Título: Análisis de las Capacidades Cibernéticas del Ejército Nacional [1]

Mayor Willian Lobaton Ochoa[2]

Tutor: Lucas Adolfo Giraldo Ríos[3]

Escuela Superior de Guerra General "Rafael Reyes Prieto"

1. Resumen

Para aminorar los riesgos en el campo cibernético, se demanda una estrategia exhaustiva para neutralizar, si es necesario, la resistencia a los ataques disruptivos y destructivos. Por ello, este estudio tiene como objetivo determinar las capacidades cibernéticas en el Ejército Nacional Colombiano, para esto es necesario realizar un diagnóstico de dichas capacidades bajo el modelo DOMPILEM, que permita proponer recomendaciones para la identificación y fortalecimiento de las capacidades cibernéticas del Ejército Nacional Colombiano. Metodológicamente, se contextualizó en una investigación con un paradigma mixto, con un diseño no experimental, de tipo campo, bajo un nivel transaccional y descriptivo, apoyado en un instrumento tipo cuestionario conformado por contentivo de ítems, señalando alternativas a escala Lickert, aplicada a los expertos en Ciberseguridad del Ejército Nacional de la ciudad de Bogotá.

Palabras claves: Ciberseguridad, Capacidades Cibernéticas, Amenazas, Ataque cibernético.

---

[1] Capítulo de reflexión resultado de investigación del proyecto: a) "Análisis de las Capacidades Cibernéticas del Ejército Nacional" perteneciente al grupo de investigación de Centro de Gravedad categorizado en (A1) por el Ministerio de Ciencia, Tecnología e Innovación de Colombia (MINCIENCIAS). El proyecto se encuentra adscrito y financiado por la Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia.

[2] Mayor del Ejército Nacional de Colombia del Arma de Logística. Especialización en Gerencia Logística de la Escuela de Logística del Ejército, Colombia. Profesional en Ciencias Militares de la Escuela Militar de Cadetes José María Córdova, Colombia. contacto: willian.lobaton@buzonejercito.mil.co

[3] Administrador de Empresas, Especialista en Gestión Financiera Empresarial, Magister en Innovación y Magister en Administración (MBA), actualmente candidato a doctor en Ingeniería de la Universidad Nacional de Colombia. Contacto: lucas.giraldo@esdegue.edu.co

2. Introducción

En el entorno mundial, las naciones, en especial las más desarrolladas, han vislumbrado la amenaza cibernética, llegando a convertirse en una de las más altas prioridades de cada gobierno, ello debido a las particularidades propias del ciberespacio que atenúan aspectos como la ilegalidad, el anonimato, factible acceso, escaso control del gobierno, veloz efusión de información, imperceptible, bajos peligros y elevado efecto por el poder en términos de la función de devastación, inadecuado manejo o toma de control de sistemas tecnológicos y sus secuelas, así como además por la productividad en términos económicos o políticos por individuos, empresas y Estados, estableciendo la amenaza cibernética en una inquietud presente y futura para los Estados, sin embargo, una vez que la dependencia tecnológica es una situación ineludible, con la cual precisamente van a tener que entenderse los habitantes y la sociedad, sobre todo la que se aguanta cada vez más la actividad económica y social de las naciones. (Villanueva, J., 2020).

Si bien a medida que la información comenzó a ser desplazada al entorno digital y las comunicaciones pasaron a ser instantáneas, los retos de los figurantes cibernéticos del Estado, de empresas no gubernamentales y entes e individuos privados fueron más grandes en ventaja de la enorme proporción de material al cual se logra acceder, también es cierto que aumentaron las posibilidades de alcanzar a tener acceso a mucha de esta información considerada de carácter confidencial, de forma lícita o ilícita. Es en este último aporte donde entra en juego la Ciberseguridad, puesto que se encarga de proporcionar, como tu nombre lo indica, cierto nivel de seguridad los activos de carácter informativo que se encuentran alojados en el espacio digital o ciberespacio, ello a través de un tratamiento especial a los datos con el fin de protegerles contra posibles amenazas

que representen un riesgo de ser procesados, manipulados, descargados, almacenados o desviados a otros servidores de interconexión.

En la última década, Colombia ha notificado sus proyectos estratégicos de seguridad cibernética en busca de advertir y mantener el control de probables futuras ofensivas y de aumentar la magnitud informativa y la eficacia en los sistemas de seguridad del espacio cibernético.

La Ciberseguridad, hasta hace una década o dos, era un tema que se concentraba en las altas esferas del ciberespacio, sin embargo en la última década o dos, ha pasado a ser un tema del común, dado que gracias a surgimiento a gran escala de las tecnologías de la información y comunicación, cada día emergen nuevas plataformas digitales para el uso de todo aquel que tenga acceso a un dispositivo con conexión a internet, esto quiere decir que diariamente millones de personas están descargando nuevas aplicaciones móviles, ingresando a portales web, registrando sus datos personales en el espacio digital, lo que ha despertado un puntual interés en saber que tan seguros son estos espacios y que tan resguardada se encuentra su identidad en dichos accesos.

Al respecto, son muchos los panoramas que pueden dar cabida al manejo indiscriminado de la información de carácter *confidencial* que diariamente circula en el ciberespacio, también con muchas las consecuencias negativas que esto conlleva, y es que la globalización de la era digital, ha generado un nuevo mundo de oportunidades a la conductas delictivas y antisociales, donde cada tanto aparecen nuevas formas de atentar contra la privacidad de particulares, empresas y sistemas de información de dominio de los Estados, he allí donde reside la importancia de la Ciberseguridad a nivel político y táctico.

En Colombia frente a la evidente dificultad en el manejo del ciberespacio y asumiendo presente la digitalización y la globalización mundial, donde todos los días el

uso de las tecnologías de la información y las comunicaciones se presenta como un recurso indispensable para las ocupaciones cotidianas, se hace realmente necesario que el Estado trabaje en la creación, configuración y establecimiento de un plan formativo en materia de Ciberseguridad, del cual participe el Ejército Nacional y todos los cuerpos de seguridad en un contexto de constante amenaza cibernética con el objeto de optimizar y mantener constante actualización sus capacidades y conocimientos respecto al tema, ante probables escenarios de riesgo que pretendan afectar la autonomía, libertad, integridad de la nación y mandato constitucional. (Gómez C. y Luciano, M., y Franco, C., 2020).

Lo anterior, se conecta con la idea de que actualmente los cuerpos de seguridad, ya poco se enfrentan al enemigo en territorio físico, sino en el espacio virtual, frente a un enemigo muchas veces anónimo, imperceptible y latente, que atenta contra la misma seguridad nacional, sabiendo que la intrusión física en una institución, no causaría mayor estrago, comparado con la magnitud de una intrusión digital en los bancos de información del Estado, entidades bancarias, instituciones educativas, grandes corporaciones y demás ámbitos, son escenarios posibles en los cuales no podría percibirse el riesgo hasta el intento de ingreso o cuando ya ha sido intervenido el espacio privado.

A modo de contextualizar la problemática y exponer un caso reciente sobre la Ciberseguridad y los cibera taques y como Colombia no escapa de ello, se trae a colación el accidente informático acaecido en 2017, del que serían blanco numerosas compañías y entidades gubernamentales de índole internacional, se catalogó en su momento como un ataque cibernético de gran envergadura, el mismo logró bloquear las operaciones de los ordenadores con la amenaza de habilitarlos únicamente con el pago en las conocidas bitcoin o cryptos (criptomonedas), este virus informático perjudicó

sistemas operativos en Brasil, Francia, Alemania Rusia, España Reino Unido, Estados Unidos, Colombia y otros, por lo que se entiende la creciente preocupación acerca de la importancia de la Ciberseguridad y la relevancia de las capacidades que posean los cuerpos de seguridad en este ámbito, a fin de resguardar a la nación.

¿Es por lo expresado en líneas anteriores, que se considera indispensable considerar cuales son las capacidades reales con las que cuenta el Ejército Nacional colombiano, en tema de Ciberseguridad, efectivamente este brazo armado del Estado posee las herramientas adecuadas para enfrentar o para avistar el riesgo inminente de un ciberataque?

3. Metodología

El diseño de la investigación es mixto, lo que significa elementos tanto cualitativos como cuantitativos, tomando en cuenta que se identificaran las dimensiones de las capacidades de seguridad cibernética del Ejercito Nacional Colombiano. Definido en palabras de Hernández, Fernández y Baptista (2014), es un conjunto de procesos sistemáticos, empíricos y críticos de investigación e implican la recolección y el análisis de datos cuantitativos y cualitativos, así como su integración y discusión conjunta, para realizar inferencias producto de toda la información recabada y lograr un mayor entendimiento del fenómeno bajo estudio y fidedigna para entender, unificar, corregir o aplicar el conocimiento.

De este modo, el tipo de investigación se clasifica como descriptiva de campo aplicado, debido a que se describirá las etapas de madurez de la capacidad cibernética aplicada por el Ejército Nacional Colombiano, buscando especificar las particularidades importantes que inciden en dichos criterios. Las investigaciones descriptivas Bernal

(2010), señala usan criterios sistemáticos que permiten situar de manifiesto la composición o la conducta de los fenómenos de análisis, suministrando de esa misma forma, datos de manera sistemática y comparable con la de otras fuentes. A su vez en este estudio se aplicará un diseño no experimental transeccional, porque su variable en estudio, capacidades cibernéticas, no se manipulará deliberadamente.

Se considera que la población estará integrada por cuatro (4) expertos en Ciberseguridad del Ejército Nacional de la ciudad de Bogotá, por lo cual se establece sus propiedades esenciales, sin controlar el contexto. Los informantes serán escogidos a través de una muestra no probabilístico por conveniencia, de acuerdo con Báez, J. y Pérez, I. (2009), lo que posibilita elegir expertos que accedan ser integrados, esto, basado en la correcta accesibilidad y cercanía de los individuos para el investigador.

Finalmente, las técnicas e instrumentos de recolección de datos será mediante el uso de una encuesta para diagnosticar a la luz del DOMPILEM con la intención de comprobar el nivel de madurez de las capacidades cibernéticas aplicadas por el Ejército Nacional Colombiano, de este modo, Hernández, Fernández y Baptista (2014), consideran el cuestionario, como la herramienta más usada para recoger los datos y se apoya en una batería de preguntas en relación a una o más variables a medir.

4. Diagnóstico de las capacidades cibernéticas del Ejército Nacional Colombiano bajo el modelo DOMPILEM.

En este contexto la Ciberseguridad es considerada una serie de herramientas, políticas, nociones de estabilidad, salvaguardas de estabilidad, directrices, procedimientos de administración de peligros, ocupaciones, formación, prácticas adecuadas, seguros y tecnologías que tienen la posibilidad de manipular para defender

los activos de la organización y los usuarios en el ciberentorno. (Recomendación UIT–T X.1205, 2008).

La ciberseguridad está definida como la capacidad del Estado para reducir el grado de peligro al que permanecen expuestos sus habitantes, frente a las amenazas o incidentes de naturaleza cibernética, como son las transacciones financieras, la defensa de información privada, los derechos primordiales de los individuos por internet, la propiedad intelectual de los documentos por internet, la confidencialidad de los sistemas, las tendencias administrativas por internet, el proceso, almacenamiento y transmisión de datos; cada una de estas responsabilidades más la administración y uso de cualquier otro tipo de datos que necesite ser resguardada se hallan a cargo del Centro Cibernético de la Policía Nacional, estas y las otras ocupaciones de representación preventiva que poseen por objeto, afirmar la utilización de las redes propias y negarlo a terceros. (Peralta, O., 2015).

De esta manera, explica Hudson Analytix (2017), que la seguridad cibernética, es la función de defender o defenderse contra la entrada no autorizada o la utilización del ciberespacio para ataques cibernéticos, se apoya en las medidas colectivas implementadas para proteger de un sistema informático o computarizado contra amenazas cibernéticas, como hackers, servicios de inteligencia extranjeros y sindicatos criminales organizados, entre otros.

Se puede decir que la seguridad del ciberespacio, no solo constituye una necesidad personal o propia de las organizaciones, sino que además es un tema de seguridad y autonomía nacional que interviene en el gobierno nacional, la política nacional e internacional en diversos niveles, la totalidad de la economía y defensa de la información de sus habitantes. El Estado y sus instancias regionales tienen que encarar el desafío de la seguridad y protección del ciberespacio, así como, defender y asegurar

la entrada, uso además de los contenidos a la sociedad civil en el campo virtual, siendo conscientes de su consecuencia local, nacional y universal. (Vargas, R., Recalde, L., y Reyes, R., 2017).

De este modo, las capacidades cibernéticas se desarrollan su arquitectura conceptual bajo el módulo principal codificado en lenguaje C, un módulo de propulsión codificado en lenguaje Python, otro módulo de guiado en lenguaje PERL y una carga explosiva útil codificado bajo el lenguaje C++. (Trama, G., y Vergara, E., 2017). Bajo este escenario existen capacidades cibernéticas, donde la ciberguerra, como principalmente se denomina, es concentra en 2 (o más) militares que únicamente extienden habilidades cibernéticas maliciosas contra los sistemas de la otra parte, dando por derivación muerte y devastación, para conseguir una serie de fines gubernamentales claros.

Las capacidades cibernéticas, necesita en primera instancia, localizar el grado de la guerra en el que será empleada. Por esto, Plan de capacidad conceptual del Ejército de EE. UU., para operaciones en el ciberespacio 2016-2028, apunta que estas habilidades poseen 4 recursos básicos: organización (quién), la iniciativa primordial (qué), el medio ambiente, los límites y las condiciones (dónde y cuándo) y el motivo (por qué). El "quién", identifica el grado en el cual la capacidad es solicitada.

En este sentido, las Fuerzas Especiales del Ejército Nacional, necesitan afrontar el ciberespacio como un entorno estratégico, operativo y táctico, para acomodar, practicar y suministrar a sus hombres, con la intención de utilizar medidas de prevención, disuasión, sujeción, defensa y actitud, que permitan robustecer las habilidades de Ciberseguridad, para afrontar las amenazas o ataques cibernéticos que logren perjudicar la infraestructura crítica cibernética de la nación y situar en peligro la estabilidad nacional, la custodia de la autonomía y el orden constitucional del Estado, así como

provocar perjuicios masivos, disminuir la economía, y/o afectar la moral pública y la confianza. (Realpe, M., y J. Cano, 2020).

Para tal resultado, el Ministerio de Defensa Nacional de Colombia en el año 2012, aprobó la construcción y activación del Comando Conjunto Cibernético (CCOCI), con la funcionalidad primordial de ejercer la Ciberseguridad del país y conducir operaciones militares cibernéticas a grado estratégico, para ser garantes de la estabilidad y custodia del país en el ciberespacio. Del mismo modo, se ordenó la construcción de cimentaciones organizacionales al interior de cada Fuerza llamadas Unidades Cibernéticas, de esta forma, una en el Ejército Nacional, otra en la Armada Nacional y una tercera en la Fuerza Aérea de Colombia, con las cuales el CCOCI ejecutará y coordinará acciones de Ciberseguridad y operaciones de Ciberdefensa de la nación. (Comando Conjunto Cibernético, 2017). En otra instancia, por medio de la Resolución 7144 de 2018, se creó el Plan Estratégico del Sector Defensa y Seguridad una Guía de Planeamiento Estratégico 2016-2018, donde se identifica las próximas tácticas a ser adelantadas:

a) Evaluar las habilidades operacionales y de soporte prioritarias para formular propuestas de solución materiales y no materiales acorde a los requerimientos del ámbito a mediano y extenso plazo.

b) Diseñar de manera conjunta y coordinada indicadores que permitan medir todos los elementos de capacidad (Doctrina, Organización, Material/Equipo, Personal e Infraestructura), como parte de la obra y desarrollo del Sistema de Monitoreo de capacidades.

c) Alinear la planificación estratégica con la idealización presupuestal por medio de la formulación de los proyectos de inversión bajo la metodología de Organización basada en habilidades.

d) Desarrollar e llevar a cabo un proceso presupuestario por programas vinculados a habilidades que permitan articular las resoluciones no materiales así como las resoluciones materiales con financiación de las Fuerzas para la preparación anual de presupuesto.

Es fundamental destacar que el Ministerio de Tecnologías de la Información y Comunicaciones (MinTIC), diseñó un modelo de gobernanza que robustecerá la coordinación positiva entre los diferentes actores del ámbito digital, por medio del Decreto 338, del 8 de marzo de 2022, en el cual se establece la definición y el alcance que van a tener los Grupos de Respuesta a Incidentes Cibernéticos (colCERT), asesorando, apoyando y coordinando a las diversas piezas interesadas para la idónea administración de los peligros e incidentes digitales.

Aunado a ello, Acosta, O. (2012), señala que la Organización del Tratado del Atlántico Norte (OTAN), con el objetivo de ayudar una obtención coordinada e interoperable de las capacidades de ciberdefensa entre las naciones, le encargó a la Agencia de Consulta, Comando y Control de la Organización del Tratado del Atlántico Norte (NC3A), hacer una extracción, categorización o taxonomía de las capacidades de ciberdefensa, con el fin de ofrecer una iniciativa clara de sus puntos operativos y dividir el esfuerzo de desarrollo u obtención en partes manejables que logren ser tratadas de manera sin dependencia; esta clasificación desglosa la ciberdefensa en 6 zonas de capacidad:

a. Detección de actividad maliciosa: capacidad que se implementa por medio de la recolección de información de una vasta gama de sensores, base para la investigación que separe los flujos de tráfico entre entidades malignas, que posibilite una evaluación del caso; ésta se consigue relacionando entidades maliciosas entre sí y con las entidades de procedencia y destino, además de considerar el histórico de ocupaciones entre ellas.

b. Prevención, mitigación y terminación de ataques;

c. Estudio dinámico de peligros, ataques y perjuicios;

d. Recuperación de ciberataques: capacidad para recuperarse de un ataque por medio de la reposición del sistema y la información a su estado original y a sus características de estabilidad.

e. Toma de decisiones oportunas: capacidad de dictaminar sobre las actividades a ser implementadas de forma adecuada, ya que en el espacio cibernético los eventos tienen la posibilidad de realizarse de manera vertiginosa, esto implicará que en muchas situaciones la contestación sea automática para asegurar que es suficientemente instantánea. Sea como sea, va a ser preciso la toma de decisiones por individuos para coordinar los resultados de diversas respuestas y escoger la mejor vía a continuar en el proceso de custodia.

f. Administración de la información de ciberdefensa: capacidad de recopilar y compartir información de manera que posibilite un trueque veloz y fiable entre diversas partes. Entre la información sobre ciberdefensa a compartir se encontrará una estimación del fin del contrincante y de su capacidad, así como, información sobre las vulnerabilidades conocidas, programa maligno, las evaluaciones y certificaciones de los diversos productos de programa y hardware.

Ahora bien, en palabras de Realpe, M., y J. Cano (2020), el modelo de planeamiento por capacidades DOMPILEM (*Doctrina, Organización, Material, Personal, Infraestructura, Liderazgo, Entrenamiento, Mantenimiento*), consienten conformar unas capacidades que reconozcan la expansión operativa necesaria para responder ante las nuevas amenazas cibernéticas, a razón de ello, se describe:

Doctrina: cómo se combate.

Organización: cómo es el diseño de la fuerza.

Material: componentes ineludibles para proveer las fuerzas con el objetivo de que puedan manipular de manera efectiva.

Personal: recurso humano preciso para combatir en la guerra, afrontar contingencias o participar en operaciones de paz.

Instalaciones: bienes inmuebles.

Liderazgo y educación: cómo preparar a los comandantes en cada uno de los escalones para conducir el combate a través del desarrollo profesional.

Entrenamiento: cómo debe ser la preparación para el combate desde el adiestramiento básico hasta la formación individual de especialistas y el entrenamiento en los diferentes escalones.

Mantenimiento: acciones que se solicitan para el sostenimiento de la capacidad en el tiempo.

Por otro lado, es importante acotar que la Resolución 7144 de 2018, expone que la capacidad, corresponde a la habilidad de una unidad militar o policial, de hacer una labor, bajo ciertos estándares (como tiempo, distancia, simultaneidad, entre otros.), por medio de la unión de sus respectivos elementos: Ideología y documentos que aguantan la capacidad, Organización, Material y equipo, Personal e Infraestructura, (DOMPI). Estas capacidades se catalogan en diversos niveles según su naturaleza y objetivo. Al grupo de niveles de habilidades se le nombra Taxonomía de Capacidades, siendo las que posibilitan la acción de las Fuerzas para el cumplimiento de sus misiones y responden a la naturaleza y especialización de todas ellas.

Cabe agregar que el Comando General de las Fuerzas Militares (COGFM, 2018), plantea que la táctica militar garantiza un enfoque grupal, integral y sistémico que posibilita completar los diversos frentes y aristas en relación con la Ciberseguridad y Ciberdefensa Nacional para mejorar la efectividad operacional en el ciberespacio,

proporcionando principios primordiales que guíen el trabajo de las Unidades de las Fuerzas Militares de Colombia (FF.MM.) hacia un objetivo común; se necesita poner en claro que las Fuerzas Militares de Colombia es el concepto utilizado para denotar colectivamente todos los elementos del Batallón, Armada y Fuerza Aérea.

Para cerrar, la táctica militar de ciberseguridad, es una contestación positiva a los peligros y amenazas a los que se ve enfrentada la seguridad y protección de la nación de cara a las tecnologías disruptivas, con ello, un modelo sistémico con base en fines estratégicos analizados en todos los elementos del modelo DOMPILEN; con esto ha sido exacto precisar y conceptualizar prospectivamente hacia donde tienen que ir las Fuerzas Militares para desarrollar habilidades militares en el desarrollo de operaciones cibernéticas, soportadas en un marco legal y constitucional.

5. Etapas de madurez de la capacidad cibernética aplicada por el Ejército Nacional Colombiano.

En relación al objetivo específico numero dos el cual se propuso identificar etapas de madurez de la capacidad cibernética aplicada por el Ejército Nacional Colombiano, en este contexto existen 5 etapas, planteadas por Agrafiotis, L., Nagyfejeo, E., Bada, M., y Kastelic, A. (2020), que fluctúan a partir de la etapa inicial hasta la etapa dinámica. La etapa inicial involucra una orientación apropiada de la capacidad, en lo que la etapa dinámica personifica un enfoque estratégico y la funcionalidad de ajustarse dinámicamente o de modificar en contestación a consideraciones del medio ambiente. Las 5 etapas se describen como: etapa inicial, formativa, fundada, estratégica y dinámica.

Con respecto a la *Etapa Inicial*, en este periodo no existe madurez en ciberseguridad, o bien está en un estado bastante embrionario; consigue la existencia en debates iniciales sobre la construcción de capacidad sobre temas de estabilidad cibernética, sin embargo no se han acogido medidas específicas. En este periodo no hay pruebas notorias de la capacidad en temas de estabilidad cibernética. (Agrafiotis, L., Nagyfejeo, E., Bada, M., y Kastelic, A., 2020).

Siguiendo la misma línea, Ayllón (2007) expone que es la definición de los objetivos y recursos, donde se ha de prestar especial atención a la definición de requisitos así como a recopilar la información necesaria para el resto del proyecto, o al menos para afrontar la siguiente fase con garantías.

Por otro lado, Pérez (2007) manifiesta que esta fase tiene como finalidad recopilar la información clave del proyecto y es el documento inicial utilizado para formalizar la autorización del líder del proyecto, para solicitar y comprometer los recursos de la organización. Es importante destacar, que en dicha fase, se hace referencia al presupuesto del proyecto en términos muy generales. Para Chamoun (2004), la fase de iniciación indica como establecer la visión del proyecto, el qué y la misión por cumplir, sus objetivos, la justificación del mismo, las restricciones y supuestos.

Para los autores Ayllón (2007), Pérez (2007), Chamoun (2004), la iniciación es la fase para coleccionar información importante para la organización; aspecto que guarda semejanza, no obstante, el investigador fija posición con lo planteado por Ayllón (2007) al afirmar que esta fase se maneja para confrontar la sucesiva fase con cauciones. Por último, Palomo (2010), expresa que en esta fase la madurez profesional es baja y los miembros del grupo no suelen tener claros los objetivos del equipo y cuál va a ser su contribución a los mismos. La madurez grupal

sele ser alta, ya que los componentes del mismo aunque, muestren interés, ilusión y expectativas positivas con respecto al futuro del grupo, aunque no han desarrollado sistemas de interacción efectivos y no existen sentimientos de pertenencia.

En este sentido, el autor antes mencionado acota, que durante esta fase, habrá una gran dependencia del líder y los miembros mostraran un cierto grado de ansiedad, al no estar claras sus funciones, roles y las futuras relaciones interpersonales. Ante dicha situación los resultados del grupo son medios o bajos y el esfuerzo se centra fundamentalmente en definir las metas y funciones; cómo enfocar las distintas actividades; y que competencias serán precisas para logar los objetivos.

Por otro lado, en la *Etapa Formativa*, ciertos puntos comenzaron a desarrollarse y a ser formulados, sin embargo tienen la posibilidad de ser apropiada, desorganizadas, mal definidas o sencillamente nuevos. No obstante, la prueba de este aspecto podría ser precisamente verificada. (Agrafiotis, L., Nagyfejeo, E., Bada, M., y Kastelic, A. 2020)

Al mismo tiempo, Global Cyber Security Capacity Centre (2016), explica que en esta etapa varias propiedades de los puntos se comienzan a realizar y a ser formuladas, sin embargo, podrían no estar desorganizadas, o determinada o sencillamente ser nueva, no obstante, se puede mostrar precisamente prueba de esta actividad. En palabras de Urrutia, F., Treppel, A., Daniell, A., y South, M. (2019), hay varias iniciativas sobre ciberseguridad, los enfoques ad-hoc, alta dependencia del personal y fuerza reactiva frente a incidentes de estabilidad. No obstante, Nowersztern, A., Kagelmacher, D., Barrett, K., y Ramírez, R. (2020), de esta etapa formativa, ciertos puntos comenzaron a crecer y formularse, pero tienen la posibilidad de ser ad hoc, desordenados, mal definidos, o sencillamente nuevos, sin embargo, se puede enseñar evidentemente prueba de este aspecto.

En relación a la *Etapa Consolidada*, los indicadores del aspecto permanecen instalados y en funcionamiento. No obstante, no se le dio mucha importancia a la concesión de recursos. Se han tomado escasas decisiones sobre las ventajas en relación a la inversión relativa en este aspecto, no obstante en esta fase es servible y está determinada. (Agrafiotis, L., Nagyfejeo, E., Bada, M., y Kastelic, A., 2020).

Plantea Global Cyber Security Capacity Centre (2016), que esta fase consolida los recursos del aspecto orden y funcionamiento; sin embargo, no hay consideraciones bien establecidas respecto a la asignación de recursos, tomando escasas elecciones de compromiso en relación con la transformación referente a diversos recursos del aspecto, haciendo énfasis a que la apariencia es servible y concluyente.

Abordando los criterios de Urrutia, F., Treppel, A., Daniell, A., y South, M. (2019), hay ciertos lineamientos para la ejecución de las actividades, siendo dependencia del personal para continuar en el desarrollo de los procesos y documentación de las actividades. Asimismo, Nowersztern, A., Kagelmacher, D., Barrett, K., y Ramírez, R. (2020), manifiestan que las guías permanecen instalados y en funcionamiento, no obstante, le dan poca importancia a la asignación de recursos, tomando escasas elecciones sobre las ventajas en interacción al cambio relativo en este aspecto, tomando en cuenta que la fase es aprovechable y está terminante.

Tratando lo concerniente a la *Etapa Estratégica*, en este periodo, se han tomado decisiones sobre qué indicadores del exterior son relevantes y cuáles son menos relevantes para la entidad o el Estado en especial, esta fase es importante, irradia el hecho de que estas elecciones se realizaron condicionadas por las situaciones particulares del Estado o de las empresas. (Agrafiotis, L., Nagyfejeo, E., Bada, M., y Kastelic, A., 2020).

Dentro del conjunto, Global Cyber Security Capacity Centre (2016), explica que se han proclamado preferencias sobre las piezas más relevantes del exterior, viendo que son menos relevantes para la organización o el territorio específico; la fase estratégica refleja el hecho de que estas preferencias se hayan proclamado, acorde a las situaciones de la organización o territorio determinado. Tratando de profundizar, Urrutia, F., Treppel, A., Daniell, A., y South, M. (2019), se define por la formalización y documentación de políticas y métodos, así como de la gobernanza de la ciberseguridad tomando en cuenta los ritmos de seguimiento.

Otra forma de contribuir, Nowersztern, A., Kagelmacher, D., Barrett, K., y Ramírez, R. (2020), en este periodo se han tomado disposiciones sobre qué indicadores de este aspecto son relevantes y cuáles son lo menos para la organización o el Estado, reflejando el hecho de que estas disposiciones se realizaron condicionadas por las situaciones particulares del Estado o de las empresas.

Por último, la *Etapa Dinámica*, en este periodo hay componentes claros para cambiar la táctica en función de las situaciones dominantes, como la figura tecnológica del ámbito de amenaza, el problema mundial o un cambio importante en una esfera de interés, muestra de ello puede ser el delito cibernético o la privacidad. Las empresas dinámicas han perfeccionado procedimientos para cambiar las tácticas variables a medio camino. La toma inmediata de elecciones, la reasignación de recursos y la atención constante al ámbito cambiante son propiedades de esta fase. (Agrafiotis, L., Nagyfejeo, E., Bada, M., y Kastelic, A. 2020).

En torno a Global Cyber Security Capacity Centre (2016), en esta etapa, hay mecanismos establecidos para cambiar la táctica dependiendo de las situaciones vigentes, como por ejemplo la tecnología en un ambiente amenazado, problema mundial o un cambio relevante en un entorno de interés, ejemplificando, ciberdelincuencia o

privacidad. Las empresas dinámicas han desarrollado procedimientos para modificar tácticas sin perder su ritmo, la instantánea toma de decisiones, reasignación de recursos y la atención constante a los cambios en el ámbito son propiedades de esta etapa.

De acuerdo con Urrutia, F., Treppel, A., Daniell, A., y South, M. (2019), el Responsable de Seguridad de la Información (RSI), tiene un papel clave en el control y optimización del Sistema de gestión de la seguridad de la información (SGSI), llevando a cabo un control interno, se labora en la optimización continua y la ciberseguridad está alineada con las metas y tácticas de la organización.

Finalizando Nowersztern, A., Kagelmacher, D., Barrett, K., y Ramírez, R. (2020), en este periodo hay mecanismos claros para variar la táctica en funcionalidad de las situaciones prevalentes, como la sofisticación tecnológica del ámbito de amenaza, el problema universal o un cambio importante en un área de inquietud, las entidades dinámicas han perfeccionado procedimientos para modificar las tácticas con tranquilidad. De este modo, se muestra en la tabla 1, de manera resumida las etapas de madurez de la capacidad cibernética.

Tabla 1.

Etapas de madurez de la capacidad cibernética

Etapas de madurez de la capacidad cibernética	
Inicial	No existe madurez en ciberseguridad o se encuentra en un estado básico.
Formativa	Consiste en que ciertos puntos comenzaron a crecer y formularse, sin embargo tiene la posibilidad de ser adecuado, desordenados, mal definidos, o sencillamente nuevos.
Consolidada	Las pautas permanecen instalados y en funcionamiento. No obstante, no se le dió importancia a la asignación de recursos.
Estratégica	En este momento se han realizado decisiones sobre qué pautas de este aspecto son relevantes y cuáles no para la entidad o el estado en especial.
Dinámica	En este momento hay elementos claros para cambiar la táctica en funcionalidad de las situaciones valiosas, como la figura tecnológica del ámbito de amenaza, el conflicto global o un cambio notable en un área de inquietud.

Fuente: Elaboración propia

Ahora bien, desde el estado de madurez existen estas dimensiones de las capacidades de seguridad cibernética, las consultas se asentaron en el Modelo de Madurez de la Capacidad de Seguridad Cibernética para los países (CCM, por sus siglas en inglés) del Centro Global de Capacidad en Estabilidad Cibernética (GCSCC), señalan Agrafiotis, L., Nagyfejeo, E., Bada, M., y Kastelic, A. (2020), que encierra 5 dimensiones de la función de ciberseguridad. Cada magnitud está concertada por un número de componentes que figuran y precisan lo cual supone que cada elemento refiera con capacidad de ciberseguridad, existiendo las siguientes:

Figura 1. Dimensiones de la función de ciberseguridad. Fuente: Elaboración propia adaptada de Agrafiotis, L., Nagyfejeo, E., Bada, M., y Kastelic, A. (2020).

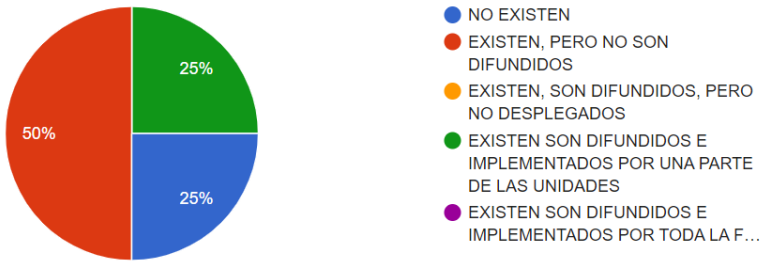
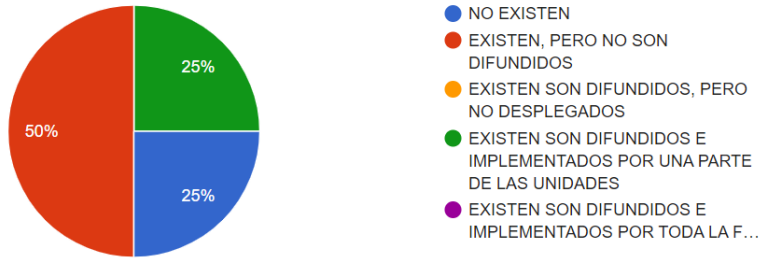
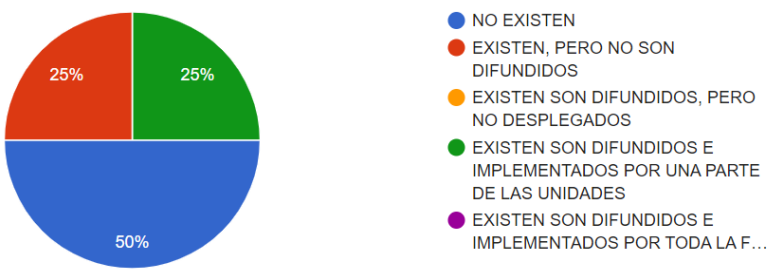
Estas cinco (5) dimensiones comprenden la extensa superficie de expansión que deberían ser consideradas una vez que se desea mejorar la capacidad en ciberseguridad, se reconoce que estas dimensiones tienen la posibilidad de superponerse unas con otras

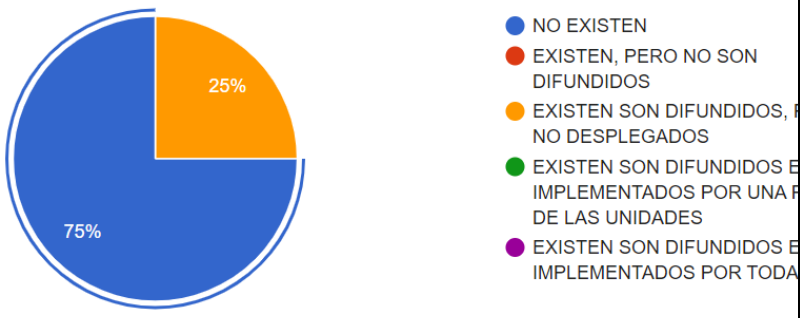
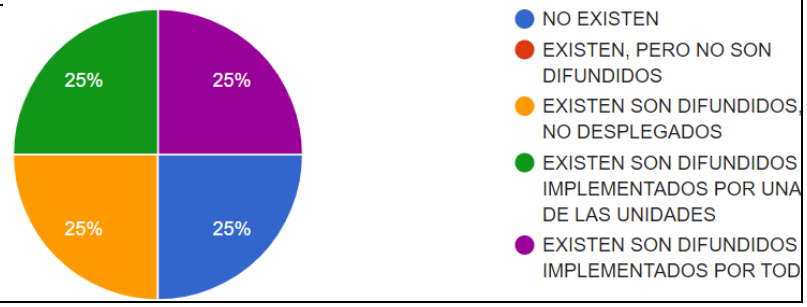
en determinados puntos, y, por cierto, el centro de capacidad espera entender la interdependencia en medio de las habilidades en ciberseguridad una vez que haga otras revisiones de capacidad nacional.

6. Recomendaciones para la identificación y fortalecimiento de las capacidades cibernéticas del Ejército Nacional Colombiano

En este apartado, se presentan los resultados obtenidos por medio de la aplicación de la encuesta a cuatro expertos en la materia, iniciando por aquellas interrogates relativas a la doctrina:

En torno a la Doctrina

Interrogantes	Respuestas cotejadas
1.¿Existen manuales conjuntos y por fuerza?	
2. ¿Existen planes de protección?	
3.¿Existen manuales de operaciones cibernéticas?	

4.¿Existen manuales de apoyo cibernético ?	
5. ¿ Existen acuerdos convenios?	

Fuente: Elaboración propia (2022)

Como se evidencia en la tabla anterior, en lo referido a la doctrina, se procedió a efectuar un total de cinco (5) preguntas a los encuestados, la primera de ellas con la intencipon de conocer si existen manuales conjuntos y por fuerza, ante lo cual el 50% respondieron que si existen pero que los mismo no son difundidos, mientras que una parte de los encuentasdos respondieron que existen, son difundidos y empleados por una parte, y la parte restante de los encuestados (25%), respondieron que no existen rales manuales conjuntos y por fuerza.

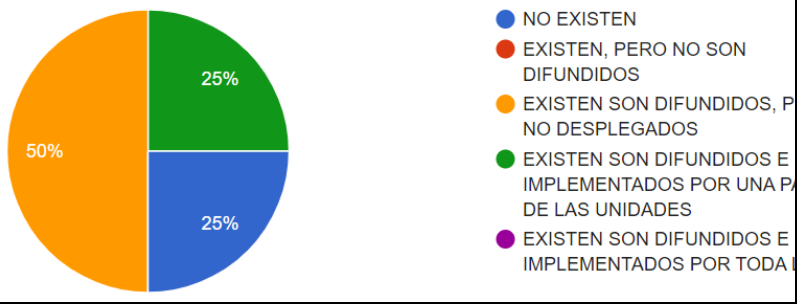
Seguidamente, se procedipo a efectuar la segunda interrogante la cual se planteo conocer si existen existen planes de protección, frente a lo cual el 50% de los encuestados aseveró que dichos planes si existen más no son difundidos, el 25% de los mismos expresa que estos planes no existen, mientras que el 25% de la poblacion objeto de estudio afirma que dichos planes si existen, son difundidos e implementados por una parte de las unidades. Para el tercer interrogante, encargado de saber si existen manuales de operaciones ciberneticas, el 50% de la poblacion encuestada contesto que estos manuales

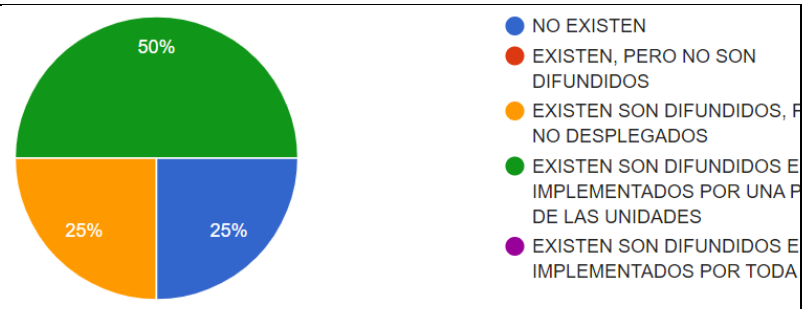
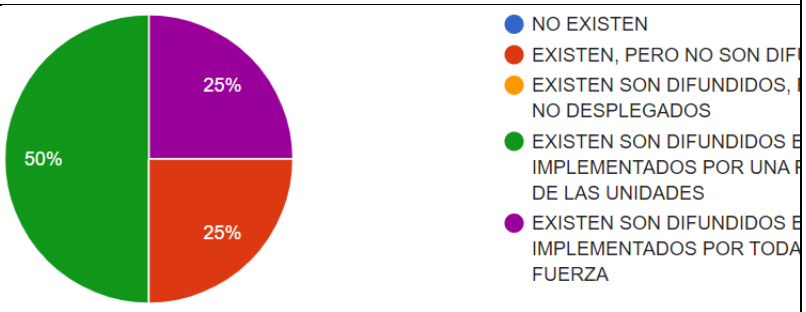
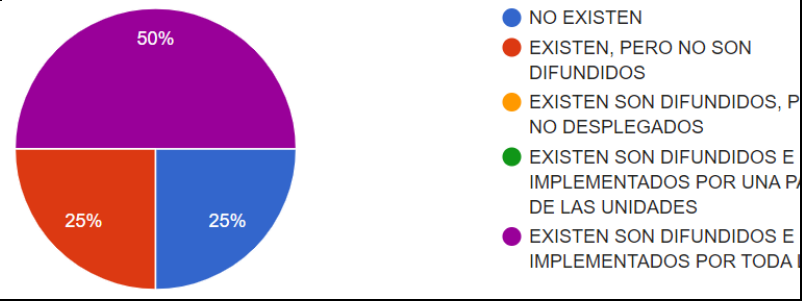
no existen, al tiempo que la parte restante se divide entre la opcion existen pero no son difundidos y existen, son difundidos e implementados por una parte de las unidades.

Para el cuarto interrogante, ocupado en descibrir si existen manuales de apoyo cibernetico, se encuentr una respuesta parcializada, siendo que la mayoria de la poblacion encuestada, representada por el 75% afirma que estos manuales no existen, difiriendo por completo con el 25% restante, quienes expresan que dicho manuales si existen, sin difundidos pero no desplegados. Por ultimo, para el quinto interrogante, destinado a conocer si existen acuerdos de convivencia, se encontraron cuatro respuestas igualemete divididas al 25% respectivamente, donde una primera parte expresa que estos acuerdos existen, son difundidos e implementados por toda la fuerza, otro 25% opina que existen, son difundidos peron no desplegados, 25% manifiesta que existen son difundidos e implementados por una parte de las unidades y el 25% restante afirma que estos acuerdos no existen.

A continuación se presentan los resultados correspondiente a las interrogantes en torno a la organización:

En torno a la Organización

Interrogantes	Respuestas cotejadas
6. ¿Existe un nuevo componente militar?	

7. ¿Existen equipos interdisciplinarios?	
8. ¿Existen equipos de batalla?	
9. ¿Existe la conformación ligas nacionales e internacionales?	

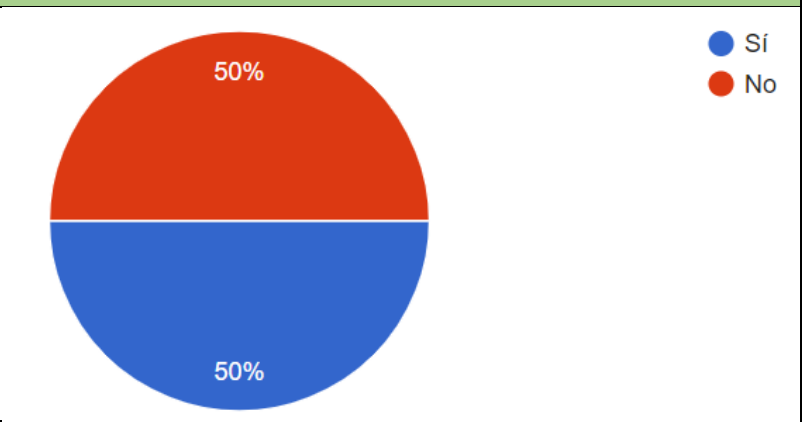
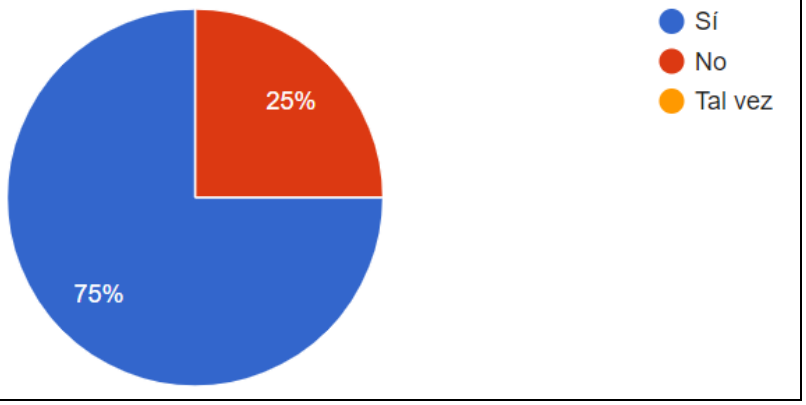
Fuente: Elaboración propia (2022)

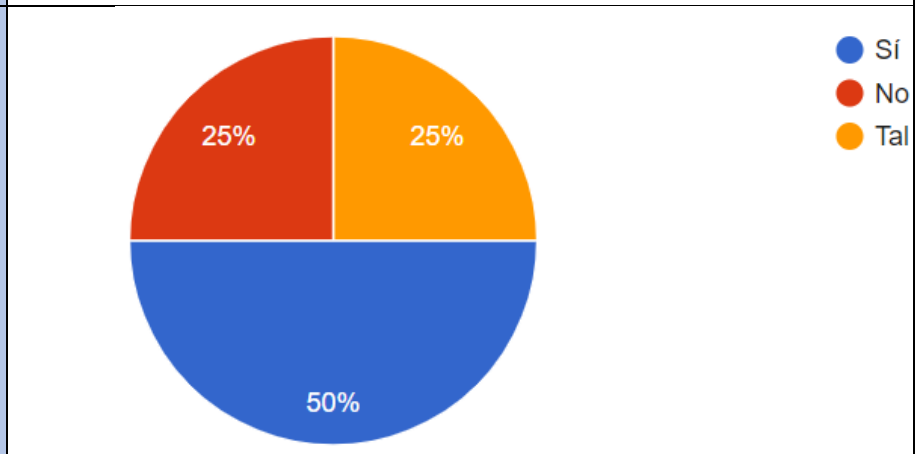
En referencia a la sexta interrogante, la cual se propuso indagar si existe un nuevo componente miltar, el 50% de la poblacio encuestada estuvo deacuerdo en que si existe un nuevo componente militar, que es difundido mas no desplegado, el 50% restante de los encuestados en un 25% respectivamente manifestaron que no existe tal componene o que existe, es difundido e implementado por una parte de las unidades. Seguidamete para la septima interrogante encargada de indagar si existen equipos iterdisciplinarios, el 50% de los encuestados manifestaron que si existen equipos interdisciplinarios, mientras que un 25% expresa que esxisten, son difundidos pero no son desplegados y el 25% restante opina que dichos equipos interdisciplinarios no existen.

Por otra parte, en lo que respecta a la interrogante numero ocho, se propuso conocer si exsten equipos de batalla, ante lo cual el 50% de los encuestados expone que si existen, que esta informacion es difundida y que es palicada por una parre de las unidades, mientras que un 25% comunica que estos equipos existen pero no es difundida su existencia, ello frente al 25% restante que manifiesta que estos equipos existen, su existencia es difundida e implementada por toda la fuerza. Por ultimo, el noveno interrogante encargado de dilucidar si existe la conformacion de ligas nacionales e internacionales, el 50% de los encuestados manifestaron que existen, son difundidas e implementadas por toda la fuerza.

A continuación se presentan los resultados obtenidos mediante encuesta, en torno al material:

En torno al Material

Interrogantes	Respuestas cotejadas
10.¿ Considera usted que se manejan hardware & softwares adecuados?	
11. ¿ Considera usted que existen plataformas compartidas para beneficio del ejercito?	

12. ¿Diría usted que el ejercito cuenta con equipo de combate cibernético especializado de alto nivel?	

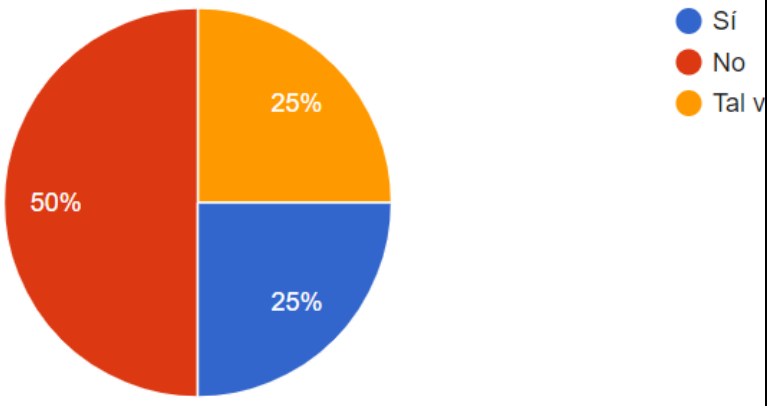
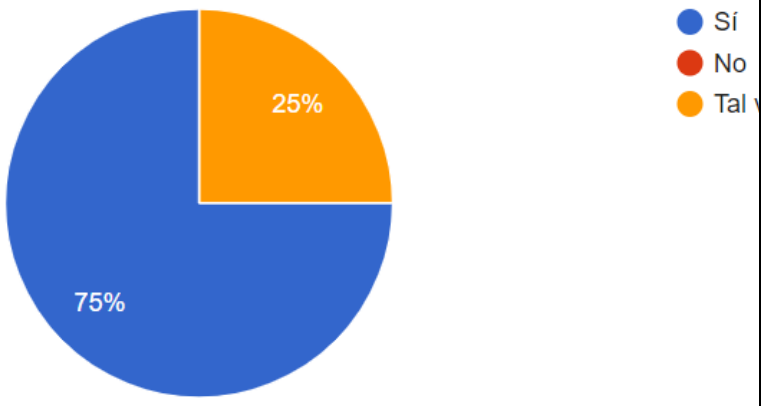
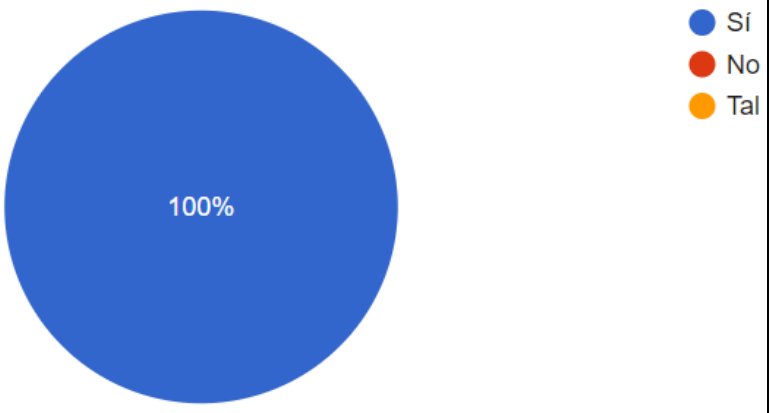
Fuente: Elaboración propia (2022)

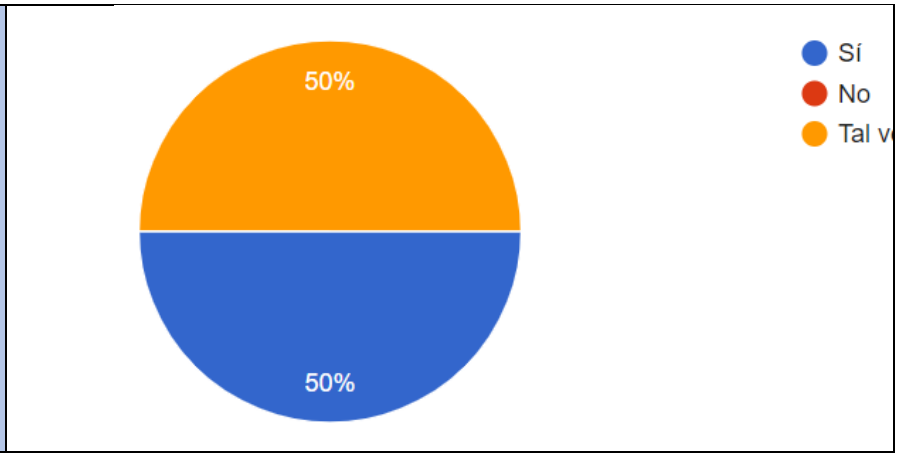
En lo referido al decimo interrogante, indaga si los encuestados consideran que se manejan hardware y software adecuados, ante lo cual se evidencio una respuesta dividida, donde el 50% de la poblacion encuestada expone que no, mientras el 50% restante indica que si se manejan y son adecuados. Seguidamente para la interrogante numero once, donde se buca saber si los encuestados consideran que existen plataformas compartidas para beneficio del ejercito, el 75% de la poblacion objeto de etudio manifestó que si, mientras que el 25% restante de los encuestados sostiene una respuesta negativa ante el planteamiento.

Para dar respuesta al interrogante numero doce, donde se pregunta a los encuestados si dirian que el jercito cuenta con equipo de combate cibernetico especializado de alto nivel, el 50% de los mismos considera que si es asi, mientras que un 25% respone ante ello de forma negativa y el 25% restante de los encuestados expresa que tal vez si cuenten con el equipo cibernetico especializado y que este sea de alto nivel.

Acontinuación se presentan las respuestas obtenidas entorno al personal:

En torno al Personal

Interrogantes	Respuestas cotejadas
13.¿ Considera usted que el ejercito cuenta con la debida capacidad militar y civil?	
14. ¿Cuenta con comandos cibernéticos?	
15. ¿ Cuenta con apoyo de sector político y privado?	

16. ¿ Cuenta con personal nacional e internacional ?	

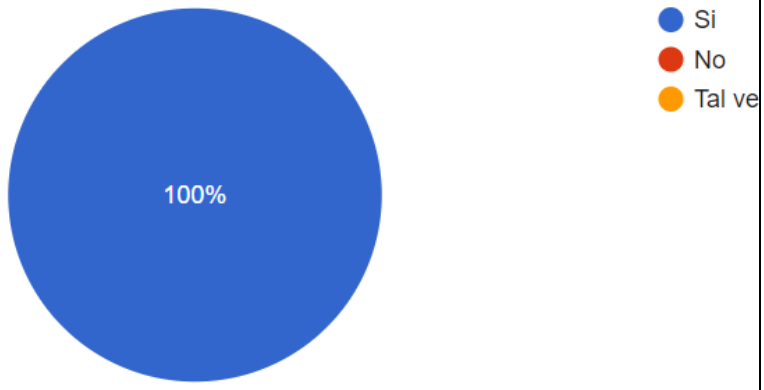
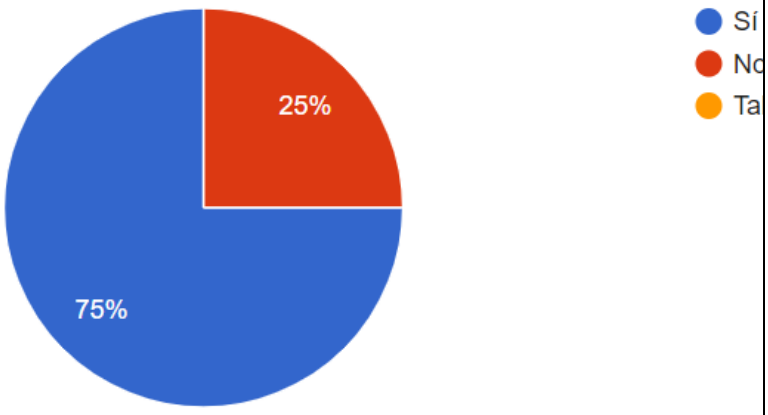
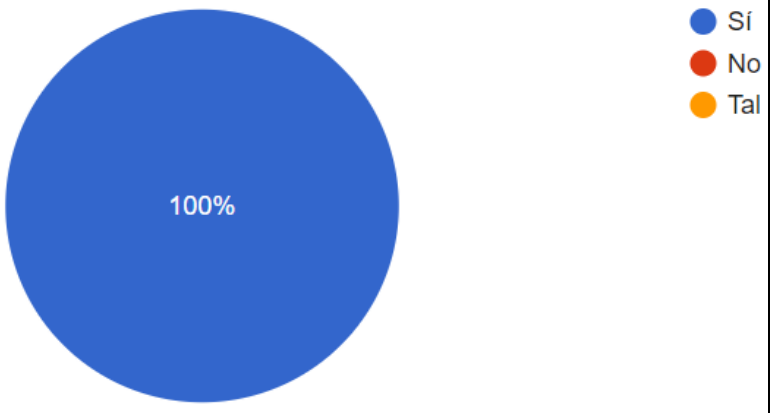
Fuente: Elaboración propia (2022)

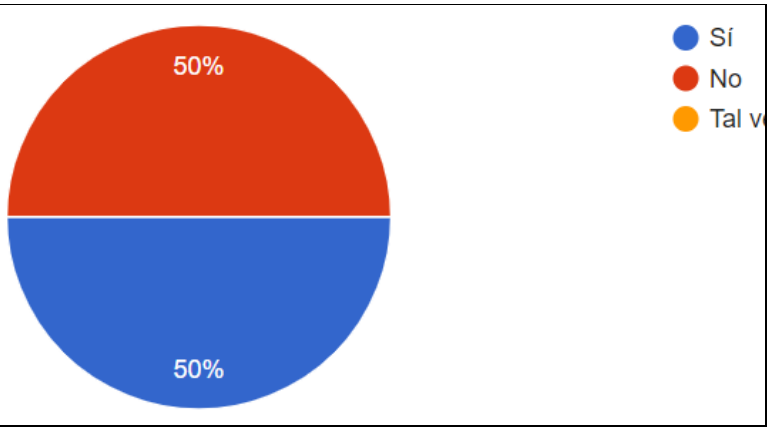
Respecto al interrogante numero trece, al indagar sobre si los encuestados consideran que el Ehjercito cuenta con la debida capacidad militar y civil, se pudo evidenciar que la mayoria de los encuestados representados por un 50% manifiesta que no cuentan con tal personal, sin embargo un 25% manifiesta que si, al tiempo que el 25% restante expresa que tal vez si cuenten con el mismo. Por otra parte, para el interrogante numero catorce, el 75% de la poblacion objeto de estudio afirma que el Ejercito si cuenta con comandos ciberneticos, frente al 25% que responde de forma dubitativa al expresar que tal vez sea asi, enlo referido al interrogante numero quince, el 100% de la poblacion encuestada estudo de acuerdo al responder de forma positiva y aceptar que el Ejercito si cuenta con apoyo de sentor politico y privado.

Por ultimo, para la interrogante numero dieciseis, encargada de indagar si el Ejercito Colombiano cuenta con persoal nacional e internacional, se encuentra nuevamente una opinion dividida de forma igualitaria, representadas por un 50% que manifiesta que si cuentan con tal personal, minetras que el 50% restante opina que tal vez cuenten con ello.

A continuacion se presentan los resultados de la encuesta obtenidos en torno a las instalaciones:

En torno a las instalaciones

Interrogantes	Respuestas cotejadas
17. ¿ Cuenta con oficinas, laboratorios, salas apropiadas?	
18. ¿ Cuenta con instalaciones propias y de terceros?	
19. ¿ Cuentan con sala mando y control cibernético?	

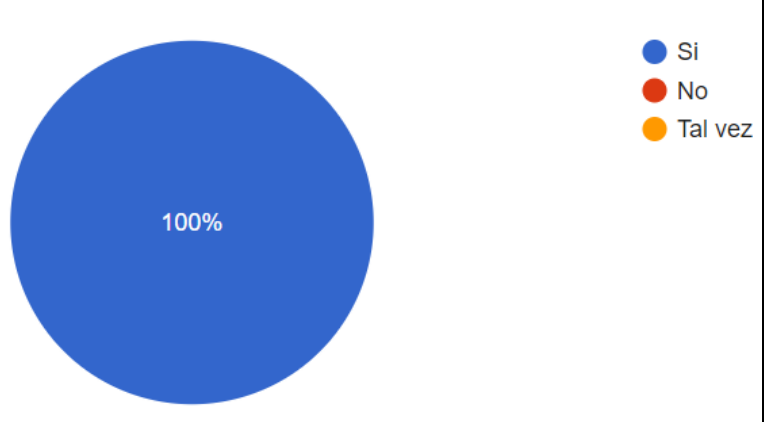
20. ¿ Cuentan con salas de intercambio cibernético propia y de terceros?	

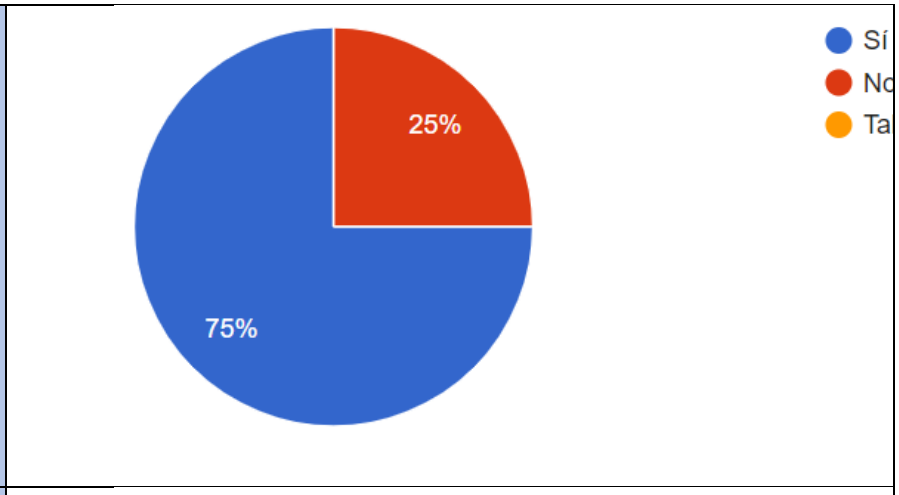
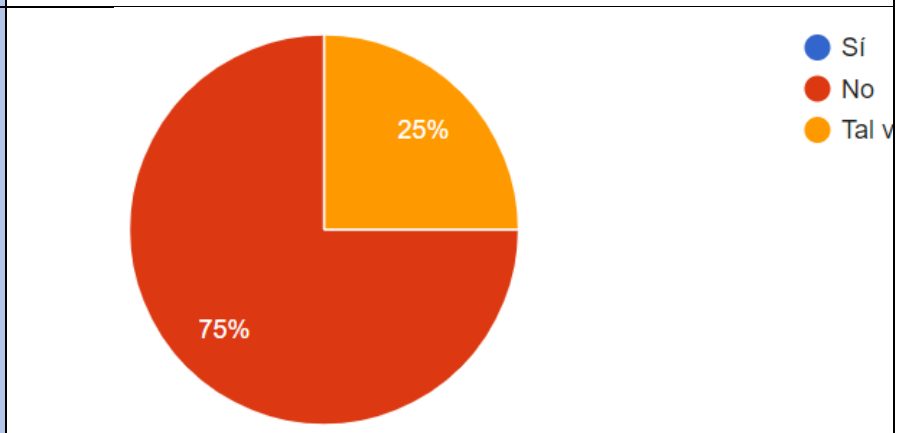
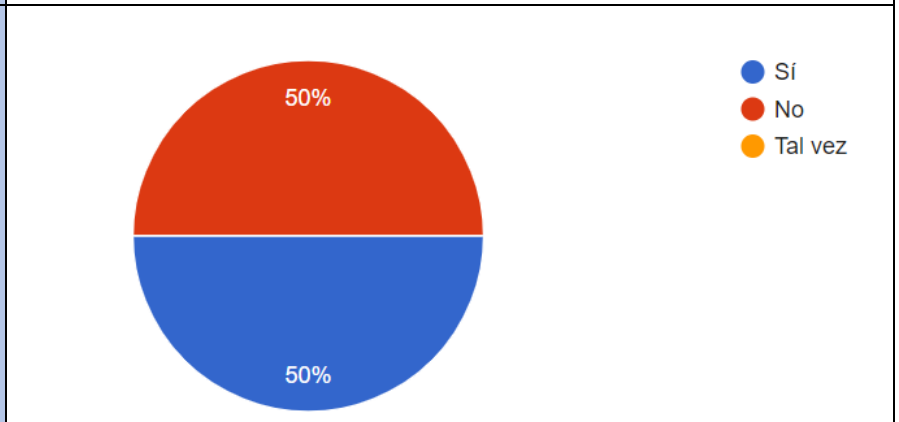
Fuente: Elaboración propia (2022)

Respecto del interrogante numero diecisiete, encargado de conocer si se cuenta con oficinas, lboratorios y salas apropiadas, el 100% de los encuestados afirma que si cuentan con estas caracteristicas, de igual forma el mismo porcentaje expresa que sí cuenta con sala de mando y control sibernetico, mientras que un 25% contesta que no cuentan con instalaciones propias y de terceros, seguidamete un 50% manifiesta que no cuentan con salas de intercambio cibernetico propia de terceros, lo cual se enfremta al 50% que afirma que si cuentan con dichas salas.

A coninuacion se presentan las respuesta obtenidas a traves de la encuesta aplicada, en torno al liderazgo:

En torno al Liderazgo

Interrogantes	**Respuestas cotejadas**
21. ¿ Manejan estrategias, expertos y especialistas técnicos?	

22. ¿ cuentan con expertos en activos estratégicos sectoriales?	
23. ¿tienen plan de carrera cibernética?	
24. ¿Manejan expertos cibernéticos internacionalistas?	

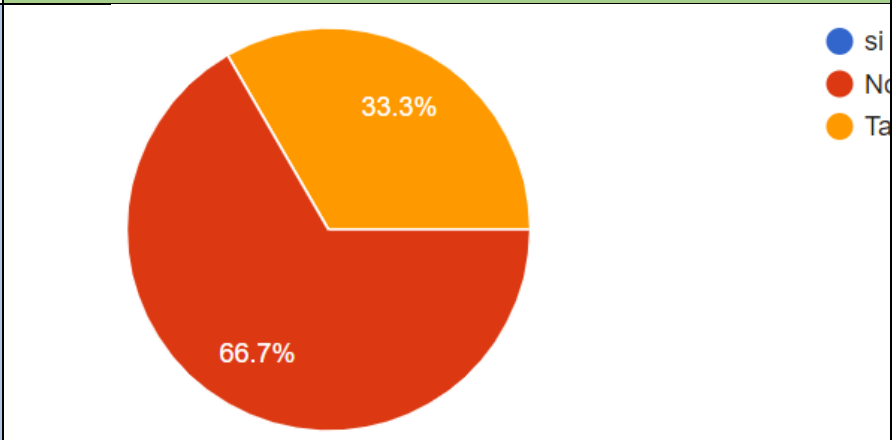
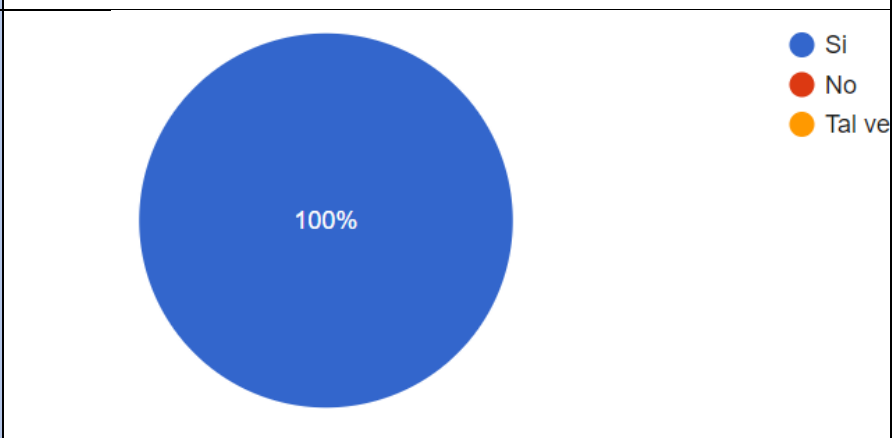
Fuente: Elaboración propia (2022)

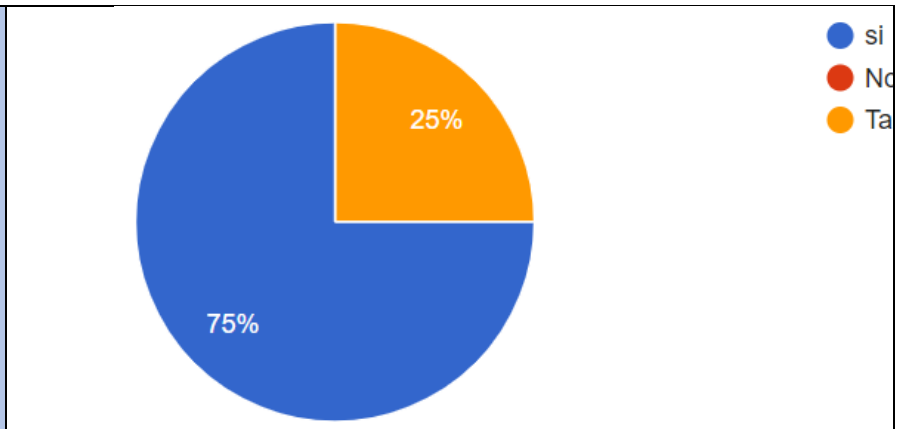
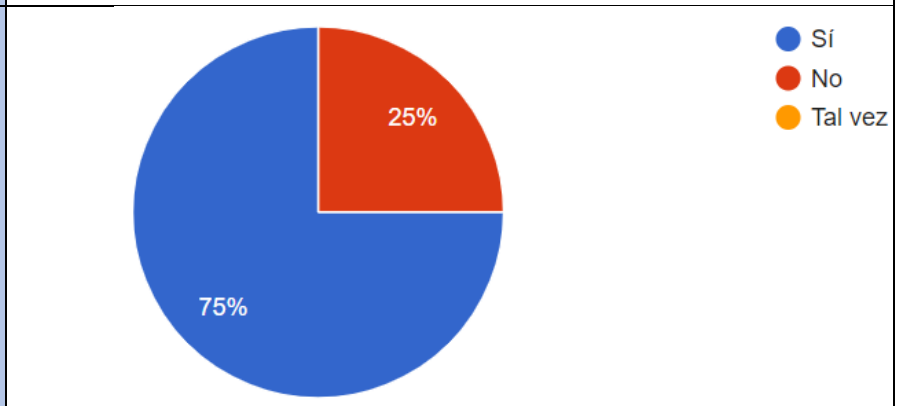
Para el interrogante numero veintiuno, el cual se propuso conocer si se manejan estrategias, espertos y especialistas tecnicos, el 100% de los encuestados responde de manera positiva, para el interrogante numero doce, donde se quiere conocer si cuentan con expertos en activos estrategicos sectoriales, se encuentra una opinion dividida donde

el 75% de los encuestados responde que si cuentan con los mismos, mientras que un 25% responde de manera negativa. Por su parte para el interrogante numero ventitres, el 75% de la poblacion encuestada expresa que no, cuentan con un plan de carrera cibernetica, mientras que el 25% por ciento de la poblacion encuestada comunica que tal vez cuenten con uno. Por ultimo, para el interrogante numero venticuatro, donde se pregunta si manejan expertos ciberneticos internacionalistas, el 50% de los encuestados responde de forma negativa, y el 50% restante afirma que si manejan sicho personal.

A continuación se presentan los resultados obtenidos para la seccion referida al entrenamiento:

En torno al Entrenamiento

Interrogantes	Respuestas cotejadas
25. ¿Considera usted que manejan sistemas control industrial?	
26. ¿cuentan con simulación olimpiadas cibernéticas?	

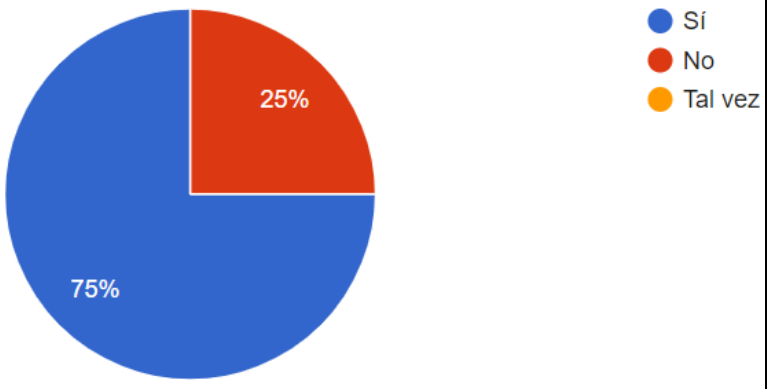
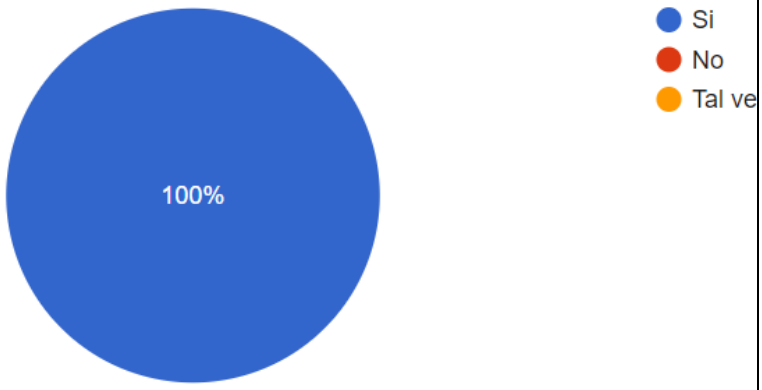
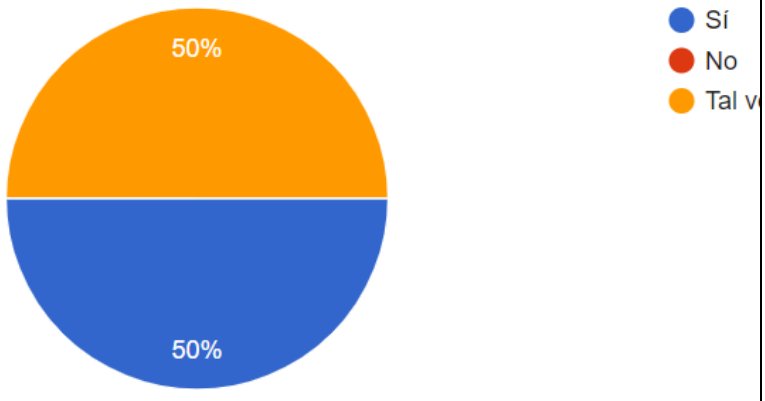
27. ¿tienen entrenamiento interinstitucional?	
28. ¿manejan cursos internacionales?	

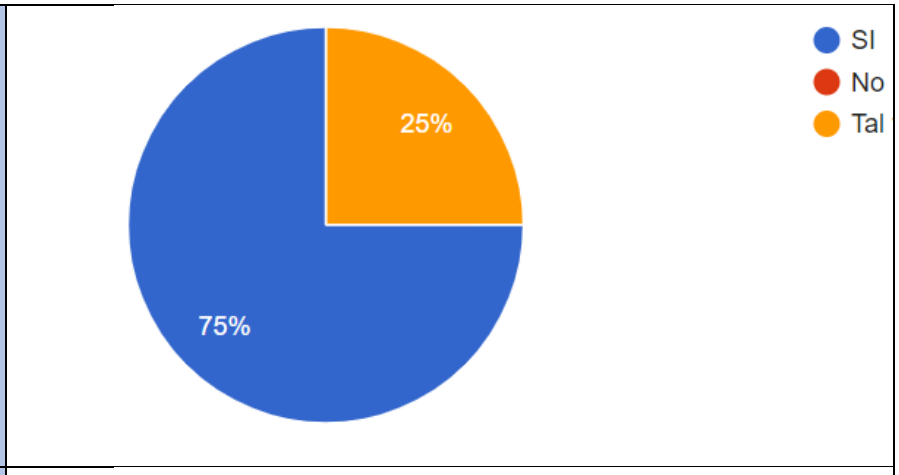
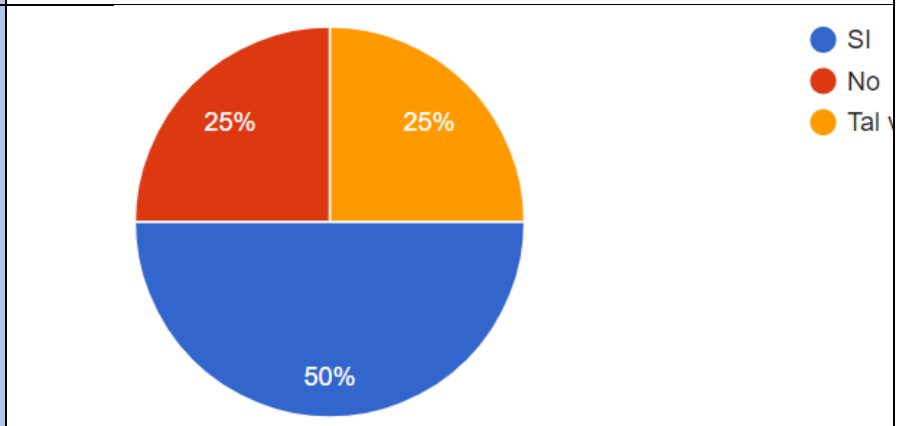
Fuente: Elaboración propia (2022)

Para el interrogante numero venticinco, donde se desea saber si los encuentados consideran que manejan sistemas de control industrial, el 66,7% expresa que no, mientras que el 33,3% manifiesta que si son manejados dichos sistemas. Para el interrogante ventiseis, el 100% de la poblacion encuestada manifiesta que si cuentan con simulacion de olimpiadas ciberneticas, mientras que para el interogante ventisiete el 75% de los encuestados indica que si tiene entrenamiento interinstitucional frente al 25% que expresa que este planteamiento no es acertado. Seguidamente, para e interrogante numero ventiocho, donde se pretendia conocer si manejan cursos internacionales, el 75% de la poblacion afirma recibir dichos cursos, mientras que el 25% dice que no.

A continuación, se presentan llas respuestas conseguidas en relacion al mantenimiento:

En torno al Mantenimiento

Interrogantes	Respuestas cotejadas
29.¿cuentan con plataformas cibernéticas?	
30.¿tienen sistemas de defensa cibernética?	
31.¿manejan plataformas de operaciones cibernéticas?	

32.¿tienen sistemas de apoyo?	
33.¿cuentan con sistemas de intercambio?	

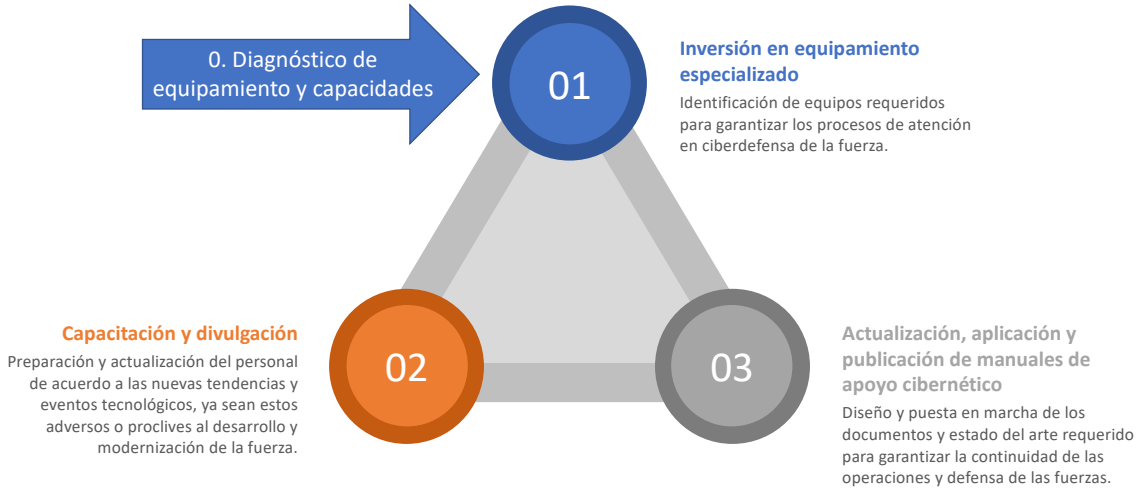
Fuente: Elaboración propia (2022)

En concordancia a lo reflejado en la tabla anterior, se envidencia que para el interrogante numero veintinueve, el 75% de los encuestados manifiesta que si cuentan con plataformas ciberneticas, mientras que el 25% restante expone que esto no es de esa manera, pues indican que no cuentan con dichas plataformas, por su parte, para el interrogante numero treinta, el 100% de la poblacion objeto de estudio manifiesta que si tienen sistemas de defensa cibernetica, lo cual se considera un aspecto pisitivo, mientras que para el interrogante numero treintaiuno se aprecia una respuesta dividida en proporciones iguales, cuando el 50% de la poblacion indica que si manejan anivel práctivo, plataformas de oprnaciones siberneticas siendo que el 50% restante indica que tal ves sea asi, lo que permite inferir que este 50% quizas no ha tenido acceso a las mismas.

Por otro lado, para el interrogante numero treinta y dos, el 75% de la poblacion objeto de analisis, manifiesta que en el Ejercito Colombiano si tiene sistemas de apoyo, mientras que el 25% de los mismos indica que talvez este planteamiento sea cierto, Por ultimo, y para finalizar con los resultados de la encuesta aplicada a los cuatro participantes, la interrogante numero treinta y dos se propuso conocer si el Ejercio Colombiano cuenta con sistema de intercambio, planteamiento ante el cual el 50% de la poblacion encuestada manifestó que si cuentan con dichos sistemas, mientras que un 25% de los mismos indico que tal vez sea de esta manera, frente al 25% restante que expone que el Ejercito Colombiano no cuenta con sistemas de intercambio.

Partiendo de los resultados obtenidos con la aplicación del instrumento metodológico, se propone el siguiente ciclo pensado en el fortalecimiento de las capacidades ciberneticas del Ejercito Nacional Colombiano, el cual consta de tres (3), factores clave que, desde la postura del autor, serviran para la construccion y actualización de bases tanto teoricas como prácticas en el area especifica atienente a los posibles ataques ciberneticos a los que se pueda enfrentar la nacion en la actualidad.

Ciclo para el fortalecimiento de las capacidades cibernéticas del Ejército Nacional Colombiano



Fuente: Elaboración propia (2022).

En este sentido, como se pudo apreciar en la imagen anterios, los tres factores plasmados se enfocan directamente a la preparacion tanto a nivel intelectual, como práctica de los integrantes del Ejercito Nacional Colombiano, destacando como punto inicial la urgente actualización del material disponible a modo de manuales a los que se tengan acceso, asi mismo, este material debe ser de dominio unicamente de aquellas personas que se esten preparando en el área, dado que es un material de consumo interno del cuerpo del Ejercito, debe ser administrado con total discreción y el mismo debe ser, como ya se ha mencionado, actualizado de forma periodica, a fin de poder estar a la vanguardia en el tema y que las capacidades de respuesta sean a la altura de los riesgos a los que se puedan enfrentar.

Seguidamente, se menciona el factor de inversión en equipamento especializado, pues asi como el material intelectual deber ser actualizado de forma periodica, tambien es cierto que los equipos de alta tecnología que garanticen la correcta y efectiva ejecusion de los conocimientos adquiridos, debe ser el apropiado para que ambos factores aseguren el resultado esperado, y ello solo puede ser alcanzado a traves de una importante inversión, que este de la mano con las capacitaciones debidas en el área.

Por ultimo, el factor capacitacion y divulgación, como ya se mencionó, una vez actualizado el material intelectual, este acompañado de la tenencia del equipo tecnologico apropiado, debe combinarse con la constante capaciación, enfocada en generar equipos de espuesta rapida y conciente ante las distintas amenazas que hoy en día se presentan y que son tan cambiantes y aceleradas como el actual ritmo de vida. De manera tal, que con la puesta en marcha del mencionado ciclo, y su constante repetición, podrá entonces ser garantizado el fortalecimiento de las actuales y futuras capacidades ciberneticas con las que cuente el Ejercito Nacional Colombiano.

7. Conclusiones

Partiendo del diagnostico inicial y los resultados obtenidos a partir de la aplicación del instrumento, se concluye que: Frente al **diagnóstico de las capacidades cibernéticas del Ejército Nacional Colombiano bajo el modelo DOMPILEM**, los resultados arrojados en el instrumento aplicado, permitieron conocer que para el enfoque de capacidades en cuanto a la doctrina que actualemnte se maneja, una parte importante de la plantilla del Ejercito, manifiesta que existen manuales conjuntos por fuerza, sin embargo, que estos no son difundidos, lo que resulta preocupante, dado que el tenerlos pero no conocerlos, es igual que no haber manejado nunca esta información, lo que permite concluir que actualemnte no existe mayor manejo de esta información por parte del cuerpo de defensa nacional.

De igual forma, se concluye que lo anterior ocurre con los planes de proteccion en el area de ciberseguridad, asi como con la existencia de manuales de operaciones ciberneticas, pues la mayoria de las personas consultadas manifesto que estos planes existen, mas no son difundidos entre los participantes, lo que deja inferir que es un conocimiento que no esta siendo aprovechado, siendo ello perjudicial para el logro del objetivo fundamental que es el resguardo y proteccion de la nacion. En cuanto a la existencia de manuales de apoyo cibernetico y acuerdos convenios, un alto porcentaje de encuestados dejo ver que estos no existen, por lo que se puede concluir que es asi, o en su defecto, si existen no son divulgados, lo que en la práctica resulta igualmente perjudicial a la seguridad nacional.

Por otra parte, en torno a la organización, se concluye que actualmente en el Ejercito Nacional Colombiano una procion mediana reconce la existencia de un nuevo

componente militar, sin embargo, esta informacion no es manejada por la mayoría. Con preocupacion se evidencia que solo una parte del Ejercito reconoce la existencia de equipos multidisciplinarios y su accion entreo del mismo, al igual que a los equipos de batalla, de lo que se puede concluir que es necesario hacer cambios en el funcionamiento y divulgacion de la organización de estos equipos en el Ejercito Nacional Colombiano.

Arora bien, respecto del material, se pudo concluir que es necesaria la actualizacion e inversion en cuanto a hardwares y softwares adecuados para el funcionamiento del área de ciberseguridad, ello tomando en cuenta la importancia de este equipamento para que las espectativas de seguridad sean cubiertas, de igual manera, se evidencian falencias en cuanto a la existencia de plataformas compartidas para beneficio del ejercito. Por lo anterior, se deduce que efectivamente las capacidades Ciberneticas del Ejercito Nacioal, se encuentran, al menos en cuestion de equipo tecnologico, en estado crítico.

En el mismo orden de ideas, analizando las capacidades del Ejecito Nacional Colombiano desde el modelo DOMPILEM, se concluye que en lo atinente al personal, en la actualidad no se cuenta con la debida capacidad militar y civil para llevar a cabo acciones de ciberseguridad que resulten efectivas en su propsito, aunque se cuenta con los comandos ciberneticos básicos para ello, y con el completo apoyo de sectores publicos y privados, pero con el agravante de la falta de organización y debida gestion de recursos orientados a mejorar los aspectos antes resaltados.

Continuando con el diagnostico, efectivamente el Ejercito Nacional Colombiano cuenta, hasta ahora, con oficinas, laboratorios y salas apropiadas para la implementacion de actividades de ciberseguridad, no obstante, se evidencia que parte significativa de dichas instalaciones no suelen ser propias, por lo que su utilizacion es limitada, aunque

cuenta con salas de control cibernetico, las mismas no suelen ser de intercambio, sino de uso interno y solo para miembros del mismo, cuando lo ideal seria poder compatir estas actividades con otros cuerpos de seguridad internacional donde se propicie un intercambio de informacion conjunta que potencialice las capacidades de los participantes propios y externos.

Siguiendo con la parte aosicada al liderazgo, se concluye que aun cuando se cuenta con estrategias variadas, expertos y especialistas tecnicos en el area de analsis, el Ejercito Nacional Colombiano no cuenta con un plan de carrera en el area de cibernetica que permita a los participantes crecer y ser aun de mayor utilidad para el mismo. Por su parte, en cuanto al entrenamiento, se concluye que el Ejercito, no maneja sistemas de control industrial que permita evaluar con regularidad de eficacia y correcta conduccion de estos, aunque por el contrario si cuentan con cursos de tallaje internacional, importantes para su aprendizaje academico, que puede ser optimizado llevado a la practica, siendo que en materia de mantenimiento tanto de instalaciones como del equipo disponible, este si se lleva a cabo de forma efectiva.

Continuando con las conclusiones para el presente estudio, tenemos para las etapas de madurez de la capacidad cibernética aplicada por el Ejército Nacional Colombiano, se pudo inferir que tomando en cuenta las falencias encontradas en el objetivo anterior, en la actualidad la etapa de madurez en la que se encuentra el Ejercito puede ser estimada como una etapa formativa, donde ciertas áreas o fases ya se encuentran en desarrollo, mientras que otras apenas serán formuladas, sin embargo, las áreas de desarrollo se encuentran desorganizadas o mal definidas, como es el caso de el establecimiento y aplicación de manuales formales de apoyo cibernetico.

De igual forma, en esta estapa de madurez formativa, se encuentran las areas de personal y reconocimiento de la existencia de un nuevo componente militar, espacios

adecuados para la eficiente capacitacion y la actualizacion de quipos tecnologicos, asi como tambien la divulgacion del material intelectual sobre ciberseguridad. Sin embargo, al respecto se concluye además que, es probable que con los ajustes requeridos pronto se alcance a pasar de esta etapa formativa a la etapa consolidada, donde ya muchos aspectos se encuentren plenamente desarrollados y en pleno funcionamiento, sin embargo, aun se deben ajustar detalles referidos a la importncia en la concesión de recursos para la debida actualizacion de cada componente del DOMPILEM.

Por ultimo, se plantean las siguientes recomendaciones para la identificación y fortalecimiento de las capacidades cibernéticas del Ejército Nacional Colombiano, significando el Ciberespacio un recien nacido escenario de Guerra, el Ejército Nacional necesita estar preparado frente al mismo, sobre todo considerando que este acarrea diversas problemáticas como son los ataques cibernéticos anonimos,asi como la atribución intencionada de ellos, con un gran nivel de dificultad para constatar que así sea y un aspecto aún más complicado la oportuna y clara definición de las fronteras geográficas desde donde estos ataques son ejecutados.

En este sentido, ha sido evidente que el Estado colombiano, consciente de la lo complicado que es el escenario del Ciberespacio, y considerando la digitalización, sumada a la globalización, que aumenta de manera desmesurada el uso de las tecnologías emergentes, la expansion y rapida divulgación de la información y el mundo de las comunicaciones, que en la actualidad se condideran tan necesaria para el desarrollo de las actividades diarias, intenta adaptarse a toda velocidd a este virgen escenario de guerra con el firme proposito de disponer de las herramientas y conocimiento optimos frente a posibles confrontaciones que atenten contra la soberanía, independencia, integridad y del orden constitucional.

En este sentido y en conconancia con lo explorado en la investigacion previa, se recomienda:

En primer lugar, la configuración de procesos enfocados a la gestión de incidentes cibernéticos, con el objetivo de generar mejores escenarios frente a la toma de decisiones y el establecimiento de rutas tendientes a la priorización, indagación y mejor capacidad de respuesta frente a los incidentes detectados, de igual forma, gestar la produción de una retroalimentación activa basada en los conocimientos e instrucccion recibidas, que conduzcan a las unidades correspondientes a la evolucion positiva frente a las necesidades actuales en torno a la ciberseguridad nacional.

Aunado a ello, se recomienda establecer parametros reales que permitan determinar en una escala de riesgos, los ataques que realemente signifiquen un peligro potencial, asi como la frecuencia de los mismos y que ello permita disgnosticar las áreas que en la actualidad y en el futuro puedan encontrarse en situacion vulnerable, dependiendo de los avances tecnologicos dentro y fuera del territorio, con el porpósito de poder adelantar programas de investigacion permanente, capacitaciones continuas y prácticas de campo (ciberespacio), que faciliten la prevencion y capacidad de reaccion ante estos ataques.

Por otra parte, es necesario evaluar las capacidades actuales de las que dispone el Ejercito Nacional Colombiano a nivel aptitudinal entre el personal, depurar las unidades al frente de estas actividades, asi como tambien, hacer un balance de equipos e instalaciones que se encuentren acorde a las necesidades tecnologicas que se requieren para optimizar la seguridad cibernetica actual, procurando que se avance con rapidez y eficacia en las etapas de madurez planteadas anteriormente.

En este sentido, es primordial tomar en cuenta aspectos de la norma ISO/IEC 27035 donde se enmarcan técnicas de seguridad y Gestión de incidentes de seguridad

de la información, donde claramente se proporcionan las pautas referentes a la planificación y preparación para la respuesta frente a incidentes, estas directrices se encuentran fundamentadas principalmente en la fase de planificación y preparación, y en la fase de Lecciones aprendidas, todas del modelo de Fases de gestión de incidentes de seguridad de la información. Sin embargo, para que todo lo anterior se pueda gestar de forma efectiva y genere los resultados esperados, es necesario que se realice una importante inversion en infraestructura, equipamento y personal de inducción, que posibiliten el fortalecimiento de las capacidades cibernéticas del Ejército Nacional Colombiano.

8. Recomendaciones

Este modelo derivado del análisis de las capacidades evaludas debería ser presentado y desplegado a la Brigada de interoperabilidad de comunicaciones, computación y ciberdefensa del Ejercito Nacional y de esta manera se pueda avanzar en el cierre de las brechas identificadas en términos de GAP´s para elevar el nivel de madurez de dichas capacidades encontradas.

Replicar este análisis a otras divisiones y fuerzas toda vez que la relación entre unidades, fuerzas o divisiones es simbiótica, lo que quiere decir que al elevar o mantener estándares altos de desempeño en diversas fuerzas, el efecto sobre el conjunto de acciones y unidades será mayor.

Este tipo de estudios debería realizarse de manera longitudinal, con lo cual se recomienda que se realice nuevamente en seis meses, de modo tal que se pueda evidenciar el avance del despliegue de mejoras y; también, el surgimiento o desarrollo de otras capacidades con ausencia de fortaleza.

9. Referencias

Acosta, O. (2012). *Capacidades para la Defensa en el Espacio cibernético*. Monografías del Centro Superior de Estudios de la Defensa Nacional (CESEDEN). Nro. 126. Publicaciones Oficiales del Ministerio de Defensa en España.

Agrafiotis, L., Nagyfejeo, E., Bada, M., y Kastelic, A. (2020). *Revisión de capacidades de Ciberseguridad. Secretaría del Comité Interamericano contra el Terrorismo de la Organización de los Estados Americanos (CICTE/OEA)*. Brasil.

Báez, J. y Pérez, I. (2009). *Metodología de la investigación*. 5ta Edición. Madrid, ESIC.

Bernal, C. (2010). *Metodología de la Investigación, administración, economía, humanidades y ciencias sociales*. 3ra Edición. Editorial Pearson Educación. Colombia.

Camacho, J. (2016). *Evolución de la Ciberdefensa y la Seguridad de la Información en Colombia*. [Trabajo de especialización, Universidad Militar Nueva Granada]

Camelo, L. (2015). ¿Qué tan preparado está el Gobierno contra ataques cibernéticos? *Revista Semana. Bogotá: Colombia* 4, (1), pp. 1. Recuperado de: http://www.semana.com/tecnologia/articulo/que-tan-preparado-esta-el-gobierno-contraataques-ciberneticos/431602-3

Comando Conjunto Cibernético (2017). *Plan Nacional de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia*. https://bit.ly/2UIsMYy

Comando General de las Fuerzas Militares COGFM. (2018). *Manual Fundamental Conjunto MFC 1.0.* Bogotá, Colombia.

Consejo Nacional de Política Económica y Social, de Colombia República de Planeación Departamento Nacional. (2011). *Lineamientos de política para ciberseguridad y ciberdefensa CONPES 3701-2011*. Internet, 43

Cujabante, X., Bahamón, M., Prieto, J., y Quiroga, J. (2020). Ciberseguridad y ciberdefensa en Colombia: un posible modelo a seguir en las relaciones cívico-militares. *Revista Científica General José María Córdova*, 18(30), pp. 357-377. Recuperado de; http://dx.doi.org/10.21830/19006586.588

Decreto 338 (*marzo 2022*). *Titulo 21 a la parte2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones*. Bogotá, Colombia.

Departamento Nacional de Planeación. (2020). *Política Nacional de Confianza y Seguridad Digital*. Documento CONPES 3995, 51.

Ejército de Colombia. EJC. (2017). *Manual Fundamental Doctrina. Centro de Doctrina del Ejército - CEDOE*, Ed. Vol. 1. Bogotá: Imprenta Militar del Ejército Restricciones. Recuperado de: www.cedoe.mil.co

Global Cyber Security Capacity Centre (2016). *Modelo de Madurez de Capacidades de Ciberseguridad para Naciones (CMM).* University of Oxford. https://www.senado.cl/appsenado/index.php?mo=transparencia&ac=doctoInformeAsesoria&id=7840

Gómez C. y Luciano, M., y Franco, C. (2020). *Análisis y estrategia de implementación de un marco de trabajo de ciberseguridad para la unidad de Ciberdefensa del Ejército Nacional*. Universidad de los Andes.

Hernández, R.; Fernández, C.; y Baptista, P. (2014). *Metodología de la Investigación*. Sexta Edición. Mc Graw-Hill Interamericana Editores, S.A. DE C.V. México.

Hudson Analytix (2017). *Glosario sobre Términos de Seguridad Cibernética para la Comisión Interamericana de Puertos Organización de los Estados Americanos*. New Jersey, Estados Unidos de América.

Ministerio de Defensa Nacional. Resolución 7144 de 2018. (*Octubre 5*). Modelo de Planeación y Desarrollo de Capacidades de la Fuerza Pública. Diario Oficial No. 50.737 de 5 de octubre de 2018. Bogotá, Colombia.

Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. (2014). *Agenda estratégica de innovación: Ciberseguridad. Plan Vive digital*. Recuperado de: https://xdoc.mx/documents/agenda-estrategica-de-innovacion-ciberseguridad-5dfd2bf1b0288

Nowersztern, A., Kagelmacher, D., Barrett, K., y Ramírez, R. (2020). *Ciberseguridad Riesgos, Avances y el camino a seguir en América Latina y el Caribe. Reporte Ciberseguridad 2020.* Banco Interamericano de Desarrollo (BID) y Organización de los Estados Americanos (OEA). https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe

Peralta, O (2015). *Ciberseguridad: nuevo enfoque de las fuerzas militares de Colombia*. [Trabajo de especialización, Universidad Militar Nueva Granada]

Realpe, M., y J. Cano (2020). *Amenazas Cibernéticas a la Seguridad y Defensa Nacional. Reflexiones y perspectivas en Colombia*. Recuperado de: https://doi.org/10.12804/si9789587844337.10

Recomendación UIT–T X.1205 (2008). *Serie x: Redes de Datos, Comunicaciones de Sistemas Abiertos y Seguridad.* Unión Internacional de Telecomunicaciones.

Trama, G., y Vergara, E., (2017). *Operaciones militares cibernéticas: planeamiento y ejecución en el nivel operacional.* 1a ed. Buenos Aires: Escuela Superior de Guerra Conjunta de las Fuerzas Armadas.

Urrutia, F., Treppel, A., Daniell, A., y South, M. (2019). *Ciberseguridad Marco NIST. Un abordaje integral de la Ciberseguridad.* Edición 5. Organización de Estados Americanos (OEA) y AWS. https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf

US Army TRADOC Pamphlet 525-7-8 (2010). *Plan de capacidad conceptual del Ejército de EE. UU., para operaciones en el ciberespacio 2016-2028*. Recuperado de: https://irp.fas.org/doddir/army/pam525-7-8.pdf

Vargas, R., Recalde, L., y Reyes, R., (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: Modelo ecuatoriano de gobernanza en ciberdefensa. *Revista Latinoamericana de Estudios de Seguridad URVIO, 20*, pp. 31-45. DOI: http://dx.doi.org/10.17141/urvio.20.2017.2571

Villanueva, J. (2020). *La ciberdefensa en Colombia*. Universidad Piloto de Colombia. Villanueva.

10. Anexos

ENCUESTA PARA REALIZAR EL DIAGNOSTICO DOMPILEM
Análisis de las Capacidades Cibernéticas del Ejército Nacional

EXPERTO No.	
Nombre	
Cargo	
Experiencia	
Formación	

Diagnóstico de las capacidades cibernéticas del Ejército Nacional Colombiano bajo el modelo DOMPILEM

DOMPILEM	0 NO EXISTEN	1 EXISTEN, PERO NO SON DIFUNDIDOS	2 EXISTEN SON DIFUNDIDOS, PERO NO DESPLEGADOS	3 EXISTEN SON DIFUNDIDOS E IMPLEMENTADOS POR UNA PARTE DE LAS UNIDADES	4 EXISTEN SON DIFUNDIDOS E IMPLEMENTADOS POR TODA LA FUERZA
DOCTRINA					
Manuales conjuntos y por fuerza					
Planes de protección					
Manuales de operaciones cibernéticas					
Manuales de apoyo cibernético					
Acuerdos convenios					
ORGANIZACIÓN					
Un nuevo componente militar					
Equipos interdisciplinarios					
Equipos de batalla					
Conformación ligas					
Nacionales internacionales					
MATERIAL					
Hardware y Software					
Plataformas compartidas					
Equipo de combate cibernético					
Especializado alto nivel					
PERSONAL					
Militar y Civil					
Comandos cibernéticos					
Sector político y privado					
Nacional e internacional					
INSTALACIONES					
Oficinas laboratorios salas					
Propias y de terceros					
Sala mando y control cibernético					
Salas de intercambio cibernético					
Propia y de terceros					
LIDERAZGO					
Estrategias, expertos, especialistas técnicos					
Expertos en activos estratégicos sectoriales					
Plan de carrera cibernética					
Expertos cibernéticos					
Internacionalistas					
ENTRENAMIENTO					
Persistente					
Sistemas control industrial					
Simulación olimpiadas cibernéticas					
Entrenamiento interinstitucional					
Cursos internacionales					
MANTENIMIENTO					
Plataformas cibernéticas					
Sistemas de defensa cibernética					
Plataformas de operaciones cibernéticas					
Sistemas de apoyo					
Sistemas de intercambio					