curso demanda el uso de métodos prospectivos, el Mi Mac y Delphi. El primero, el Mic Mac, dará a la investigación la opción de divisar estrategias de

gestión, mediante la identificación de vectores de correlación para el contexto, el entorno y el macro-sistema. El segundo, el Delphi, busca plantear una evaluación micro-sistémica de aportes y contribuciones cualitativas, orientadas por un personal de cuatro expertos. Para el desarrollo del Delphi fue utilizada una herramienta de categoría transeccional, la cual busca interconectar los resultados que fueron obtenidos con un margen de riesgo: considerable, alarmante o probable.

Ambos ejercicios buscan dar un respaldo metodológico a la formulación del proyecto organizacional por diseñar. El estudio en prospectiva entregará a esta investigación un carácter objetivo, orientado a la estructuración de variables de tipología múltiple, las cuales hallan en la construcción de escenarios y contextos una solución anticipada, regulada mediante la proposición de diferentes hipótesis.

El estudio prospectivo coadyuvará en esta investigación a evaluar diferentes escenarios, en los que el vacío o vacíos funcionales procedentes del sistema de ciberseguridad del Centro de Educación Militar, termina siendo un productor de afectaciones con tipologías técnicas y socio humanísticas, estas, producto del desconocimiento generalizado de los funcionarios frente al tema de las TIC y sistemas de información organizacional.

El estudio está compuesto por tres partes: planteamiento de las hipótesis, desarrollo de los dos métodos prospectivos y análisis observacional de los resultados obtenidos.

Primera parte: planteamiento de las hipótesis

Las hipótesis del estudio corresponden a las categorías: exploratorias, descriptivas y transeccionales. Las hipótesis a utilizar son las siguientes:

Hipótesis A

En un escenario no mayor a cinco años, el CEMIL afrontará disrupciones técnicas, producto del aumento de incidencias generadas por ciber-delitos básicos como el robo de identidades para el personal de funcionarios, la suplantación, el secuestro y extracción de

informáticas, modificación de sistemas de información y alteración de ciber-sistemas orientados al fortalecimiento de Data Warehouses. (Actor 1)

ii. **Magister Mauricio Gómez Saavedra**, especialista en seguridad informática, co-propietario de la empresa M.L. Design SAS. Mencionado es experto en temáticas que están ligadas al desarrollo de software para fortalecer sistemas de información a nivel inter-organizacional. El profesional posee experiencia en: construcción de redes y configuración de códigos de seguridad informática. (Actor 2)

iii. **Especialista Juan Camilo Yáñez**, consultor de Cyberdata Colombia. El especialista posee conocimientos claves en temáticas que están ligadas con la configuración de redes de ciber-seguridad y ciber-prevención. El mencionado ha diseñado modelos de gestión para la implementación de software de anticipación, prospectiva y ciberseguridad organizacional. (Actor 3)

vi. **Ingeniero de software Manuel José Restrepo**, profesional en desarrollo de software bi-varial. El campo de acción que posee este experto yace en la relación causal que existe entre ciber-seguridad, instalación de redes y elementos de ciber-protección y desarrollo de software especializados, de punto y macro. (Actor 4)

Los cuatro actores hacen parte del panel experto que demanda el empleo del Método Delphi. Ahora, para desarrollar el proceso de análisis y deducción es diseñada una matriz de observación y puntualización de ponderados, regulada por seis categorías. Las categorías son las siguientes:

a. Ponderación del experto frente a las "afectaciones sobre el objetivo del CEMIL"
b. Ponderación del experto frente al nivel de "afectaciones generadas por la debilidad del sub-sistema de ciber-seguridad"
c. Ponderación del experto frente al nivel de "desarticulación de procesos, producto de afecciones generadas pro ciber-ataques de menor, mediano y gran alance – CEMIL"

d. Ponderación del experto frente a la ralentización "de procesos coligados con la educación debido a la inherencia cultural que existe entre ciber-delito e interacción frecuente".

e. Ponderación del experto frente a la concepción de "nuevas ciber-acciones coligadas con la ralentización de subsistemas y secuestro e información situada en la nube (data warehouse- CEMIL".

f. Ponderación del experto frente a "la inserción de virologías desconocidas, superiores en tecnología al código de programación que regula al firewall del CEMIL".

Con las categorías y los actores, se procede al desarrollo del ejercicio Delphi. El resultado es el siguiente:

Tabla 10

Ejercicio de ponderación por parte de expertos

Actores	H1						H2						H3					
	A	B	C	D	E	F	A	B	C	D	E	F	A	B	C	D	E	F
Actor 1	0,7	0,6	0,4	0,8	0,9	0,8	0,5	0,8	0,8	0,7	0,78	0,91	0,6	0,8	0,5	0,7	0,93	0,93
Actor 2	0,8	0,7	0,9	0,9	0,9	0,3	0,6	0,5	0,9	0,6	0,88	0,94	0,3	0,9	0,4	0,6	0,97	0,94
Actor 3	0,8	0,8	0,4	0,8	0,9	0,7	0,7	0,5	0,2	0,5	0,95	0,95	0,7	0,3	0,2	0,78	0,88	0,87
Actor 4	0,9	0,8	0,5	0,9	0,8	0,9	0,4	0,6	0,5	0,8	0,9	0,88	0,6	0,2	0,3	0,73	0,93	0,79
Factor de riesgo alterno	3,2	2,9	2,2	3,4	3,5	2,7	2,2	2,4	2,4	2,6	3,51	3,68	2,2	2,2	1,4	2,81	3,71	3,53
Factor de probabilidad	0,3	0,3	0,2	0,3	0,3	0,2	0,2	0,22	0,2	0,24	0,32	0,33	0,2	0,2	0,13	0,26	0,34	0,32
Factor de posibilidad	1,9	1,7	1,3	2	2,1	1,6	1,3	1,43	1,4	1,55	2,09	2,19	1,31	1,31	0,83	1,67	2,21	2,1

Fuente: elaboración del investigador

En la primera parte del análisis prospectivo fue realizado un estudio de las variables y categorías mediante metodología Delphi. Del estudio es pertinente deducir que los cuatro actores involucrados concluyeron que:

i. El escenario probable corresponde a la categoría E. En este existirán nuevas ciber-acciones coligadas con la ralentización de subsistemas y secuestro de información

situada en la nube (data warehouse- CEMIL). El escenario da a entender que a la par de los avances tecnológicos también están las ciberamenazas, en especial aquellas que hallan en la debilidad de los subsistemas de gestión para la ciberseguridad del CEMIL, un cúmulo de debilidades socio-humanísticas y técnicas.

ii. El escenario de mayores posibilidades correspondió a procesos coligados con la educación, debido a la inherencia cultural que existe entre ciber-delito e interacción frecuente. Esta parte de la investigación es importante para reconocer que los actores del estudio concluyeron que, en efecto, existe una tipología cultural que está sujeta a la costumbre. El componente cultural deduce en tanto, que el personal de funcionarios del CEMIL ve en el ciber-delito o en las ciber-acciones ralentizantes, situaciones de poca alteridad, comunes, diarias y sin sentido alguno. Entonces, obsérvese que, desde la perspectiva de los actores involucrados, hay una visión alterna en la que el concepto cultural, forjado en pro de las insuficiencias educativas en materias de ciber-seguridad, termina siendo un elemento de valor, influencia y modificación de entornos, escenarios y contextos.

iii. Otro de los escenarios en consideración corresponde a la reducción de acciones objetivas que coadyuven a cumplir con la función institucional del Centro de Educación Militar. En cuanto a esto, es necesario conceptualizar que la continua interrupción de actividades, producto del daño de los software y demás sistemas de información sujeta al esquema de función que posee el CEMIL termina generando caos organizacional, y disrupciones administrativas. De ahí que sea necesario el análisis de las falencias socio-humanísticas coligadas al desconocimiento de las medidas de control y protección primarias.

El gráfico fractal del método Delphi es el siguiente:

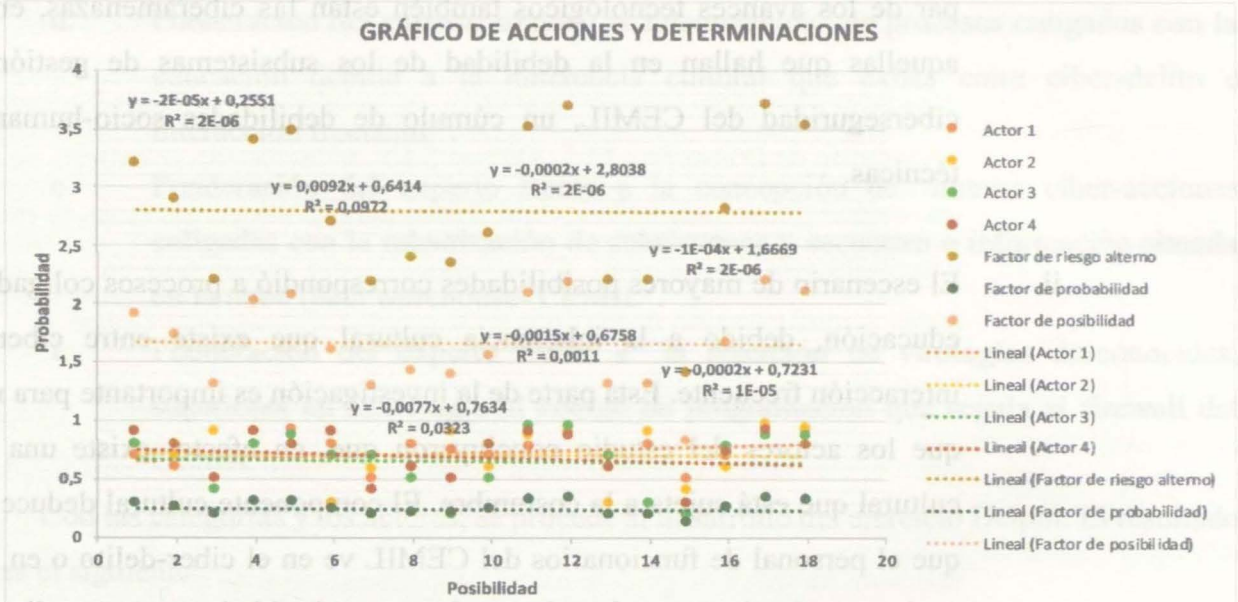

Figura 19 Resultados del Método Delphi
Fuente: elaboración propia

Ahora bien, con base en los insumos generados por la primera parte del estudio prospectivo, se hace necesario la inclusión de un método de construcción de escenarios a partir de las variables interpuestas. En este caso, es indispensable discernir que el método encuentra en las "multi-causas y multi-actores" elementos permitentes, los cuales dinamizan una construcción de posibles perspectivas a partir de rol correlacional de las variables. Las variables a emplear en este caso son las siguientes:

i. Insuficiencia conceptual del capital humano frente a temas asociados con ciberseguridad y SIC (Sistemas de Información).

ii. Debilidad tecnológica de los sistemas asociadas con la no "encriptación" de las informaciones primarias (objetivas de CEMIL)

iii. Insuficiencia de controles de acceso a red (NAC)

iv. Insuficiencia de software adecuados para el fortalecimiento del firewall

v. Insuficiencia de software indicados para la prevención de Phishing y UTM

vi. Insuficiencia de software indicados para la prevención de virologías alineadas con Spyware.

vii. No hay software especializados para la protección del data warehouse del CEMIL

viii. No hay herramientas de monitorización y *reporting*

ix. No hay un código de seguridad que pueda garantizar la protección de la información y gestión operativa que subyace en la blackboard.

x. El concepto de ciberseguridad en el CEMIL es sectorial, no es integral, por ende, hay zonas con poca protección.

xi. No hay análisis BYOD

xii. No hay iniciativas allegadas a las auditorias de código

Las variables deben correlacionarse con el orden indicativo que demandan las categorías:

A. Objetivos educacionales del CEMIL
B. Estructura y subsistema de ciber-seguridad CEMIL
C. Surgimiento de nuevas fenomenologías inter-sistémicas
D. Surgimiento de nuevos factores de afectación
E. Surgimiento de nuevos elementos de animadversión
F. Incremento de las problemáticas debido a la insuficiencia de estrategias
G. Problemáticas ligadas a gobernanza de datos
H. Problemáticas ligadas con "migración de datos"
I. Problemáticas ligadas con "intervención de agentes endógenos"
J. Problemáticas ligadas con "intervención de agentes exógenos"

El procedimiento por desarrollar genera un ejercicio de correlación entre variables y categorías. La fase de transección de datos busca entregar deducciones y conclusiones que permitan conocer, en tres escenarios, cuáles vendrían a ser los impactos derivados de la poca

intervención o desalineación entre el sistema de ciber-seguridad y las fallas asociadas con la insuficiencia de gestiones de tipología socio-humanística (Capital humano). El ejercicio de Mic Mac es el siguiente:

Tabla 11
Ejercicio Mic Mac

Correlación	A	B	C	D	E	F	G	H	I	J
I	0,91	0,68	0,83	0,68	0,92	0,79	0,83	0,79	0,82	0,78
Ii	0,8	0,82	0,83	0,82	0,91	0,77	0,82	0,76	0,85	0,77
Iii	0,92	0,88	0,72	0,93	0,88	0,75	0,84	0,82	0,99	0,68
Iv	0,76	0,92	0,66	0,79	0,82	0,79	0,88	0,81	0,93	0,64
V	0,75	0,83	0,68	0,75	0,59	0,82	0,93	0,83	0,92	0,66
Vi	0,88	0,74	0,65	0,78	0,77	0,81	0,97	0,85	0,91	0,61
Vii	0,83	0,88	0,63	0,76	0,73	0,88	0,92	0,86	0,79	0,83
viii	0,69	0,82	0,69	0,93	0,82	0,83	0,91	0,84	0,83	0,91
ix	0,81	0,88	0,62	0,92	0,84	0,68	0,68	0,82	0,82	0,92
x	0,77	0,95	0,63	0,68	0,88	0,77	0,74	0,81	0,81	0,91
Xi	0,76	0,94	0,88	0,66	0,81	0,91	0,76	0,93	0,86	0,93
Xii	0,72	0,71	0,92	0,92	0,82	0,88	0,77	0,99	0,88	0,94
Probabilidad	10,51	10,96	9,65	10,53	10,7	10,59	10,96	11,02	11,32	10,49
Inferencia	2,6275	27,4	24,125	26,325	26,75	26,475	27,4	27,55	28,3	26,225

Fuente: elaboración del investigador

El desarrollo del método Mic Mac identifica una serie de vectores organizacionales que están sujetos a la construcción de tres escenarios, dos posibles y uno probable. De los escenarios sobresalen diferentes aspectos, todos ellos coligados con múltiples falencias y fallas funcionales del sistema general de ciber-seguridad del Centro de Educación Militar. El resultado del ejercicio de Mic Mac, en pro de los escenarios por plantear, son los siguientes:

Escenario A

En un periodo temporal no mayor a cinco años, el CEMIL tendrá que afrontar problemáticas primarias, derivadas del secuestro y robo de información de la data warehouse. Ello indica que el sub-sistema de ciber-seguridad del CEMIL será débil, poco objetivo, encaminado hacia la concurrencia de falencias tales como: violación de la red mediante

códigos Ransomware, contaminación de los SIC con virologías que están sujetas a DodDs, Phishing y Bet-83. La vulneración de los factores y propuestas de seguridad obligará al CEMIL a reestructurar el sistema general de ciber-seguridad. En este escenario es indispensable desarrollar capacitaciones en temáticas de ciber-seguridad para el capital humano ya que, como se ha discutido a la largo del trabajo de investigación, el precepto de ciber-delito y demás, se ha vuelto en un factor de naturalezas subsecuentes, común y cotidiano.

Escenario B

En un periodo temporal no mayor a cinco años, el CEMIL deberá cambiar en totalidad el sistema de ciber-seguridad. Esto implica un costo de inversión no programado. Por ello, cualquier propuesta estratégica que se diseñe deberá integrar en sus planteamientos dos líneas estratégicas, las técnicas y las socio-humanísticas. De no hacerlo, y con base en las contribuciones del panel de actores, el CEMIL deberá enfrentar dos contingencias. La primera de ellas hace alusión a la ralentización de los sistemas de información, debido al surgimiento de ciber-amenazas que no fueron planteadas en las matrices de prevención y anticipación del riesgo. La segunda, compete a la consolidación de fenómenos de contextos. Esta consolidación refiere a la configuración de patrones de entorno en los que el ciber delito y la violación inter-sistémica de los conceptos nace de las insuficiencias que posee el capital humano del Centro de Educación Militar, ya sea desde las dimensiones conceptuales o desde la inexistencia de un protocolo de prevención.

Escenario C

En un periodo temporal no mayor a cinco años, el CEMIL deberá reestructurar la estrategia utilizada para prevenir y anticipar toda afectación que venga de factores y de actores exógenos. La necesidad llevará al Centro de Educación Militar a realizar una inversión de tipología organizacional. Ello implicará el desarrollo de modelos de gestión en

ciberseguridad que sirvan para proteger ambos aspectos, capital humano y centros de recopilación y almacenamiento de datos históricos. En este escenario, la recomendación vendría a sugerir el cambio del sistema, no obstante, es importante demarcar que todo cambio debe contraer una serie de alteraciones culturales, orientadas hacia la prevención de afectaciones mediante la preparación y educación en temáticas de ciberseguridad para el personal de funcionarios.

Discusión del ejercicio e identificación de problemas actuales

El ejercicio en prospectiva demuestra a claridad que existen diferentes falencias, unas de tipo organizacional (capital humano) y otras de categoría técnica. En la primera parte, el modelo Delphi llevó a determinar que el CEMIL necesita un cambio enfocado en dos problemas, los de la prevención, producto del desconocimiento disciplinar de su personal, y el técnico, resultado de procesos de actualización erróneos.

Con el método Delphi se pudo concluir que el escenario más probable, de no solucionar la problemática, concierne al surgimiento de nuevas ciber-acciones. Ellas, estarán ligadas a una afectación continua de los subsistemas. Las afectaciones para el caso yacen en: el secuestro de la información y el acceso ilegal a la data warehouse del Centro de Educación Militar.

Eso lleva a discutir que el escenario con mayores posibilidades corresponde a la alteridad de procesos coligados con la educación, en especial de los que encuentran relación con interacción e intercambio de conocimientos e información confidencial mediante el uso de la plataforma blackboard.

Uno de los aspectos que mayor interés suscita en el escenario de posibilidades, corresponde al incremento de las afectaciones a raíz de las problemáticas meta-conceptuales del capital humano. De acuerdo con el panel de expertos, el personal de funcionarios "se acostumbró a interactuar con el ciber-delito". Este hecho imposibilita la optimización de los sub-sistemas de ciberseguridad a partir de la tecnificación del mismo únicamente.

La aseveración propuesta se respalda con los resultados obtenidos en la segunda fase del estudio prospectivo. Con el método Mic Mac, el autor de este proyecto de investigación obtuvo suficiente información para identificar tres patrones que enmarcan al precepto natural de la problemática. El primero de ellos corresponde a la constante evolución de los códigos de afectación que superan al firewall que posee el Centro de Educación Militar.

El segundo, como se ha descrito con anterioridad, subyace en relación causal, capital humano y desconocimiento de las normas para proteger y prevenir cualquier tipo de incidente asociado con seguridad informática. El tercero nace de la insuficiencia técnica que posee un sistema de ciberseguridad generalizado, poco enfocado en temáticas de seguridad informática que dinamicen y garanticen el funcionamiento adecuado de los servicios de pedagogía militar.

Ahora bien, una de las ventajas del estudio en prospectiva, cuyo lapso temporal de afectación fue de 60 meses (cinco años), consistió en dar una identificación clara de las problemáticas supuestas. En tanto, el estudio proporcionaría a la investigación una prelación exacta de las problemáticas por solventar. Las problemáticas están descritas en la tabla que se relaciona a continuación:

Tabla 12
Problemáticas identificadas- estudio en prospectiva

Problemática identificada	Naturaleza del problema	Forma de solución
Inexistencia de un modelo de prevención y supervisión en temáticas de ciberseguridad	Organizacional	Estrategia mediante metodología VIRO
Desactualización y poca micro focalización del subsistema de ciber-seguridad para el sistema de información e interacción que posee el CEMIL	Técnico	Proyecto

Insuficiencias meta-conceptuales del capital humano en relación con tópicos que sugieran prevenir y proteger la información mediante acciones cotidianas (ciber-seguridad en el trabajo)	Organizacional	Estrategia de preparación
Inexistencia de un software que pueda proteger a la data warehouse que posee el Centro de Educación Militar	Técnico	Proyecto

Fuente: elaboración del investigador

Las cuatro problemáticas que fueron identificadas, junto con los datos recolectados y las falencias ya analizadas en las fases diagnósticas, llevan a este ciclo investigativo a una siguiente fase, la estructuración de soluciones. Para ello, tal y como fue planteado en la matriz DOFA (estrategias 1 y 2), resulta conveniente desarrollar una solución conjunta, ya que existen cuatro problemas claves, dos de naturaleza organizacional y dos de naturaleza técnica.

Por tal razón, el proyecto deberá contar con una solución factible para cada una de las fenomenologías planteadas. La metodología adecuada en cuanto al desarrollo técnico del proyecto es la siguiente, Metodología de Enfoque Marco Lógico.

Estructuración del proyecto mediante Metodología Enfoque Marco Lógico

El ejercicio de estructuración del proyecto para la optimización del Sistema de ciber-seguridad del Centro de Educación Militar deberá orientarse al desarrollo de los siguientes puntos:

i. Árbol de problemas
ii. Árbol de objetivos
iii. Identificación de necesidades

iv. Identificación de los stakeholders
v. Identificación de riesgos
vi. Derivación de costos
vii. Estrategia de aplicación (categoría – capital humano)
viii. Indicadores de gestión (resultados esperados)

Los puntos propuestos facilitarán y agilizarán el proceso de formulación del ciclo de vida del proyecto. Cada uno de los puntos plantea una descripción detallada de sus causas. Al final, el lector encontrará una gráfica sujeta a los principios de la arquitectura empresarial, en la que están descritas cada una de las tareas por ejecutar.

Árbol de problemas

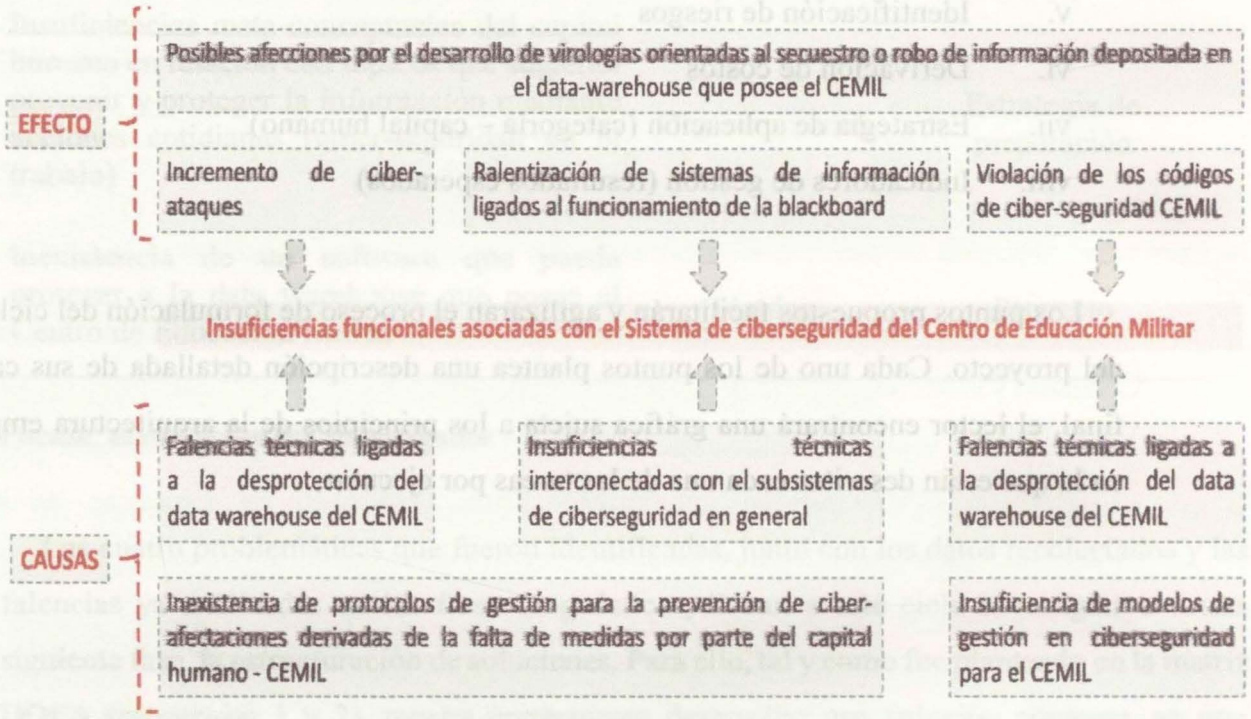

Figura 20 Árbol de problemas
Fuente: elaboración propia

Como problema principal – necesidad causal para la estructuración del proyecto- es expuesta la insuficiencia funcional que está asociada con el sistema de ciber-seguridad del Centro de Educación Militar.

Tres causales dinamizan el problema. Estas son; insuficiencias técnicas interconectadas con el subsistema de ciber-seguridad, inexistencia de protocolos de gestión para la prevención de ciber-afectaciones a la data warehouse que posee el CEMIL y ausencia de medidas y protocolos de prevención puestos en práctica por el capital humano.

Árbol de objetivos

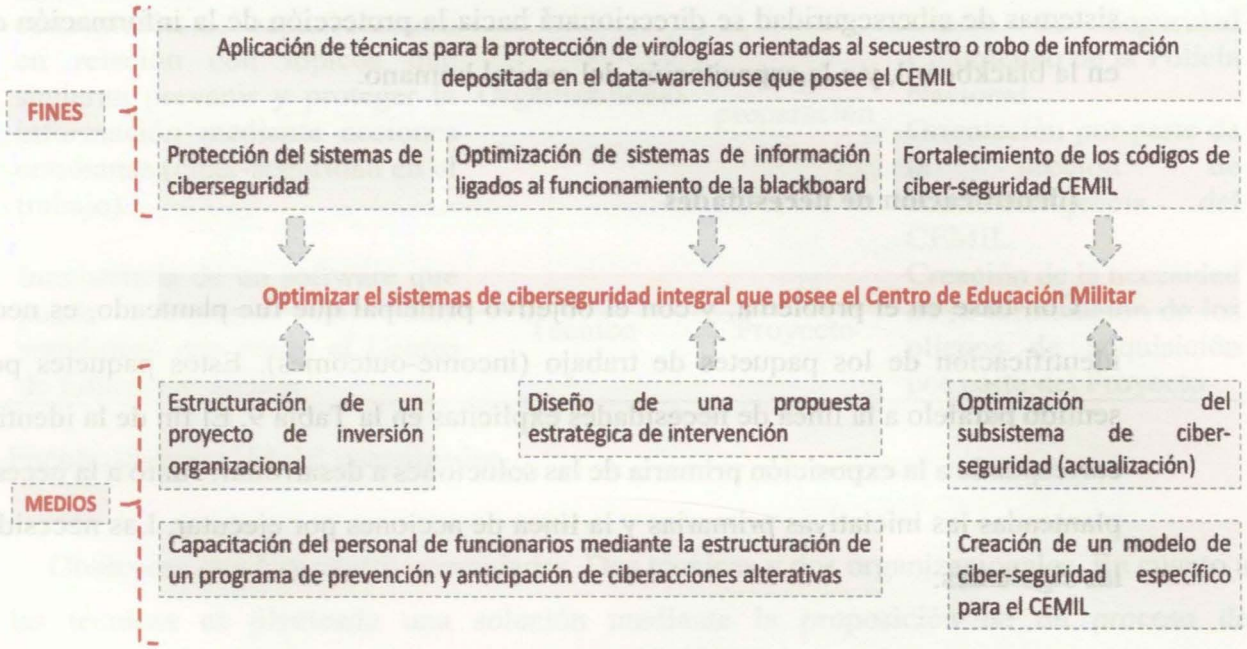

Figura 21 Árbol de objetivos
Fuente: elaboración propia

El objetivo del proyecto en estructuración corresponde a la optimización de los sistemas de ciberseguridad del Centro de Educación Militar. Para su desarrollo son expuestos seis medios principales. Sin embargo, hay cuatro de necesidad primaria: el diseño de una propuesta estratégica de intervención, la optimización del subsistema de ciberseguridad, la capacitación del personal y la creación de un modelo de ciber-seguridad específico. Cabe destacar que este último aspecto es de difícil de consolidar, pues no hay proyectos disponibles para producir el facto de descentralización sistémica (separación del subsistema del CEMIL de los sistemas de ciberseguridad primario).

Los fines planteados corresponden a la aplicación de técnicas para la protección de virologías orientadas al secuestro o robo de información depositada en el data warehouse. Asimismo, el proyecto busca fortalecer los códigos de ciberseguridad del CEMIL mediante un proceso de actualización. Finalmente, es conveniente discutir que la optimización de los

sistemas de ciberseguridad se direccionará hacia la protección de la información que fluye en la blackboard, y a la capacitación del capital humano.

Identificación de necesidades

Con base en el problema, y con el objetivo principal que fue planteado, es necesaria la identificación de los paquetes de trabajo (income-outcomes). Estos paquetes poseen un sentido paralelo a la línea de necesidades explícitas en la Tabla 9. El fin de la identificación, corresponde a la exposición primaria de las soluciones a desarrollar. Junto a la necesidad son planteadas las iniciativas primarias y la línea de acciones por ejecutar. Las necesidades son las siguientes:

Tabla 13
Identificación de necesidades y acciones (paquetes de trabajo)

Problemática identificada	Naturaleza del problema	Forma de solución	Paquete de trabajo
Inexistencia de un modelo de prevención y supervisión en temáticas de ciberseguridad	Organizacional	Estrategia mediante metodología VIRO	Programación de capacitación con el Centro de Seguridad Cibernético de la Policía Nacional Orientación por parte de la sección de contrainteligencia del CEMIL Creación de la sección de seguridad informática en el CEMIL Creación del modelo de prevención y anticipación de riesgos
Desactualización y poca micro focalización del subsistema de ciber-seguridad para el sistema de información e interacción que posee el CEMIL	Técnico	Proyecto	Creación de la necesidad en la formulación de los pliegos de adquisición por parte del Proyecto

Insuficiencias meta-conceptuales del capital humano en relación con tópicos que sugieran prevenir y proteger la información mediante acciones cotidianas (ciber-seguridad en el trabajo)	Organizacional	Estrategia de preparación	Programación de capacitación con el Centro de Seguridad Cibernético de la Policía Nacional Orientación por parte de la sección de contrainteligencia del CEMIL
Inexistencia de un software que pueda proteger la data warehouse que posee el Centro de Educación Militar	Técnico	Proyecto	Creación de la necesidad en la formulación de los pliegos de adquisición por parte del Proyecto

Fuente: elaboración del investigador

Obsérvese que hay cuatro necesidades. Dos técnicas y dos organizacionales. En cuanto a las técnicas es planteada una solución mediante la proposición de un proceso de configuración y actualización. Las otras dos, las organizacionales, se solucionarán mediante la estructuración de programas de capacitación y protocolos de control y supervisión.

Por consiguiente, para solventar las necesidades que fueron inidentificadas es necesario:

i. **Primero,** programación de capacitación con el Centro de Seguridad Cibernético de la Policía Nacional.
ii. **Segundo,** orientación por parte de la sección de contrainteligencia del CEMIL.
iii. **Tercero,** creación de la sección de seguridad informática en el CEMIL
iv. **Cuarto,** creación del modelo de prevención y anticipación de riesgos
v. **Quinto,** creación de la necesidad en la formulación de los pliegos de adquisición por parte del proyecto.

Identificación de los stakeholders

La identificación de los stakeholders (interesados en solucionar la problemática) se realizó mediante el desarrollo de la matriz que se plantea a continuación:

Tabla 14
Identificación de stakeholders

Interesado (stakeholders)	Nivel de influencia		Nivel de capacidad para materializar la acción	
	Estratégica	Económica	Estratégica	Económica
Dirección para la Gestión de Proyectos	4	9	4	10
Dirección del CEMIL	10	4	9	3
Sección de contrainteligencia	10	2	4	9
Administradores del sistema de información	8	2	8	3
Administración de la blackboard	3	2	4	3
Administración del sistema de educación virtual	9	5	7	2

Fuente: elaboración del investigador

La ponderación de los stakeholders da a entender que:

- Primero, para el desarrollo del proyecto es indispensable contar con el apoyo económico de la Dirección para la Gestión de Proyectos. Este actor es un elemento procedimental primario. De él subyacen los respaldos financieros, hecho por el que la necesidad en este documento debe formularse en pro de los lineamientos del Enfoque de Marco Lógico.

- Segundo, la dirección del CEMIL posee un nivel de capacidad para materializar la acción de tipología 10. Esto significa que el Centro de Educación Militar es un ente de control y ejecución, pero no de financiación.

- Tercero, los administradores del sistema de información son actores con influencias y capacidades estratégicas correlacionadas a la formulación de propuestas de intervención. Estos tienen la oportunidad y habilidad de reestructurar el sistema de ciberseguridad a partir de perspectivas pedagógicas – socio-humanísticas.

- Cuarto, el personal que está inmerso en la administración de los sistemas de educación virtual – blackboard- se caracteriza por la posesión de altos niveles sucesivos de control e intervención. Esta capacidad nace de la interacción constante entre estudiantes, requerimientos, sistema tecnológico y administración de la información (confidencial, reservada clasificada).

Identificación de riesgos

La identificación de los problemas principales, objetivos, priorización de necesidades e identificación de stakeholders lleva a desplegar un ejercicio de desagregación, ponderación y reconocimiento de los riesgos que podrían desestabilizar el desarrollo de las cuatro líneas funcionales del proyecto (fines expuestos en el árbol de objetivos). Para la identificación de riesgos es empleada una metodología *Risk Management*. Esta metodología es utilizada en procesos de estructuración tipo PMI. El método busca evaluar la sucesión de riegos a partir de:

i. Probabilidad de ocurrencia
ii. Posibilidad de ocurrencias
iii. Impactos sobre el objetivo del CEMIL
iv. Impactos sobre el esquema funcional de los sistemas de información CEMIL
v. Capital humano
vi. Secuestro de información
vii. Afectaciones directas a la data warehouse
viii. Desfinanciación
ix. Estrategias pedagógicas poco funcionales

x. Insuficiencias de medidas de control para la supervisar procesos de prevención
xi. Poca supervisión en cuanto medidas de protección (socio-humanístico)
xii. Aumento de nuevas virologías, capaces de irrumpir con el firewall del CEMIL
xiii. Ausencia de un ente de control que haga cumplir las políticas de control y prevención por proponer.

Las variables expuestas hacen parte del segmento de riesgos. Ahora, con base en el esquema que propone el ejercicio de Risk Management es ejecutada la ponderación y posterior análisis de los riesgos del proyecto.

Tabla 15
Identificación riesgos para el proyecto

Riesgo identificado	Objetivo del CEMIL	Funciones pedagógicas del CEMIL	Funciones tecnológicas del CEMIL (educación virtual)	Promedio - riesgo fractal	Tipo de riesgo
Probabilidad de ocurrencia	0,91	0,76	0,66	0,77666667	Medio
Posibilidad de ocurrencias	0,73	0,71	0,65	0,69666667	Bajo
Impactos sobre el objetivo del CEMIL	0,92	0,93	0,44	0,76333333	Medio
Impactos sobre el esquema funcional de los sistemas de información CEMIL	0,69	0,82	0,77	0,76	Medio
Capital humano	0,92	0,95	0,91	0,92666667	Alto
Secuestro de información	0,88	0,94	0,98	0,93333333	Alto
Afectaciones directas al data warehouse	0,88	0,82	0,89	0,86333333	Medio
Desfinanciación	0,56	0,54	0,71	0,60333333	Bajo
Estrategias pedagógicas poco funcionales	0,78	0,74	0,77	0,76333333	Medio
Insuficiencias de medidas de control para la supervisar	0,49	0,83	0,76	0,69333333	Bajo

procesos de prevención					
Poca supervisión en cuanto medidas de protección (socio-humanístico)	0,89	0,92	0,91	0,90666667	**Alto**
Aumento de nuevas virologías, capaces de irrumpir con el firewall del CEMIL	0,66	0,72	0,81	0,73	**Medio**
Ausencia de un ente de control que haga cumplir las políticas de control y prevención por proponer.	0,93	0,92	0,98	0,94333333	**Alto**

Fuente: elaboración del investigador

La matriz de riesgos del proyecto en estructuración es clave para llegar a generar tres interpretaciones. Primero, el riesgo más propenso a la obstaculización corresponde a la ausencia de un ente de control que haga cumplir las políticas de prevención y supervisión a proponer en los protocolos de gestión para un modelo de ciber-seguridad en el CEMIL.

Segundo, la insuficiencia de medidas de supervisión para controlar la acción del capital humano es uno de los factores que mayores afectaciones podrían llegar a presentar. Por consiguiente, esta debe ser considerada una tarea crítica al interior del marco objetivo formulado por el proyecto.

Tercero, gran parte de los riesgos, para el caso de este ejercicio, poseen afinidad con el capital humano. Entonces, es indispensable reconocer que la formulación de estrategias de instrucción y pedagogía en temáticas de ciberseguridad para el capital humano es imprescindible.

Cuarto, los riesgos presentados poseen interconexión directa con: elementos de ejecución, elementos de análisis y acciones principales. Ello lleva a reflexionar acerca de las rutas críticas por elaborar a la hora de dar completitud a las tareas principales del proyecto. Frente

a esto, es necesario denotar que las acciones principales del proyecto están clasificadas en dos: técnicas y organizacionales.

La identificación de los riesgos permite dar celeridad a la siguiente fase, la explicación detallada de actividades necesarias mediante la proposición de la estructura de marco lógico. El marco lógico en este caso entrará a discriminar cada una de las actividades necesarias, por fin, meta y objetivo cercano.

Desarrollo de la matriz de Marco Lógico

Hasta esta parte de la investigación se realizó un proceso de formulación en el que fueron identificadas las necesidades principales, siendo dos de tipología técnica y dos de categoría organizacional. Una vez identificadas las necesidades, el ciclo investigativo llevó al desarrollo de un proceso de identificación del problema *ad hoc* y de sus causales. Frente al problema hallado, fue propuesto un objetivo general de proyecto, el cual busca optimizar y actualizar el subsistema de ciberseguridad que posee el Centro de Educación Militar. Identificados el problema y el objetivo de solución, el proceso investigativo procedió a analizar el factor de riesgo. De esa parte, del análisis del riesgo, sobresaldrían tres factores: el concepto técnico, el precepto socio-humanístico y la insuficiencia de protocolos de control, prevención y supervisión.

Las fases que ya fueron ejecutadas llevan a una nueva etapa, la construcción de la matriz de marco lógico. En el marco estarán consignadas las acciones u actividades por desarrollar. De ahí, que sean propuestas las tareas críticas, priorizadas y regulares. De la matriz de marco lógico se extraerán dos factores de interés: las acciones por valorizar (costos) y las acciones por ejecutar sin necesidad de generar costos de inversión inicial o secundaria. La matriz de marco lógico es la siguiente:

Tabla 16
Matriz de Marco Lógico – Proyecto CEMIL

Variables	Objetivo	Metas	Indicadores	Fuentes de verificación	Supuestos
Fin	Creación del protocolo de prevención	Diseñar un protocolo divido en tres secciones: normas aplicativas, regulaciones experimentales y condicionamientos bases	Cumplimiento del protocolo en un 84,2% (nivel de cumplimiento mínimo para prevenir ciber-ataques)	Acta de difusión del protocolo	Cumplimento del protocolo y reducción de ciber-afectaciones en un 80%

		Difundir el protocolo en las diferentes áreas de gestión	Cumplimiento de los protocolos por parte del 93% de los funcionarios (porcentaje mínimo de aceptación para la reducción de impactos)	Aplicación de estrategias para la supervisión y control en cuanto al cumplimiento del protocolo	Cumplimiento medio de los protocolos y reducción del 60% de posibles ciber-afectaciones
		Supervisar el cumplimiento del protocolo planteado			incumplimiento de los protocolos, lo que llevaría a una reconfiguración de los factores de prevención
Propósito	Crear un protocolo de prevención y anticipación de ciber-afectaciones	Prevenir toda afectación derivada del concepto ciber en el Centro de Educación Militar	Difusión y entrega final del protocolo para el personal de funcionarios que laboran en el CEMIL, personal de estudiantes militares y personal conexo	Aplicación de protocolo	Cumplimento del protocolo y reducción de ciber-afectaciones en un 80% (Fin óptimo)
Resultados	Protocolo de prevención y anticipación de ciber-afectación para el Centro de Prevención y Anticipación	Consolidación del protocolo de anticipación y prevención	Completitud 100% del protocolo de anticipación y prevención	Aplicación del protocolo	Cumplimiento del protocolo y reducción de ciber-afectaciones en un 75%
Acciones	Desarrollo del protocolo	Desarrollo del protocolo de prevención y supervisión	Completitud 100% del protocolo de anticipación y prevención	Aplicación del protocolo	Desarrollo del 100% del protocolo
	Difusión del protocolo				Difusión del protocolo en un 80%

	Metodologías de supervisión				Proposición de las metodologías de supervisión
Fin	Actualización del subsistema general de ciber-seguridad que posee el CEMIL	Aplicar un proceso de actualización para el subsistema de general de ciber-seguridad que posee el CEMIL	Actualización del subsistema de ciber-seguridad del CEMIL antes del 2025	Informe de actualización de software y sistemas de optimización - producto del proceso final de contratación en caso de que esa sea la figura de adquisiciones	Cumplimiento del proceso de actualización en un 80% mínimo (porcentaje mínimo de aceptación)
		Inclusión de un sistema BYOP-P defense puntualizado a: blackboard y warehouse CEMIL	Protección del blackboard y warehouse. Esto, con un porcentaje de aceptación del 80%	Informe de actualización de software y sistemas de optimización - producto del proceso final de contratación en caso de que esa sea la figura de adquisiciones	Cumplimiento del proceso de actualización en un 80% mínimo (porcentaje mínimo de aceptación)
		Inclusión de un sistema BYOP-P para la protección de las comunicaciones - cortafuegos - VPN, IPS, UTM, filtro de contenidos, P2P y control de ancho de banda	Protección de los sistemas de información en los que exige un volumen de datos relativamente altos (80% en cumplimiento)	Informe de actualización de software y sistemas de optimización - producto del proceso final de contratación en caso de que esa sea la figura de adquisiciones	Cumplimiento del proceso de actualización en un 80% mínimo (porcentaje mínimo de aceptación)
		Inclusión de un sistema BYOP-P defense puntualizado a: anti-malware, anti-spam y anti-phishing	Adaptación del 100% de los sistemas de protección: antimalware, anti spam y anti-phishing	Informe de actualización de software y sistemas de optimización - producto del proceso final de contratación en caso de que esa sea la figura de adquisiciones	Cumplimiento del proceso de actualización en un 80% mínimo (porcentaje mínimo de aceptación)

		Inclusión de un Managed detection and response (MDR) al subsistema de ciberseguridad CEMIL	Adaptación del MDR al subsistema de seguridad CEMIL	Informe de actualización de software y sistemas de optimización - producto del proceso final de contratación en caso de que esa sea la figura de adquisiciones	Cumplimiento del proceso de actualización en un 80% mínimo (porcentaje mínimo de aceptación)
		Inclusión de elementos técnicos ligados al proceso de prevención y anticipación de ciberamenazas mediante el factor de Telemetría	Adaptación del proceso de análisis y prevención de ciber-ataques mediante el facto contextual que contraen las constantes de Telemetría	Informe de actualización de software y sistemas de optimización - producto del proceso final de contratación en caso de que esa sea la figura de adquisiciones	Cumplimiento del proceso de actualización en un 80% mínimo (porcentaje mínimo de aceptación)
Propósito	Adquirir servicios de actualización correlacionados con el proceso de actualización del subsistema general de ciber-seguridad CEMIL	Adquisición del 85% de los servicios de actualización para el subsistema de ciberseguridad CEMIL	Cumplimiento del 90% de la adecuación del proceso de actualización y optimización del subsistema de ciber-seguridad del CEMIL	Informes de prevención y protección de subsistemas claves como el data-warehouse y la blackboard del CEMIL	Cumplimiento del 90% de la adecuación del proceso de actualización y optimización del subsistema de ciber-seguridad del CEMIL
Resultados	Actualización y optimización del subsistema de ciber-seguridad del Centro de Educación Militar				
Acciones	Las descritas en el segmento de los fines				
Fin	Desarrollar un proceso de gestión del conocimiento para instruir al personal de	Aplicar el proceso de gestión del conocimiento e instrucción disciplinar al personal de funcionarios del CEMIL	Aplicación del protocolo en un 90% nivel mínimo de aceptación)	Informe de gestión semestral - explicación de los resultados derivados del proceso aplicativo	Los propuestos en el plan de contingencia del proyecto

	funcionarios del CEMIL				
Propósito	Instruir al personal de funcionarios en temáticas correlacionadas con ciber-seguridad micro-focalizada	Obtener personal preparado, consiente de los riesgos derivados de un escenario de interacción entre personas y sistemas de información, sin consideración alguna coligada con ciber-seguridad y prevención	Aplicación del protocolo en un 90% nivel mínimo de aceptación)	Informe de gestión semestral - explicación de los resultados derivados del proceso aplicativo	Los propuestos en el plan de contingencia del proyecto
Resultados	Personal del CEMIL alineado a los protocolos de gestión, protección y prevención de ciber-delitos o ciber-amenazas	Personal de funcionarios capacitado, instruido y consiente de los problemas generados por el paradigma ciber	Aplicación del protocolo en un 90% nivel mínimo de aceptación)	Informe de gestión semestral - explicación de los resultados derivados del proceso aplicativo	Los propuestos en el plan de contingencia del proyecto
Acciones	Programación de capacitación con el Centro de Seguridad Cibernético de la Policía Nacional	Identificación de los riesgos derivados de un escenario de interacción entre personas y sistemas de información, sin consideración alguna coligada con ciber-seguridad y prevención	Establecer un convenio interno con el Centro Cibernético de la Policía para desarrollar campañas de capacitación	Informe de gestión semestral - explicación de los resultados derivados del proceso aplicativo	Los propuestos en el plan de contingencia del proyecto
	Orientación por parte de la sección de contrainteligencia del CEMIL	Identificación de los riesgos derivados de un escenario de interacción entre personas y sistemas de información, sin consideración alguna coligada con ciber-seguridad y prevención	Exigir a la sección de contra-inteligencia el desarrollo de un protocolo de atención y prevención de ciber-delitos interconectados con: robo o secuestro de la información	Informe de gestión semestral - explicación de los resultados derivados del proceso aplicativo	Los propuestos en el plan de contingencia del proyecto

	Creación de la sección de seguridad informática en el CEMIL	Identificación de los riesgos derivados de un escenario de interacción entre personas y sistemas de información, sin consideración alguna coligada con ciber-seguridad y prevención	Creación de la sección de seguridad informática del CEMIL	Informe de gestión semestral - explicación de los resultados derivados del proceso aplicativo	Los propuestos en el plan de contingencia del proyecto
	Creación del modelo de prevención y anticipación de riesgos	Identificación de los riesgos derivados de un escenario de interacción entre personas y sistemas de información, sin consideración alguna coligada con ciber-seguridad y prevención	Formulación del modelo de prevención y anticipación (configuración al 100% antes de finalizar este proyecto)	Informe de gestión semestral - explicación de los resultados derivados del proceso aplicativo	Los propuestos en el plan de contingencia del proyecto

Fuente: elaboración del investigador

El marco lógico debe entenderse como la hoja de ruta del proyecto en sus etapas de ejecución. Hay tres fines pertinentes. Uno de esos fines compete a las dos gestiones técnicas, mientras que las otras dos son solucionables a partir de la proposición de un protocolo de prevención y modelo de gestión coligado con la concepción de instrucciones para el personal del CEMIL. Otra de las actividades de solución expuestas corresponde a la creación de una sección de ciberseguridad o seguridad informática en el CEMIL. Para dar al lector un ejemplo gráfico de lo planteado hasta esta parte de la investigación es diseñada la figura que se relaciona a continuación:

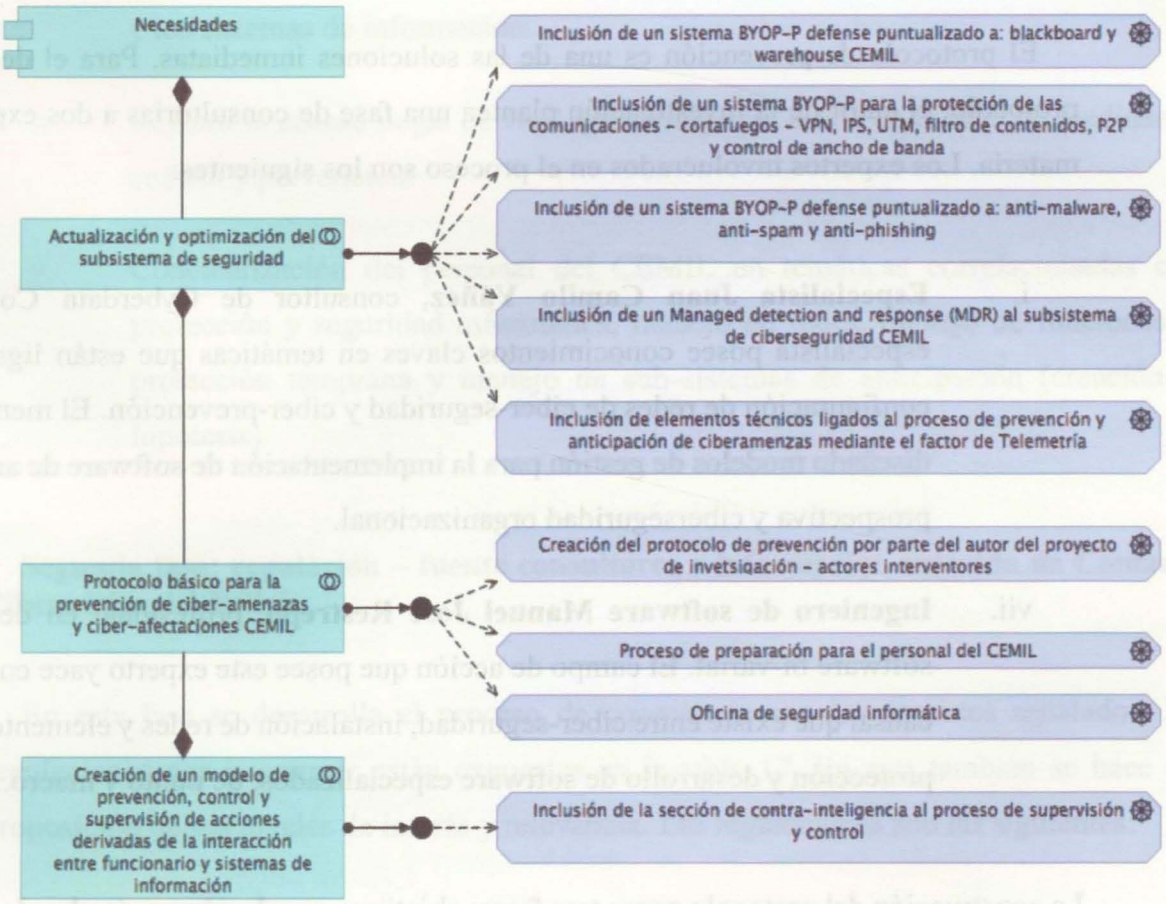

Figura 22 Necesidades – soluciones resumidas
Fuente: elaboración propia

En la figura 22

Hay un resumen de las soluciones. Hay en total, nueve elementos de solución. Cinco de ellos hacen parte del segmento "adquisición" propuesto en la matriz de Marco Lógico. Las otras cuatro son formuladas y diseñadas en los dos acápites que se proporcionan en la siguiente.

Diseño del protocolo de prevención, anticipación y protección del subsistema de ciber-seguridad del Centro de Educación Militar

El protocolo de prevención es una de las soluciones inmediatas. Para el desarrollo del protocolo, el autor de la investigación plantea una fase de consultorías a dos expertos en la materia. Los expertos involucrados en el proceso son los siguientes:

i. **Especialista Juan Camilo Yáñez**, consultor de Cyberdata Colombia. El especialista posee conocimientos claves en temáticas que están ligadas con la configuración de redes de ciber-seguridad y ciber-prevención. El mencionado ha diseñado modelos de gestión para la implementación de software de anticipación, prospectiva y ciberseguridad organizacional.

vii. **Ingeniero de software Manuel José Restrepo**, profesional en desarrollo de software bi-varial. El campo de acción que posee este experto yace en la relación causal que existe entre ciber-seguridad, instalación de redes y elementos de ciber-protección y desarrollo de software especializados, de punto y macro.

La construcción del protocolo posee tres fases: objetivos, regulación y métodos de evaluación y supervisión. En cada una de las fases, subyace un proceso explicativo.

Primera fase: objetivos del protocolo

Estos son los objetivos del protocolo:

i. Desarticular todo elemento de animadversión contextual que pueda generar afinidad cultural entre el ciber-delito, ciber-acciones e interacción constante entre el usuario (personal del CEMIL) y el sub-sistema.

ii. Prevenir ciber-afectaciones generadas por la incursión de ciber-acciones delictivas, producto de una migración constante de datos sin control o supervisión.

iii. Anticipar fenomenologías cibernéticas, producto de la interacción entre el usuario y los sistemas de información.

iv. Reducir el acceso ilegal de virologías complejas a raíz de la falta de medidas de control y prevención.

v. Concientización del personal del CEMIL en temáticas correlacionadas con: protección y seguridad informática, manejo de redes, manejo de funciones de protección temprana y manejo de sub-sistemas de anticipación (creación de hipótesis).

Segunda fase: regulación – fuente consultores e información extraída de Comando Cibernético del Policía

En esta fase se desarrolla el proceso de consultoría con los expertos señalados. Las regulaciones por interponer están expuestas en la tabla 17. En esta también se hace una proposición de sus niveles de interés y relevancia. Las regulaciones son las siguientes:

Tabla 17
Regulaciones

Regulación	Sección	Nivel de importancia
Adaptación de la norma ISO 27032 a los sistemas de gestión y función (áreas de gestión)	Control interno	**Alto**
Prohibición del uso de USB´s, flash drive, discos duros extraíbles o cualquier otro elemento de recolección de datos desde la fuente principal	Sección de contra-inteligencia	**Alto**
Análisis del riesgo enfatizado en vulnerabilidades, activos críticos, códigos de seguridad débil y restauración de sistemas información afectados por virologías externas	Control interno	**Alto**
Regulación para la prohibición de extracción de información confidencial, clasificada o reservada - información que competa a cualquiera de los procesos educacionales involucrados con la plataforma o el data warehouse del Centro de Educación Militar	Sección de contra-inteligencia	**Alto**
Reasignación de los equipos funcionales que posean acceso a la red y designación de responsabilidades y roles de trabajo	Sección cuarta	**Bajo**
Nombramiento de un jefe de área para el cuidado y cumplimiento de las políticas básicas de ciber-seguridad	Sección de contra-inteligencia	**Bajo**
Restricción de acceso a espacios virtuales (website) no autorizados en la lista de herramientas a emplear para la tramitología de los procesos educacionales del CEMIL	Control interno	**Medio**
Autentificación de códigos de seguridad para el acceso diario del personal de funcionarios del Centro de Educación Militar	Sección de contra-inteligencia	**Bajo**
Aplicación mensual de la metodología AA.RR.	Control interno	**Medio**
Evaluación mensual de la metodología AA.RR.	Control interno	**Medio**
Reunión mensual para conocer, de parte de funcionarios, posibles riesgos asociados con ciber-seguridad que no se hallan considerado en las matrices principales de AA.RR.	Control interno	**Medio**

Fuente: elaboración del investigador

El protocolo acá expuesto está conformado por 11 parámetros. Del número de parámetros propuestos hay cuatro que poseen un alto valor. Tres de nivel bajo y cuatro de nivel medio. Una de las particularidades deduciría que todos los parámetros poseen asociatividad con el capital humano, siendo esta una de las vulnerabilidades del subsistema de ciberseguridad vigente.

Otro aspecto llama la atención, la inclusión del marco normativo ISO 27032. La inclusión del marco implicará el desarrollo de políticas de prevención y anticipación para los espectros de seguridad de la información, seguridad de redes, seguridad en internet y seguridad de infraestructura digital crítica.

De la misma manera, al incluir el marco normativo ISO 27032, el CEMIL tendrá que integrar en sus estrategias de ciberseguridad metodologías para la medición del riesgo, en este caso, metodología AA.RR. Su aplicación contrae el uso de procesos de evaluación y supervisión de los dinamizantes que fluctúan o ralentizan toda animadversión sistemática que esté asociado con los factores de riesgo, sean ellos técnicos o socio-humanístico.

Dos medidas alternas nacen del protocolo. La primera corresponde a la prohibición de acceso a zonas o espacios virtuales no autorizados y relacionados con la actividad *per se* de los funcionarios. La segunda, referencia a la prohibición de uso de tipo de dispositivo con los que se pueda extraer o secuestrar información de los SIC que posee el CEMIL.

Finalmente, el protocolo es clave para entender y reconocer la necesidad que subyace en la asignación de un jefe de área que posea como responsabilidad en sus funciones "la supervisión de acciones contrarias que puedan resultar coadyuvando con la ruptura de los códigos de seguridad, la pérdida de información o afectaciones al data warehouse del CEMIL (centro de almacenamiento de datos).

El protocolo planteado, facilita en tanto, proponer un modelo de gestión en ciberseguridad para prevenir y anticipar toda afectación, producto de la alteridad inter-sistémica que se genera por el surgimiento de nuevas ciberamenazas. El protocolo lleva entonces a la siguiente fase de la investigación, el modelo de gestión en ciberseguridad.

Modelo de gestión en ciber-seguridad para prevenir ciber-afectaciones, productos del ataque subsecuente al Centro de Educación Militar

Para el modelo de gestión son utilizadas tres bases claves. Estas bases son:

i. Esquema de ciber-seguridad para organizaciones con altos flujos de información. Este esquema se solicita al Comando Cibernético de la Policía mediante solicitud 014 de 2020, enviada por el autor de esta investigación.

ii. Aplicación de los esquemas funcionales que posee el marco normativo ISO 27032.

iii. Acciones derivadas de los conceptos de ciber-protección y ciber-prevención.

El modelo por plantear cuenta con cuatro objetivos, estos son:

i. Primero, orientar los lineamientos del Centro de Educación Militar en tópicos que están ligados a la interacción usuario (personal del CEMIL) y SIC (Sistema de Información).

ii. Segundo, prevenir toda ciber-afectación, producto de ciber-ataques constantes a los sistemas de información que posee el Centro de Educación Militar.

iii. Tercero, anticipar cualquier hipótesis de ciber-ataque, a través de la detección de debilidades, sean estas de tipología técnica o socio-humanística.

iv. Cuarto, mejorar estándares operativos necesarios para el correcto funcionamiento del subsistema de seguridad y del sistema pedagógico virtual del Centro de Educación Militar.

Ahora bien, el modelo de gestión en ciberseguridad es planteado en pro de cuatro acciones. (Ver figura 23). Cada una de estas acciones posee una línea de procedimientos, metas e indicadores por cumplir.

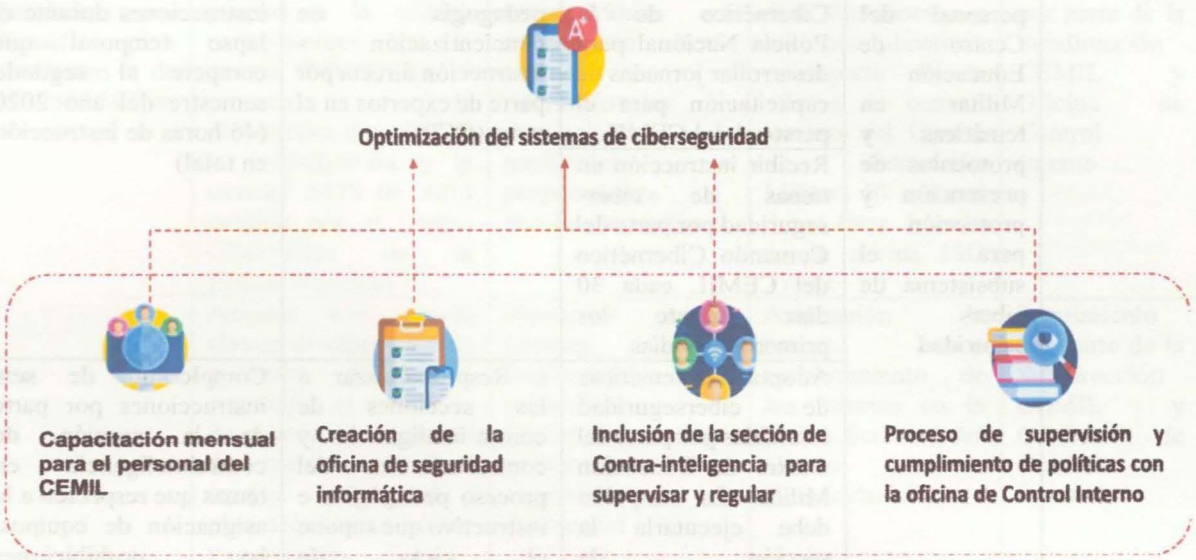

Figura 23 Estructura del modelo basado en ISO 27032
Fuente: elaboración propia

En la figura 23 son expuestas las tareas básicas que componen la estructura de función que debe contener el modelo de ciber-seguridad. Con base en la estructura, la investigación procede a desarrollar el proceso explicativo. Para tal fin son diseñadas cuatro matrices. Cada una de estas presenta el fin, las metas y sus indicadores.

Primer componente: capacitación mensual para el personal del CEMIL

Explicación del componente:

Tabla 18
Primer componente

Objetivo	Acciones	Fines	Indicadores de cumplimiento	Método de supervisión

Instruir al personal del Centro de Educación Militar en temáticas y protocolos de prevención y protección para el subsistema de ciber-seguridad	Solicitud al Centro Cibernético de la Policía Nacional para desarrollar jornadas de capacitación para el personal del CEMIL	i. Instrucción y pedagogía en concientización - instrucción directa por parte de expertos en el tema (CCP)	Completitud de seis instrucciones durante el lapso temporal que compete al segundo semestre del año 2020 (46 horas de instrucción en total)	Seguimiento por parte de la oficina de control interno
	Recibir instrucción en temas de ciber-seguridad por parte del Comando Cibernético del CEMIL cada 30 días durante los primeros 180 días			
	Adoptar las temáticas de ciberseguridad instruidas por parte del Centro de Educación Militar. La adopción debe ejecutarla la sección de contrainteligencia y la sección de control interno	i. Responsabilizar a las secciones de contra-inteligencia y control interno del proceso pedagógico e instructivo que supone el ciclo de concientización del capital humano con lo que respecta a los procesos de ciberseguridad y ciber-prevención	Completitud de seis instrucciones por parte de la sección de contrainteligencia en temas que respecten a la asignación de equipos, las prohibiciones básicas de uso y la prevención que demandan los procesos de acceso abierto a la red (46 horas total)	Seguimiento por parte de la sección de contra-inteligencia
	Evaluar conocimientos y realizar procesos de seguimiento y supervisión	Analizar conocimientos aprendidos y evaluar la capacidad crítica y observacional del personal de funcionarios del CEMIL en cuanto a las temáticas de ciber-seguridad y ciber-prevención	Completitud de evaluaciones semestrales; las evaluación - métodos- deben diseñarse en pro de los conocimientos impartidos y de las técnicas de prevención que hayan sido configuradas	Seguimiento por parte de la oficina de control interno

Fuente: elaboración del investigador

Segundo componente: creación de la oficina de seguridad informática

Explicación del componente:

Tabla 19
Segundo componente

Objetivo	Acciones	Fines	Indicadores de cumplimiento	Método de supervisión

Crear la oficina de seguridad informática para el Centro de Educación Militar	Asignar funciones propias a la oficina concernientes con la norma ISO 27032, el protocolo de prevención descrito en la investigación y la circular 5578 de 2014 emitida por el Centro Cibernético de la Policía Nacional	Establecer la normatividad a aplicar sin alterar normas internacionales regulaciones nacionales o proposiciones funcionales internas	Emisión del manual de funciones y acciones aplicativas por parte de la oficina de control interno del Centro de Educación Militar. El manual debe estar basado en la norma ISO 27032	Seguimiento por parte de la Subdirección CEMIL y Oficina de Control Interno
	Asignar tres cargos claves: el supervisor de procesos de ciber-seguridad, el evaluador de procesos y el gestor de buenas prácticas, medias de control y planes de mejoramiento y corrección	Identificar el personal de funcionarios responsables de procesos de control, prevención, supervisión y evaluación	Asignación de cargos y nombramiento de los mismos en la Orden Semanal del Centro de Educación Militar	Seguimiento por parte de la Subdirección CEMIL y Oficina de Control Interno
	Diseñar los métodos de supervisión, evaluación y rendimiento de cuentas	Diseño de los métodos y medidas de control	Exposición, crítica y configuración de métodos ante el consejo Académico y Directivo del Centro de Educación Militar	Seguimiento por parte de la Subdirección CEMIL y Oficina de Control Interno

Fuente: elaboración del investigador

Tercer componente: integración de la sección de contrainteligencia a la sección de seguridad informática

Explicación del componente:

Tabla 20
Tercer componente

Objetivo	Acciones	Fines	Indicadores de cumplimiento	Método de supervisión
	Definición y asignación de las funciones de prevención, control y monitoreo de los parámetros regulatorios propuestos en el protocolo de función	Involucrar a la sección de contrainteligencia en temáticas que estén ligadas a seguridad informática "física", concerniente con la aplicación de medidas de seguridad internas	Asignación de responsabilidades en la orden semanal del CEMIL	Seguimiento por parte de la oficina de Control Interno y subdirección CEMIL
Definir los procesos de contra-inteligencia que concierne al concepto de ciberseguridad y ciber-prevención en el CEMIL	Diseñar propuestas estratégicas conjuntas entre el personal de la oficina de seguridad informática y la sección de contrainteligencia que sirvan para reducir el número de debilidades, físicas o conceptuales, del personal del CEMIL frente a las variables: ciber-seguridad y ciber-prevención	Desarrollar planteamientos estratégicos que coadyuven al CEMIL a reducir posibilidades y probabilidades de impacto. Para eso es necesario que ambos actores, sección de contrainteligencia y oficina de seguridad informática, se encarguen del despliegue de campañas para materializar protocolos y principios coligados con seguridad interna digital (física o virtual)	Producción de dos propuestas estratégicas conjuntas por mes	Seguimiento por parte de la oficina de Control Interno y subdirección CEMIL

Fuente: elaboración del investigador

Cuarto componente: procesos de supervisión por parte de la oficina de control interno

Explicación del componente:

Tabla 21
Tercer componente

Objetivo	Acciones	Fines	Indicadores de cumplimiento	Método de supervisión

Diseño de las estrategias de seguimiento, control, prevención e intervención en caso de incidentes cibernéticos	Plan de seguimiento, supervisión y concientización del capital humano en tres ejes principales: prevención de acciones, comportamientos irregulares y anticipación al robo o secuestro de información	Reducir posibilidades y probabilidades concernientes a: ciberataques, robo de información, secuestro de datos, suplantación, violación de los códigos de seguridad del data-warehouse del CEMIL	Plan de seguimiento, supervisión y concientización (100%)	Seguimiento por parte de la oficina de control interno, sección de seguridad informática y sección de contra-inteligencia
	Plan de intervención en caso de incidentes informáticos, producto de errores cometidos por el personal de funcionarios		Plan de intervención para atender incidentes cibernéticos	

Fuente: elaboración del investigador

Los cuatro componentes hacen parte del modelo de gestión en ciberseguridad para la prevención de ciberataques. Los ciberataques, según diagnósticos ya ejecutados, son el producto de vacíos conceptuales por parte del personal del CEMIL o de debilidades técnicas procedentes del subsistema de ciber-seguridad vigente.

Los componentes del modelo de gestión están caracterizados por la objetividad de cuatro sub-procesos: supervisión, prevención, anticipación y control de las medidas programadas. Para dar a los lectores una perspectiva gráfica del modelo de gestión y de objetivos bases es diseñada la figura 24.

Figura 24 Objetividad modelo de gestión – ciberseguridad CEMIL
Fuente: elaboración propia

Con la estructuración del protocolo y el diseño de los componentes que hacen parte del modelo, esta investigación pasa a una fase subsecuente: la identificación de costos del segmento técnico de la estrategia de optimización.

Capacitación al personal de estudiantes

La capacitación mensual dirigida al personal de estudiantes busca establecer hábitos en ciber-seguridad para que sean aplicados tanto en su rol de alumnos durante la permanencia en el CEMIL, como en el desempeño de su quehacer profesional, como oficiales, suboficiales o soldados profesionales del Ejército Nacional.

Mediante el conocimiento del esquema de ciber-seguridad para organizaciones con altos flujos de información, el estudiante identificara la importancia de cumplir con los protocolos de ciber-seguridad y políticas emitidas por la oficina de seguridad informática de la institución; entendiendo que no solo es necesario proteger la contraseña principal de usuario, sino también verificar los dispositivos desde donde se accede a las plataformas institucionales, la red que está usando, el licenciamiento que tiene los equipos para conectarse, el lugar físico donde realiza el acceso a las plataformas, entre otras.

Costos del proyecto (sección de adquisición de adquisiciones técnicas)

Los costos del proyecto corresponden, exclusivamente, al segmento de adquisiciones técnicas que comprenden acciones coligadas con el objetivo Nº 3 de la matriz de marco lógico. Para dar completitud al desarrollo de la investigación son calculados los costos asociados con la línea de adquisiciones. Los costos son los siguientes:

Tabla 22
Costos del segmento técnico

Tipo de adquisición	Costo total	Cotización 1	Cotización 2	Cotización 3	Depreciación promedio (15

					años con actualización)
Sistema BYOP-P defense puntualizado a: blackboard y warehouse CEMIL	$ 18.000.000	$17.554.271	$ 23.400.000	$ 21.600.000	-$ 17.910.000
Sistema BYOP-P para la protección de las comunicaciones - cortafuegos - VPN, IPS, UTM, filtro de contenidos, P2P y control de ancho de banda	$ 21.000.000	$19.228.000	$ 27.300.000	$ 25.200.000	-$ 20.895.000
Sistema BYOP-P defense puntualizado a: anti-malware, anti-spam y anti-phishing	$ 17.000.000	$15.780.000	$ 22.100.000	$ 20.400.000	-$ 16.915.000
Sistema Managed detection and response (MDR) al subsistema de ciberseguridad CEMIL	$ 18.000.000	$16.200.000	$ 23.400.000	$ 21.600.000	-$ 17.910.000
Software de medición por Telemetría	$ 26.000.000	$21.890.228	$ 33.800.000	$ 31.200.000	-$ 25.870.000
Total adquisiciones	$100.000.000	$90.652.499	$ 130.000.000	$ 120.000.000	-$ 99.500.000

Fuente: elaboración del investigador

El costo estimado para dar completitud al concepto de "adquisiciones" es de $ 100.000.000 de pesos, subdivididos en cuatro conjuntos: la blackboard y warehouse, la adquisición y actualización de corta fuegos, la adquisición de anti-malware y anti-spam y la adquisición de un Managed Detection.

Conclusiones

El trabajo de investigación finalizó con la estimación, cálculo y derivación de costos bases para el segmento de adquisiciones técnicas. Las adquisiciones técnicas hacen parte de la línea de objetivos concernientes al concepto de optimización y actualización del subsistema de ciber-seguridad del Centro de Educación Militar.

El proceso de formulación de este proyecto apuntó hacia el desarrollo de dos subcategorías, la organizacional (soluciones internas competentes al factor reagrupación) y la técnica (adquisición de software de actualización). Para llegar a esa parte de la investigación fue necesaria la realización de cuatro procesos previos.

El primero de ellos correspondió al diagnóstico generalizado del modelo de ciber-seguridad que posee el Centro de Educación Militar. En esta etapa de la investigación, fueron aplicadas dos herramientas, una matriz DOFA y un ejercicio de análisis de factores de entorno, exógenos y endógenos. Aplicar estas herramientas coadyuvó al ciclo de investigación a determinar que: i) el subsistema de ciber-seguridad del Centro de Educación Militar posee múltiples falencias de tipología inter-sistémicas, siendo en este caso la insuficiencia de elementos técnicos correlacionados con la protección de la blackboard y el data warehouse del CEMIL y los vacíos conceptuales que posee el capital humano del centro, dos dinamizantes del debilitamiento del esquema de ciber-protección, ciberseguridad y ciber-prevención.

El segundo proceso correspondió al análisis micro-etnográfico de los preceptos que hacen parte del marco de cultura organizacional del CEMIL. En esta parte fueron identificados tres patrones de interés. El primero de ellos compete a la relación causal que existe entre las afectaciones desencadenadas por virologías comunes (ciber-delito) y cotidianidad, siendo esta última un factor de acople, costumbre y tolerancias objetivas a elementos alterativos coligados a ciber-afectaciones. El segundo, pertenece a la ausencia de conocimientos que estén asociados con los protocolos de prevención. Tercero, insuficiencia conceptual interconectada con la ejecución de protocolos básicos.

El tercer proceso, estructuración del proyecto, segmentó su desarrollo en siete fases. Primero, árbol de problemas, en el que se identificaron las insuficiencias funcionales del subsistema de ciber-seguridad como situación problémica primaria. Segundo, desarrollo del árbol de objetivos, en el que se planteó un proceso de actualización y optimización del subsistema de ciber-seguridad CEMIL. Aunado a esto, como tercer proceso, fueron identificadas las necesidades por solucionar. De esa parte vendrían a sobresalir la falta de instrucción técnica y procedimental en temáticas de ciber-seguridad para el personal de funcionarios del CEMIL, la inexistencia de un software integral para mejorar la protección de los procesos que contienen gran flujo y volumen de datos, el data warehouse del CEMIL y su blackboard. Como tercera necesidad fueron identificadas las fallas funcionales coligadas con la inexistencia de protocolos de gestión y ciber-prevención y ciberseguridad *ad hoc*.

Seguido a ello, fueron planteados los riesgos. Uno de los riesgos principales, alterativos para el cumplimiento de los protocolos de función y materialización de las actividades pertinentes, correspondió a la ausencia de jornadas de capacitación y preparación que están interconectadas con tópicos direccionados hacia la prevención, intervención y acción temprana. De la matriz de ponderación de riesgos, provendrían dos factores más, la insuficiencia de medidas de control para supervisar procesos de prevención y las fallas relacionales, derivadas de una supervisión minimizada en cuanto a la configuración de medidas de protección (socio-humanístico).

De la evaluación de riesgos vino la estructuración de la matriz de marco lógico, de la que vendrían a resaltarse tres acciones claves: la actualización de subsistema de ciber-seguridad, la preparación del capital humano y el diseño de un protocolo y un modelo de gestión micro focalizado, basado en la norma ISO 27032. El marco lógico facilitó el desarrollo de las soluciones de manera segmentada. Frente a esto, fue necesario principalmente, desarrollar el protocolo y plantear el modelo de gestión. Seguido a esto, fueron calculados los costos bases para la adquisición de los programas de optimización y actualización.

Finalmente, como respuesta a la pregunta de investigación, se confirma que para optimizar el modelo de ciberseguridad organizacional que posee el Centro de Educación Militar, a fin de prevenir traumatismos inter-sistémicos derivados del impacto multidimensional generado por actores endógenos (unidad) y exógenos (ciber-delictivos), es necesario dar ejecución al proyecto formulado, toda vez que el mismo está apuntado a solucionar falencias socio-humanísticas y vacíos inter-sistémicos de tipología técnica.

Referencias

Bert, L. (2016). Characteristics and specified alternatives. En L. Bert, *Cybersecuirity, defense contruction ina complex operational enviroment* (pág. 05). Baltimore: Blue S.

Bolaños, A. (2019). Retos y perspectivas de ciberseguridad en América Latina - focalización en Colombia. *Redes Latan*, 45-69.

Borja, H. (2016). *Ciberseguridad en el siglo XXI, una perspectiva desde las funciones estatales y privadas.* Bogotá: Nievo horizonte.

Cala, I. (2019). Ciber-escenarios, una perspectiva diferente a la aproximación de ciberseguridad y vigilancia tecnológica. *Tecnología y sociedad*, 12-31.

Carreño, L. (2019). El diseño de modelos de ciber-seguridad, viabilidad y estrategia de intervención. *Revista Redes*, 56-68.

Castelbondo, P. (2017). Ciberseguridad, ciberespacio y sistemas de defensa suramericanos ¿complejos de seguridad? *Society and secuirity*, 12-26.

Castillo, P. (2017). Seguridad informática, retos y oportunidades. *Seguridad virtual*, 08-17.

Castillo, P. (2019). Cyber-secuirity, a multi-actor approach. *Technology*, 23-38.

Chesney, R. (2020). Cybersecurity Law, Policy, and Institutions (version 3.0). *Policy and Institutions*, 34-39.

Centro de Educación Militar . (2017). Informe, resultado del proceso para el establecimiento de la situación en Ciberseguridad del CEMIL. Bogotá D.C.: CEMIL - Archivo.

Comando Cibernético de la Policía Nacional. (12 de enero de 2020). *Centro Cibernético Policial*. Obtenido de https://caivirtual.policia.gov.co/#observatorio

De Ocampo, F. (2019). Ciberseguridad en las organizaciones modernas - virtualización de acciones. *Cyber-defense*, 10-13.

Dewell, P. (2015). Game theory applied to ciberscuirity frame. *International Sociology*, 11-43.

DNP. (2011). *CONPES 3701.* Bogotá D.C.: DNP Pub.

Do, C., Tran, N., Hong, C., Kamhoua, C., Kwiat, K., Blasch, E., & Iyengar, S. (2017). Game theory for cyber security and privacy. *ACM Computing Surveys* , 50-55.

Donahue, O. (2017). Ciberdefene, praxis and theory, a paradox? *International secuirity*, 11-19.

Fraile, A. (21 de mayo de 2018). *"La Teoría de Juegos" aplicada a la Ciberseguridad.* Obtenido de AT ITS Secuirity: https://www.linkedin.com/pulse/la-teor%C3%ADa-de-juegos-aplicada-ciberseguridad-alvaro-fraile-hernández/

Goodman, W. (2010). *Cyber deterrence: Tougher in theory than in practice?* Washington D C : Committee on Armed Services.

Henández, P. (2017). Ciberseguridad, análisis compartimentado de los niveles de seguridad informática: retos prospectivos. *Sociedad latinoamericana*, 09-18.

Impre-system. (2019). *Ciber-secuirity, challenges and obstacles derived from IMS systems.* Maryland: New Research Pub.

Klein, I. (2017). Nuevos conflictos, globalización y nueva era. En L. Klein, *Conflictos modernos, escenarios bélicos y nuevos elementos conflictuales* (pág. 10). Delaware: Red. Ed.

Lynn, J. (2016). *Modern geopolitic systems, visions from globalization and world wide new contexts.* Boston: Republic ed.

Ministerio TIC. (27 de junio de 2013). *Decreto 1377 de 2013*. Obtenido de https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

Posada, R. (2017). El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual. *Revista Nuevo Foro Penal* , 72-78.

Prensky, M. (2001). Digital Natives, Digital Immigrants. *MCB University Press*, 27-39.

Ramírez, E. (2020). *Prospectivas en ciber-seguridad, construcción de escenarios y delimitación de hipótesis.* Bogotá D.C.: Info-red.

Ramírez, J. (2017). *Ciberdefensa, un desafío multidimensional para el Estado.* Bogotá D.C.: Mey. Pub.

Roy, S., Ellis, C., Shiva, S., Dasgupta, D., Shandilya, V., & Wu, Q. (2010). A survey of game theory as applied to network security. *2010 43rd Hawaii International Conference on System Sciences* (pág. 10). Honolulu: IEEE.

Salazar, O. (2017). Cyberdefense, a new tipology of threats. *Cinerworld*, 06-33.