Acciones de mejora en seguridad digital para que las Fuerzas Militares de Colombia garanticen la protección del derecho a la información de los ciudadanos

MY. JOHNNATAN AMAURI GIL SALCEDO

Artículo para optar al título profesional:

Magister en Derechos Humanos y Derecho Internacional de los Conflictos Armados

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia
2024

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

DATOS GENERALES		
Nombre del estudiante	**:**	MY. Johnnatan Amauri Gil Salcedo
Identificación	**:**	1057570583
Programa académico	**:**	Maestría en Derechos Humanos y Derecho Internacional de los Conflictos Armados
Tutor metodológico	**:**	Garay Acevedo Claudia Patricia
Tutor temático	**:**	MY. (R) Alfonso Rodríguez Moreno
Fecha de entrega	**:**	17 de mayo de 2024
Extensión	**:**	6.000 – 8.000 palabras

DECLARACIÓN DE ORIGINALIDAD Y CESIÓN DE DERECHOS

El autor declara que este artículo fue escrito de acuerdo con la normatividad de la Escuela Superior de Guerra "General Rafael Reyes Prieto" (ESDEG) y no existe ningún potencial conflicto de interés relacionado con este. Las posturas y aseveraciones presentadas son resultado de un ejercicio académico e investigativo que no representan la posición oficial ni institucional de la ESDEG, las Fuerzas Militares de Colombia o el Ministerio de Defensa Nacional.

Este artículo es enteramente mi propio trabajo y no ha sido presentado para la obtención de un título en esta u otra Institución de Educación Superior. Se han referenciado todos los trabajos y puntos de vista de otros autores, así como los datos de otras fuentes utilizadas. No se emplearon herramientas de generación de contenido por Inteligencia Artificial para su elaboración.

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

Acciones de mejora en seguridad digital para que las Fuerzas Militares de Colombia garanticen la protección del derecho a la información de los ciudadanos

Actions to improve digital security so that the Colombian Military Forces guarantee the protection of citizens' right to information

Johnnatan Amauri Gil Salcedo[1]

Escuela Superior de Guerra "General Rafael Reyes Prieto"

[1] Mayor del Ejército Nacional de Colombia. Candidato a Magíster en Derechos Humanos y Derecho Internacional de los Conflictos Armados, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Profesional en Ciencias Militares, Escuela Militar de Cadetes "General José María Córdova", Colombia. Contacto: johnnatan.gil@esdeg.edu.co

Resumen: El acelerado desarrollo de las tecnologías en las últimas décadas ha representado un reto para las naciones en temas de seguridad y protección de la información de los ciudadanos, puesto que han surgido nuevas problemáticas en relación al uso de estas, que se transforman en las amenazas para la seguridad nacional y hasta para la economía y protección del ciudadano común. Se conoce que este no es un tema aislado de los países, ya que todos se encuentran en riesgo de vulnerabilidad de la información y ataques cibernéticos, situación que ha llevado a las naciones a crear políticas públicas y estrategias de ciberseguridad, para mitigar y hacer frente a las distintas amenazas que se pueden presentar para los estados y su ciudadanía. El objetivo de la presente investigación es proponer acciones de mejora en seguridad digital para que las Fuerzas Militares de Colombia garanticen el derecho de información a los ciudadanos, con base en la descripción de los antecedentes históricos y el conocimiento de las estrategias implementadas a nivel nacional e internacional en seguridad de la información, por medio de una metodología cualitativa y con enfoque descriptivo que permita conocer las estrategias actuales y proponer las acciones que mejoran estos procesos de defensa ciudadana.

Palabras clave: seguridad digital, derecho a la información, Fuerzas Militares de Colombia, derechos humanos.

Abstract: The accelerated development of technologies in recent decades has represented a challenge for nations in terms of security and protection of citizens' information, since new problems have arisen in relation to their use, which become threats to national security and even for the economy and protection of the common citizen. It is known that this is not an issue isolated to countries, since all are at risk of information vulnerability and cyber attacks, a situation that has led nations to create public policies and cybersecurity strategies, to mitigate and address to the different threats that may arise for states and their citizens. The objective of this research is to propose actions to improve digital

security so that the Colombian Military Forces guarantee the right to information to citizens, based on the description of the historical background and knowledge of the strategies implemented at the national and national level. international in information security, through a qualitative methodology and with a descriptive approach that allows us to know the current strategies and propose actions that improve these citizen defense processes.

Keywords: digital security, right to information, Colombian Military Forces, human rights.

[T1] Introducción

Las Fuerzas Militares de Colombia están conformadas por el Ejército Nacional, la Armada Nacional y la Fuerza Aérea Colombiana, su objetivo es la Defensa de la soberanía, la independencia y el Orden Constitucional (Corte Constitucional, 1991, art. 217), en ese proceso de Defensa se han implementado avances tecnológicos, por ejemplo: 1. Imágenes de multimisión que funcionan con cámaras de cuadro térmico, 2. Sistemas de vigilancia multisensores infrarrojos, 3. Vehículos aéreos no tripulados, y en la actualidad se está avanzando en la implementación de la 4. Inteligencia Artificial (Espitia et al, 2020).

Los avances tecnológicos también representan riesgos para la seguridad digital, es decir, que genera vulneración en la protección y control de comunicación, información, datos, afectando la disponibilidad, integridad y confidencialidad (Hernández, 2020). Al respecto se conoce que en el año 2022 los hackers conocidos como "Guacamaya"[2] realizaron una posible filtración de documentos con datos sensibles de las Fuerzas Militares de Colombia (El Colombiano, 2022). De igual manera, Mozo y Ardila (2022) indican que la ciberdelincuencia es una amenaza silenciosa y cada vez más especializada que puede conllevar a ataques hacia el Ejército de Colombia, existen riesgos de **phishing[3], ingeniería**

[2] Organización internacional de hackers que publica informes anónimos y documentos filtrados de los gobiernos, fuerzas armadas y empresas

[3] Tipo de ciberataque que engaña a las personas para que les suministren datos personales, esto lo logran a través de correos electrónicos, mensajes de texto, llamadas telefónicas, sitios web.

social[4], malware[5], ransomware[6], denegación de servicios [7]y filtración de datos[8], entre otros.

Para entender la importancia de realizar este estudio es relevante conocer que la ciberdelincuencia no es una problemática reciente, como parte del origen en Colombia se menciona el grupo de Anonymous que inició en el país el 11 de abril de 2011, reconocido como un colectivo de hackers internacionales que logró tumbar por más de ocho horas las páginas web del Ministerio del Interior, el Ministerio de Defensa, la Presidencia de la República y el sitio oficial de Juan Manuel Santos, en ese entonces Presidente de Colombia. En cuanto al paro nacional realizado en ese mismo año, este grupo brindó apoyo a través de sus actos para tumbar las páginas del Ejército Nacional de Colombia, el Senado de la República, la Policía Nacional y cuentas personales de algunos miembros del Gobierno Nacional. El mensaje que dejaba este grupo era que en el país había llegado una guerra global por la libertad de la información en internet (AS Colombia, 2021).

[4] Técnicas de manipulación que emplean los ciberdelincuentes para acceder a información privada de los ciudadanos. Para lograrlo, se basan en la forma en que las personas piensas y se comportan, aprovechan los errores humanos.

[5] Es un software malicioso, creado intencionalmente para afectar los sistemas informáticos y a los usuarios. Casi todos los ciberataques modernos hacen uso de algún tipo de malware.

[6] Es un tipo de malware que genera riesgo para las personas y sus dispositivos por los actos extorsivos, se debe pagar un rescate para poder usar el dispositivo.

[7] Intento malicioso de generar tráfico a una propiedad web con la intención de interrumpir el correcto funcionamiento y evitar que esté disponible para los usuarios.

[8] Corresponde a cualquier incidente de seguridad que conlleva a un acceso no autorizado a información confidencial por parte de personas malintencionadas.

La presencia de Anonymous en el país se intensificaba con las amenazas a la seguridad en instituciones bancarias y financieras a cargo de delincuentes informáticos internos y externos que buscan apropiarse de la información confidencial de los usuarios, estos hechos evidenciaban la importancia de la seguridad informática y las debilidades que la hacían más vulnerable, generando conciencia sobre la ciberseguridad (Orozco, 2011). En ese mismo año, 14 de julio de 2011 se dio origen al CONPES 3701 de 2011 para crear la Política para Ciberseguridad y Ciberdefensa en Colombia.

A nivel internacional, la problemática de la ciberdelincuencia ha estado presentado desde años atrás, en el 2010 fue popular los wikileaks una página creada para filtrar más de 799.000 documentos del Ejército de Estados Unidos de América sobre las guerras de Afganistán e Irak, entre otros materiales para dar a conocer escándalos del gobierno (Miranda, 2019). En el 2011 el Fondo Monetario Internacional fue víctima de un ataque cibernético en el que se buscaba instalar un software que funcionaba como espía digital en los sistemas para conocer datos sensibles sobre la economía de diversos países; en abril del mismo año, la compañía Sony se vio obligada a desconectar de su red PlayStation Network debido a que por medio de un ataque lograron robarle información confidencial de más de 100 millones de cuentas (BBC, 2011).

Los anteriores hechos descritos, demuestran que los ataques a la seguridad digital de las organizaciones del país en vez de reducirse, se han venido aumentando gracias al nivel de especialización, diversificación, actualización e innovación en las técnicas de ataque haciendo uso de las oportunidades tecnológicas (Vigoya, 2024).

Esta realidad ha impulsado la necesidad de fortalecer las acciones para prevenir y gestionar la infraestructura tecnológica del sector Defensa del país, que ayuden a prevenir incidentes cibernéticos a través del cumplimiento de estándares de tecnología mundial (Presidencia de la República, 2023), esta prioridad de formación está justificada precisamente en la ausencia de competencias en Seguridad Digital en el personal de las Fuerzas Militares de Colombia y la necesidad de una constante actualización de información según los avances de la tecnología que permita garantizar los Derechos Humanos de los Colombianos, y aportar al cumplimiento de las funciones para la Defensa Nacional (Fuerzas Militares de Colombia, 2024).

El Estado colombiano ha sido consciente del nivel de complejidad del Ciberespacio[9] y con respecto al proceso de digitalización y globalización mundial, en el cual se tiene uso intensivo de las tecnologías de la información y las comunicaciones, espacio que se presta para la presencia de amenazas y delitos, como el robo de la información y acceso indebido a ella, por lo tanto, fue necesario construir una estrategia de Ciberdefensa para la protección de las actividades diarias y la información de los ciudadanos, en este caso, el Ejército Nacional se ha adaptado de forma rápida al nuevo contexto con el propósito de estar preparado ante las posibles confrontaciones que puedan afectar la Soberanía, la Independencia, la Integridad del Territorio Colombiano y el Orden Constitucional (Cáceres, 2017).

[9] Espacio virtual que permite a las personas emplear software para acceder y compartir datos a través de correos electrónicos, páginas web, aplicaciones, entre otros.

Los procesos y estrategias de Ciberdefensa en Colombia iniciaron con las Fuerzas Militares de Colombia en el año 2011, con el establecimiento del documento CONPES[10] 3701 de los "Lineamientos de política para la Ciberseguridad y Ciberdefensa", con la creación de una comisión intersectorial que fue conformada por el COLCERT[11] de Colombia, el Centro Cibernético Policial (CCP)[12] y el Comando Conjunto Cibernético (CCOCI)[13] de las Fuerzas Militares de Colombia, que se encargan de liderar la Defensa y la Seguridad digital del país, con el fin de proteger la legitimidad de la información (Gómez et al. 2020).

Con el enfoque del CONPES 3701, el Comando Conjunto Cibernético de las Fuerzas Militares de Colombia se creó la unidad de Ciberdefensa del Ejército Nacional, con la inclusión de las Tecnologías de la Información y las Comunicaciones (TIC), proporcionando un gran avance de las TIC enfocadas en la protección de los sistemas de información del país frente a las potenciales y futuras amenazas cibernéticas; En Colombia existe un marco normativo para establecer disposiciones para establecer disposiciones en relación con los delitos informáticos (Gómez et al. 2020).

[10] Consejo Nacional de Política Económica y Social, la máxima autoridad nacional de asesorías en planeación al Gobierno, reglamentada en la Ley 19 de 1958.

[11] Grupo de Respuesta a Emergencias Cibernéticas de Colombia reglamentado en la Resolución 473 del 17 de febrero de 2022, para coordinar la prevención, mitigación, gestión y respuesta a los incidentes en seguridad digital en el sector público y privado.

[12] Centro Cibernético Policial, plataforma virtual de la Policía Nacional de Colombia para prevenir la comisión de delitos por internet, encargado de la seguridad ciudadana en el ciberespacio.

[13] Comando Conjunto Cibernético, responsable de la defensa del país en el ciberespacio y de garantizar la protección de las infraestructuras cibernéticas a través de operaciones militares en el ciberespacio

En el país se han creado en conjunto con el Gobierno Nacional y las Fuerzas Armadas de Colombia, las entidades especializadas como la Unidad de Servicios de Información y Análisis Financiero (UIAF)[14] y el Grupo de Delitos Informáticos de la Policía Nacional, para ofrecer una mejor coordinación y adelantar acciones de investigación y sanciones de delitos cibernéticos, todo con el apoyo de tecnologías de seguridad para la protección de las infraestructuras tecnológicas militares y donde el Ejército Nacional puede detectar y evidenciar los posibles ataques cibernéticos que puedan vulnerar la integridad, la disponibilidad y la confidencialidad de la información (UIAF, 2022).

[T1] Metodología

El estudio se realiza bajo la metodología de investigación cualitativa, la cual se utiliza para comprender y explicar el comportamiento, los elementos y las características de las personas o de un grupo objetivo, para Hernández Sampieri la investigación cualitativa modela un proceso inductivo que se contextualiza en un ambiente natural y con la recolección de datos es posible establecer la relación entre los participantes de la investigación, encontrando sus experiencias y las ideologías. En este enfoque las variables no están definidas con intensión de ser manipuladas y permite el análisis de una realidad subjetiva (Hernández Sampieri, 2014).

Además, la investigación cualitativa no tiene principios estadísticos, se caracteriza por la no conceptualización de las preguntas de investigación y por el no uso de números para

[14] Unidad de Información y Análisis Financiero que tiene la capacidad de intervenir al Estado para identificar acciones relacionadas con el lavado de activos, además de contribuir a la prevención.

obtener las conclusiones de los datos conseguidos y permite la dispersión de la información. Con el enfoque cualitativo hay una gran variedad de ideas y de interpretaciones que permiten el enriquecimiento de las investigaciones y sus contenidos, para una mejor comprensión de los fenómenos sociales que son más complejos y permite al investigador ir más allá de la medición de las variables involucradas (Hernández Sampieri, 2014).

El enfoque de la investigación es descriptivo-propositivo, que tiene como objetivo la descripción de las variables, este tipo de enfoque de la investigación le permite al investigador describir los fenómenos, las situaciones, contextos y diferentes eventos del tema de estudio en cuestión. Estos estudios buscan especificar cuáles son las propiedades, las características y los perfiles de las personas participantes en la investigación, ofreciendo una información detallada de cada una de las variables y elementos de estudio (Hernández Sampieri et al, 2006).

En cuanto a la técnica de estudio es la revisión de la literatura, la cual permite al investigador detectar, obtener y consultar la bibliografía y otro tipo de material científico que puede resultar útil para los propósitos del estudio, asimismo, permite extraer y recopilar la información que es relevante y necesaria, además, que añade información precisa y diferentes opiniones al problema actual de investigación. La revisión de bibliografía es selectiva, se revisa la información de cientos de artículos de revistas, se consultan libros y otros materiales que están dentro de las diferentes áreas del conocimiento (Hernández Sampieri, 1991).

[T1] Desarrollo del objetivo

1. Descripción del contexto histórico de la seguridad digital de las Fuerzas Militares de Colombia

La acelerada innovación de las herramientas digitales y los medios electrónicos, ha llevado al aumento del acceso a internet, generando oportunidades en el avance y desarrollo de las sociedades como unos de los resultados de la globalización. En el campo militar la situación también ha llevado a incorporar estrategias y nuevos adelantos tecnológicos para asegurar la seguridad y la información de las sociedades, como respuesta a las amenazas de la seguridad nacional (ONU, 2023).

En el caso particular de Colombia, este ha sido uno de los primeros países de Latinoamérica que se ha interesado por incorporar lineamientos de política pública por medio del CONPES 3701 del año 2011. Este documento surge como una respuesta ante la frecuencia de los ciberataques que han aumentado, y cada vez son más sofisticados y difíciles de descifrar, por lo tanto, el país ha implementado medidas de seguridad más eficientes y se prepara constantemente para afrontar las amenazas que alteren la integridad de los sistemas digitales y la información (Cáceres, 2017).

Adicionalmente, se conoce que el CONPES 3701 de 2011 es un documento que resalta la necesidad del trabajo colectivo con el compromiso del Gobierno Nacional que ayude a garantizar la seguridad de la información en el contexto nacional, por lo que deberá cumplirse con las normar técnicas, y lo establecido en estándares tanto nacionales como internacionales, además de acatar las iniciativas propuestas para la protección de

infraestructura crítica y ciberseguridad. En cuanto a la normativa, se conoce: 1. Ley 527 de 1999, 2. Ley 599 de 2000, 3. Ley 962 de 2005, 4. Ley 1150 de 2007, 5. Ley 1273 de 2009, 6. Ley 1341 de 2009, 7. Resolución de la Comisión de Regulación de Comunicaciones 2258 de 2009, 8. Circular 052 de 2007 (Departamento Nacional de Planeación, 2011).

La seguridad multidimensional y cibernética se ha adoptado por los países del hemisferio sur, principalmente desde la Declaración de Seguridad de las Américas en el año 2003, donde el contexto de la seguridad se enfoca en los aspectos económicos, políticos, sociales y ambientales, donde se identifican amenazas no tradicionales, como son los casos de delincuencia transnacional, el tráfico de drogas y las armas, el lavado de dinero y los ataques cibernéticos, siendo necesario abordar estas amenazas de una manera integral y cooperativa con todos los territorios (Chillier & Freeman, 2005).

Las Fuerzas Militares de Colombia han sido las instituciones encargadas de garantizar la protección de la soberanía y su territorio, así mismo de la población, velando por el cumplimiento de su misión Constitucional que fue consagrada en el Artículo 217 de la Constitución Política (1991), para defender la independencia y la integridad del territorio nacional. De esta manera, las Fuerzas Militares de Colombia han tenido la responsabilidad constitucional de mantener la seguridad y la protección en el ciberespacio, que es uno de los escenarios que se ha convertido en un nuevo campo de conflicto (Ramírez, 2003).

Desde comienzos del siglo XX, se han liberado guerras y batallas por los espacios de tierra y mar, pero es pasando los XX y XIX, que los avances de la tecnología en las Fuerzas Militares de Colombia con tres dominios (aire, espacio y ciberespacio), cambiaron la lógica del planteamiento y las distintas operaciones estarían relacionadas con la Seguridad y la

Defensa de las naciones. Allí comienza el papel importante de las instituciones militares y su responsabilidad en la seguridad global, bajo las interconexiones a nivel mundial y la falta de barreras físicas.

Desde el siglo XXI se tiene el reconocimiento de escenarios estratégicos donde comienzan los riesgos y amenazas sobre las naciones, hay desequilibrio y está en juego la estabilidad y la seguridad de los territorios, surgiendo ataques a través del ciberespacio. Los ataques cibernéticos han sido con intencionalidad económica y política, que genera consecuencias negativas y diversos conflictos entre los países, al mismo tiempo que luchan por el poder y la posesión de tierras, mares, aire y espacios (López, 2022).

A nivel nacional, el Ministerio de Defensa publica la Política de Seguridad de la Información[15] para el año 2014, con numerosas iniciativas para mejorar la seguridad de la información, evaluando las capacidades que están relacionadas con el ciberespacio y las que las Fuerzas Armadas de Colombia deben tener junto con concepto de Estrategia Militar, desde allí, se concibe un nuevo escenario estratégico y la ciberseguridad se tiene en cuenta para comenzar a provisionar este campo de acción. En la política se definen los organismos de operación, como la Unidad de Gestión General, la Dirección de Justicia Penal Militar y las Fuerzas Militares de Colombia, junto con la normatividad sobre contrataciones, régimen disciplinario y acceso y uso de las herramientas tecnológicas (Cáceres, 2017).

[15] Documento que integra las directrices y lineamientos generales para proteger los activos de información y garantizar la seguridad de los datos en la gestión de procesos internos

Para el año 2016 en Colombia, el Ministerio de Tecnologías de la Información y las Comunicaciones se une al área de seguridad de la información de las Fuerza Militares de Colombia, donde se incluyen temas de investigación y apoyo en desarrollo e innovación para un mayor conocimiento y adelanto en los temas de ataques cibernéticos, elaborando un sin número de tácticas especializadas para combatir los problemas y las amenazas a la información del territorio. Desde este momento han sido más evidentes las acciones que se adelantan en los sistemas seguros y resistentes, como la mejora de los estándares y los protocolos para dar protección a los ciberataques y disminuir los puntos vulnerables de los territorios (Gómez et al, 2020).

Se han generado ajustes a los marcos normativos y reglamentarios para crear una doctrina única en el control de los ataques del ciberespacio para mejor control por parte de las Fuerzas Militares de Colombia, creando un mayor fomento en la educación y experticia en los temas de Ciberseguridad y Ciberdefensa, como estrategias de entrenamiento que acreditan y aseguran los esfuerzos de las instituciones para proteger la información de los ciudadanos (Gómez et al, 2020).

Como parte de los cambios normativos, en el año 2016 el Departamento Nacional de Planeación generó un nuevo documento CONPES 3854 llamado "Política Nacional de Seguridad Digital" con el objetivo de fortalecer la seguridad digital del país, y darle continuidad a la estrategia de Ciberdefensa según lo establecido en el CONPES 3701 y CONPES 3995 que corresponde a la "Política Nacional de Confianza y Seguridad Digital" (Departamento Nacional de Planeación, 2020).

Complementario a lo anterior el CONPES 3854 ha buscado lograr el fortalecimiento a través de la integración de las diferentes partes interesadas, que en conjunto aporten a la identificación, gestión, tratamiento y mitigación de los riesgos de seguridad digital presentes en las actividades socioeconómicas que hacen parte del entorno digital, siendo un proceso caracterizado por la solidaridad, colaboración y asistencia. Estas acciones son valoradas también por sus aportes hacia el desarrollo económico y social de la nación. Otro de los cambios significativos es la gestión de riesgos asociados a la seguridad digital por lo que se propone un tratamiento dividido en las etapas de tomar, reducir (medidas de seguridad, innovación y preparación), transferir y evitar (Departamento Nacional de Planeación, 2016).

> Aunque estas políticas permitieron en su momento que el país avanzara en materia de seguridad digital, cabe anotar que no se logró un avance considerable en cuestiones de confianza digital. Esto debido a que no se involucró en mayor medida a todas las múltiples partes interesadas relacionadas con la seguridad digital más allá del Gobierno Nacional, con el fin de generar confianza digital (Departamento Nacional de Planeación, 2020, p.9).

La ejecución de la política de CONPES 3854 entre 2016 a 2019 implicó una inversión de $85.070 millones de pesos, siendo los principales participantes el Ministerio de Tecnologías de la Información y las Comunicaciones, el Ministerio de Defensa Nacional, la Dirección Nacional de Inteligencia y el Departamento Nacional de Planeación. También se estimó que la puesta en marcha de la política nacional de seguridad digital para el año 2020

generó impactos positivos a nivel económico en temas de empleo y crecimiento del Producto Interno Bruto[16] (Departamento Nacional de Planeación, 2016).

Para el 2022 por medio de la Resolución 473[17] del Ministerio de Tecnologías de la Información y las Comunicaciones, se crea el Grupo Interno de Trabajo de Respuesta a Emergencias Cibernéticas de Colombia - COLCERT. Grupo que se ha fortalecido en capacidades y fortaleza de la Fuerza Pública. Así la defensa pasa a estar a cargo del Comando Conjunto Cibernético y es apoyado por el Ejército Nacional, Armada Nacional y la Fuerza Aérea Colombiana, y la seguridad de la Información en el contexto ciudadano queda a cargo del Centro Cibernético Policial manejado por la Policía Nacional (Santos, 2022).

El 25 de abril de 2023, el ministro de Defensa, Iván Velázquez, establece nuevos lineamientos sobre la Política de Seguridad y la Defensa, ofreciendo "Garantías para la vida y la paz", estos lineamientos y políticas han establecido los objetivos y los principios para guiar las acciones y las estrategias de la seguridad del país. Y dentro de estos objetivos se incluyen los elementos para la protección de la vida, la integridad del territorio nacional y los ciudadanos. Esta política aborda específicamente las capacidades defensivas y ofensivas de las Fuerzas Militares de Colombia en el ciberespacio, y en los últimos años, haciendo el

[16] Indicador monetario de los bienes y servicios que adquieren los consumidores y son producidos en un país por un periodo establecido, por lo que permite conocer la riqueza que genera un país.

[17] A través de esta resolución el Ministerio de Tecnologías de la Información y Comunicaciones adicionó el artículo 1. de la Resolución 002108 del 2020, COLCERT, para articular y coordinar la ciberseguridad nacional del sector público y privado.

uso de herramientas digitales para guardar la información estratégica en las redes informáticas (Mindefensa, 2022).

En los últimos años en el país la ciberdefensa y la seguridad de la información ha llegado hasta un alto nivel de desarrollo que el Ministerio de Defensa apoya de forma continua las capacitaciones y la formación de los profesionales en el conocimiento y la adquisición de nuevas tecnologías para el sector Defensa (Gómez et al, 2020).

[T1] Desarrollo del objetivo

2. Prácticas actuales de seguridad digital de las Fuerzas Militares en Colombia y de países a nivel mundial.

Todo tipo de Estado debe ser responsable de desarrollar estrategias y acciones que permitan la satisfacción de las funciones básicas que garanticen la idoneidad de los ciudadanos y su protección, salvaguardar su información y procurar su Defensa ciudadana, entre las principales acciones están las estrategias de la educación, la salud, la justicia, la seguridad social, además, la comunicación, el transporte, la seguridad y la defensa. Por lo tanto, los diferentes gobiernos deben interactuar por medio de la integración y la coordinación con los gobiernos, organismos y con organizaciones privadas, importantes para la administración y la gestión de infraestructuras, servicios e instalaciones (Londoño, 2007).

Esto es igualmente importante para hacer frente a las amenazas, como una cuestión individual de cada estado y de manera colectiva, con los estándares de seguridad

cibernética tanto a nivel nacional como a nivel mundial. Entre las diferentes acciones y estrategias se tienen las iniciadas por la Unión Internacional de las Comunicaciones (UIT), la Organización de las Naciones Unidas especializada en las Tecnologías de Información y Comunicación, que desarrollan programas de seguridad adhiriendo una gran cantidad de miembros y Estados para velar por la seguridad nacional e internacional, siempre con el enfoque de minimizar la vulnerabilidad de la información (Ospina & Sanabria, 2020).

La UIT es líder en la materia y desarrolla un modelo de legislación de seguridad cibernética que es compatible con las legislaciones nacionales y puede ser pasado a los diferentes miembros de la cooperación. Así, los gobiernos interactúan con diferentes agencias para la legislación y la investigación sobre los delitos cibernéticos. Entre otras estrategias está el Convenio sobre Ciberdelincuencia de Budapest, es uno de los marcos de referencia de los países para el desarrollo de las legislaciones nacionales (Ospina & Sanabria, 2020).

En estos trabajos conjuntos también se señalan las acciones de los gobiernos, de los cuerpos de policía con sus planes de contingencia, la Interpol y las diferentes organizaciones privadas, que se están constantemente actualizando para hacer frente a las amenazas y vulnerabilidad de la información. En este sentido, se puede presentar a Estados Unidos de América como el primer país en desarrollar, publicar y difundir las Estrategias de Seguridad Cibernética, desde el año 2003 (Policia Nacional, 2020).

Y desde ahí mantiene constantes estrategias y mecanismos para evitar ataques digitales sobre la información y la seguridad de la misma, entre ella mantiene la actualización de las infraestructuras de información y de comunicación. Además, implementa un software

altamente desarrollado para reducir la vulnerabilidad de los Estados Unidos de América a los ciberataques, minimizando los daños y reduciendo el tiempo de recuperación en caso de presentarse ataques cibernéticos (Candau, 2011).

Por otra parte, tiene uno de los principales organismos que hace mayor frente a la seguridad cibernética de las redes y de las infraestructuras, es el FISMA[18], que se crea como herramienta para la aplicación de un sistema de gestión de riesgos, con el fin de estandarizar procedimientos de ciberseguridad para todas las dependencias de gobierno. Una estrategia en conjunto con la creación del FISMA es la National Military Strategy for Cyberspace Operations, que describe las operaciones de las Fuerzas Militares de Estados Unidos (Cáceres, 2017).

Por otro lado, están las estrategias de Brasil, que se han presentado con un menor grado de desarrollo, pero mantiene la misma tendencia de operaciones, ante esto crea organismos que están especializados en ciberseguridad o ciberdefensa, estableciendo políticas y estrategias que garanticen la seguridad y minimicen la vulnerabilidad de la información y las operaciones. Desde 2012, Brasil estableció la Política de Defensa Cibernética, con componentes militares del poder nacional, y adjudicó otras entidades relacionadas con la Defensa o la CiberGuerra. En estos procesos se incluye al Ministerio de Defensa y acciones conjuntas con las comunidades académicas y el sector público y privado (Santos, 2022).

[18] Organismo responsable de la seguridad cibernética de las redes federales y de las infraestructuras críticas, que a su vez impulsó la creación de un sistema de gestión de riesgos para estandarizar procedimientos de ciberseguridad en las agencias de gobierno.

Esta nación, igual que Estados Unidos de América, se enfoca en los procesos y programas de integración y cooperación internacional, firmando acuerdos bilaterales y convenios de cooperación tecnológica y de producción para la Defensa. Por su parte, Argentina también sobresale en temas de seguridad criptográfica y la seguridad informática. Junto a Chile, Costa Rica, República Dominicana y México, forman parte del Convenio del Consejo de Europa en Delito Cibernético, que son organismos especializados en seguridad y/o Defensa cibernética (Santos, 2022).

En Perú, el Ejercito del Perú establece normas en relación con el tratamiento de la información y su protección, con la conformación de la Directiva Única para el Funcionamiento del Sistema de Telemática y Estadística del Ejército (DUFSITELE), que hace uso de la tecnología para el mejor funcionamiento y reporte de la información. También está la Directiva sobre los Lineamientos de Seguridad de la Información para la Ciberdefensa, que se encarga de la óptima protección de la información digital de los centros de informática del Ejército del Perú (Moreano, 2019).

A nivel nacional, las políticas de seguridad y de protección de la información digital se han establecido como las normas y disposiciones que sirven como herramientas para salvaguardar y proteger los activos críticos de información digital. Estas estrategias incluyen acciones de concientización con los colaboradores de las organizaciones, informando sobre la importancia y la sensibilidad de la información y el servicio a la institución. Se tiene personal encargado solamente para la Oficina de Tecnología, los cuales se encargan de documentar y mantener actualizadas las políticas y normas (Moreano, 2019).

Las Fuerzas Armadas de Colombia realizan evaluaciones periódicamente sobre los funcionarios y estrategias implementadas, para validar su efectividad y poder definir las modificaciones más importantes para garantizar el cumplimiento. Las Fuerzas Armadas de Colombia utilizan los sistemas informáticos y la plataforma tecnológica de "La Agencia Logística De Las Fuerzas Militares" con el fin de mantener vínculos claros y activos de los medios digitales, como el correo, las redes de Internet y de Intranet[19]. Esta implementación de los sistemas y plataformas tecnológicas mantienen la privacidad y confidencialidad de los datos propios de la Entidad y la ciudadanía, incluyendo también un control y manejo de programa de virus, para revisión periódica de los equipos de cómputo (Santos, 2022).

Adicionalmente, se realizan operaciones de instalación de software bajo fuentes externas, y la descarga de documentos desde la Intranet o Internet, que tenga instalado un software para la detección de virus en los recursos tecnológicos de la Institución. Y está prohibido instalar cualquier tipo de software o programa no autorizado por la Oficina de Tecnología de la Agencia (Gómez et al, 2020).

La Institución de las Fuerzas Armadas en Colombia cuenta con una estructura de la organización con funciones de responsabilidad para velar por la seguridad de la información y los datos. En temas de informática, en la Institución se mantiene la centralización de todas las acciones que están relacionadas con la Seguridad de la Información de la Entidad. Estableciendo internamente las políticas, normas y los

[19] Plataforma digital privada que tiene el objetivo de apoyar a los colaboradores de una organización para que hagan uso de contenidos, archivos, herramientas, que ayuden a la comunicación segura, el trabajo en equipo y la generación de valor.

procedimientos de Seguridad de la Información, controlando desde esta instancia todas las actividades de control y acceso, el monitoreo de los sistemas informáticos y la capacitación de los usuarios (Santos, 2022).

Esta entidad ha creado equipos de emergencia ante la presencia de los incidentes de seguridad, para poder dar respuesta rápida y eficiente a los ataques de virus, a las intrusiones y la recuperación de información y rastreo de las posibles nuevas intrusiones. Para estas gestiones se tiene el Grupo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT, que es el organismo encargado a nivel nacional para atender los temas de ciberseguridad y ciberdefensa (Cortés, 2015).

También El Comando Conjunto Cibernético de las Fuerzas Militares – CCOCI que se encuentra dirigido por el Comando General de las Fuerzas Militares, asigna las funciones dentro de las Fuerzas Militares de Colombia de acuerdo a las especialidades, este grupo tiene el fin de prevenir y poder contrarrestar las amenazas y los ataques de naturaleza cibernética (Cortés, 2015).

Adicionalmente, El Centro Cibernético Policial – CCP, que se ocupa de la ciberseguridad del territorio colombiano, esta institución ofrece información, redes de apoyo y de protección sobre los delitos cibernéticos y desarrollan labores de prevención, asistencia, investigación y de judicialización de los delitos informáticos que se cometen en el país, dicho grupo tiene un trabajo conjunto con el COLCERT (Cortés, 2015).

En el país también se han implementado estrategias de fortalecimiento de ciberseguridad y ciberdefensa, con mecanismos de cooperación internacional y la adhesión a diferentes

instrumentos de carácter internacional, y para estas gestiones, el gobierno ha destinado altos presupuestos, por encima de los $16 mil billones de pesos, y que establece también la asignación de una agencia de vigilancia que trabaja de la mano con los grupos y comandos de la Policía Nacional y el Ejército Nacional para los temas de ciberseguridad (Policia Nacional, 2020).

En la actualidad, los cuerpos de Ejército a nivel nacional e internacional le están apostando a las estrategias con Inteligencia Artificial, esto como respuesta al acelerado desarrollo tecnológico y a la implementación de herramientas digitales e innovadoras para el desarrollo de diversas operaciones en todos los campos de acción. Con la Inteligencia Artificial los grupos militares pueden identificar patrones ocultos y amenazas en contra de la información, les permite actuar de forma oportuna y eficiente, manteniendo segura la información y protegiendo los datos de los ciudadanos (Pardo, 2024).

[T1] Desarrollo del objetivo

3. Acciones de mejora para la gestión de seguridad digital de las Fuerzas Militares de Colombia y garantizar la protección del Derecho a la Información a los ciudadanos.

La gestión de seguridad digital ha representado un reto para las Fuerzas Militares de Colombia, que a su vez ha implicado la toma de decisiones informadas para emprender estrategias y proyectos, como consecuencia de esto se conoce de la prevalencia de acciones

normativas en asuntos de contrataciones, acceso y uso de herramientas; lineamientos de política pública fundamentados en el CONPES; además de la creación de Unidad de Gestión General, la Dirección de Justicia Penal Militar y las Fuerzas Militares de Colombia; investigaciones y capacitación a profesionales; creación de sistemas más seguros y resistentes a los ciberataques. Sin embargo, se debe considerar que estas acciones no han sido suficientes para lograr una mayor confianza digital y se tiene como principal acción de mejora una amplia inclusión de las instituciones interesadas en garantizar la seguridad digital para que participen en la evaluación de la problemática y en las posibles soluciones (Departamento Nacional de Planeación, 2020).

Así mismo, es indispensable la creación de programas de seguridad en las que participen varios miembros y Estados interesados tanto por la seguridad nacional como mundial, impulsados a la vez por la reducción de la vulnerabilidad de los datos (Ospina y Sanabria, 2020). Algunos de estos miembros pueden ser organizaciones privadas o públicas como la INTERPOL, las cuales deben contribuir a la evaluación de la seguridad digital para gestionar las amenazas y tener fortaleza en aquellos puntos vulnerables (Policía Nacional, 2020).

En ese mismo sentido, se recomienda la inclusión del Ministerio de Defensa, comunidades académicas, y el sector público y privado a nivel nacional e internacional que puedan integrar esfuerzos en programas de cooperación internacional, acuerdos bilaterales, convenios de cooperación en tecnología, además de desarrollar soluciones innovadoras que permita una respuesta eficiente ante las ciberamenazas. Esta postura de inclusión debe implicar la participación activa para la construcción de mejores prácticas, apoyar a otros

países, y poder así recibir ayuda de otras naciones según las necesidades en seguridad (Santos, 2022).

En Colombia ya existen actualizaciones normativas para la seguridad digital, de acuerdo a como se mencionó anteriormente en el Objetivo 1. Así mismo, se han creado diferentes políticas que pueden requerir de una nueva actualización del modelo de legislación, para que se pueda garantizar la compatibilidad entre las políticas existentes y la normativa vigente. Esto también es clave para que los gobiernos encuentren un apoyo en la legislación para gestionar aquellos delitos cibernéticos que implican incumplimientos de las políticas establecidas (Ospina y Sanabria, 2020).

A partir de la experiencia de Brasil en la gestión de la seguridad digital, se recomienda en este caso, que las Fuerzas Militares de Colombia conserven el interés por crear políticas y estrategias direccionadas a garantizar la seguridad digital, y como parte del proceso de ejecución, monitoreo y evaluación, suele ser necesaria la creación de nuevas entidades que apoyen la defensa (Santos, 2022).

Complementario a lo anterior, se propone a las Fuerzas Militares de Colombia que tengan un constante compromiso con la evaluación de la seguridad digital para poder identificar oportunidades de mejora que conlleven a la actualización de las infraestructuras de información y de comunicación. Las creaciones de algunos software pueden impactar positivamente en la minimización de los daños de los ataques cibernéticos y mejorar el tiempo de recuperación después de que estos se presenten (Candau, 2011). De igual forma, se recomienda el uso de FISMA que es una herramienta que contribuye a la estandarización

de procesos de ciberseguridad para las diferentes dependencias de una institución como lo pueden ser las Fuerzas Militares de Colombia (Cáceres, 2017).

Así mismo, se recomienda la aplicación de la tecnología de cifrado de seguridad de la información en la gestión de sistemas de datos militares, esto debido a sus aportes para la protección de información sensible, por ejemplo: los planes de operaciones o comunicaciones estratégicas, otro beneficio es la integridad de los datos, seguridad en los comunicados, prevenir espionajes y cumplir con la normativa vigente (Zheng, 2017).

En este punto es relevante mencionar que la tecnología que se pueda implementar para la seguridad de la información, debe priorizar la prevención de los riesgos, es decir, con capacidad preventiva, de forma que se garantice la disponibilidad tecnológica y de servicios ante las situaciones amenazantes que se puedan presentar (Atif y Sean, 2014).

Otra de las acciones es la creación de una directiva única para el funcionamiento tecnológico que se enfoca precisamente en evaluar el funcionamiento de estas herramientas para el reporte y protección de datos, también sugiere que se cuente con un Centro de Respuesta a Incidentes Cibernéticos en donde se realicen actividades de monitoreo, identificación y respuesta ante las amenazas, y que estas se puedan gestionar con apoyo nacional e internacional (Moreano, 2019).

Como parte del compromiso de actualización en el uso de herramientas de tecnología es importante que las Fuerzas Militares de Colombia cuenten con un protocolo para la descarga de programas o software con el fin de evitar riesgos en la seguridad de la información, además que debe tener programas de antivirus (Gómez et al, 2020). Otro de

los protocolos necesarios es el de comunicación en la informática militar para garantizar la seguridad en el intercambio de datos entre sistemas militares; este documento debe también propiciar la confidencialidad, integridad y disponibilidad de la información sensible; e incluir estrategias sólidas para fortalecer los canales de comunicación contra las ciberamenazas en evolución (Kumar, 2024).

Otro de los avances significativos a nivel mundial de la tecnología es la Inteligencia Artificial por lo que se sugiere a las Fuerzas Militares de Colombia que profundicen en este conocimiento para que puedan implementar mejores prácticas que ayuden a la seguridad digital de una forma más rápida, efectiva, segura y en menor tiempo, esto es viable en los enfoques de detección de amenazas, autenticación, protección de datos, gestión de redes, vigilancia, simulaciones, para capacitaciones, automatización de tareas, predicciones, entre otros (Pardo, 2024).

No obstante, es importante que las Fuerzas Militares de Colombia sean conscientes de que el uso de la Inteligencia Artificial también genera riesgos y amenazas para la misma seguridad de la información, por lo que deben ser cuidadosos en el diseño y codificación en el uso de esta tecnología. También deben crear unos criterios éticos en el manejo de esta tecnología (Jayakumar et al, 2021).

En este punto es relevante recomendar que las Fuerzas Militares de Colombia deben brindar capacitaciones a sus miembros para que puedan actualizar sus conocimientos con base a la nueva legislación, políticas, programas, estrategias, y herramientas tecnológicas, logrando así garantizar el correcto manejo y cumplimiento por parte de los profesionales (Moreano, 2019). Estas capacitaciones deben brindar un aprendizaje multidisciplinar de alta

especialización, por lo que las instituciones deben realizar cambios disruptivos para poderlo lograr, siendo capacitación online una oportunidad de acceso a la formación cibernética (González, 2019).

Adicionalmente, se recomienda que las Fuerzas Militares de Colombia puedan fortalecer la formación híbrida por varios factores, en un primer momento porque ante la presencia de una pandemia o dificultades de desplazamiento, no hay obstáculos para capacitarse; y en la presencialidad pueden acceder a laboratorios para experimentar lo aprendido en la teoría. Así mismo, es necesario capacitar a los militares en el desarrollo de habilidades de cooperación civil-militar que hacen parte de las principales tendencias a nivel mundial para la seguridad de la información. También, se recomienda a la institución en mención que al igual que se deben actualizar la normativa, políticas y estrategias, estos programas de formación también deben hacerlo, tanto en los contenidos que se enseñan como en las técnicas que se emplean, considerando que los avances educativos sugieren el aprovechamiento de herramientas como la gamificación y las que brinda la Inteligencia Artificial generativa (Cambria y Marchisio, 2023).

Se recomienda que al igual y como lo hacen en las academias militares de Estados Unidos de América, en Colombia se debe buscar la formación con un enfoque para que los líderes militares sean líderes ciberestratégicos y con sus conocimientos puedan aportar a la toma de decisiones para la seguridad de la información (Spidalieri y McArdle, 2016).

Además de las capacitaciones, es importante que las Fuerzas Militares de Colombia fortalezcan el sistema de evaluación periódico de las estrategias implementadas para la seguridad digital, este compromiso es significativo para analizar el cumplimiento de

objetivos, riesgos, establecer acciones de mejora y ejecutarlas para mejorar así la seguridad digital. Así mismo, se debe evaluar el funcionamiento de los equipos de cómputo y demás herramientas de tecnología para evitar la presencia de virus y aportar seguridad (Santos, 2022).

La seguridad digital es un compromiso exigente de garantizar por parte de las Fuerzas Militares de Colombia, por lo que en un principio se requiere del acceso a recursos económicos suficientes para poder garantizar la financiación de las estrategias que deben integrar la tecnología militar, la biotecnología, la realidad virtual, la estrategia militar, el contexto geopolítico, capacidades de combate y considerar la evolución de la demografía (Trad, 2022).

Marco teórico

Uno de los principales líderes en seguridad digital es Greg Young, quien se encuentra especializado en seguridad institucional. Esta persona ve la seguridad digital como un elemento de gran importancia para las empresas y organizaciones, es una acción de protección ante las amenazas de delincuentes que pueden utilizar software para los ataques de ransomware o cryptojacking y, por lo tanto, los sistemas de control digitales para las ciber amenazas se han enfocado sistemas sofisticados ante los ataques de Estados - Nación. El señor Young se enfoca en estudios de la seguridad de redes, tendencias de amenazas, la seguridad de datacenters, seguridad de redes en la nube y la microsegmentación. Adicionalmente, comparte su experiencia con la creación de cuadrantes sobre firewall, IPS, WAF y UTM y como Oficial en la policía militar, lidera procesos y proyectos de

contrainteligencia y desarrollo la seguridad de tarjetas inteligentes (IT Digital Security, 2022).

Por su parte, el señor Félix Arteaga es el principal investigador del Real Instituto Elcano y del Instituto de Cuestiones Internacionales y Política Exterior (INCIPE), es especialista en la Seguridad Interior de la Guardia Civil, considera la seguridad digital como una de las estrategias y alternativas que sirven para mejorar los riesgos habituales de la seguridad en diferentes espacios y considera que es indispensable las políticas en seguridad militar y de defensa a través de un trabajo cooperativo de las naciones para protección civil y de los ataques sobre la Fuerza Pública. Expone que es importante los adelantos y las declaraciones sobre Seguridad y Defensa de las regiones para que contribuyan a la estabilidad (Ministerio de Defensa, 2023).

Por último, Barry Buzan quien es un gran exponente en el estudio de los medios estratégicos de la tecnología militar y las Relaciones Internacionales, define la seguridad digital en el campo militar como la dominación de lo militar y la dependencia de la tecnología de subordinación que se adaptan para asumir las amenazas y ataques que provocan los delincuentes. Este autor resalta la importancia y el uso efectivo de los armamentos como uno de los avances de la tecnología militar como una representación de las relaciones anormales entre las naciones, ante los debates políticos y el potencial militar adversario, reconociendo que los medios militares y la tecnología en este campo son también problemas de seguridad, por los armamentos nucleares que se utilizan para Defensa y protección de la sociedad en los conflictos militares (Sisco & Chacón, 2004).

[T1] Conclusiones

Las Fuerzas Militares de Colombia tienen como principales compromisos: 1. Defender la Soberanía, 2. Independencia, 3. Integralidad del Territorio y del 4. Orden Constitucional, para lograrlo, han empleado herramientas tecnológicas que contribuyen a una gestión efectiva, sin embargo, el uso de este tipo de estrategias a su vez ha implicado riesgos en la seguridad de la información por los actos de grupos delictivos. Ante este escenario, la Institución ha implementado diferentes tipos de estrategias a través de políticas públicas como: 1. CONPES 3701 de los "Lineamientos de política para la Ciberseguridad y Ciberdefensa" del año 2011, 2. CONPES 3854 llamado "Política Nacional de Seguridad Digital" del año 2016; 3. Desarrollo de la Unidad de Gestión General, la 4. Dirección de Justicia Penal Militar y las Fuerzas Militares de Colombia, 5. Grupo Interno de Trabajo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT; fortalecimiento de la normatividad sobre contrataciones, régimen disciplinario y acceso y uso de las herramientas tecnológicas; investigación, desarrollo e innovación; y también han implementado las capacitaciones a los profesionales para la adquisición de nuevas competencias.

Al igual que las Fuerzas Militares de Colombia se han interesado en implementar prácticas para la seguridad de la información, también lo han hecho otros países a nivel mundial resaltando estrategias como la inclusión de diversos miembros y estados para el análisis y toma de decisiones en seguridad nacional e internacional; se han realizado esfuerzos para que la legislación sean compatibles con las políticas, proyectos y estrategias existentes; otras actividades han sido los esfuerzos por implementar actualizaciones de las infraestructuras de información y comunicación como el sistema de gestión de riesgos para

estandarizar procedimientos de ciberseguridad; se han creado organismos que están especializados en ciberseguridad o ciberdefensa; la cooperación internacional también ha sido clave para la creación de acuerdos bilaterales y convenios de cooperación tecnológica y de producción para la defensa.

A partir del análisis realizado sobre la gestión de seguridad digital de las Fuerzas Militares de Colombia y las prácticas implementadas en otros países, se identificaron acciones de mejora para esta Institución las cuales se fundamentan en mejorar la inclusión de otros miembros y entidades para la toma de decisiones informadas, actualización de la legislación para que sea coherente con los proyectos y políticas existentes, crear nuevos departamentos o entidades que apoyen la defensa, fortalecer las acciones de evaluación de la seguridad digital para implementar acciones de mejora, crear programas o software que se adapten a las exigencias o necesidades de la institución, tecnología de cifrado de seguridad, prevención de los riesgos, protocolos para la descarga de programas o software y para la comunicación en la informática digital, aprovechar la Inteligencia Artificial pero también tener un enfoque de prevención por los riesgos que genera, fortalecer el proceso de capacitación a través de la formación digital o híbrida orientada al desarrollo de habilidades de cooperación civil-militar para que sean líderes ciberestratégicos, y garantizar el acceso a los recursos económicos suficientes para la ejecución de estas estrategias.

Se concluye que las Fuerzas Militares de Colombia es una institución reconocida a nivel mundial por sus buenas prácticas para garantizar la seguridad digital, sin embargo, el rápido avance que han tenido las técnicas para los ataques cibernéticos aumenta la necesidad de mejoramiento continuo y de actualización de las prácticas. En esta investigación se sugieren una serie de cambios, prevaleciendo el uso de herramientas tecnológicas que se

adapten a las necesidades específicas de la institución, y la capacitación para que los militares puedan manejarlas y ser líderes ciberestratégicos. Por último, se hace necesario que estas prácticas estén en constante evaluación para verificar su pertinencia e identificar nuevas oportunidades de mejora.

[T1] Referencias

AS Colombia. (2021). Anonymous en Colombia: Cuál ha sido su último movimiento y qué más planean hacer. https://colombia.as.com/colombia/2021/05/06/actualidad/1620334033_976860.html

Atif, A. y Sean, M. (2014). Information security strategies: towards an organizational multi-strategy perspective. Journal of Intelligent Manufacturing, 25, 357–370. https://link.springer.com/article/10.1007/s10845-012-0683-0

BBC. (2011). El FMI estuvo bajo ataque cibernético. https://www.bbc.com/mundo/noticias/2011/06/110612_1014_tecnologia_fmi_ciberataque_dc

Cáceres, J. (2017). *Colombia, estrategia nacional en ciberseguridad y ciberdefensa.* Ejercito de Colombia.

Candau, J. (2011). Estrategias nacionales de ciberseguridad, ciberterrorismo. Dialnet.

Chillier, G., & Freeman, L. (2005). El Nuevo Concepto de Seguridad Hemisférica de la OEA: Una Amenaza en Potencia. Oficina en Washington para Asuntos Latinoamericanos .

Cortés, R. (2015). Estado actual de la política pública de ciberseguridad y ciberdefensa en Colombia. *Revista de Derecho, comunicaciones y nuevas tecnologías*(14). doi:Dialnet-EstadoActualDeLaPolitcaPublicaDeCiberseguridadYCib-7496888.pdf

Departamento Nacional de Planeación. (2011). Lineamientos de política para ciberseguridad y ciberdefensa. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

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

Gómez, C. A., May, L., & Franco, C. W. (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.

González de Escalada, C. (2019). Online distance learning as a factor of disruptive innovation in military education. Campus Virtuales, 8(1), 87-98. https://redined.educacion.gob.es/xmlui/bitstream/handle/11162/184562/Art.%207.pdf?sequence=1&isAllowed=y

Hernández Sampieri, R. (1991). *Metodología de la investigación.* McGraw-Hill Interamericana de México.

Hernández Sampieri, R. (2014). *Metodología de la investigación.* Mc Graw Hill.

Hernández Sampieri, R., Fernández, C., & Baptista, P. (2006). *Metodología de la investigación.* McGraw-Hill Interamericana.

IT Digital Security. (24 de Enero de 2022). Éstos son los principales riesgos que asume un entorno industrial inseguro. Obtenido de IT Digital Security: https://www.itdigitalsecurity.es/actualidad/2020/01/estos-son-los-principales-riesgos-que-asume-un-entorno-industrial-inseguro

Jayakumar, P.; Nawaz, S. y Jhanjhi, N. (2021). Artificial Intelligence and Military Applications: Innovations, Cybersecurity Challenges & Open Research Areas. Preprints. https://www.preprints.org/manuscript/202108.0047/v1

Kumar, R. (2024). Securing communication protocols in military computing. Network Security, (4). https://www.magonlinelibrary.com/doi/abs/10.12968/S1353-4858%2824%2970011-7

Londoño, M. (2007). Deberes y derechos procesales en el estado social de derecho. *Opinión Jurídica*, *6*(11). doi:http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1692-25302007000100004

López, J. O. (2022). De las tecnologías para la guerra a la guerra por la tecnología. *Revista de Relaciones Internacionales, Estrategia y Seguridad, 17*(2), 7-12. doi:https://www.redalyc.org/journal/927/92775579001/html/

Mindefensa. (2022). Política de Seguridad, Defensa y Convivencia Ciudadana. Ministerio de Defensa nacional.

Ministerio de Defensa. (2023). Hacia una política de cooperación en seguridad y defensa con Iberoamérica. Centro Superior de Estudios de la Defensa Nacional.

Miranda, B. (2011). Julian Assange: así fue la gran filtración de documentos clasificados en 2010 por la que EE.UU. pide la extradición del fundador de WikiLeaks. https://www.bbc.com/mundo/noticias-internacional-47902652

Moreano, L. A. (2019). Empleo de la inteligencia para contrarrestar la corrupción en las entidades públicas y privadas del perú. Escuela Militar de Chorrillos "CRL FRANCISCO BOLOGNESI".

ONU. (2023). *Influencia de las tecnologías digitales*. Obtenido de Organización de las Naciones Unidas: https://www.un.org/es/un75/impact-digital-technologies

Orozco Donado, M.I. (2011). Técnicas utilizadas por delincuentes informáticos para realizar fraudes via medios electrónicos. Universidad Piloto de Colombia. https://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/7100/Art%c3%adculoMarthaOrozco.pdf?sequence=1&isAllowed=y

Ospina, M. R., & Sanabria, P. E. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. *Revista Criminalidad, 62*(2). doi:http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082020000200199

Pardo, J. (10 de diciembre de 2024). *Las Fuerzas Militares de Colombia ahora apuestan por la revolución de la inteligencia artificial*. Obtenido de Infobae: https://www.infobae.com/colombia/2023/12/10/las-fuerzas-militares-de-colombia-ahora-apuestan-por-la-revolucion-de-la-inteligencia-artificial/

Policia Nacional. (2020). Estrategia Institucional para la seguridad ciudadana: Plan nacional de vigilancia comunitaria por cuadrantes (PNVC). Policia Nacional de Colombia.

Ramírez, A. (2003). Estructura organizacional y legal de las Fuerzas Militares y su sistema de escalafonamiento. Congreso de la República De Colombia .

Santos, M. D. (2022). Marco regulatorio de la ciberseguridad y ciberdefensa dentro de la sociedad de la información y el conocimiento. Universidad Andina Simón Bolívar.

Sisco, C., & Chacón, O. (2004). Barry Buzan y la teoría de los complejos de seguridad. *Revista Venezolana de Ciencia Política (25), 125-146.* doi:http://www.saber.ula.ve/bitstream/handle/123456789/24849/articulo7.pdf;jsessionid=8179ABF6A5E45F9E4803CD8F61095773?sequence=2

Spidalieri, F. y McArdle, J. (2016). Transformar a la próxima generación de líderes militares en líderes ciberestratégicos: el papel de la educación en ciberseguridad en las academias militares de EE. UU. La revisión de la defensa cibernética, 1 (1). https://www.jstor.org/stable/26267304?seq=1

UIAF. (2022). *Evaluación Nacional del Riesgo de Lavado de Activos, Financiación del Terrorismo y Proliferación de Armas de Destrucción Masiva.* Unidad de Información y Análisis Financiero.

Vigoya González, A.M. (2024). Ataques de ransomware más relevantes en los últimos cinco añosque han afectado a las organizaciones colombianas. (Tesis de posgrado, Universidad Nacional). https://repository.unad.edu.co/jspui/bitstream/10596/61622/1/5317088.pdf

Zheng, X. (2017). The Application of Information Security Encryption Technology in Military Data System Management. *Conference paper, 423–428.* https://link.springer.com/chapter/10.1007/978-981-10-6232-2_49